UNIVARIATE RATIONAL SUMS OF SQUARES

TERESA KRICK, BERNARD MOURRAIN, AND AGNES SZANTO

Abstract. Given rational univariate polynomials f and g such that $\gcd(f,g)$ and $f/\gcd(f,g)$ are relatively prime, we show that g is non-negative on all the real roots of f if and only if g is a sum of squares of rational polynomials modulo f. We complete our study by exhibiting an algorithm that produces a certificate that a polynomial g is non-negative on the real roots of a non-zero polynomial f, when the above assumption is satisfied.

Keywords. Positive polynomials; Sum of Squares; Semi-Definite Matrix; Convex cone; Real roots; Exact computation; Certificate;

1. Introduction

It is a classical result that a real univariate polynomial is *non-negative on all* $\mathbb{R}$ if and only if it is a sum of squares of real polynomials (and in fact, 2 polynomials are enough). It was then proved by Landau in 1905, see [6], that every univariate polynomial with *rational coefficients* which is non-negative on all $\mathbb{R}$ is a sum of 8 squares of *rational polynomials* (this result was improved in [11], lowering the bound of 8 to the optimal value of 5).

We call this the *global case*, when we consider non-negativity on all $\mathbb{R}$. The *local case* is when we consider analogous questions for a polynomial which is non-negative on the real roots of another non-zero polynomial. More explicitly, the corresponding statement is: Given a non-zero polynomial $f \in \mathbb{R}[x]$, is it true that a polynomial $g \in \mathbb{R}[x]$ is non-negative on all the real roots of f if and only if it is congruent modulo f to a sum of squares of polynomials in $\mathbb{R}[x]$? That is, if there exist polynomials $h_i \in \mathbb{R}[x]$, $1 \le i \le N$ for some $N \in \mathbb{N}$, such that

$$h := \sum_{i=1}^{N} h_i^2 \quad \text{satisfies} \quad h \equiv g \mod f.$$

In [9], P. Parrilo gives a very simple construction that shows that this is indeed the case in a zero-dimensional radical setting of multivariate

The research of Teresa Krick is partly supported by CONICET PIP-11220130100073CO and BID-PICT 2018-02315. The work of Bernard Mourrain is partly supported by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Actions, grant agreement 813211 (POEMA). The research of Agnes Szanto is partly supported by NSF grant CCF-1813340.

polynomials. In our specific setting his result shows that every $g \in \mathbb{R}[x]$ which is non-negative on all the real roots of a *squarefree* polynomial $f \in \mathbb{R}[x]$ is congruent modulo f to a sum of squares of real polynomials. In this paper, we consider the corresponding *rational* question: Given polynomials $f, g \in \mathbb{Q}[x]$ such that g is non-negative on all the real roots of f, is it true that g is congruent modulo f to a sum of squares of polynomials $h_i \in \mathbb{Q}[x]$? Note that this is equivalent to say that g is congruent modulo f to a *rational positive weighted sum* of squares of polynomials in $\mathbb{Q}[x]$, that is, that there exist $\omega_i \in \mathbb{Q}_+$ and $h_i \in \mathbb{Q}[x]$, $1 \le i \le N$, such that

$$h := \sum_{i=1}^{N} \omega_i \, h_i^2 \quad \text{satisfies} \quad h \equiv g \mod f, \tag{1}$$

since for $\omega_i = m/n \in \mathbb{Q}$ with $m, n \in \mathbb{N}$, $\omega_i h_i^2 = mn(h_i/n)^2$.

The positive weighted sum of squares h is commonly called a *sum of squares (SOS) decomposition* of g modulo f, and such a decomposition, together with the polynomial $q \in \mathbb{Q}[x]$ such that $g = h + q\, f$ is a *certificate* of the non-negativity of g on the real roots of f.

The existence and computation of rational SOS decompositions of positive polynomials has been investigated in the univariate case for instance in [2], [8], or in the multivariate case in [10], [4]. A counter-example in [13] shows that, in the multivariate case, a rational polynomial which is a sum of squares of real polynomials cannot always be decomposed as a rational sum of squares. In [5], [3], rational Artin's type certificates of positivity, that is, fractions of two rational weighted sums of squares polynomials are considered.

