

ADDENDUM TO “FACTORING NON-NEGATIVE OPERATOR VALUED TRIGONOMETRIC POLYNOMIALS IN TWO VARIABLES”

MICHAEL DRITSCHER, IGOR KLEP, SCOTT MCCULLOUGH, AND JURIJ VOLČIČ

ABSTRACT. Factorization for positive semidefinite matrix-valued polynomials over a nonsingular compact affine real surface is established. Corollaries include Fejér–Riesz factorization for bivariate matrix polynomials that take positive semidefinite values and resolutions to questions posed by Mehta-Slofstra-Zhao and Savchuk-Schmüdgen. An explicit example shows a conclusion of [Dri25, Theorem, p. 519] that arises organically from its proof need not hold. The difficulty is traced to [Dri25, Theorem 3.7].

1. INTRODUCTION

The main result of this note, Theorem 3.1, is a factorization for positive semidefinite matrix-valued polynomials over a nonsingular compact affine surface over $\mathbb{R}$. A principal corollary is Fejér–Riesz factorization for bivariate matrix polynomials that take positive semidefinite values.

Theorem 1.1. *Given a positive integers d and n and $n \times n$ complex matrices $A_{j,k}$ for $-d \leq j, k \leq d$, if the $n \times n$ matrix-valued Laurent polynomial*

$$A(z, w) = \sum_{j,k=-d}^d A_{j,k} z^j w^k$$

satisfies, $A(z, w) \succeq 0$ for all $|z| = 1 = |w|$, then there exist positive integers e and m and $m \times n$ matrices $B_{j,k}$ for $0 \leq j, k \leq e$ such that $A(z, w) = B(z, w)^ B(z, w)$ for all $|z| = 1 = |w|$, where B is the analytic matrix-valued polynomial*

$$B(z, w) = \sum_{j,k=0}^e B_{j,k} z^j w^k.$$

The article contains two further corollaries to Theorem 3.1. Corollary 4.2 answers an open problem on positivity in tensor products from [MSZ26] that arose in quantum information theory. Corollary 4.3 asserts that $M_n(\mathbb{C}[S^2])$ admits a perfect Positivstellensatz, answering a question from [SS12, Section 11].

Theorem 1.1 is mute on degree bounds. It is known that, even in the scalar case, for a given d , no bound on e in Theorem 1.1 exists [Sce05, Corollary 5.5]. In particular, Theorem 1.1 can not hold in general with operator coefficients $A_{j,k}$. While no bound on e exists, it is still possible certain partial degree bounds can hold. However, it is shown via an explicit example that the degree bound in the statement of bivariate matrix-valued Fejér–Riesz factorization [Dri25, Theorem 4.1] that arises organically from its proof need not hold. As a related example shows, the difficulty in the proof of [Dri25, Theorem 4.1] lies in [Dri25, Theorem 3.7]. These examples appear in Section 2. The main result is developed in Section 3. The three corollaries are found in Section 4. While the examples above by no means rule out an operator-theoretic proof of

2020 *Mathematics Subject Classification.* 47A68, 14P10, 13C10 (Primary); 47B35, 13J30.

Key words and phrases. Fejér–Riesz factorization, matrix-valued polynomials, real algebraic surfaces, sum of squares, Positivstellensatz, bivariate trigonometric polynomials, projective modules over regular rings.

Theorem 1.1 in the vein of [Dri25], in the interest of correcting the record in a timely fashion, the proof given here relies on results and methods of commutative algebra and real algebraic geometry, which also generalizes to other nonsingular compact surfaces in Theorem 3.1.

Use of AI. The authors acknowledge the use of GPT-5.6 Sol and GPT-5.5 during the preparation of this note. Following the authors' identification of a flaw in the original proof, the model was utilized to explore and construct explicit counterexamples to intermediate statements and to suggest candidate arguments for the revised proof of Theorem 3.1. All counterexamples, proofs, and mathematical details were independently checked, verified, and formalized by the authors, who assume full responsibility for their mathematical correctness.

Acknowledgments. This work was performed within the project COMPUTE, which is funded within the QuantERA II Programme that has received funding from the EU's H2020 research and innovation programme under the GA No. 101017733 . IK also acknowledges support of the Slovenian Research Agency program P1-0222 and grants J1-50002, N1-0217, J1-60011, J1-50001, J1-3004 and J1-60025. JV was supported by the Marsden Fund MFP-UOA2528 from Government funding, administered by the Royal Society Te Apārangi, and the New Staff grant 3734441 by the Faculty of Science, the University of Auckland.

Thanks. The authors thank Greg Blekherman, Abhay Jindal, Michael Jury, James Pascoe, Daniel Plaumann, Rainer Sinn and Aljaž Zalar for discussions. The second and third authors also thank Jacob Levenson for discussions of and related to the many fruitful ideas in [Dri25] that led to the article [KLM+] and a follow-up currently in preparation.

2. COUNTEREXAMPLES

This section develops counterexamples to the results in [Dri25]. In the first subsection we present an example showing that the conclusion of [Dri25, Theorem 3.7] need not hold. The second subsection then develops a counterexample to the degree bound of the main result, [Dri25, Theorem 4.1].

