NULL- AND POSITIVSTELLENSÄTZE FOR RATIONALLY RESOLVABLE IDEALS

IGOR KLEP[1], VICTOR VINNIKOV, AND JURIJ VOLČIČ[2]

ABSTRACT. Hilbert's Nullstellensatz characterizes polynomials that vanish on the vanishing set of an ideal in $\mathbb{C}[\underline{X}]$. In the free algebra $\mathbb{C}<\underline{X}>$ the vanishing set of a two-sided ideal $\mathcal{I}$ is defined in a dimension-free way using images in finite-dimensional representations of $\mathbb{C}<\underline{X}>/\mathcal{I}$. In this article Nullstellensätze for a simple but important class of ideals in the free algebra – called tentatively *rationally resolvable* here – are presented. An ideal is rationally resolvable if its defining relations can be eliminated by expressing some of the $\underline{X}$ variables using noncommutative rational functions in the remaining variables. Whether such an ideal $\mathcal{I}$ satisfies the Nullstellensatz is intimately related to embeddability of $\mathbb{C}<\underline{X}>/\mathcal{I}$ into (free) skew fields. These notions are also extended to free algebras with involution. For instance, it is proved that a polynomial vanishes on all tuples of spherical isometries iff it is a member of the two-sided ideal $\mathcal{I}$ generated by $1-\sum_j X_j^{\intercal} X_j$. This is then applied to free real algebraic geometry: polynomials positive semidefinite on spherical isometries are sums of Hermitian squares modulo $\mathcal{I}$. Similar results are obtained for nc unitary groups.

1. INTRODUCTION

In algebraic geometry Hilbert's Nullstellensatz is a classical result characterizing polynomials vanishing on an algebraic set:

Theorem 1.1 (Hilbert's Nullstellensatz). *Let $f, h_1, \dots, h_s \in \mathbb{C}[\underline{X}]$ and*

$$Z := \{a \in \mathbb{C}^g \mid h_1(a) = \cdots = h_s(a) = 0\}.$$

If $f|_Z = 0$, then for some $r \in \mathbb{N}$, f^r belongs to the ideal $(h_1, \dots, h_s)$.

Due to its importance it has been generalized and extended in many different directions. For instance, there are noncommutative versions due to Amitsur [Ami57], Bergman [HM04], and Helton et al. [HMP07, CHMN13]. Here our main interest is in *free noncommutative Nullstellensätze* describing vanishing in free algebras. That is, given a two-sided ideal $\mathcal{I}$ in a free algebra $\Bbbk<\underline{X}>$, we consider polynomials f vanishing under all finite-dimensional representations of $\Bbbk<\underline{X}>/\mathcal{I}$. If each such f is in $\mathcal{I}$, then we say that $\mathcal{I}$ has

Date: March 29, 2017.

2010 *Mathematics Subject Classification.* Primary 13J30, 16R50; Secondary 46L89, 14P05.

Key words and phrases. Nullstellensatz, free algebra, rational identity, division ring, skew field, spherical isometry, nc unitary group, Positivstellensatz, real algebraic geometry, free analysis.

[1]Supported by the Marsden Fund Council of the Royal Society of New Zealand. Partially supported by the Slovenian Research Agency grants P1-0222, L1-4292 and L1-6722. Part of this research was done while the author was on leave from the University of Maribor.

[2]Research supported by The University of Auckland Doctoral Scholarship.

the Nullstellensatz property. Hence this is a noncommutative analog of a radical ideal in classical algebraic geometry.

In this paper we focus on an important class of ideals we call rationally resolvable. These are ideals in which all generators can be eliminated by solving for some of the variables in terms of noncommutative rational functions in the remaining variables (see Definition 2.2 for a precise statement). Noncommutative rational functions are elements of a free skew field $\Bbbk\langle\!\langle \underline{X} \rangle\!\rangle$, i.e., the field with "the least" rational relations between its generators X_j. If for a rationally resolvable ideal $\mathcal{I}$ the quotient ring $\Bbbk\langle\underline{X}\rangle/\mathcal{I}$ admits a "nice" embedding in a (free) skew field, then $\mathcal{I}$ has the Nullstellensatz property; the rigorous formulation is given in Theorem 2.5 and Proposition 2.6. For instance, we obtain the following.

Theorem 1.2. *Let $\mathcal{I} \subseteq \Bbbk\langle\underline{X}\rangle/\mathcal{I}$ be a (formally) rationally resolvable ideal. If $\Bbbk\langle\underline{X}\rangle/\mathcal{I}$ is a Sylvester domain (e.g., a free ideal ring), then $\mathcal{I}$ satisfies the Nullstellensatz property.*

See Theorem 2.5(a) and Proposition 2.6(a) for the proof. Subsection 2.5 gives examples illustrating the strength of our results in Section 2. In particular, we show the following.

Corollary 1.3. *Let $f \in \Bbbk\langle\underline{X},\underline{Y}\rangle$.*

(a) *If $f(\underline{A},\underline{B}) = 0$ for all $n \in \mathbb{N}$ and $(\underline{A},\underline{B}) \in M_n(\Bbbk)^{2g}$ such that $A_jB_j = I_n$ for $j = 1,\dots,g$, then $f \in (1-X_1Y_1, 1-Y_1X_1, \dots, 1-X_gY_g, 1-Y_gX_g)$.*
(b) *If $f(\underline{A},\underline{B}) = 0$ for all $n \in \mathbb{N}$ and $(\underline{A},\underline{B}) \in M_n(\Bbbk)^{2g}$ with $A_1B_1 + \cdots + A_gB_g = I_n$, then $f \in (1 - X_1Y_1 - \cdots - X_gY_g)$.*
(c) *If $f(\underline{A},\underline{B}) = 0$ for all $n \in \mathbb{N}$ and $(\underline{A},\underline{B}) \in M_n(\Bbbk)^{2g^2}$ such that $(A_{ij})_{ij}(B_{ij})_{ij} = I_{gn}$, then*
$$f \in \left(\delta_{ij} - \sum_{k=1}^{g} X_{ik}Y_{kj}, \delta_{ij} - \sum_{k=1}^{g} Y_{ik}X_{kj} \colon 1 \le i,j \le g\right),$$
where δ_{ij} denotes Kronecker's delta.

See Corollaries 2.8 and 2.9 for the proofs. To obtain size bounds needed on the dimensions of the finite-dimensional representations of $\Bbbk\langle\underline{X}\rangle/\mathcal{I}$ for these Nullstellensätze, we employ systems theory realizations for noncommutative rational functions; see [BR11, Chapters 1 and 2] or [BGM05, HMV06, KVV09]. Our rational functions do not admit scalar regular points in general, so we present the necessary modifications of the classical theory to handle matrix centers in Section 3. As a side product we obtain size bounds needed to test for rational identities, see Theorem 3.8. This machinery is then applied to Nullstellensätze in Subsection 3.3: for a noncommutative polynomial f and a rationally resolvable ideal $\mathcal{I}$ we give explicit bounds on the dimension of the finite-dimensional representations of $\Bbbk\langle\underline{X}\rangle/\mathcal{I}$ needed to test whether f vanishes under all these representations (Theorem 3.9).

Section 4 applies our results to $*$-ideals in free algebras with involution. We show that the $*$-ideals corresponding to unitaries and spherical isometries [HMP04] satisfy the Nullstellensatz property (Theorem 4.8), and give in Theorem 4.10 a Nullstellensatz for noncommutative unitary groups [Bro81, Wo87]. These results can be summarized as follows.

Corollary 1.4. *Let* $f \in \mathbb{C}\texttt{<}\underline{X}, \underline{X}^\intercal\texttt{>}$.

(a) *If* $f(\underline{A}, \underline{A}^*) = 0$ *for all* $n \in \mathbb{N}$ *and* $\underline{A} \in M_n(\Bbbk)^g$ *where* A_j *are unitary, then* $f \in (1 - X_1X_1^\intercal, 1 - X_1^\intercal X_1, \dots, 1 - X_gX_g^\intercal, 1 - X_g^\intercal X_g)$.
(b) *If* $f(\underline{A}, \underline{A}^*) = 0$ *for all* $n \in \mathbb{N}$ *and* $\underline{A} \in M_n(\Bbbk)^g$ *with* $A_1A_1^\intercal + \cdots + A_gA_g^\intercal = I_n$*, then* $f \in (1 - X_1X_1^\intercal - \cdots - X_gX_g^\intercal)$.
(c) *If* $f(\underline{A}, \underline{A}^*) = 0$ *for all* $n \in \mathbb{N}$ *and* $\underline{A} \in M_n(\Bbbk)^{g^2}$ *such that* $(A_{ij})_{ij}$ *is a unitary matrix, then*

$$f \in \left(\delta_{ij} - \sum_{k=1}^{g} X_{ik}X_{kj}^\intercal, \delta_{ij} - \sum_{k=1}^{g} X_{ik}^\intercal X_{kj} \colon 1 \le i, j \le g \right).$$

As before, these results are effective (i.e., we obtain concrete size bounds). To extend our involution-free statements to $*$-ideals in free algebras with involution, we use (real) algebraic geometry, cf. Subsection 4.3. The paper concludes in Subsection 4.5 with Positivstellensätze for a few selected examples of rationally resolvable ideals. For example, the following result solves a problem from [HMP04] on spherical isometries, i.e., tuples of matrices $(A_1, \dots, A_g)$ satisfying $A_1^*A_1 + \cdots + A_g^*A_g = I$.

Theorem 1.5. *If* $f \in \mathbb{C}\texttt{<}\underline{X}, \underline{X}^\intercal\texttt{>}$ *of degree* $d-1$ *is nonnegative on all spherical isometries of size* $(2g+1)^d$*, then*

$$f = \sum_j p_j^\intercal p_j + q$$

for some $p_j \in \mathbb{C}\texttt{<}\underline{X}, \underline{X}^\intercal\texttt{>}$ *of degrees at most* d *and* $q \in (1 - X_1^\intercal X_1 \cdots - X_g^\intercal X_g)$.

Theorem 1.5 is proved as Corollary 4.14 in Subsection 4.5.

Acknowledgments. The authors thank Warren Dicks and Pere Ara for their help with Corollary 2.9.

2. Rationally resolvable ideals and Nullstellensätze

In this section we introduce two notions of rationally resolvable ideals and identify important classes and examples of those satisfying a Nullstellensatz. Loosely speaking, an ideal is rationally resolvable if from each of its generators one variable can be expressed as a noncommutative rational function of other variables; see Definition 2.2 for a precise statement. The main result here is Theorem 2.5, and interesting examples are presented in Subsection 2.5.

2.1. **Notation and terminology.**

2.1.1. *Words and nc polynomials.* Given a field $\mathbb{k}$, and positive integers n, g, let $M_n(\mathbb{k})$ denote the $n\times n$ matrices with entries from $\mathbb{k}$ and $M_n(\mathbb{k})^g$ the set of g-tuples of such $n\times n$ matrices. For simplicity, we shall always assume $\operatorname{char}\mathbb{k} = 0$.

We write $<\underline{X}>$ for the monoid freely generated by $\underline{X} = \{X_1, \dots, X_d\}$, i.e., $<\underline{X}>$ consists of **words** in the g noncommuting letters $X_1, \dots, X_g$ (including the empty word $\varnothing$ which plays the role of the identity 1). With $|w| \in \mathbb{N}\cup\{0\}$ we denote the length of word $w \in <\underline{X}>$. Let $\mathbb{k}<\underline{X}>$ denote the associative $\mathbb{k}$-algebra freely generated by $\underline{X}$, i.e., the elements of $\mathbb{k}<\underline{X}>$ are polynomials in the noncommuting variables $\underline{X}$ with coefficients in $\mathbb{k}$. Its elements are called **(nc) polynomials**. An element of the form aw where $0 \neq a \in \mathbb{R}$ and $w \in <\underline{X}>$ is called a **monomial** and a its **coefficient**. Sometimes we also use Y_j to denote noncommuting variables.

2.1.2. *Polynomial evaluations.* If $p \in \mathbb{k}<\underline{X}>$ is an nc polynomial and $\underline{A} \in M_n(\mathbb{k})^g$, the evaluation $p(\underline{A}) \in M_n(\mathbb{k})$ is defined by simply replacing X_i by A_i. For example, if $p(x) = 3X_1X_2 - X_1^2$, then

$$p\left(\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & -1 \end{bmatrix}\right) = 3\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 2 & -1 \end{bmatrix} - \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 9 & -4 \\ -2 & 1 \end{bmatrix}.$$

In other words, evaluations of nc polynomials at $\underline{A} \in M_n(\mathbb{k})^g$ are representations

$$\mathrm{ev}_{\underline{A}} : \mathbb{k}<\underline{X}> \to M_n(\mathbb{k}), \quad p \mapsto p(\underline{A}).$$

2.1.3. *Ideals.* Let $S = \{f_1, \dots, f_s\} \subseteq \mathbb{k}<\underline{X}>$. The **two-sided ideal** generated by S is

$$\mathcal{I}(S) := \Big\{ \sum_{i=1}^{n} \sum_{j=1}^{s} g_{ij} f_j h_{ij} \mid n \in \mathbb{N},\, g_{ij}, h_{ij} \in \mathbb{k}<\underline{X}> \Big\}. \tag{2.1}$$

It is the smallest subset of $\mathbb{k}<\underline{X}>$ containing S and closed under addition and multiplication (from left and right) with elements from $\mathbb{k}<\underline{X}>$.

2.1.4. *Zero sets.* There are many noncommutative generalizations of Hilberts Nullstellensatz. The ones that concern us here replace point evaluations $\mathbb{C}[\underline{X}] \to \mathbb{C}$ by some class of representations of the noncommutative algebra that we are dealing with. For the case of the free algebra $\mathbb{k}<\underline{X}>$ the most reasonable class of representations, so far, seems to be the class of all finite dimensional representations. In other words, we replace evaluations of commutative polynomials on points in $\mathbb{C}^g$ by evaluations of nc polynomials on g-tuples of $n \times n$ matrices over $\mathbb{k}$, for all $n \in \mathbb{N}$.

There is (at least) one other choice to be made in the noncommutative setting: we have to decide whether we are dealing with one-sided ideals or with two-sided ideals giving rise to different types of vanishing. We refer the reader to [BK11] for a more extensive overview of noncommutative Nullstellensätze. Here we focus on (strong) vanishing and hence on two-sided ideals.

To a (two-sided) ideal $\mathcal{I} \subseteq \mathbb{k}<\underline{X}>$ we associate its **zero set**

$$Z(\mathcal{I}) := \bigcup_{n\in\mathbb{N}} \{\underline{A} \in M_n(\mathbb{k})^g \mid \forall g \in \mathcal{I} :\ g(\underline{A}) = 0\}. \tag{2.2}$$

In contrast with the classical case (cf. Theorem 1.1), it may very well happen that $Z(\mathcal{I}) = \varnothing$ for a proper ideal $\mathcal{I} \subsetneq \Bbbk\langle\underline{X}\rangle$. For instance, take $\mathcal{W} = (X_1X_2 - X_2X_1 - 1)$.

