LowRankUnivariateSOS

Chenyang Yuan

August 19, 2026

Chapter 1

Proof Outline

This blueprint documents the Lean package `LowRankUnivariateSOS`. It is intended to be self-contained at the level of the formal proof strategy: the optimization model, the algebraic reductions, the hgroup step, and the factor-peeling transport are all stated here in the same order in which the formal proof uses them.

The endpoint is the theorem `rankTwo_no_spurious_socp` in `RankTwoMain.lean`. The Lean statement is slightly stronger than the one in the paper: it is proved for an arbitrary positive-definite bilinear form on the polynomial space, not just for one fixed inner product.

This is the final formal claim.

Theorem 1. *For every sum-of-squares polynomial p and every second-order critical point $u = (u_1, u_2)$ of the quadratic-penalty objective,*

$$\sigma(u) - p = 0.$$

Equivalently,

$$\sigma(u) = p,$$

so every SOCP is globally optimal.

1.1 Optimization Model

This definition fixes the objective and the exact FOCP/SOCP equations.

Definition 2. The formal model is defined in `PolynomialModel.lean` and `Socp.lean`. For a pair of polynomials $u = (u_1, u_2)$,

$$\sigma(u) = u_1^2 + u_2^2, \qquad A_u(v) = u_1 v_1 + u_2 v_2, \qquad \text{residual}(p, u) = \sigma(u) - p.$$

The objective is

$$f_p(u) = \langle \sigma(u) - p, \sigma(u) - p \rangle.$$

The FOCP condition is

$$\forall v, \qquad \langle A_u(v), \sigma(u) - p \rangle = 0.$$

In Lean this is `IsFOCP`. The Hessian quadratic form is

$$\text{hessianTerm}(p, u, v) = \langle \sigma(v), \sigma(u) - p \rangle + 2\|A_u(v)\|^2.$$

The SOCP condition is the FOCP condition together with

$$\forall v, \qquad 0 \le \mathrm{hessianTerm}(p, u, v).$$

In the kernel directions used later in the proof,

$$A_u(v) = 0 \quad \Longrightarrow \quad 0 \le \langle \sigma(v), \sigma(u) - p \rangle.$$

In Lean this full condition is `IsSOCP`.

This is the abstract inequality package used at the end of the proof.

Proposition 3. *Write*

$$r = \sigma(u) - p.$$

Then the SOCP conditions give

$$\forall q \in \mathrm{im}(A_{u_{\mathrm{img}}}), \qquad \langle q, r \rangle = 0$$

for the transformed image used later in the proof, and

$$\forall w \in \ker(A_u), \qquad 0 \le \langle \sigma(w), r \rangle.$$

So if one can prove

$$p = q_{\mathrm{img}} + \sum_i \sigma(w_i), \qquad q_{\mathrm{img}} \in \mathrm{im}(A_{u_{\mathrm{img}}}), \qquad w_i \in \ker(A_u),$$

then

$$0 \le \langle p, r \rangle = \langle q_{\mathrm{img}}, r \rangle + \sum_i \langle \sigma(w_i), r \rangle.$$

Evaluating the FOCP condition at $v = u$ gives

$$\langle \sigma(u), r \rangle = 0,$$

hence

$$f_p(u) = \langle r, r \rangle = \langle \sigma(u) - p, r \rangle = -\langle p, r \rangle \le 0.$$

Since always $f_p(u) \ge 0$, it follows that

$$f_p(u) = 0, \qquad r = 0.$$

This is exactly the abstract content of `factored_h1_residual_eq_zero`.

1.2 Reduced Factorization

This is the first algebraic reduction.

Proposition 4. *Lean constructs a decomposition*

$$u = a \cdot u_0, \qquad \gcd(u_{0,1}, u_{0,2}) = 1.$$

In Lean this is the structure `ReducedFactorization` produced by `gcd_sigma_decomposition`. The companion theorem `no_real_roots_sigma_reduced` proves

$$\forall x \in \mathbb{R}, \qquad \sigma(u_0)(x) \neq 0.$$

So the common factor of u_1, u_2 is isolated in a, while the reduced pair u_0 is coprime and its sum of squares has no real roots.

