Mathematische Zeitschrift manuscript No.
(will be inserted by the editor)

J.William Helton · Scott McCullough · Mihai Putinar

Strong Majorization in a Free $*-$ Algebra

Received: date / Revised: date

Abstract We study, in the spirit of modern real algebra, the interplay between left ideals of the free $*$-algebra $\mathbb{F}$ with n generators, and their suitably defined zero sets; and similarly between quadratic submodules of $\mathbb{F}$ and their positivity sets.

Mathematics Subject Classification (2000) 46A55, 06F25, 41A63

Keywords Positivstellensatz · Nullstellensatz · Free $*$-algebra

1 Introduction

The present note is a continuation of our study of positivity in a free $*$-algebra [6], by further exploring Nullstellensätze and Positivstellensätze phenomena. The parallel to the well known analogous commutative statements is striking: the free algebra framework has sometimes simpler statements (for instance no need of higher powers in the generic Nullstellensatz) and straightforward proofs (based on elementary convexity techniques rather than Tarski's principle). This is partially explained by the great flexibility of the finite dimensional representations of the free $*$-algebra, which replace the more rigid point evaluations in the commutative case.

Partially supported by grants from the National Science Foundation and the Ford Motor Co.

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

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

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

Let $p(x,x^*)$ be a non-commutative polynomial in the free variables (with involution) $(x,x^*) = (x_1,\dots,x_n,x_1^*,\dots,x_n^*)$. Already the zero set of a p has a variety of meanings when evaluating on an n-tuple of real $d \times d$ matrices X, and possibly on a vector $v \in \mathbb{R}^d$:
(i) $\{X : p(X) = 0\}$,
(ii) $\{X : p(X)$ is not an invertible matrix $\}$, or
(iii) $\{(X,v) : \ p(X)v = 0\}$.
There are corresponding levels of notions involving positivity.

Our principal aim is to develop the third concept of zero set; the only existing result being what we call the Bergman Nullstellensatz, since it was proved by G. Bergman, see [5], after being conjectured by the authors of [5]. Besides their intrinsic interest and timely discovery, the results contained in this note have potential applications to modern system theory.

1.1 Definitions

We recall here some terminology and basic notations. There are several areas of mathematics involved and we try to use terminology which is easily learned by all but tilt toward the conventions of Marshall [10] and the references [2] [7].

Throughout this note $\mathbb{N}$ stands for the set of natural numbers and $\mathbb{R}$ for the field of real numbers. We consider variables $x = (x_1,...,x_n)$, $x^* = (x_1^*,...,x_n^*)$ and the free algebra $\mathbb{F} = \mathbb{R}\langle x,x^*\rangle$. We equip $\mathbb{F}$ with the canonical $\mathbb{R}$-linear involution:

$$(x_k)^* = x_k^*, \quad (x_k^*)^* = x_k, \ \ 1 \le k \le n,$$

and $(fg)^* = g^*f^*$, $\ f,g \in \mathbb{F}$. A word in the variables (x,x^*) will sometimes be called a *monomial*. A word $w(x)$ depending only on the x variables will be called *analytic*; an analytic polynomial in $\mathbb{F}$ is a linear combination of analytic words. We denote by $\mathbb{A}$ the subalgebra of analytic polynomials of $\mathbb{F}$. Note that $\mathbb{A}$ is not closed under the involution. Let I be a left ideal of $\mathbb{F}$. The associated *symmetrized subspace* is

$$\mathrm{sym}(I) = \{f + f^*;\ f \in I\}.$$

If $p = \{p_1,...,p_m\} \in \mathbb{F}^m$ is a set of polynomials, then we denote by $\mathbb{F}p = \mathbb{F}p_1 + ... + \mathbb{F}p_m$ the left ideal generated by p_j.

The algebra $\mathbb{F}$ carries an important intrinsic order given by the cone of sums of squares. A *sum of squares* (SOS) σ is, as the name suggests, an expression of the form

$$\sigma = \sum_{j=1}^{N} s_j^* s_j, \tag{1}$$

where each $s_j \in \mathbb{F} = \mathbb{R}\langle x,x^*\rangle$, and N is a natural number. The set of all sums of squares in $\mathbb{F}$ is customarily denoted by Σ^2. It is a convex cone, the smallest positivity cone in the $*$-algebra $\mathbb{F}$.

A polynomial p is symmetric if $p = p^*$. The linear space of all *symmetric polynomials* will be denoted by $\mathrm{sym}\mathbb{F}$. If also σ is a sum of squares as in equation (1) and if p is a symmetric polynomial, define

$$\sigma \star p = \sum s_j^* p s_j.$$

We will evaluate polynomials f in $\mathbb{F}$ to n-tuples of matrices. Specifically, if $X = (X_1,\dots,X_n) \in M_d(\mathbb{R})^n$ is a set of $d \times d$ real matrices, we denote by X^* the corresponding adjoints (i.e. transposes), and set $f(X,X^*)$ to be the corresponding $d \times d$ matrix. We will freely interpret $f(X,X^*)$ as a linear operator on $\mathbb{R}^d$. The notation $f(X,X^*) \geq 0$ means non-negativity in the operator sense.

The *zero set* of a left ideal $I \subset \mathbb{F}$ is by definition

$$V(I) = \{(X,v) \in \bigcup_{d\geq 1}(M_d(\mathbb{R})^n \times \mathbb{R}^d);\ \ v \neq 0,\ f(X)v = 0,\ \text{ all } f \in I\}.$$

We use the same notation $V(S)$ for the common zero set of all polynomials belonging to a set $S \subset \mathbb{F}$. As an obvious observation, (X,v) is a zero of $\sigma = \sum s_j^* s_j \in \Sigma^2$ if and only if (X,v) is a zero of each s_j.

Let $S \subset \mathrm{sym}\mathbb{F}$. The *positivity set of S* is by definition

$$K_S = \{(X,v) \in \bigcup_{d\geq 1}(M_d(\mathbb{R})^n \times \mathbb{R}^d);\ \ v \neq 0,\ \langle f(X)v,\ v\rangle \geq 0,\ \text{ all } f \in S\}.$$

The *quadratic module* associated to a set $S \subset \mathrm{sym}\mathbb{F}$ is

$$M_S = \{\sum_i h_i^* f_i h_i;\ f_i \in S \cup \{1\},\ \ h_i \in \mathbb{F}\}.$$

By definition, a quadratic module M_S is *archimedean* if there exists $C > 0$ with the property $C^2 - x_1^* x_1 - \ldots - x_n^* x_n \in M_S$. In particular, but not equivalently, there exists a C such that if $s(X)$ is positive semidefinite for all $s \in S$, then $\|(X_1,\dots,X_n)\| \leq C$. Operator theorists often call a cone with this type of property *absorbing*. More specifically, this means for a convex cone $M \subset \mathbb{F}$ that the element 1 belongs its *algebraic interior*: for every $f \in \mathbb{F}$ there exists $\lambda > 0$ with the property $1 + \lambda f \in M$. In the context of the algebra $\mathbb{F}$ and assuming that the convex cone contains all sums of squares and is closed with respect to conjugations there is no distinction between archimedean and absorbing which is readily proved starting from the observation that $C^2(C^2 - ww^*) = (C^2 - ww^*)^2 + w(C^2 - w^* w)w^*$.

One of the basic technical lemmas involved in all recent proofs pertaining to positivity aspects in a free $*$-algebra is a Minkowski separation argument. We isolate it below for the convenience of the reader.

