THE PROCESI–SCHACHER CONJECTURE AND HILBERT'S 17TH PROBLEM FOR ALGEBRAS WITH INVOLUTION

IGOR KLEP AND THOMAS UNGER

ABSTRACT. In 1976 Procesi and Schacher developed an Artin–Schreier type theory for central simple algebras with involution and conjectured that in such an algebra a totally positive element is always a sum of hermitian squares. In this paper elementary counterexamples to this conjecture are constructed and cases are studied where the conjecture does hold. Also, a Positivstellensatz is established for noncommutative polynomials, positive semidefinite on all tuples of matrices of a fixed size.

Dedicated to David W. Lewis on the occasion of his 65th birthday.

1. INTRODUCTION

Artin's 1927 affirmative solution of Hilbert's 17th problem (*Is every nonnegative real polynomial a sum of squares of rational functions?*) arguably sparked the beginning of the field of real algebra and consequently real algebraic geometry (cf. [BCR, PD]).

Starting with Helton's seminal paper [Hel], in which he proved that every positive semidefinite real or complex noncommutative polynomial is a sum of hermitian squares of *polynomials*, variants of Hilbert's 17th problem in a *noncommutative* setting have become a topic of current interest with wide-ranging applications (e.g. in control theory, optimization, engineering, mathematical physics, etc.); see [dOHMP] for a nice survey. Most of these results have a functional analytic flavour and are what Helton et al. call *dimensionfree*, that is, they deal with evaluations of noncommutative polynomials in matrix algebras of arbitrarily large size.

Procesi and Schacher in their 1976 Annals of Mathematics paper [PS] introduce a notion of orderings on central simple algebras with involution, prove a real Nullstellensatz, and a weak noncommutative version of Hilbert's 17th problem. A strengthening of the latter is proposed as a conjecture [PS, p. 404]: *In a central simple algebra with involution, a totally positive element is always a sum of hermitian squares.*

We explain in Section 5 how these results can be applied to study non-dimensionfree positivity of noncommutative polynomials. Roughly speaking, a noncommutative polynomial all of whose evaluations in $n \times n$ matrices (for *fixed n*) are positive semidefinite, is a sum of hermitian squares with denominators and weights.

A brief outline of the rest of the paper is as follows: in Section 2 we fix terminology and summarize some of the Procesi–Schacher results in a modern language. Then in Section 3 we present counterexamples to the Procesi–Schacher conjecture, while Section 4 contains a study of examples (mainly in the split case) where the conjecture is true.

For general background on central simple algebras with involution we refer the reader to [KMRT] and for the theory of quadratic forms over fields we refer to [Lam].

2. The Procesi–Schacher Conjecture

Let F be a formally real field and let A be a central simple algebra with involution σ and centre K. Assume that F is the fixed field of σ (i.e., $\sigma|_F = \mathrm{id}_F$). The involution σ is of the *first kind* if $K = F$, and of the *second kind* (also called *unitary*) otherwise. In this case $[K : F] = 2$ and $\sigma|_K$ is the non-trivial element in $\mathrm{Gal}(K/F)$.

Let D be a division algebra over K with involution τ and fixed field F. Let h be an n-dimensional hermitian or skew-hermitian form over (D, τ). Then h gives rise to an involution on $M_n(D)$, the *adjoint involution* ad_h, defined by

$$\mathrm{ad}_h(X) = H \cdot \tau(X)^t \cdot H^{-1},$$

for all $X \in M_n(D)$, where H is the Gram matrix of h, t denotes the transpose map on $M_n(D)$ and $\tau(X)$ signifies applying τ to the entries of X. It is well-known that every central simple algebra with involution (A, σ) is of the form $(M_n(D), \mathrm{ad}_h)$, where n is unique, D is unique up to isomorphism and h is unique up to multiplicative equivalence (see [KMRT, 4.A]).

If σ is of the first kind, then σ is called *orthogonal* or *symplectic* if σ becomes adjoint to a quadratic or alternating form, respectively, after scalar extension to a *splitting field* of A (i.e., an extension field L of K such that $A \otimes_K L \cong M_n(L)$). We denote the subspace of σ-symmetric elements of A by $\mathrm{Sym}(A, \sigma)$.

Let $\leq$ be an ordering on F. We identify $\leq$ with its *positive cone* $P = \{x \in F \mid 0 \leq x\}$ via

$$x \leq y \Leftrightarrow y - x \in P$$

for all $x, y \in F$. In this case we also write $\leq_P$ instead of $\leq$.

Procesi and Schacher [PS, §1] consider central simple algebras A, equipped with a *positive involution* σ, i.e., an involution whose *involution trace form* T_σ is positive semidefinite with respect to the ordering $\leq_P$ on F,

$$T_\sigma(x) := \mathrm{Trd}(\sigma(x)x) \geq_P 0 \quad \text{for all } x \in A.$$

Here $\mathrm{Trd} : A \to F$ (the *trace*) denotes the reduced trace $\mathrm{Trd}_{A/F}$ if σ is of the first kind and the composition $\mathrm{Trd}_{K/F} \circ \mathrm{Trd}_{A/K}$ if σ is of the second kind. The form T_σ is a nonsingular quadratic form over F, cf. [KMRT, §11]. If $\dim_K A = n$, then $\dim T_\sigma = n$ if σ is of the first kind and $\dim T_\sigma = 2n$ if σ is of the second kind.

Remark 2.1. The notion of positive involution seems to have been considered first by Weil in his groundbreaking paper [Wei].

Procesi and Schacher also define a notion of *positive elements* in (A, σ), cf. [PS, §V]. For greater clarity we have adapted their definitions as follows:

Definition 2.2.

(1) An ordering $\leq_P$ of F is called a σ-*ordering* if it makes the involution σ positive, i.e., if

$$0 \leq_P \mathrm{Trd}(\sigma(x)x) \quad \text{for all } x \in A.$$

(2) Suppose $\leq_P$ is a σ-ordering on F. An element $a \in \mathrm{Sym}(A, \sigma)$ is called σ-*positive with respect to* $\leq_P$ if the quadratic form $\mathrm{Trd}(\sigma(x)ax)$ is positive semidefinite with respect to $\leq_P$. That is, if

$$0 \leq_P \mathrm{Trd}(\sigma(x)ax) \quad \text{for all } x \in A.$$

(3) An element $a \in \mathrm{Sym}(A, \sigma)$ is called *totally σ-positive* if it is positive with respect to all σ-orderings on F.

