POSITIVE TRACE POLYNOMIALS AND THE UNIVERSAL PROCESI-SCHACHER CONJECTURE

IGOR KLEP[1], ŠPELA ŠPENKO[2], AND JURIJ VOLČIČ[3]

ABSTRACT. Positivstellensätze are fundamental results in real algebraic geometry providing algebraic certificates for positivity of polynomials on semialgebraic sets. In this article Positivstellensätze for trace polynomials positive on semialgebraic sets of $n \times n$ matrices are provided. A Krivine-Stengle-type Positivstellensatz is proved characterizing trace polynomials nonnegative on a general semialgebraic set K using weighted sums of hermitian squares with denominators. The weights in these certificates are obtained from generators of K *and* traces of hermitian squares. For compact semialgebraic sets K Schmüdgen- and Putinar-type Positivstellensätze are obtained: every trace polynomial positive on K has a sum of hermitian squares decomposition with weights and without denominators. The methods employed are inspired by invariant theory, classical real algebraic geometry and functional analysis.

Procesi and Schacher in 1976 developed a theory of orderings and positivity on central simple algebras with involution and posed a Hilbert's 17th problem for a universal central simple algebra of degree n: is every totally positive element a sum of hermitian squares? They gave an affirmative answer for $n = 2$. In this paper a negative answer for $n = 3$ is presented. Consequently, including traces of hermitian squares as weights in the Positivstellensätze is indispensable.

1. INTRODUCTION

Positivstellensätze are pillars of modern real algebraic geometry [BCR98, PD01, Mar08, Sce09]. A Positivstellensatz is an algebraic certificate for a real polynomial to be positive on a set described by polynomial inequalities. For a finite set $S \subset \mathbb{R}[\boldsymbol{\xi}] = \mathbb{R}[\xi_1, \dots, \xi_g]$ let K_S denote the semialgebraic set of points $\alpha \in \mathbb{R}^g$ for which $s(\alpha) \geq 0$ for all $s \in S$. The most fundamental result here is the Krivine-Stengle Positivstellensatz (see e.g. [Mar08, Theorem 2.2.1]), which characterizes polynomials that are positive on K_S as weighted sums of squares with denominators, where weights are products of elements in S. This theorem is the real analog of Hilbert's Nullstellensatz and a far-reaching generalization of Artin's solution to Hilbert's 17th problem. If the set K_S is compact, a simpler description of strict positivity on K_S is given by Schmüdgen's Positivstellensatz [Scm91]. If moreover S generates an archimedean quadratic module, then Putinar's Positivstellensatz [Put93] presents an even simpler form of strictly positive polynomials on K_S. The latter leads to a variety of applications of real algebraic geometry via semidefinite programming [WSV12, BPT13] in several areas of applied mathematics and engineering. By

Date: April 30, 2018.

2010 *Mathematics Subject Classification.* Primary 16R30, 13J30; Secondary 16W10, 14P10.

Key words and phrases. Trace ring, generic matrices, positive trace polynomial, Positivstellensatz, Real Nullstellensatz, Procesi-Schacher conjecture.

[1]Supported by the Marsden Fund Council of the Royal Society of New Zealand. Partially supported by the Slovenian Research Agency grants J1-8132, N1-0057 and P1-0222.

[2]The second author is a FWO [PEGASUS]^2 Marie Skłodowska-Curie fellow at the Free University of Brussels (funded by the European Union Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 665501 with the Research Foundation Flanders (FWO)). During part of this work she was also a postdoc with Sue Sierra at the University of Edinburgh.

[3]Supported by the University of Auckland Doctoral Scholarship and the Deutsche Forschungsgemeinschaft (DFG) Grant No. SCHW 1723/1-1.

adapting the notion of a quadratic module and a preordering to $\mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$, many of the results described above extend to matrix polynomials [GR74, SH06, Cim12].

Positivstellensätze are also key in noncommutative real algebraic geometry [dOHMP09, Scm09, Oza13], where the theory essentially divides into two parts between which there is increasing synergy. The dimension-free branch started with Helton's theorem characterizing free noncommutative polynomials, which are positive semidefinite on all matrices of all sizes, as sums of hermitian squares [Hel02]. This principal result was followed by various Positivstellensätze in a free algebra [HM04, HKM12, KVV17], often with cleaner statements or stronger conclusions than their commutative counterparts. These dimension-free techniques are also applied to positivity in operator algebras [NT10, Oza16] and free probability [GS14]. Trace positivity of free polynomials presents the algebraic aspect of the renowned Connes' embedding conjecture [KS08, Oza13]. In addition to convex optimization [BPT13], free positivity certificates frequently appear in quantum information theory [NC10] and control theory [BEFB94]. On the other hand, the dimension-dependent branch is less developed. Here the main tools come from the theory of quadratic forms, polynomial identities and central simple algebras with involution [KMRT98, Row80, AU15]. A fundamental result in this context, a Hilbert's 17th problem, was solved by Procesi and Schacher [PS76]: totally positive elements in a central simple algebra with a positive involution are weighted sums of hermitian squares, and the weights arise as traces of hermitian squares. Analogous conclusions hold for trace positive polynomials [Kle11]. The basic problem here is whether the traces of hermitian squares are actually needed; cf. [KU10, AU+, SS12].

We next outline the contributions of this paper. Let $\mathbb{T}$ be the **free trace ring**, i.e., the $\mathbb{R}$-algebra with involution $*$ generated by noncommuting variables $x_1,\dots,x_g$ and symmetric commuting variables $\operatorname{Tr}(w)$ for words w in x_j,x_j^* satisfying $\operatorname{Tr}(w_1w_2)=\operatorname{Tr}(w_2w_1)$ and $\operatorname{Tr}(w^*)=\operatorname{Tr}(w)$. Let $\operatorname{Sym}\mathbb{T}$ be the subspace of symmetric elements, T the center of $\mathbb{T}$ and $\operatorname{Tr}:\mathbb{T}\to T$ the natural T-linear map. For a fixed $n\in\mathbb{N}$, the evaluation of $\mathbb{T}$ at $X\in\mathrm{M}_n(\mathbb{R})^g$ is defined by $x_j\mapsto X_j$, $x_j^*\mapsto X_j^{\mathrm{t}}$ and $\operatorname{Tr}(w)\mapsto\operatorname{tr}(w(X))$.

Example. Consider $f=5\operatorname{Tr}(x_1x_1^*)-2\operatorname{Tr}(x_1)(x_1+x_1^*)\in\mathbb{T}$. We claim that f is positive (semidefinite) on $\mathrm{M}_2(\mathbb{R})$. For $X\in\mathrm{M}_2(\mathbb{R})$ write

$$H_1=X-X^{\mathrm{t}},\qquad H_2=XX^{\mathrm{t}}-X^{\mathrm{t}}X,\qquad H_3=X^2-2XX^{\mathrm{t}}+2X^{\mathrm{t}}X-(X^{\mathrm{t}})^2.$$

If H_1 is invertible, then one can check (see Example 6.5 for details) that

$$f(X)=\frac{5}{2}H_1H_1^{\mathrm{t}}+\frac{1}{2}H_1^{-1}H_2H_2^{\mathrm{t}}H_1^{-\mathrm{t}}+\frac{1}{2}H_1^{-1}H_3H_3^{\mathrm{t}}H_1^{-\mathrm{t}}$$

and hence $f(X)\succeq 0$, so $f\succeq 0$ on $\mathrm{M}_2(\mathbb{R})$ by continuity. On the other hand, f is not positive on $\mathrm{M}_3(\mathbb{R})$:

$$f\left(\begin{pmatrix}2&0&0\\0&1&0\\0&0&1\end{pmatrix}\right)=5\operatorname{Tr}\left(\begin{pmatrix}4&0&0\\0&1&0\\0&0&1\end{pmatrix}\right)I_3-2\operatorname{Tr}\left(\begin{pmatrix}2&0&0\\0&1&0\\0&0&1\end{pmatrix}\right)\begin{pmatrix}4&0&0\\0&1&0\\0&0&1\end{pmatrix}=\begin{pmatrix}-2&0&0\\0&14&0\\0&0&14\end{pmatrix}\not\succeq 0.$$

In the rest of the paper we will develop a systematic theory for positivity of trace polynomials.

For $S\subset\operatorname{Sym}\mathbb{T}$ let

$$K_S=\{X\in\mathrm{M}_n(\mathbb{R})^g\colon s(X)\succeq 0\ \forall s\in S\}.$$

If S is finite, then K_S is the **semialgebraic set** described by S. A set $\mathfrak{Q}\subset\operatorname{Sym}\mathbb{T}$ is a **cyclic quadratic module** if

$$1\in\mathfrak{Q},\quad \mathfrak{Q}+\mathfrak{Q}\subseteq\mathfrak{Q},\quad h\mathfrak{Q}h^*\subseteq\mathfrak{Q}\ \ \forall h\in\mathbb{T},\quad \operatorname{Tr}(\mathfrak{Q})\subset\mathfrak{Q}.$$

A cyclic quadratic module $\mathfrak{T}$ is a **cyclic preordering** if $T\cap\mathfrak{T}$ is closed under multiplication.

Proposition. *If $\mathfrak{T} \subset \mathbb{T}$ is a cyclic preordering, then $f|_{K_{\mathfrak{T}}} \succeq 0$ for every $f \in \mathfrak{T}$.*

The converse of this simple proposition fails in general, but the next noncommutative version of the Krivine-Stengle Positivstellensatz uses cyclic preorderings to describe noncommutative polynomials positive semidefinite on a semialgebraic set K_S.

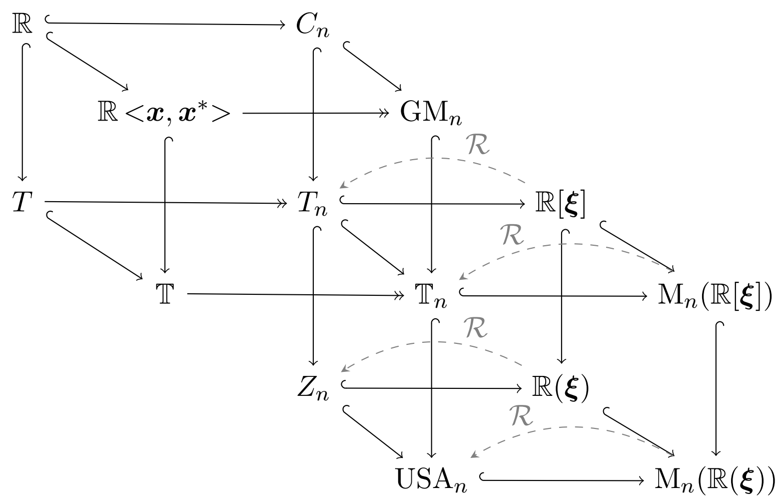
Theorem B'. *Let $S \cup \{f\} \subset \operatorname{Sym}\mathbb{T}$ be finite and let $\mathfrak{T}$ be the smallest cyclic preordering containing S. Then $f|_{K_S} \succeq 0$ if and only if*

$$(t_1 f)|_{\mathrm{M}_n(\mathbb{R})^g} = (f^{2k} + t_2)|_{\mathrm{M}_n(\mathbb{R})^g} \qquad \textit{and} \qquad (f t_1)|_{\mathrm{M}_n(\mathbb{R})^g} = (t_1 f)|_{\mathrm{M}_n(\mathbb{R})^g}$$

for some $k \in \mathbb{N}$ and $t_1, t_2 \in \mathfrak{T}$.

See Theorem B below for an extended version in a slightly different language. The existence of trace identities on $n \times n$ matrices suggests that the problem of positivity on $n \times n$ matrices should be treated in an appropriate quotient of $\mathbb{T}$, which we describe next.

Let $\mathbb{T}_n$ be the **trace ring of generic $n \times n$ matrices**, i.e., the $\mathbb{R}$-algebra generated by generic matrices $\Xi_1, \dots, \Xi_g$, their transposes and traces of their products. Here $\Xi_j = (\xi_{j\imath\jmath})_{\imath\jmath}$ is an $n \times n$ matrix whose entries are independent commuting variables. The $\mathbb{R}$-subalgebra $\mathrm{GM}_n \subset \mathbb{T}_n$ generated by $\Xi_j, \Xi_j^{\mathrm{t}}$ is called the **ring of generic $n \times n$ matrices** and has a central role in the theory of polynomial identities [Pro76, Row80]. The ring of central quotients of GM_n is the **universal central simple algebra with orthogonal involution** of degree n, denoted USA_n. The ring $\mathbb{T}_n$ also has a geometric interpretation. Let the orthogonal group $\mathrm{O}_n(\mathbb{R})$ act on $\mathrm{M}_n(\mathbb{R})^g$ by simultaneous conjugation. If $\mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$ is identified with polynomial maps $\mathrm{M}_n(\mathbb{R})^g \to \mathrm{M}_n(\mathbb{R})$, then $\mathbb{T}_n$ is the ring of polynomial $\mathrm{O}_n(\mathbb{R})$-concomitants in $\mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$, i.e., equivariant maps with respect to the $\mathrm{O}_n(\mathbb{R})$-action [Pro76]. If C_n, T_n, Z_n are the centers of $\mathrm{GM}_n, \mathbb{T}_n, \mathrm{USA}_n$, respectively, and $\mathcal{R}$ is the "averaging" Reynolds operator for the $\mathrm{O}_n(\mathbb{R})$-action, then we have the following diagram.



The elements of $\mathbb{T}_n$ are called **trace polynomials** and the elements of T_n are called **pure trace polynomials**. Since every evaluation of $\mathbb{T}$ at a tuple of $n \times n$ matrices factors through $\mathbb{T}_n$, it suffices to prove our Positivstellensätze in the ring $\mathbb{T}_n$. The purpose of this reduction is of course not to merely state Theorem B' in a more compact form. Our proofs crucially rely on algebraic properties of $\mathbb{T}_n$ and their interaction with invariant and PI theory [Pro76, Row80].

The contribution of this paper is twofold. We prove the Krivine-Stengle, Schmüdgen and Putinar Positivstellensätze for the trace ring of generic matrices in terms of cyclic quadratic modules and preorderings. We also prove Putinar's Positivstellensatz for the ring of generic matrices (without traces). The proofs intertwine techniques from invariant theory, real algebraic geometry, PI theory and functional analysis. Our second main result is a counterexample to the (universal) Procesi-Schacher conjecture.

1.1. **Main results and reader's guide.** After this introduction we recall known facts about polynomial identities, positive involutions, and the rings GM_n and $\mathbb{T}_n$ in Section 2, where we also prove some preliminary results that are used in the sequel.

Section 3 deals with the question of Procesi and Schacher [PS76], which is a noncommutative version of Hilbert's 17th problem for central simple $*$-algebras. We say that $a \in \mathrm{USA}_n$ is **totally positive** if $a(X) \succeq 0$ for every $X \in \mathrm{M}_n(\mathbb{R})^g$ where a is defined. Then the universal Procesi-Schacher conjecture states that totally positive elements in USA_n are sums of hermitian squares in USA_n. While this is true for $n = 2$ [PS76, KU10], we show that the conjecture fails for $n = 3$.

Theorem A. *There exist totally positive elements in* USA_3 *that are not sums of hermitian squares in* USA_3*.*

The proof (see Theorem 3.2) relies on the central simple $*$-algebra USA_3 being split, i.e., $*$-isomorphic to $\mathrm{M}_3(Z_3)$ with some orthogonal involution. After explicitly determining the involution using quadratic forms (Proposition 3.4 of Tignol) and a transcendental basis of Z_3 (Lemma 3.5), we use Prestel's theory of semiorderings [PD01] to produce an example of a totally positive element (a trace of a hermitian square) in USA_3 that is not a sum of hermitian squares (Proposition 3.6).

Section 4 first introduces cyclic quadratic modules and cyclic preorderings for the trace ring $\mathbb{T}_n$, which are defined analogously as for $\mathbb{T}$ above. The main result in this section is the following version of the Krivine-Stengle Positivstellensatz for $\mathbb{T}_n$.

Theorem B. *Let* $S \cup \{a\} \subset \operatorname{Sym} \mathbb{T}_n$ *be finite and* $\mathfrak{T}$ *the cyclic preordering generated by* S*.*

(1) $a|_{K_S} \succeq 0$ *if and only if* $at_1 = t_1 a = a^{2k} + t_2$ *for some* $t_1, t_2 \in \mathfrak{T}$ *and* $k \in \mathbb{N}$*.*
(2) $a|_{K_S} \succ 0$ *if and only if* $at_1 = t_1 a = 1 + t_2$ *for some* $t_1, t_2 \in \mathfrak{T}$*.*
(3) $a|_{K_S} = 0$ *if and only if* $-a^{2k} \in \mathfrak{T}$ *for some* $k \in \mathbb{N}$*.*

See Theorem 4.13 for the proof, which decomposes into three parts. First we show that the finite set of constraints $S \subset \operatorname{Sym} \mathbb{T}_n$ can be replaced by a finite set $S' \subset T_n$ (Corollary 4.4). To prove this central reduction we use the fact that the positive semidefiniteness of a matrix can be characterized by symmetric polynomials in its eigenvalues and apply compactness of the real spectrum in the constructible topology [BCR98, Section 7.1]. In the second step we apply results on central simple algebras with involution and techniques from PI theory to prove the following extension theorem.

Theorem C. *Let* $R \supseteq \mathbb{R}$ *be a real closed field. Then an* $\mathbb{R}$*-algebra homomorphism* $\phi : T_n \to R$ *extends to an* $\mathbb{R}$*-algebra homomorphism* $\mathbb{R}[\boldsymbol{\xi}] \to R$ *if and only if* $\phi(\operatorname{tr}(hh^{\mathrm{t}})) \geq 0$ *for all* $h \in \mathbb{T}_n$*.*

Since $T_n = \mathbb{R}[\boldsymbol{\xi}]^{\mathrm{O}_n(\mathbb{R})}$, this statement resembles variants of the Procesi-Schwarz theorem [PS85, Theorem 0.10] (cf. [CKS09, Brö98]). Nevertheless, it does not seem possible to deduce Theorem C from these classical results; see Appendix B for a fuller discussion. Theorem C, proved as Theorem 4.8 below, is essential for relating evaluations of pure trace polynomials with orderings on T_n via Tarski's transfer principle (Proposition 4.12). Finally, by combining the first two steps we obtain a reduction to the commutative situation, where we can apply an existing abstract version of the Krivine-Stengle Positivstellensatz [Mar08, Theorem 2.5.2].

Since trace polynomials are precisely $\mathrm{O}_n(\mathbb{R})$-concomitants in $\mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$, one might naively attempt to prove Theorem B by simply applying the Reynolds operator for the $\mathrm{O}_n(\mathbb{R})$-action to analogous Positivstellensätze for matrix polynomials [Scm09, Cim12]. However, the Reynolds operator is not multiplicative and it does not preserve squares of trace polynomials, so in this manner one obtains only weak and inadequate versions of Theorem B.

In Section 5 we refine the strict positivity certificate (2) of Theorem B in the case of compact semialgebraic sets. We start by introducing archimedean cyclic quadratic modules, which encompass an algebraic notion of boundedness. Following the standard definition we say that a cyclic quadratic module $\mathfrak{Q} \subseteq \mathbb{T}_n$ is **archimedean** if for every $h \in \mathbb{T}_n$ there exists $\rho \in \mathbb{Q}_{>0}$ such that $\rho - hh^{\mathrm{t}} \in \mathfrak{Q}$. Then we prove Schmüdgen's Positivstellensatz for trace polynomials.

Theorem D. *Let $S \cup \{a\} \subset \operatorname{Sym} \mathbb{T}_n$ be finite and $\mathfrak{T}$ be the cyclic preordering generated by S. If K_S is compact and $a|_{K_S} \succ 0$, then $a \in \mathfrak{T}$.*

In the proof (see Theorem 5.3) we apply techniques similar to those in the proof of Theorem B. That is, we replace S by finitely many central constraints and apply Theorem C to reduce to the commutative setting, where we use an abstract version of Schmüdgen's Positivstellensatz [Sce03].

Finally, we have the following version of Putinar's Positivstellensatz for $\mathbb{T}_n$ and GM_n, combining Theorems 5.5 and 5.7.

Theorem E.

(a) *Let $\mathfrak{Q} \subset \operatorname{Sym} \mathbb{T}_n$ be an archimedean cyclic quadratic module and $a \in \operatorname{Sym} \mathbb{T}_n$. If $a|_{K_{\mathfrak{Q}}} \succ 0$, then $a \in \mathfrak{Q}$.*

(b) *Let $\mathfrak{Q} \subset \operatorname{Sym} \mathrm{GM}_n$ be an archimedean quadratic module and $a \in \operatorname{Sym} \mathrm{GM}_n$. If $a|_{K_{\mathfrak{Q}}} \succ 0$, then $a \in \mathfrak{Q}$.*

Theorem E is proved in a more functional-analytic way. We start by assuming $a \notin \mathfrak{Q}$ and find an extreme separation of a and $\mathfrak{Q}$. Then we apply a Gelfand-Naimark-Segal construction towards finding a tuple of $n \times n$ matrices in $K_{\mathfrak{Q}}$ at which a is not positive definite. For GM_n this is done using polynomial identities techniques, while for $\mathbb{T}_n$ we use Theorem C. As a consequence we have the following statement for noncommutative polynomials.