2.2. **The free skew field.** The universal skew field of fractions of the free algebra $\Bbbk\langle\underline{X}\rangle$ is called the **free skew field** and denoted by $\Bbbk\langle\!\langle\underline{X}\rangle\!\rangle$. We call its elements (nc) rational functions. Let us describe in a bit more detail in a language suitable for our investigation how they are obtained. We start with nc polynomials in $\Bbbk\langle\underline{X}\rangle$, add their formal inverses, allow addition and multiplication, and then repeat this procedure. This gives rise to nc rational expressions. We emphasize that an expression includes the order in which it is composed and no two distinct expressions are identified, e.g., $(X_1) + (-X_1)$, $(-1) + (((X_1)^{-1})(X_1))$, and 0 are different nc rational expressions.

Evaluation of polynomials naturally extends to rational expressions. If r is a rational expression in $\underline{X}$ and $\underline{A} \in M_n(\Bbbk)^g$, then $r(\underline{A})$ is defined - in the obvious way - as long as any inverses appearing actually exist. Generally, a nc rational expression r can be evaluated on a g-tuple A of $n \times n$ matrices in its domain of regularity, $\operatorname{dom} r$, which is defined as the set of all g-tuples of square matrices of all sizes such that all the inverses involved in the calculation of $r(\underline{A})$ exist. From here on we assume that all rational expressions under consideration have nonempty domains.

Two rational expressions r_1 and r_2 are equivalent if $r_1(\underline{A}) = r_2(\underline{A})$ at any $\underline{A} \in \operatorname{dom} r_1 \cap \operatorname{dom} r_2$. Then an equivalence class of rational expressions is a rational function. The set $\Bbbk\langle\!\langle\underline{X}\rangle\!\rangle$ of all rational functions is a skew field. It has the following universal property: if D is a skew field, then every homomorphism $\phi : \Bbbk\langle\underline{X}\rangle \to D$ extends to a **local homomorphism** from $\Bbbk\langle\!\langle\underline{X}\rangle\!\rangle$ to D, i.e., ϕ extends to a homomorphism $\varphi : K \to D$ for some subring $\Bbbk\langle\underline{X}\rangle \subseteq K \subseteq \Bbbk\langle\!\langle\underline{X}\rangle\!\rangle$ such that for every $u \in K$, $\varphi(u) \neq 0$ implies $u^{-1} \in K$. For a comprehensive study of (free) skew fields we refer to Cohn [Coh95, Coh06].

A rational expression is of **height** h if the maximal number of nested inverses in it is h. The **height** of a rational function is then defined as the minimum of heights of all the rational expressions representing it. We let $\Bbbk\langle\!\langle\underline{X}\rangle\!\rangle_h \subseteq \Bbbk\langle\!\langle\underline{X}\rangle\!\rangle$ denotes the subring of all rational functions whose height is at most h. If r is a tuple of rational functions, then $h(r)$ denotes the maximum of heights of its components.

2.3. **Rationally resolvable ideals.**

Notation 2.1. We first introduce some additional notation. Fix a partition of the variables

$$\underline{X} = \underline{X}' \cup \underline{X}'' = \{X_1', \dots, X_{g'}'\} \cup \{X_1'', \dots, X_{g''}''\}, \tag{2.3}$$

hereafter called the **decomposition** of $\underline{X}$, and a tuple $r = (r_1, \dots, r_{g''})$ of rational functions $r_j \in \Bbbk\langle\!\langle\underline{X}'\rangle\!\rangle$, to which we assign the following objects. Let $\operatorname{dom} r \subseteq \bigcup_n M_n(\Bbbk)^{g'}$ be the common domain of regularity of the r_j and

$$\Gamma(r) = \{(\underline{A}, r(\underline{A})) \mid \underline{A} \in \operatorname{dom} r\} \subseteq \bigcup_n M_n(\Bbbk)^g$$

the **graph** of r. Let R_r be the subring of $\Bbbk\langle\!\langle\underline{X}\rangle\!\rangle$ generated by $\Bbbk\langle\!\langle\underline{X}'\rangle\!\rangle_{h(r)}$ and $\Bbbk\langle\underline{X}\rangle$. In particular, R_r contains $\underline{X}''$ and all r_j. Finally, let $\mathcal{I}_r$ be the ideal in R_r generated by the set $\{\underline{X}_j'' - r_j(\underline{X}')\}_j$.

Definition 2.2. Let $\mathcal{I}$ be an ideal in $\Bbbk\mathord{<}\underline{X}\mathord{>}$.

(1) $\mathcal{I}$ is **formally rationally resolvable (frr)** with respect to a decomposition of $\underline{X}$ and a tuple r as in Notation 2.1 if
   (a) $\mathcal{I} \cap \Bbbk\mathord{<}\underline{X}'\mathord{>} = 0$; and
   (b) $\mathcal{I}$ generates $\mathcal{I}_r$ as an ideal in R_r.
(2) $\mathcal{I}$ is **geometrically rationally resolvable (grr)** with respect to a decomposition of $\underline{X}$ and a tuple r as in Notation 2.1 if
   (a) $\Gamma(r) \subseteq Z(\mathcal{I})$; and
   (b) every polynomial in $\Bbbk\mathord{<}\underline{X}\mathord{>}$, which vanishes on $\Gamma(r)$, also vanishes on $Z(\mathcal{I})$.

In both cases we call r the **rational resolvent** of $\mathcal{I}$.

From a geometric perspective the grr property is more appealing, however frr is easier to handle algebraically.

2.4. **A Nullstellensatz.** Theorem 2.5 below is the basic version of our Nullstellensatz.

Definition 2.3. An ideal $\mathcal{I} \subseteq \Bbbk\mathord{<}\underline{X}\mathord{>}$ is said to have the **Nullstellensatz property** if for each $f \in \Bbbk\mathord{<}\underline{X}\mathord{>}$,

$$f \in \mathcal{I} \quad \Leftrightarrow \quad f|_{Z(\mathcal{I})} = 0. \tag{2.4}$$

In classical algebraic geometry this coincides with being a radical ideal by Hilbert's Nullstellensatz.

Proposition 2.4. *Assume the setup is as in Notation 2.1. Then:*

(a) *There exists an isomorphism $\alpha : R_r/\mathcal{I}_r \to \Bbbk\,\mathord{<\!\!\!\{}\underline{X}'\mathord{\}\!\!\!>}_{h(r)}$;*
(b) *A polynomial $p \in \Bbbk\mathord{<}\underline{X}\mathord{>}$ vanishes on $\Gamma(r)$ if and only if $p \in \mathcal{I}_r \cap \Bbbk\mathord{<}\underline{X}\mathord{>}$;*
(c) *Assume the ideal $\mathcal{I}$ of $\Bbbk\mathord{<}\underline{X}\mathord{>}$ is grr with rational resolvent r. Then $\mathcal{I}$ satisfies the Nullstellensatz property if and only if $\mathcal{I} = \mathcal{I}_r \cap \Bbbk\mathord{<}\underline{X}\mathord{>}$.*

Proof. (i) The isomorphism is given by $\underline{X}' \mapsto \underline{X}'$ and $\underline{X}'' \mapsto r(\underline{X}')$.
(ii) Let $p \in \Bbbk\mathord{<}\underline{X}\mathord{>}$ be arbitrary. By [Ami66, Theorem 16], $p(\underline{A}, r(\underline{A})) = 0$ for all $\underline{A} \in \operatorname{dom} r$ if and only if $q = p(\underline{X}', r(\underline{X}'))$ equals 0 in $\Bbbk\,\mathord{<\!\!\!\{}\underline{X}'\mathord{\}\!\!\!>}$. Since the height of q is at most $h(r)$, the former is equivalent to $p \in \mathcal{I}_r$ by (i), so the claim follows.
(iii) By the definition, $\mathcal{I}$ is grr and has the Nullstellensatz property if and only if

$$\mathcal{I} = \left\{ p \in \Bbbk\mathord{<}\underline{X}\mathord{>} \mid p|_{\Gamma(r)} = 0 \right\},$$

but the latter equals $\mathcal{I}_r \cap \Bbbk\mathord{<}\underline{X}\mathord{>}$ by (ii). ■

Let S be a subring of R_1 and R_2. The **coproduct of** R_1 **and** R_2 **over** S is a ring $R_1 *_S R_2$ with homomorphisms $\vartheta_1 : R_1 \to R_1 *_S R_2$ and $\vartheta_2 : R_2 \to R_1 *_S R_2$ satisfying $\vartheta_1|_S = \vartheta_2|_S$ such that for every other ring U with homomorphisms $\vartheta_1' : R_1 \to U$ and $\vartheta_2' : R_2 \to U$ satisfying $\vartheta_1'|_S = \vartheta_2'|_S$ there exists a unique homomorphism $\vartheta : R_1 *_S R_2 \to U$ such that $\vartheta_1' = \vartheta \circ \vartheta_1$ and $\vartheta_2' = \vartheta \circ \vartheta_2$. In other words, $R_1 *_S R_2$ is the categorical pushout of R_1 and R_2 over S. We say that $R_1 *_S R_2$ is **faithful** if the canonical maps $R_1 \to R_1 *_S R_2$ and $R_2 \to R_1 *_S R_2$ are one-to-one.

Theorem 2.5. *Let $\mathcal{I}$ be an ideal of $\Bbbk\langle \underline{X} \rangle$.*

(a) *If $\mathcal{I}$ is frr with rational resolvent r and the coproduct of $\Bbbk\langle \underline{X} \rangle/\mathcal{I}$ and $\Bbbk(\!\!<\underline{X}'>\!\!)_{h(r)}$ over $\Bbbk\langle \underline{X}' \rangle$ is faithful, then $\mathcal{I}$ is grr and satisfies the Nullstellensatz property.*

(b) *If $\mathcal{I}$ is grr and satisfies the Nullstellensatz property, then $\Bbbk\langle \underline{X} \rangle/\mathcal{I}$ embeds into a free skew field.*

Proof. (a) Assume there exists a commutative diagram

$$\begin{tikzcd}
\Bbbk\langle \underline{X}' \rangle \arrow[r, hook] \arrow[d, hook] & \Bbbk\langle \underline{X} \rangle/\mathcal{I} \arrow[d, "\phi_1"] \\
\Bbbk(\!\!<\underline{X}'>\!\!)_{h(r)} \arrow[r, "\phi_0"'] & \mathcal{C}
\end{tikzcd}$$

where

$$\mathcal{C} = \Bbbk\langle \underline{X} \rangle/\mathcal{I} *_{\Bbbk\langle \underline{X}' \rangle} \Bbbk(\!\!<\underline{X}'>\!\!)_{h(r)}$$

is the coproduct. Since $\mathcal{I} \subseteq \mathcal{I}_r$, the inclusion $\Bbbk\langle \underline{X} \rangle \subseteq R_r$ induces a homomorphism $\beta : \Bbbk\langle \underline{X} \rangle/\mathcal{I} \to R_r/\mathcal{I}_r$. Since the sets $\underline{X}'$ and $\underline{X}''$ are disjoint, R_r is the coproduct of $\Bbbk\langle \underline{X} \rangle$ and $\Bbbk(\!\!<\underline{X}'>\!\!)_{h(r)}$ over $\Bbbk\langle \underline{X}' \rangle$, thus ϕ_0 and the composite of the quotient map $\Bbbk\langle \underline{X} \rangle \to \Bbbk\langle \underline{X} \rangle/\mathcal{I}$ and ϕ_1 induce a homomorphism $R_r \to \mathcal{C}$ whose kernel includes $\mathcal{I}$ and thus also $\mathcal{I}_r$. Therefore there exists a homomorphism $\phi_2 : R_r/\mathcal{I}_r \to \mathcal{C}$ such that the diagram

$$\begin{tikzcd}
\Bbbk\langle \underline{X} \rangle/\mathcal{I} \arrow[r, "\phi_1"] \arrow[d, "\beta"'] & \mathcal{C} \\
R_r/\mathcal{I}_r \arrow[ur, "\phi_2"'] &
\end{tikzcd}$$

commutes. Since ϕ_1 is injective by assumption, β is also injective, and so $\mathcal{I} = \mathcal{I}_r \cap \Bbbk\langle \underline{X} \rangle$. Therefore $\mathcal{I}$ is grr and has the Nullstellensatz property by Proposition 2.4(iii).

(b) Let r be the rational resolvent of $\mathcal{I}$. Consider the mapping

$$\Phi : \Bbbk\langle \underline{X} \rangle \to \Bbbk(\!\!<\underline{X}'>\!\!), \quad p \mapsto p(\underline{X}', r(\underline{X}')). \tag{2.5}$$

This homomorphism is a composition of a quotient map, β from (A), α from Proposition 2.4(i) and an inclusion. But α is injective by the assumption and Proposition 2.4(iii), so we have $\ker \Phi = \mathcal{I}$ and therefore obtain an embedding $\Bbbk\langle \underline{X} \rangle/\mathcal{I} \hookrightarrow \Bbbk(\!\!<\underline{X}'>\!\!)$. ■

The second assumption in Theorem 2.5(a) might be somewhat difficult to check, so we present in Proposition 2.6 two alternative sufficient conditions for the conclusion of Theorem 2.5(a) to hold that are easier to verify.

Proposition 2.6 and its proof rely heavily upon the theory of skew fields as presented in [Coh95], so we recall a few definitions. A $n \times n$ matrix A over a ring R is **full** if $A = BC$ for $n \times m$ matrix B and $m \times n$ matrix C implies $m \geq n$. A homomorphism $\varphi : R \to S$ is

honest if it maps full matrices over R to full matrices S when applied entry-wise. A ring R is a **free ideal ring**, or **fir**, if every left (right) ideal in R is a free left (right) R-module of unique rank; see [Coh06, Section 2.2] and [Coh06, Proposition 5.5.1]. Typical examples are free algebras and free group algebras. The most important property of a fir for our purpose is that it honestly embeds into its universal skew field of fractions. However, being fir is quite a strong condition; for example, $\mathbb{k}[x, y]$ is not a fir since (x, y) is not a free left $\mathbb{k}[x, y]$-module. A bit wider class of rings with honest embeddings into universal skew fields of fractions are Sylvester domains [Coh66, Theorem 4.5.8]; see also [Coh06, Section 5.5] and [DS78] for an extensive study.

Proposition 2.6. *Let $\mathcal{I}$ be frr with rational resolvent r. Then the coproduct of $\mathbb{k}\langle\underline{X}\rangle/\mathcal{I}$ and $\mathbb{k}(\!\langle\underline{X}'\rangle\!)_{h(r)}$ over $\mathbb{k}\langle\underline{X}'\rangle$ is faithful if*

(a) *$\mathbb{k}\langle\underline{X}\rangle/\mathcal{I}$ is a fir, or more generally, a Sylvester domain; or*
(b) *$h(r) \leq 1$ and $\mathbb{k}\langle\underline{X}\rangle/\mathcal{I}$ embeds into a skew field.*

Proof. Observe that the coproduct of R_1 and R_2 over S is faithful if R_1 and R_2 embed into some ring in a way such that the embeddings agree on S.