2.1. Theorem 3.7. There is an explicit verifiable counterexample to [Dri25, Theorem 3.7] even for the case where all the coefficient Hilbert spaces are the complex numbers (one dimensional). Accordingly we restrict our attention to the case $\mathfrak{K} = \mathfrak{H} = \mathbb{C}$. To describe this setting, we use the standard notation $L^\infty = L^\infty(\mathbb{T})$ for the space of bounded measurable complex-valued functions on the unit circle $\mathbb{T}$ with respect to Lebesgue measure. Likewise, $L^2 = L^2(\mathbb{T})$ and $H^2 = H^2(\mathbb{T})$ denote the usual Hilbert space and Hardy-Hilbert space, respectively, of L^2 functions on the unit circle. In particular, H^2 consists of those L^2 functions with vanishing negative Fourier coefficients; equivalently, those L^2 functions that are the boundary values of functions analytic in the unit disk $\mathbb{D}$. An element $\varphi \in L^\infty$ induces an operator (multiplication operator) $M_\varphi : L^2 \rightarrow L^2$ by $M_\varphi f = \varphi f$, known as a bilateral Toeplitz operator. Letting $P_+ : L^2 \rightarrow H^2$ denote the orthogonal projection, the operator $T_\varphi : H^2 \rightarrow H^2$ defined by

$$T_\varphi f = P_+ \varphi f,$$

is the *unilateral Toeplitz operator with symbol φ* . The operator M_φ is the bilateral version of T_φ .

Turning to the concrete example, fix $0 < r < 1$ and let $a = 2(1 + r)$ and $b = 1 + rz$ and set $A = T_a$ and $B = T_b$. In the notation of [Dri25], the Toeplitz operator B has degree $(1, 0)$ since b , written as $b_+ + b_-$, where b_- is a conjugate analytic polynomial and b is an analytic polynomial,

the degrees of b_+ and b_- are 1 and 0, respectively. Let $M = \frac{1}{2}A$, and consider the block 2×2 matrix,

$$\begin{pmatrix} A - M & B \\ B^* & M \end{pmatrix} : \begin{matrix} H^2 & H^2 \\ \oplus & \mapsto \oplus \\ H^2 & H^2 \end{matrix}.$$

It is positive semidefinite (denoted $\succeq 0$), since pointwise for $|z| = 1$,

$$\begin{pmatrix} (1+r) & 1+rz \\ 1+r\bar{z} & (1+r) \end{pmatrix} \succeq 0.$$

Thus the pair (A, B) satisfies the hypotheses of [Dri25, Theorem 3.7].

Let $m = |b|$ and observe $0 \preceq 2T_m \preceq T_a$ since $a \geq 2m \geq 0$ pointwise. On the other hand, if $T = T_f$ is a Toeplitz operator and there a g such that $0 \leq T_g \leq T_a$, and

$$\begin{pmatrix} T_f - T_g & T_b \\ T_b^* & T_g \end{pmatrix} \succeq 0,$$

then $f \geq g \geq 0$ and at the same time $m^2 = |b|^2 \leq (f - g)g$. Thus $f \geq 2m$. Equivalently, $T_f \geq 2T_m$. It follows that, in the statement of [Dri25, Theorem 3.7], $M \in \mathcal{M} \neq \emptyset$ and $\hat{A} = 2T_m$. Moreover, with this choice of $f = 2m$, the only choice for g is m . Hence, in the statement of [Dri25, Theorem 3.7], $\hat{M} = T_m$ so that $\hat{A} - \hat{M} = \hat{M} = T_m$. To see that the claimed existence of Toeplitz operators $R_E = V_E E$ and $R_F = V_F F$ (the exact description of E, F and V_E, V_F does not play a role) satisfying

$$\hat{M} = R_F^* R_F = T_m = R_E^* R_E = \hat{A} - \hat{M}, \quad B = R_F^* R_E = T_b \quad (2.1)$$

leads to a contradiction, let u and v denote the symbols of R_E and R_F , respectively. In brief, from equation (2.1) it follows that $u^*u = v^*v = m$ and $|u^*v| = |b| = m$. Thus u and v are (pointwise a.e.) collinear, which leads to a contradiction (see the details below).

To pinpoint the difficulty in the proof of [Dri25, Theorem 3.7] and using the notation therein, where $\mathfrak{E} = \mathfrak{F} = \mathbb{C}$ and $S_E = S_F = S$ are the unilateral shifts, the coefficients of $g_n = (I - S^n S^{*n})G S^n h_{1,n}$ beyond n are 0; and not that the first n coefficients of g_n are 0, as claimed. Consequently, the claim that $(g_n)_n$ converges to 0, and hence $f_2 = 0$, is not justified. This claim is then used to show S_W is a shift, where W and S_W are constructed during the proof. We next describe this construction and show, in the present example, S_W is not a shift, using the fact S_W is a shift if and only if

$$\cap_{n=0}^{\infty} \tilde{S}^n \overline{\text{range } W} = \{0\}, \quad (2.2)$$

where $\tilde{S} = M_z$ is the bilateral shift of multiplication by z on L^2 .

The two positive Toeplitz operators $R_E^* R_E$ and $R_F^* R_F$ are the same with symbol m . The polynomial b has no zeros in a neighborhood of the closed unit disk and hence admits an (analytic) square root q . Thus,

$$|q|^2 = m = |b|$$

Choose $E = F = T_q$. Let $G = V_F^* V_E$. Then $G = T_u$ is a unilateral Toeplitz operator satisfying

$$B = F^* G E$$

as in [Dri25, Theorem 3.7]. Therefore

$$T_b = T_q^* G T_q = T_q^* T_\mu T_q = T_{\bar{q}\mu q}.$$

Thus, on the boundary of the unit disk,

$$b = \bar{q} \mu q = \mu |q|^2 = \mu m.$$

Since $m = |b|$,

$$\mu = \frac{b}{m} = \frac{b}{|b|}$$

a.e. on the boundary of the disk. Since $|\mu| = 1$ a.e., the bi-infinite multiplication operator $\tilde{G} = M_\mu$ is unitary, as claimed in the proof of [Dri25, Theorem 3.7].