Corollary E'. *Let $\mathfrak{Q} \subset \operatorname{Sym} \mathbb{R}\langle \boldsymbol{x}, \boldsymbol{x}^* \rangle$ be an archimedean quadratic module and $a \in \mathbb{R}\langle \boldsymbol{x}, \boldsymbol{x}^* \rangle$. If $a|_{K_{\mathfrak{Q}}} \succ 0$, then $a = q + f$ for some $q \in \mathfrak{Q}$ and $f \in \mathbb{R}\langle \boldsymbol{x}, \boldsymbol{x}^* \rangle$ satisfying $f|_{\mathrm{M}_n(\mathbb{R})^g} = 0$.*

Proof. If $\pi : \mathbb{R}\langle \boldsymbol{x}, \boldsymbol{x}^* \rangle \to \mathrm{GM}_n$ is the canonical $*$-homomorphism, then $\pi(\mathfrak{Q})$ is an archimedean module in GM_n and hence $\pi(a) \in \pi(\mathfrak{Q})$ by Theorem E(b). Corollary E' now follows because the kernel of π consists precisely of the polynomial identities for $n \times n$ matrices. □

The paper concludes with Section 6 containing examples and counterexamples. In Appendix A where we present algebraic constructions of the Reynolds operator for the action of $\mathrm{O}_n(\mathbb{R})$ on polynomials and matrix polynomials as alternatives to the integration over the orthogonal group, which is of interest in mathematical physics [CŚ06]. Appendix B explains why the Procesi-Schwarz theorem cannot be used to obtain the extension theorem C.

Acknowledgments. The authors thank Jean-Pierre Tignol for sharing his expertise and generously allowing us to include his ideas that led to the counterexample for the universal Procesi-Schacher conjecture, and James Pascoe for his thoughtful suggestions. We also acknowledge fruitful Oberwolfach discussions with Cordian Riener and Markus Schweighofer.

2. Preliminaries

In this section we collect some background material and preliminary results needed in the sequel.

2.1. **Polynomial and trace $*$-identities.** Throughout the paper let F be a field of characteristic 0. Let $\boldsymbol{x} = \{x_1, \dots, x_g\}$ and $\boldsymbol{x}^* = \{x_1^*, \dots, x_g^*\}$ be freely noncommuting variables, and let $<\boldsymbol{x}, \boldsymbol{x}^*>$ be the free monoid generated by x_j, x_j^*. The free algebra $F<\boldsymbol{x}, \boldsymbol{x}^*>$ is then endowed with the unique involution of the first kind determined by $x_j \mapsto x_j^*$. If $\mathcal{A}$ is an F-algebra with involution τ and $f = f(x_1, \dots, x_g, x_1^*, \dots, x_g^*) \in F<\boldsymbol{x}, \boldsymbol{x}^*>$ is such that

$$f(a_1, \dots, a_g, a_1^\tau, \dots, a_g^\tau) = 0$$

for all $a_j \in \mathcal{A}$, then f is a **polynomial $*$-identity** of $(\mathcal{A}, \tau)$.

Let $\sim$ be the equivalence relation on $<\boldsymbol{x}, \boldsymbol{x}^*>$ generated by

$$w_1 w_2 \sim w_2 w_1, \qquad w_1 \sim w_1^*$$

for $w_1, w_2 \in <\boldsymbol{x}, \boldsymbol{x}^*>$. Let $\operatorname{Tr}(w)$ be the equivalence class for $w \in <\boldsymbol{x}, \boldsymbol{x}^*>$. Then we define the **free trace ring with involution** $\mathbb{T} = T \otimes_F F<\boldsymbol{x}, \boldsymbol{x}^*>$, where T is the free commutative F-algebra generated by $\operatorname{Tr}(w)$ for $w \in <\boldsymbol{x}, \boldsymbol{x}^*>/\sim$. Note that $\operatorname{Tr}(1) \in \mathbb{T}$ is one of the generators of T and not a real scalar. If $\mathcal{A}$ is an F-algebra, then an F-linear map $\chi : \mathcal{A} \to F$ satisfying $\chi(ab) = \chi(ba)$ for $a, b \in \mathcal{A}$ is called an **F-trace** on $\mathcal{A}$. If

$$f = \sum_i \alpha_i \operatorname{Tr}(w_{i1}) \cdots \operatorname{Tr}(w_{i\ell_i}) w_{i0}, \qquad \alpha_i \in F,\ w_{ij} \in <\boldsymbol{x}, \boldsymbol{x}^*>$$

satisfies

$$\sum_i \alpha_i \chi(w_{i1}(a)) \cdots \chi(w_{i\ell_i}(a)) w_{i0}(a) = 0$$

for every tuple a of elements in $\mathcal{A}$, then f is a **trace $*$-identity** of $(\mathcal{A}, \tau, \chi)$.

2.1.1. *A particular trace $*$-identity.* For $n \in \mathbb{N}$ let t denote the transpose involution on $\mathrm{M}_n(F)$ and let s denote the symplectic involution on $\mathrm{M}_{2n}(F)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\mathsf{s}} = \begin{pmatrix} d^{\mathsf{t}} & -b^{\mathsf{t}} \\ -c^{\mathsf{t}} & a^{\mathsf{t}} \end{pmatrix}.$$

Let $\operatorname{tr} : \mathrm{M}_n(F) \to F$ be the usual trace. Finally, for $X \in \mathrm{M}_n(F)$ let $X^{\oplus d} \in \mathrm{M}_{dn}(F)$ denote the block-diagonal matrix with d diagonal blocks all equal to X.

Fix $m \in \mathbb{N}$. For a t-antisymmetric $A \in \mathrm{M}_{2m}(F)$ let $\operatorname{pf}(A) \in F$ be its Pfaffian, $\operatorname{pf}(A)^2 = \det(A)$. Suppose that $A_1, A_2 \in \mathrm{M}_{2m}(F)$ are t-antisymmetric and A_2 is invertible. Now consider

$$f = \operatorname{pf}(A_2) \operatorname{pf}(tA_2^{-1} - A_1) \in F[t].$$

Then f^2 is the characteristic polynomial of A_1A_2, so $\pm f$ is monic of degree m and the coefficients of f are polynomials in the entries of A_1, A_2 by Gauss' lemma. Also, as in the proof of the Cayley-Hamilton theorem we see that $f(A_1A_2) = 0$.

Hence for every t-antisymmetric $A_1, A_2 \in \mathrm{M}_{2m}(F)$ there exists $f = t^m + \sum_k (-1)^k c_k t^{m-k} \in F[t]$ such that $f(A_1A_2) = 0$. If A_1A_2 has distinct eigenvalues $\lambda_1, \dots, \lambda_m$, then their blocks in the Jordan decomposition of A_1A_2 have multiplicity 2 and

$$2\left(\sum_{j=1}^m \lambda_j^i\right) = \operatorname{tr}\left((A_1A_2)^i\right)$$

for $i \in \mathbb{N}$. Now Newton's identities imply

$$kc_k = \sum_{i=1}^k \frac{1}{2}(-1)^{i-1} \operatorname{tr}\left((A_1A_2)^k\right) c_{k-i}$$

for $1 \le k \le m$ and $c_0 = 1$.

Now define $f_m \in \mathbb{T}$ as

$$f_m = \sum_{k=0}^{m} (-1)^k f'_k \cdot (x_1x_2)^{m-k}$$

with $f'_0 = 1$ and

$$f'_k = \sum_{i=1}^{k} \frac{1}{2k}(-1)^{i-1} \operatorname{tr}\left((x_1x_2)^k\right) f'_{k-i} \tag{2.1}$$

for $1 \le k \le m$. The following lemmas will be important for distinguishing between different types of involutions of the first kind in the sequel.

Lemma 2.1. *For every $m \in \mathbb{N}$, $f_m(x_1 - x_1^*, x_2 - x_2^*)$ is a $*$-trace identity of $(\mathrm{M}_{2m}(F), \mathsf{t}, \mathrm{tr})$.*

Proof. Observe that the set of pairs of t-antisymmetric $A_1, A_2 \in \mathrm{M}_{2m}(F)$, such that A_1A_2 has m distinct eigenvalues, is Zariski dense in the set of all pairs of t-antisymmetric $A_1, A_2 \in \mathrm{M}_{2m}(F)$. Hence the conclusion follows by the construction of f_m. □

Lemma 2.2. *For every $n, m \in \mathbb{N}$ and $d \in \mathbb{N} \setminus 2\mathbb{N}$ there exist s-antisymmetric $A_1, A_2 \in \mathrm{M}_{2n}(F)$ such that*

$$f_m\left(A_1^{\oplus d} A_2^{\oplus d}\right) \neq 0.$$

Proof. Every t-symmetric matrix $S \in \mathrm{M}_{2n}(F)$ can be written as $S = (-SJ)J$, where $J = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $-SJ, J$ are s-antisymmetric matrices. Hence it suffices to prove that $f_m(S^{\oplus d}) \neq 0$ holds for

$$S = \operatorname{diag}(\overbrace{1, \dots, 1}^{2n-1}, 0) \in \mathrm{M}_{2n}(F).$$

Since $\operatorname{tr}((S^{\oplus d})^k) = d(2n-1)$ is odd, we can use (2.1) and induction on k to show that

$$k! f'_k(S^{\oplus d}) \in \left\{\frac{\ell}{2^k} : \ell \in \mathbb{Z}\right\} \setminus \left\{\frac{\ell}{2^{k-1}} : \ell \in \mathbb{Z}\right\}$$

for $1 \le k \le m$. In particular we have $f'_m(S^{\oplus d}) \neq 0$ and thus $f_m(S^{\oplus d}) \neq 0$. □

For $n \in \mathbb{N}$ and $m \in 2\mathbb{N}$ let $\mathscr{I}(n, \mathsf{t})$ denote the set of polynomial $*$-identities of $(\mathrm{M}_n(F), \mathsf{t})$ and let $\mathscr{I}(m, \mathsf{s})$ denote the set of polynomial $*$-identities of $(\mathrm{M}_m(F), \mathsf{s})$. By [Row80, Corollary 2.5.12 and Remark 2.5.13] we have $\mathscr{I}(m, \mathsf{s}) \subseteq \mathscr{I}(n, \mathsf{t})$ if and only if $2n \le m$.

Proposition 2.3. *Let $n \in \mathbb{N}$ and $m \in 2\mathbb{N}$. Then $\mathscr{I}(n, \mathsf{t}) \subseteq \mathscr{I}(m, \mathsf{s})$ if and only if $2m \le n$.*

Proof. ($\Rightarrow$) Let

$$c_m = \sum_{\pi \in \mathrm{Sym}_m} \operatorname{sgn} \pi \, x_{\pi(1)} x_{m+1} x_{\pi(2)} x_{m+2} \cdots x_{2m-1} x_{\pi(m)}$$

be the mth Capelli polynomial [Row80, Section 1.2]. If $\mathcal{A}$ is a central simple F-algebra and $a_1, \dots, a_m \in \mathcal{A}$, then $\{a_1, \dots, a_m\}$ is linearly dependent over F if and only if

$$c_g(a_1, \dots, a_g, b_1, \dots, b_{m-1}) = 0 \qquad \forall b_i \in \mathcal{A}$$

by [Row80, Theorem 1.4.34].

Now assume $n < 2m$. If $A_1, A_2 \in \mathrm{M}_n(F)$ are t-antisymmetric, then the set

$$\left\{A_1A_2, \dots, (A_1A_2)^{\lfloor n/2 \rfloor + 1}\right\}$$

is linearly dependent. Indeed, for an even n this holds directly by Lemma 2.1, while for an odd n we use the fact that A_1A_2 is singular and then apply Lemma 2.1 for $n+1$. On the other hand, since every t-symmetric matrix in $\mathrm{M}_m(F)$ is a product of two s-antisymmetric matrices, there exist s-antisymmetric $A_1, A_2 \in \mathrm{M}_m(F)$ such that $\{1, \dots, (A_1A_2)^{m-1}\}$ is linearly independent. Since $\lfloor \frac{n}{2} \rfloor + 1 \le m$,

$$c_m\Big((x_1 - x_1^*)(x_2 - x_2^*), \dots, ((x_1 - x_1^*)(x_2 - x_2^*))^m, x_3, \dots, x_{m+1}\Big)$$

is a $*$-identity of $\mathrm{M}_n(F)$ endowed with t but is not a $*$-identity of $\mathrm{M}_m(F)$ endowed with s.

($\Leftarrow$) By [Row80, Corollary 2.3.32] we can assume that F is algebraically closed; let $i \in F$ be such that $i^2 = -1$. Since $m \in 2\mathbb{N}$, $(\mathrm{M}_m(F), \mathsf{s})$ $*$-embeds into $(\mathrm{M}_{2m}(F), \mathsf{t})$ via

$$(\mathrm{M}_m(F), \mathsf{s}) \hookrightarrow (\mathrm{M}_{2m}(F), \mathsf{t}), \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{1}{2} \begin{pmatrix} a+d & i(a-d) & c-b & i(b+c) \\ i(d-a) & a+d & i(b+c) & b-c \\ b-c & -i(b+c) & a+d & i(a-d) \\ -i(b+c) & c-b & i(d-a) & a+d \end{pmatrix}.$$

□

Remark 2.4. The same reasoning as in the proof of Proposition 2.3 also implies that elements of $\mathscr{J}(n, \mathsf{t})$ are polynomial *-identities of $\mathrm{M}_m(F)$ with an involution of the second kind if and only if $2m \le n$. Recall that an involution on $\mathrm{M}_m(F)$ is of the second kind if it induces an automorphism of order two on F.

2.2. **Generic matrices and the trace ring.** For $g, n \in \mathbb{N}$ let

$$\boldsymbol{\xi} = \{\xi_{j\imath\jmath} \colon 1 \le j \le g, 1 \le \imath, \jmath \le n\}$$

be a set of commuting indeterminates. We recall the terminology from Section 1. Let

$$\Xi_j = (\xi_{j\imath\jmath})_{\imath\jmath} \in \mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$$

be $n \times n$ generic matrices and let $\mathrm{GM}_n \subset \mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$ be the $\mathbb{R}$-algebra generated by Ξ_j and their transposes Ξ_j^{t}. Furthermore, let $\mathbb{T}_n \subset \mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$ be the $\mathbb{R}$-algebra generated by GM_n and traces of elements in GM_n. This algebra is called the **trace ring** of $n \times n$ generic matrices (see e.g. [Pro76, Section 7]) and inherits the transpose involution t and trace tr from $\mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$. Let $C_n \subset T_n \subset \mathbb{R}[\boldsymbol{\xi}]$ be the centers of GM_n and $\mathbb{T}_n$, respectively. The elements of $\mathbb{T}_n$ are called **trace polynomials** and the elements of T_n are called **pure trace polynomials**.

There is another, more invariant-theoretic description of the trace ring. Define the following action of the orthogonal group $\mathrm{O}_n(\mathbb{R})$ on $\mathrm{M}_n(\mathbb{R})^g$:

$$(X_1, \dots, X_g)^u := (uX_1u^{\mathsf{t}}, \dots, uX_gu^{\mathsf{t}}), \qquad X_j \in \mathrm{M}_n(\mathbb{R}),\ u \in \mathrm{O}_n(\mathbb{R}) \tag{2.2}$$

and consider $\mathbb{R}[\boldsymbol{\xi}]$ as the coordinate ring of $\mathrm{M}_n(\mathbb{R})^g$. By [Pro76, Theorems 7.1 and 7.2], T_n is the ring of $\mathrm{O}_n(\mathbb{R})$-invariants in $\mathbb{R}[\boldsymbol{\xi}]$ and $\mathbb{T}_n$ is the ring of $\mathrm{O}_n(\mathbb{R})$-concomitants in $\mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$, i.e., elements $f \in \mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$ satisfying

$$f(X^u) = uf(X)u^{\mathsf{t}}$$

for all $X \in \mathrm{M}_n(\mathbb{R})^g$ and $u \in \mathrm{O}_n(\mathbb{R})$.

We list a few important properties of GM_n and $\mathbb{T}_n$ that will be used frequently in the sequel.

(a) Let $\mathscr{J}(n, \mathsf{t}, \mathrm{tr}) \subset \mathbb{T}$ denote the set of trace $*$-identities of $(\mathrm{M}_n(\mathbb{R}), \mathsf{t}, \mathrm{tr})$. Then $\mathrm{GM}_n \cong \mathbb{R}\langle \boldsymbol{x}, \boldsymbol{x}^* \rangle / \mathscr{J}(n, \mathsf{t})$ by [Row80, Remark 3.2.31] and $\mathbb{T}_n \cong \mathbb{T}/\mathscr{J}(n, \mathsf{t}, \mathrm{tr})$ by [Pro76, Theorem 8.4].

(b) By [Pro76, Theorem 20.1], the ring of central quotients of GM_n is a central simple algebra of degree n, which is also the ring of rational $\mathrm{O}_n(\mathbb{R})$-concomitants in $\mathrm{M}_n(\mathbb{R}(\boldsymbol{\xi}))$. It is called the **universal central simple algebra with orthogonal involution** of degree n. We denote it by USA_n and its center by Z_n. Note that USA_n is also the ring of central quotients of $\mathbb{T}_n$.

(c) By [Pro76, Theorem 7.3], T_n is a finitely generated $\mathbb{R}$-algebra and $\mathbb{T}_n$ is finitely spanned over T_n. In particular, T_n and $\mathbb{T}_n$ are Noetherian rings.

2.2.1. *Reynolds operator.* This subsection is to recall some basic properties of the Reynolds operator [DK02, Subsection 2.2.1]. Let G be an algebraic group and X an affine G-variety. The **Reynolds operator** $\mathcal{R} : F[X] \to F[X]^G$ is a linear map with the properties:

(1) $\mathcal{R}(f) = f$ for $f \in F[X]^G$,
(2) $\mathcal{R}$ is a G-module homomorphism; i.e., $\mathcal{R}(f^u) = \mathcal{R}(f)$ for $f \in F[X], u \in G$.

The Reynolds operator is hence a G-invariant projection onto the space of the invariants. The Reynolds operator exists if G is linearly reductive and is then unique (see e.g. [DK02, Theorem 2.2.5]).

Let M, N be G-modules and $f : M \to N$ a G-module homomorphism. Denote by M^G, N^G the modules of invariants of M, N, resp., the corresponding Reynolds operators by $\mathcal{R}_M, \mathcal{R}_N$, resp., and f^G a G-module homomorphism f restricted to M^G. Then $\mathcal{R}_N f = f^G \mathcal{R}_M$. This easily follows by the uniqueness of the Reynolds operator. The Reynolds operator is thus functorial.

In our case $\mathrm{O}_n(\mathbb{R})$ acts on $\mathrm{M}_n(\mathbb{R})^g$ by simultaneous conjugation as in (2.2). Since $\mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$ can be identified with polynomial maps $\mathrm{M}_n(\mathbb{R})^g \to \mathrm{M}_n(\mathbb{R})$, we have the Reynolds operator $\mathcal{R}_n : \mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}]) \to \mathbb{T}_n$ with respect to the action (2.2). Since $\mathrm{O}_n(\mathbb{R})$ is a compact Lie group, $\mathcal{R}_n$ can be given by the averaging integral formula (with respect to the normalized left Haar measure μ on $\mathrm{O}_n(\mathbb{R})$)

$$\mathcal{R}_n(f) = \int_{\mathrm{O}_n(\mathbb{R})} f^u \, d\mu(u). \tag{2.3}$$

Consequently $\mathcal{R}_n$ is a trace-intertwining $\mathbb{T}_n$-module homomorphism, i.e.,

$$\mathcal{R}_n(hf) = h\mathcal{R}_n(f), \qquad \mathcal{R}_n(fh) = \mathcal{R}_n(f)h, \qquad \mathrm{tr}(\mathcal{R}_n(f)) = \mathcal{R}_n(\mathrm{tr}(f)) \tag{2.4}$$

for all $h \in \mathbb{T}_n$ and $f \in \mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$. In Appendix A we present algebraic ways of computing $\mathcal{R}_n$.

2.3. **Positive involutions and totally positive elements.** Let $\mathcal{A}$ be a central simple algebra with involution τ and $*$-center F (that is, F is the subfield of $*$-invariant elements in the center of $\mathcal{A}$). The F-space of τ-symmetric elements in $\mathcal{A}$ is denoted $\mathrm{Sym}\,\mathcal{A}$. Following the terminology of [PS76] and [KU10], an ordering $\geq$ of F is a **$*$-ordering** if $\mathrm{tr}_{\mathcal{A}}(aa^\tau) \geq 0$ for every $a \in \mathcal{A}$. In this case we also say that τ is **positive** with respect to such an ordering. An element $a \in \mathrm{Sym}\,\mathcal{A}$ is **positive** in a given $*$-ordering if the hermitian form $x \mapsto \mathrm{tr}(x^\tau a x)$ on $\mathcal{A}$ is positive semidefinite. Finally, $a \in \mathrm{Sym}\,\mathcal{A}$ is **totally positive** if it is positive with respect to every $*$-ordering.