Elements of the form $\sigma(x)x$ with $x \in A$ are called *hermitian squares*. The set of hermitian squares of A is clearly a subset of $\mathrm{Sym}(A, \sigma)$. It is also clear that the hermitian squares of K are all in F.

Example 2.3. Sums of hermitian squares and sums of traces of hermitian squares are examples of totally σ-positive elements, as easy verifications will show.

One of the main results in [PS] explains that these are essentially the only examples. It can be considered as a noncommutative analogue of Artin's solution to Hilbert's 17th problem:

Theorem 2.4. [PS, Theorem 5.4] *Let A be a central simple algebra with involution σ, centre K and fixed field F. Let $\alpha_1, \ldots, \alpha_m \in F$ be elements appearing in a diagonalisation of the quadratic form $\mathrm{Trd}(\sigma(x)x)$. Then for $a \in \mathrm{Sym}(A, \sigma)$ the following statements are equivalent:*

  (i) *a is totally σ-positive;*

  (ii) *there exist $x_{i,\varepsilon} \in A$ with*

$$a = \sum_{\varepsilon \in \{0,1\}^m} \alpha^\varepsilon \sum_i \sigma(x_{i,\varepsilon})x_{i,\varepsilon}.$$

  (As usual, α^ε denotes $\alpha_1^{\varepsilon_1} \cdots \alpha_m^{\varepsilon_m}$.)

In the case $n = \deg A = 2$, the weights α_j are superfluous (we will come back to this later). Procesi and Schacher [PS, p. 404] conjecture that this is also the case for $n > 2$:

The PS Conjecture. *In a central simple algebra A with involution σ, every totally σ-positive element is a sum of hermitian squares. (Equivalently: the trace of a hermitian square is always a sum of hermitian squares.)*

Remark 2.5. The two statements in the PS Conjecture are indeed equivalent: the necessary direction follows from the fact that traces of hermitian squares are totally σ-positive, as observed in Example 2.3.

For the sufficient direction, assume that the trace of a hermitian square is always a sum of hermitian squares. Let $a \in \mathrm{Sym}(A, \sigma)$ be totally σ-positive. Then a can be expressed in terms of the entries in a diagonalization of the form $\mathrm{Trd}(\sigma(x)x)$ as in Theorem 2.4(ii). Let β be such an entry. Thus, $\beta = \mathrm{Trd}(\sigma(y)y)$ for some $y \in A$. By the assumption there are $x_1, \ldots, x_\ell \in A$ such that $\beta = \sum_i \sigma(x_i)x_i$. Since $\beta \in F$, the expression in Theorem 2.4(ii) can now be rewritten as a sum of hermitian squares.

As mentioned a few lines earlier, Procesi and Schacher provide supporting evidence for their conjecture for the case $\deg A = 2$. Another case where the PS Conjecture is true has been well-known since the 1970s:

Example 2.6. Let A be the full matrix ring $M_n(F)$ over a formally real field F endowed with the transpose involution $\sigma = t$. Since $\mathrm{Trd} = \mathrm{tr}$, every ordering of F is a σ-ordering. We claim that $a \in \mathrm{Sym}(A, \sigma)$ is totally σ-positive if and only if a is a positive semidefinite matrix in $A \otimes_F R = M_n(R)$ for any real closed field R containing F (equivalently: for any real closure of F).

Indeed, if a is totally σ-positive, then for all $x \in A$, $\mathrm{tr}(x^t a x)$ is positive with respect to every $(\sigma$-)ordering of F, i.e., $\mathrm{tr}(x^t a x) \in \sum F^2$. A diagonalisation of the quadratic form $\mathrm{tr}(x^t a x)$ will contain only sums of squares in F (as it would otherwise violate the total σ-positivity). Hence this quadratic form remains positive semidefinite under every ordered field extension of F.

The converse implication is also easy: if a is positive semidefinite over $M_n(R)$ for every real closed field $R \supseteq F$, then the trace of $x^t a x$ for $x \in A$ is nonnegative under the ordering of R and hence under all orderings of F. By definition, this means that a is totally σ-positive.

Moreover, every totally σ-positive element of (A, σ) is a sum of hermitian squares. Essentially, this goes back to Gondard and Ribenboim [GR] and has been reproved several times [Djo, FRS, HN, KS]. It also follows easily from Theorem 2.4 for it suffices to show that the trace of a hermitian square is a sum of hermitian squares. But this is clear: if $a = [a_{ij}]_{1 \le i, j \le n} \in A$, then

$$\mathrm{Trd}(\sigma(a)a) = \sum_{i,j=1}^n a_{ij}^2$$

is obviously a sum of (hermitian) squares in F.

The reader will have no problems extending this example to the case $K = F(\sqrt{-1})$ and $A = M_n(K)$ endowed with the conjugate transpose involution $\overline{}t$.

3. The Counterexamples

When the transpose involution in the previous example is replaced by an arbitrary orthogonal involution σ on $M_n(F)$ (i.e., an involution which is adjoint to a quadratic form over F), the equivalence between totally σ-positive elements and sums of hermitian squares is in general no longer true, as we proceed to show in this section. We assume throughout that F_0 is a formally real field.

Lemma 3.1. *Let $F = F_0((X))((Y))$, the iterated Laurent series field in two commuting variables X and Y. The quadratic form*

$$q = \langle X, Y, XY \rangle$$

does not weakly represent 1 over F. In fact this is already true over the rational function field $F_0(X, Y)$.