Express $L^2 = H_-^2 \oplus H^2$, where H_-^2 is the orthogonal complement of H^2 in L^2 . The Hankel operator H_μ with symbol u is the operator $H_\mu : H^2 \rightarrow H_-^2$ defined by

$$H_u f = P_- u f,$$

where P_- is the orthogonal projection of L^2 onto H_-^2 . The operator $W : L^2 \rightarrow H^2 \oplus H^2$ is given in block form as

$$\begin{pmatrix} D & 0 \\ G & I \end{pmatrix} = \begin{pmatrix} H_\mu & 0 \\ T_u & I \end{pmatrix} : \begin{matrix} H^2 & H_-^2 \\ \oplus & \mapsto \oplus \\ H^2 & H^2 \end{matrix}.$$

The operator S_W is the Lowdenslager isometry associated to W . What is important here is that S_W is unitary, and not a shift, if the range of W is dense. Indeed, in this case the intersection in equation (2.2) is all of L^2 . To prove that $\text{range } W$ is dense, it suffices to show DH^2 is dense in H_-^2 . Equivalently, it suffices to show if $h \in H^2$ and $uh \in H^2$, then $h = 0$. Suppose $h \neq 0$. Since $|\mu| = 1$, h and μh would have the same boundary modulus, their outer factors are the same. Letting φ and ψ denote the inner factors of μh and h respectively,

$$\mu \psi = \varphi$$

a.e. on the boundary of the disk.¹ Hence the same is true of

$$\mu^2 \psi^2 = \varphi^2.$$

Since

$$\mu^2 = \frac{b}{\bar{b}} = \frac{1 + rz}{r + z}$$

on the boundary of the disk,

$$(1 + rz)\psi^2 = (r + z)\varphi^2$$

on the boundary of the disk, and since both $(1 + rz)\psi^2$ and $(r + z)\varphi^2$ are analytic in the disk, they are equal in the disk. But the right hand side has a zero of odd order at $-r$; whereas the left hand side has a zero of even order at $-r$, a contradiction that shows $h = 0$ and completes the proof that S_W is not a shift. It is essentially this same argument that shows colinearity of u and v together with $|u| = |v|$, which gives $g = \frac{u}{v}$ is unimodular, that produces the contradiction above.

2.2. A counterexample to degree bounds. This section presents an example where the degree bound $2d_1 - 1$ in [Dri25, Theorem 4.1] does not hold. Fix $0 < \rho < 1$ and let p and q denote the analytic polynomials in the complex variable w ,

$$p(w) = w - \rho, \quad q(w) = 1 - \rho w.$$

¹So u is a function of bounded type.

Thus,

$$\theta(w) = \frac{p(w)}{q(w)}$$

is the Blaschke factor with zero at ρ and so is unimodular on the boundary $\mathbb{T}$ of the unit disk $\mathbb{D}$ in the complex plane $\mathbb{C}$. Let

$$h(w) := q(w)^* q(w) = (1 - \rho w^{-1})(1 - \rho w) = \frac{p(w)q(w)}{w},$$

and note, for $|w| = 1$,

$$h(w) = 1 + \rho^2 - \rho w - \rho w^{-1} \in \mathbb{C}[w, w^{-1}].$$

Generally we identify hermitian squares of analytic polynomials as elements of $\mathbb{C}[w, w^{-1}]$, where $w \in \mathbb{T}$ is implicit.

Let

$$P(z, w) = h(w)I_4 + zB(w) + z^{-1}B(w)^*, \quad (2.3)$$

where,

$$B(w) = \frac{1}{\sqrt{2}w} \begin{pmatrix} 0 & 0 & 0 & p^2 \\ q^2 & 0 & p^2 & 0 \\ 0 & 0 & 0 & -q^2 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Thus $\deg_z P = \deg_w P = 1$, and B is a matrix-valued polynomial in w of degree 1.

The next proposition provides the counterexample to the degree bound in [Dri25, Theorem 4.1].

Proposition 2.1. *With the above notation, $P = G^*G$ where G is a 2×4 matrix-valued analytic polynomial with $\deg_z G = 2$,*

$$G(z, w) = \begin{pmatrix} \frac{qz}{\sqrt{2}} & \frac{p+q}{2} & \frac{pz}{\sqrt{2}} & \frac{p-q}{2}z^2 \\ \frac{qz}{\sqrt{2}} & \frac{p-q}{2} & -\frac{pz}{\sqrt{2}} & \frac{p+q}{2}z^2 \end{pmatrix}. \quad (2.4)$$

In particular $P(z, w) \succeq 0$ for all $|z| = 1 = |w|$.

Further, if n is a positive integer and F is a $n \times 4$ matrix-valued analytic polynomial such that $P = F^*F$, then $\deg_z F \geq 2$.

Before turning to the proof proper we introduce some notation and record a lemma. Let

$$B_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad M_0 = \frac{1}{2} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

In terms of the orthonormal basis

$$u_1 = e_2, \quad v_1 = \frac{e_1 + e_3}{\sqrt{2}}, \quad u_2 = \frac{e_1 - e_3}{\sqrt{2}}, \quad v_2 = e_4$$

of $\mathbb{C}^4$,

$$B_0 = u_1 v_1^* + u_2 v_2^*, \quad M_0 = v_1 v_1^* + v_2 v_2^*$$

and

$$B_0^* B_0 = M_0, \quad B_0 B_0^* = I - M_0, \quad B_0^2 = 0, \quad B_0^* u_j = v_j. \quad (2.5)$$

The following lemma exposes the key uniqueness feature of this example.

Lemma 2.2. *If M is a 4×4 matrix and*

$$J = \begin{pmatrix} I - M & B_0 \\ B_0^* & M \end{pmatrix} \succeq 0, \quad (2.6)$$

then $M = M_0$.