Let $\alpha_1, \dots, \alpha_n \in F$ be the elements appearing in a diagonalization of the form $x \mapsto \mathrm{tr}(xx^\tau)$ on $\mathcal{A}$. By [PS76, Theorem 5.4], a symmetric $s \in \mathcal{A}$ is totally positive if and only if it has a weighted sum of hermitian squares representation

$$s = \sum_{I \in \{0,1\}^n} \alpha^I \sum_i h_{I,i} h_{I,i}^\tau, \tag{2.5}$$

where $\alpha^I = \alpha_1^{I_1} \cdots \alpha_n^{I_n}$ and $h_{I,i} \in \mathcal{A}$.

Let $\Omega_n \subset T_n$ be the **preordering** generated by $\mathrm{tr}(hh^{\mathrm{t}})$ for $h \in \mathbb{T}_n$, i.e., the set of all sums of products of $\mathrm{tr}(hh^{\mathrm{t}})$ (note that $c^2 = \mathrm{tr}((\frac{c}{\sqrt{n}})^2) \in \Omega_n$ for every $c \in T_n$, so Ω_n is really a preordering). Further, let

$$\mho_n = \left\{ \sum_i \omega_i h_i h_i^{\mathrm{t}} \colon \omega_i \in \Omega_n, h_i \in \mathbb{T}_n \right\}.$$

Note that $\Omega_n = \mathrm{tr}(\mho_n)$.

Lemma 2.5. *Let $f \in \mathrm{Sym}\,\mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$. If $f(X) \succeq 0$ for all $X \in \mathrm{M}_n(\mathbb{R})^g$, then $\mathcal{R}_n(f) = c^{-2} q$ for some $q \in \mho_n$ and $c \in T_n \setminus \{0\}$.*

Proof. By the integral formula (2.3) it is clear that $\mathcal{R}_n(f)(X) \succeq 0$ for all $X \in \mathrm{M}_n(\mathbb{R})^g$. Hence $\mathcal{R}_n(f)$ is a totally positive element in USA_n by [KU10, Lemma 5.3], so

$$\mathcal{R}_n(f) = \sum_{I \in \{0,1\}^{n^2}} \alpha^I \sum_i h_{I,i} h_{I,i}^{\mathsf{t}}$$

for some $h_{I,i} \in \mathrm{USA}_n$ and a diagonalization $\langle \alpha_1, \dots, \alpha_{n^2} \rangle$ over Z_n of the form $x \mapsto \mathrm{tr}(xx^{\mathsf{t}})$ on USA_n. Hence $\alpha_k = \mathrm{tr}(\tilde{h}_k \tilde{h}_k^{\mathsf{t}})$ for some $\tilde{h}_k \in \mathrm{USA}_n$. Since USA_n is the ring of central quotients of $\mathbb{T}_n$, there exist $q \in \mathfrak{N}_n$ and $c \in T_n$ such that $\mathcal{R}_n(f) = c^{-2} q$. □

As demonstrated in Example 6.2, the denominator in Lemma 2.5 is in general indispensable even if f is a hermitian square or $f \in \mathbb{R}[\boldsymbol{\xi}]$. For more information about images of squares under Reynolds operators for reductive groups acting on real affine varieties see [CKS09].

Remark 2.6. In particular, the linear operator $\mathcal{R}_n$ does not map squares in $\mathbb{R}[\boldsymbol{\xi}]$ into Ω_n or hermitian squares in $\mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$ into $\mathfrak{N}_n$. Hence our Positivstellensätze in the sequel cannot simply be deduced from their commutative or matrix counterparts by averaging with $\mathcal{R}_n$. Furthermore, even if one were content with using totally positive polynomials (which by Lemma 2.5 are of the form $c^{-2}q$ for $q \in \mathfrak{N}_n$ and $c \in T_n \setminus \{0\}$) instead of $\mathfrak{N}_n$, one could still not derive our results since $\mathcal{R}_n$ is not multiplicative.

3. Counterexample to the 3×3 universal Procesi-Schacher conjecture

By [PS76, Corollary 5.5] every totally positive element in USA_2 is a sum of hermitian squares, i.e., of the form $c^{-2} \sum_i h_i h_i^{\mathsf{t}}$ for $c \in C_2$ and $h_i \in \mathrm{GM}_2$. Indeed, by (2.5) it suffices to show that $\mathrm{tr}(aa^{\mathsf{t}})$ is a sum of hermitian squares. Since USA_2 is a division ring, we have

$$\mathrm{tr}(aa^{\mathsf{t}}) = a^{\mathsf{t}} a + (\det(a) a^{-1})(\det(a) a^{-1})^{\mathsf{t}}$$

for every $a \in \mathrm{USA}_2 \setminus \{0\}$ by the Cayley-Hamilton theorem. In their 1976 paper [PS76], Procesi and Schacher asked if the same holds true for $n > 2$:

Conjecture 3.1 (The universal Procesi-Schacher conjecture)**.** *Let $n \geq 2$. Then every totally positive element in USA_n is a sum of hermitian squares.*

By (2.5), Conjecture 3.1 is equivalent to the following: every trace of a hermitian square in USA_n is a sum of hermitian squares in USA_n. In this section we show that Conjecture 3.1 fails for $n = 3$:

Theorem 3.2. *There exist totally positive elements in USA_3 that are not sums of hermitian squares in USA_3.*

In the first step of the proof we identify the split central simple algebra USA_3 as a matrix algebra $\mathrm{M}_3(F)$ for a rational function field F, endowed with an involution of the orthogonal type. For the constructive proof of Theorem 3.2 we then use Prestel's theory of semiorderings [PD01].

We recall some terminology of quadratic forms from [KMRT98]. Let F be a field and V an n-dimensional vector space. Quadratic forms q and q' are equivalent if there exists $\theta \in \mathrm{GL}_F V$ such that $q' = q \circ \theta$. Quadratic forms q and q' are similar if αq and q' are equivalent for some $\alpha \in F \setminus \{0\}$. Every quadratic form is equivalent to a diagonal quadratic form, which is denoted $\langle \alpha_1, \dots, \alpha_n \rangle$ for $\alpha_i \in F$.

First we fix $g = 1$ and write $\Xi = \Xi_1$. Since USA_3 is an odd degree central simple algebra with involution of the first kind, USA_3 is split by [KMRT98, Corollary 2.8]. Let us fix a $*$-representation $\mathrm{USA}_3 = \mathrm{End}_{Z_3} V$, where V is a 3-dimensional vector space over Z_3, the center of

USA_3. By [KMRT98, Proposition 2.1], there exists a symmetric bilinear form $b : V \times V \to Z_3$ such that

$$b(xu, v) = b(u, x^{\mathtt{t}} v)$$

for all $u, v \in V$ and $x \in \operatorname{End}_{Z_3} V$, where $\mathtt{t}$ denotes the involution on $\operatorname{End}_{Z_3} V$ originating from USA_3. Let $q : V \to Z_3$ given by $q(u) = b(u, u)$ be the associated quadratic form.

Lemma 3.3. *Let $a \in \operatorname{End}_{Z_3} V$ be $\mathtt{t}$-antisymmetric with $\operatorname{tr}(a^2) \neq 0$. Define $e = 1 - 2\operatorname{tr}(a^2)^{-1} a^2$. Then e is a symmetric idempotent of rank 1 such that $V = \operatorname{im} e \perp \ker e$. Moreover, $\operatorname{im} a = \ker e$ and $\ker a = \operatorname{im} e$, and the determinant of the restriction of q to $\ker e$ is $-\frac{1}{2}\operatorname{tr}(a^2)$.*

Proof. Since a and $a^{\mathtt{t}} = -a$ have the same trace and determinant, we have $\operatorname{tr}(a) = \det(a) = 0$, so by the Cayley-Hamilton theorem it follows that

$$a^3 - \frac{1}{2}\operatorname{tr}(a^2) a = 0. \tag{3.1}$$

Hence $a^4 = \frac{1}{2}\operatorname{tr}(a^2)a^2$ and it is straightforward to check that e is a symmetric idempotent. It has rank 1 because $\operatorname{tr}(e) = 1$, and the decomposition $V = \operatorname{im} e \oplus \ker e$ is orthogonal because e is symmetric. The equation (3.1) also yields $ea = ae = 0$, hence $\operatorname{im} a \subseteq \ker e$ and $\operatorname{im} e \subseteq \ker a$. Since the rank of every antisymmetric matrix is even, we have $\operatorname{im} a = \ker e$ and $\operatorname{im} e = \ker a$.

To prove the last statement, observe that the restriction of a to $\ker e$ is an antisymmetric operator with determinant $-\frac{1}{2}\operatorname{tr}(a^2)$, and the determinant of the restriction of q to $\ker e$ is the square class of the determinant of any nonzero antisymmetric operator; see [KMRT98, Proposition 7.3]. □

Proposition 3.4. *For $i = 1, 2$ let $a_i \in \operatorname{End}_{Z_3} V$ be $\mathtt{t}$-antisymmetric with $\operatorname{tr}(a_i^2) \neq 0$, and let $e_i = 1 - 2\operatorname{tr}(a_i^2)^{-1} a_i^2$. If $e_1 e_2 = e_2 e_1 = 0$, then q is similar to $\langle 1, -\frac{1}{2}\operatorname{tr}(a_1^2), -\frac{1}{2}\operatorname{tr}(a_2^2)\rangle$.*

Proof. Let $e_3 = 1 - e_1 - e_2$ and $V_i = \operatorname{im} e_i$ for $i = 1, 2, 3$; we have $\dim V_i = 1$ for each i. Moreover, if $u \in V_i$ and $v \in V_j$ for $i \neq j$, then

$$b(u, v) = b(e_i u, e_j v) = b(u, e_i e_j v) = 0.$$

Therefore $V = V_1 \perp V_2 \perp V_3$. We have $\ker e_1 = V_2 \perp V_3$ and $\ker e_2 = V_1 \perp V_3$, and Lemma 3.3 shows that the determinant of the restriction of q to $\ker e_i$ is $-\frac{1}{2}\operatorname{tr}(a_i^2)$ for $i = 1, 2$. If $\alpha \in Z_3 \setminus \{0\}$ is such that the restriction of q to V_3 is equivalent to $\langle \alpha \rangle$, then it follows that the restriction of q to V_i is equivalent to $\langle -\frac{\alpha}{2}\operatorname{tr}(a_i^2)\rangle$ for $i = 1, 2$. Hence q is equivalent to $\langle \alpha, -\frac{\alpha}{2}\operatorname{tr}(a_1^2), -\frac{\alpha}{2}\operatorname{tr}(a_2^2)\rangle$. □

Now let

$$\begin{aligned} a_1 &= \Xi - \Xi^{\mathtt{t}}, & a_2 &= e_1 \Xi (1 - e_1) - (1 - e_1)\Xi^{\mathtt{t}} e_1, \\ e_1 &= 1 - 2\operatorname{tr}(a_1^2)^{-1} a_1^2, & e_2 &= 1 - 2\operatorname{tr}(a_2^2)^{-1} a_2^2, \\ \beta_1 &= -\frac{1}{2}\operatorname{tr}(a_1^2), & \beta_2 &= -\frac{1}{2}\operatorname{tr}(a_2^2). \end{aligned}$$

Since a_1, a_2 are nonzero, it follows from $a_i^3 - \frac{1}{2}\operatorname{tr}(a_i^2)a_i = 0$ that $\beta_i \neq 0$ for $i = 1, 2$. It is also easy to check that $e_1 e_2 = e_2 e_1 = 0$, so the conclusion of Proposition 3.4 holds. Hence we can choose a basis of V in such a way that

$$x^{\mathtt{t}} = \operatorname{diag}(1, \beta_1, \beta_2)^{-1} x^{\tau} \operatorname{diag}(1, \beta_1, \beta_2) \tag{3.2}$$

for all $x \in \operatorname{End}_{Z_3} V$, where τ is the transpose in $\mathrm{M}_3(Z_3) = \operatorname{End}_{Z_3} V$ with respect to the chosen basis of V.

The field Z_3 is rational over $\mathbb{R}$ by [Sal02, Theorem 1.2] and of transcendental degree 6 by [BS88, Theorem 1.11]. Inspired by [For79, Section 3] we present an explicit transcendental basis for Z_3 over $\mathbb{R}$. Denote

$$s=\frac{1}{2}(\Xi+\Xi^{\mathrm{t}}),\qquad a=\frac{1}{2}(\Xi-\Xi^{\mathrm{t}}),\qquad s_0=s-\frac{1}{3}\operatorname{tr}(s)$$

and

$$\begin{aligned}
&\alpha_1=\operatorname{tr}(s), &&\alpha_4=\frac{\operatorname{tr}(a^2)^2\operatorname{tr}(s_0^2)-6\operatorname{tr}(s_0a^2)^2}{\operatorname{tr}(a^2)^2\operatorname{tr}(s_0^2)-4\operatorname{tr}(a^2)\operatorname{tr}(s_0^2a^2)-2\operatorname{tr}(s_0a^2)^2},\\
&\alpha_2=\operatorname{tr}(a^2), &&\alpha_5=\frac{\operatorname{tr}(a^2)^3\operatorname{tr}(s_0^3)+6\operatorname{tr}(s_0a^2)^3}{\operatorname{tr}(a^2)^2\operatorname{tr}(s_0^2)-6\operatorname{tr}(s_0a^2)^2},\\
&\alpha_3=\operatorname{tr}(s_0a^2), &&\alpha_6=\frac{\operatorname{tr}(as_0a^2s_0^2)}{\operatorname{tr}(a^2)^2\operatorname{tr}(s_0^2)-6\operatorname{tr}(s_0a^2)^2}.
\end{aligned}\tag{3.3}$$

Lemma 3.5. *The elements $\alpha_1,\dots,\alpha_6$ are algebraically independent over $\mathbb{R}$, $Z_3=\mathbb{R}(\alpha_1,\dots,\alpha_6)$, and*

$$\beta_1=-\frac{1}{2}\alpha_2,\qquad \beta_2=\frac{288\alpha_2^3\alpha_4^2\alpha_6^2-(3\alpha_3\alpha_4+2\alpha_4\alpha_5+9\alpha_3)^2}{9\alpha_2^2(\alpha_4+1)}.\tag{3.4}$$

Proof. Using a computer algebra system one can verify that the determinant of the Jacobian matrix $\mathrm{J}_{\alpha_1,\dots,\alpha_6}$ is nonzero, so by the Jacobian criterion $\alpha_1,\dots,\alpha_6$ are algebraically independent over $\mathbb{R}$. Likewise, (3.4) is checked by a computer algebra system.

A minimal set of generators of pure trace polynomials in two 3×3 generic matrices without involution is given in [ADS06, Section 1] or in the proof of [LV88, Proposition 7]. Replacing the first generic matrix by s and the second generic matrix by a we obtain the following generators of T_3:

$$\operatorname{tr}(s),\quad \operatorname{tr}(s_0^2),\quad \operatorname{tr}(s_0^3),\quad \operatorname{tr}(a^2),\quad \operatorname{tr}(s_0a^2),\quad \operatorname{tr}(s_0^2a^2),\quad \operatorname{tr}(as_0a^2s_0^2).\tag{3.5}$$

From (3.3) we can directly see that (3.5) are rational functions in $\alpha_1,\dots,\alpha_6,\operatorname{tr}(s_0)^2$; for example,

$$\operatorname{tr}(s_0^3)=\frac{\alpha_5(\alpha_2^2\operatorname{tr}(s_0^2)-6\alpha_3^2)-6\alpha_3^3}{\alpha_2^3}.$$

Then we use a computer algebra system to verify that

$$\operatorname{tr}(s_0^2)=\frac{2\alpha_4}{\alpha_4+1}\beta_2+\frac{6\alpha_3^2}{\alpha_2^2}$$

is a rational function in $\alpha_1,\dots,\alpha_6$ and hence $Z_3=\mathbb{R}(\alpha_1,\dots,\alpha_6)$. □

Proposition 3.6. *$\beta_1\beta_2\in Z_3$ is totally positive in* USA_3 *but is not a sum of hermitian squares in* USA_3.

Proof. Since $\beta_1\beta_2=\operatorname{tr}(hh^{\mathrm{t}})$ for

$$h=\begin{pmatrix}0&0&0\\0&0&\beta_2\\0&0&0\end{pmatrix},$$

$\beta_1\beta_2$ is totally positive in USA_3. Now suppose $\beta_1\beta_2=\sum_i r_ir_i^{\mathrm{t}}$ for $r_i\in\mathrm{USA}_3$. If $r_i=(\rho_{i\imath\jmath})_{\imath\jmath}$, then the $(1,1)$-entry of $\sum_i r_ir_i^{\mathrm{t}}$ equals

$$\sum_i\left(\rho_{i11}^2+\beta_1^{-1}\rho_{i12}^2+\beta_2^{-1}\rho_{i13}^2\right)$$

and therefore

$$1=\beta_1\beta_2\sum_i\left(\frac{\rho_{i11}}{\beta_1\beta_2}\right)^2+\beta_2\sum_i\left(\frac{\rho_{i12}}{\beta_1\beta_2}\right)^2+\beta_1\sum_i\left(\frac{\rho_{i13}}{\beta_1\beta_2}\right)^2.\tag{3.6}$$

By [PD01, Exercise 5.5.3 and Lemma 5.1.8] there exists a semiordering $Q \subset \mathbb{R}(\alpha_1, \dots, \alpha_6)$ satisfying $\alpha_2, -\alpha_4, -\alpha_2\alpha_4 \in Q$ and $p \in Q \cap \mathbb{R}[\alpha_1, \dots, \alpha_6]$ if and only if the term of the highest degree in p belongs to Q. These assumptions on Q yield $-\beta_1, -\beta_2, -\beta_1\beta_2 \in Q$, so (3.6) implies $-1 \in Q$, a contradiction. □

Proof of Theorem 3.2. To be more precise we write $\mathrm{USA}_{3,g}$ for USA_3 generated by g generic matrices Ξ_j. Proposition 3.6 proves Theorem 3.2 for $g = 1$. Now let $g \in \mathbb{N}$ be arbitrary; note that $\mathrm{USA}_{3,1}$ naturally $*$-embeds into $\mathrm{USA}_{3,g}$. Let $s \in \mathrm{USA}_{3,1}$ be a totally positive element that is not a sum of hermitian squares in $\mathrm{USA}_{3,1}$. Suppose that s is a sum of hermitian squares in $\mathrm{USA}_{3,g}$, i.e.,

$$s = c^{-2} \sum_j h_i h_i^{\mathrm{t}}$$

for some $c, h_i \in \mathrm{GM}_{3,g}$ with c central. Since the sets of polynomial $*$-identities of $\mathrm{GM}_{3,1}$ and $\mathrm{GM}_{3,g}$ coincide, it is easy to see that there exists a $*$-homomorphism $\phi : \mathrm{GM}_{3,g} \to \mathrm{GM}_{3,1}$ satisfying $\phi(\Xi_1) = \Xi_1$ and $\phi(c) \neq 0$. Then

$$s = \phi(c)^{-2} \sum_j \phi(h_i)\phi(h_i)^{\mathrm{t}}$$

is a sum of hermitian squares in $\mathrm{USA}_{3,1}$, a contradiction. □

We do not know if Conjecture 3.1 holds for $n = 4$, where USA_4 is a division biquaternion algebra by [Pro76, Theorem 20.1] and hence does not split. In [AU+] the authors use signatures of hermitian forms to distinguish between sums of hermitian squares and general totally positive elements.

4. The Krivine-Stengle Positivstellensatz for trace polynomials

In this section we prove the Krivine-Stengle Positivstellensatz representing trace polynomials positive on semialgebraic sets in terms of weighted sums of hermitian squares with denominators.

4.1. Cyclic quadratic modules and preorderings.

For a finite $S \subset \operatorname{Sym} \mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$ let

$$K_S = \{X \in \mathrm{M}_n(\mathbb{R})^g : s(X) \succeq 0 \ \forall s \in S\}$$

be the **semialgebraic set** described by S. A set $\mathfrak{Q} \subseteq \operatorname{Sym} \mathbb{T}_n$ is a **cyclic quadratic module** if

$$1 \in \mathfrak{Q}, \quad \mathfrak{Q} + \mathfrak{Q} \subseteq \mathfrak{Q}, \quad h\mathfrak{Q}h^{\mathrm{t}} \subseteq \mathfrak{Q} \ \ \forall h \in \mathbb{T}_n, \quad \mathrm{tr}(\mathfrak{Q}) \subset \mathfrak{Q}.$$

A cyclic quadratic module $\mathfrak{T} \subseteq \operatorname{Sym} \mathbb{T}_n$ is a **cyclic preordering** if $\mathfrak{T} \cap T_n$ is closed under multiplication. For $S \subset \operatorname{Sym} \mathbb{T}_n$ let $\mathfrak{Q}_S^{\mathrm{tr}}$ and $\mathfrak{T}_S^{\mathrm{tr}}$ denote the cyclic quadratic module and preordering, respectively, generated by S. For example, $\mathfrak{Q}_\emptyset^{\mathrm{tr}} = \mathfrak{T}_\emptyset^{\mathrm{tr}} = \mathfrak{N}_n$.