Proof. Assume for the sake of contradiction that $m \times q$ represents 1 for some positive integer m. Then the form

$$\varphi := \langle 1 \rangle \perp m \times \langle -X, -Y, -XY \rangle$$

is isotropic over F. This leads to a contradiction by repeated application of Springer's theorem on fields which are complete with respect to a discrete valuation, cf. [Lam, Chapter VI, §1]. Since $F_0(X, Y)$ embeds into F the proof is finished. ∎

Theorem 3.2. *Let $F = F_0(X, Y)$. Let $A = M_3(F)$ and $\sigma = \mathrm{ad}_q$, where*

$$q = \langle X, Y, XY \rangle.$$

The (σ-symmetric) element XY is totally σ-positive, but is not a sum of hermitian squares in (A, σ).

Proof. It is clear that $XY \in \mathrm{Sym}(A, \sigma)$ since $XY \in F$.

We first show that XY is totally σ-positive. Since $T_\sigma \simeq q \otimes q$ (see [Lew, p. 227] or [KMRT, 11.4]) we have

$$\mathrm{sign}_P T_\sigma = (\mathrm{sign}_P q)^2 \in \{1, 9\}$$

for any ordering $P \in X_F$. (Here $\mathrm{sign}_P T_\sigma$ denotes the signature of the quadratic form T_σ with respect to the ordering P.) Hence, the set of σ-orderings on F is not empty. It is exactly the set of $P \in X_F$ with $\mathrm{sign}_P T_\sigma = 9$. (Note that F has orderings for which both X and Y, and thus XY, are positive so that the value $\mathrm{sign}_P T_\sigma = 9$ can indeed be attained.)

Let P be any σ-ordering on F. Then we have for any $a \in A$,

$$\mathrm{Trd}(\sigma(a)a) \geq_P 0$$

(by definition) and so for any $a \in A$,

$$\mathrm{Trd}(\sigma(a)XYa) = XY \, \mathrm{Trd}(\sigma(a)a) \geq_P 0,$$

since $XY \geq_P 0$ (for otherwise $\mathrm{sign}_P T_\sigma = 1$ and P would not be a σ-ordering on F). Hence, XY is totally σ-positive. An alternative argument showing that XY is totally σ-positive can be given by observing that $XY = \mathrm{Trd}(\sigma(b)b)$ for

$$b = \begin{bmatrix} 0 & X & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Next we show that XY is not a sum of hermitian squares in $(A, \sigma) = (M_3(F), \mathrm{ad}_q)$. We identify XY with XYI_3 in $M_3(F)$, where I_3 denotes the 3×3 identity matrix. Assume

for the sake of contradiction that XYI_3 is a sum of elements of the form $\sigma(a)a$ with $a = [a_{ij}]_{1 \le i, j \le 3} \in M_3(F)$. Recall that

$$\sigma(a)a = \mathrm{ad}_q(a)a = \begin{bmatrix} X \\ & Y \\ & & XY \end{bmatrix} \cdot a^t \cdot \begin{bmatrix} X \\ & Y \\ & & XY \end{bmatrix}^{-1} \cdot a.$$

The $(3,3)$-entry of $\sigma(a)a$ is equal to

$$Ya_{13}^2 + Xa_{23}^2 + a_{33}^2.$$

By our assumption there are $s_1, s_2, s_3 \in \sum F^{\times 2}$ such that

$$XY = Ys_1 + Xs_2 + s_3,$$

which is equivalent with

$$1 = X^{-1}s_1 + Y^{-1}s_2 + X^{-1}Y^{-1}s_3.$$

Thus, 1 is weakly represented by the quadratic form

$$\langle X^{-1}, Y^{-1}, X^{-1}Y^{-1} \rangle \simeq \langle X, Y, XY \rangle = q,$$

which is impossible by Lemma 3.1. This finishes the proof. ∎

The previous theorem gives us a counterexample to the PS Conjecture. It shows that the conjecture is in general not true for full matrix algebras equipped with an orthogonal involution. In contrast, when we equip a full matrix algebra with a *symplectic* involution, we will show in Theorem 4.7 below that the conjecture does hold.

Thus, we could ask if the PS Conjecture also holds for non-split central simple algebras with symplectic involution. The answer is "no":

Theorem 3.3. *Let $F = F_0(X, Y)$. Let $A = M_3(F) \otimes_F H \cong M_3(H)$, where $H = (-1, -1)_F$ is Hamilton's quaternion division algebra over F. Equip A with the involution $\sigma = \mathrm{ad}_q \otimes \gamma$, where γ is quaternion conjugation and $\sigma = \mathrm{ad}_q$ for*

$$q = \langle X, Y, XY \rangle.$$

The algebra A is central simple over F of degree 6 and the involution σ is symplectic. The (σ-symmetric) element XY is totally σ-positive, but is not a sum of hermitian squares in (A, σ).

Proof. The assertion about (A, σ) is clear, as is the fact that $XY \in \mathrm{Sym}(A, \sigma)$ since $XY \in F$.

It is easy to verify that the involution trace form of γ, T_γ, is isometric to $\langle 2 \rangle \otimes N_H$, where $N_H = \langle 1, 1, 1, 1 \rangle$ is the norm form of H. Here $N_H(x) := \mathrm{Nrd}_H(x)$ for all $x \in H$, where Nrd_H denotes the reduced norm on H. Since $T_\sigma = T_{\mathrm{ad}_q \otimes \gamma} \simeq T_{\mathrm{ad}_q} \otimes T_\gamma$, we have

$$\mathrm{sign}_P T_\sigma = (\mathrm{sign}_P T_{\mathrm{ad}_q})(\mathrm{sign}_P T_\gamma) = 4\,\mathrm{sign}_P T_{\mathrm{ad}_q} \in \{4, 36\}$$

for any ordering $P \in X_F$. Hence, the set of σ-orderings on F is not empty. It is exactly the set of $P \in X_F$ with $\mathrm{sign}_P T_\sigma = 36$. (Note again that this value can indeed be attained since there are orderings on F for which both X and Y, and thus XY, are positive.) Arguing similarly as in the proof of Theorem 3.2 we can verify that XY is totally σ-positive.