(a) We claim that the inclusion $\mathbb{k}\langle\underline{X}'\rangle \hookrightarrow \mathbb{k}\langle\underline{X}\rangle/\mathcal{I}$ is honest. Indeed, assume that a $n \times n$ matrix A over $\mathbb{k}\langle\underline{X}'\rangle$ has a factorization $A = B_0C_0$, where B_0 is $n \times m$ matrix and C_0 is $m \times n$ matrix over $\mathbb{k}\langle\underline{X}\rangle/\mathcal{I}$. Therefore there exist matrices B_1 and C_1 over $\mathbb{k}\langle\underline{X}\rangle$ of the same sizes as B_0 and C_0, respectively, such that $A - B_1C_1$ is a matrix over $\mathcal{I}$. If we apply the homomorphism Φ from (2.5) in the proof of Theorem 2.5(b) on B_1 and C_1 entry-wise, we get $A = B_2C_2$ for matrices B_2 and C_2 over $\mathbb{k}(\!\langle\underline{X}'\rangle\!)$ of appropriate sizes. Since $\mathbb{k}\langle\underline{X}'\rangle$ is a Sylvester domain with the universal skew field of fractions $\mathbb{k}(\!\langle\underline{X}'\rangle\!)$, the inclusion $\mathbb{k}\langle\underline{X}'\rangle \subseteq \mathbb{k}(\!\langle\underline{X}'\rangle\!)$ is honest, so there exist matrices B_3 and C_3 over $\mathbb{k}\langle\underline{X}'\rangle$ of sizes $n \times m$ and $m \times n$, respectively, such that $A = B_3C_3$. Therefore the claim holds. Thus $\mathbb{k}(\!\langle\underline{X}'\rangle\!)$ embeds into the universal skew field of fractions D of $\mathbb{k}\langle\underline{X}\rangle/\mathcal{I}$ by [Coh95, Theorem 4.5.10], so

$$\begin{tikzcd}
\mathbb{k}\langle\underline{X}'\rangle \arrow[r, hook] \arrow[d, hook] & \mathbb{k}\langle\underline{X}\rangle/\mathcal{I} \arrow[d, hook] \\
\mathbb{k}(\!\langle\underline{X}'\rangle\!) \arrow[r, hook] & D
\end{tikzcd}$$

is a desired diagram.

(b) If $\mathbb{k}\langle\underline{X}\rangle/\mathcal{I}$ embeds into a skew field D, then $\mathbb{k}\langle\underline{X}'\rangle$ also embeds into D. Since $\mathbb{k}(\!\langle\underline{X}'\rangle\!)$ is the universal skew field of fractions of $\mathbb{k}\langle\underline{X}'\rangle$, there exists a local homomorphism from $\mathbb{k}(\!\langle\underline{X}'\rangle\!)$ to a skew subfield of D generated by the image of $\mathbb{k}\langle\underline{X}'\rangle$. Therefore $\mathbb{k}(\!\langle\underline{X}'\rangle\!)_1$ also embeds into D and the diagram

$$\begin{tikzcd} \Bbbk\mathop{<}\underline{X}'\mathop{>} \arrow[r, hook] \arrow[d, hook] & \Bbbk\mathop{<}\underline{X}\mathop{>}/\mathcal{I} \arrow[d, hook] \\ \Bbbk\mathop{(\!<}\underline{X}'\mathop{>\!)}_1 \arrow[r, hook] & D \end{tikzcd}$$

commutes. ■

2.5. **Examples and counterexamples.** In this subsection we present examples illustrating the strength of our results. We start with a simple family of ideals satisfying the assumptions of Theorem 2.5(a). Thus these ideals are all rationally resolvable in both senses and satisfy the Nullstellensatz property.

Example 2.7. For some $i_1, \dots, i_m, j_1, \dots, j_n \in \mathbb{N}$ with $i_1 \neq j_1$ and $i_m \neq j_n$ consider

$$\mathcal{I} = (X_{i_1} \cdots X_{i_m} - X_{j_1} \cdots X_{j_n}) \subseteq \Bbbk\mathop{<}\underline{X}\mathop{>}.$$

As a side product of a result by Lewin and Lewin in [LL78, Theorem 3] on embedding of the group algebra of a torsion-free one-relator group into a skew field, $\Bbbk\mathop{<}\underline{X}\mathop{>}/\mathcal{I}$ embeds into a skew field by [LL78, Corollary 6.3]. If at least one symbol appears exactly once in the given relation, $\mathcal{I}$ is also frr, so $\mathcal{I}$ satisfies the Nullstellensatz property by Proposition 2.6(b) and Theorem 2.5(a).

For example, if $\mathcal{I} = (X_1X_2X_3 - X_3X_1^2)$, then we choose the decomposition $\underline{X} = \{X_1, X_3\} \cup \{X_2\}$ and the resolvent $r = X_1^{-1}X_3X_1^2X_3^{-1}$. Note that R_r is then the ring generated by $\Bbbk\mathop{<}\underline{X}\mathop{>}$ and f^{-1} for nonzero $f \in \Bbbk\mathop{<}X_1, X_3\mathop{>}$, and $\mathcal{I}$ generates the ideal $\mathcal{I}_r = (X_2 - X_1^{-1}X_3X_1^2X_3^{-1})$ in R_r.

We continue with two families of ideals satisfying the Nullstellensatz property that will be revisited in Section 4 where we discuss noncommutative unitary groups and spherical isometries.

2.5.1. *Towards nc unitary groups.* For $1 \leq \ell \leq n$ let $X_\ell = (X_{ij}^{(\ell)})_{ij}$ and $Y_\ell = (Y_{ij}^{(\ell)})_{ij}$ be $g_\ell \times g_\ell$ matrices of free noncommuting symbols. Moreover, let Rel_ℓ be the set of entries of the matrices $X_\ell Y_\ell - I_{g_\ell}$ and $Y_\ell X_\ell - I_{g_\ell}$. Consider the ideal

$$\mathcal{U}' = (\mathrm{Rel}_1 \cup \cdots \cup \mathrm{Rel}_n)$$

in the ring

$$\Bbbk\mathop{<}\underline{X}, \underline{Y}\mathop{>} = \Bbbk\mathop{<}X_{ij}^{(\ell)}, Y_{ij}^{(\ell)} \colon 1 \leq \ell \leq n,\ 1 \leq i,j \leq g_\ell\mathop{>}.$$

Corollary 2.8. *The ideal $\mathcal{U}'$ satisfies the Nullstellensatz property.*

Proof. The quotient $\Bbbk\mathop{<}\underline{X}, \underline{Y}\mathop{>}/\mathcal{U}'$ is a fir by [Ber74, Theorem 6.1] and [Coh95, Theorem 5.3.9] since

$$\Bbbk\mathop{<}\underline{X}, \underline{Y}\mathop{>}/\mathcal{U}' = \Bbbk\mathop{<}\underline{X}^{(1)}, Y^{(1)}\mathop{>}/(\mathrm{Rel}_1) *_k \cdots *_k \Bbbk\mathop{<}\underline{X}^{(n)}, Y^{(n)}\mathop{>}/(\mathrm{Rel}_n).$$

Thus it is a Sylvester domain by [Coh95, Proposition 4.5.5]. Also, $\mathcal{U}'$ is frr, since Y_ℓ's entries can be expressed as rational functions of X_ℓ's entries from the defining equations.

This can be done by recursive application of the blockwise inversion formula (see e.g. [HJ85, Subsection 0.7.3]),

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}^{-1} = \begin{bmatrix} (A-BD^{-1}C)^{-1} & A^{-1}B(CA^{-1}B-D)^{-1} \\ (CA^{-1}B-D)^{-1}CA^{-1} & (D-CA^{-1}B)^{-1} \end{bmatrix}$$

on matrices X_ℓ. Therefore $\mathcal{U}'$ satisfies the condition of Proposition 2.6(a). ■

2.5.2. *Towards spherical isometries.* Let $\mathcal{S}' = (X_1Y_1 + \cdots + X_gY_g - 1) \subsetneq \Bbbk\!<\!\underline{X},\underline{Y}\!>$ for variables $\underline{X} = \{X_1,\dots,X_g\}$ and $\underline{Y} = \{Y_1,\dots,Y_g\}$.

Corollary 2.9. *The ideal $\mathcal{S}'$ satisfies the Nullstellensatz property.*

Proof. Since $\mathcal{S}'$ is frr with rational resolvent $r = X_1^{-1}(1-X_2Y_2-\cdots-X_gY_g)$, by Proposition 2.6(b) it suffices to prove that $\Bbbk\!<\!\underline{X},\underline{Y}\!>/\mathcal{S}'$ embeds into a skew field. Let

$$R := \Bbbk\!<\!X_{ij}, Y_{ij} \mid 1 \le i,j \le g,\ (X_{ij})(Y_{ij}) = (Y_{ij})(X_{ij}) = I_g\!>.$$

As seen in Corollary 2.8 this ring is a fir and therefore embeddable into a skew field. There is a normal form in R consisting of nc polynomials without terms containing $X_{i1}Y_{1j}$ or $Y_{i1}X_{1j}$ (cf. [Coh66]). It is easy to see that there is a normal form in the ring $\Bbbk\!<\!\underline{X},\underline{Y}\!>/\mathcal{S}'$ consisting of polynomials without X_1Y_1. Now map

$$\Bbbk\!<\!\underline{X},\underline{Y}\!>/\mathcal{S}' \to R, \quad X_i \mapsto X_{2i}, \quad Y_i \mapsto Y_{i2}.$$

This is an embedding at the normal form level, hence $\Bbbk\!<\!\underline{X},\underline{Y}\!>/\mathcal{S}'$ embeds in R. ■

Note that $\Bbbk\!<\!\underline{X},\underline{Y}\!>/\mathcal{S}'$ is a hereditary ring, $(g-1)$-fir but not g-fir by [Ber74, Theorem 6.1], hence it is not a Sylvester domain by [DS78, Proposition 11].

2.5.3. *Counterexamples.* Lastly, we list a few examples which show that the assumptions of Theorem 2.5 cannot be weakened.

Example 2.10.
(1) Even if an ideal $\mathcal{I}$ is rationally resolvable in both senses, this does not imply the Nullstellensatz property or that $\Bbbk\!<\!\underline{X}\!>/\mathcal{I}$ embeds into a skew field; an easy counterexample is $(1-XY) \subsetneq \Bbbk\!<\!X,Y\!>$.
(2) The Weyl algebra is an Ore domain and therefore embeddable into a skew field, but its defining ideal $(XY-YX-1) \subsetneq \Bbbk\!<\!X,Y\!>$ does not satisfy the Nullstellensatz property.
(3) The ring $\Bbbk\!<\!X,Y\!>/(XY)$ has zero divisors and therefore cannot embed into a skew field, but (XY) has the Nullstellensatz property. This follows from the fact that for every $m,n \in \mathbb{N}_0$, not both zero, there exist matrices A and B such that

$$B^mA^n \neq 0, \quad AB = 0, \quad B^{m+1} = 0 = A^{n+1}.$$

Concretely, one can choose the $(m+n+1)\times(m+n+1)$ matrices

$$A = \sum_{i=1}^{n} E_{i,i+1}, \quad B = \sum_{i=n+2}^{n+m} E_{i,i+1} + E_{m+n+1,1}$$

where $E_{i,j}$ are the standard matrix units.

(4) The property frr does not imply grr. The ideal $\mathcal{I} = (X - XYX) \subseteq \Bbbk\text{<}X, Y\text{>}$ is frr with rational resolvent $r = X^{-1}$. Assume that $\mathcal{I}$ is grr. Then obviously exactly one of the symbols X and Y belongs to the first set of the decomposition (2.3), for example X (the other case is treated similarly). Thus $(X - XYX)$ is grr with rational resolvent $s = p(X)q(X)^{-1}$, where p and q are coprime univariate polynomials. Consider the polynomial $q(X)Y - p(X)$. It obviously equals 0 on $\Gamma(s)$, but it does not vanish in $(0, 0)$ if $p(0) \neq 0$ or in $(1, 1)$ if $p(0) = 0$. This is a contradiction since these two points belong to the zero set of $(X - XYX)$.

(5) The Nullstellensatz property together with grr does not imply frr. Consider the ideal

$$(ZW - WZ, Z^3 - W^2) \subseteq \Bbbk\text{<}X, Y, Z, W\text{>}$$

and rational functions $r_Z = (XY^{-1}X)^2$ and $r_W = (XY^{-1}X)^3$. Then

$$\mathcal{I}_r \cap \Bbbk\text{<}X, Y, Z, W\text{>} = (ZW - WZ, Z^3 - W^2).$$

The inclusion $\supseteq$ is trivial and the inclusion $\subseteq$ follows from the fact that the set of words of the form

$$m_0 Z^{e_1} W^{f_1} m_1 \cdots Z^{e_l} W^{f_l} m_l,$$

where $f_i \in \{0, 1\}$ and m_i are words in X and Y, is linearly independent over $\Bbbk$ in $R_r/\mathcal{I}_r$. Thus the given ideal is grr and satisfies the Nullstellensatz property by Proposition 2.4(c). However, it is not frr. Indeed, otherwise at least one of Z, W is in the second set of the decomposition (2.3), say W, and then

$$W - s = \sum_i a_i(ZW - WZ)b_i + \sum_i c_i(Z^3 - W^2)d_i \tag{2.6}$$

holds for some $a_i, b_i, c_i, d_i \in F\text{<}W\text{>}$ and $s \in F$, where $F = \Bbbk\,\langle\!\!\langle X, Y, Z \rangle\!\!\rangle$. Since $F[W]$ is a homomorphic image of $F\text{<}W\text{>}$. Then the equation (2.6) implies $W - s$ is in the ideal of $F[W]$ generated by a polynomial of degree 2, namely the image of $W^2 - Z^3$, which is a contradiction.

3. Realization theory for noncommutative rational functions and bounds for the Nullstellensatz

In this section we give size bounds needed to check the vanishing property $f|_{Z(\mathcal{I})} = 0$ for a grr ideal $\mathcal{I}$. More precisely, we present a concrete bound N, depending on f and the rational resolvent of $\mathcal{I}$, such that $f|_{Z(\mathcal{I})} = 0$ is equivalent to $f|_{Z(\mathcal{I}) \cap M_N(\Bbbk)^g} = 0$; see Theorem 3.9.