Lemma 4.1. *Let $S \subseteq \operatorname{Sym} \mathbb{T}_n$.*

(1) *If $\mathfrak{Q}$ is a cyclic quadratic module, then $\mathrm{tr}(\mathfrak{Q}) = \mathfrak{Q} \cap T_n$.*
(2) *Elements of $\mathfrak{Q}_S^{\mathrm{tr}}$ are precisely sums of*

$$q_1, \qquad h_1 s_1 h_1^{\mathrm{t}}, \qquad \mathrm{tr}(h_2 s_2 h_2^{\mathrm{t}}) q_2$$

for $q_i \in \mathfrak{N}_n$, $h_i \in \mathbb{T}_n$ and $s_i \in S$.
(3) *$\mathfrak{T}_S^{\mathrm{tr}} = \mathfrak{Q}_{S'}^{\mathrm{tr}}$, where*

$$S' = S \cup \left\{ \prod_i \mathrm{tr}(h_i s_i h_i^{\mathrm{t}}) : h_i \in \mathbb{T}_n, s_i \in S \right\}.$$

Proof. Straightforward. □

Our main result of this subsection is a reduction to central generators for cyclic quadratic modules, see Corollary 4.4. It will be used several times in the sequel. In its proof we need the following lemma.

Lemma 4.2. *Let R be an ordered field, $\lambda_1,\dots,\lambda_n\in R$ and $p_i=\sum_{j=1}^n\lambda_j^i$ for $i\in\mathbb{N}$. If $\lambda_{j_0}<0$ for some $1\le j_0\le n$, then there exists $f\in\mathbb{Q}[p_1,\dots,p_n][\zeta]$ such that*

$$\sum_{j=1}^n f(\lambda_j)^2\lambda_j<0. \tag{4.1}$$

Proof. Denote $E=\mathbb{Q}(p_1,\dots,p_n)$ and $F=\mathbb{Q}(\lambda_1,\dots,\lambda_n)$. For every $f=\sum_{i=0}^{n-1}\alpha_i\zeta^i\in F[\zeta]$ we have

$$\sum_{j=1}^n f(\lambda_j)^2\lambda_j=\sum_j\sum_{i,i'}\alpha_i\alpha_{i'}\lambda_j^{i+i'+1}=\sum_{i,i'}\left(\sum_j\lambda_j^{i+i'+1}\right)\alpha_i\alpha_{i'}=\sum_{i,i'}p_{i+i'+1}\alpha_i\alpha_{i'}. \tag{4.2}$$

Note that $p_i\in E$ for every $i\in\mathbb{N}$ and define $P\in\mathrm{M}_n(E)$ by $P_{ij}=p_{i+j-1}$. If $\lambda_{j_0}<0$, then there clearly exists $f_0\in F[\zeta]$ of degree $n-1$ such that $f_0(\lambda_{j_0})\neq0$ and $f_0(\lambda_j)=0$ for $\lambda_j\neq\lambda_{j_0}$. Then f_0 satisfies (4.1), so P is not positive semidefinite as a matrix over F by (4.2). Since $P=QDQ^{\mathrm{t}}$ for some $Q\in\mathrm{GL}_n(E)$ and diagonal $D\in\mathrm{M}_n(E)$, we conclude that P is not positive semidefinite as a matrix over E, so there exists $v=(\beta_0,\dots,\beta_{n-1})^{\mathrm{t}}\in E^n$ such that $v^{\mathrm{t}}Pv<0$. By (4.2), $f_1=\sum_{i=0}^{n-1}\beta_i\zeta^i\in E[\zeta]$ satisfies (4.1). After clearing the denominators of the coefficients of f_1 we obtain $f\in\mathbb{Q}[p_1,\dots,p_n][\zeta]$ satisfying (4.1). □

The proof of the next proposition requires some well-known notions and facts from real algebra that we recall now. Let Λ be a commutative unital ring. Then $P\subset\Lambda$ is a **ordering** if P is closed under addition and multiplication, $P\cup-P=\Lambda$ and $P\cap-P$ is a prime ideal in Λ. Note that every ordering in Λ gives rise to a ring homomorphism from Λ into a real closed field and vice versa. The set of all orderings is the **real spectrum** of Λ, denoted $\operatorname{Sper}\Lambda$. For $a\in\Lambda$ let $K(a)=\{P\in\operatorname{Sper}\Lambda\colon a\in P\}$. Then the sets $K(a)$ and $\operatorname{Sper}\Lambda\setminus K(a)$ for $a\in\Lambda$ form a subbasis of the **constructible topology** [BCR98, Section 7.1] (also called patch topology [Mar08, Section 2.4]). By [BCR98, Proposition 1.1.12] or [Mar08, Theorem 2.4.1], $\operatorname{Sper}\Lambda$ endowed with this topology is a compact Hausdorff space. In particular, since the sets $K(a)$ are closed in $\operatorname{Sper}\Lambda$, they are also compact.

Proposition 4.3. *For every $s\in\operatorname{Sym}\mathbb{T}_n$ let $\mathcal{O}\subset\mathbb{T}_n$ be the ring of polynomials in s and $\operatorname{tr}(s^i)$ for $i\in\mathbb{N}$ with rational coefficients, and set*

$$S=\{\operatorname{tr}(hsh)\colon h\in\mathcal{O}\}\subset\operatorname{tr}\left(\mathfrak{Q}^{\operatorname{tr}}_{\{s\}}\right).$$

Then there exists a finite subset $S_0\subset S$ such that $K_{\{s\}}=K_{S_0}$.

Proof. First we prove that for every real closed field R we have

$$\{X\in\mathrm{M}_n(R)^g\colon s(X)\succeq0\}=\bigcap_{c\in S}\{X\in\mathrm{M}_n(R)^g\colon c(X)\ge0\}. \tag{4.3}$$

The inclusion $\subseteq$ is obvious. Let $X\in\mathrm{M}_n(R)^g$ be such that $s(X)$ is not positive semidefinite. Since R is real closed and pure trace polynomials are $\mathrm{O}_n(\mathbb{R})$-invariant, we can assume that $s(X)=\operatorname{diag}(\lambda_1,\dots,\lambda_n)$ is diagonal and $\lambda_j<0$ for some j. If $p_i=\operatorname{tr}(s(X)^i)$, then by Lemma 4.2 there exists a polynomial $f\in\mathbb{Q}[p_1,\dots,p_n][\zeta]$ such that

$$\sum_{i=1}^n f(\lambda_i)^2\lambda_i<0.$$

If $h\in\mathcal{O}$ is such that $h(X)=f(s(X))$, then $\operatorname{tr}(h(X)s(X)h(X))<0$. Hence $\supseteq$ in (4.3) holds.

Let $\sigma_j = \operatorname{tr}(\wedge^j s) \in T_n$ for $1 \le j \le n$, where $\wedge^j s$ denotes the jth exterior power of s; hence σ_j are signed coefficients of the characteristic polynomial for s and

$$\{X \in \mathrm{M}_n(R)^g : s(X) \succeq 0\} = \{X \in \mathrm{M}_n(R)^g : \sigma_1(X) \ge 0, \dots, \sigma_n(X) \ge 0\}$$

for all real closed fields R. In terms of $\operatorname{Sper} \mathbb{R}[\boldsymbol{\xi}]$ and the notation introduced before the proposition, (4.3) can be stated as

$$\bigcap_{j=1}^{n} K(\sigma_j) = \bigcap_{c \in S} K(c) \tag{4.4}$$

by the correspondence between homomorphisms from $\mathbb{R}[\boldsymbol{\xi}]$ to real closed fields and orderings in $\mathbb{R}[\boldsymbol{\xi}]$. Since the complement of the left-hand side of (4.4) is compact in the constructible topology, there exists a finite subset $S_0 \subset S$ such that

$$\bigcap_{j=1}^{n} K(\sigma_j) = \bigcap_{c \in S_0} K(c)$$

and consequently

$$K_{\{s\}} = K_{\{\sigma_1,\dots,\sigma_n\}} = K_{S_0}. \qquad \square$$

Corollary 4.4. *For every finite set $S \subset \operatorname{Sym} \mathbb{T}_n$ there exists a finite set $S' \subset \operatorname{tr}(\mathfrak{Q}_S^{\mathrm{tr}})$ such that $K_S = K_{S'}$.*

Proof. Let $S = \{s_1, \dots, s_\ell\}$. By Proposition 4.3 there exist finite sets $S_i \subset \mathfrak{Q}^{\mathrm{tr}}_{\{s_i\}} \cap T_n$ with $K_{S_i} = K_{\{s_i\}}$. If $S' = S_1 \cup \cdots \cup S_\ell$, then

$$S' \subset \bigcup_i \mathfrak{Q}^{\mathrm{tr}}_{\{s_i\}} \cap T_n \subset \mathfrak{Q}^{\mathrm{tr}}_S \cap T_n$$

and

$$K_{S'} = \bigcap_i K_{S_i} = \bigcap_i K_{\{s_i\}} = K_S. \qquad \square$$

Corollary 4.5. *For every cyclic quadratic module $\mathfrak{Q} \subseteq \operatorname{Sym} \mathbb{T}_n$ we have $K_{\mathfrak{Q}} = K_{\operatorname{tr}(\mathfrak{Q})}$.*

Proof. Direct consequence of Corollary 4.4. $\square$

4.2. **An extension theorem.** The main result in this subsection, Theorem 4.8, characterizes homomorphisms from pure trace polynomials T_n to a real closed field R which arise via point evaluations $\xi_{j\imath\jmath} \mapsto \alpha_{j\imath\jmath} \in R$.

We start with some additional terminology. Let F be a field and let $\mathcal{A}$ be a finite-dimensional simple F-algebra with center C. If $\operatorname{tr}_{\mathcal{A}}$ is the reduced trace of $\mathcal{A}$ as a central simple algebra and $\operatorname{tr}_{C/F}$ is the trace of the field extension C/F, then

$$\operatorname{tr}_{\mathcal{A}}^F = \operatorname{tr}_{C/F} \circ \operatorname{tr}_{\mathcal{A}} : \mathcal{A} \to F$$

is called the **reduced F-trace** of $\mathcal{A}$ [DPRR05, Section 4].

Proposition 4.6. *Let $R \supseteq \mathbb{R}$ be a real closed field and $\mathcal{A}$ a finite-dimensional semisimple R-algebra with an R-trace χ and a split involution, which is positive on every simple factor. Assume there exists a trace preserving $*$-homomorphism $\Phi : \mathbb{T}_n \to \mathcal{A}$ such that $\Phi(T_n) \subseteq R$ and $\mathcal{A}$ is generated by $\Phi(\mathbb{T}_n)$ over R. Then there exists a trace preserving $*$-embedding of $\mathcal{A}$ into $(\mathrm{M}_n(R), \mathrm{t}, \operatorname{tr})$.*

Proof. Let $\mathcal{A} \cong \mathcal{A}_1 \times \cdots \times \mathcal{A}_\ell$ be the decomposition in simple factors and let n_k be the degree of $\mathcal{A}_k$ for $1 \le k \le \ell$. Moreover, let $C = R[i]$ be the algebraic closure of R and $H = (\frac{-1,-1}{R})$ the division quaternion algebra over R. By [PS76, Theorem 1.2], each of $\mathcal{A}_k$ is $*$-isomorphic to one of the following:

(I) $\mathrm{M}_{n_k}(R)$ with the transpose involution;
(II) $\mathrm{M}_{n_k}(C)$ with the conjugate-transpose involution;
(III) $\mathrm{M}_{n_k/2}(H)$ with the symplectic involution.

Without loss of generality assume that there are $1 \le \ell_1 \le \ell_2 \le \ell$ such that $\mathcal{A}_{n_k}$ is of type (I) for $k \le \ell_1$, of type (II) for $\ell_1 < k \le \ell_2$, and of type (III) for $\ell_2 < k$. By [DPRR05, Theorem 4.2] there exist $d_1, \dots, d_\ell \in \mathbb{N}$ such that

$$\chi\left(\sum_k a_k\right) = \sum_k d_k \operatorname{tr}^R_{\mathcal{A}_k}(a_k) \tag{4.5}$$

for $a_k \in \mathcal{A}_k$. We claim that $d_k \in 2\mathbb{N}$ for every $k > \ell_2$. Let $n' = \lceil \frac{n}{2} \rceil$ and fix $k > \ell_2$. By Lemma 2.1, $f = f_{n'}(x_1 - x_1^*, x_2 - x_2^*)$ is a $*$-trace identity for $\mathbb{T}_n$. Therefore f is also a $*$-trace identity for $\mathcal{A}$ by the assumptions on Φ. Hence f is a $*$-trace identity for $(\mathcal{A}_k, \tau_k, d_k \cdot \operatorname{tr}^R_{\mathcal{A}_k})$, where τ_k is the restriction of the involution on $\mathcal{A}$. Since $*$-trace identities are preserved by scalar extensions and

$$C \otimes_R \left(\mathcal{A}_k, \tau_k, d_k \cdot \operatorname{tr}^R_{\mathcal{A}_k}\right) \cong C \otimes_R \left(\mathrm{M}_{n_k/2}(H), \mathsf{s}, d_k \cdot (\operatorname{tr}_H \circ \operatorname{tr})\right) \cong \left(\mathrm{M}_{n_k}(C), \mathsf{s}, d_k \cdot \operatorname{tr}\right),$$

f is a $*$-trace identity for $(\mathrm{M}_{n_k}(C), \mathsf{s}, d_k \cdot \operatorname{tr})$. Now Lemma 2.2 implies $d_k \in 2\mathbb{N}$.

Thus we have

$$n = \sum_{k \le \ell_1} d_k n_k + \sum_{\ell_1 < k \le \ell_2} 2 d_k n_k + \sum_{\ell_2 < k} 4 \frac{d_k}{2} n_k \tag{4.6}$$

by (4.5) and the definition of the reduced R-trace. The standard embeddings

$$\psi_1 : C \hookrightarrow \mathrm{M}_2(R), \qquad \alpha + \beta i \mapsto \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$$

$$\psi_2 : H \hookrightarrow \mathrm{M}_4(R), \qquad \alpha + \beta i + \gamma j + \delta k \mapsto \begin{pmatrix} \alpha & -\beta & -\gamma & -\delta \\ \beta & \alpha & -\delta & \gamma \\ \gamma & \delta & \alpha & -\beta \\ \delta & -\gamma & \beta & \alpha \end{pmatrix}$$

transform conjugate-transpose involution and symplectic involution into transpose involution; moreover, ψ_1 preserves the reduced R-trace, while ψ_2 doubles it. Therefore we have trace preserving $*$-embeddings

$$(\mathrm{M}_{n_k}(R), \mathsf{t}, d_k \cdot \operatorname{tr}) \hookrightarrow (\mathrm{M}_{d_k n_k}(R), \mathsf{t}, \operatorname{tr}), \qquad X \mapsto X^{\oplus d_k}$$

for $k \le \ell_1$,

$$\left(\mathrm{M}_{n_k}(C), *, d_k \cdot (\operatorname{tr}_{C/R} \circ \operatorname{tr})\right) \hookrightarrow (\mathrm{M}_{2 d_k n_k}(R), \mathsf{t}, \operatorname{tr}), \qquad X \mapsto \psi_1(X)^{\oplus d_k}$$

for $\ell_1 < k \le \ell_2$, and

$$\left(\mathrm{M}_{n_k/2}(H), \mathsf{s}, d_k \cdot (\operatorname{tr}_H \circ \operatorname{tr})\right) \hookrightarrow (\mathrm{M}_{2 d_k n_k}(R), \mathsf{t}, \operatorname{tr}), \qquad X \mapsto \psi_2(X)^{\oplus d_k/2}$$

for $\ell_2 < k$, where ψ_1 and ψ_2 are applied entry-wise. By (4.6) we can combine these embeddings to obtain a trace preserving $*$-embedding

$$\begin{aligned} \mathcal{A} &\xrightarrow{\cong} \mathcal{A}_1 \times \cdots \times \mathcal{A}_\ell \\ &\xrightarrow{\cong} \prod_{k \le \ell_1} \mathrm{M}_{n_k}(R) \times \prod_{\ell_1 < k \le \ell_2} \mathrm{M}_{n_k}(C) \times \prod_{\ell_2 < k} \mathrm{M}_{n_k/2}(H) \\ &\hookrightarrow \prod_{k \le \ell_1} \mathrm{M}_{d_k n_k}(R) \times \prod_{\ell_1 < k \le \ell_2} \mathrm{M}_{2 d_k n_k}(R) \times \prod_{\ell_2 < k} \mathrm{M}_{2 d_k n_k}(R) \\ &\hookrightarrow (\mathrm{M}_n(R), \mathsf{t}, \operatorname{tr}). \end{aligned}$$

□

Lemma 4.7. *Let Λ be a Noetherian domain with $\operatorname{char}\Lambda \neq 2$, M a finitely generated Λ-module, K a field, $\phi:\Lambda\to K$ a ring homomorphism, and $b: M\times M\to\Lambda$ a symmetric Λ-bilinear form. Let $\pi: M\to K\otimes_\phi M$ be the natural homomorphism. Then there exist $u_1,\dots,u_\ell\in M$ such that $\{\pi(u_1),\dots,\pi(u_\ell)\}$ is a K-basis of $K\otimes_\phi M$ and $\phi(b(u_i,u_{i'}))=0$ for $i\neq i'$.*

Proof. Let $\ell=\dim_K(K\otimes_\phi M)$. We prove the statement by induction on ℓ. The case $\ell=1$ is trivial. Now assume that statement holds for $\ell-1$ and suppose $K\otimes_\phi M$ is of dimension ℓ.

If $\phi\circ b=0$, we are done. Otherwise there exists $u_1\in M\setminus\ker\pi$ with $b(u_1,u_1)\notin\ker\phi$. Indeed, if $\phi(b(u,u))=0$ for all $u\in M\setminus\ker\pi$, then $\phi(b(u,u))=0$ for all $u\in M$, so by

$$2b(u,v)=b(u+v,u+v)-b(u,u)-b(v,v)$$

it follows that $\phi(b(u,v))=0$ for every $u,v\in M$. Clearly there exist $v_2,\dots,v_\ell\in M$ such that $\{\pi(u_1),\pi(v_2)\dots,\pi(v_\ell)\}$ is a K-basis of $K\otimes_\phi M$. For $2\le i\le\ell$ let

$$v_i'=b(u_1,u_1)v_i-b(u_1,v_i)u_1$$

and let M' be the Λ-module generated by v_i'. Note that $b(u_1,v)=0$ for all $v\in M'$ and $\dim_K(K\otimes_\phi M')=\ell-1$ since $\phi(b(u_1,u_1))$ is invertible in K. Hence we can apply the induction hypothesis to obtain $u_2,\dots,u_\ell\in M'$ such that $\{\pi(u_1),\dots,\pi(u_\ell)\}$ is a K-basis of $K\otimes_\phi M$ and $\phi(b(u_i,u_{i'}))=0$ for all $i\neq i'$. □

Theorem 4.8. *Let $R\supseteq\mathbb{R}$ be a real closed field. Then an $\mathbb{R}$-algebra homomorphism $\phi:T_n\to R$ extends to an $\mathbb{R}$-algebra homomorphism $\varphi:\mathbb{R}[\boldsymbol{\xi}]\to R$ if and only if $\phi(\Omega_n)\subseteq R_{\ge0}$.*

Proof. The implication ($\Rightarrow$) is obvious, so we prove ($\Leftarrow$). In the terminology of [DPRR05, Subsection 2.3], $\mathbb{T}_n$ is an n–Cayley-Hamilton algebra. Since $\mathbb{T}_n$ is finitely spanned over T_n, $\mathcal{A}'=R\otimes_\phi\mathbb{T}_n$ is a finite-dimensional R-algebra which inherits an involution τ' and an R-trace $\chi':\mathcal{A}'\to R$ from $\mathbb{T}_n$. By [DPRR05, Subsection 2.3] $\mathcal{A}'$ is again an n–Cayley-Hamilton algebra. Let $\mathcal{J}$ be the Jacobson radical of $\mathcal{A}'$. Since $\mathcal{A}'$ is finite-dimensional, elements of $\mathcal{J}$ are characterized as generators of nilpotent ideals. Hence clearly $\mathcal{J}^{\tau'}\subseteq\mathcal{J}$. Moreover, if $f\in\mathcal{J}$, then $\chi'(f)=0$ by applying [DPRR05, Proposition 3.2] to the scalar extension of $\mathcal{A}'$ by the algebraic closure of R and [Lam91, Theorem 5.17].