In [7], algorithms to compute positivity certificates and bounds on their bit complexity and the size of their output are presented, including Artin's type certificates and rational weighted sums of squares certificates for positive polynomials on compact basic semi-algebraic sets. The algorithms work under some strictly positivity assumptions. They involve numeric-symbolic tools such as the perturbation algorithm of [2], the rounding-projection algorithm of [10] or Semi-Definite Programming solvers.

In this paper, we first show, by a direct method, that a rational univariate polynomial g, strictly positive on the real roots of a rational squarefree polynomial f, admits a rational SOS decomposition modulo f. This can be seen as a very very special case of Putinar's Theorem [12] over *rational* numbers. We extend the result to rational univariate polynomials g that are non-negative at the roots of f, under an assumption specified in our main result:

Theorem. *Let $f \in \mathbb{Q}[x]$ be a non-zero polynomial of degree n and $g \in \mathbb{Q}[x]$ be such that $\gcd(f, g)$ and $f/\gcd(f, g)$ are relatively prime. Assume that g is non-negative on all the real roots of f. Then there* *exist rational positive weights* $\omega_i \in \mathbb{Q}_+$ *and rational polynomials* $h_i \in \mathbb{Q}[x]$ *of degree* $< n$, $1 \le i \le N$ *for some* $N \in \mathbb{N}$, *such that*

$$h := \sum_{i=1}^{N} \omega_i \, h_i^2 \quad \textit{satisfies} \quad h \equiv g \mod f.$$

Note that when f is squarefree, our assumption on $\gcd(f,g)$ and $f/\gcd(f,g)$ being relatively prime is automatically satisfied. Furthermore, this assumption seems to be optimal in order for such an SOS decomposition to exist, as the following example demonstrates [9, Remark 1]: For $f = x^2$ and $g = x$, g is non-negative on all the (real) roots of f but there is no such SOS decomposition. Note that in this case $\gcd(f,g) = x = f/\gcd(f,g)$ and the polynomials f and g do not satisfy the assumption of our theorem.

The proof of our theorem is developed in Section 2. It proceeds by first tackling in Subsection 2.1 the case when g is strictly positive on all the real roots of a squarefree polynomial f of degree n: by modifying the construction in [9], we first show there always exists a *real* SOS decomposition h of g modulo f,

$$h = [1, x, \dots, x^{n-1}] \, Q \, [1, x, \dots, x^{n-1}]^T$$

with $Q \in \mathbb{R}^{n \times n}$ symmetric and *positive definite*. This enables us to perturb the real coefficients in matrix Q in order to turn them rational, while keeping the condition of remaining an SOS decomposition for g modulo f, as done in [10] for the global case (with the difference that here we know there always exists such a positive definite real matrix). In a second step, Subsection 2.2 deals with the case of a non squarefree polynomial f, applying Hensel lifting and Chinese Remainder Theorem recombination. We finally relax the strictly positive condition to non-negative under our assumption.

In this paper, we also address the following algorithmic question: Can we produce an algorithm that computes a rational SOS certificate, which size is related to the geometry of the input polynomials?

Several algorithms can be used to certify that a polynomial g is non-negative at the roots of f. We refer to [1] for a general presentation of these algorithms, based for instance on Sturm-Habicth sequences or isolation of real roots.

The algorithm that we describe in Section 3 does not require to isolate or approximate the roots of f. It computes a certificate of non-negativity by computing an SOS decomposition of g modulo f using two main ingredients. The first ingredient is an adaptation of the rounding-projection algorithm of [10] to the case of a rational polynomial g strictly positive on the real roots of a squarefree polynomial f, following the proof of Proposition 2.7. The second ingredient is a reduction of the general case when $\gcd(f,g)$ and $f/\gcd(f,g)$ are relatively prime, to the strictly positive case, then lifting the rational SOS decompositions via Hensel lifting and Chinese Remainder Theorem, following the proof of our main theorem.

Acknowledgment. We thank the organizers of the MCA 2021 session “Symbolic computation: theory, algorithms and applications”, Alicia Dickenstein, Alexey Ovchinnikov and Veronika Pillwein, who invited Agnes Szanto to submit a publication related to her talk to the Revista de la Unión Matemática Argentina, that started this collaboration and research project.