Before proceeding, note that the involution γ is adjoint to the hermitian form $\langle 1 \rangle_\gamma$ over (H, γ). Hence, σ is adjoint to the hermitian form $h = q \otimes \langle 1 \rangle_\gamma = \langle X, Y, XY \rangle_\gamma$ over (H, γ). Thus

$$h(x, y) = \gamma(x_1)Xy_1 + \gamma(x_2)Yy_2 + \gamma(x_3)XYy_3$$

for vectors $x = (x_1, x_2, x_3)$ and $y = (y_1, y_2, y_3)$ in the right H-vector space H^3.

Next we show that XY is not a sum of hermitian squares in $(A, \sigma) = (M_3(H), \mathrm{ad}_h)$. We identify XY with XYI_3 in $M_3(H)$, where I_3 denotes the 3×3 identity matrix. Assume for the sake of contradiction that XYI_3 is a sum of elements of the form $\sigma(a)a$ with $a = [a_{ij}]_{1 \le i,j \le 3} \in M_3(H)$. Recall that

$$\sigma(a)a = \mathrm{ad}_h(a)a = \begin{bmatrix} X & & \\ & Y & \\ & & XY \end{bmatrix} \cdot \gamma(a)^t \cdot \begin{bmatrix} X & & \\ & Y & \\ & & XY \end{bmatrix}^{-1} \cdot a,$$

where $\gamma(a) = [\gamma(a_{ij})]_{1 \le i,j \le 3}$. The $(3, 3)$-entry of $\sigma(a)a$ is equal to

$$\gamma(a_{13})Ya_{13} + \gamma(a_{23})Xa_{23} + \gamma(a_{33})a_{33} = YN_H(a_{13}) + XN_H(a_{23}) + N_H(a_{33}).$$

Since $N_H = \langle 1, 1, 1, 1 \rangle$, each of $N_H(a_{13})$, $N_H(a_{23})$, $N_H(a_{33})$ is a sum of four squares in F. Thus, by our assumption there are $s_1, s_2, s_3 \in \sum F^{\times 2}$ such that

$$XY = Ys_1 + Xs_2 + s_3.$$

We can now finish the proof with an appeal to Lemma 3.1, as in the proof of Theorem 3.2. ∎

Remark 3.4. By tensoring $(M_3(F), \mathrm{ad}_q)$ with Hamilton's quaternion division algebra, equipped with a *unitary* involution one obtains a counterexample in the non-split unitary case. We leave the details, which are similar to those in the proof of Theorem 3.3, to the diligent reader.

Remark 3.5. From a real algebra perspective it is clear that these counterexamples to the PS Conjecture can easily be seen to work over any formally real field F that admits a proper semiordering (see [PD, §5] for details and unexplained terminology). Given such a field F, endowed with a proper semiordering, take negative $a, b \in F$ such that ab is negative as well. Then $q = \langle a, b, ab \rangle$ does not weakly represent 1 (the quadratic module generated by $\{-a, -b, -ab\}$ is proper) and thus in $M_3(F)$, endowed with the involution $\sigma = \mathrm{ad}_q$, the element ab is totally σ-positive, but not a sum of hermitian squares (as the proof of Theorem 3.2 shows).

4. Positive Results

Procesi and Schacher [PS, p. 404 and 405] prove their conjecture for central simple algebras A of degree two, i.e., quaternion algebras, with arbitrary involution σ by appealing to matrices and the Cayley–Hamilton theorem. We start this section by giving an alternative argument motivating some of the generalizations that follow.

Throughout this section we assume that the base field F is formally real.

Proposition 4.1. *Let A be a quaternion algebra* (*not necessarily division*) *with centre K, equipped with an arbitrary involution σ. Let F be the fixed field of (A, σ). Each entry occurring in a diagonalisation of T_σ is a sum of hermitian squares.*

Proof. (i) We first consider involutions of the first kind on A. Let A be the quaternion algebra $(a, b)_F$ with F-basis $\{1, i, j, k\}$ where i, j and k anti-commute, $ij = k$, $i^2 = a$ and $j^2 = b$.

If σ is symplectic, then σ is the unique quaternion conjugation involution γ on A. An easy computation gives $T_\sigma = T_\gamma \simeq \langle 2 \rangle \otimes \langle 1, -a, -b, ab \rangle$. We have

$$1 = \gamma(1)1, \quad -a = \gamma(i)i, \quad -b = \gamma(j)j, \quad ab = \gamma(k)k.$$

If σ is orthogonal, then $\sigma = \mathrm{Int}(u) \circ \gamma$, where $u \in A$ satisfies $\gamma(u) = -u$. From [KMRT, 11.6] we know that

$$T_\sigma \simeq \langle 2 \rangle \otimes \langle 1, \mathrm{Nrd}_A(u), -\mathrm{Nrd}_A(s), -\mathrm{Nrd}_A(su) \rangle$$

for some $s \in A$ with $\sigma(s) = s = -\gamma(s)$. Now,

$$\mathrm{Nrd}_A(u) = u\gamma(u) = u\gamma(u)u^{-1}u = \sigma(u)u;$$
$$-\mathrm{Nrd}_A(s) = -\gamma(s)s = \sigma(s)s;$$
$$-\mathrm{Nrd}_A(su) = -\mathrm{Nrd}_A(s)\mathrm{Nrd}_A(u) = -\gamma(s)s\,\mathrm{Nrd}_A(u) = \sigma(s)\sigma(u)us = \sigma(us)us.$$

(ii) Finally, let $K = F(\sqrt{\delta})$ and let A be a quaternion algebra over K with unitary involution σ whose restriction to K is τ, where τ is determined by $\tau(\sqrt{\delta}) = -\sqrt{\delta}$. By a well-known result of Albert [KMRT, 2.22] there exists a unique quaternion F-subalgebra $A_0 \subseteq A$ such that

$$A = A_0 \otimes_F K \text{ and } \sigma = \gamma_0 \otimes \tau,$$

where γ_0 is quaternion conjugation on A_0. Then $T_\sigma \simeq T_{\gamma_0} \otimes T_\tau \simeq T_{\gamma_0} \otimes \langle 1, -\delta \rangle$. Since $\tau(\sqrt{\delta})\sqrt{\delta} = -\delta$, we are finished by the symplectic part of the proof. ∎

This shows in particular that the PS Conjecture is true for full matrix algebras of degree two over a formally real field F since these are just split quaternion algebras.