This separates the common factor into the good part and the peelable part.

Proposition 5. *Assume $a \neq 0$. Then Lean produces a factorization*

$$a = g_{\text{base}} \prod_i r_i$$

such that

$$\forall i, \qquad r_i \mid \sigma(u_0), \qquad \gcd(g_{\text{base}}, \sigma(u_0)) = 1.$$

The peeled terminal factor is

$$g = \text{peelTerminalScale}(g_{\text{base}}, [r_1, \dots, r_n]),$$

and satisfies

$$\gcd(g, \sigma(u_0)) = 1.$$

Informally, each bad factor r_i is replaced by one copy of X^2, while the coprime part g_{base} is kept unchanged.

1.3 The hgroup Step and the $h = 1$ Case

This definition records the explicit image and kernel generators used in the $h = 1$ argument.

Definition 6. The basic constructions are

$$\text{scalePair}(g, u) = (gu_1, gu_2), \qquad \text{perpPair}(t, u) = (-tu_2, tu_1).$$

They satisfy

$$A_{gu}(\text{perpPair}(t, u)) = 0, \qquad \sigma(\text{perpPair}(t, u)) = t^2 \sigma(u).$$

Hence if

$$s = q_1^2 + q_2^2,$$

then

$$s\,\sigma(u) = \sigma(\text{perpPair}(q_1, u)) + \sigma(\text{perpPair}(q_2, u)),$$

so $s\,\sigma(u)$ lies in the cone generated by kernel squares. On the image side, coprimality gives Bézout surjectivity:

$$\gcd(u_1, u_2) = 1 \quad \Longrightarrow \quad \forall q\ \exists v,\ A_u(v) = q.$$

Therefore

$$\forall q\ \exists v,\ A_{gu}(v) = gq.$$

This is the algebraic division step behind the paper's hgroup argument.

Lemma 7. *If p and q are SOS polynomials and $\gcd(g, q) = 1$, then there exist s, t such that*

$$p = g\,t + s\,q, \qquad s \text{ is SOS.}$$

Lean proves this by choosing Bézout coefficients

$$ag + bq = 1$$

and defining

$$s = b^2 pq, \qquad t = p(2a - a^2 g).$$

Then

$$g\,t + s\,q = p(g(2a - a^2 g) + b^2 q^2) = p(ag(2 - ag) + (bq)^2) = p,$$

using $bq = 1 - ag$. *The SOS claim for* s *is exactly*

$$b^2 \text{ is SOS}, \quad p \text{ is SOS}, \quad q \text{ is SOS} \quad \Longrightarrow \quad b^2 pq \text{ is SOS},$$

formalized by `isSOS_mul`.

This converts the hgroup identity into the paper's image-plus-cone condition.

Proposition 8. *Assume*

$$\gcd(u_{0,1}, u_{0,2}) = 1, \qquad p = g\,q + s\,\sigma(u_0), \qquad s \text{ is SOS}.$$

Then

$$gq \in \mathrm{im}(A_{gu_0}), \qquad s\,\sigma(u_0) \in \mathrm{cone}(\sigma(\ker(A_{gu_0}))),$$

and therefore

$$p \in \mathrm{im}(A_{gu_0}) + \mathrm{cone}(\sigma(\ker(A_{gu_0}))).$$

This is the formal $h = 1$ *reduction used later by the abstract SOCP argument.*

1.4 Factor Peeling

This definition packages the one-parameter family used in a single peeling step.

Definition 9. A peeling witness is a family v_η satisfying

$$A_u(v_\eta) = a_{\mathrm{const}}, \qquad \sigma(v_\eta) = \eta^2 q_{\mathrm{quad}} + 2\eta q + \sigma_{\mathrm{const}},$$

with

$$q_{\mathrm{quad}} \in \mathrm{im}(A_{u_{\mathrm{img,prev}}}).$$

So the quadratic coefficient is already controlled by the previous stage, while the linear coefficient is the new target q. Lean stores the local step in `PeelingStepWitness` and `RotatedPeelingData`. The recursive transport is stored in

`HasPeelingWitness`, `PeelingPath`, `PeelingSchedule`.

This is the one-factor orthogonality transport.