Lemma 1 *Suppose $M \subset \mathbb{F}$ is closed with respect to positive linear combinations; i.e., if $p,q \in M$ and $s,t > 0$, then $sp + tq \in M$. If 1 belongs to the algebraic interior of M, if C is a convex cone and $C \cap M \subset \{0\}$, then there exists a linear functional $L : \mathbb{F} \longrightarrow \mathbb{R}$ such that*

$$L(q) \leq 0 \leq L(p),\ \ q \in C,\ \ p \in M,$$

and $L(1) > 0$.

Proof Let $S = C - M + 1$. Then S is a convex set. The hypothesis that 1 is an algebraic interior point of M implies that S is absorbing: given $f \in \mathbb{F}$ there exists $t > 0$ so that $1 + t(-f) \in M$ so that $tf \in -M + 1 \subset C - M + 1$. Consequently it makes sense to talk of the Minkowski functional p of S so that $p(x) = \inf\{t > 0 : \frac{x}{t} \in S\}$. In particular, $p(1) \geq 1$.

Define $\lambda(t1) = t$ on the one dimensional subspace of $\mathbb{F}$ spanned by 1. One readily checks that $|\lambda(t1)| \leq p(t1)$ and hence λ extends to a linear functional L on $\mathbb{F}$ satisfying $L \leq p$. In particular $L \leq 1$ on S.

For $m \in M$ and $c \in C$,

$$L(c) - L(m) + 1 = L(c - m + 1) \leq p(c - m + 1) \leq 1.$$

Hence $L(c) \leq L(m)$.

Because C is a cone it follows that $L(C) \leq 0 \leq L(M)$ and at the same time $L(1) = 1 > 0$. □

The discovery of this result goes back to Eidelheit and Kakutani (see for instance [8] §17.1(3)). In this form it is due to Koethe. Its versatility was independently remarked by M. Krein [9].

1.2 Outline of Results

We give five classes of results.

- Section 2 concerns a non-commutative polynomial q which is nonnegative on the zero set $V(p)$ of a set of analytic polynomials $p_1, \cdots, p_m$. Our proof relies on an extension lemma for tuples of matrices.
- In section 3 we propose an abstract Bergman type Nullstellensatz. Key here is that zero sets involve tuples of operators on finite dimensional spaces of all dimensions. Notably this produces a radical free Nullstellensatz of interest in the commutative case.
- Section 4 gives a sums of squares criteria for hereditary polynomials (those with adjoint/transpose variables all to the left of the untransposed variables) involving zero sets of tuples of commuting matrices.
- Section 5 gives a Nullstellensatz for arbitrary polynomials. However, we pay for this generality by getting an approximate formula. Again zero sets based on finite dimensional matrix spaces suffice.
- The last section, see Section 6, concerns the behavior of a polynomial q on a "noncommutative semialgebraic set". In this section the results demand consideration of tuples of bounded operators X on a possibly infinite dimensional space rather than only tuples of matrices. Also the last topic requires an archimedean assumption, while the others do not.

The title of this paper reflects that $\langle f(X)v, v\rangle \geq 0$ implies $\langle g(X)v, v\rangle \geq 0$ is a stronger statement than $f(X)$ is positive semidefinite implies $g(X)$ is positive semidefinite.

2 A Nichtnegativstellensatz on "Analytic Varieties"

We use the notation and conventions introduced in the preceding section.

Theorem 1 (Nichtnegativstellensatz). *Let $p \in \mathbb{A}^m$ and assume that $q \in \mathrm{sym}\mathbb{F}$ satisfies $V(p) \subset K_{\{q\}}$. Then*

$$q \in \Sigma^2 + \mathrm{sym}(\mathbb{F}p).$$

If in addition, $\langle q(X)v, v\rangle = 0$, for every $(X, v) \in V(p)$, then $q \in \mathrm{sym}(\mathbb{F}p)$.

The following fact, of independent interest, appears as a necessary step in the proof of the preceding result.

Theorem 2 (Nullstellensatz). *Let $p \in \mathbb{A}^m$ and $q \in \mathbb{F}$. If $V(p) \subset V(q)$, then $q \in \mathbb{F}p$.*

Note that in the latter theorem q need not be symmetric.

The strategy and main parts of the proof of Theorem 1 are modeled after those in [6], and we will not repeat them. Instead, we will simply point out the novelty needed to treat the more general situation covered by the new Nichtnegativstellensatz. First we will need to prove Theorem 2. Towards this end we start with an operator extension lemma.

Lemma 2 *Let $x = \{x_1,\dots,x_n\}$, $y = \{y_1,\dots,y_n\}$ be free, non-commuting variables. Let H be a finite dimensional Hilbert space, and let X be an n-tuple of linear operators acting on H. Fix a degree $d \geq 1$ and let Z be the set of all words in x,y, starting to the right with a y_j, $1 \leq j \leq n$, and of degree at most d.*

Then there exists a larger finite dimensional Hilbert space $H \subset K$, an n-tuple of linear transformations $\tilde{X}$ acting on K, such that

$$\tilde{X}_j|_H = X_j, \;\; 1 \leq j \leq n,$$

and the subspaces

$$z(\tilde{X},\tilde{X}^*)H = \{z(\tilde{X},\tilde{X}^*)u;\; u \in H\}$$

are linearly independent; that is for every choice $\{u_z : z \in Z \cup \{1\}, u_z \in H\} \neq \{0\}$ (i.e., for each nonzero function $u : Z \cup \{1\} \to H$) the set

$$\{z(\tilde{X},\tilde{X}^*)u_z, \;\; z \in Z \cup \{1\}\},$$

is linearly independent.

Proof As a matter of notation, let $|w|$ denote the length of a word w and let $\mathscr{F}_d$ denote the polynomials in $\mathbb{F}$ of degree at most d. View $\mathscr{F}_d$ as a the Hilbert space with orthonormal basis the words of length at most d. Let $K = \mathscr{F}_d \otimes H$. Identify H isometrically as a subspace of K via the embedding $h \mapsto 1 \otimes h$. More generally, let H_j denote the span of $\{w \otimes h : |w| = j, h \in H\}$. With this notation, $H = H_0$ and $K = \oplus_{j=0}^{d} H_j$.

The extended operators $\tilde{X}_j : K \longrightarrow K$ will have a three diagonal $(d+1)\times(d+1)$ block-matrix structure:

$$\tilde{X}_j = \begin{pmatrix} X_j & A_j(1)^* & 0 & 0 & \dots \\ 0 & 0 & A_j(2)^* & 0 & 0 \\ 0 & B_j(2) & 0 & A_j(3)^* & \ddots \\ 0 & 0 & B_j(3) & 0 & \ddots \\ \vdots & \ddots & \ddots & \ddots & \ddots \end{pmatrix}.$$

The linear operators $A_j(k), B_j(k) : H' \longrightarrow H'$ will be chosen later. This construction assures the validity of the first requirement in the statement: if $w(x)$ is a monomial (i.e. word) in the variables x, and $u \in H$, then

$$w(\tilde{X})u = w(X)u.$$

Let $z(x,y) = z_{i_m} z_{i_{m-1}} ... z_{i_1}$ be a word in the variables x, y, that is $i_1, i_2, ..., i_m \in \{1, 2, ..., n\}$ and $z_i = x$ or $z_i = y$. Assume that the rightmost variable in the word is a y: $z_{i_1} = y_{i_1}$.