Proof. For $j = 1, 2$, put

$$x_j(z) = -zu_j + v_j$$

and compute $(zB_0 + z^{-1}B_0^*)x_j(z) = -x_j(z)$ for $|z| = 1$, so that

$$(I + zB_0 + z^{-1}B_0^*)x_j(z) = 0.$$

Hence

$$\langle J\gamma_j, \gamma_j \rangle = \langle (I + zB_0 + z^{-1}B_0^*)x_j, x_j \rangle = 0,$$

where

$$\gamma_j(z) = \begin{pmatrix} x_j(z) \\ zx_j(z) \end{pmatrix}.$$

Since the matrix J (of equation (2.6)) is positive semidefinite and $J\gamma_j = 0$, it follows that, for $|z| = 1$,

$$(B_0^* + zM)x_j(z) = 0.$$

On the other hand, from equation (2.5),

$$B_0^*x_j = -zv_j$$

and thus, $Mx_j(z) = v_j$; that is,

$$Mv_j = v_j = M_0v_j, \quad Mu_j = 0 = M_0u_j.$$

Because $\{u_1, u_2, v_1, v_2\}$ is a basis of $\mathbb{C}^4$, it follows that $M = M_0$. □

Proof of Proposition 2.1. Let

$$S(w) = \begin{pmatrix} \frac{q}{\theta} & 0 & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & q \end{pmatrix}.$$

Using the relations

$$p = w\bar{q}, \quad h = \bar{q}q = \frac{pq}{w}, \quad \bar{q}p = h\theta = \frac{p^2}{w}, \quad q\bar{p} = h\theta^{-1} = \frac{q^2}{w}, \quad (2.7)$$

valid for $|w| = 1$, direct computation shows, for $|z| = 1 = |w|$, that $F^*F = P$. Further, the function S satisfies $S(w)^*S(w) = hI_4$ and

$$S(w)^*B_0S(w) = \frac{1}{\sqrt{2}w} \begin{pmatrix} 0 & 0 & 0 & h\theta \\ \frac{h}{\theta} & 0 & \frac{h}{\theta} & 0 \\ 0 & 0 & 0 & h\theta \\ 0 & 0 & 0 & 0 \end{pmatrix} = B(w). \quad (2.8)$$

Arguing by contradiction, suppose there is an n and an $n \times 4$ matrix-valued analytic trigonometric polynomial

$$F(z, w) = F_0(w) + zF_1(w)$$

such that $P = F^*F$. Comparing coefficients in equation (2.3) to those of F^*F gives,

$$F_0^*F_0 = hI - M, \quad F_0^*F_1 = B,$$

where $M = F_1^* F_1$. In particular,

$$M_{j,k} = (F_1^* F_1)_{j,k} \in \mathbb{C}[w, w^{-1}] \quad (2.9)$$

for $1 \leq j, k \leq 4$ and $|w| = 1$. Let

$$G(w) := \begin{pmatrix} hI - M & B \\ B^* & M \end{pmatrix} = \begin{pmatrix} F_0^* \\ F_1^* \end{pmatrix} \begin{pmatrix} F_0 & F_1 \end{pmatrix} \succeq 0.$$

For $|w| = 1$, using equation (2.8),

$$0 \preceq \begin{pmatrix} S^{-*}(w) & 0 \\ 0 & S^{-*}(w) \end{pmatrix} G \begin{pmatrix} S^{-1}(w) & 0 \\ 0 & S^{-1}(w) \end{pmatrix} = \begin{pmatrix} I - \widetilde{M} & B_0 \\ B_0^* & \widetilde{M} \end{pmatrix} \succeq 0,$$

where $\widetilde{M} = S^{-*} M S^{-1}$. Lemma 2.2 gives, for $|w| = 1$,

$$\widetilde{M}(w) = M_0,$$

hence

$$F_1^* F_1 = M(w) = S^*(w) M_0 S(w) = \frac{1}{2} \begin{pmatrix} h & 0 & \frac{p^3}{wq} & 0 \\ 0 & 0 & 0 & 0 \\ \frac{w\bar{p}^3}{\bar{q}} & 0 & p\bar{p} & 0 \\ 0 & 0 & 0 & q\bar{q} \end{pmatrix} \quad (2.10)$$

and, comparing with equation (2.9), we have arrived at the contradiction $M_{1,3} \notin \mathbb{C}[w, w^{-1}]$. $\square$

3. AN EXACT MATRICIAL POSITIVSTELLENSATZ ON COMPACT SMOOTH REAL SURFACES

In this section we state and prove a sum-of-squares theorem for matrices over polynomials on compact smooth real surfaces. In particular, this theorem implies the matricial bivariate Fejér–Riesz theorem; see Corollary 4.1 below.

Theorem 3.1. *Let X be a nonsingular irreducible affine surface over $\mathbb{R}$ such that $X(\mathbb{R})$ is compact, and let R be the ring of real polynomial functions on X . If $A = A^* \in M_d(\mathbb{C}) \otimes_{\mathbb{R}} R$ is such that $A(p) \succeq 0$ for all $p \in X(\mathbb{R})$, then there exist $m \in \mathbb{N}$ and $B \in M_{m \times d}(\mathbb{C}) \otimes_{\mathbb{R}} R$ such that $A = B^* B$.*

Remark 3.2. *It suffices to prove the statement for real symmetric matrices over R : if $A \in \text{Sym}_d(R)$ and $A \succeq 0$ on $X(\mathbb{R})$, then $A = B^T B$ for some $B \in M_{m \times d}(R)$.*

Indeed, suppose a hermitian $\mathbf{A} \in M_d(\mathbb{C}) \otimes_{\mathbb{R}} R$ satisfies $\mathbf{A} \succeq 0$ on $X(\mathbb{R})$. There is a unitary matrix $U \in M_{2d}(\mathbb{C})$ such that

$$A := U \begin{pmatrix} \mathbf{A} & 0 \\ 0 & \overline{\mathbf{A}} \end{pmatrix} U^* \in \text{Sym}_d(R).$$

By the real statement above, $A = B^T B$ for some $B \in M_{m \times 2d}(R)$. Let $E = (I \ 0) \in M_{d \times 2d}(\mathbb{R})$; then $\mathbf{A} = EU^ AUE^T = (BUE^T)^*(BUE^T)$.*

Thus, we restrict to the real symmetric case from hereon.