Part (ii) of the proof of Proposition 4.1 motivates the following more general result:

Theorem 4.2. *Let A and B be central simple algebras with centre K, equipped with arbitrary involutions σ and τ, respectively. Assume that (A, σ) and (B, τ) have the same fixed field F. If the PS Conjecture holds for (A, σ) and (B, τ), it also holds for the tensor product $(A \otimes_K B, \sigma \otimes \tau)$.*

Proof. This is a simple computation, using the fact that $T_{\sigma \otimes \tau} \simeq T_\sigma \otimes T_\tau$ and that elements of A commute with elements of B in the tensor product $A \otimes_K B$. ∎

Corollary 4.3. *Let $(Q_1, \sigma_1), \ldots, (Q_\ell, \sigma_\ell)$ be quaternion algebras with arbitrary involution over K and with common fixed field F. The PS Conjecture holds for the tensor product $\bigotimes_{i=1}^{\ell}(Q_i, \sigma_i)$.*

Proof. This is an immediate consequence of Proposition 4.1 and Theorem 4.2. ∎

Corollary 4.4. *Let $A = M_n(F)$ be a split algebra of* 2-*power degree $n = 2^\ell$, equipped with an orthogonal involution σ which is adjoint to an n-fold Pfister form over F. The PS Conjecture holds for (A, σ).*

Proof. By Becher's proof of the Pfister Factor Conjecture [Bec], (A, σ) decomposes as

$$(A, \sigma) \cong \bigotimes_{i=1}^{\ell} (Q_i, \sigma_i),$$

where $(Q_1, \sigma_1), \ldots, (Q_\ell, \sigma_\ell)$ are quaternion algebras with involution. An appeal to Corollary 4.3 finishes the proof. ∎

Corollary 4.5. *Let $A = M_n(K)$ be a split algebra of* 2-*power degree $n = 2^\ell$, equipped with a hyperbolic involution σ of any kind. Let F be the fixed field of (A, σ). The PS Conjecture holds for (A, σ).*

Proof. Recall from [BST, Theorem 2.1] that the involution σ is hyperbolic if there exists an idempotent $e \in A$ such that $\sigma(e) = 1 - e$ or, equivalently, if the adjoint (quadratic, alternating or hermitian) form of σ is hyperbolic.

If $\ell = 1$ this is just the split version of Proposition 4.1. Assume now that $\ell \geq 2$. By [BST, Theorem 2.2], (A, σ) decomposes as

$$(A, \sigma) \cong \bigotimes_{i=1}^{\ell} (Q, \sigma_i),$$

where $Q = M_2(K)$ and $\sigma_1, \ldots, \sigma_\ell$ are involutions on Q. An appeal to Corollary 4.3 finishes the proof. ∎

Corollary 4.6. *Let $A = M_n(F)$ be a split algebra of* 2-*power degree $n = 2^\ell$, equipped with a symplectic involution σ. The PS Conjecture holds for (A, σ).*

Proof. If σ is a symplectic involution, it is hyperbolic (since it is adjoint to an alternating form over F which is automatically hyperbolic) and we are finished by Corollary 4.5. ∎

In fact, the PS Conjecture is true for *any* split algebra with symplectic involution. Such an algebra is always of even degree.

Theorem 4.7. *Let $A = M_n(F)$ be a split algebra of even degree $n = 2m$, equipped with a symplectic involution σ. The PS Conjecture holds for (A, σ).*

Proof. Since σ is symplectic, the quadratic form T_σ is hyperbolic (see [Lew, p. 227] or [KMRT, Proof of 11.7]). Thus $T_\sigma \simeq m \times \langle 1, -1 \rangle$ and it suffices to show that -1 is a sum of hermitian squares in A. We identify -1 with $-I_n$, where I_n denotes the $n \times n$ identity matrix in $A = M_n(F)$.

Since σ is symplectic, we have $\sigma = \text{Int}(S) \circ t$, where t denotes transposition and $S \in \text{GL}_n(F)$ satisfies $S^t = -S$. Since S is skew-symmetric, there exists a matrix $P \in \text{GL}_n(F)$ such that $P^t S P = B$, where B is the block diagonal matrix with m blocks $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} \right]$ on the diagonal.

Let X be the block diagonal matrix with m blocks $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$ on the diagonal. Then $X^t B X = B^{-1}$. Hence with $Y = P X P^t$, we have $Y^t S Y = S^{-1}$. Thus

$$\sigma(SY)SY = S(SY)^t S^{-1} SY = SY^t S\,^t Y = SY^t(-S)Y = -SS^{-1} = -I_n.\qquad\blacksquare$$

5. Positive noncommutative polynomials

5.1. **Algebras of generic matrices with involution.** After studying the PS Conjecture in the setting of central simple algebras with involution, we proceed to interpret these results as well as Theorem 2.4 for non-dimensionfree positivity of noncommutative (NC) polynomials.

Motivated by problems in optimization and control theory, Helton [Hel] proved that a symmetric real or complex NC polynomial, all of whose images under algebra $*$-homomorphisms into $M_n(\mathbb{R})$, $n \in \mathbb{N}$, are positive semidefinite (i.e., a dimensionfree positive NC polynomial), is a sum of hermitian squares. What we are interested in, is positivity under evaluations in $M_n(\mathbb{R})$ for a *fixed n*.

To tackle this problem we introduce the language of generic matrices [Row]. Verifying a condition on evaluations of an NC polynomial in the algebra of $n \times n$ matrices is often conveniently done in the algebra of generic matrices. In this subsection we recall the definition of generic matrices with involution, while our main result on positive NC polynomials (i.e., a Positivstellensatz) is presented in the next subsection.

As in the classical construction of the algebra of generic matrices (see e.g. [Row, §1.3]), it is possible to construct the algebra of generic matrices *with involution* [PS, §II]. To each type of involution (orthogonal, symplectic and unitary) an algebra of generic matrices with involution can be associated, as we now explain. We assume from now on that K is a field of characteristic 0 with involution $*$ and fixed field F.