Therefore $\mathcal{A}=\mathcal{A}'/\mathcal{J}$ is a finite-dimensional semisimple R-algebra with involution τ and an R-trace $\chi:\mathcal{A}\to R$. If $\Phi:\mathbb{T}_n\to\mathcal{A}$ is the canonical $*$-homomorphism, then

$$\chi\circ\Phi=\Phi\circ\operatorname{tr}. \tag{4.7}$$

We claim that $\tau(aa^\tau)\ge0$ for every $a\in\mathcal{A}$. Indeed, if $\pi:\mathbb{T}_n\to R\otimes_\phi\mathbb{T}_n$ is the canonical $*$-homomorphism, then by Lemma 4.7 there exist a finite set $\{u_i\}_i$ of symmetric elements in $\mathbb{T}_n$ and a finite set $\{v_j\}_j$ of antisymmetric elements in $\mathbb{T}_n$ such that $\{\pi(u_i)\}_i\cup\{\pi(v_j)\}_j$ form an R-basis of $R\otimes_\phi\mathbb{T}_n$ and

$$\phi(\operatorname{tr}(u_iu_{i'}))=\phi(\operatorname{tr}(v_jv_{j'}))=\phi(\operatorname{tr}(u_iv_j))=0$$

for all $i\neq i'$ and $j\neq j'$. If

$$a=\sum_i\alpha_i\Phi(u_i)+\sum_j\beta_j\Phi(v_j),\qquad \alpha_i,\beta_j\in R,$$

then

$$\chi(aa^\tau)=\sum_i\alpha_i^2\phi(\operatorname{tr}(u_iu_i^{\mathrm{t}}))+\sum_j\beta_j^2\phi(\operatorname{tr}(v_jv_j^{\mathrm{t}}))\ge0$$

by (4.7).

By Wedderburn's structure theorem we have

$$\mathcal{A}=\mathcal{A}_1\times\cdots\times\mathcal{A}_\ell$$

for some finite-dimensional simple R-algebras $\mathcal{A}_k$. Moreover, by [DPRR05, Theorem 4.2] there exist $d_1,\dots,d_\ell\in\mathbb{N}$ such that

$$\chi\left(\sum_k a_k\right)=\sum_k d_k \operatorname{tr}^R_{\mathcal{A}_k}(a_k) \tag{4.8}$$

for $a_k\in\mathcal{A}_k$.

Next we show that τ is split, i.e., $(\mathcal{A}_k)^\tau\subseteq\mathcal{A}_k$ for $1\le k\le\ell$. Since every involution preserves centrally primitive idempotents [Lam91, Section 22], for every k there exists k' such that $(\mathcal{A}_k)^\tau\subseteq\mathcal{A}_{k'}$. Suppose that τ is not split and without loss of generality assume $(\mathcal{A}_1)^\tau\subseteq\mathcal{A}_2$. Let $e_1\in\mathcal{A}_1$ and $e_2\in\mathcal{A}_2$ be the identity elements, respectively. Then

$$\begin{aligned}\chi\big((e_1-e_2)(e_1-e_2)^\tau\big)&=\chi\big((e_1-e_2)(e_2-e_1)\big)\\&=\chi(-e_1-e_2)\\&=-d_1\operatorname{tr}^R_{\mathcal{A}_1}(e_1)-d_2\operatorname{tr}^R_{\mathcal{A}_2}(e_2)<0,\end{aligned}$$

a contradiction.

Let τ_k be the restriction of τ on $\mathcal{A}_k$. By (4.8) and the previous paragraph it follows that $\operatorname{tr}^R_{\mathcal{A}_k}(aa^{\tau_k})\ge 0$ and hence $\operatorname{tr}_{\mathcal{A}_k}(aa^{\tau_k})\ge0$ for every $a\in\mathcal{A}_k$, so τ_k is a positive involution.

Therefore the assumptions of Proposition 4.6 are met and we obtain a trace preserving $*$-homomorphism $\Psi:\mathbb{T}_n\to\mathrm{M}_n(R)$ extending ϕ. Now we define $\varphi:\mathbb{R}[\boldsymbol{\xi}]\to R$ by

$$\varphi(\xi_{j\imath\jmath})=\Psi(\Xi_j)_{\imath\jmath}.$$ □

Remark 4.9. The condition $\phi(\Omega_n)\subseteq R_{\ge0}$ in Theorem 4.8 is clearly necessary since $\operatorname{tr}(hh^*)$ is a nonzero sum of squares in $\mathbb{R}[\boldsymbol{\xi}]$ for every nonzero $h\in\mathbb{T}_n$. Moreover, it is not vacuous. For example, let τ be the involution on $\mathbb{H}$ defined by $u^\tau=iu^{\mathsf{s}}i^{-1}$ for $u\in\mathbb{H}$, where s is the standard symplectic involution on $\mathbb{H}$. Then τ is of orthogonal type and we have a trace preserving $*$-epimorphism $\Phi:\mathbb{T}_2\to\mathbb{H}$ defined by $\Phi(\Xi_1)=i$ and $\Phi(\Xi_2)=j$. Since $\Phi(T_2)=\mathbb{R}$, the restriction yields a homomorphism $\phi:T_2\to\mathbb{R}$ and $\phi(\operatorname{tr}(\Xi_2\Xi_2^{\mathsf{t}}))=-1$.

Corollary 4.10. *Let $\phi:T_n=\mathbb{R}[\boldsymbol{\xi}]^{\mathrm{O}_n(\mathbb{R})}\to R$ be an $\mathbb{R}$-algebra homomorphism into a real closed field $R\supseteq\mathbb{R}$. Then the following are equivalent:*

- (i) *ϕ extends to an $\mathbb{R}$-algebra homomorphism $\varphi:\mathbb{R}[\boldsymbol{\xi}]\to R$;*
- (ii) *$\phi(\mathbb{R}[\boldsymbol{\xi}]^{\mathrm{O}_n(\mathbb{R})}\cap\sum\mathbb{R}[\boldsymbol{\xi}]^2)\subseteq R_{\ge0}$;*
- (iii) *$\phi(\operatorname{tr}(hh^{\mathsf{t}}))\in R_{\ge0}$ for all $h\in\mathbb{T}_n$.*

Remark 4.11. At first glance one might ponder whether Theorem 4.8 could be derived from the Procesi-Schwarz theorem [PS85]. In Appendix B we explain why this does not seem to be the case.

4.3. **Stellensätze.** We are now ready to give the main result of this section, the Krivine-Stengle Positivstellensatz for trace polynomials a that are positive (semidefinite) on K_S, see Theorem 4.13. In the proof we use Corollary 4.4 to reduce the problem to the commutative ring $T_n[a]$. Before applying the abstract Positivstellensatz for commutative rings, we need the relation between orderings and matrix evaluations of trace polynomials that is given in Proposition 4.12 below, which is a crucial consequence of the extension Theorem 4.8 and Tarski's transfer principle.

Proposition 4.12. *Let $S\subset T_n$ be finite, $a\in\operatorname{Sym}\mathbb{T}_n$ and P an ordering in $T_n[a]$ containing $S\cup\Omega_n$.*

1. *$a|_{K_S}\succeq0$ implies $a\in P$.*
2. *$a|_{K_S}\succ0$ implies $a\in P\setminus -P$.*

(3) $a|_{K_S} = 0$ *implies* $a \in P \cap -P$.

Proof. Let P be an ordering in $T_n[a]$ containing S and let $\sigma_j = \operatorname{tr}(\wedge^j a) \in T_n$ for $1 \leq j \leq n$.

(1) The restriction of P to T_n gives rise to a real closed field R and a homomorphism $\phi : T_n \to R$ satisfying $\phi(S \cup \Omega_n) \subseteq R_{\geq 0}$. By Theorem 4.8 we extend it to a homomorphism $\varphi : \mathbb{R}[\boldsymbol{\xi}] \to R$. Suppose that $\varphi(\sigma_j) < 0$ for some j; in other words, there exist $\alpha \in R^{gn^2}$ such that $\sigma_j(\alpha) < 0$ and $s'(\alpha) \geq 0$ for all $s' \in S$. By Tarski's transfer principle [Mar08, Theorem 1.4.2] there exists $\alpha' \in \mathbb{R}^{gn^2}$ such that $\sigma_j(\alpha') < 0$ and $s'(\alpha') \geq 0$ for all $s' \in S$. But this contradicts $\sigma_j|_{K_S} \geq 0$, which is a consequence of $s|_{K_S} \succeq 0$. Hence $\phi(\sigma_j) = \varphi(\sigma_j) \geq 0$ for all j, so $\sigma_j \in P$ for all j. By the Cayley-Hamilton theorem we have

$$(-a)^n + \sum_{j=1}^{n} \sigma_j (-a)^{n-j} = 0. \tag{4.9}$$

Suppose $a \notin P$. Then $-a \in P$, so (4.9) implies $(-a)^n \in P \cap -P$. Therefore $a \in P \cap -P$, a contradiction.

(2) Because $a|_{K_S} \succ 0$ implies $\sigma_j|_{K_S} > 0$, we obtain $\sigma_j \in P \setminus -P$ for all j by the same reasoning as in (1). If $a \notin P \setminus -P$, then $-a \in P$, so (4.9) implies $\sigma_n \in P \cap -P$, a contradiction.

(3) If $a|_{K_S} = 0$, then $a|_{K_S} \succeq 0$ and $-a|_{K_S} \succeq 0$, so $a \in P \cap -P$ by (1). □

Theorem 4.13 (Krivine-Stengle Positivstellensatz for trace polynomials)**.** *Let* $S \cup \{a\} \subset \operatorname{Sym} \mathbb{T}_n$ *be finite.*

(1) $a|_{K_S} \succeq 0$ *if and only if* $at_1 = t_1 a = a^{2k} + t_2$ *for some* $t_1, t_2 \in \mathfrak{T}_S^{\mathrm{tr}}$ *and* $k \in \mathbb{N}$.
(2) $a|_{K_S} \succ 0$ *if and only if* $at_1 = t_1 a = 1 + t_2$ *for some* $t_1, t_2 \in \mathfrak{T}_S^{\mathrm{tr}}$.
(3) $a|_{K_S} = 0$ *if and only if* $-a^{2k} \in \mathfrak{T}_S^{\mathrm{tr}}$ *for some* $k \in \mathbb{N}$.

Proof. The directions ($\Leftarrow$) are straightforward. For the implications ($\Rightarrow$), by Corollary 4.4 we can assume that $S \subset T_n$. Let T be the preordering in $T_n[a]$ generated by $S \cup \Omega_n$. Note that $T \subset \mathfrak{T}_S^{\mathrm{tr}}$ since $S \subset T_n$. If $a|_{K_S} \succeq 0$, then $a \in P$ for every ordering P of $T_n[a]$ containing T by Proposition 4.12. Therefore $t_1 a = a^{2k} + t_2$ for some $t_1, t_2 \in T$ and $k \in \mathbb{N}$ by the abstract Positivstellensatz [Mar08, Theorem 2.5.2], so (1) is holds. (2) and (3) are proved analogously. □

Remark 4.14. In general we cannot choose a central t_1 in Theorem 4.13; see Example 6.4.

Remark 4.15. A clean Krivine-Stengle Positivstellensatz for generic matrices clearly does not exist for $n = 3$ due to Theorem 3.2. Moreover, in Example 6.3 we show that even for $n = 2$, where Conjecture 3.1 holds, the traceless equivalent of Theorem 4.13 for GM_n fails.

Corollary 4.16. *If* $S \subset \operatorname{Sym} \mathbb{T}_n$ *is finite, then* $K_S = \emptyset$ *if and only if* $-1 \in \mathfrak{T}_S^{\mathrm{tr}}$.

Proof. If $K_S = \emptyset$, then $-1|_{K_S} \succ 0$, so by Theorem 4.13 there exist $t_1, t_2 \in \mathfrak{T}_S^{\mathrm{tr}}$ such that $(-1)t_1 = 1 + t_2$, so $-1 = t_1 + t_2 \in \mathfrak{T}_S^{\mathrm{tr}}$. The converse is trivial. □

Corollary 4.17. *Let* $s \in \operatorname{Sym} \mathbb{T}_n$. *Then* $s(A) \not\succeq 0$ *for all* $A \in \mathrm{M}_n(\mathbb{R})^g$ *if and only if*

$$-1 = \sum_i \omega_i \prod_j \operatorname{tr}(h_{ij} s h_{ij}^{\mathrm{t}})$$

for some $\omega_i \in \Omega_n$ *and* $h_{ij} \in \mathbb{T}_n$.

Proof. Follows by Corollary 4.16 and Lemma 4.1. □

Corollary 4.18 (Real Nullstellensatz for trace polynomials)**.** *Let* $\mathcal{J} \subset \mathbb{T}_n$ *be an ideal and assume* $\operatorname{tr}(\mathcal{J}) \subseteq \mathcal{J}$. *For* $h \in \mathbb{T}_n$ *the following are equivalent:*

(i) *for every* $X \in \mathrm{M}_n(\mathbb{R})^g$, $u(X) = 0$ *for every* $u \in \mathcal{J}$ *implies* $h(X) = 0$;
(ii) *there exists* $k \in \mathbb{N}$ *such that* $-(h^{\mathrm{t}} h)^k \in \mathfrak{N}_n + \mathcal{J}$.

Proof. The implication (2) $\Rightarrow$ (1) is clear. Conversely, $\mathbb{T}_n$ is Noetherian, so $\mathcal{J}$ is (as a left ideal) generated by some $u_1,\dots,u_\ell \in \mathbb{T}_n$. Let $S = \{-u_1^t u_1,\dots,-u_\ell^t u_\ell\}$; then (1) is equivalent to $h^t h|_{K_S} = 0$. Hence (1) $\Rightarrow$ (2) follows by Theorem 4.13(3) and $\mathfrak{T}_S^{tr} \subseteq \mathfrak{N}_n + \mathcal{J}$. □

Corollary 4.19. *Let $S \subset \mathbb{T}_n$. Then*

$$\{A \in \mathrm{M}_n(\mathbb{R})^g : s(A) = 0 \ \forall s \in S\} = \emptyset$$

if and only if

$$-1 = \omega + \sum_i \mathrm{tr}(h_i s_i)$$

for some $\omega \in \Omega_n$, $h_i \in \mathbb{T}_n$ and $s_i \in S$.

We mention that Hilbert's Nullstellensatz for $n \times n$ generic matrices over an algebraically closed field is given by Amitsur in [Ami57, Theorem 1].

5. Positivstellensätze for compact semialgebraic sets

In this section we give certificates for positivity on compact semialgebraic sets. We prove a version of Schmüdgen's theorem [Scm91] for trace polynomials (Theorem 5.3). We also present a version of Putinar's theorem [Put93] for trace polynomials (Theorem 5.7) and for generic matrices (Theorem 5.5).

5.1. Archimedean (cyclic) quadratic modules.

A cyclic quadratic module $\mathfrak{Q} \subset \mathbb{T}_n$ is **archimedean** if for every $h \in \mathbb{T}_n$ there exists $\rho \in \mathbb{Q}_{>0}$ such that $\rho - hh^t \in \mathfrak{Q}$. Equivalently, for every $s \in \mathrm{Sym}\,\mathbb{T}_n$ there exists $\varepsilon \in \mathbb{Q}_{>0}$ such that $1 \pm \varepsilon s \in \mathfrak{Q}$.

For a cyclic quadratic module $\mathfrak{Q}$ let $H_{\mathfrak{Q}}$ be the set of elements $h \in \mathbb{T}_n$ such that $\rho - hh^t \in \mathfrak{Q}$ for some $\rho \in \mathbb{Q}_{>0}$. It is clear that $\mathfrak{Q}$ is archimedean if and only if $H_{\mathfrak{Q}} = \mathbb{T}_n$.

Proposition 5.1. *$H_{\mathfrak{Q}}$ is a trace $*$-subalgebra over $\mathbb{R}$ in $\mathbb{T}_n$.*

Proof. $H_{\mathfrak{Q}}$ is a $*$-subalgebra over $\mathbb{R}$ by [Vid59]. Let $h \in H_{\mathfrak{Q}}$. Then $s = h + h^t \in H_{\mathfrak{Q}}$ and let $\rho \in \mathbb{Q}_{>0}$ be such that $\rho^2 - s^2 \in \mathfrak{Q}$. Then

$$\rho \pm s = \frac{1}{2\rho}\left((\rho \pm s)^2 + (\rho^2 - s^2)\right) \in \mathfrak{Q}$$

and consequently $n\rho \pm \mathrm{tr}(s) \in \mathfrak{Q}$. Therefore

$$(n\rho)^2 - \mathrm{tr}(s)^2 = \frac{1}{2n\rho}\big((\rho - s)(\rho + s)(\rho - s) + (\rho + s)(\rho - s)(\rho + s)\big) \in \mathfrak{Q},$$

so $\mathrm{tr}(h) = \frac{1}{2}\mathrm{tr}(s) \in H_{\mathfrak{Q}}$. □

Corollary 5.2. *A cyclic quadratic module $\mathfrak{Q}$ is archimedean if and only if there exists $\rho \in \mathbb{Q}_{>0}$ such that $\rho - \sum_j \Xi_j \Xi_j^t \in \mathfrak{Q}$.*

Proof. ($\Rightarrow$) is trivial. Conversely, $\rho - \sum_j \Xi_j \Xi_j^t \in \mathfrak{Q}$ implies $\Xi_j \in H_{\mathfrak{Q}}$ for $1 \le j \le n$, so $H_{\mathfrak{Q}} = \mathbb{T}_n$ since $\mathbb{T}_n$ is generated by Ξ_j as a trace $*$-subalgebra over $\mathbb{R}$ by Proposition 5.1. □

It is easy to see that $K_{\mathfrak{Q}}$ is compact if $\mathfrak{Q}$ is archimedean. The converse fails already with $n = 1$ ([Mar08, Section 7.3] or [PD01, Example 6.3.1]). If $K_{\mathfrak{Q}}$ is compact, say $\|X\| \le N$ for all $X \in K_{\mathfrak{Q}}$, then we can add $N^2 - \sum_j \Xi_j \Xi_j^t$ to $\mathfrak{Q}$ to make it archimedean without changing $K_{\mathfrak{Q}}$.

5.2. **Schmüdgen's Positivstellensatz for trace polynomials.** In this subsection we prove a version of Schmüdgen's Positivstellensatz for trace polynomials a that are positive on a compact semialgebraic set K_S. The proof is a two-step commutative reduction. Firstly, the constraints S are replaced with central ones by Corollary 4.4. Then the abstract version of Schmüdgen's Positivstellensatz is used in the commutative ring $T_n[a]$.

Theorem 5.3 (Schmüdgen's Positivstellensatz for trace polynomials)**.** *Let $S \cup \{a\} \subset \operatorname{Sym} \mathbb{T}_n$ be finite. If K_S is compact and $a|_{K_S} \succ 0$, then $a \in \mathfrak{T}_S^{\mathrm{tr}}$.*

Proof. First we apply Corollary 4.4 to reduce to the case $S \subset T_n$. Let T be the preordering in $T_n[a]$ generated by $S \cup \Omega_n$. Note that $K_S = K_T$ and $T \subset \mathfrak{T}_S^{\mathrm{tr}}$.

Let $b \in T_n[a]$ be arbitrary. Since K_S is compact, there exists $\beta \in \mathbb{R}_{\geq 0}$ such that $\beta \pm b|_{K_S} \succeq 0$. Then $\beta \pm b \in P$ for every ordering P in $T_n[a]$ containing $T \supset S \cup \Omega_n$ by Proposition 4.12. In the terminology of [Sce03], T is weakly archimedean. Since $T_n[a]$ is a finitely generated $\mathbb{R}$-algebra, T is an archimedean preordering in $T_n[a]$ by the abstract version of Schmüdgen's Positivstellensatz [Sce03, Theorem 3.6]. Similarly, Proposition 4.12 implies $a \in P \setminus -P$ for every ordering P in $T_n[a]$ containing $T \supset S \cup \Omega_n$, so $a \in T$ by [Sce03, Proposition 3.3] or [Mon98, Theorem 4.3]. $\square$

Corollary 5.4. *Let $S \subset \operatorname{Sym} \mathbb{T}_n$ be finite. Then $\mathfrak{T}_S^{\mathrm{tr}}$ is archimedean if and only if K_S is compact.*

5.3. **Putinar's Positivstellensatz for generic matrices.** Our next theorem is a Putinar-type Positivstellensatz for generic matrices on compact semialgebraic sets, which requires a functional analytic proof. While the proof generally follows a standard outline (using a separation argument followed by a Gelfand-Naimark-Segal construction), several modifications are needed. For instance, the separation is taken to be extreme in a convex sense, and polynomial identities techniques are applied to produce $n \times n$ matrices.

A set $\mathfrak{Q} \subseteq \operatorname{Sym} \mathrm{GM}_n$ is a **quadratic module** if

$$1 \in \mathfrak{Q}, \quad \mathfrak{Q} + \mathfrak{Q} \subseteq \mathfrak{Q}, \qquad h\mathfrak{Q}h^{\mathrm{t}} \subseteq \mathfrak{Q} \ \ \forall h \in \mathrm{GM}_n .$$

We say that $\mathfrak{Q}$ is **archimedean** if for every $h \in \mathrm{GM}_n$ there exists $\rho \in \mathbb{Q}_{>0}$ such that $\rho - aa^{\mathrm{t}} \in \mathfrak{Q}$. As in Corollary 5.2 we see that a quadratic module is archimedean if and only if it contains $\rho - \sum_j \Xi_j \Xi_j^{\mathrm{t}}$ for some $\rho \in \mathbb{Q}_{>0}$.