Let X be as in Theorem 3.1; the proof of (the real symmetric version of) Theorem 3.1 below relies heavily on commutative algebra, so we start by underlining the properties of the ring R . Since $X \subset \mathbb{C}^n$ is defined over $\mathbb{R}$, its vanishing ideal is of the form $\mathbb{C} \otimes_{\mathbb{R}} J$ for an ideal $J \subset \mathbb{R}[x_1, \dots, x_n]$, and $R = \mathbb{R}[x_1, \dots, x_n]/J$. Then, the ring R is a noetherian domain (since X is irreducible) of dimension 2 (since X is a surface). Since X is nonsingular, R is regular, in the sense that all its localizations at prime ideals are regular local rings. Note that since R is a

domain of dimension 2, it has three kinds of prime ideals: $\{0\}$, the maximal ideals (corresponding to points in X), and the remaining ones, corresponding to irreducible curves in X , which have height one (see [Mat89, Section 5] for more on height). The latter height-one primes are crucial in the proof. Let K be the field of fractions of R ; note that K is formally real, in the sense that -1 is not a sum of squares in K . If $\mathfrak{p}$ is a height-one prime of R , then $R_{\mathfrak{p}}$ is a regular local ring of dimension 1, and thus a discrete valuation ring by [Mat89, Theorem 11.2]. Furthermore, within K ,

$$R = \bigcap_{\text{ht } \mathfrak{p}=1} R_{\mathfrak{p}} \quad (3.1)$$

by the localization intersection property for normal (and in particular, regular) noetherian domains [Mat89, Theorem 11.5].

Given symmetric $d \times d$ matrix A over R that is positive semidefinite, finding a factorization $A = B^{\top}B$ over R is guided by the following steps:

- (1) A admits a factorization $T^{\top}T$ with $m \times d$ matrix over the field K . More generally, for each curve on X , one can find such a factorization that is regular along the curve. This step relies on existing 1-dimensional sum-of-squares results, and diagonalizations over discrete valuation rings.
- (2) The image of R^d in K^m under T lies in an R -module L with two distinguished properties: L is projective, and the standard symmetric bilinear form on L has values in R . The module L is obtained by patching (akin to (3.1)) of the local modules associated with factorizations along the curves from the previous step.
- (3) Since L is projective, the standard form extends to a point-wise positive definite form on a free R -module, i.e., it is given by a positive definite matrix over R ; then a standard matricial Positivstellensatz on compact sets implies that it is a sum of hermitian squares of linear forms. Projecting back to L , we obtain a decomposition of the standard form into hermitian squares of linear forms on L .
- (4) Since the standard form on L is valued in R , the hermitian squares of linear forms specialised to the image of T are valued in R , and give rise to a decomposition of A as a sum of hermitian squares over R .

Remark 3.3. *Let us compare the above sketched proof of Theorem 3.1 with the scalar case $d = 1$, established in [Sce06, Corollary 3.6]. Both proofs rely heavily on positivity and sums of squares in local rings, and local-global patchings. However, [Sce06] utilizes localizations at maximal ideals, while the proof below relies on localizations at height-one prime ideals; consequently, the patching procedures also differ considerably.*

3.1. Rational factorizations. We first establish rational factorizations of A that are regular along given curves.

Proposition 3.4. *For every height-one prime $\mathfrak{p} \subset R$ there exist $m \in \mathbb{N}$ and $C \in M_{m \times d}(R_{\mathfrak{p}})$ such that $A = C^{\top}C$.*

Proof. Since $R_{\mathfrak{p}}$ is a discrete valuation ring, every symmetric matrix over it is congruent (over $R_{\mathfrak{p}}$) to a diagonal matrix. Namely, there exists $P \in GL_d(R_{\mathfrak{p}})$ such that $P^{\top}AP$ is a diagonal matrix. If a is its diagonal entry, then $a = u^{\top}Au$ for some $u \in R_{\mathfrak{p}}^d$. Since A is positive semidefinite on $X(\mathbb{R})$, a is a positive semidefinite element in $R_{\mathfrak{p}}$, and therefore a sum of squares in $R_{\mathfrak{p}}$ by [Sce01, Theorem 3.9] since $R_{\mathfrak{p}}$ is a discrete valuation ring (alternatively, $s^2u = v \in R^d$ for some $s \in R \setminus \mathfrak{p}$, then $s^2a = v^{\top}Av \in R$ is nonnegative on $X(\mathbb{R})$, and thus a sum of squares in R by

[Sce06, Corollary 3.4], so a is a sum of squares in $R_{\mathfrak{p}}$. Consequently, the diagonal matrix $P^{\top}AP$ factors as $B^{\top}B$ for some $B \in M_{m \times d}(R_{\mathfrak{p}})$. Then, take $C = BP^{-1}$. $\square$

By Proposition 3.4 applied to any height-one prime, there exist $m \in \mathbb{N}$ and $T \in M_{m \times d}(K)$ such that $A = T^{\top}T$. Since R is a noetherian domain, then for every nonzero $a \in R$, the height-one primes containing a are precisely the minimal primes containing a by Krull's principal ideal theorem [Mat89, Theorem 13.5], and there are only finitely many of them by [Mat89, Theorem 6.5]. By applying this fact to the denominators of entries in T , we see that they belong to only finitely many height-one primes $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ of R , which we call exceptional. For each $i = 1, \dots, s$, choose a local factorization

$$A = C_i^{\top}C_i, \quad C_i \in M_{m_i \times d}(R_{\mathfrak{p}_i})$$

from Proposition 3.4. After adding zero rows to all these matrices, we may regard T and every C_i as matrices with a common number of rows, m .