Next we evaluate $z(\tilde{X}, \tilde{X}^*)$ at a vector $u \in H \subset K$, starting to read the word z from the right. First we encounter an element of the form

$$\tilde{X}_j^* u = \begin{pmatrix} X_j^* & 0 & 0 & 0 & \dots \\ A_j(1) & 0 & B_j(2)^* & 0 & \\ 0 & A_j(2) & 0 & B_j(3)^* & \\ 0 & 0 & A_j(3) & 0 & \dots \\ \vdots & & & \ddots & \end{pmatrix} \begin{pmatrix} u \\ 0 \\ 0 \\ 0 \\ \vdots \end{pmatrix} = \begin{pmatrix} X_j^* u \\ A_j(1)u \\ 0 \\ 0 \\ \vdots \end{pmatrix}.$$

Suppose that the next operation is applying $\tilde{X}_\ell$. We obtain

$$\tilde{X}_\ell \tilde{X}_j^* u = \begin{pmatrix} \cdots \\ \cdots \\ B_\ell(2)A_j(1)u \\ 0 \\ 0 \\ \vdots \end{pmatrix}.$$

In general, starting the counting from zero, the m-th entry of $z(\tilde{X}, \tilde{X}^*)u$ will be

$$z(\tilde{X}, \tilde{X}^*)u = \begin{pmatrix} \vdots \\ C_{i_m}(m) \dots C_{i_2}(2) C_{i_1}(1)u \\ 0 \\ 0 \\ \vdots \end{pmatrix},$$

where $C_{i_k}(k) = A_{i_k}(k)$ if $z_{i_k} = y_{i_k}$ and $C_{i_k}(k) = B_{i_k}(k)$ if $z_{i_k} = x_{i_k}$ (in the word z).

We claim that one can choose the linear operators $A_j(k)$ and $B_j(k)$, so that all possible compositions

$$C_{i_m}(m) \dots C_{i_2}(2) C_{i_1}(1) : H \longrightarrow H_m, \quad (C = A \text{ or } B) \tag{2}$$

of length m $(m \le d)$ are injective and have mutually orthogonal ranges. Explicitly, define $A_j(k) : H_{j-1} \to H_j$ by $A_j(k)(w(x,y) \otimes h) = [(y_j w(x,y)) \otimes h]$ for $h \in H$ and $\deg(w) = k-1$; and similarly $B_j(k)(w(x,y) \otimes h) = [(x_j w(x,y)) \otimes h]$ for $h \in H$, $\deg(w) = k-1$.

To complete the proof, suppose $u : Z \cup \{1\} \to H$ is a nonzero function and consider the sums

$$s_j = \sum_{|z|=j} z(\tilde{X}, \tilde{X}^*) u_z$$

and $s = \sum_0^d s_j$. Note that $P_{H_d} s_d$ is a linear combination of terms like in equation (2) with products of length d. Consequently, $s_d = 0$ if and only if $u_z = 0$ for each $|z| = d$. Similar reasoning then shows that $s = 0$ if and only if $u = 0$ and the proof is complete. $\square$

Corollary 1 *Let $x = \{x_1, \ldots, x_n\},\ y = \{y_1, \ldots, y_n\}$ be free, non-commuting variables. Let H be a finite dimensional Hilbert space, and let X, Y be two n-tuples of linear operators acting on H. Fix a degree $d \geq 1$.*

Then there exists a larger finite dimensional Hilbert space $H \subset K$, an n-tuple of linear transformations $\tilde{X}$ acting on K, such that

$$\tilde{X}_j|_H = X_j, \;\; 1 \leq j \leq n,$$

and for every polynomial $p \in \mathbb{R}\langle x, y\rangle$ of degree at most d and vector $v \in H$,

$$p(\tilde{X}, \tilde{X}^*)v = 0 \;\Rightarrow p(X, Y)v = 0.$$

Proof Let $\tilde{X}$ denote a tuple of matrices as constructed in Lemma 2.

In order to prove the second statement, let us decompose the non-commutative polynomial $p(x, y)$ as follows:

$$p(x, y) = \sum_{z \in Z} z(x, y) f_z(x),$$

where $f_z(x)$ is a polynomial in the variables x and the word $z(x, y) \in Z$ starts to the right with a y_j (or is a scalar). Assume that the vector $v \in H$ satisfies

$$0 \neq p(X, Y)v = \sum_z z(X, Y) f_z(X)v.$$

In particular not all vectors $f_z(X)v \in H$ are zero; i.e., the function $u : Z \cup \{1\} \mapsto H$ given by $z \mapsto u_z = f_z(X)v$ is nonzero. From Lemma 2 it follows that

$$p(\tilde{X}, \tilde{Y})v = \sum_{z \in Z \cup \{1\}} z(\tilde{X}, \tilde{Y}) f_z(X)v \neq 0.$$

$\square$

Proof (of Theorem 2). If the polynomial q in the statement is analytic, then the result follows from the Bergman Nullstellensatz, Theorem 3 below. Because it plays a central role in the next section, and because it is needed here, we have included the proof in Section 3 below.

We will reduce the general case to q analytic, with the help of our dilation lemma. Assume that, for all $d \in \mathbb{N}$ and pairs $(X, v) \in M_d(\mathbb{R})^n \times \mathbb{R}^d$,

$$\sum_{j=1}^m \|p_j(X)v\| = 0 \;\Rightarrow q(X, X^*)v = 0.$$

Fix (X, v) such that $\sum_{j=1}^m \|p_j(X)v\| = 0$ and let $Y \in M_d(\mathbb{R})^n$ be an arbitrary n-tuple of $d \times d$ matrices. In view of the above corollary, there exists a larger (finite dimensional) space $\mathbb{R}^d \subset K$, and an n-tuple $\tilde{X}$ of linear operators acting on K, such that

$$0 = p_j(X)v = p_j(\tilde{X})v, \ \ 1 \le j \le m,$$

and therefore

$$q(\tilde{X}, \tilde{X}^*)v = 0 \ \Rightarrow q(X,Y)v = 0.$$

Thus, the stated Nullstellensatz for analytic polynomials in the variables (x,y) applies:

$$q(x,y) = \sum_{j=1}^{m} r_j(x,y)p_j(x),$$

where $r_j \in \mathbb{R}\langle x,y\rangle, \ \ 1 \le j \le m$. In other terms, by replacing $y = x^*$, we find $q \in \mathbb{F}p$ and the proof is complete. □

Proof (of Theorem 1). At this stage we can simply repeat, word by word, the proof of the main result in [6]. We simply remark that Theorem 2 implies, under the assumption and notation in Theorem 1,

$$\sum_{j=1}^{k} f_j(x,x^*)^* f_j(x,x^*) \in \mathrm{sym}(\mathbb{F}p)$$

is equivalent to

$$V(p_1,...,p_m) \subset V(f_1,...,f_k).$$

□

3 Non-commutative Nullstellensätze

Compared to the domain marked by Hilbert's Nullstellensatz and its many consequences, there have been few attempts made to find similar results in non-commutative rings. An early success in this direction is due to Amitsur [1]. We recall below his main result, and prove a variation of it. The latter is close to the spirit of the present note.

Now let $\mathbb{F} = \mathbb{C}\langle x_1,...,x_g\rangle$ be the free $\mathbb{C}$-algebra with g generators. Let $\mathfrak{I}$ be a bilateral ideal of $\mathbb{F}$ and fix an order d. The *hard zero set* of $\mathfrak{I}$, at order d, is

$$\mathfrak{V}_d(\mathfrak{I}) = \{(X_1,\ldots,X_n);\ X_j \in M_d(\mathbb{C}), 1 \le j \le g,\ f(X) = 0, f \in \mathfrak{I}\}.$$

Here $M_d(\mathbb{C})$ is the algebra of complex $d \times d$ matrices. Let $\mathfrak{M}_d$ be the bilateral ideal of $\mathbb{F}$ generated by the relations satisfied by any pair of matrices of order d (defining the PI ring structure).