Let $\mathcal{I}$ be grr with rational resolvent r. Recall that

$$f|_{Z(\mathcal{I})} = 0 \iff f|_{\Gamma(r)} = 0,$$

which is furthermore equivalent to $f(\underline{X}', r(\underline{X}'))$ being a rational identity. Therefore we are interested in providing bounds for testing whether a rational expression is a rational identity. This can be achieved through realization theory for rational expressions (see [BR11, KVV09, BGM05, HMV06] for realization theory of rational expressions defined in a scalar point and [CR94] for realizations over infinite-dimensional skew fields). Here we present its aspects that are relevant for the task at hand; a more thorough discussion of this subject will be given elsewhere [Vol+]. As we shall need power series expansions about non-scalar points, we start by introducing generalized polynomials (which will form homogeneous components of these power series) in Subsection 3.1. Subsection 3.2 then presents the general realization theory, and its application to the bounds for the Nullstellensatz property are in Subsection 3.3. As an auxiliary result we present size bounds needed to test whether a rational expression is a rational identity, see Theorem 3.8.

Throughout this section let $\underline{Y} = \{Y_1, \dots, Y_g\}$ be a set of freely noncommuting letters and $\mathcal{A} = M_m(\Bbbk)$.

3.1. **Generalized polynomials.** The elements of the free product

$$\mathcal{A}<\underline{Y}> = M_m(\Bbbk) *_{\Bbbk} \Bbbk<\underline{Y}>$$

are called **generalized (nc) polynomials** over $M_m(\Bbbk)$. They can be evaluated in $M_{ms}(\Bbbk)$ via embedding $a \mapsto a \otimes I_s$ of $M_m(\Bbbk)$ into $M_{ms}(\Bbbk)$ and we have

$$\operatorname{Hom}_{M_m}(M_m(\Bbbk)<\underline{Y}>, M_{ms}(\Bbbk)) \cong \operatorname{Hom}(\mathfrak{W}_m(\Bbbk<\underline{Y}>), M_s(\Bbbk)), \tag{3.1}$$

where $\mathfrak{W}_m$ denotes *the matrix reduction functor* as in [Coh95, Section 1.7]. For a free algebra we have

$$\mathfrak{W}_m(\Bbbk<\underline{Y}>) = \Bbbk\langle\mathfrak{Y}\rangle,$$

where

$$\mathfrak{Y} = \{\mathfrak{y}_{ij}^{(k)} \colon 1 \le i,j \le m,\ 1 \le k \le g\}$$

is a set of independent freely noncommuting letters. The isomorphism (3.1) follows from the isomorphism

$$M_m(\Bbbk)<\underline{Y}> \to M_m(\Bbbk\langle\mathfrak{Y}\rangle), \quad E_{ii} Y_k E_{jj} \mapsto \mathfrak{y}_{ij}^{(k)} \cdot E_{ij}, \tag{3.2}$$

where E_{ij} are the standard matrix units in $M_m(\Bbbk)$.

Proposition 3.1. *If $f \in \mathcal{A}<\underline{Y}>$ is of degree h and vanishes on matrices of size $m\lceil\frac{h+1}{2}\rceil$, then $f = 0$.*

Proof. Since the isomorphism (3.2) preserves polynomial degrees, the proposition follows from (3.1) and a well-known fact that there are no nonzero polynomial identities on $M_s(\Bbbk)$ of degree less than $2s$ (see e.g. [Row80, Lemma 1.4.3]). ■

For $Y_i \in \underline{Y}$ let $\mathcal{A}^{Y_i}$ denote the $\mathcal{A}$-bimodule in $\mathcal{A}<\underline{Y}>$ generated by Y_i, i.e. $\mathcal{A}^{Y_i} = \sum \mathcal{A}Y_i\mathcal{A}$, and more generally, $\mathcal{A}^w = \mathcal{A}^{w_1} \cdots \mathcal{A}^{w_{|w|}}$ for $w \in <\underline{Y}>$ (here we set $\mathcal{A}^1 = \mathcal{A}$). Note that $\mathcal{A}^w$ and $\mathcal{A}^{\otimes |w|}$ are isomorphic as $\mathcal{A}$-bimodules; in particular, as a $\mathcal{A}$-bimodule, $\mathcal{A}^w$ does not depend on the letters in w, but just on the length of w.

Lemma 3.2. *Let $w = Y_1 \cdots Y_k$. If $f \in \mathcal{A}^w$ vanishes on $\mathcal{A}$, then $f = 0$.*

Proof. We prove the claim by induction on k. Assume $f \in \mathcal{A}^{Y_1}$ vanishes on $\mathcal{A}$ and consider the homomorphism of $\Bbbk$-algebras

$$\phi : \mathcal{A} \otimes_{\Bbbk} \mathcal{A}^{\mathrm{op}} \to \operatorname{End}_{\Bbbk}(A), \quad a \otimes b \mapsto L_a R_b,$$

where L_a and R_b are multiplications by a on the left and by b on the right, respectively. It is a classical result (see e.g. [Lam91, Theorem 3.1]) that the $\Bbbk$-algebra $\mathcal{A} \otimes \mathcal{A}^{op}$ is simple. Therefore ϕ is injective. Since f can be considered as an element of $\mathcal{A} \otimes \mathcal{A}^{op}$ and its evaluation then corresponds to $\phi(f)$, we have $f = 0$.

Now assume that statement holds for k. Suppose $f \in \mathcal{A}^{Y_1} \cdots \mathcal{A}^{Y_{k+1}}$ vanishes on $\mathcal{A}$. We can write it as

$$f = \sum_i f_i Y_{k+1} a_i,$$

where $a_i \in \mathcal{A}$ are $\Bbbk$-linearly independent and $f_i \in \mathcal{A}^{Y_1} \cdots \mathcal{A}^{Y_k}$. Let $b_1, \dots b_k \in \mathcal{A}$ be arbitrary and $\tilde{f} = f(b_1, \dots, b_k, y_{k+1})$. By the basis of induction we have $\tilde{f} = 0$. Since a_i are $\Bbbk$-linearly independent, we have $f_i(b_1, \dots, b_k) = 0$ for all i. Since b_j were arbitrary, we have $f_i = 0$ by the induction hypothesis and therefore $f = 0$. ■

3.2. **Generalized series.** The completion of $\mathcal{A}<\underline{Y}>$ with respect to the $(\underline{Y})$-adic topology is the algebra of **generalized formal series** over $\mathcal{A}$ and is denoted by $\mathcal{A}\ll\underline{Y}\gg$. We refer the reader to [KVV14, Voi04, Voi10, AM15, HKM11, Pas14] for analytic approaches to free function theory.

If a series $S \in \mathcal{A}\ll\underline{Y}\gg$ is written as

$$S = \sum_{w \in <\underline{Y}>} \sum_{i=1}^{n_w} a_{w,i}^{(0)} w_1 a_{w,i}^{(1)} w_2 \cdots w_{|w|} a_{w,i}^{(|w|)}, \tag{3.3}$$

then let

$$[S, w] = \sum_i a_{w,i}^{(0)} w_1 a_{w,i}^{(1)} w_2 \cdots w_{|w|} a_{w,i}^{(|w|)}. \tag{3.4}$$

This is a well-defined element of $\mathcal{A}<\underline{Y}>$ even though the expansion (3.3) is not uniquely determined. Note that the homogeneous components of S, i.e., $\sum_{|w|=h}[S, w]$ for fixed $h \in \mathbb{N}_0$, also belong to $\mathcal{A}<\underline{Y}>$.

In this exposition, we treat generalized series in a purely algebraic way. However, if $\Bbbk$ is a field of real or complex numbers, one can also consider matrix norms and therefore study the convergence of generalized series in the norm topology; see [KVV14, Section 8.2] for details.

As in the classical setting, a series $S \in \mathcal{A}\ll\underline{Y}\gg$ is invertible if and only if $[S, 1]$ is invertible in $\mathcal{A}$; in that case we have $[S^{-1}, 1] = a^{-1}$ and

$$[S^{-1}, w] = -\sum_{\substack{uv=w, \\ v \neq w}} a^{-1}[S, u][S^{-1}, v] \tag{3.5}$$

for $|w| > 0$.

A series S is **recognizable** if for some $n \in \mathbb{N}$ there exist $\mathbf{c} \in \mathcal{A}^{1\times n}$, $\mathbf{b} \in \mathcal{A}^{n\times 1}$ and $A^{Y_i} \in (\mathcal{A}^{Y_i})^{n\times n}$ for $Y_i \in \underline{Y}$ such that $[S, w] = \mathbf{c}A^w\mathbf{b}$ for all $w \in <\underline{Y}>$, where the notation

$$A^w = A^{w_1} \cdots A^{w_{|w|}} \in (\mathcal{A}^w)^{n\times n}$$

is used. In this case $(\mathbf{c}, A, \mathbf{b})$ is called a *linear representation of dimension* n of S. Observe that one can also write

$$S = \sum_w \mathbf{c}A^w\mathbf{b} = \mathbf{c}\left(\sum_w A^w\right)\mathbf{b} = \mathbf{c}\left(I_n - \sum_{i=1}^g A^{Y_i}\right)^{-1}\mathbf{b}.$$

The following theorem shows that the set of recognizable series is closed under basic arithmetic operations.

Theorem 3.3. *For $i \in \{1,2\}$ let S_i be a recognizable series with representation $(\mathbf{c}_i, A_i, \mathbf{b}_i)$ of dimension n_i and S be an invertible recognizable series with representation $(\mathbf{c}, A, \mathbf{b})$ of dimension n. Then:*

(1) 1 *is recognizable with representation* $(1, 0, 1)$*;*
(2) $Y_i + a$ *for* $a \in \mathcal{A}$ *is recognizable with representation*

$$\left(\begin{pmatrix} 1 & a \end{pmatrix}, \begin{pmatrix} 0 & \delta_{ij}Y_j \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) \tag{3.6}$$

of dimension 2, where δ_{ij} is the Kronecker's delta;
(3) $S_1 + aS_2$ *is recognizable with a representation*

$$\left(\begin{pmatrix} \mathbf{c}_1 & a\mathbf{c}_2 \end{pmatrix}, \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}, \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}\right) \tag{3.7}$$

of dimension $n_1 + n_2$;
(4) S_1S_2 *is recognizable with a representation*

$$\left(\begin{pmatrix} \mathbf{c}_1 & \mathbf{c}_1\mathbf{b}_1\mathbf{c}_2 \end{pmatrix}, \begin{pmatrix} A_1 & A_1\mathbf{b}_1\mathbf{c}_2 \\ 0 & A_2 \end{pmatrix}, \begin{pmatrix} 0 \\ \mathbf{b}_2 \end{pmatrix}\right) \tag{3.8}$$

of dimension $n_1 + n_2$;
(5) S^{-1} *is recognizable with a representation*

$$\left(\begin{pmatrix} -a^{-1}\mathbf{c} & a^{-1} \end{pmatrix}, \begin{pmatrix} A(I - \mathbf{b}a^{-1}\mathbf{c}) & A\mathbf{b}a^{-1} \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) \tag{3.9}$$

of dimension $n+1$, where $a = [S, 1]$.

Proof. (1) and (2) are trivial.

(3) This is clear since

$$[S_1 + aS_2, w] = [S_1, w] + a[S_2, w] = \mathbf{c}_1A_1^w\mathbf{b}_1 + a\mathbf{c}_2A_2^w\mathbf{b}_2 = \begin{pmatrix} \mathbf{c}_1 & a\mathbf{c}_2 \end{pmatrix} \cdot \begin{pmatrix} A_1^w & 0 \\ 0 & A_2^w \end{pmatrix} \cdot \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}.$$

(4) If $w = w_1 \cdots w_\ell$, let $M_j = A_1^{w_j}$, $N_j = A_2^{w_j}$ and $Q = \mathbf{b}_1\mathbf{c}_2$. Since

$$\begin{aligned} [S_1S_2, w] &= \sum_{uv=w} [S_1, u][S_2, w] = \mathbf{c}_1\mathbf{b}_1\mathbf{c}_2A_2^w\mathbf{b}_2 + \mathbf{c}_1\left(\sum_{uv=w,|u|>0} A_1^u\mathbf{b}_1\mathbf{c}_2A_2^v\right)\mathbf{b}_2 \\ &= (\mathbf{c}_1Q)N_1\cdots N_\ell c_2 + \mathbf{c}_1\left(\sum_{k=1}^{\ell} M_1\cdots M_kQN_{N+1}\cdots N_\ell\right)\mathbf{b}_2, \end{aligned}$$

it is enough to prove the equality

$$\prod_{j=1}^{\ell}\begin{pmatrix} M_j & M_jQ \\ 0 & N_j\end{pmatrix} = \begin{pmatrix} \prod_{j=1}^{\ell} M_j & \sum_{k=1}^{\ell}\left(\prod_{j=1}^{k} M_j\right) Q \left(\prod_{j=k+1}^{\ell} N_j\right) \\ 0 & \prod_{j=1}^{\ell} N_j\end{pmatrix}$$

and this can be easily done by induction on ℓ.

(5) If $w = w_1\cdots w_\ell$, let $M_j = A^{w_j}$ and $Q = \mathbf{b}a^{-1}\mathbf{c}$. The statement is proved by induction on ℓ. It obviously holds for $\ell = 0$, so let $\ell \geq 1$. Note that representation (3.9) yields a series T with

$$[T, w] = -a^{-1}\mathbf{c}A^{w_1}(I - \mathbf{b}a^{-1}\mathbf{c})\cdots A^{w_{\ell-1}}(I - \mathbf{b}a^{-1}\mathbf{c})A^{w_\ell}\mathbf{b}a^{-1}.$$

By (3.5) and the inductive step we have

$$\begin{aligned}[S^{-1}, w] &= -\sum_{uv=w, v\neq w} a^{-1}[S,u][T,v] \\ &= -a^{-1}\mathbf{c}\left(M_1\cdots M_\ell - \sum_{i=1}^{l-1} M_1\cdots M_iQM_{i+1}(I-Q)\cdots M_{\ell-1}(I-Q)M_\ell\right)\mathbf{b}a^{-1} \\ &= -a^{-1}\mathbf{c}M_1(I-Q)\cdots M_{\ell-1}(I-Q)M_\ell\mathbf{b}a^{-1} \\ &= [T,w]\end{aligned}$$

and thus the statement holds. ■

Let $(\mathbf{c}, A, \mathbf{b})$ be a linear representation of dimension n. For $N \in \mathbb{N}\cup\{0\}$ we define

$$\mathcal{U}_N = \{\mathbf{u} \in \mathcal{A}^{1\times n} \colon \mathbf{u}A^w\mathbf{b} = 0\ \forall |w| \leq N\}.$$

These are left $\mathcal{A}$-modules and $\mathcal{U}_N \supseteq \mathcal{U}_{N+1}$. Furthermore, let

$$\mathcal{U}_\infty = \bigcap_{N\in\mathbb{N}} \mathcal{U}_N.$$

In the language of control theory, this module represents an obstruction for the *controllability* of the realization [BGM05, Section 5] of a rational function defined in 0.