3.2. Patching local modules. Equip the vector space K^m with the standard bilinear form $\langle u, v \rangle = u^{\top}v$ and the associated quadratic form $\langle v, v \rangle$. Since K is formally real, this quadratic form is anisotropic: if $\sum_j v_j^2 = 0$, then all $v_j = 0$. For each exceptional prime $\mathfrak{p}_i$, the assignments $Tv \mapsto C_i v$ define an isometry between $\text{im}(T)$ and $\text{im}(C_i)$. Indeed, if $\langle Tv, Tv \rangle = v^{\top}Av = \langle C_i v, C_i v \rangle$, and $\ker T = \ker C$ because the standard form is anisotropic. By the Witt extension theorem [Bae78, Theorem III.4.1], there exists an orthogonal $g_i \in O_m(K)$ such that

$$g_i T = C_i. \quad (3.2)$$

For every height-one prime $\mathfrak{p}$, define an $R_{\mathfrak{p}}$ -module in K^m by

$$L_{\mathfrak{p}} = \begin{cases} g_i^{-1} R_{\mathfrak{p}_i}^m, & \mathfrak{p} = \mathfrak{p}_i, \\ R_{\mathfrak{p}}^m, & \mathfrak{p} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}. \end{cases} \quad (3.3)$$

Then,

$$TR_{\mathfrak{p}}^d \subseteq L_{\mathfrak{p}} \quad \text{for every height-one } \mathfrak{p}. \quad (3.4)$$

Indeed, if $\mathfrak{p}$ is exceptional, this holds by (3.2); if $\mathfrak{p}$ is not exceptional, then the denominators of entries in T do not lie in $\mathfrak{p}$, and are therefore invertible in $R_{\mathfrak{p}}$. Moreover, every $L_{\mathfrak{p}}$ is self-dual for the standard pairing:

$$L_{\mathfrak{p}}^{\#} := \{z \in K^m : \langle z, L_{\mathfrak{p}} \rangle \subseteq R_{\mathfrak{p}}\} = L_{\mathfrak{p}}. \quad (3.5)$$

This is clear for non-exceptional primes; for an exceptional prime $\mathfrak{p}_i$, it follows from orthogonality of g_i .

Next, define

$$L := \bigcap_{\text{ht } \mathfrak{p}=1} L_{\mathfrak{p}} \subseteq K^m. \quad (3.6)$$

By [Bou89, Theorem VII.4.3], L is a finitely generated reflexive R -module whose localization at each height-one prime $\mathfrak{p}$ equals $L_{\mathfrak{p}}$. Here, an R -module M has the dual R -module $M^* = \text{Hom}_R(M, R)$; then, M is reflexive if the natural R -module homomorphism $M \rightarrow M^{**}$ is an isomorphism. Since R is a regular ring of dimension 2, L is a finitely generated projective R -module by [Har80, Corollary 1.4].

Observe that the standard pairing on K^m restricts to an R -valued unimodular pairing on L . Indeed, for $w, z \in L$ we have $\langle w, z \rangle \in R_{\mathfrak{p}}$ for every height-one $\mathfrak{p}$ by (3.5); hence $\langle w, z \rangle \in R$ by

(3.1). Now denote

$$L^\# = \{z \in K^m : \langle z, L \rangle \subseteq R\}.$$

By the previous observation, $L \subseteq L^\#$; on the other hand, localization gives $(L^\#)_\mathfrak{p} = L_\mathfrak{p}^\# = L_\mathfrak{p}$ for all height-one primes, and so $L^\# \subseteq \bigcap_{\text{ht } \mathfrak{p}=1} L_\mathfrak{p} = L$. Therefore,

$$L^\# = L. \quad (3.7)$$

Finally, (3.4) implies

$$TR^d \subseteq L. \quad (3.8)$$

3.3. Factorization of the standard form on the patched module. Since $L \subseteq L^\#$, we have a unimodular quadratic form $h : L \rightarrow R$ on the projective module L given by $h(z) = \langle z, z \rangle$. For $p \in X(\mathbb{R})$ let $\mathbb{R}(p)$ denote $\mathbb{R}$ with the R -module structure $a \cdot \alpha = a(p)\alpha$ (i.e., $\mathbb{R}(p)$ is the residue field of R at p).

Lemma 3.5. *For $p \in X(\mathbb{R})$, the induced quadratic form $h_p : L \otimes_R \mathbb{R}(p) \rightarrow \mathbb{R}$ is positive definite.*

Proof. Let $z \in L$. Viewed in K^m , write $z = (z_1, \dots, z_m)$ and choose a common nonzero denominator $a \in R$ such that $az_i \in R$ for all i . Then

$$a^2 h(z) = \sum_{i=1}^m (az_i)^2. \quad (7.1)$$

At every $p \in X(\mathbb{R})$ such that $a(p) \neq 0$, (7.1) gives $h(z)(p) \geq 0$. The zero set of a nonzero regular function on the real surface $X(\mathbb{R})$ has empty interior; hence the set where $a \neq 0$ is dense. By continuity, $h(z)(p) \geq 0$ for every $p \in X(\mathbb{R})$. Since every element of the fiber $L \otimes_R \mathbb{R}(p) = L/\mathfrak{m}_p L$ has a representative in L , the fiber form h_p is positive semidefinite.