Theorem 5.5 (Putinar's Positivstellensatz for generic matrices)**.** *Let $\mathfrak{Q} \subset \operatorname{Sym} \mathrm{GM}_n$ be an archimedean quadratic module and $a \in \operatorname{Sym} \mathrm{GM}_n$. If $a|_{K_{\mathfrak{Q}}} \succ 0$, then $a \in \mathfrak{Q}$.*

Proof. Assume $a \in \operatorname{Sym} \mathrm{GM}_n \setminus \mathfrak{Q}$. We proceed in several steps.

Step 1: Separation.
Consider $\mathfrak{Q}$ as a convex cone in the vector space $\operatorname{Sym} \mathrm{GM}_n$ over $\mathbb{R}$. Since $\mathfrak{Q}$ is archimedean, for every $s \in \operatorname{Sym} \mathbb{T}_n$ there exists $\varepsilon \in \mathbb{Q}_{>0}$ such that $1 \pm \varepsilon s \in \mathfrak{Q}$, which in terms of [Bar02, Definition III.1.6] means that 1 is an algebraic interior point of the cone $\mathfrak{Q}$ in $\operatorname{Sym} \mathbb{T}_n$. By the Eidelheit-Kakutani separation theorem [Bar02, Corollary III.1.7] there exists a nonzero $\mathbb{R}$-linear functional $L_0 : \operatorname{Sym} \mathrm{GM}_n \to \mathbb{R}$ satisfying $L_0(\mathfrak{Q}) \subseteq \mathbb{R}_{\geq 0}$ and $L_0(a) \leq 0$. Moreover, $L_0(1) > 0$ because $\mathfrak{Q}$ is archimedean, so after rescaling we can assume $L_0(1) = 1$. Let $L : \mathrm{GM}_n \to \mathbb{R}$ be the symmetric extension of L_0, i.e., $L(f) = \frac{1}{2} L_0(f + f^{\mathrm{t}})$ for $f \in \mathrm{GM}_n$.

Step 2: Extreme separation.
Now consider the set $\mathcal{C}$ of all linear functionals $L' : \mathrm{GM}_n \to \mathbb{R}$ satisfying $L'(\mathfrak{Q}) \subseteq \mathbb{R}_{\geq 0}$ and $L'(1) = 1$. This set is nonempty because $L \in \mathcal{C}$. Endow GM_n with the norm

$$\|p\| = \max \{ \|p(X)\|_2 \colon X \in \mathrm{M}_n(\mathbb{R})^g, \|X\|_2 \leq 1 \} .$$

By the Banach-Alaoglu theorem [Bar02, Theorem III.2.9], the convex set $\mathcal{C}$ is weak*-compact. Thus by the Krein-Milman theorem [Bar02, Theorem III.4.1] we may assume that our separating functional L is an extreme point of $\mathcal{C}$.

Step 3: GNS construction.
On GM_n we define a semi-scalar product $\langle p, q\rangle = L(q^{\mathrm{t}}p)$. By the Cauchy-Schwarz inequality for semi-scalar products,

$$\mathcal{N} = \left\{q \in \mathrm{GM}_n \mid L(q^{\mathrm{t}}q) = 0\right\}$$

is a linear subspace of GM_n. Hence

$$\langle \overline{p}, \overline{q}\rangle = L(q^{\mathrm{t}}p) \tag{5.1}$$

is a scalar product on $\mathrm{GM}_n/\mathcal{N}$, where $\overline{p} = p + \mathcal{N}$ denotes the residue class of $p \in \mathrm{GM}_n$ in $\mathrm{GM}_n/\mathcal{N}$. Let H denote the completion of $\mathrm{GM}_n/\mathcal{N}$ with respect to this scalar product. Since $1 \notin \mathcal{N}$, H is non-trivial.

Next we show that $\mathcal{N}$ is a left ideal of GM_n. Let $p, q \in \mathrm{GM}_n$. Since $\mathfrak{Q}$ is archimedean, there exists $\varepsilon > 0$ such that $1 - \varepsilon p^{\mathrm{t}}p \in \mathfrak{Q}$ and therefore

$$0 \le L(q^{\mathrm{t}}(1 - \varepsilon p^{\mathrm{t}}p)q) \le L(q^{\mathrm{t}}q). \tag{5.2}$$

Hence $q \in \mathcal{N}$ implies $pq \in \mathcal{N}$.

Because $\mathcal{N}$ is a left ideal, we can define linear maps

$$M_p : \mathrm{GM}_n/\mathcal{N} \to \mathrm{GM}_n/\mathcal{N}, \qquad \overline{q} \mapsto \overline{pq}$$

for $p \in \mathrm{GM}_n$. By (5.2), M_p is bounded and thus extends to a bounded operator $\hat{M}_p$ on H.

Step 4: Irreducible representation of GM_n.
The map

$$\pi : \mathrm{GM}_n \to \mathcal{B}(H), \qquad p \mapsto \hat{M}_p$$

is clearly a $*$-representation, where $\mathcal{B}(H)$ is endowed with the adjoint involution $*$. Observe that $\eta = \overline{1} \in H$ is a cyclic vector for π by construction and

$$L(p) = \langle \pi(p)\eta, \eta\rangle. \tag{5.3}$$

Write $\mathcal{A} = \pi(\mathrm{GM}_n)$. We claim that the self-adjoint elements in the commutant $\mathcal{A}'$ of $\mathcal{A}$ in $\mathcal{B}(H)$ are precisely real scalar operators. Let $P \in \mathcal{A}'$ be self-adjoint. By the spectral theorem, P decomposes into real scalar multiples of projections belonging to $\{P\}'' \subseteq \mathcal{A}'$. So it suffices to assume that P is a projection. By way of contradiction suppose that $P \notin \{0, 1\}$; since η is cyclic for π, we have $P\eta \neq 0$ and $(1 - P)\eta \neq 0$. Hence we can define linear functionals L_j on GM_n by

$$L_1(p) = \frac{\langle \pi(p)P\eta, P\eta\rangle}{\|P\eta\|^2} \qquad \text{and} \qquad L_2(p) = \frac{\langle \pi(p)(1 - P)\eta, (1 - P)\eta\rangle}{\|(1 - P)\eta\|^2}$$

for all $p \in \mathrm{GM}_n$. One checks that L is a convex combination of L_1 and L_2. Since also $L_j \in \mathcal{C}$, we obtain $L = L_1 = L_2$ by the extreme property of L. Let $\lambda = \|P\eta\|^2$; then (5.3) implies

$$\langle \pi(p)\eta, \lambda\eta\rangle = \lambda\langle \pi(p)\eta, \eta\rangle = \langle \pi(p)P\eta, P\eta\rangle = \langle P\pi(p)\eta, P\eta\rangle = \langle \pi(p)\eta, P\eta\rangle$$

for all $p \in \mathrm{GM}_n$. Therefore $P\eta = \lambda\eta$ since η is a cyclic vector for π. Then $\lambda \in \{0, 1\}$ since P is a projection, a contradiction.

Next we show that π is an irreducible representation. Suppose that $U \subseteq H$ is a closed π-invariant subspace and $P : H \to U$ the orthogonal projection. If $p \in \mathrm{GM}_n$ and $p^{\mathrm{t}} = \pm p$, then

$$\pi(p)P = P\pi(p)P = \pm(P\pi(p)P)^* = \pm(\pi(p)P)^* = P\pi(P).$$

Consequently $P \in \mathcal{A}'$ and hence $P \in \mathbb{R}$. Since P is an orthogonal projection, we have $P \in \{0, 1\}$, so π is irreducible.

Step 5: Transition to $n \times n$ matrices.
We claim that $\mathcal{A}$ is a prime algebra. Indeed, suppose $a\mathcal{A}b = 0$ for $a, b \in \mathcal{A}$. If $b \neq 0$, then there is a $u \in H$ with $bu \neq 0$. Since π is irreducible, the vector space $V = \mathcal{A}bu$ is dense in H. Now $aV = 0$ implies $aH = 0$, i.e., $a = 0$.

Since the $*$-center of $\mathcal{A}$ equals $\mathbb{R}$, we have $\pi(C_n) = \mathbb{R}$, so $\mathcal{A}$ is generated by $\pi(\Xi_j)$ for $1 \leq j \leq g$ as an $\mathbb{R}$-algebra with involution. Let $f \in \mathbb{R}\langle \boldsymbol{x}, \boldsymbol{x}^* \rangle$ be a polynomial $*$-identity of $(\mathrm{M}_n(\mathbb{R}), \mathsf{t})$. Then $f(p_1, \dots, p_k, p_1^{\mathsf{t}}, \dots, p_k^{\mathsf{t}}) = 0$ for all $p_i \in \mathrm{GM}_n$. Therefore

$$f(\pi(p_1), \dots, \pi(p_k), \pi(p_1)^*, \dots, \pi(p_k)^*) = \pi(f(p_1, \dots, p_k, p_1^{\mathsf{t}}, \dots, p_k^{\mathsf{t}})) = 0,$$

so f is a polynomial $*$-identity for $\mathcal{A}$. By the $*$-version of Posner's theorem [Row73, Theorem 2] it follows that $\mathcal{A}$ is central simple algebra of degree $n' \leq n$ with involution $*$ and with $*$-center $\mathbb{R}$. Furthermore, the involution on $\mathcal{A}$ is positive since it is a restriction of the adjoint involution on $\mathcal{B}(H)$. By [PS76, Theorem 1.2], $\mathcal{A}$ is $*$-isomorphic to one of

$$(\mathrm{M}_{n'}(\mathbb{R}), \mathsf{t}), \qquad (\mathrm{M}_{n'}(\mathbb{C}), *), \qquad (\mathrm{M}_{n'/2}(\mathbb{H}), \mathsf{s}).$$

Since $\mathcal{A} = \Phi(\mathrm{GM}_n)$, $\mathcal{A}$ satisfies all polynomial $*$-identities of $(\mathrm{M}_n(\mathbb{R}), \mathsf{t})$. If $(\mathcal{A}, *) \cong (\mathrm{M}_{n'/2}(\mathbb{H}), \mathsf{s})$, then Proposition 2.3 implies $\frac{n'}{2} \leq 2n$. Similarly, $(\mathcal{A}, *) \cong (\mathrm{M}_{n'}(\mathbb{C}), *)$ implies $2n' \leq n$ by Remark 2.4. Hence in all cases there exists a $*$-embedding of $(\mathcal{A}, *)$ into $(\mathrm{M}_n(\mathbb{R}), \mathsf{t})$, so we can assume that $X_j := \hat{M}_{\Xi_j} \in \mathrm{M}_n(\mathbb{R})$, $* = \mathsf{t}$ and $\eta \in \mathbb{R}^d$. Since $L(\mathfrak{Q}) \subseteq \mathbb{R}_{\geq 0}$, (5.3) implies that $q(X)$ is positive semidefinite for all $q \in \mathfrak{Q}$, so $X \in K_{\mathfrak{Q}}$.

Step 6: Conclusion.
By (5.1) we have

$$0 \geq L(a) = \langle \overline{a}, \overline{1} \rangle = \langle a(X, X^{\mathsf{t}})\eta, \eta \rangle.$$

Therefore a is not positive definite at $X \in K_{\mathfrak{Q}}$. □

5.4. **Putinar's theorem for trace polynomials.** Our final result in this section is Putinar's Positivstellensatz for trace polynomials, Theorem 5.7. Our proof combines functional analytic techniques from the proof of Theorem 5.5 with an algebraic commutative reduction.

Lemma 5.6. *Let $\mathfrak{Q} \subset \mathrm{Sym}\, \mathbb{T}_n$ be an archimedean cyclic quadratic module and $c \in T_n$. If $c|_{K_{\mathfrak{Q}}} > 0$, then $c \in \mathfrak{Q}$.*

Proof. Assume $c \in \mathrm{Sym}\, \mathbb{T}_n \setminus \mathfrak{Q}$. Steps 1–4 in the proof of Theorem 5.5 work if we replace GM_n with $\mathbb{T}_n$. Hence we obtain a Hilbert space H, a $*$-representation $\pi : \mathbb{T}_n \to \mathcal{B}(H)$ with $\pi(T_n) = \mathbb{R}$, and a cyclic unit vector $\eta \in H$ for π such that the linear functional

$$L : \mathbb{T}_n \to \mathbb{R}, \qquad p \mapsto \langle \pi(p)\eta, \eta \rangle$$

satisfies $L(\mathfrak{Q}) \subseteq \mathbb{R}_{\geq 0}$ and $L(c) \leq 0$. Let $\phi = \pi|_{T_n} : T_n \to \mathbb{R}$. By the proof of Theorem 4.8, ϕ extends to a trace preserving $*$-homomorphism $\Psi : \mathbb{T}_n \to \mathrm{M}_n(\mathbb{R})$. Let $X_j = \Psi(\Xi_j) \in \mathrm{M}_n(\mathbb{R})$ for $j = 1, \dots, g$. Because $\pi(T_n) = \mathbb{R}$, we have $L|_{T_n} = \pi|_{T_n}$ and therefore $\mathrm{tr}(q(X)) = \phi(\mathrm{tr}(q)) \geq 0$ for every $q \in \mathfrak{Q}$, so $X \in K_{\mathfrak{Q}}$ by Corollary 4.5 and $c(X) = \phi(c) \leq 0$. □

Theorem 5.7 (Putinar's theorem for trace polynomials)**.** *Let $\mathfrak{Q} \subset \mathrm{Sym}\, \mathbb{T}_n$ be an archimedean cyclic quadratic module and $a \in \mathrm{Sym}\, \mathbb{T}_n$. If $a|_{K_{\mathfrak{Q}}} \succ 0$, then $a \in \mathfrak{Q}$.*

Proof. Let $\sigma_j = \mathrm{tr}(\wedge^j a)$ and assume $a|_{K_{\mathfrak{Q}}} \succ 0$. Since $K_{\mathfrak{Q}}$ is compact, there exists $\varepsilon > 0$ such that $(\sigma_j - \varepsilon)|_{K_{\mathfrak{Q}}} > 0$ for all $1 \leq j \leq n$. By Lemma 5.6 we have $\sigma_j - \varepsilon \in \mathfrak{Q}$ for all j. Let $c_1, \dots, c_N$ be the generators of T_n as an $\mathbb{R}$-algebra. Since $\mathfrak{Q}$ is archimedean, there exist $\rho_1, \dots, \rho_N \in \mathbb{Q}_{>0}$ such that $\rho_i - c_i^2 \in \mathfrak{Q}$. Write

$$S = \left\{ \sigma_j - \varepsilon, \rho_i - c_i^2 : 1 \leq j \leq n, 1 \leq i \leq N \right\}$$

and let Q be the quadratic module in $T_n[a]$ generated by $S \cup \Omega_n$. Clearly we have $Q \subset \mathfrak{Q}$ and $a|_{K_Q} > 0$. Let $H_Q \subseteq T_n[a]$ be the subring of bounded elements with respect to Q, i.e., $b \in T_n[a]$ such that $\rho - b^2 \in Q$ for some $\rho \in \mathbb{Q}_{>0}$. Because c_i generate T_n, we have $T_n \subseteq H_Q$. Since H_Q is integrally closed in $T_n[a]$ by [Bru79, Section 6.3] or [Scw03, Theorem 5.3], we also have $a \in H_Q$. Hence Q is archimedean. If P is an ordering in $T_n[a]$ containing $S \cup \Omega_n$, then $a \in P \setminus -P$ by

Proposition 4.12. Therefore $a \in Q \subset \mathfrak{Q}$ by Jacobi's representation theorem [Mar08, Theorem 5.4.4]. □

6. Examples

In this section we collect some examples and counterexamples pertaining to the results presented above.

Example 6.1. Proposition 4.3 states that for every $s \in \operatorname{Sym} \mathbb{T}_n$ there exists a finite set $S \subset \operatorname{tr}(\mathfrak{Q}^{\mathrm{tr}}_{\{s\}})$ such that $K_{\{s\}} = K_S$. Let us give a concrete example of such a set for $n = 3$. Let $\sigma_j = \operatorname{tr}(\wedge^j s)$; using the Cayley-Hamilton theorem and the relations between σ_j and $\operatorname{tr}(s^i)$ it is easy to check that

$$
\begin{aligned}
\operatorname{tr}(s) &= \sigma_1, \\
\operatorname{tr}\left((s-\sigma_1)s(s-\sigma_1)\right) &= \sigma_1\sigma_2 + 3\sigma_3, \\
\operatorname{tr}\left((s^2-\sigma_1 s+\sigma_2)s(s^2-\sigma_1 s+\sigma_2)\right) &= \sigma_2\sigma_3, \\
\operatorname{tr}\left((s-\sigma_1-1)s(s-\sigma_1-1)\right) &= \sigma_1 + 4\sigma_2 + 3\sigma_3 + \sigma_1\sigma_2.
\end{aligned}
$$

Denote these elements by $c_1, c_2, c_3, c_4 \in \operatorname{tr}(\mathfrak{Q}^{\mathrm{tr}}_{\{s\}})$. We claim that $K_{\{s\}} = K_{\{c_1,c_2,c_3,c_4\}}$. It suffices to prove the inclusion $\supseteq$.

To simplify the notation let $s = s^{\mathrm{t}} \in \mathrm{M}_3(\mathbb{R})$. If $s \not\succeq 0$, then $\sigma_j < 0$ for some j. If $\sigma_1 < 0$, then $c_1 < 0$. Hence assume $\sigma_1 \geq 0$. If σ_2, σ_3 are of opposite sign, then $c_3 < 0$. If $\sigma_1 > 0$ and $\sigma_2, \sigma_3 \leq 0$, then $c_2 < 0$. Finally, if $\sigma_1 = 0$ and one of σ_2, σ_3 equals 0, then $\sigma_3 < 0$ implies $c_2 < 0$ and $\sigma_2 < 0$ implies $c_4 < 0$.

Example 6.2. The denominator in Lemma 2.5 is unavoidable even if f is a hermitian square or $f \in \mathbb{R}[\boldsymbol{\xi}]$. For example, let $n = 4$ and $a = \Xi_1 - \Xi_1^{\mathrm{t}}$. Then $\det(a)$ is a square in $\mathbb{R}[\boldsymbol{\xi}]$. Suppose $\det(a) \in \Omega_4$, i.e.,

$$
\det(a) = \sum_i \operatorname{tr}(h_{i1}h_{i1}^{\mathrm{t}}) \cdots \operatorname{tr}(h_{im_i}h_{im_i}^{\mathrm{t}})
$$

for some $h_{ij} \in \mathbb{T}_n$. Because a is independent of $\Xi_1 + \Xi_1^{\mathrm{t}}$ and Ξ_j for $j > 1$, we can assume that h_{ij} are polynomials in a and $\operatorname{tr}(a^k)$ for $k \in \mathbb{N}$. Moreover, $\det(a)$ is homogeneous of degree 4 with respect to the entries of a, so h_{ij} are of degree at most 2 with respect to a. Finally, $\operatorname{tr}(a) = 0$, so we conclude that

$$
\det(a) = \sum_i \operatorname{tr}\left((\alpha_i a^2 + \beta_i \operatorname{tr}(a^2))^2\right), \qquad \alpha_i, \beta_i \in \mathbb{R}.
$$

If R is a real closed field containing $\mathbb{R}(\boldsymbol{\xi})$, then there exist $\lambda, \mu \in R$ that are algebraically independent over $\mathbb{R}$ such that

$$
a = \begin{pmatrix} 0 & -\lambda & 0 & 0 \\ \lambda & 0 & 0 & 0 \\ 0 & 0 & 0 & -\mu \\ 0 & 0 & \mu & 0 \end{pmatrix}
$$

after an orthogonal basis change. Therefore

$$
(\lambda\mu)^2 = 2\sum_i \left((\alpha_i\lambda^2 + 2\beta_i(\lambda^2+\mu^2))^2 + (\alpha_i\mu^2 + 2\beta_i(\lambda^2+\mu^2))^2\right),
$$

which is clearly a contradiction.

Example 6.3. Next we show that a traceless equivalent of Theorem 4.13 fails for GM_2. A quadratic module $\mathfrak{T} \subseteq \operatorname{Sym}\mathrm{GM}_n$ is a **preordering** if $\mathfrak{T} \cap C_n$ is closed under multiplication. For $S \subset \operatorname{Sym}\mathrm{GM}_n$ let $\mathfrak{Q}_S$ and $\mathfrak{T}_S$ denote the quadratic module and preordering, respectively, generated by S. For example, $\mathfrak{T}_\emptyset = \mathfrak{Q}_\emptyset$ is the set of sums of hermitian squares in GM_n.