Amitsur's theorem asserts that, for a fixed element $p \in F$, the inclusion

$$\mathfrak{V}_d(\mathfrak{I}) \subset \mathfrak{V}_d(p)$$

holds if and only if there exists an integer N with the property

$$p^N \in \mathfrak{I} + \mathfrak{M}_d.$$

We propose below to free the degree d. For a rich class of left ideals I we obtain then a stronger statement, by eliminating the need of taking any higher power of p. We return now to our convention of taking real scalars, noting that the complex case can be obtained by embedding the complex numbers into M_2, the 2×2 matrices with real entries.

The *zero set* of an element q in a unital algebra is the set ordered pairs (π,γ), where $\pi : \mathscr{A} \to \mathscr{L}(H)$ is a representation of $\mathscr{A}$ as linear transformations on a *finite dimensional* real vector space H (thus here $\mathscr{L}(H)$ denotes the linear maps on H), the vector γ is a nonzero element of H and $\pi(q)\gamma = 0$. Let $V(q)$ denote this zero set. In the case that $\mathscr{A} = \mathbb{F}$ this reduces to our usual notion of zero set.

If I is a left ideal in $\mathscr{A}$, the zero set of I, denoted $V(I)$, is the intersection, of the zero sets $V(p)$ for $p \in I$. For a unital algebra say that a left ideal I is *weakly radical* if $V(I) \subset V(q)$ implies $q \in I$.

The weakly radical condition on I can be stated in terms of the existence of sufficiently many left ideals J containing I. Indeed, if $\pi : \mathscr{A} \to \mathscr{L}(H)$ is a representation and $\gamma \in H$, then

$$J = \{a \in \mathscr{A} : \pi(a)\gamma = 0\} \tag{3}$$

is a left ideal which contains I if and only if $\pi(a)\gamma = 0$ for every $a \in I$. On the other hand, if J is a left ideal, then the left regular representation induces a representation $\rho : \mathscr{A} \to \mathscr{L}(\mathscr{A}/J)$ given by $\rho(a)(b+J) = (ab+J)$. In this case J contains I if and only if $\rho(a)(1+J) = 0$ for every $a \in I$.

For a left ideal J in $\mathscr{A}$, the codimension of J, denoted $\mathrm{codim}(J)$, is the dimension of the vector space $\mathscr{A}/J$.

Proposition 1 *A left ideal I in a unital algebra $\mathscr{A}$ is a weakly radical ideal if and only if*

$$I = \bigcap \{J : J \textit{ is a left ideal containing } I \textit{ and } \mathrm{codim}(J) < \infty\} \tag{4}$$

Proof Suppose the left ideal I ratifies the equality in equation (4) and that $q \notin I$. There exists a left ideal J containing I such that $q \notin J$ and the vector space $H = \mathscr{A}/J$ is finite dimensional. Let ρ denote the left regular representation as above. Since $q \notin J$, it follows that $\rho(q)[1] = [q] \neq 0$; whereas for each $a \in I$, $\rho(a)[1] = [a] = 0$. Hence I is a weakly radical ideal.

Conversely, suppose I is a weakly radical ideal and let $q \notin I$ be given. There exists a finite dimensional vector space H, a representation $\pi : \mathscr{A} \to \mathscr{L}(H)$, and a vector $\gamma \in H$ such that $\pi(q)\gamma \neq 0$, but at the same time $\pi(a)\gamma = 0$ for each $a \in I$. Let J denote the left ideal as in equation (3) corresponding to the pair (π,γ). By construction, J contains I and $q \notin J$. Thus to finish the proof it only remains to show that J has finite codimension.

Since $a \in J$ if and only if $\pi(a)\gamma = 0$ the mapping from $W = \{\pi(a)\gamma : a \in \mathscr{A}\}$ into $\mathscr{A}/J$ given by $\pi(a)\gamma \mapsto a+J$ is well defined and one-one. It is evidently onto and is thus a vector space isomorphism $S : W \to \mathscr{A}/J$. Since H is finite dimensional so is W and hence J has finite codimension. (As an aside, with ρ coming from the left regular representation as a above, $S\tilde{\pi}(a) = \rho(a)S$, where $\tilde{\pi}$ denotes the corresponding cyclic representation, $\tilde{\pi}(a) = \pi(a)|_W$.) $\square$

We are of course primarily interested in the weakly radical property and accordingly in the examples below this is verified by showing various ideals satisfy equation (4). However, it is interesting to note that for $\mathscr{A} = \mathbb{F}$ every finitely generated ideal is a weakly radical ideal as found in [5]. The proof, due to Bergman, proceeds by checking the weakly radical condition directly giving little indication of how to concretely construct the ideal J containing I but not q. On the other hand, there are ideals in $\mathbb{F}$ which are not weakly radical ideals. For instance, if I is the two sided ideal generated by the canonical commutation relations, then $\mathbb{F}/I$ is the Weyl algebra which admits no (nontrivial) finite dimensional representations. Indeed, the right ideal generated by the canonical commutation relations can not be contained in any nontrivial left ideal whose codimension is finite.

For completeness we include the statement and proof of the Bergman Nullstellensatz.

Theorem 3 **([5])** *Let I be a left ideal in $\mathbb{F}$. If I is finitely generated (as a left ideal), then I is weakly radical.*

Proof Fix $q \in \mathbb{F}$ and suppose $p_1, \dots, p_n$ generate I as a left ideal. Assuming $V(I) \subset V(q)$, we will show $q \in I$.

Choose N so that N is strictly larger than the maximum of the degrees of $\{p_1, \dots, p_n, q\}$. Let $\mathscr{P}_N$ denote the polynomials in $\mathbb{F}$ of degree at most N and likewise $\mathscr{P}_{N-1}$. The vector space $\mathbb{F}/I$ may well be infinite dimensional; however $\mathscr{W}_N$, the image of $\mathscr{P}_N$ in $\mathbb{F}/I$ is finite dimensional. Similarly, let $\mathscr{W}_{N-1}$ denote the image of $\mathscr{P}_{N-1}$ in $\mathbb{F}/I$. Let $[a] = a + I$ denote the class of $a \in \mathbb{F}$ in the quotient $\mathbb{F}/I$. Thus $\mathscr{W}_N = \{[a] : a \in \mathscr{P}_N\}$. Further, if $a \in \mathscr{P}_{N-1}$, then $[a] = 0$ if and only if $a \in \mathscr{P}_{N-1} \cap I$.

Because $\mathscr{W}_N$ is finite dimensional and $\mathscr{W}_{N-1}$ is a subspace there is a complementary subspace $\mathscr{L}$ in $\mathscr{W}_N$ so that $\mathscr{W}_{N-1} + \mathscr{L} = \mathscr{W}_N$ and $\mathscr{W}_{N-1} \cap \mathscr{L} = (0)$.

Define operators $X_j : \mathscr{W}_{N-1} \to \mathscr{W}_N$ as follows. Given $w \in \mathscr{W}_{N-1}$, choose any representative $a \in \mathscr{P}_{N-1}$ such that $[a] = w$ and define $X_j w = [x_j a]$. This is well defined since $[a] = w = [b]$ if and only if $a - b \in I$ in which case $x_j a - x_j b \in I$. Extend X_j to all of $\mathscr{W}_N$ (denoting these extended operators still by X_j) by asking that $X_j \ell = 0$ for $\ell \in \mathscr{L}$.