Let $K\langle \overline{X}, \overline{X}^* \rangle$ be the free algebra with involution over $(K, *)$, i.e., the algebra with involution, freely generated by the noncommuting variables $\overline{X} := (X_1, X_2, \ldots)$. Its elements (called *NC polynomials*) are (finite) linear combinations of words in (the infinitely many) letters $\overline{X}, \overline{X}^*$.

Fix a type $\mathrm{J} \in \{\text{orthogonal, symplectic, unitary}\}$. Let $\mathfrak{a}_{\mathrm{J}_n} \subseteq K\langle \overline{X}, \overline{X}^* \rangle$ denote the ideal of all identities satisfied by degree n central simple K-algebras with type J involution. That is, $f = f(X_1, \ldots, X_k, X_1^*, \ldots, X_k^*) \in K\langle \overline{X}, \overline{X}^* \rangle$ is an element of $\mathfrak{a}_{\mathrm{J}_n}$ if and only if for every central simple algebra A of degree n with type J involution σ and every $a_1, \ldots, a_k \in A$,

$$f(a_1, \ldots, a_k, \sigma(a_1), \ldots, \sigma(a_k)) = 0.$$

Then $\mathrm{GM}_n(K, \mathrm{J}) := K\langle \overline{X}, \overline{X}^* \rangle / \mathfrak{a}_{\mathrm{J}_n}$ is the *algebra of generic $n \times n$ matrices with type J involution*.

Remark 5.1. An alternative description of the algebra of generic matrices with involution can be obtained as follows. Let $\zeta := (\zeta_{ij}^{(\ell)} \mid 1 \le i, j \le n, \ \ell \in \mathbb{N})$ denote commuting variables and form the polynomial algebra $K[\zeta]$ endowed with the involution extending $*$ and fixing $\zeta_{ij}^{(\ell)}$ pointwise. Consider the $n \times n$ matrices $Y_\ell := [\zeta_{ij}^{(\ell)}]_{1 \le i,j \le n} \in M_n(K[\zeta])$, $\ell \in \mathbb{N}$. Each Y_ℓ is called a *generic matrix*.

(a) If $\mathsf{J} \in \{\text{orthogonal, unitary}\}$, then the (unital) K-subalgebra of $M_n(K[\zeta])$ generated by the Y_ℓ and their transposes is (canonically) isomorphic to $\mathrm{GM}_n(K, \mathsf{J})$.

(b) If $\mathsf{J} = \text{symplectic}$, then n is even, say $n = 2m$. Consider the usual symplectic involution

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix} \mapsto \begin{bmatrix} w^t & -y^t \\ -z^t & x^t \end{bmatrix}$$

on $M_{2m}(K[\zeta])$. Then the (unital) K-subalgebra of $M_n(K[\zeta])$ generated by the Y_ℓ and their images under this involution is (canonically) isomorphic to $\mathrm{GM}_n(K, \mathsf{J})$.

If $n = 1$, then $\mathsf{J} \in \{\text{orthogonal, unitary}\}$ and $\mathrm{GM}_1(K, \mathsf{J})$ is isomorphic to $K[\zeta]$ endowed with the involution introduced above. Hence in the sequel we will always assume $n \geq 2$.

Let $\mathsf{J} \in \{\text{orthogonal, symplectic, unitary}\}$. For $n \geq 2$, $\mathrm{GM}_n(K, \mathsf{J})$ is a PI algebra and a domain (cf. [PS, §II]). Hence its central localization is a division algebra $\mathrm{UD}_n(K, \mathsf{J})$ with involution, which we call the *generic division algebra* with type J involution of degree n. As we will only consider the canonical involution on $\mathrm{GM}_n(K, \mathsf{J})$ and $\mathrm{UD}_n(K, \mathsf{J})$ we use $*$ to denote it.

5.2. A Positivstellensatz.

Let $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ be endowed with the complex conjugation involution $\overline{}$. Our aim in this subsection is to deduce a non-dimensionfree version of Helton's sum of hermitian squares theorem. We will describe symmetric NC polynomials f all of whose evaluations in $M_n(\mathbb{K})$ are positive semidefinite, see Theorem 5.3.

We start with a lemma characterizing total $*$-positivity in the algebra of generic matrices $\mathrm{GM}_n(\mathbb{K}, \mathsf{J})$. The proof of the following proposition uses some elementary model theory, e.g. Tarski's transfer principle for real closed fields. All the necessary background can be found in [PD, §1 and §2] or, alternatively, [BCR, §1].

Lemma 5.2. *Let $n \in \mathbb{N}$. If $\mathbb{K} = \mathbb{R}$, let $\mathsf{J} = \text{orthogonal}$ and if $\mathbb{K} = \mathbb{C}$, let $\mathsf{J} = \text{unitary}$. If $a = a^* \in \mathrm{GM}_n(\mathbb{K}, \mathsf{J})$ is totally σ-positive under each $*$-homomorphism from $\mathrm{GM}_n(\mathbb{K}, \mathsf{J})$ to $M_n(\mathbb{K})$ endowed with a positive type J involution σ, then a is totally $*$-positive (in $\mathrm{UD}_n(\mathbb{K}, \mathsf{J})$).*