Lemma 3.4. *If $\mathcal{U}_N = \mathcal{U}_{N+1}$, then $\mathcal{U}_{N+1} = \mathcal{U}_{N+2}$.*

Proof. If $\mathbf{u} \notin \mathcal{U}_{N+2}$, then $\mathbf{u}A^{Y_iw}\mathbf{b} \neq 0$ for some $Y_i \in \underline{Y}$ and $|w| = k \leq N+1$. Let $f \in \mathcal{A}^{Y_iw}$ be the nonzero entry of $\mathbf{u}A^{Y_iw}\mathbf{b}$. Let $\{Z_0, \dots, Z_k\}$ be auxiliary freely noncommuting letters; since $\mathcal{A}^{Y_iw}$ as a $\mathcal{A}$-module depends only on length of Y_iw, we can treat f as an element of $\mathcal{A}^{Z_0\cdots Z_k}$ and $f(Z_0,\dots,Z_k) \neq 0$. By Lemma 3.2, there exists $b \in \mathcal{A}$ such that $f(b, Z_1, \dots, Z_k) \neq 0$. Going back to module $\mathcal{A}^w \cong \mathcal{A}^{Z_1\cdots Z_k}$, we have $f(b, w_1, \dots, w_k) \neq 0$ and so $\mathbf{u}A^{Y_i}|_{Y_i=b}A^w\mathbf{b} \neq 0$. Therefore $\mathbf{u}A^{Y_i}|_{Y_i=b} \notin \mathcal{U}_{N+1} = \mathcal{U}_N$ and hence $\mathbf{u}A^{Y_i}|_{Y_i=b}A^{w'}\mathbf{b} \neq 0$ for some $|w'| = k' \leq N$. Let $g \in \mathcal{A}^{Z_0w'}$ be such entry of $\mathbf{u}A^{Y_i}|_{Y_i=Z_0}A^{w'}\mathbf{b}$ that $g(b, w'_1, \dots, w'_{k'}) \neq 0$. Thus $g \neq 0$ and also $g(Y_i, w'_1, \dots, w'_{k'}) \neq 0$. Therefore $\mathbf{u}A^{Y_i}A^{w'}\mathbf{b} \neq 0$ and $\mathbf{u} \notin \mathcal{U}_{N+1}$. ■

Lemma 3.5. *If a representation $(\mathbf{c}, A, \mathbf{b})$ is of dimension n, then $\mathcal{U}_\infty = \mathcal{U}_{mn-1}$, where $m^2 = \dim_{\Bbbk}\mathcal{A}$.*

Proof. The statement trivially holds for $\mathbf{b}=0$, so we assume $\mathbf{b}\neq 0$. By Morita equivalence between $M_m(\Bbbk)$ and $\Bbbk$, the dimension of every left $\mathcal{A}$-module as a vector space over $\Bbbk$ is divisible by m. Since the dimension of the vector space $\mathcal{A}^{1\times n}$ over k is m^2n and $\mathbf{b}\neq 0$, the descending chain of left $\mathcal{A}$-modules $\{\mathcal{U}_N\}_{N\in\mathbb{N}}$ stops by Lemma 3.4 and

$$\mathcal{A}^{1\times n}\supseteq\mathcal{U}_0\supseteq\mathcal{U}_1\supseteq\cdots\supseteq\mathcal{U}_{mn-1}=\mathcal{U}_{mn}=\cdots. \qquad \blacksquare$$

Proposition 3.6. *If* $(\mathbf{c},A,\mathbf{b})$ *is a representation of dimension* n *and* $\mathbf{c}A^w\mathbf{b}=0$ *for all* $|w|<mn$*, then* $(\mathbf{c},A,\mathbf{b})$ *represents the zero series.*

Proof. The assumption asserts $\mathbf{c}\in\mathcal{U}_{mn-1}$, so $\mathbf{c}A^w\mathbf{b}=0$ for all $w\in<\underline{Y}>$ by Lemma 3.5. $\blacksquare$

Let r be a rational expression in $\underline{X}$ and assume it is defined in $\underline{P}\in M_m(\Bbbk)^g$. Then r can be formally expanded into a generalized series about $\underline{P}$; more precisely, $r(\underline{Y}+\underline{P})$ can be considered as an element of $\mathcal{A}\ll\underline{Y}\gg$. Since $r(\underline{Y}+\underline{P})$ lies in the rational closure of $\mathcal{A}<\underline{Y}>$, it is a recognizable series by Theorem 3.3. We say that a linear representation $(\mathbf{c},A,\mathbf{b})$ is a **realization of r about $\underline{P}$** if $(\mathbf{c},A,\mathbf{b})$ is a representation of $r(\underline{Y}+\underline{P})$.

Example 3.7.

(1) Let $r=X_1^{-1}(1-\sum_{j=2}^g X_jY_j)$. The right-hand side expression is defined in the scalar point $(1,0,\dots,0)$; so $r=S(X_1-1,X_2,Y_2,\dots,X_g,Y_g)$ for $S=(Y+1)^{-1}(1-\sum_{j=2}^g X_jY_j)$ and the latter can be expanded into a (generalized) series. If $g=1$, then S has a linear representation $(1,-Y,1)$ of dimension 1. Otherwise if $g\geq 2$, then one can easily check that the inverse of

$$\begin{bmatrix} 1+Y & 0 & X_2 & \cdots & X_g \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & -Y_2 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -Y_g & 0 & \cdots & 1 \end{bmatrix}$$

equals

$$\begin{bmatrix} (1+Y)^{-1} & -(1+Y)^{-1}\sum_{j>1}X_jY_j & -(1+Y)^{-1}X_2 & \cdots & -(1+Y)^{-1}X_g \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & Y_2 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & Y_g & 0 & \cdots & 1 \end{bmatrix}$$

so S has a representation

$$\left(\begin{bmatrix}1 & 0 & 0 & \cdots & 0\end{bmatrix},\quad -YE_{11},\ -X_2E_{13},\ Y_2E_{32},\ \dots,\ -X_gE_{1,g+1},\ Y_gE_{g+1,2},\quad \begin{bmatrix}1\\1\\0\\\vdots\\0\end{bmatrix}\right)$$

of dimension $g+1$, where $E_{ij}\in\Bbbk^{(g+1)\times(g+1)}$ are the standard matrix units.

(2) Next consider $r = (X_1X_2 - X_2X_1)^{-1}$. Let $\underline{P} = (P_1, P_2)$ be a pair of 2×2 matrices such that $Q = (P_1P_2 - P_2P_1)^{-1}$ exists, e.g. $P_1 = E_{12}$ and $P_2 = E_{21}$. Then $r(X_1, X_2) = S(X_1 - P_1, X_2 - P_2)$, where

$$S = Q(1 - (P_2Y_1 - Y_1P_2)Q - (Y_2P_1 - P_1Y_2)Q - (Y_2Y_1 - Y_1Y_2)Q)^{-1}.$$

Using the blockwise inversion formula (see e.g. [HJ85, Subsection 0.7.3]) it can be easily seen that S has a representation

$$\left(\begin{pmatrix} Q & 0 & 0 \end{pmatrix}, \begin{pmatrix} -Y_1P_2Q + P_2Y_1Q & Y_1 & 0 \\ 0 & 0 & 0 \\ -Y_1Q & 0 & 0 \end{pmatrix}, \begin{pmatrix} Y_2P_1Q - P_1Y_2Q & 0 & -Y_2 \\ -Y_2Q & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}\right)$$

of dimension 3.

We can now give the main result of this subsection, namely explicit size bounds required for testing whether a nc rational expression is a rational identity.

Theorem 3.8. *Let r be a rational expression in $\underline{X}$. Assume r admits a realization of dimension n about a point in $M_m(\Bbbk)^g$. If r is an identity on matrices of size $N = m\lceil \frac{mn}{2} \rceil$, then r is a rational identity.*

Proof. Let $\underline{P} \in M_m(\Bbbk)^g \cap \operatorname{dom} r$ and $(\mathbf{c}, A, \mathbf{b})$ be a realization of r about $\underline{P}$ of dimension n. Let $\underline{X}(N)$ be the tuple of generic $N \times N$ matrices, i.e. $X_j(N) = (x_{\imath\jmath}^{(j)})_{\imath\jmath}$, where $x_{\imath\jmath}^{(j)}$ are independent commuting variables. Because $M_m(\Bbbk)^g \cap \operatorname{dom} r \neq \varnothing$ and N is a multiple of m, we also have $M_N(\Bbbk)^g \cap \operatorname{dom} r \neq \varnothing$, so r can be evaluated on $\underline{X}(N)$. Then $r(\underline{X}(N))$ is a matrix of commutative rational functions and the matrix of their expansions about $\underline{P}$ is

$$M(\underline{X}(N)) = \sum_w \mathbf{c}\left(A^w|_{\underline{Y}=\underline{X}(N)-\underline{P}}\right)\mathbf{b}. \tag{3.10}$$

The formal differentiation of these commutative power series yields

$$\frac{\mathrm{d}}{\mathrm{d}t^h} M\big(\underline{P} + t(\underline{X}(N) - \underline{P})\big)\Big|_{t=0} = h! \sum_{|w|=h} \mathbf{c}\left(A^w|_{\underline{Y}=\underline{X}(N)-\underline{P}}\right)\mathbf{b}. \tag{3.11}$$

If r vanishes on matrices of size N, then $r(\underline{X}(N)) = 0$ and so $M(\underline{X}(N)) = 0$; therefore the left-hand the side of (3.11) equals 0 for every h, hence the same holds for the right-hand side. Since $\sum_{|w|=h} \mathbf{c}(A^w|_{\underline{Y}=\underline{X}-\underline{P}})\mathbf{b}$ is a generalized polynomial of degree h, we have $\mathbf{c}A^w\mathbf{b} = 0$ for all $|w| < mn$ by Proposition 3.1. Finally r is a rational identity by Proposition 3.6. ∎

3.3. **Bounds for grr ideals.** We now have enough tools at our disposal to prove the main result of this section.

Theorem 3.9. *Let $\mathcal{I}$ be grr ideal with rational resolvent $r = (r_1, \dots, r_k)$. Assume there is a tuple of $m \times m$ matrices $\underline{P} \in \operatorname{dom} r$ and that rational functions r_j can be defined by rational expressions with realizations about $\underline{P}$ of dimensions at most n.*

If $f \in \Bbbk\mathord{<}\underline{X}\mathord{>}$ is of degree u and has v terms, and vanishes on $Z(\mathcal{I}) \cap M_N(\Bbbk)^g$, where

$$N = m\lceil \tfrac{muv\max(n,2)}{2} \rceil, \tag{3.12}$$

then f vanishes on $Z(\mathcal{I})$.

Proof. As already observed at the beginning of this section, it is enough to prove that $q = f(\underline{X}', r(\underline{X}'))$ is a rational identity. By the assumptions and Theorem 3.3, this rational function can be defined by a rational expression with realization about $\underline{P}$ of dimension at most $uv\max(n,2)$. Indeed, when constructing the realization of q using Theorem 3.3 from realizations of r_j, every symbol in f contributes a realization of dimension either 2 (if it belongs to $\underline{X}'$) or at most n (if it belongs to $\underline{X}''$), and the sums and products result in addition of the dimensions of intermediate realizations. Now the statement follows by Theorem 3.8. ∎

Corollary 3.10. *Assume the setting of Theorem 3.9. If $f \in \Bbbk\mathord{<}\underline{X}\mathord{>}$ is of degree d and vanishes on $Z(\mathcal{I}) \cap M_{N'}(\Bbbk)^g$, where*

$$N' = m\lceil \tfrac{md(g+1)^d\max(n,2)}{2} \rceil,$$

then f vanishes on $Z(\mathcal{I})$.

Let us determine the bound N in (3.12) from Theorem 3.9 as a function of uv for some concrete ideals.

Example 3.11.

(1) The ideal $\mathcal{T}' = (1 - X_1Y_1, 1 - Y_1X_1, \dots, 1 - X_gY_g, 1 - Y_gX_g)$ is a special case of an ideal from Corollary 2.8, so it is grr. Its rational resolvent consists of the functions X_j^{-1}, which have realizations of dimension 1 about the point $(1,\dots,1)$ by Example 3.7(1). Thus Theorem 3.9 implies $N = uv$.

(2) Let $g \geq 2$; the ideal $\mathcal{S}' = (X_1Y_1 + \cdots + X_gY_g - 1)$ was studied in Corollary 2.9 and is grr. By Example 3.7(1), its resolvent has a realization of dimension $g + 1$ about a scalar point, so $N = \lceil \frac{g+1}{2} uv \rceil$.

(3) Consider the ideal $\mathcal{I} = (1 - (X_1X_2 - X_2X_1)X_3) \subseteq \Bbbk\mathord{<}\underline{X}\mathord{>}$; evidently it is grr with rational resolvent $r = (X_1X_2 - X_2X_1)^{-1}$. Hence $N = 6uv$ by Example 3.7(2).

(4) Lastly, let $X = (X_{ij})_{ij}$ and $Y = (Y_{ij})_{ij}$ be $g \times g$ matrices with freely noncommuting entries and let $\mathcal{U}'$ be the ideal generated by the entries of $XY - I_g$ and $YX - I_g$. Assume $g > 1$; the case $g = 1$ is treated in (1). As already observed in the proof of Corollary 2.8, $\mathcal{U}'$ is grr, with the resolvent consisting of the entries of X^{-1}. Since the (i,j)-th entry of this matrix equals

$$e_i^t(I_g - (-X_g + I_g))^{-1}e_j,$$

where e_i and e_j are the standard unit vectors in $\Bbbk^g$, it has a realization of dimension g about I_g. Therefore Theorem 3.9 yields $N = \lceil \frac{g}{2} uv \rceil$.

4. Null- and Positivstellensätze for $*$-ideals

In this section we turn our attention to algebras with involution. In addition to zero sets this setting also rises questions about positivity sets of nc polynomials [HMP07]. We give Null- and Positivstellensätze for certain classes of rationally resolvable $*$-ideals in free $*$-algebras. We prove a Nullstellensatz for nc unitary groups and spherical isometries (see Theorems 4.10 and 4.8) and use it to deduce Positivstellensätze in Subsection 4.5, following work of Helton, McCullough and Putinar [HMP04]. To pass between our results for free algebras and free $*$-algebras we employ (real) algebraic geometry, cf. Subsection 4.3.

We shall be interested in the free $*$-algebra. Let $<\underline{X},\underline{X}^\intercal>$ be the monoid freely generated by $\underline{X}=\{X_1,\dots,X_g\}$ and $\underline{X}^\intercal=\{X_1^\intercal,\dots,X_g^\intercal\}$, i.e., $<\underline{X},\underline{X}^\intercal>$ consists of words in the $2g$ noncommuting letters $X_1,\dots,X_g,X_1^\intercal,\dots,X_g^\intercal$ (including the empty word $\varnothing$ which plays the role of the identity 1). For a field $\Bbbk$ endowed with an involution (an automorphism of order 2) let $\Bbbk<\underline{X},\underline{X}^\intercal>$ denote the $\Bbbk$-algebra freely generated by $\underline{X},\underline{X}^\intercal$. This is a free algebra with involution $^\intercal$ that is uniquely determined by the involution of the base field and the rule $X_j^{\intercal\intercal}=X_j$. An ideal $\mathcal{I}\subseteq\Bbbk<\underline{X},\underline{X}^\intercal>$ is called a $*$**-ideal** if $\mathcal{I}^\intercal=\mathcal{I}$.