The tuple $X = (X_1, \dots, X_n)$ constructed above gives rise to a representation of $\mathbb{F}$ on the finite dimensional vector space $\mathscr{W}_N$. In accordance with our conventions, this representation will be denoted as $\mathbb{F} \ni a \mapsto a(X)$. Choosing $\gamma = [1]$ as the distinguished vector, $p_j(X)[1] = [p_j] = 0$ for each j since $p_j \in \mathscr{P}_{N-1} \cap I$. That is, $(X, [1]) \in V(p_j)$ for each j. Hence, as $\cap V(p_j) \subset V(q)$, it follows that $q(X)[1] = [q] = 0$. Since $q \in \mathscr{P}_{N-1}$, this means $q \in I$ and the proof is complete. $\square$

In view of the Bergman Nullstellensatz and the example of the Weyl algebra, we ask

Question 1 For which finitely generated unital algebras $\mathscr{A}$ is every finitely generated left ideal a weakly radical ideal?

A series of simple examples are of independent interest.

3.1 Commutative Algebra

If $\mathbb{F}/I$ is commutative, then (4) holds by Krull's intersection theorem. Thus we obtain a Nullstellensatz for commutative polynomials which does not involve the radical.

In this commutative setting the *(commutative) hard zero set* of a polynomial p in the commutative polynomial ring $\mathbb{C}[x_1,...,x_g]$ consists of g-tuples of commuting matrices X such that $p(X)=0$ and will be denoted $Z(p)$. The *(commutative) hard zero* set of an ideal I is defined analogously and denoted $Z(I)$.

Theorem 4 *Let I be an ideal in the commutative polynomial ring $\mathbb{C}[x_1,...,x_g]$ and let $q \in \mathbb{C}[x_1,...,x_g]$ be given. Then*

$$q \in I \text{ if and only if } V(I) \subset V(q).$$

This theorem is in sharp contrast to the classical Nullstellensatz which requires the radical ideal.

Note that in the definition of weakly radical ideal it may be assumed that the vector γ is cyclic for the representation π. In this case, and because of commutativity, the condition $p(X)\gamma = 0$ for each $p \in I$ implies $p(X) = 0$ for each $p \in I$. Thus to prove Theorem 4 it suffices to show that the ideal I satisfies equation (4).

Proof What matters is that $\mathscr{A} = \mathbb{C}[x_1,\dots,x_g]$ is a commutative Noetherian ring with unit with the property that if $M \subset \mathscr{A}$ is a maximal ideal and n is a positive integer, then $\mathscr{A}/M^n$ is finite dimensional (as a vector space).

The quotient $\mathscr{R} = \mathbb{C}[x_1,\dots,x_g]/I$ is a unital commutative Noetherian ring with the finiteness property above on maximal ideals. Most of the proof consists of showing,

$$(0) = \cap\{M^n : M \text{ a maximal ideal of } \mathscr{R}, n \in \mathbb{N}^+\}.$$

Let $p \in \mathscr{R}$, $p \neq 0$, be given. Let $N = \{x \in \mathscr{R} : xp = 0\}$. Then N is a proper ideal of $\mathscr{R}$ and there is a maximal ideal M containing N.

Let $S = \mathscr{R} \setminus M$, the complement of M in $\mathscr{R}$. Recall the construction of $\mathscr{R}_M$, the localization of $\mathscr{R}$ to M, as the quotient ring $S^{-1}\mathscr{R}$ of $\mathscr{R}$. This is the ring of of quotients r/s, for $r \in \mathscr{R}$ and $s \in S$ with $r/s = r'/s'$ if and only if there exists $t \in S$ so that $t(rs' - r's) = 0$ and the expected ring operations.

Let ϕ_S denote the map localizing $\mathscr{R}$ to M; i.e., $\phi_S : \mathscr{R} \to \mathscr{R}_M$, $\phi_S(r) = rs/s$, for any s in $S = \mathscr{R} \setminus M$. The choice of M guarantees that $\phi_S(p) \neq 0$ as $\phi_S(r) = 0$ if and only if $rs = 0$ for some $s \in S$.

Apply a version of Krull's intersection Lemma to the unique maximal ideal M_M of $\mathscr{R}_M$ to conclude that $\cap M_M^n = (0)$ and hence there is an integer k so that $\phi_S(p) \notin M_M^k = \phi_S(M^k)$. Thus, $p \notin \phi_S^{-1}(\phi_S(M^k)) \supset M^k$.

To finish the proof, suppose $q \notin I$ so that $[q]$, the class of q in the quotient $\mathscr{R}$, is nonzero. From what has been proved, there exists a maximal ideal M in $\mathscr{R}$ and a positive integer k so that $[q] \notin M^k$. There exists a maximal ideal $M_0 \subset \mathscr{A}$ such that $M = M_0/I$. Hence $M^k = (M_0^k + I)/I$ and thus $q \notin M_0^k + I$. Since M_0^k has finite codimension in $\mathscr{R}$, the ideal $M_0^k + I$ has finite codimension in $\mathscr{A}$. □

3.2 Enveloping Algebras of Semi-Simple Lie Algebras

Assume that $F/I_0 = U(\mathfrak{g})$ is the enveloping algebra of a semi-simple complex Lie algebra. Due to the fact that there are sufficiently many finite dimensional representations of $U(\mathfrak{g})$, the ideal I_0 is weakly radical. It would be interesting to know whether $U(\mathfrak{g})$ is a candidate for a positive solution to Question 1. In other terms, is it true that every left ideal of $U(\mathfrak{g})$ is weakly radical?

3.3 Homogeneous ideals in $\mathbb{F}$

We thank Dan Rogalski for suggesting the following example.

A left ideal I in $\mathbb{F}$ is *homogeneous* if it is generated (as a left ideal) by homogeneous elements of $\mathbb{F}$.

Theorem 5 *Every homogeneous ideal in $\mathbb{F}$ is a weakly radical ideal.*

Proof Let I be a given homogeneous left ideal. Let J denote the (two sided) ideal in $\mathbb{F}$ generated by $\{x_1,\dots,x_n\}$. We claim

$$I = \cap\{I + J^N : N \in \mathbb{N}^+\}. \tag{5}$$

To prove (5), it suffices to show, if $q \in \cap(I+J^N)$, then $q \in I$. Accordingly, let such a q of degree $N-1$ be given. Since $q \in I + J^N$, there exists finitely many homogeneous polynomials $r_1,\dots,r_\ell \in I$ (repetition allowed), monomials m_j, and a polynomial $s \in J^N$ such that

$$q = \sum_{j=1}^{\ell} m_j r_j + s.$$

Further, without loss of generality, it may be assumed that the degree of each $m_j r_j$ is at most $N-1$ (or else it can be combined with s). Since there can be no cancellation between s and $\sum m_j r_j$ and since the degree of q is $N-1$, we have $s = 0$ and $q \in I$. □

4 Commutative Hereditary Sums of Squares

We work in the algebra $B = \mathbb{C}[x^*] \otimes_{\mathbb{C}} \mathbb{C}[x]$, where the variables $x = (x_1,...,x_g)$ commute and $x^* = (x_1^*,...,x_g^*)$ are commutative, but they do not commute jointly. The anti-linear involution works on the set of linearly independent generators (products of monomials) as:

$$[x^{*\beta} \otimes x^\alpha]^* = x^{*\alpha} \otimes x^\beta,$$

where $\alpha, \beta \in \mathbb{N}^g$ and we use the multi-index notation. An element $q \in B$ is called a *hereditary polynomial*, and it can be uniquely written as a linear combination of elementary tensors:

$$q(x,x^*) = \sum_{\alpha,\beta} Q_{\alpha,\beta} x^{*\beta} \otimes x^\alpha,$$

with $Q_{\alpha,\beta} \in \mathbb{C}$.