On the other hand, (3.7) states that the adjoint map $L \rightarrow L^*$ is an isomorphism. Tensoring with the residue field at p shows that h_p is nondegenerate, and thus positive definite. $\square$

We next convert fiber-wise positive definiteness into an algebraic Gram factorization. The compactness of $X(\mathbb{R})$ is used only in the following proposition.

Proposition 3.6. *Let P be a finitely generated projective R -module, and let $g : P \times P \rightarrow R$ be a symmetric bilinear form whose quadratic form is positive definite on every real fiber. Then there exist finitely many $\ell_1, \dots, \ell_N \in P^*$ such that*

$$g(z, z) = \sum_{j=1}^N \ell_j(z)^2 \quad \text{for all } z \in P.$$

Proof. Choose a finitely generated projective module Q with $P \oplus Q \cong R^r$. Choose generators $\mu_1, \dots, \mu_t$ of Q^* , and define

$$\gamma(y) = \sum_{j=1}^t \mu_j(y)^2.$$

The form γ is positive definite on every real fiber of Q : the reductions of the μ_j generate the dual of each fiber, so they cannot all vanish on a nonzero fiber vector.

Under an isomorphism $P \oplus Q \cong R^r$, the quadratic form $g \oplus \gamma$ is given by a symmetric matrix $H \in \text{Sym}_r(R)$, which is positive definite at every $p \in X(\mathbb{R})$. Since $X(\mathbb{R})$ is compact, there is $\rho \in \mathbb{R}$ such that $\rho^2 - \sum_{i=1}^n x_i^2$ is strictly positive on $X(\mathbb{R})$. Thus, $\rho^2 - \sum_{i=1}^n x_i^2$ is a sum of squares in R by [Scu91, Corollary 3]. This archimedean relation allows one to apply the matricial version of Putinar's Positivstellensatz [SH06, Theorem 2] to H , showing that $H = G^\top G$ for some $G \in M_{N,r}(R)$. Equivalently, $g \oplus \gamma$ is a finite sum of squares of linear functionals on

$P \oplus Q$. Restricting these functionals to the direct summand P gives the asserted representation of g . $\square$

3.4. Final step in the proof of Theorem 3.1. Let T and L be as constructed in the previous subsections. By (3.8), we view T as an R -linear map $R^d \rightarrow L$. The quadratic form $h(z) = \langle z, z \rangle$ on L is positive definite on every real fiber by Lemma 3.5. Proposition 3.6 therefore gives $\ell_1, \dots, \ell_N \in L^*$ such that

$$h(z) = \sum_{j=1}^N \ell_j(z)^2.$$

For $v \in R^d$,

$$v^\top A v = \langle T v, T v \rangle = h(T v) = \sum_{j=1}^N (\ell_j \circ T)(v)^2.$$

Each $\ell_j \circ T$ is an element of $(R^d)^*$, and hence has the form $(\ell_j \circ T)(v) = \sum_{i=1}^d b_{ji} v_i$ for some $b_{ji} \in R$. If $B = (b_{ji})$, then

$$v^\top A v = v^\top B^\top B v \quad \text{for all } v,$$

and therefore $A = B^\top B$. $\square$

4. COROLLARIES

This section contains three corollaries of Theorem 3.1. The first the matricial bivariate Fejér–Riesz theorem; the second answers an open problem on positivity in tensor products [MSZ26] that arose in quantum information theory; and the third answers a question from [SS12, Section 11] by showing $M_4(\mathbb{C}[S^1 \times S^1])$ admits a perfect Positivstellensatz.

Corollary 4.1. *If $A \in M_n(\mathbb{C}[S^1 \times S^1])$ is positive semidefinite on $S^1 \times S^1$, then there are $m \in \mathbb{N}$ and $B \in M_{m \times d}(\mathbb{C}[S^1 \times S^1])$ such that $A = B^* B$.*

Next, we apply Corollary 4.1 to an open problem on positivity in tensor products [MSZ26]. Therein, the authors consider $*$ -algebras of the form $\mathcal{A}_{m,n} := \mathbb{C}[\mathbb{Z}_m^{*n} \times \mathbb{Z}_m^{*n}]$ for $m, n \geq 2$; these are relevant in quantum information science, as they are the algebras of observables in bipartite Bell scenarios. In [MSZ26, Corollary 1.2], they show that unless $m = n = 2$, the algebra $\mathcal{A}_{m,n}$ contains a positive semidefinite element (i.e., positive semidefinite in all $*$ -representations of $\mathcal{A}_{m,n}$), but is not a sum of hermitian squares in $\mathcal{A}_{m,n}$. In [MSZ26, Example 6.8], they ask whether positive semidefinite elements in $\mathcal{A}_{2,2}$ are sums of hermitian squares.