4.1. Embedding quotients by rationally resolvable $*$-ideals into skew fields with involution.

Let $\mathcal{I}$ be a frr $*$-ideal in $\Bbbk<\underline{X},\underline{X}^\intercal>$ with rational resolvent r. Because we are now dealing with two different partitions of nc variables, namely $\underline{X}\cup\underline{X}^\intercal=\underline{X}'\cup\underline{X}''$, where the right-hand side comes from the decomposition (2.3), we introduce some additional notation:

$$\underline{X}^{(1)}=\underline{X}'\cap\underline{X}'^\intercal,\quad \underline{X}^{(2)}=\underline{X}'\setminus\underline{X}^{(1)},\quad \underline{X}^{(3)}=\underline{X}^{(2)\intercal},\quad \underline{X}^{(4)}=\underline{X}''\setminus\underline{X}^{(3)}.$$

For example, if $g=3$, $X'=\{X_1,X_1^\intercal,X_2\}$ and $X''=\{X_2^\intercal,X_3,X_3^\intercal\}$, then $\underline{X}^{(1)}=\{X_1,X_1^\intercal\}$, $\underline{X}^{(2)}=\{X_2\}$, $\underline{X}^{(3)}=\{X_2^\intercal\}$ and $\underline{X}^{(4)}=\{X_3,X_3^\intercal\}$. Some caution is needed when considering these partitions as arguments in an expression. If, for example, $s=s(U,V)$ is an expression in two variables, we write $s(\underline{X}^{(1)})=s(X_1,X_1^\intercal)$ and $s(\underline{X}^{(1)\intercal})=s(X_1^\intercal,X_1)$, because here $\underline{X}^{(1)}$ and $\underline{X}^{(1)\intercal}$ are different as lists of arguments, although they are equal as sets.

Let $r_\bullet$ be the subtuple of r corresponding to $\underline{X}^{(3)}$.

Lemma 4.1. *If the notation is as above, then*

$$\underline{X}^{(2)}=r_\bullet^\intercal\left(\underline{X}^{(1)\intercal},r_\bullet(\underline{X}')\right)\tag{4.1}$$

holds in $\Bbbk\mathpalette{\langle\!\langle}{}\underline{X}'\mathpalette{\rangle\!\rangle}{}$.

Proof. By definition, $\mathcal{I}_r=R_r\mathcal{I}R_r$ holds and therefore

$$\underline{X}^{(3)}-r_\bullet\left(\underline{X}^{(1)},\underline{X}^{(2)}\right)\in R_r\mathcal{I}R_r.$$

Since $\mathcal{I}$ is closed under involution, it also follows that

$$\underline{X}^{(2)}-r_\bullet^\intercal\left(\underline{X}^{(1)\intercal},\underline{X}^{(3)}\right)\in R_{r^\intercal}\mathcal{I}R_{r^\intercal},$$

where $R_{r^\intercal}$ is the subring generated by $\Bbbk\mathpunct{<\!\!\!(}\underline{X}'^\intercal\mathpunct{)\!\!\!>}$ and $\Bbbk\mathpunct{<}\underline{X},\underline{X}^\intercal\mathpunct{>}$. Combining these two results yields

$$\underline{X}^{(2)} - r_\bullet^\intercal\left(\underline{X}^{(1)\intercal}, r_\bullet\left(\underline{X}^{(1)},\underline{X}^{(2)}\right) + R_r\mathcal{I}R_r\right) \in R_{r^\intercal}\mathcal{I}R_{r^\intercal}.$$

Since $\Gamma(r)\subseteq Z(\mathcal{I})$, substituting $\underline{X}'$ and $\underline{X}''$ by $\underline{A}$ and $r(\underline{A})$ in these expressions, respectively, we have

$$\underline{A}^{(2)} - r_\bullet^\intercal\left(\underline{A}^{(1)\intercal}, r_\bullet(\underline{A})\right) = 0$$

for all tuples $\underline{A}$ in the intersection of domains of all rational functions that appear in the upper expressions. Since this set can be again realized as a domain of a rational function, the considered equalities give rise to rational identities by [Ami66, Theorem 16]. ∎

Proposition 4.2. *If a $*$-ideal $\mathcal{I}$ in $\Bbbk\mathpunct{<}\underline{X},\underline{X}^\intercal\mathpunct{>}$ satisfies the assumptions of Theorem 2.5*(a)*, then $\Bbbk\mathpunct{<}\underline{X},\underline{X}^\intercal\mathpunct{>}/\mathcal{I}$ $*$-embeds into a free skew field with an involution.*

Proof. By Theorem 2.5, the homomorphism

$$\Phi : \Bbbk\mathpunct{<}\underline{X},\underline{X}^\intercal\mathpunct{>} \to \Bbbk\mathpunct{<\!\!\!(}\underline{X}'\mathpunct{)\!\!\!>}, \quad p\mapsto p(\underline{X}', r(\underline{X}'))$$

induces an embedding $\Bbbk\mathpunct{<}\underline{X}\mathpunct{>}/\mathcal{I}\hookrightarrow \Bbbk\mathpunct{<\!\!\!(}\underline{X}'\mathpunct{)\!\!\!>}$. Define an antilinear antihomomorphism of $\Bbbk$-algebras $i:\Bbbk\mathpunct{<}\underline{X}'\mathpunct{>}\to\Bbbk\mathpunct{<\!\!\!(}\underline{X}'\mathpunct{)\!\!\!>}$ by setting

$$i(\underline{X}^{(1)}) = \underline{X}^{(1)\intercal}, \quad i(\underline{X}^{(2)}) = r_\bullet(\underline{X}').$$

By the universal property of $\Bbbk\mathpunct{<\!\!\!(}\underline{X}'\mathpunct{)\!\!\!>}$ as stated in [Coh95, Section 4.4], there exists a local antilinear antihomomorphism $\Bbbk\mathpunct{<\!\!\!(}\underline{X}'\mathpunct{)\!\!\!>}\supseteq K\to\Bbbk\mathpunct{<\!\!\!(}\underline{X}'\mathpunct{)\!\!\!>}$ which we also denote i. By Lemma 4.1, $i(\Bbbk\mathpunct{<}\underline{X}'\mathpunct{>})\subseteq K$, so there is a homomorphism $j:\Bbbk\mathpunct{<}\underline{X}'\mathpunct{>}\to\Bbbk\mathpunct{<\!\!\!(}\underline{X}'\mathpunct{)\!\!\!>}$ defined as $j(p)=i(i(p))$. By the same argument as above, j extends to a local homomorphism of free skew fields with domain $L\subseteq K$. Since $j=\mathrm{id}_L$ holds by (4.1) in Lemma 4.1, j is injective and therefore $\Bbbk\mathpunct{<\!\!\!(}\underline{X}'\mathpunct{)\!\!\!>}=L=K$ by the definition of a local homomorphism. Therefore i is an involution of the free skew field $\Bbbk\mathpunct{<\!\!\!(}\underline{X}'\mathpunct{)\!\!\!>}$. Now the claim follows since Φ is compatible with i and the involution on $\Bbbk\mathpunct{<}\underline{X},\underline{X}^\intercal\mathpunct{>}$. ∎

4.2. **Examples.** In this short subsection we present the main examples of interest to us: nc trigonometric and spherical polynomials, as well as nc unitary groups.

4.2.1. *$*$-representations.* From here on let $\Bbbk=\mathbb{C}$. If $p\in\mathbb{C}\mathpunct{<}\underline{X},\underline{X}^\intercal\mathpunct{>}$ is an nc polynomial and $\underline{A}\in M_n(\mathbb{C})^g$, the evaluation $p(\underline{A})\in M_n(\mathbb{C})$ is defined by simply replacing X_i by A_i and $X_i^\intercal$ by A_i^*, where $*$ is the conjugate transposition. These polynomial evaluations give rise to finite-dimensional $*$-representations of nc polynomials. The notion of a zero set of a $*$-ideal translates accordingly:

$$Z_*(\mathcal{I}) := \bigcup_{n\in\mathbb{N}}\{\underline{A}\in M_n(\mathbb{C})^g \mid \forall g\in\mathcal{I}:\ g(\underline{A},\underline{A}^*)=0\}.$$

4.2.2. *nc trigonometric polynomials.* Let

$$\mathcal{T} = (1 - X_1^\intercal X_1,\, 1 - X_1 X_1^\intercal,\, \dots,\, 1 - X_g^\intercal X_g,\, 1 - X_g X_g^\intercal) \tag{4.2}$$

be a $*$-ideal of $\mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle$. The quotient $\mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle/\mathcal{T}$ is called the algebra of **nc trigonometric polynomials**. Obvioulsy it is isomorphic to the group algebra of the free group on g letters. We are interested in finite-dimensional $*$-representations of $\mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle/\mathcal{T}$, i.e., we evaluate $p \in \mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle$ at g-tuples consisting of unitaries U_j.

4.2.3. *nc spherical polynomials.* Let

$$\mathcal{S} = (1 - X_1^\intercal X_1 - \cdots - X_g^\intercal X_g) \tag{4.3}$$

be a $*$-ideal of $\mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle$. The quotient $\mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle/\mathcal{S}$ is called the algebra of **nc spherical polynomials**. Here we consider evaluations of $p \in \mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle$ at g-tuples of **spherical isometries** $\underline{A}$.

4.2.4. *nc unitary groups.* Let $X = (X_{ij})_{ij}$ be a $g \times g$ matrix of freely noncommuting symbols and let $\mathcal{U}$ be the ideal in

$$\mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle = \mathbb{C}\langle X_{ij}, X_{ij}^\intercal : 1 \le i, j \le g \rangle$$

generated by the set of $2g^2$ relations imposed by $XX^\intercal = I_g$ and $X^\intercal X = I_g$. Then the algebra $\mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle/\mathcal{U}$ is a **nc unitary group**. The notion is due to Brown [Bro81]; see also [Wo87]. The points of the corresponding zero set are g^2-tuples $\underline{A} = (A_{ij})_{i,j=1}^g$ of square matrices of the same size satisfying $\underline{A}^* \underline{A} = I_g$. We say that such tuple is a **g-partitioned unitary**. Matrices A_{ij} are called blocks of $\underline{A}$.

4.3. **Real structure on a complex variety.** The aim of this subsection is to establish a few assertions from algebraic geometry that will enable us to use the results of Section 2 in the involution setting. By a **variety** we always mean a Zariski closed subset of an affine space.

Let V be a $\mathbb{C}$-vector space. A map $J : V \to V$ is a **real structure on** V if it is conjugate-linear and satisfies $J^2 = \mathrm{id}_V$. If V_J is the J-fixed subspace of V, then $\dim_\mathbb{R} V_J = \dim_\mathbb{C} V$. If $\mathcal{X} \subseteq V$ is a $\mathbb{C}$-variety, then J is a real structure on $\mathcal{X}$ if $J(\mathcal{X}) \subseteq \mathcal{X}$. In this case there is a corresponding conjugate-linear homomorphism $J^* : \mathbb{C}[\mathcal{X}] \to \mathbb{C}[\mathcal{X}]$ of coordinate rings. Moreover, we get a real structure J_x on the tangent space $\Theta_{\mathcal{X},x}$ of $\mathcal{X}$ at x for any $x \in \mathcal{X}$. Let $\mathcal{X}_J$ be the J-fixed subset of $\mathcal{X}$; this is a $\mathbb{R}$-variety. It is not hard to see that $\Theta_{\mathcal{X}_J,x} = (\Theta_{\mathcal{X},x})_{J_x}$ for $x \in \mathcal{X}_J$.

The following proposition is well-known (see e.g. [Bec82, Lemma 1.5] or [DE70, Theorem 4.9] for stronger versions), but we provide a short proof for the sake of completeness.

Proposition 4.3. *Let $\mathcal{X}$ be an irreducible $\mathbb{C}$-variety with a real structure J and assume there exists $x \in \mathcal{X}_J$ which is a nonsingular point of $\mathcal{X}$. Then $\mathcal{X}_J$ is Zariski dense in $\mathcal{X}$.*

Proof. Let $\dim_\mathbb{C} \mathcal{X} = N$. Since x is nonsingular, we have

$$N = \dim_\mathbb{C} \Theta_{\mathcal{X},x} = \dim_\mathbb{R} (\Theta_{\mathcal{X},x})_{J_x} = \dim_\mathbb{R} \Theta_{\mathcal{X}_J,x}.$$

If $\mathcal{X}_J \subseteq \mathcal{X}'$ for some complex subvariety $\mathcal{X}' \subseteq \mathcal{X}$, then $\Theta_{\mathcal{X}_J,x} + i\Theta_{\mathcal{X}_J,x} \subseteq \Theta_{\mathcal{X}',x}$, so $\dim_{\mathbb{C}} \Theta_{\mathcal{X}',x} = N$ and therefore $\mathcal{X}' = \mathcal{X}$ by irreducibility. Hence $\mathcal{X}_J$ is Zariski dense in $\mathcal{X}$. ■

For later use we introduce

$$\mathcal{X}(g,n) = \left\{ (\underline{A}, \underline{B}) \in M_n(\mathbb{C})^g \times M_n(\mathbb{C})^g \colon \sum_{k=1}^{g} A_k B_k = I_n \right\} \tag{4.4}$$

for arbitrary $g, n \in \mathbb{N}$. This is a $\mathbb{C}$-variety with real structure $J(\underline{A}, \underline{B}) = (\underline{B}^*, \underline{A}^*)$ and

$$\mathcal{X}(g,n)_J = \left\{ (\underline{A}, \underline{A}^*) \in M_n(\mathbb{C})^g \times M_n(\mathbb{C})^g \colon \sum_{k=1}^{g} A_k A_k^* = I_n \right\}.$$

Proposition 4.4. *The variety $\mathcal{X}(g,n)$ is nonsingular and irreducible. Therefore $\mathcal{X}(g,n)_J$ is Zariski dense in $\mathcal{X}(g,n)$.*

Proof. Let

$$p = \sum_{k=1}^{g} X_k Y_k - I_n,$$

where X_k and Y_k are generic $n \times n$ matrices. The entries of p are the defining equations for $\mathcal{X}(g,n)$ and

$$\frac{\partial p_{\imath\jmath}}{\partial x_{ij}^{(k)}} = \begin{cases} y_{j\jmath}^{(k)} & \text{if } \imath = i \\ 0 & \text{otherwise,} \end{cases} \qquad \frac{\partial p_{\imath\jmath}}{\partial y_{ij}^{(k)}} = \begin{cases} x_{\imath i}^{(k)} & \text{if } \jmath = j \\ 0 & \text{otherwise.} \end{cases} \tag{4.5}$$

Let Jac be the Jacobian matrix corresponding to p, i.e. the $n^2 \times 2gn^2$ matrix

$$\operatorname{Jac} = \begin{pmatrix} \frac{\partial p_{\imath\jmath}}{\partial x_{ij}^{(k)}} & \frac{\partial p_{\imath\jmath}}{\partial y_{ij}^{(k)}} \end{pmatrix}_{\imath,\jmath;i,j,k}.$$

By (4.5), one can observe that every column of Jac is of the form $\mathbf{u} \otimes e_\ell$ or $e_\ell \otimes \mathbf{v}^t$, where $\mathbf{u}$ is a column of X_k, $\mathbf{v}$ is a row of Y_k, and $e_\ell \in \mathbb{C}^{n\times 1}$ is the ℓ-th standard unit vector. Therefore

$$\operatorname{rank} \operatorname{Jac}(\underline{A}, \underline{B}) = n \dim_{\mathbb{C}} \left(\operatorname{span}\{\text{columns of } \underline{A},\ \text{columns of } \underline{B}^t\} \right)$$

for every $(\underline{A}, \underline{B}) \in M_n(\mathbb{C})^g \times M_n(\mathbb{C})^g$. If $(\underline{A}, \underline{B}) \in \mathcal{X}(g,n)$, then the columns of $\underline{A}$ are linearly independent, so $\operatorname{Jac}(\underline{A}, \underline{B})$ has full rank. Therefore $\mathcal{X}(g,n)$ is nonsingular.