Fix $n = 2$ and let

$$s = \Xi_1 + \Xi_1^{\mathrm{t}}, \qquad a = \Xi_1 - \Xi_1^{\mathrm{t}}, \qquad f = [s^2, a][s, a].$$

Since $f = \operatorname{tr}(s)[s,a]^2$, it is clear that $f|_{K_{\{s\}}} \succeq 0$. We will show that there do not exist $t_1, t_2 \in \mathfrak{T}_S$ and $k \in \mathbb{N}$ such that

$$ft_1 = t_1 f = f^{2k} + t_2. \tag{6.1}$$

It clearly suffices to assume $g = 1$. If R is a real closed field containing $\mathbb{R}(\boldsymbol{\xi})$, then after diagonalizing s we may assume that

$$s = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \qquad a = \begin{pmatrix} 0 & -\mu \\ \mu & 0 \end{pmatrix}$$

for some $\lambda_1, \lambda_2, \mu \in R$ that are algebraically independent over $\mathbb{R}$. Let $h \in \mathrm{GM}_2$ be homogeneous of degree (d, e) with respect to (s, a). Then it is not hard to check that

$$hsh^{\mathrm{t}} = \mu^{2e} \begin{pmatrix} \lambda_1 \tilde{h}(\lambda_1, \lambda_2)^2 & 0 \\ 0 & \lambda_2 \tilde{h}(\lambda_2, \lambda_1)^2 \end{pmatrix} \tag{6.2}$$

for some homogeneous polynomial $\tilde{h} \in \mathbb{R}[y_1, y_2]$ of degree d. Therefore

$$\sum_i h_i s h_i^{\mathrm{t}} \in C_2 \quad \Rightarrow \quad h_i = 0 \ \forall i,$$

so we deduce that

$$\mathfrak{T}_{\{s\}} = (\mathfrak{T}_\emptyset \cap C_2) \cdot \mathfrak{Q}_{\{s\}}. \tag{6.3}$$

Now suppose that (6.1) holds for some $t_1, t_2 \in \mathfrak{T}_S$ and $k \in \mathbb{N}$. Since f is homogeneous of degree $(5, 2)$ with respect to (s, a), t_1, t_2 can be taken homogeneous as well. Then t_2 is of degree $(10k, 4k)$ and t_1 is of degree $(10k - 5, 4k - 2)$. In particular, the total degrees of t_1 and t_2 are odd and even, respectively, so by (6.3) we conclude that $t_2 \in \mathfrak{T}_\emptyset$ and t_1 is of the form $\sum_i h_i s h_i^{\mathrm{t}}$ for $h_i \in \mathrm{GM}_2$. Hence (6.2) implies

$$t_1 = \mu^{4k-2} \begin{pmatrix} \lambda_1 \sum_i \tilde{h}_i(\lambda_1, \lambda_2)^2 & 0 \\ 0 & \lambda_2 \sum_i \tilde{h}_i(\lambda_2, \lambda_1)^2 \end{pmatrix}$$

for some homogeneous $\tilde{h}_i \in \mathbb{R}[y_1, y_2]$. Now

$$f = (\lambda_1 + \lambda_2)(\lambda_1 - \lambda_2)^2 \mu^2$$

implies

$$ft_1 = (\lambda_1 + \lambda_2)\mu^{4k}(\lambda_1 - \lambda_2)^2 \begin{pmatrix} \lambda_1 \sum_i \tilde{h}_i(\lambda_1, \lambda_2)^2 & 0 \\ 0 & \lambda_2 \sum_i \tilde{h}_i(\lambda_2, \lambda_1)^2 \end{pmatrix}. \tag{6.4}$$

The nonempty set

$$\{X \in \mathrm{M}_2(\mathbb{R}) \colon \det(s(X)) < 0 \text{ and } \operatorname{tr}(s(X)) > 0\}$$

is open in the Euclidean topology, so by (6.4) there exists $X \in \mathrm{M}_2(\mathbb{R})$ such that $(st_1)(X)$ is nonzero and indefinite. However, this contradicts $ft_1 = f^{2k} + t_2 \in \mathfrak{T}_\emptyset$.

Example 6.4. Here we show that the element t_1 in Theorem 4.13 cannot be chosen central in general. Let $n=2$, $s=\frac{1}{2}(\Xi_1+\Xi_1^{\mathrm{t}})$ and $S=\{\mathrm{tr}(s)^3,\det(s)^3\}$. Suppose $t_1 s = s^{2k}+t_2$ for some $k\in\mathbb{N}$ and $t_1,t_2\in\mathfrak{T}_S^{\mathrm{tr}}$ and $t_1\in T_2$. Let

$$\Psi:\mathbb{T}\to \mathrm{M}_2(\mathbb{R}[\zeta]),\qquad \Xi_1\mapsto \begin{pmatrix}\zeta & 0\\ 0 & 1\end{pmatrix}.$$

Since $(\zeta+1)^3=\zeta^3+(\frac{3}{2}\zeta+1)^2+\frac{3}{4}\zeta^2$, we conclude that $\Psi(t_1)$ belongs to the commutative preordering generated by ζ^3 and $\Psi(t_2)$ belongs to the matricial preordering generated by ζ^3 in $\mathrm{M}_2(\mathbb{R}[\zeta])$. But then $\Psi(t_1)\Psi(s)=\Psi(s)^{2k}+\Psi(t_2)$ contradicts [Cim12, Example 4].

Example 6.5. Let $f=5\,\mathrm{Tr}(\Xi_1\Xi_1^{\mathrm{t}})-2\,\mathrm{Tr}(\Xi_1)(\Xi_1+\Xi_1^{\mathrm{t}})\in\mathbb{T}_2$. We will show that f is totally positive and write it as a sum of hermitian squares in USA_2. Write $\Xi=\Xi_1=(\xi_{\imath\jmath})_{\imath\jmath}$ and let

$$u=\begin{pmatrix}\eta_1 & \eta_2\end{pmatrix},\qquad v=\begin{pmatrix}\xi_{22}\eta_1 & \xi_{21}\eta_2 & \xi_{12}\eta_2 & \xi_{11}\eta_1 & \xi_{22}\eta_2 & \xi_{21}\eta_1 & \xi_{12}\eta_1 & \xi_{11}y_2\end{pmatrix}.$$

Then ufu^{t} can be viewed as a quadratic form in v and

$$ufu^{\mathrm{t}}=vG_\alpha v^{\mathrm{t}},\qquad G_\alpha=\begin{pmatrix}
5 & \alpha & \alpha & -2 & 0 & 0 & 0 & 0\\
\alpha & 5 & 0 & -\alpha-2 & 0 & 0 & 0 & 0\\
\alpha & 0 & 5 & -\alpha-2 & 0 & 0 & 0 & 0\\
-2 & -\alpha-2 & -\alpha-2 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & -\alpha-2 & -\alpha-2 & -2\\
0 & 0 & 0 & 0 & -\alpha-2 & 5 & 0 & \alpha\\
0 & 0 & 0 & 0 & -\alpha-2 & 0 & 5 & \alpha\\
0 & 0 & 0 & 0 & -2 & \alpha & \alpha & 5
\end{pmatrix}$$

for $\alpha\in\mathbb{R}$. Observe that G_α is positive semidefinite if and only if $-\frac{7}{2}\le\alpha\le-\frac{5}{2}$. Hence f is indeed totally positive and a sum of hermitian squares in $\mathrm{M}_2(\mathbb{R}[\boldsymbol{\xi}])$. By diagonalizing G_α at $\alpha=-\frac{5}{2}$ we obtain

$$f=\frac{5}{2}(\xi_{12}-\xi_{21})^2+\frac{1}{2}\tilde{H}_2\tilde{H}_2^{\mathrm{t}}+\frac{1}{2}\tilde{H}_3\tilde{H}_3^{\mathrm{t}},$$

where

$$\tilde{H}_2=\begin{pmatrix}\xi_{12}+\xi_{21} & \xi_{22}-\xi_{11}\\ \xi_{11}-\xi_{22} & \xi_{12}+\xi_{21}\end{pmatrix},\qquad \tilde{H}_3=\begin{pmatrix}2(\xi_{12}+\xi_{21}) & \xi_{11}-3\xi_{22}\\ \xi_{22}-3\xi_{11} & 2(\xi_{12}+\xi_{21})\end{pmatrix}.$$

Note that while $\tilde{H}_2\tilde{H}_2^{\mathrm{t}},\tilde{H}_3\tilde{H}_3^{\mathrm{t}}\in\mathrm{Sym}\,\mathbb{T}_2$, we can compute $\mathcal{R}_2(\tilde{H}_2)=\mathcal{R}(\tilde{H}_3)=0$, so $\tilde{H}_2,\tilde{H}_3\notin\mathbb{T}_2$. However, if we set

$$H_1=\Xi-\Xi^{\mathrm{t}},\qquad H_2=\Xi\Xi^{\mathrm{t}}-\Xi^{\mathrm{t}}\Xi,\qquad H_3=\Xi^2-2\Xi\Xi^{\mathrm{t}}+2\Xi^{\mathrm{t}}\Xi-(\Xi^{\mathrm{t}})^2,$$

then

$$H_1H_1^{\mathrm{t}}=(\xi_{12}-\xi_{21})^2,\qquad H_2H_2^{\mathrm{t}}=(\xi_{12}-\xi_{21})^2\tilde{H}_2\tilde{H}_2^{\mathrm{t}},\qquad H_3H_3^{\mathrm{t}}=(\xi_{12}-\xi_{21})^2\tilde{H}_3\tilde{H}_3^{\mathrm{t}}$$

and so

$$f=\frac{5}{2}H_1H_1^{\mathrm{t}}+\frac{1}{2}H_1^{-1}H_2H_2^{\mathrm{t}}H_1^{-\mathrm{t}}+\frac{1}{2}H_1^{-1}H_3H_3^{\mathrm{t}}H_1^{-\mathrm{t}}.$$

A. Constructions of the Reynolds operator

In this appendix we describe a few more ways of constructing $\mathcal{R}_n$ for the action of $\mathrm{O}_n(\mathbb{R})$ on $\mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$ defined in Subsection 2.2. We refer to [Stu08] for algorithms for finite group actions. Let $\mathcal{R}_n':\mathbb{R}[\boldsymbol{\xi}]\to T_n$ be the restriction of $\mathcal{R}_n:\mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])\to\mathbb{T}_n$, i.e., the Reynolds operator for the action of $\mathrm{O}_n(\mathbb{R})$ on $\mathbb{R}[\boldsymbol{\xi}]$ given by

$$f^u=f(u\Xi_1u^{\mathrm{t}},\dots,u\Xi_gu^{\mathrm{t}})$$

for $f\in\mathbb{R}[\boldsymbol{\xi}]$ and $u\in\mathrm{O}_n(\mathbb{R})$.

A.1. **Computing $\mathcal{R}'_n$.** We start by describing two ways of obtaining $\mathcal{R}'_n$.

A.1.1. *First method.* We follow [DK02, Section 4.5.2] to present an algorithm for computing $\mathcal{R}'_n$. We define a linear map $c \in \mathbb{R}[\mathrm{O}_n(\mathbb{R})]^*$:

$$c(r) = \frac{\mathrm{d}}{\mathrm{d}t}\frac{\mathrm{d}}{\mathrm{d}s}\sum_{i,j=1}^{n} r\big((1+se_{ij})(1+te_{ij})\big) - r\big((1+se_{ij})(1+te_{ji})\big)\Big|_{s=t=0},$$

where e_{ij}, $1 \le i,j \le n$, denote the standard matrix units in $\mathrm{M}_n(\mathbb{R})$. (In fact, c equals the Casimir operator of the Lie algebra $\mathfrak{o}_n$ of skew symmetric matrices of the group $\mathrm{O}_n(\mathbb{R})$ up to a scalar multiple.) For example, if $n=2$, then

$$\begin{aligned} c(u_{11}u_{22}) &= \frac{\mathrm{d}}{\mathrm{d}t}\frac{\mathrm{d}}{\mathrm{d}s}\Big(\big((1+se_{12})(1+te_{12})\big)_{11}\big((1+se_{12})(1+te_{12})\big)_{22} - \\ &\quad -\big((1+se_{12})(1+te_{21})\big)_{11}\big((1+se_{12})(1+te_{21})\big)_{22} + \\ &\quad +\big((1+se_{21})(1+te_{21})\big)_{11}\big((1+se_{21})(1+te_{21})\big)_{22} - \\ &\quad -\big((1+se_{21})(1+te_{12})\big)_{11}\big((1+se_{21})(1+te_{12})\big)_{22}\Big)\Big|_{s=t=0} \\ &= \frac{\mathrm{d}}{\mathrm{d}t}\frac{\mathrm{d}}{\mathrm{d}s}(1-st+1-st)\Big|_{s=t=0} \\ &= -2. \end{aligned}$$

For $f \in \mathbb{R}[\boldsymbol{\xi}]$, $u = (u_{\imath\jmath})_{\imath\jmath} \in \mathrm{O}_n(\mathbb{R})$, write f^u as $\sum_i f_i\mu_i$, where f_i are linearly independent polynomials in the variables $\xi_{j\imath\jmath}$ and μ_i are polynomials in the variables $u_{\imath\jmath}$. Define

$$\tilde{c}(f) = \sum f_i c(\mu_i).$$

Find the monic polynomial p of smallest degree such that $p(\tilde{c})(f)=0$. If $p(0)\neq 0$, set $\mathcal{R}''_n(f)=f$. If $p(0)=0$, write $p(t)=tq(t)$ and define $\mathcal{R}''_n(f) = q(0)^{-1}q(\tilde{c}(f))$. By [DK02, Proposition 4.5.17], $\mathcal{R}''_n$ defines the Reynolds operator for the action of $\mathrm{SO}_n(\mathbb{R})$ on $\mathbb{R}[\boldsymbol{\xi}]$. Since $\mathrm{O}_n(\mathbb{R})/\mathrm{SO}_n(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$, setting $\mathcal{R}'_n(f) = \frac{1}{2}(\mathcal{R}''_n(f)+\mathcal{R}''_n(f)^v)$, where v is an arbitrary element in $\mathrm{O}_n(\mathbb{R})\setminus\mathrm{SO}_n(\mathbb{R})$, we obtain the Reynolds operator for the action of $\mathrm{O}_n(\mathbb{R})$ on $\mathbb{R}[\boldsymbol{\xi}]$.

A.1.2. *Second method.* Here we mention another way of computing the Reynolds operator $\mathcal{R}'_n$ in terms of an integral. This approach is based on the way the invariants of $\mathrm{O}_n(\mathbb{R})$ for the action on $\mathbb{R}[\boldsymbol{\xi}]$ were described by Procesi in [Pro76]. Let $f \in \mathbb{R}[\boldsymbol{\xi}]$. We first multihomogenize f as a function $f : \mathrm{M}_n(\mathbb{R})^g \to \mathbb{R}$, then multilinearize its homogeneous components f_i and view f_i as an element $\overline{f}_i \in (\mathrm{M}_n(\mathbb{R})^{\otimes d_i})^*$ for $d_i = \deg(f_i)$. Since $\mathrm{M}_n(\mathbb{R}) \cong V^*\otimes V$ for a n-dimensional vector space V on which $\mathrm{O}_n(\mathbb{R})$ acts naturally, and V^* is isomorphic as a $\mathrm{O}_n(\mathbb{R})$-module to V, $\overline{f}_i$ can be seen as an element $\tilde{f}_i \in V^{\otimes 2d_i}$. The monomial $\xi_{1\imath_1\jmath_1}\cdots\xi_{d\imath_d\jmath_d}$ corresponds to the element

$$e_{\imath_1}\otimes e_{\jmath_1}\otimes\cdots\otimes e_{\imath_d}\otimes e_{\jmath_d},$$

where e_i, $1\le i\le n$, is an orthonormal basis of V. Then we can compute $\mathcal{R}'_n(\overline{f}_i)$ by integrating the function $u \mapsto (\tilde{f}_i)^u$ over $\mathrm{O}_n(\mathbb{R})$. To obtain $\mathcal{R}'_n(f_i)$ we need to restitute $\mathcal{R}'_n(\overline{f}_i)$ and multiply the result by a suitable integer. Finally, $\mathcal{R}'_n(f) = \sum \mathcal{R}'_n(f_i)$.

A.2. **From $\mathcal{R}'_n$ to $\mathcal{R}_n$.** Once we have $\mathcal{R}'_n$, we can compute $\mathcal{R}_n$ as follows.

A.2.1. *First method.* Let $f \in \mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$. We can assume that f is independent of Ξ_g. Let us compute $\mathcal{R}'_n(\mathrm{tr}(f\Xi_g))$. Since this is an invariant, linear in Ξ_g, it has the form

$$\mathcal{R}'_n(\mathrm{tr}(f\Xi_g)) = \mathrm{tr}\left(f_0\Xi_g\right)$$

for some $f_0 \in \mathbb{T}_n$. Here we used the fact that $\mathrm{tr}(h\Xi_g^{\mathrm{t}}) = \mathrm{tr}(h^{\mathrm{t}}\Xi_g)$ for $h \in \mathbb{T}_n$. We define $\mathcal{R}_n(f) = f_0$. We claim that $\mathcal{R}_n : \mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}]) \to \mathbb{T}_n$ is the Reynolds operator. We have $\mathcal{R}_n(f) = f$ for $f \in \mathbb{T}_n$ since $\mathcal{R}'_n(\mathrm{tr}(f\Xi_g)) = \mathrm{tr}(f\Xi_g)$ as $\mathrm{tr}(f\Xi_g) \in T_n$. For $u \in \mathrm{O}_n(\mathbb{R})$, $f \in \mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$ we have

$$\mathrm{tr}((f^u)\Xi_g) = \mathrm{tr}((f\Xi_g)^u) = \mathrm{tr}(f\Xi_g)^u,$$

where the first equality follows as Ξ_g is an invariant and the second one since tr is linear. Thus, $\mathcal{R}_n(f^u) = \mathcal{R}_n(f)$, and $\mathcal{R}_n$ is the Reynolds operator.

A.2.2. *Second method.* If we have $\mathcal{R}'_n$, then the Reynolds operator can also be computed by expressing an element $f \in \mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$ as an $\mathbb{R}(\boldsymbol{\xi})$-linear combination of $\Xi_1^i\Xi_1^{\mathrm{t}j}$, $0 \le i,j \le n-1$. Note that these elements are linearly independent in $\mathrm{M}_n(\mathbb{R}(\boldsymbol{\xi}))$ as there exists $X \in \mathrm{M}_n(\mathbb{R})$ such that $X^iX^{\mathrm{t}j}$, $0 \le i,j \le n-1$, are linearly independent. We denote $\Xi_1^i\Xi_1^{\mathrm{t}j}$, $0 \le i,j \le n-1$, by $y_1,\dots,y_{n^2}$. Let c be a n^2-normal (i.e., multilinear and alternating in the first n^2-variables) central polynomial of $\mathrm{M}_n(\mathbb{R})$ in $2n^2-1$ variables. (See e.g. [Row80, Section 1.4] for the construction of such polynomials and for the proofs of their properties mentioned below.) Since $y_1,\dots,y_{n^2}$ are independent we can find $y_{n^2+1},\dots,y_{2n^2-1} \in \mathrm{GM}_n$ such that

$$0 \neq c(y_1,\dots,y_{n^2},y_{n^2+1},\dots,y_{2n^2-1}) = z \in C_n.$$

If $g \ge n^2$, we can take $y_{n^2+1} = \Xi_2,\dots,y_{2n^2-1} = \Xi_{n^2}$. Then f can be written as follows

$$f = \sum_{i=1}^{n^2}(-1)^{i-1}z^{-1}c(f,y_1,\dots,y_{i-1},y_{i+1},\dots,y_d)y_i. \tag{A.1}$$

Let $z_i(f) = \mathcal{R}'_n(c(f,y_1,\dots,y_{i-1},y_{i+1},\dots,y_d))$. We define

$$\mathcal{R}_n(f) = \sum_{i=1}^{n^2}(-1)^{i+1}z^{-1}z_i(f)y_i.$$

If $f \in \mathbb{T}_n$, then the coefficients in the expression (A.1) are already in T_n, so in this case $\mathcal{R}_n(f) = f$. Note that $\mathcal{R}'_n(z_i(f^u)) = \mathcal{R}'_n(z_i(f))$ for $u \in \mathrm{O}_n(\mathbb{R})$ and $f \in \mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}])$. Therefore $\mathcal{R}_n(f^u) = \mathcal{R}_n(f)$ and $\mathcal{R}_n : \mathrm{M}_n(\mathbb{R}[\boldsymbol{\xi}]) \to \mathbb{T}_n$ is the Reynolds operator.

B. How not to prove the extension Theorem 4.8

One might attempt to prove Theorem 4.8 using geometric invariant theory of Lie groups [PS85, Brö98, CKS09]. Here we explain why this approach fails.