2. Existence of a rational SOS decomposition

2.1. The squarefree and strictly positive case.

In this section we assume that $f \in \mathbb{R}[x]$ is a squarefree polynomial and that $g \in \mathbb{R}[x]$ is strictly positive on the real roots of f. We fix the following notation.

Notation 2.1. We denote

$$f = \sum_{i=0}^{n} f_i\, x^i = f_n(x-\xi_1)\cdots(x-\xi_n) \ \text{ with } \ \xi_i \neq \xi_j \in \mathbb{C} \ \text{ for } \ i \neq j,$$

where $\xi_1, \dots, \xi_k$ are the real roots of f (for some $0 \le k \le n$) while the complex non-real roots are labeled as ξ_{k+2i-1}, ξ_{k+2i} with $\xi_{k+2i-1} = \overline{\xi_{k+2i}}$ for $1 \le i \le \frac{n-k}{2}$.

The Lagrange basis for $\xi_1, \dots, \xi_n$ is denoted by $u_1, \dots, u_n \in \mathbb{C}[x]$, i.e.

$$u_i = \prod_{j \neq i} \frac{x-\xi_j}{\xi_i - \xi_j} = \frac{f}{f'(\xi_i)(x-\xi_i)} \quad \text{for } 1 \le i \le n. \tag{2}$$

It satisfies that for any polynomial $p \in \mathbb{C}[x]$ one has

$$p(x) \equiv \sum_{i=1}^{n} p(\xi_i)\, u_i(x) \mod f. \tag{3}$$

The basis $u_1, \dots, u_n$ is also defined by the conditions $\deg(u_i) \le n-1$, $1 \le i \le n$ and $u_i(\xi_j) = \delta_{i,j}$ for $1 \le i, j \le n$. This implies by (3) that

$$u_i^2 \equiv u_i \mod f \ \text{ for } 1 \le i \le n \ \text{ and } \ u_i u_j \equiv 0 \mod f \ \text{ for } i \neq j. \tag{4}$$

Given $g \in \mathbb{R}[x]$, Parrilo constructed in [9] the following real polynomial

$$\begin{aligned}\sum_{i=1}^{k} g(\xi_i)\, u_i^2 + \sum_{i=1}^{(n-k)/2} &\Big(\sqrt{g(\xi_{k+2i})}u_{k+2i} + \sqrt{g(\overline{\xi_{k+2i}})}\overline{u_{k+2i}}\Big)^2 \\ &= \sum_{i=1}^{n} g(\xi_i)\, u_i^2 + 2 \sum_{i=1}^{(n-k)/2} |g(\xi_{k+2i})|\, u_{k+2i-1} u_{k+2i},\end{aligned} \tag{5}$$

where the identity follows from the fact that the interpolation polynomials associated to the complex non-real roots of f are pairwise conjugate, i.e. $\overline{u_{k+2i}} = u_{k+2i-1}$.

This polynomial is a sum of squares in $\mathbb{R}[x]$ whenever g is non-negative on the real roots of f, as shown by identity (5), since for $1 \le i \le \frac{n-k}{2}$,

$$\sqrt{g(\xi_{k+2i})}u_{k+2i} + \sqrt{g(\overline{\xi_{k+2i}})}\,\overline{u_{k+2i}} = 2\Re(\sqrt{g(\xi_{k+2i})}u_{k+2i}),$$

where $\Re$ denotes the real part. Furthermore, it is congruent to g modulo f since by (4) and (3) we have

$$\sum_{i=1}^{n} g(\xi_i)\, u_i^2 + 2\sum_{i=1}^{(n-k)/2} |g(\xi_{k+2i})|\, u_{k+2i-1}u_{k+2i} \equiv \sum_{i=1}^{n} g(\xi_i)\, u_i \equiv g \mod f.$$

Inspired by this construction, we define for fixed $\lambda_i \in \mathbb{R}$, $1 \le i \le \frac{n-k}{2}$, the polynomial

$$h = \sum_{i=1}^{n} g(\xi_i)\, u_i^2 + 2\sum_{i=1}^{(n-k)/2} \lambda_i\, u_{k+2i-1}u_{k+2i} \tag{6}$$

which is also congruent to g modulo f for any choice of λ_i, $1 \le i \le \frac{n-k}{2}$.