If q is an hereditary polynomial and $X = (X_1, \ldots, X_g)$ is a tuple of commuting matrices (of any size), then $q(X,X^*)$ defined in the natural way:

$$q(X,X^*) = \sum_{\alpha,\beta} Q_{\alpha,\beta} X^{*\beta} X^{\alpha}.$$

Note that X^* denotes the adjoint tuple with respect to the inner product of the space where X acts.

The hereditary polynomial q is a sum of squares if there exists n and $r_j \in \mathbb{C}[x]$ for $j = 1, \ldots, n$ so that

$$q(x,x^*) = \sum_{j=1}^{n} r_j(x)^* \otimes r_j(x)$$

written more succinctly as $q = \sum r_j^* r_j$. Note, if q is a sum of squares and X is a tuple of commuting matrices, then $q(X,X^*) \succeq 0$ (is positive semidefinite). We have the following sums of squares criteria for hereditary polynomials.

Theorem 6 *The hereditary polynomial q is a sum of squares if and only if for every tuple of commuting matrices, $q(X,X^*)$ is positive semidefinite.*

The proof actually proves something more quantitative.

First remark that q is a sum of squares if and only if the associated matrix $(Q_{\alpha,\beta})$ is positive semi-definite.

To prove the only non-trivial implication, assume that the hereditary polynomial $q \in B$ is not a sum of squares. Let $d = \max\{\deg_x q, \deg_{x^*} q\}$, so that the indices running in the matrix Q satisfy $|\alpha|, |\beta| \leq d$. Let $\mathfrak{m}$ denote the ideal with generators $x_1, \ldots, x_g$; it is the maximal ideal corresponding to the point $x = 0$. We define the finite dimensional quotient module

$$H = \mathbb{C}[x]/\mathfrak{m}^{d+1},$$

where $\mathfrak{m}^{d+1}$ denotes the $d+1$ power of the ideal $\mathfrak{m}$. On H define the multiplication operators $X_j[f] = [x_j f]$ based on the variables x_j. They commute and have the vector $\xi = [1]$ jointly cyclic.

Since the matrix Q is not positive semi-definite, there are complex numbers c_α, $|\alpha| \leq d$, such that

$$\sum_{\alpha,\beta} Q_{\alpha,\beta} c_\alpha \overline{c_\beta} < 0.$$

Choose a positive ε, small enough, so that

$$\sum_{\alpha,\beta} Q_{\alpha,\beta} [c_\alpha \overline{c_\beta} + \varepsilon \delta_{\alpha,\beta}] < 0,$$

where the latter is the Kronecker symbol. On the other hand, the matrix

$$M_{\alpha,\beta} = Q_{\alpha,\beta} + \varepsilon \delta_{\alpha,\beta}$$

is strictly positive definite. Define on H the Hermitian product

$$\langle [x^\alpha], [x^{*\beta}] \rangle = M_{\alpha,\beta}.$$

In other words,

$$\langle X^{*\beta} X^{\alpha} \xi, \xi \rangle = M_{\alpha,\beta}.$$

In conclusion,

$$\langle q(X,X^*)\xi, \xi \rangle = \sum Q_{\alpha,\beta} M_{\alpha,\beta} < 0,$$

proving that there exists a g-tuple of commuting matrices X with the property that $q(X,X^*)$ is not positive semi-definite.

Note that the proof offers a bound $N(d)$ on the size of matrices we have to test positivity, assuming that d is the degree of the polynomial q. We leave this detail to the interested reader.

We can equally work with commutative polynomials $q(z,\bar{z}) \in \mathbb{C}[z,\bar{z}]$, where $z,\bar{z}$ are commuting variables. For instance the complex coordinates and their conjugates in $\mathbb{C}^g$. If we put by convention all adjoints X_j^* to the left of X_k, in $q(X,X^*)$, then the same proof applies and yields the following result.

Corollary 2 *Let $q \in \mathbb{C}[z,\bar{z}]$ be given. There exist polynomials $r_j \in \mathbb{C}[z]$, $1 \leq j \leq n$, with*

$$q(z,\bar{z}) = \sum_{j=1}^{n} |r_j(z)|^2,$$

if and only if, for all commuting g-tuples of matrices X we have $q(X,X^*) \geq 0$.

For more details about such (hermitian, or subharmonic) decompositions, see [12]. For noncommutative hereditary polynomials the analogous theorem is used in Nick Slinglend's UCSD thesis in studying the effect of noncommutative biholomorphic maps.

5 An Approximate Nullstellensatz on Arbitrary Varieties

In this section we propose a Nullstellensatz for an arbitrary non-commutative polynomial q vanishing on a basic algebraic set in $\mathbb{F}$. However, we pay for this huge generality by only obtaining an approximate formula. A counterexample is given in [5] to a Nullstellensatz as clean as Theorem 2, when q and the defining equations p of the support set are not analytic.

Theorem 7 *Suppose $q, p_1, \ldots p_n \in \mathbb{F}$, and assume that the zero set $V(\{p_1, \ldots, p_n\})$ is non-empty. Then*

$$V(\{p_1, \ldots, p_n\}) \subset V(q)$$

if and only if there exists $C_{min} > 0$ with the property that for each pair of real numbers $C > C_{min}$ and $\lambda > 0$, there exist sums of squares $\sigma_+, \sigma_-, \sigma_j \in \Sigma^2$, $j = 1, 2, \ldots, n$, such that

$$q^* q + \sigma_+ + \sigma_- \star (C^2 - \sum x_j^* x_j) = \lambda + \sum_{j=1}^{n} p_j^* \sigma_j p_j. \qquad (6)$$

Remark 1 Notable is that this theorem applies to non-analytic polynomials, and it does not require the key cone to have the archimedean property. The bound C_{min} is defined by

$$C_{min} = \inf_{(X,v)\in V(\{p_1,\ldots,p_n\})} \|X\|.$$

Proof We assume that $V(p)$ is non-empty, and consider constants $C > C_{min}$.

One direction is straightforward. Let $(X,v) \in V(\{p_1,\ldots,p_n\})$ and take $C > \|X\|$. Assume that for every $\lambda > 0$ there exist sums of squares σ_+, σ_-, and σ_j $(1 \le j \le n)$ so that equation (6) holds. Thus,

$$\|q(X)v\|^2 + r_+ + r_- = \lambda$$

where r_- and r_+ are both nonnegative. It follows that $\|q(X)v\|^2 \le \lambda$. Since $\lambda > 0$ is arbitrary, $q(X)v = 0$.

To prove the converse, suppose that $V(\{p_1,\ldots,p_n\}) \subset V(q)$, fix a constant $C > C_{\min}$ and assume by contradiction that there exists a $\lambda_0 > 0$ so that it is not possible to solve equation (6). (It follows it is not possible to solve equation (6) for $\lambda_0 > \lambda > 0$. On the other hand, for large enough λ the equation does have a solution.) We will show there exists $(X,v) \in V(\{p_1,\ldots,p_n\})$ with $v \ne 0$, but $q(X)v \ne 0$. This is accomplished by a familiar cone separation argument and a GNS (Gelfand-Naimark-Segal) construction.