Corollary 4.2. *If $a \in \mathcal{A}_{2,2}$ is positive semidefinite, then $a = \sum_i b_i^* b_i$ for some $b_i \in \mathcal{A}_{2,2}$.*

Proof. First, observe that $\mathbb{Z}_2 * \mathbb{Z}_2 \cong \mathbb{Z} \rtimes \mathbb{Z}_2$ (where $\mathbb{Z}_2$ acts on $\mathbb{Z}$ by changing the sign). Then, $(\mathbb{Z}_2 * \mathbb{Z}_2) \times (\mathbb{Z}_2 * \mathbb{Z}_2) \cong (\mathbb{Z} \times \mathbb{Z}) \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$, with the component-wise action α of $\mathbb{Z}_2 \times \mathbb{Z}_2$ on $\mathbb{Z} \times \mathbb{Z}$. Consequently, $\mathcal{A}_{2,2}$ is a cross product

$$\mathcal{A}_{2,2} \cong \mathbb{C}[S^1 \times S^1] \rtimes_\alpha (\mathbb{Z}_2 \times \mathbb{Z}_2).$$

Note that the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 4. By [SS12, Proposition 5.4], there is a strong conditional expectation $\vartheta : M_4(\mathbb{C}[S^1 \times S^1]) \rightarrow \mathcal{A}_{2,2}$. That is, $\mathcal{A}_{2,2}$ embeds into $M_4(\mathbb{C}[S^1 \times S^1])$, and ϑ is a unital map of $\mathcal{A}_{2,2}$ -bimodules that maps preserves sums of hermitian squares. If $a \in \mathcal{A}_{2,2}$ is positive semidefinite, then a is also positive semidefinite in $M_4(\mathbb{C}[S^1 \times S^1])$ by [SS12, Lemma 5.5]. Hence, a is a sum of hermitian squares in $M_4(\mathbb{C}[S^1 \times S^1])$ by Corollary 4.1. By applying ϑ to this decomposition, we conclude that a is a sum of hermitian squares in $\mathcal{A}_{2,2}$. $\square$

Finally, in [SS12, Section 11], the authors ask whether the $*$ -algebra $M_n(\mathbb{C}[S^2])$ admits a perfect Positivstellensatz (i.e., positive semidefinite elements are sums of hermitian squares). They also point out that a perfect Positivstellensatz for $M_2(\mathbb{C}[S^2])$ implies a perfect Positivstellensatz for the “noncommutative sphere”

$$\mathbb{C} \langle s_1, s_2, s_3 \mid s_i^* = s_i \text{ for } i = 1, 2, 3, \ s_1^2 + s_2^2 + s_3^2 = 1, \ s_i s_j = -s_j s_i \text{ for } i \neq j \rangle.$$

Theorem 3.1 applies to $X = \{x_1^2 + x_2^2 + x_3^2 = 1\}$, whose real points form the sphere S^2 , and we obtain the following.

Corollary 4.3. *If $A \in M_n(\mathbb{C}[S^2])$ is positive semidefinite on S^2 , then A is a sum of hermitian squares in $M_n(\mathbb{C}[S^2])$.*

REFERENCES

- [Bou89] N. Bourbaki: *Commutative Algebra. Chapters 1–7*, Elem. Math., Springer-Verlag, Berlin, 1989.
- [Bae78] R. Baeza: *Quadratic forms over semilocal rings*, Lecture Notes in Math. 655, Springer-Verlag, Berlin-New York, 1978.
- [Dri25] M. Dritschel, *Factoring non-negative operator valued trigonometric polynomials in two variables*, Math. Ann. 391, 515–537 (2025). <https://doi.org/10.1007/s00208-024-02895-9>
- [Har80] R. Hartshorne: *Stable reflexive sheaves*, Math. Ann. 254 (1980) 121–176.
- [KLM+] I. Klep, J. Levenson and S. McCullough, *Fejér–Riesz factorization for positive noncommutative trigonometric polynomials*, arXiv:2511.09267.
- [Mat89] H. Matsumura: *Commutative ring theory*, Cambridge Stud. Adv. Math. 8, Cambridge University Press, Cambridge, 1989.
- [MSZ26] A. Mehta, W. Slofstra, Y. Zhao: *Positivity is undecidable in tensor products of free algebras*, J. Eur. Math. Soc. (2026) doi:10.4171/JEMS/1786.
- [SS12] Y. Savchuk, K. Schmüdgen: *Positivstellensätze for algebras of matrices*, Linear Algebra Appl. 436 (2012) 758–788.
- [Sce01] C. Scheiderer: *On sums of squares in local rings*, J. reine angew. Math. 540 (2001) 205–227.
- [Sce05] C. Scheiderer: *Non-existence of degree bounds for weighted sums of squares representations*, J. Complexity 21 (2005) 823–844.
- [Sce06] C. Scheiderer: *Sums of squares on real algebraic surfaces*, Manuscripta Math. 119 (2006) 395–410.
- [SH06] C. W. Scherer, C. W. J. Hol: *Matrix sum-of-squares relaxations for robust semi-definite programs*, Math. Prog. 107 (2006) 189–211.
- [Scu91] K. Schmüdgen: *The K -moment problem for compact semi-algebraic sets*, Math. Ann. 289 (1991) 203–206.
- [Voi21] J. Voight: *Quaternion algebras*, Grad. Texts in Math. 288, Springer, Cham, 2021.

SCHOOL OF MATHEMATICS, STATISTICS AND PHYSICS, HERSCHEL BUILDING, UNIVERSITY OF NEWCASTLE, NEWCASTLE UPON TYNE NE1 7RU, UK

Email address: michael.dritschel@ncl.ac.uk

UNIVERSITY OF LJUBLJANA, FACULTY OF MATHEMATICS AND PHYSICS, JADRANSKA 21, 1000 LJUBLJANA & UNIVERSITY OF PRIMORSKA, FACULTY OF MATHEMATICS, NATURAL SCIENCES AND INFORMATION TECHNOLOGIES, GLAGOLJAŠKA 8, 6000 KOPER, SLOVENIA.

Email address: igor.klep@fmf.uni-lj.si

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF FLORIDA, GAINESVILLE, FL

Email address: sam@ufl.edu

THE UNIVERSITY OF AUCKLAND, DEPARTMENT OF MATHEMATICS, PRIVATE BAG 92019, AUCKLAND 1142, NEW ZEALAND.

Email address: jurij.volcic@auckland.ac.nz