Proof. Suppose $a \in \mathrm{GM}_n(\mathbb{K}, \mathsf{J})$ is not totally $*$-positive. Then there is a $*$-ordering $\leq$ of the fixed field Z of the centre of $\mathrm{UD}_n(\mathbb{K}, \mathsf{J}))$ under which $\mathrm{Trd}(x^* a x)$ is not positive semidefinite. Let $\langle \alpha_1, \dots, \alpha_m \rangle$ be the diagonalisation of $\mathrm{Trd}(x^* x)$ with $\alpha_i = \alpha_i^* \in Z$. (Here $m = n^2$ if the involution is of the first kind and $m = 2n^2$ otherwise.) Given that Z is the field of fractions of the symmetric centre Z_0 of $\mathrm{GM}_n(\mathbb{K}, \mathsf{J})$, we may even assume $\alpha_i \in Z_0$. We also diagonalise $\mathrm{Trd}(x^* a x)$ as $\langle \beta_1, \dots, \beta_m \rangle$ with $\beta_i \in Z_0$. Clearly, $\alpha_i > 0$ and one of the β_i, say β_1, is negative with respect to the given $*$-ordering $\leq$. Let $\overline{Z}^{\mathrm{rc}}$ denote the real closure of Z with respect to this ordering and form $A := \mathrm{UD}_n(\mathbb{K}, \mathsf{J}) \otimes_Z \overline{Z}^{\mathrm{rc}}$ endowed with the involution $\sigma = * \otimes \mathrm{id}$. Then A is a central simple algebra over a real closed (if $\mathsf{J} = \text{orthogonal}$) or algebraically closed field (if $\mathsf{J} = \text{unitary}$). Moreover, its involution σ is positive. Hence by the classification result [PS, Theorem 1.2] of Procesi and Schacher, A is either $M_n(\overline{Z}^{\mathrm{rc}})$ endowed with the transpose (if $\mathsf{J} = \text{orthogonal}$) or

$M_n(\overline{Z})$ endowed with the complex conjugate transpose involution (if J = unitary). Here $\overline{Z}$ is the algebraic closure $\overline{Z}^{\mathrm{rc}}(\sqrt{-1})$ of $\overline{Z}^{\mathrm{rc}}$ and the complex conjugate maps $r+t\sqrt{-1} \mapsto r-t\sqrt{-1}$ for $r,t \in \overline{Z}^{\mathrm{rc}}$.

For $b \in \mathrm{GM}_n(\mathbb{K}, \mathrm{J})$ let $\hat{b} \in \mathbb{K}\langle \overline{X}, \overline{X}^* \rangle$ denote a preimage of b under the canonical map $\mathbb{K}\langle \overline{X}, \overline{X}^* \rangle \to \mathrm{GM}_n(\mathbb{K}, \mathrm{J})$. Every $*$-homomorphism $\mathrm{GM}_n(\mathbb{K}, \mathrm{J}) \to M_n(L)$ for a $*$-field extension L of $\mathbb{K}$, where $M_n(L)$ is given a type J involution, yields a $*$-homomorphism $\mathbb{K}\langle \overline{X}, \overline{X}^* \rangle \to M_n(L)$, so is essentially given by a point $s \in M_n(L)^{\mathbb{N}}$ describing the images of the X_i under this induces map.

By construction, the image $\beta_1 \otimes 1$ of β_1 under the embedding of algebras with involution $\mathrm{GM}_n(\mathbb{K}, \mathrm{J}) \to A$ is not σ-positive. Let s denote the corresponding evaluation point. By Example 2.6, this means that $\hat{\beta}_1(s, \overline{s}^t) = \beta_1 \otimes 1$ is not positive semidefinite. Consider the following elementary statement:

(1)
$$\exists\, n \times n \text{ matrices } x = (x_1, \dots, x_N) : \hat{\alpha}_i(x, \overline{x}^t) \text{ is positive semidefinite } \wedge$$
$$\hat{\beta}_1(x, \overline{x}^t) \text{ is not positive semidefinite.}$$

(N is the maximal number of variables appearing in one of the $\hat{\alpha}_i, \hat{\beta}_1$.)

Obviously such $n \times n$ matrices x_i can be found over $\overline{Z}^{\mathrm{rc}}$ or $\overline{Z}$; just take $x_i = s_i$. By Tarski's transfer principle, the above elementary statement (1) can be satisfied in $\mathbb{K}$. This yields a $*$-homomorphism $\mathbb{K}\langle \overline{X}, \overline{X}^* \rangle \to M_n(\mathbb{K})$ endowed with the (positive) involution $\overline{}t$ and in turn (by universality) a $*$-homomorphism $\mathrm{GM}_n(\mathbb{K}, \mathrm{J}) \to (M_n(\mathbb{K}), \overline{}t)$. By the construction, the image of a under this mapping will not be positive semidefinite. This finishes the proof. ∎

In order to state the Positivstellensatz, we need to recall the notion of *central polynomials* for $n \times n$ matrices. These are $f \in K\langle \overline{X}, \overline{X}^* \rangle$ whose image in $\mathrm{GM}_n(K, \mathrm{J})$ is central. Equivalently, the image of f under a $*$-homomorphism from $K\langle \overline{X}, \overline{X}^* \rangle$ to $M_n(K)$ endowed with a type J involution, is always a scalar matrix. If it is nonzero, we call f *nonvanishing*. The existence of nonvanishing central polynomials is nontrivial; we refer to [Row, §1; Appendix A] for details.

Theorem 5.3 (Positivstellensatz). *Suppose $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ is endowed with the complex conjugate involution $\overline{}$. Let $g = g^* \in \mathbb{K}\langle \overline{X}, \overline{X}^* \rangle$, $n \in \mathbb{N}$ and fix a type $\mathrm{J} \in \{orthogonal, unitary\}$ according to the type of involution on $\mathbb{K}$. Choose $\alpha_1, \dots, \alpha_m \in \mathbb{K}\langle \overline{X}, \overline{X}^* \rangle$ whose images in $\mathrm{GM}_n(\mathbb{K}, \mathrm{J})$ form a diagonalisation of the quadratic form $\mathrm{Trd}(x^*x)$ on $\mathrm{UD}_n(\mathbb{K}, \mathrm{J})$. Then the following are equivalent:*

(i) *for any $s \in M_n(\mathbb{K})^{\mathbb{N}}$, $g(s, \overline{s}^t)$ is positive semidefinite;*
(ii) *there exists a nonvanishing central polynomial $h \in \mathbb{K}\langle \overline{X}, \overline{X}^* \rangle$ for $n \times n$ matrices and $p_{i,\varepsilon} \in \mathbb{K}\langle \overline{X}, \overline{X}^* \rangle$ with*

$$h^* g h \equiv \sum_{\varepsilon \in \{0,1\}^m} \alpha^\varepsilon \sum_i p_{i,\varepsilon}^* p_{i,\varepsilon} \quad (\mathrm{mod}\ \mathfrak{a}_{\mathrm{J}_n}).$$

Proof. Given a congruence as in (ii), it is clear that (i) holds whenever $h(s, \overrightarrow{s}^t) \neq 0$. As the set of all such s is Zariski dense, (i) holds for all $s \in M_n(\mathbb{K})^{\mathbb{N}}$.