Let $\mathscr{C}$ denote the convex cone

$$\mathscr{C} = \{\sigma_+ + \sigma_- \star (C^2 - x^*x) : \sigma_\pm \in \Sigma^2\}$$

and let $\mathscr{L}$ denote the vector subspace

$$\mathscr{L} = \{\lambda + \mu q^*q + \sum_{j=1}^n p_j^* s_j p_j;\ \lambda,\mu \in \mathbb{R}, \quad s = s^*\}$$

in the vector space of all symmetric polynomials of $\mathbb{F}$. On $\mathscr{L}$ define the linear functional $L : \mathscr{L} \to \mathbb{R}$ by

$$L(\lambda + \mu q^*q + \sum_{j=1}^n p_j^* s_j p_j) = \lambda + \lambda_0 \mu.$$

To verify the correctness of this definition, suppose that

$$\lambda + \mu q^*q + \sum_{j=1}^n p_j^* s_j p_j = 0. \tag{7}$$

By evaluating equation (7) at a zero of the n-tuple $(p_1,\ldots,p_n)$ we find $\lambda = 0$. If we prove that $\mu = 0$, then the functional L will be well defined. Assume that $\mu \ne 0$. By possibly simultaneously changing s_i into multiples γs_i $(1 \le i \le n)$, we can assume that $q^*q + \sum_{j=1}^n p_j^* s_j p_j = 0$. Next we decompose each s_i as a difference of sums of squares

$$s_i = \sigma_i^+ - \sigma_i^-.$$

Whence

$$q^*q + \sum_{j=1}^n p_j^* \sigma_j^+ p_j = \sum_{j=1}^n p_j^* \sigma_j^- p_j.$$

Since $\lambda_0 \in \mathscr{C}$, this would imply that equation (6) is solvable for $\lambda = \lambda_0$, a contradiction. Thus, $L : \mathscr{L} \longrightarrow \mathbb{R}$ is well defined.

The immediate goal is to show $L(\mathscr{L} \cap \mathscr{C}) \geq 0$. To this end, suppose that $\lambda, \mu \in \mathbb{R}$, $s \in \mathbb{F}$ is symmetric, and

$$r = \lambda + \mu q^* q + \sum p_i^* s_i p_i \in \mathscr{C}.$$

Write $s_i = \sigma_i^+ - \sigma_i^-$, where $\sigma_i^{\pm}$ are sums of squares. This gives,

$$\lambda + \mu q^* q + \sum p_i^* \sigma_i^+ p_i \in \mathscr{C}. \tag{8}$$

Let $(X, v) \in V(\{p_1, \ldots, p_n\})$, $\|X\| < C$, so that, by assumption, $q(X)v = 0$. By evaluating equation (8) on (X, v) one finds $\lambda \geq 0$. Thus, if $\mu \geq 0$, then $L(r) \geq 0$ as desired. If $\mu < 0$, then, by dividing equation (8) by $\frac{-1}{\mu}$ one finds

$$\frac{\lambda}{-\mu} + \sum p_i^* \left(\frac{\sigma_i^+}{-\mu} \right) p_i \in q^* q + \mathscr{C},$$

and therefore $\frac{\lambda}{-\mu} > \lambda_0$. Hence we again find that $L(r) \geq 0$.

Therefore the linear functional L is positive on a subspace which contains the identity, and $L(1) = 1$. Since the archimedean cone $\mathscr{C}$ contains the order unit 1, the linear functional L can be extended by Corollary 9.12 on page 87 in [4] to a $\mathscr{C}$-positive linear functional on all symmetric polynomials.

We can proceed with the GNS construction. Consider the bilinear form on polynomials in x by

$$\langle r, s \rangle = L(r^* s + s^* r).$$

Since L is $\mathscr{C}$ positive and $\mathscr{C}$ contains squares, this form is positive semi-definite. Let $\mathscr{H}$ denote the Hilbert space obtained moding out null vectors and completing the resultant pre-Hilbert space. Abusing notation, for a polynomial s, let s denote the class of s in this Hilbert space. Define operators X_j on $\mathscr{H}$ by declaring $X_j s = x_j s$, for polynomials s. Since $s^*(C^2 - x_j^* x_j)s \in \mathscr{C}$ and since L is $\mathscr{C}$-positive,

$$C^2 \langle s, s \rangle - \langle x_j s, x_j s \rangle = L(\, s^*(C^2 - x_j^* x_j)s \,) \geq 0.$$

It follows that X_j passes to a well defined map modulo null vectors and then extends to the completion $\mathscr{H}$. The resultant operators will still be denoted X_j.

Since $q(X)1 = q$ and $L(q^* q) = \lambda_0 > 0$, it follows that $q(X)1$ is not zero. On the other hand, for each j, $p_j(X)1 = p_j$ and $L(p_j^* p_j) = 0$ so that $p_j(X)1 = 0$.

One can argue that, so far we have defined the zero set as pairs of operators and vectors attached to a finite dimensional Hilbert space, and above we have constructed a possibly infinite dimensional one. This anomaly can be restored by taking the orthogonal projection Π of $\mathscr{H}$ onto the finite dimensional subspace

$$\mathscr{H}_N = \bigvee_{\deg(w) \leq N} w(X, X^*)1,$$

where the linear span is taken over all words w of degree at most N. The diagonal truncation $X_j(N) \mapsto \Pi X_j \Pi$ will produce the desired finite dimensional objects. More specifically, for every polynomial $r(x, x^*)$ of degree less that N we will have

$$r(X, X^*)1 = r(X(N), X(N)^*)1.$$

Thus, $V(q)$ does not contain $V(\{p_1,\dots,p_n\})$, a contradiction. This completes the proof. $\square$

Remark 2 Denoting the left ideal associated to the set of polynomials $P=(p_1,...,p_n)$ by $\mathbb{F}P=\mathbb{F}p_1+\ldots+\mathbb{F}p_n$, the identity (6) in the statement of Theorem 7 can be replaced by

$$q^*q\in\lambda-M_{C^2-\sum x_j^*x_j}+\mathrm{sym}(\mathbb{F}P).$$

6 Majorization on Semi-algebraic Sets

The following theorem collects into a single statement some facts about polynomial majorization based on comparing their evaluation on pairs (X,v). Similar facts but ignoring the finer structure of keeping track of a vector v were originally proved in [5,7].

At this point we depart from our earlier convention, now allowing zeros of $p\in\mathbb{F}$ to consist of pairs (X,v) where $X=(X_1,\dots,X_n)$ is a tuple of bounded operators on a separable Hilbert space and $v\in H$ is a distinguished vector such that $p(X)v=0$. For clarity we use the notation $\mathbb{V}(p)$ and $\mathbb{V}(I)$ to denote this more liberal notion of zero set of p and the zero set of a subset $I\subset\mathbb{F}$.

Likewise, for a subset $S\subset\mathbb{F}$, let $\mathbb{K}_S$ denote those tuples (X,v), where X is an n-tuple of bounded operators on a common separable Hilbert space H and v is a distinguished vector in H, for which $\langle s(X)v,v\rangle\geq 0$ for all $s\in S$.

Theorem 8 *Let $q,p_1,\dots,p_n\in\mathrm{sym}\mathbb{F}$ and denote $P=\{p_1,\dots,p_n\}$. Let C_P denote the cone generated by $p_1,\dots,p_n$:*

$$C_P=\{\sum_j t_jp_j:\ \ all\ t_j\in\mathbb{R}^+\}.$$

Let S denote another finite set of polynomials (for example, $S=\{M^2-x^*x\}$, with M large), such that the quadratic module M_S is archimedean.