Let G be a compact Lie group with an orthogonal representation on $W = \mathbb{R}^N$. The invariant ring $\mathbb{R}[W]^G$ is a finitely generated $\mathbb{R}$-algebra; let $p_1,\dots,p_m$ be its generators. Let $(\cdot,\cdot)$ denote a G-invariant inner product on W and its dual on W^*. Since the differentials $\mathrm{d}p_i : W \to W^*$ are G-equivariant, we have $(\mathrm{d}p_i,\mathrm{d}p_j) \in \mathbb{R}[W]^G$. Finally let

$$H = \big((\mathrm{d}p_i,\mathrm{d}p_j)\big)_{i,j} \in \mathrm{M}_m(\mathbb{R}[W]^G).$$

The following theorem is a reformulation of the celebrated Procesi-Schwarz theorem [PS85, Theorem 0.10] and is essentially due to Schrijver [Scr+] (see also [Scr08]). We thank M. Schweighofer for drawing our attention to Schrijver's work.

Theorem B.1 (Procesi-Schwarz). *Let $\phi : \mathbb{R}[W]^G \to R$ be an $\mathbb{R}$-algebra homomorphism into a real closed field $R \supseteq \mathbb{R}$. Then the following are equivalent:*

(i) *ϕ extends to an $\mathbb{R}$-algebra homomorphism $\varphi : \mathbb{R}[W] \to R$;*

(ii) $\phi(\mathbb{R}[W]^G \cap \sum \mathbb{R}[W]^2) \subseteq R_{\geq 0}$;
(iii) $\phi(H) \in \mathrm{M}_m(R)$ *is positive semidefinite.*

Proof. While (i)⇒(ii) and (i)⇒(iii) are straightforward, (iii)⇒(ii) is involved and proved in [PS85, Theorem 0.10] and [CKS09, Subsection 2.7]. Hence we are left with (ii)⇒(i). Without loss of generality we can assume that $\phi(\mathbb{R}[W]^G)$ generates R as a field.

First we observe that if $\mathcal{R} : \mathbb{R}[W] \to \mathbb{R}[W]^G$ is the Reynolds operator for the action of G, then $\mathcal{R}(\sum \mathbb{R}[W]^2) \subseteq \sum \mathbb{R}[W]^2$. Note that since G acts linearly on W, the action of G on $\mathbb{R}[W]$ does not increase the degree of polynomials. Since G is compact, $\mathcal{R}$ is given by the integration formula $\mathcal{R}(f) = \int_G f^g \, d\mu(g)$, where μ is the normalized left Haar measure. If $f \in \mathbb{R}[W]$ is of degree d, then $\mathcal{R}(f^2)$ is a limit of sums of squares of degree $2d$. Using Carathéodory's theorem [Bar02, Theorem I.2.3] it is easy to see that the cone of sums of squares in $\mathbb{R}[W]$ of degree at most $2d$ is closed in the space of polynomials of degree at most $2d$ (cf. [Mar08, Section 4.1]). Hence we conclude that $\mathcal{R}(f^2)$ is indeed a sum of squares in $\mathbb{R}[W]$.

Now let $T \subseteq \mathbb{R}[W]$ be the preordering generated by $\phi^{-1}(R_{\geq 0})$. We claim that $-1 \notin T$. Otherwise $-1 = s_0 + \sum_{i \geq 1} s_i t_i$ for some $s_i \in \sum \mathbb{R}[W]^2$ and $t_i \in \phi^{-1}(R_{\geq 0})$. By applying $\mathcal{R}$ we get

$$-1 = \mathcal{R}(s_0) + \sum_{i \geq 1} \mathcal{R}(s_i) t_i. \tag{B.1}$$

By the above observation we have $\mathcal{R}(s_i) \in \mathbb{R}[W]^G \cap \sum \mathbb{R}[W]^2$, so (B.1) implies

$$-1 = \phi(-1) = \phi(\mathcal{R}(s_0)) + \sum_{i \geq 1} \phi(\mathcal{R}(s_i)) \, \phi(t_i) \geq 0,$$

a contradiction. Therefore we can extend T to an ordering $P \subset \mathbb{R}[W]$, which gives rise to a homomorphism $\varphi_0 : \mathbb{R}[W] \to R_0$, where R_0 is the real closure of the ordered field of fractions of $\mathbb{R}[W]/(P \cap -P)$. Since

$$\ker \phi \subseteq T \cap -T \subseteq P \cap -P = \ker \varphi_0,$$

we see that φ_0 extends ϕ and hence $R \subseteq R_0$. By the Artin-Lang homomorphism theorem [BCR98, Theorem 4.1.2] there exists a homomorphism $\varphi : \mathbb{R}[W] \to R$ satisfying $\ker \varphi = \ker \varphi_0$. Thus φ extends ϕ. □

Theorem B.1 can be used to prove the following weakened version of Theorem 4.8.

Corollary B.2. *An $\mathbb{R}$-algebra homomorphism $\phi : T_n \to \mathbb{R}$ extends to an $\mathbb{R}$-algebra homomorphism $\varphi : \mathbb{R}[\boldsymbol{\xi}] \to \mathbb{R}$ if and only if $\phi(\Omega_n) \subseteq \mathbb{R}_{\geq 0}$.*

Let us outline the proof. Let $p_1, \dots, p_m$ be generators of the $\mathbb{R}$-algebra $T_n = \mathbb{R}[\boldsymbol{\xi}]^{\mathrm{O}_n(\mathbb{R})}$. Their differentials $\mathrm{d}p_i : \mathrm{M}_n(\mathbb{R})^g \to (\mathrm{M}_n(\mathbb{R})^g)^*$ are $\mathrm{O}_n(\mathbb{R})$-equivariant maps. Since we can identify $(\mathrm{M}_n(\mathbb{R})^g)^*$ with $(\mathrm{M}_n(\mathbb{R})^*)^g$, and the $\mathrm{O}_n(\mathbb{R})$-equivariant polynomial maps $\mathrm{M}_n(\mathbb{R})^g \to \mathrm{M}_n(\mathbb{R})$ are precisely trace polynomials [Pro76, Theorems 7.1 and 7.2], we have $\mathrm{d}p_i \in \mathbb{T}_n^g$. On $\mathrm{M}_n(\mathbb{R})^g$ there is an $\mathrm{O}_n(\mathbb{R})$-invariant inner product

$$(X, Y) = \operatorname{tr}\left(\sum_j X_j Y_j^{\mathrm{t}}\right).$$

Finally, let $H = ((\mathrm{d}p_i, \mathrm{d}p_j))_{i,j} \in \mathrm{M}_m(T_n)$.

Let $\phi : T_n \to \mathbb{R}$ be an $\mathbb{R}$-algebra homomorphism. Then Theorem B.1 implies that ϕ extends to an $\mathbb{R}$-algebra homomorphism $\varphi : \mathbb{R}[\boldsymbol{\xi}] \to \mathbb{R}$ if and only if $\phi(H) \in \mathrm{M}_m(\mathbb{R})$ is positive semidefinite. To prove the non-trivial direction in Corollary B.2 it therefore suffices to show the following.

Lemma B.3. *If $\phi(\Omega_n) \subseteq \mathbb{R}_{\geq 0}$, then $\alpha^{\mathrm{t}} \phi(H) \alpha \geq 0$ for all $\alpha \in \mathbb{R}^m$.*

Proof. Denote $h_{ij} = (\mathrm{d}p_i)_j \in \mathbb{T}_n$. If $\alpha = (\alpha_i)_i \in \mathbb{R}^m$, then

$$\begin{aligned}\alpha^{\mathsf{t}} H\alpha &= \sum_{i_1,i_2} \alpha_{i_1}\alpha_{i_2}(\mathrm{d}p_{i_1}, \mathrm{d}p_{i_2}) \\ &= \sum_{i_1,i_2} \alpha_{i_1}\alpha_{i_2} \operatorname{tr}\left(\sum_j h_{i_1 j} h_{i_2 j}^{\mathsf{t}}\right) \\ &= \sum_j \operatorname{tr}\left(\sum_{i_1,i_2} \alpha_{i_1} h_{i_1 j}\alpha_{i_2} h_{i_2 j}^{\mathsf{t}}\right) \\ &= \sum_j \operatorname{tr}\left(\left(\sum_i \alpha_i h_{ij}\right)\left(\sum_i \alpha_i h_{ij}\right)^{\mathsf{t}}\right).\end{aligned}$$

Therefore $\phi(\operatorname{tr}(hh^{\mathsf{t}})) \geq 0$ for all $h \in \mathbb{T}_n$ implies that $\phi(H)$ is positive semidefinite. □

From the proof of Lemma B.3 we see that to prove Theorem 4.8 using the Procesi-Schwarz theorem, one would need to extend the chain of equivalences in Theorem B.1 with the condition

(iii') $\alpha^{\mathsf{t}}\phi(H)\alpha \geq 0$ for all $\alpha \in \mathbb{R}^m$.

However, (iii')⇒(iii) fails in our context.

Example B.4. Let $\mathrm{O}_2(\mathbb{R})$ act on $\mathrm{M}_2(\mathbb{R})$ by conjugation, i.e., $n = 2$ and $g = 1$ in the setting of this paper. If $\Xi = \Xi^{(2)}$ is a generic 2×2 matrix and

$$y_1 = \operatorname{tr}(\Xi), \qquad y_2 = \operatorname{tr}(\Xi^2), \qquad y_3 = \operatorname{tr}(\Xi\Xi^{\mathsf{t}}),$$

then $\mathbb{R}[\boldsymbol{\xi}]^{\mathrm{O}_2(\mathbb{R})} = \mathbb{R}[y_1, y_2, y_3]$ (see e.g. [ADS06]; algebraic independence follows from the Jacobian criterion). For this choice of generators we have

$$H = \begin{pmatrix} 2 & 2y_1 & 2y_1 \\ 2y_1 & 4y_3 & 4y_2 \\ 2y_1 & 4y_2 & 4y_3 \end{pmatrix}.$$

Let R be the real closure of the rational function field $\mathbb{R}(\varepsilon)$ endowed with the ordering $0 < \varepsilon < \alpha$ for every $\alpha \in \mathbb{R}_{>0}$. Consider the $\mathbb{R}$-algebra homomorphism

$$\phi : \mathbb{R}[y_1, y_2, y_3] \to R, \qquad y_1 \mapsto \frac{\varepsilon}{2}, \qquad y_2 \mapsto 0, \qquad y_3 \mapsto \frac{1}{8}\varepsilon^2\left(1 + \sqrt{1 + 4\varepsilon^2} - 2\varepsilon\right).$$

For $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in R^3$ we have

$$\begin{aligned}\frac{\alpha^{\mathsf{t}}\phi(H)\alpha}{2} &= \alpha_1^2 + \varepsilon\alpha_1(\alpha_2 + \alpha_3) + \frac{\varepsilon^2(1 + \sqrt{1 + 4\varepsilon^2} - 2\varepsilon)}{4}(\alpha_2^2 + \alpha_3^2) \\ &= \left(\alpha_1 + \frac{\varepsilon(\alpha_2 + \alpha_3)}{2}\right)^2 + \frac{\varepsilon^2(\sqrt{1 + 4\varepsilon^2} - 2\varepsilon)}{4}\left(\alpha_2 - \frac{\alpha_3}{\sqrt{1 + 4\varepsilon^2} - 2\varepsilon}\right)^2 - \varepsilon^3\alpha_3^2.\end{aligned} \tag{B.2}$$

If $\alpha_2, \alpha_3 \in \mathbb{R}$ and $\alpha_1 \neq 0$ or $\alpha_3 \neq -\alpha_2$, then

$$\left(\alpha_1 + \frac{\varepsilon(\alpha_2 + \alpha_3)}{2}\right)^2 > \varepsilon^3\alpha_3^2;$$

and if $\alpha_3 = -\alpha_2 \in \mathbb{R} \setminus \{0\}$, then

$$\frac{\varepsilon^2}{4}\left(\sqrt{1 + 4\varepsilon^2} - 2\varepsilon\right)\left(\alpha_2 + \frac{\alpha_2}{\sqrt{1 + 4\varepsilon^2} - 2\varepsilon}\right)^2 = \frac{\varepsilon^2}{2}\left(1 + \sqrt{1 + 4\varepsilon^2}\right)\alpha_2^2 > \varepsilon^3\alpha_2^2.$$

Therefore $\alpha^{\mathsf{t}}\phi(H)\alpha > 0$ for all $\alpha \in \mathbb{R}^3 \setminus \{0^3\}$. On the other hand, from (B.2) it is clear that we can choose $\alpha \in R^3$ such that $\alpha^{\mathsf{t}}\phi(H)\alpha = -\varepsilon^3 < 0$, so $\phi(H)$ is not positive semidefinite.

References

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

[ADS06] H. Aslaksen, V. Drensky, L. Sadikova: *Defining relations of invariants of two* 3×3 *matrices*, J. Algebra 298 (2006) 41–57.

[AU15] V. Astier, T. Unger: *Signatures of hermitian forms and "prime ideals" of Witt groups*, Adv. Math. 285 (2015) 497–514.

[AU+] V. Astier, T. Unger: *Signatures of hermitian forms, positivity, and an answer to a question of Procesi and Schacher*, preprint `arXiv:1511.06330`.

[Bar02] A. Barvinok: *A course in convexity*, Graduate Studies in Mathematics 54, American Mathematical Society, Providence, RI, 2002.

[BS88] A. Berele, D. J. Saltman: *The centers of generic division algebras with involution*, Israel J. Math. 63 (1988) 98–118.

[BPT13] G. Blekherman, P. A. Parrilo, R. R. Thomas (eds.): *Semidefinite optimization and convex algebraic geometry*, MOS-SIAM Ser. Optim. 13, SIAM, Philadelphia, PA, 2013.

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

[BEFB94] S. Boyd, L. El Ghaoui, E. Feron, V. Balakrishnan: *Linear matrix inequalities in system and control theory*, SIAM Studies in Applied Mathematics 15, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1994.

[Brö98] L. Bröcker: *On symmetric semialgebraic sets and orbit spaces*, Singularities Symposium—Łojasiewicz 70, 37–50, Banach Center Publ. 44, Polish Acad. Sci. Inst. Math., Warsaw, 1998.

[Bru79] G. W. Brumfiel: *Partially ordered rings and semi-algebraic geometry*, London Mathematical Society Lecture Note Series 37, Cambridge University Press, Cambridge-New York, 1979.

[Cim12] J. Cimprič: *Real algebraic geometry for matrices over commutative rings*, J. Algebra 359 (2012) 89–103.

[CKS09] J. Cimprič, S. Kuhlmann, C. Scheiderer: *Sums of squares and moment problems in equivariant situations*, Trans. Amer. Math. Soc. 361 (2009) 735–765.

[CŚ06] B. Collins, P. Śniady: *Integration with respect to the Haar measure on unitary, orthogonal and symplectic group*, Comm. Math. Phys. 264 (2006) 773–795.

[DPRR05] C. De Concini, C. Procesi, N. Reshetikhin, M. Rosso: *Hopf algebras with trace and representations*, Invent. Math. 161 (2005) 1–44.

[dOHMP09] M. C. de Oliveira, J. W. Helton, S. A. McCullough, M. Putinar: *Engineering systems and free semi-algebraic geometry*. In: Emerging applications of algebraic geometry, 17–61. Springer, New York, 2009.

[DK02] H. Derksen, G. Kemper: *Computational invariant theory*, Invariant Theory and Algebraic Transformation Groups, I. Encyclopaedia of Mathematical Sciences Springer-Verlag, Berlin, 2002.

[For79] E. Formanek: *The center of the ring of* 3×3 *generic matrices*, Linear Multilinear Algebra 7 (1979) 203–212.

[GR74] D. Gondard, P. Ribenboim: *Le 17e problème de Hilbert pour les matrices*, Bull. Sci. Math. (2) 98 (1974) 49–56.

[GS14] A. Guionnet, D. Shlyakhtenko: *Free monotone transport*, Invent. Math. 197 (2014) 613–661.

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

[HKM12] J. W. Helton, I. Klep, S. A. McCullough: *The convex Positivstellensatz in a free algebra*, Adv. Math. 231 (2012) 516–534.

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

[Kle11] I. Klep: *Trace-positive polynomials*, Pacific J. Math. 250 (2011) 339–352.

[KS08] I. Klep, M. Schweighofer: *Connes' embedding conjecture and sums of hermitian squares*, Adv. Math. 217 (2008) 1816–1837.

[KU10] I. Klep, T. Unger: *The Procesi-Schacher conjecture and Hilbert's 17th problem for algebras with involution*, J. Algebra 324 (2010) 256–268.

[KVV17] I. Klep, V. Vinnikov, J. Volčič: *Null- and Positivstellensätze for rationally resolvable ideals*, Linear Algebra Appl. 527 (2017) 260–293.

[KMRT98] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol: *The book of involutions*, American Mathematical Society Colloquium Publications 44, American Mathematical Society, Providence, RI, 1998.

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

[LV88] L. Le Bruyn, M. Van den Bergh: *Regularity of trace rings of generic matrices*, J. Algebra 117 (1988) 19–29.

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

[Mon98] J.-P. Monnier: *Anneaux d'holomorphie et Positivstellensatz archimédien*, Manuscripta Math. 97 (1998) 269–302.

[NC10] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*, 10th Anniversary Edition, Cambridge University Press, Cambridge, 2011.

[NT10] T. Netzer, A. Thom: *Tracial algebras and an embedding theorem*, J. Funct. Anal. 259 (2010) 2939–2960.

[Oza13] N. Ozawa: *About the Connes embedding conjecture*, Japan. J. Math. 8 (2013) 147–183.

[Oza16] N. Ozawa: *Noncommutative real algebraic geometry of Kazhdan's property (T)*, J. Inst. Math. Jussieu 15 (2016) 85–90.

[PD01] A. Prestel, C. Delzell: *Positive polynomials: from Hilbert's 17th problem to real algebra*, Springer Monographs in Mathematics, Springer-Verlag Berlin Heidelberg, 2001.

[Pro76] C. Procesi: *The invariant theory of* $n \times n$ *matrices*, Adv. Math. 19 (1976) 306–381.

[PS76] C. Procesi, M. Schacher: *A non-commutative real Nullstellensatz and Hilbert's 17th problem*, Ann. of Math. 104 (1976) 395–406.

[PS85] C. Procesi, G. Schwarz: *Inequalities defining orbit spaces*, Invent. Math. 81 (1985) 539–554.

[Put93] M. Putinar: *Positive polynomials on compact semi-algebraic sets*, Indiana Univ. Math. J. 42 (1993) 969–984.

[Row73] L. H. Rowen: *On classical quotients of polynomial identity rings with involution*, Proc. Amer. Math. Soc. 40 (1973) 23–29.

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

[Sal02] D. J. Saltman: *Invariant fields of symplectic and orthogonal groups*, J. Algebra 258 (2002) 507–534.

[SS12] Y. Savchuk, K. Schmüdgen: *Positivstellensätze for algebras of matrices*, Linear Algebra Appl. 436 (2012) 758–788.

[Sce03] C. Scheiderer: *Sums of squares on real algebraic curves*, Math. Z. 245 (2003) 725–760.

[Sce09] C. Scheiderer: *Positivity and sums of squares: a guide to recent results*, Emerging applications of algebraic geometry 149, 271–324, Springer New York, 2009.

[SH06] C. W. Scherer, C. W. J. Hol: *Matrix sum-of-squares relaxations for robust semi-definite programs*, Math. Program. 107 (2006) 189–211.

[Scm91] K. Schmüdgen: *The K-moment problem for compact semi-algebraic sets*, Math. Ann. 289 (1991) 203–206.

[Scm09] K. Schmüdgen: *Noncommutative real algebraic geometry — some basic concepts and first ideas*, Emerging applications of algebraic geometry, 325–350, IMA Vol. Math. Appl. 149, Springer, New York, 2009.

[Scr08] A. Schrijver: *Tensor subalgebras and first fundamental theorems in invariant theory*, J. Algebra 319 (2008) 1305–1319.

[Scr+] A. Schrijver: *Polynomial and tensor invariants and combinatorial parameters*, preprint, `http://homepages.cwi.nl/~lex/files/tensorc_long.pdf`.

[Scw03] M. Schweighofer: *Iterated rings of bounded elements and generalizations of Schmüdgen's Positivstellensatz*, J. Reine Angew. Math. 554 (2003) 19–45.

[Stu08] B. Sturmfels, *Algorithms in invariant theory*, second edition, Texts and Monographs in Symbolic Computation, Springer-Verlag Vienna, 2008.

[Vid59] I. Vidav: *On some ∗-regular rings*, Acad. Serbe Sci. Publ. Inst. Math. 13 (1959) 73–80.

[WSV12] H. Wolkowicz, R. Saigal, L. Vandenberghe (eds.): *Handbook of semidefinite programming: theory, algorithms, and applications*, vol. 27, Springer Science & Business Media, 2012.

Igor Klep, Department of Mathematics, University of Auckland
Email address: `igor.klep@auckland.ac.nz`

Špela Špenko, Departement Wiskunde, Vrije Universiteit Brussel
Email address: `spela.spenko@vub.ac.be`

Jurij Volčič, Department of Mathematics, Ben-Gurion University of the Negev
Email address: `volcic@post.bgu.ac.il`

NOT FOR PUBLICATION

Contents