For any variety, the intersections of its irreducible components are subsets of the singular locus; thus $\mathcal{X}(g,n)$ is irreducible if it is connected in Euclidean topology. Since $\mathrm{GL}_n(\mathbb{C})$ is connected, the same holds for $\mathcal{X}(1,n) = \{(A, A^{-1}) \colon A \in \mathrm{GL}_n(\mathbb{C})\}$. For arbitrary g, there is a surjective projection $\mathcal{X}(1, gn) \to \mathcal{X}(g,n)$, so $\mathcal{X}(g,n)$ is connected.

The last part of the statement is a consequence of Proposition 4.3. ■

4.4. **$*$-Nullstellensätze.** In this subsection we give Nullstellensätze for nc trigonometric polynomials, nc spherical polynomials, and nc unitary groups. These are obtained by combining the results of Section 2 and Subsection 4.3. Alternative proofs of these $*$-Nullstellensätze (without size bounds) with a functional-analytic flavor are presented in Appendix A below.

Let $\mathcal{X}(g,n)$ be as in Subsection 4.3.

Definition 4.5. A $*$-ideal $\mathcal{I} \subseteq \mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle$ satisfies the **$*$-Nullstellensatz property** if for each $f \in \mathbb{C}\langle \underline{X} \rangle$,

$$f \in \mathcal{I} \quad \Leftrightarrow \quad f|_{Z_*(\mathcal{I})} = 0.$$

Theorem 4.6. *Suppose $p \in \mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle$ is of degree u and has v terms. If p vanishes on all g-tuples of unitaries of size uv, then*

$$p \in \mathcal{T} = (1 - X_1^\intercal X_1,\, 1 - X_1 X_1^\intercal,\, \dots,\, 1 - X_g^\intercal X_g,\, 1 - X_g X_g^\intercal).$$

Proof. Let $n = uv$. By assumption, p vanishes on $\mathcal{X}(1,n)_J \times \cdots \times \mathcal{X}(1,n)_J$ (g factors), so it vanishes on $\mathcal{X}(1,n) \times \cdots \times \mathcal{X}(1,n)$ by Proposition 4.4. The latter variety is a subset of the zero set of $\mathcal{T}$ as an ideal without involution. By Corollary 2.8, this ideal satisfies the Nullstellensatz property. Therefore p vanishes on $Z(\mathcal{T})$ by Example 3.11(1), so $p \in \mathcal{T}$. ■

Corollary 4.7. *A nc trigonometric polynomial that vanishes under all finite-dimensional $*$-representations, equals* 0.

Theorem 4.8. *Suppose $p \in \mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle$ is of degree u and has v terms. Let $g > 1$. If p vanishes on all g-tuples of spherical isometries of size $\lceil \frac{g+1}{2} uv \rceil$, then*

$$p \in \mathcal{S} = (1 - X_1^\intercal X_1 - \cdots - X_g^\intercal X_g).$$

Proof. Let $n = \lceil \frac{g+1}{2} uv \rceil$. Since p vanishes on $\mathcal{X}(g,n)_J$, it vanishes on $\mathcal{X}(g,n)$ by Proposition 4.4. The ideal $\mathcal{S}$ satisfies the Nullstellensatz property by Corollary 2.9. Hence $p \in \mathcal{S}$ because p vanishes on the zero set of $\mathcal{S}$ by Example 3.11(2). ■

Corollary 4.9. *Let $g > 1$. A nc spherical polynomial that vanishes under all finite-dimensional $*$-representations, equals* 0.

Theorem 4.10. *Suppose $p \in \mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle$ is of degree u and has v terms. Let $g > 1$. If p vanishes on all g-partitioned unitaries with blocks of size $\lceil \frac{g}{2} uv \rceil$, then*

$$p \in \mathcal{U} = (I_g - XX^\intercal, I_g - X^\intercal X).$$

Proof. The variety of g-partitioned unitaries with blocks of size n can be naturally identified with $\mathcal{X}(1,gn)_J$. On the other hand, $\mathcal{X}(1,gn)$ can be in the same way identified with the zero set of $\mathcal{U}$. The latter is a special case of an ideal from Corollary 2.8. Therefore $p \in \mathcal{U}$ by the Nullstellensatz property and Example 3.11(4). ■

Remark 4.11. In a similar fashion, one can derive the $*$-Nullstellensätze for any $*$-ideal as in Corollary 2.8 by considering the appropriate products of varieties $\mathcal{X}(g,n)$ for various values of g and n. Furthermore, as in Theorems 4.6 and 4.8, bounds for membership testing can be established using Theorem 3.9.

Remark 4.12. Similar $*$-Nullstellensätze also hold in the real setting, i.e., when we consider evaluations of polynomials $p \in \mathbb{R}\langle \underline{X}, \underline{X}^\intercal \rangle$ at points $\underline{A} \in M_n(\mathbb{R})^g$ by replacing X_i by A_i and $X_i^\intercal$ by A_i^t, where t denotes the transposition. Using the natural $*$-embedding

$$M_n(\mathbb{C}) \hookrightarrow M_{2n}(\mathbb{R}), \quad A + iB \mapsto \begin{pmatrix} A & -B \\ B & A \end{pmatrix}$$

we see that if $p \in \mathbb{R}\langle \underline{X}, \underline{X}^\intercal \rangle$ vanishes on

$$\left\{ (\underline{A}, \underline{A}^t) \in M_{2n}(\mathbb{R})^g \times M_{2n}(\mathbb{R})^g \colon \sum_{k=1}^g A_k A_k^t = I_n \right\} \hookleftarrow \mathcal{X}(g,n)_J,$$

then it vanishes on

$$\left\{ (\underline{A}, \underline{B}) \in M_n(\mathbb{R})^g \times M_n(\mathbb{R})^g \colon \sum_{k=1}^g A_k B_k = I_n \right\} \subseteq \mathcal{X}(g,n).$$

At this point we can apply results from Sections 2 and 3 for $\Bbbk = \mathbb{R}$. Thus we obtain the $*$-Nullstellensätze for real versions of Theorems 4.6, 4.8 and 4.10, but with size bounds multiplied by 2.

4.5. **Positivstellensätze.** Let $\mathcal{Z}$ be a set of g-tuples of matrices. Then a polynomial $f \in \mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle$ is said to be **positive on** $\mathcal{Z}$ if $f(\underline{A})$ is positive semi-definite for every $\underline{A} \in \mathcal{Z}$. Obvious representatives of such polynomials are those of the form

$$\sum_i p_i^\intercal p_i + q, \tag{4.6}$$

where q vanishes on $\mathcal{Z}$. We are interested in sets $\mathcal{Z}$ for which the converse of this observation holds; that is, is every f positive semi-definite on $\mathcal{Z}$, of the form (4.6)? Such statements are traditionally called Positivstellensätze [BCR98, Mar08, Sch09, HM04, HMP05]. The basic case, where $\mathcal{Z}$ is the set of all g-tuples of matrices of all sizes, was established by Helton [Hel02]; see also [McC01]. Later on, a Positivstellensatz was also established for spherical isometries and tuples of unitaries in [HMP04]. In the case of unitaries we also refer to [NT13] for a different approach. Using Theorems 4.6 and 4.8, we can now generalize these results in two directions. First of all, we clearly identify the elements of the vanishing ideals, and we prove a Positivstellensatz for nc unitary groups.

For $d \in \mathbb{N}$, let $\mathcal{P}_d \subseteq \mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle$ be the subspace of polynomials of degree at most d and

$$\mathcal{C}_{2d} = \operatorname{co}\{p^\intercal p \colon p \in \mathcal{P}_d\}$$

the associated convex cone of sums of Hermitian squares.

Corollary 4.13. *If $f \in \mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle$ of degree $d-1$ is positive on all g-tuples of unitaries of size $(2g+1)^d$, then*

$$f \in \mathcal{C}_{2d} + (1 - X_1^\intercal X_1,\, 1 - X_1 X_1^\intercal,\, \dots,\, 1 - X_g^\intercal X_g,\, 1 - X_g X_g^\intercal).$$

Corollary 4.14. *If $f \in \mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle$ of degree $d-1$ is positive on all spherical isometries of size $(2g+1)^d$, then*

$$f \in \mathcal{C}_{2d} + (1 - X_1^\intercal X_1 - \cdots - X_g^\intercal X_g).$$

Proof of Corollaries 4.13 and 4.14. Let $\mathcal{Z}$ be the set of all tuples of unitaries (resp. spherical isometries). If a polynomial f is positive on $\mathcal{Z}$, then f is of the form (4.6) by [HMP04, Theorem 4.1] and the statement follows by Theorem 4.6 (resp. Theorem 4.8). ■

Finally, we adapt the proof of [HMP04] to yield a Positivstellensatz for nc unitary groups, characterizing all nc polynomials positive on partitioned unitaries.

Theorem 4.15. *Let $\mathcal{Z}$ be the set of g-partitioned unitaries with blocks of size $(2g^2+1)^d$. If a polynomial f of degree $d-1$ is positive on $\mathcal{Z}$, then*

$$f \in \mathcal{C}_{2d} + (I_g - \underline{X}^\intercal \underline{X},\, I_g - \underline{X}\,\underline{X}^\intercal).$$

Proof. Let $I(\mathcal{Z}) \subseteq \mathbb{C}\langle \underline{X}, \underline{X}^\intercal \rangle$ be the ideal of all polynomials vanishing on $\mathcal{Z}$, and set

$$\mathcal{P}_d(\mathcal{Z}) = \frac{\mathcal{P}_d + I(\mathcal{Z})}{I(\mathcal{Z})}, \quad \mathcal{C}_{2d}(\mathcal{Z}) = \frac{\mathcal{C}_{2d} + I(\mathcal{Z})}{I(\mathcal{Z})}.$$

We write $[p]$ to indicate the class of p in these quotients. For the following proof to work, it is crucial that $\mathcal{C}_{2d}(\mathcal{Z})$ is closed in $\mathcal{P}_{2d}(\mathcal{Z})$ [HMP04, Lemma 3.2].

By this notation, we have $f \in \mathcal{P}_{d-1}$ and it is enough to show $[f] \in \mathcal{C}_{2d}(\mathcal{Z})$ by Theorem 4.10.

Let $f \in \mathcal{P}_{d-1}$ and suppose f is positive on $\mathcal{Z}$ but $[f] \notin \mathcal{C}_{2d}(\mathcal{Z})$. As was shown in [HMP04], there is a linear functional L on $\mathcal{P}_{2d}(\mathcal{Z})$ such that $L(f) < 0$ and $L(c) > 0$ for $c \in \mathcal{C}_{2d}(\mathcal{Z}) \setminus \{0\}$. Let Λ be the functional on $\mathcal{P}_{2d}$ obtained by pulling back L. Then

$$\langle a, b\rangle = \frac{1}{2}\Lambda(a^\intercal b + b^\intercal a)$$

is a Hermitian positive semi-definite form on $\mathcal{P}_d$ and its associated Hilbert space is $\mathcal{H} = \mathcal{P}_d(\mathcal{Z})$. Note that $\dim \mathcal{H} \leq \dim \mathcal{P}_d \leq (2g^2+1)^d$, so f is positive on g-partitioned unitaries whose blocks are operators on $\mathcal{H}$. Let $\mathcal{M} = \mathcal{P}_{d-1}(\mathcal{Z})$ be its subspace and $\mathcal{N}$ the orthogonal complement of $\mathcal{M}$ in $\mathcal{H}$.

For $1 \leq i, j \leq g$, define $X_{ij}, Y_{ij} : \mathcal{M} \to \mathcal{H}$ by $X_{ij}[p] = [x_{ij}p]$ and $Y_{ij}[p] = [x_{ij}^\intercal p]$. Then

$$\langle X_{ij} a, b\rangle = \langle a, Y_{ij} b\rangle$$

for $a, b \in \mathcal{M}$. Thus the restriction of X_{ij}^* to $\mathcal{M}$ is Y_{ij}; i.e., X_{ij}^* on $\mathcal{M}$ is multiplication by $x_{ij}^\intercal$.

Let

$$U_j : \mathcal{M} \to \bigoplus_{i=1}^{g} \mathcal{H}, \qquad U_j = \bigoplus_{i=1}^{g} X_{ij}.$$

Considering the inner product on $\bigoplus \mathcal{H}$, we have

$$\langle U_i a, U_j b\rangle = \delta_{ij}\langle a, b\rangle$$

for all $a, b \in \mathcal{M}$, where δ_{ij} is the Kronecker's delta. Therefore $\{U_j\}_j$ are pairwise orthogonal isometries. Since

$$\dim\left(\sum_{j=1}^{g} \operatorname{im} U_j\right) = g \dim \mathcal{M} = g(\dim \mathcal{H} - \dim \mathcal{N}),$$

there exist pairwise orthogonal subspaces $\mathcal{N}_1, \dots, \mathcal{N}_g \subseteq \bigoplus \mathcal{H}$ of the same dimension $\dim \mathcal{N}_j = \dim \mathcal{N}$ such that

$$\sum_{j=1}^{g} \mathcal{N}_j = \left(\sum_{j=1}^{g} \operatorname{im} U_j \right)^{\perp}.$$

We can choose isometric isomorphisms $\mathcal{N} \cong \mathcal{N}_j$ and extend U_j to $V_j : \mathcal{H} \to \bigoplus \mathcal{H}$ by

$$V_j|_{\mathcal{N}} : \mathcal{N} \to \mathcal{N}_j \hookrightarrow \bigoplus_{i=1}^{g} \mathcal{H}.$$

These maps are also pairwise orthogonal isometries. If $A_{ij} = (V_j)_i$, then the g^2-tuple $\underline{A}$ satisfies $\underline{A}^* \underline{A} = I_g$ and is therefore a g-partitioned unitary whose blocks are operators on $\mathcal{H}$.