Proposition 10. *Assume one quadratic factor step*

$$g_{\mathrm{next}}\, r = X^2 g_{\mathrm{start}}, \qquad r \mid \sigma(u_0), \qquad r \mid g_{\mathrm{start}}.$$

Let

$$q \in \mathrm{im}(A_{g_{\mathrm{next}} u_0}), \qquad A_{g_{\mathrm{next}} u_0}(b) = q,$$

and define

$$\mathrm{quad} = \mathrm{perpPair}(1, g_{\mathrm{next}} u_0), \qquad \mathrm{const} = \mathrm{perpPair}(1, b), \qquad v_\eta = \eta\ \mathrm{quad} + \mathrm{const}\,.$$

Then

$$A_u(v_\eta) = A_u(\mathrm{const}),$$

and

$$\sigma(v_\eta) = \eta^2\sigma(\text{quad}) + 2\eta q + \sigma(\text{const}).$$

Moreover,

$$\sigma(\text{quad}) \in \text{im}(A_{g_{\text{start}}u_0}),$$

because r divides both $\sigma(u_0)$ and g_{start}. If the previous image is already orthogonal to the residual r_{res}, then the SOCP inequality gives

$$0 \le \langle \sigma(v_\eta), r_{\text{res}}\rangle + 2\langle A_u(v_\eta), A_u(v_\eta)\rangle = 2\eta\langle q, r_{\text{res}}\rangle + C$$

for all real η. Hence

$$\langle q, r_{\text{res}}\rangle = 0.$$

This is the content of `dot_eq_zero_of_peeling_step`*; the theorem* `image_orthogonal_of_peeling_step` *upgrades it from one polynomial q to the entire next image.*

This iterates the one-factor transport along the whole bad factor.

Proposition 11. *Starting from*

$$a = g_{\text{base}} \prod_i r_i,$$

Lean builds a peeling schedule

$$au_0 \rightsquigarrow (X^2 g_{\text{base}} r_2 \cdots r_n)u_0 \rightsquigarrow \cdots \rightsquigarrow gu_0.$$

Orthogonality propagates at each arrow by Proposition 10. Therefore the final theorem `factor_peeling_image_orthog` *gives*

$$\exists g \neq 0, \qquad \gcd(g, \sigma(u_0)) = 1, \qquad \forall q \in \text{im}(A_{gu_0}),\ \langle q, \sigma(u) - p\rangle = 0.$$

This is the Lean form of the paper's factor-peeling conclusion.

1.5 Final Assembly

This packages exactly the algebraic data needed by Proposition 3.

Proposition 12. *Start from*

$$u = au_0.$$

If

$$a = 0,$$

then the residual vanishes directly from the SOCP inequalities. If

$$a \neq 0,$$

then factor peeling gives

$$\gcd(g, \sigma(u_0)) = 1, \qquad \forall q \in \text{im}(A_{gu_0}),\ \langle q, \sigma(u) - p\rangle = 0.$$

Applying Lemma 7 with $q = \sigma(u_0)$ gives

$$p = g\,q' + s\,\sigma(u_0), \qquad s \text{ is SOS.}$$

So `rankTwo_factored_h1_setup` *returns exactly the package*

$$u = au_0, \qquad p = g\,q' + s\,\sigma(u_0), \qquad \gcd(g, \sigma(u_0)) = 1, \qquad \langle \text{im}(A_{gu_0}), \sigma(u) - p\rangle = 0.$$

1.6 How the Proof Concludes

This is the final substitution into the abstract SOCP inequality.

From Proposition 12 and Proposition 8, the polynomial p has the form

$$p = q_{\text{img}} + \sum_i \sigma(w_i), \qquad q_{\text{img}} \in \text{im}(A_{gu_0}), \qquad w_i \in \ker(A_{au_0}).$$

So Proposition 3 applies and gives

$$\sigma(u) - p = 0.$$

The theorem `rankTwo_no_spurious_socp` is therefore the short chain

reduced factorization $\Longrightarrow$ factor peeling $\Longrightarrow$ hgroup+$h = 1$ $\Longrightarrow$ image-plus-cone $\Longrightarrow$ $\sigma(u)-p = 0$.