For the converse implication note that by Lemma 5.2, $g + \mathfrak{a}_{J_n}$ is totally $*$-positive in $\mathrm{UD}_n(\mathbb{K}, J)$. Hence by Theorem 2.4 we obtain a positivity certificate

$$g + \mathfrak{a}_{J_n} = \sum_{\varepsilon \in \{0,1\}^m} (\alpha + \mathfrak{a}_{J_n})^\varepsilon \sum_i (x'_{i,\varepsilon})^* x'_{i,\varepsilon}$$

for some $x'_{i,\varepsilon} \in \mathrm{UD}_n(\mathbb{K}, J)$. Clearing denominators, there are $x_{i,\varepsilon} \in \mathrm{GM}_n(\mathbb{K}, J)$ and a nonzero central $r \in \mathrm{GM}_n(\mathbb{K}, J)$ with

$$r^*(g + \mathfrak{a}_{J_n})r = \sum_{\varepsilon \in \{0,1\}^m} (\alpha + \mathfrak{a}_{J_n})^\varepsilon \sum_i x^*_{i,\varepsilon} x_{i,\varepsilon}.$$

Lifting this equality to the free algebra yields the desired conclusion. ∎

When $n = 2$, the weights α are redundant (cf. §4 or [PS, p. 405]) and we obtain the following strengthening:

Corollary 5.4. *Suppose* $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ *is endowed with the complex conjugate involution* $\overline{}$. *Let* $g = g^* \in \mathbb{K}\langle \overline{X}, \overline{X}^* \rangle$, $n \in \mathbb{N}$ *and fix a type* $J \in \{orthogonal, unitary\}$ *according to the type of involution on* $\mathbb{K}$. *Then the following are equivalent:*

(i) *for any* $s \in M_2(\mathbb{K})^{\mathbb{N}}$, $g(s, \overline{s}^t)$ *is positive semidefinite;*
(ii) *there exists a nonvanishing central polynomial* $h \in \mathbb{K}\langle \overline{X}, \overline{X}^* \rangle$ *for* 2×2 *matrices and* $p_i \in \mathbb{K}\langle \overline{X}, \overline{X}^* \rangle$ *with*

$$h^* g h \equiv \sum_i p_i^* p_i \quad (\mathrm{mod} \ \mathfrak{a}_{J_2}).$$

Remark 5.5. By Tarski's transfer principle, Theorem 5.3 and Corollary 5.4 hold with $\mathbb{K}$ replaced by any real closed or algebraically closed field of characteristic 0.

We conclude the paper with an open problem: can Theorem 5.3 be used to give a proof of Helton's sum of hermitian squares theorem?

REFERENCES

[BST]   E. Bayer-Fluckiger, D.B. Shapiro, J.-P. Tignol, Hyperbolic involutions, *Math. Z.* **214** (1993), no. 3, 461–476.
[Bec]   K.J. Becher, A proof of the Pfister factor conjecture, *Invent. Math.* **173** (2008), no. 1, 1–6.
[BCR]   J. Bochnak, M. Coste, M.-F. Roy, *Real algebraic geometry*, Springer-Verlag, Berlin, 1998.

[dOHMP] M.C. de Olivera, J.W. Helton, S.A. McCullough, M. Putinar, Engineering Systems and Free Semi-Algebraic Geometry, *Emerging Applications of Algebraic Geometry*, 17–62, IMA Vol. Math. Appl. **149**, Springer, 2008.

[Djo]   D.Ž. Djoković, Positive semi-definite matrices as sums of squares, *Linear Algebra and Appl.* **14** (1976), no. 1, 37–40.

[FRS]   J.F. Fernando, J.M. Ruiz, C. Scheiderer, Sums of squares of linear forms, *Math. Res. Lett.* **13** (2006), no. 5-6, 947–956.

[GR]   D. Gondard, P. Ribenboim, Le 17e problème de Hilbert pour les matrices, *Bull. Sci. Math.* (2) **98** (1974), no. 1, 49–56.

[Hel]   J.W. Helton, "Positive" noncommutative polynomials are sums of squares, *Ann. of Math.* (2) **156** (2002), no. 2, 675–694.

[HN]   C.J. Hillar, J. Nie, An elementary and constructive solution to Hilbert's 17th problem for matrices, *Proc. Amer. Math. Soc.* **136** (2008), no. 1, 73–76.

[KS]   I. Klep, M. Schweighofer, Positivity certificates for matrix polynomials, in preparation.

[KMRT]   M.-A. Knus, A.S. Merkurjev, M. Rost, J.-P. Tignol, *The Book of Involutions*, Coll. Pub. **44**, Amer. Math. Soc., Providence, RI (1998).

[Lam]   T.Y. Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics **67**, American Mathematical Society, Providence, RI (2005).

[Lew]   D.W. Lewis, Trace forms, Kronecker sums, and the shuffle matrix, *Linear and Multilinear Algebra* **40** (1996), no. 3, 221–227.

[PD]   A. Prestel, C.N. Delzell, *Positive polynomials. From Hilbert's 17th problem to real algebra*, Springer-Verlag, Berlin, 2001.

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

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

[Wei]   A. Weil, Algebras with involutions and the classical groups, *J. Indian Math. Soc. (N.S.)* **24** 1960 589–623 (1961).

UNIVERSITY OF CALIFORNIA SAN DIEGO, DEPARTMENT OF MATHEMATICS, 9500 GILMAN DRIVE, LA JOLLA, CALIFORNIA 92093-0112, USA
   E-mail address: iklep@math.ucsd.edu

SCHOOL OF MATHEMATICAL SCIENCES, UNIVERSITY COLLEGE DUBLIN, BELFIELD, DUBLIN 4, IRELAND
   E-mail address: thomas.unger@ucd.ie