(i) If $\langle q(X)v,v\rangle>0$ whenever $(X,v)\in\mathbb{K}_P\cap\mathbb{K}_{M_S}$, then

$$q\in C_P+M_S. \tag{9}$$

Conversely, if (9) holds, then the first statement holds with $\langle q(X)v,v\rangle\ \geq 0$. In particular, $\mathbb{K}_P\cap\mathbb{K}_{M_S}=\emptyset$ if and only if $C_P+M_S=\mathbb{F}$.

(ii) $(X,v)\in\mathbb{K}_P\cap\mathbb{K}_{M_S}$ implies $q(X)$ is NOT negative semidefinite if and only if there exist $h_1,...,h_m\in\mathbb{F}$, such that

$$\sum_{j=1}^m h_j^*qh_j\in 1+C_P+M_S.$$

(iii) $(X,v) \in \mathbb{V}(P) \cap \mathbb{K}_{M_S}$ *implies* $q(X)$ *is NOT negative semidefinite if and only if there exists* $h_1,\dots,h_m \in \mathbb{F}$*, such that*

$$\sum_{j=1}^{m} h_j^* q h_j \in 1 + M_S + \mathrm{sym}\,\mathbb{F}P.$$

Remark 3 If $(X,v) \in \mathbb{K}_{M_S}$ and $\mathscr{M} = \{h(X)v : h \in \mathbb{F}\}$, then $\mathscr{M}$ is a reducing subspace for X (each X_j) and $s(Y)$ is positive semidefinite for each $s \in S$, where $Y = X|_{\mathscr{M}}$.

Proof In each part one direction is trivial. The other side is derivable from the same (separation and GNS scheme) proof used in §5 with the few points we now list needing clarification. In each case we build a separating linear functional $L : \mathbb{F} \longrightarrow \mathbb{R}$.

Proof of (i): Assume, in virtue of Lemma 1, that the functional L satisfies

$$L(q) \leq 0, \quad L(C_P + M_S) \geq 0, \;\; L(1) > 0.$$

Build the Hilbert space H as the Hausdorff completion of $\mathbb{F}$ with respect to $\langle f, g\rangle := L(f^*g + g^*f)$. Continue to proceed as in §5 by defining a set of multiplication operators $Y, Y_j f = x_j f$. These are well defined and bounded because of the archimedean hypothesis on M_S which implies $r^T(1 - x_j^T x_j)r \in M_S \subset C_P + M_S$ for each $r \in \mathbb{F}$ and j. The relation $Y_j^* f = x_j^* f$ readily follows from the definition of the inner product.

Now $\langle p_j(Y)[1],[1]\rangle = L(2p_j) \geq 0$ and similarly, $\langle r^T sr(Y)[1],[1]\rangle = L(2r^T sr) \geq 0$ for $s \in S$ and any r. Hence $(Y,[1]) \in \mathbb{K}_P \cap \mathbb{K}_{M_S}$, but $\langle q(Y)[1],[1]\rangle = L(q) \leq 0$.

Proof of (ii): Similarly, construct by invoking Lemma 1 the functional L with the properties

$$L(h^*qh) \leq 0, \quad L(1 + C_P + M_S) \geq 0, \quad L(1) > 0, \;\; h \in \mathbb{F}.$$

After defining the inner product $\langle\ ,\ \rangle$ from L and the multipliers Y as before, we again observe $\langle p_j(Y)1, 1\rangle = L(2p_j)$. Use $L(1 + tp_j) \geq 0$ for all $t \in \mathbb{R}^+$; by letting $t \to \infty$ to obtain $L(p_j) \geq 0$. Similarly, obtain $L(r^T sr) \geq 0$ for all $r \in \mathbb{F}$ and $s \in S$. Thus $(Y,[1]) \in \mathbb{K}_P \cap \mathbb{K}_{M_S}$.

On the other hand $0 \geq \langle q(Y)[h],[h]\rangle = L(\ h^*qh)$ for each polynomial $h \in \mathbb{F}$, and since $q(Y)$ is continuous and $\mathbb{F}$ is dense in H, the operator $q(Y)$ is negative semidefinite.

In this case the archimedean hypothesis on M_S and invariance under positive scalars implies that $t + r^T(1 - x_j^T x_j)r \in 1 + M_S \subset C_P + M_S$ for each positive real number t and $r \in \mathbb{F}$ and j. It follows that $L(r^T(1 - x_j^T x_j)r) \geq 0$ so that Y_j are well defined and bounded.

Proof of (iii): Assume as before that

$$L(h^*qh) \leq 0, \quad L(1 + M_S + \mathrm{sym}\,\mathbb{F}P) \geq 0, \;\; L(1) > 0, \;\; h \in \mathbb{F}.$$

After constructing the inner product $\langle\ ,\ \rangle$ from L and the multipliers $Y_j = M_{x_j}$, we observe $\langle r_j(Y)p_j(Y)1, 1\rangle = L(r_j p_j + p_j^* r_j^*)$. Use $L(1 + r_j p_j + p_j^* r_j^*) \geq 0$ for all r_j; by letting $r_j \to \infty$ to obtain $L(r_j p_j + p_j^* r_j^*) \geq 0$. This holds for all polynomials r_j, to include $\pm r_j$, so $L(r_j p_j + p_j^* r_j^*) = 0$. In particular $\langle p_j(Y)^* p_j(Y)1, 1\rangle = 0$ implies $p_j(Y)1 = 0$.

Computations as before show $\langle r^T sr(Y)[1],[1]\rangle \geq 0$ so that $(Y,[1]) \in \mathbb{V}(P) \cap \mathbb{K}_{M_S}$.

Since $q(Y)$ is continuous and $0 \leq L(h^T qh) = \langle q(Y)[h],[h]\rangle$ the operator $q(Y)$ is negative semidefinite. $\square$

Proofs and statements similar to (2) and (3) above appear in [7] and more generally in [3]. We mention that in [7] the evaluation matrices X_j are all symmetric, while here we remain consistent with the rest of this note and leave them unconstrained.

References

1. Amitsur, S. A.: A generalization of Hilbert's Nullstellensatz. Proc. Amer. Math. Soc. **8**, pp. 549-656 (1957)
2. Cimpric, J.: A representation theorem for archimedean quadratic modules on $*$-rings, preprint (2004)
3. Cimpric, J.: Maximal quadratic modules on $*$-rings, preprint (2005)
4. Conway, John B.: A course in operator theory. Graduate Studies in Mathematics, 21. American Mathematical Society, Providence, RI, 2000, xvi+372 pp
5. Helton, J.W., McCullough, S.: A Positivstellensatz for noncommutative polynomials. Trans. Amer. Math. Soc. **356**, pp. 3721-3737 (2004)
6. Helton, J.W., McCullough, S.,Putinar, M.: Non-negative hereditary polynomials in a free $*-$algebra. Math. Zeitschrift **250**, pp. 515-522 (2005)
7. Klep, I., Schweighofer, M., A Nichtnegativstellensatz for polynomials in noncommuting variables. Preprint (2005)
8. Koethe, G.: Topological Vector Spaces. I. Springer. Berlin (1969)
9. Krein, M.G., Rutman, M.A.: Linear operators leaving invariant a cone in a Banach space. (in Russian) Uspehi Mat. Nauk **23**, pp. 3-95 (1948)
10. Marshall, M.: Positive Polynomials and Sums of Squares. Instituti Edit. Poligraf. Int. Pisa, Roma (2000)
11. Prestel, A., Delzell, C.N.: Positive Polynomials. Springer, Berlin (2001)
12. Putinar, M.: On hermitian polynomial optimization, Arch. Math., to appear.