As in [HMP04], one can verify that the restrictions of A_{ij} to $\mathcal{M}$ are X_{ij} and that the compressions of A_{ij}^* to $\mathcal{M}$ are Y_{ij}. The rest also follows as in [HMP04]: since f is of degree $d-1$, $f(\underline{A})[1] = f(\underline{X})[1] = [f]$. By the assumption $f(\underline{B})$ is positive semi-definite for $\underline{B} \in \mathcal{Z}$, so $[f] = [f^{\intercal}]$. But then

$$\langle f(\underline{A})[1], [1] \rangle = \langle [f], [1] \rangle = \frac{1}{2}(\Lambda(f) + \Lambda(f^{\intercal})) = \Lambda(f) < 0,$$

a contradiction. ■

Remark 4.16. As in Remark 4.12 we also obtain Positivstellensätze in the real setting that are analogous to Corollaries 4.13, 4.14 and Theorem 4.15.

A. Alternative proof of $*$-Nullstellensätze

In this appendix we give alternative independent proofs of the $*$-Nullstellensätze of Subsection 4.4. These proofs are inspired by functional analytic ideas and do not yield size bounds.

We say that $\mathbb{C}$-algebra with involution $\mathcal{A}$ is **residually finite-dimensional (rfd)** if it has a separating family of finite-dimensional $*$-representations, that is, for every $a \in \mathcal{A} \setminus \{0\}$ there exists $n \in \mathbb{N}$ and a $*$-homomorphism $\varphi : \mathcal{A} \to M_n(\mathbb{C})$ with $\varphi(a) \neq 0$. Here the involution on $M_n(\mathbb{C})$ is given by conjugate transpose. Thus a $*$-ideal $\mathcal{I} \subseteq \mathbb{C}<\underline{X}, \underline{X}^{\intercal}>$ satisfies the $*$-Nullstellensatz property if and only if $\mathbb{C}<\underline{X}, \underline{X}^{\intercal}>/\mathcal{I}$ is rfd.

Lemma A.1. *Let $\mathcal{A}$ be a rfd $\mathbb{C}$-algebra. If a set $\{a_1, \dots, a_n\} \subseteq \mathcal{A}$ is linearly independent, then there exists a finite-dimensional $*$-representation π of $\mathcal{A}$ such that $\{\pi(a_1), \dots, \pi(a_n)\}$ is linearly independent.*

Proof. Assuming this statement is not true, choose n minimal such that the claim is false; then clearly $n > 1$. Therefore for every finite-dimensional $*$-representation π of $\mathcal{A}$ there exist $\lambda_i^{\pi} \in \mathbb{C}$, not all zero, such that

$$\sum_i \lambda_i^{\pi} \pi(a_i) = 0.$$

By the minimality, there exists a finite-dimensional $*$-representation ρ of $\mathcal{A}$ such that $\{\pi(a_2), \dots, \pi(a_n)\}$ is linearly independent and

$$\rho(a_1) + \sum_{i>1} \mu_i \rho(a_i) = 0$$

for some $\mu_i \in \mathbb{C}$. Considering the $*$-representation $\pi \oplus \rho$, we have

$$\sum_i \lambda_i^{\pi\oplus\rho} \pi(a_i) = 0, \quad \sum_i \lambda_i^{\pi\oplus\rho} \rho(a_i) = 0$$

and $\lambda_1^{\pi\oplus\rho} \neq 0$ for every π. Since

$$\sum_{i>1} (\lambda_1^{\pi\oplus\rho} \mu_i - \lambda_i^{\pi\oplus\rho}) \rho(a_i) = 0,$$

we conclude $\lambda_i^{\pi\oplus\rho} = \lambda_1^{\pi\oplus\rho} \mu_i$. Therefore

$$\sum_i \mu_i \pi(a_i) = 0$$

holds for all $*$-representations π. Hence $\sum_i \mu_i a_i = 0$ by assumption, so $\{a_1, \dots, a_n\}$ is linearly dependent in $\mathcal{A}$, a contradiction. ■

Proposition A.2. *If $\mathcal{A}_1$ and $\mathcal{A}_2$ are rfd $\mathbb{C}$-algebras, then $\mathcal{A}_1 *_{\mathbb{C}} \mathcal{A}_2$ is rfd $\mathbb{C}$-algebra.*

Proof. Let S_i be an arbitrary finite linearly independent subset of $\mathcal{A}_i$. For $n \in \mathbb{N}$ let $S(n, S_1, S_2)$ be a subset of $\mathcal{A}_1 *_{\mathbb{C}} \mathcal{A}_2$, whose elements are words over $S_1 \cup S_2$ of length at most n that do not contain two consecutive elements from S_1 or S_2. By Lemma A.1, there exists a finite-dimensional $*$-representation $\pi_i : \mathcal{A}_i \to M_{d_i}(\mathbb{C})$ such that $\pi_i(S_i)$ is linearly independent set. By the universal property of the free product in the category of $\mathbb{C}$-algebras with involution, there exists a $*$-homomorphism

$$\pi = \pi_1 *_{\mathbb{C}} \pi_2 : \mathcal{A}_1 *_{\mathbb{C}} \mathcal{A}_2 \to M_{d_1}(\mathbb{C}) *_{\mathbb{C}} M_{d_2}(\mathbb{C});$$

the set $\pi(S(n, S_1, S_2))$ is linearly independent by construction. Since every element of $\mathcal{A}_1 *_{\mathbb{C}} \mathcal{A}_2$ lies in the linear span of some set $S(n, A_1, A_2)$, it suffices to prove that $M_{d_1}(\mathbb{C}) *_{\mathbb{C}} M_{d_2}(\mathbb{C})$ is rfd.

By [Avi82, Proposition 2.3], $M_{d_1}(\mathbb{C}) *_{\mathbb{C}} M_{d_2}(\mathbb{C})$ $*$-embeds into a C*-algebra of linear operators on a Hilbert space, therefore it also $*$-embeds into a free product of $M_{d_1}(\mathbb{C})$ and $M_{d_2}(\mathbb{C})$ in the category of C*-algebras; the latter is rfd by [EL92, Theorem 3.2], so the assertion holds. ■

Corollary A.3. *Every finite free product of nc unitary groups is a rfd algebra.*

Proof. The algebra $\Bbbk\langle \underline{X}, \underline{X}^{\intercal} \rangle / \mathcal{U}$ is rfd by [GW89, Theorem 1.2]. The statement then holds by Proposition A.2. ■

The Nullstellensätze of Remark 4.11 (including Theorem 4.6 and Theorem 4.10) can now be viewed as various versions of Corollary A.3. However, we do not obtain any bounds by this method. We can also give another proof of Theorem 4.8.

Proof of Theorem 4.8. The algebra $\Bbbk\langle \underline{X}, \underline{X}^\intercal\rangle/\mathcal{S}$ embeds into $\Bbbk\langle \underline{X}, \underline{X}^\intercal\rangle/\mathcal{U}$ under a $*$-homomorphism analogous to the embedding in the proof of Corollary 2.9. Hence it is rfd by Corollary A.3, so $\mathcal{S}$ satisfies the $*$-Nullstellensatz property. ■

References

[AM15] J. Agler, J.E. McCarthy: Pick Interpolation for free holomorphic functions, *Amer. J. Math.* **137** (2015) 1685–1701. 13

[Ami57] S.A. Amitsur: A generalization of Hilbert's Nullstellensatz, *Proc. Amer. Math. Soc.* **8** (1957) 649–656. 1

[Ami66] S.A. Amitsur: Rational identities and applications to algebra and geometry, *J. Algebra* **3** (1966) 304–359. 6, 20

[Avi82] D. Avitzour: Free products of C*-algebras, *Trans. Amer. Math. Soc.* **271** (1982) 423–435. 27

[BGM05] J.A. Ball, G. Groenewald, T. Malakorn: Structured noncommutative multidimensional linear systems, *SIAM J. Control Optim.* **44** (2005) 1474–1528. 2, 11, 15

[Bec82] E. Becker: Valuations and real places in the theory of formally real fields, In: *Real algebraic geometry and quadratic forms (Rennes, 1981)*, 1–40, Lecture Notes in Math. **959**, Springer, 1982. 21

[BCR98] J. Bochnak, M. Coste, M.F. Roy: *Real algebraic geometry*, Results in Mathematics and Related Areas (3) **36**, Springer-Verlag, Berlin, 1998. 24

[Ber74] G.M. Bergman: Coproducts and some universal ring constructions, *Trans. Amer. Math. Soc.* **200** (1974) 33–88. 9, 10

[BK11] M. Brešar, I. Klep: Tracial Nullstellensätze, in *Notions of Positivity and the Geometry of Polynomials*, 79–101, Springer Basel, 2011. 4

[BR11] J. Berstel, C. Reutenauer: *Noncommutative rational series with applications*, Encyclopedia of Mathematics and its Applications, 137, Cambridge University Press, Cambridge, 2011. 2, 11

[Bro81] L. G. Brown: Ext of certain free product C*-algebras, *J. Operator Theory* **6** (1981) 135–141. 3, 21

[CHMN13] J. Cimprič, J.W. Helton, S. McCullough, C. Nelson: A noncommutative real Nullstellensatz corresponds to a noncommutative real ideal: algorithms, *Proc. Lond. Math. Soc. (3)* **106** (2013) 1060–1086. 1

[Coh66] P.M. Cohn: Some remarks on the invariant basis property, *Topology* **5** (1966) 215–228. 8, 10

[Coh95] P.M. Cohn: *Skew fields. Theory of general division rings*, Encyclopedia of Mathematics and its Applications **57**, Cambridge University Press, 1995. 5, 7, 8, 9, 12, 20

[Coh06] P.M. Cohn: *Free ideal rings and localization in general rings*, New Mathematical Monographs **3**. Cambridge University Press, 2006. 5, 8

[CR94] P. M. Cohn, C. Reutenauer: A normal form in free fields, *Canad. J. Math.* **46** (1994) 517–531. 11

[DS78] W. Dicks, E. D. Sontag: Sylvester domains, *J. Pure Appl. Algebra* **13** (1978) 243–275. 8, 10

[DE70] D.W. Dubois, G. Efroymson: Algebraic theory of real varieties I, In: *1970 Studies and Essays (Presented to Yu-why Chen on his 60th Birthday)*, 107–135, Math. Res. Center, Nat. Taiwan Univ., Taipei. 21

[EL92] R. Exel, T. A. Loring: Finite-dimensional representations of free product C*-algebras, *Internat. J. Math.* **3** (1992) 469–476. 27

[GW89] P. Glockner, W. von Waldenfels: The relations of the non-commutative coefficient algebra of the unitary group, In: *Quantum probability and applications, IV*, 182–220, Springer, 1989. 27

[Hel02] J.W. Helton: "Positive" noncommutative polynomials are sums of squares, *Ann. of Math.* (2) **156** (2002) 675–694. 24

[HKM11] J.W. Helton, I. Klep, S. McCullough: Proper analytic free maps, *J. Funct. Anal.* **260** (2011) 1476–1490. 13

[HM04] J.W. Helton, S. McCullough: A Positivstellensatz for non-commutative polynomials, *Trans. Amer. Math. Soc.* **356** (2004) 3721–3737. 1, 24

[HMP04] J.W. Helton, S. McCullough, M. Putinar: A non-commutative Positivstellensatz on isometries, *J. reine angew. Math.* **568** (2004) 71–80. 2, 3, 19, 24, 25, 26

[HMP05] J.W. Helton, S. McCullough, M. Putinar: Non-negative hereditary polynomials in a free -algebra, *Math. Z.* **250** (2005) 515–522. 24

[HMP07] J.W. Helton, S. McCullough, M. Putinar: Strong majorization in a free -algebra, *Math. Z.* **255** (2007) 579–596. 1, 19

[HMV06] J.W. Helton, S. McCullough, V. Vinnikov: Noncommutative convexity arises from linear matrix inequalities, *J. Funct. Anal.* **240** (2006) 105–191. 2, 11

[HJ85] R. A. Horn, C. R. Johnson: *Matrix analysis*, Cambridge University Press, 1985. 10, 17

[KVV09] D.S. Kalyuzhnyi-Verbovetskiĭ, V. Vinnikov: Singularities of rational functions and minimal factorizations: the noncommutative and the commutative setting, *Linear Algebra Appl.* **430** (2009) 869-889. 2, 11

[KVV14] D.S. Kalyuzhnyi-Verbovetskiĭ, V. Vinnikov: *Foundations of free noncommutative function theory*, Mathematical Surveys and Monographs **199**, American Mathematical Society, 2014. 13

[Lam91] T. Y. Lam: *A first course in noncommutative rings*, Graduate Texts in Mathematics **131**, Springer, 1991. 13

[LL78] J. Lewin, T. Lewin: An embedding of the group algebra of a torsion-free one-relator group in a field, *J. Algebra* **52** (1978) 39–74. 9

[Mar08] M. Marshall: *Positive polynomials and sums of squares*, Mathematical Surveys and Monographs **146**, American Mathematical Society, 2008. 24

[McC01] S. McCullough: Factorization of operator-valued polynomials in several non-commuting variables, *Linear Algebra Appl.* **326** (2001) 193–203. 24

[NT13] T. Netzer, A. Thom: Real closed separation theorems and applications to group algebras, *Pacific J. Math.* **263** (2013) 435–452. 24

[Pas14] J. E. Pascoe: The inverse function theorem and the Jacobian conjecture for free analysis, *Math. Z.* **278** (2014) 987–994. 13

[Row80] L.H. Rowen: *Polynomial identities in ring theory*, Pure and Applied Mathematics **84**, Academic Press, Inc., 1980. 12

[Sch09] C. Scheiderer: Positivity and sums of squares: a guide to recent results, In: *Emerging applications of algebraic geometry*, 271–324, IMA Vol. Math. Appl. **149**, Springer, 2009. 24

[Vol+] J. Volčič: Matrix coefficient realization theory of noncommutative rational functions, preprint `arXiv:1505.07472`. 12

[Voi04] D.-V. Voiculescu: Free analysis questions I: Duality transform for the coalgebra of $\partial_{X:B}$, *Int. Math. Res. Not.* **16** (2004) 793–822. 13

[Voi10] D.-V. Voiculescu: Free analysis questions II: The Grassmannian completion and the series expansions at the origin, *J. reine angew. Math.* **645** (2010) 155–236. 13

[Wo87] S.L. Woronowicz: Compact matrix pseudogroups, *Comm. Math. Phys.* **111** (1987) 613–665. 3, 21

Igor Klep, The University of Auckland, Department of Mathematics

E-mail address: `igor.klep@auckland.ac.nz`

Victor Vinnikov, Ben-Gurion University of the Negev, Department of Mathematics

E-mail address: `vinnikov@math.bgu.ac.il`

Jurij Volčič, The University of Auckland, Department of Mathematics

E-mail address: `jurij.volcic@auckland.ac.nz`

NOT FOR PUBLICATION

Contents