Next proposition shows that for a range of values of λ_i, this polynomial h is a sum of n linearly independent squares.

Proposition 2.2. *Let $f \in \mathbb{R}[x]$ be a squarefree polynomial as in Notation 2.1 and let $g \in \mathbb{R}[x]$ be such that $g(\xi_i) > 0$ for $1 \le i \le k$.*
Fix $\lambda_i > |g(\xi_{k+2i})|$, $1 \le i \le \frac{n-k}{2}$, and let

$$h = \sum_{i=1}^{n} g(\xi_i)\, u_i^2 + 2\sum_{i=1}^{(n-k)/2} \lambda_i\, u_{k+2i-1}u_{k+2i}$$

be the polynomial h defined in (6), which is congruent to g modulo f. Then h is a positive weighted sum of n squares of linearly independent real polynomials of degree strictly bounded by n. More precisely,

$$h = \sum_{i=1}^{n} \omega_i\, h_i^2 \tag{7}$$

where

- $h_i = u_i$ *and* $\omega_i = g(\xi_i)$ *for* $1 \le i \le k$,
- $h_{k+2i-1} = \Re(u_{k+2i}) - \dfrac{\Im(g(\xi_{k+2i}))}{\lambda_i + \Re(g(\xi_{k+2i}))}\,\Im(u_{k+2i})$,

  $h_{k+2i} = \dfrac{\sqrt{\lambda_i^2 - |g(\xi_{k+2i})|^2}}{\lambda_i + \Re(g(\xi_{k+2i}))}\Im(u_{k+2i})$,

  and $\omega_{k+2i-1} = \omega_{k+2i} = 2\,(\lambda_i + \Re(g(\xi_{k+2i})))$ *for* $1 \le i \le \frac{n-k}{2}$.

(Here $\Re$ and $\Im$ denote real and imaginary part respectively.)

Proof. We first show that the expressions in (6) and (7) coincide.

Set $\gamma_i := g(\xi_{k+2i})$ for $1 \le i \le \frac{n-k}{2}$. Applying the identity

$$\begin{aligned}
&(a+\mathbf{i}\,b)(u+\mathbf{i}\,v)^2 + (a-\mathbf{i}\,b)(u-\mathbf{i}\,v)^2 + 2\,\lambda|u+\mathbf{i}\,v|^2\\
&= \; 2\left((\lambda+a)\,u^2 - 2\,b\,u\,v + (\lambda-a)\,v^2\right)\\
&= \; 2(\lambda+a)\left((u-\frac{b}{\lambda+a}\,v)^2 + (\lambda^2-a^2-b^2)\,(\frac{v}{\lambda+a})^2\right)
\end{aligned}$$

for $\lambda + a \neq 0$, we get from Identity (6):

$$\begin{aligned}
h = &\sum_{i=1}^{k} g(\xi_i)\,u_i^2 + \sum_{i=1}^{(n-k)/2}\left(\gamma_i\,u_{k+2i}^2 + \overline{\gamma}_i\,\overline{u_{k+2i}}^2 + 2\,\lambda_i\,|u_{k+2i}|^2\right)\\
= &\sum_{i=1}^{k} g(\xi_i)\,u_i^2\\
&+ \sum_{i=1}^{(n-k)/2} 2\,(\lambda_i + \Re(\gamma_i))\left(\Re(u_{k+2i}) - \frac{\Im(\gamma_i)}{\lambda_i+\Re(\gamma_i)}\,\Im(u_{k+2i})\right)^2\\
&+ \sum_{i=1}^{(n-k)/2} 2\,(\lambda_i + \Re(\gamma_i))\left(\frac{\sqrt{\lambda_i^2-|\gamma_i|^2}}{\lambda_i+\Re(\gamma_i)}\Im(u_{k+2i})\right)^2
\end{aligned}$$

since $\lambda_i > |\gamma_i|$ implies $\lambda_i + \Re(\gamma_i) \neq 0$ and $\lambda_i^2 - |\gamma_i|^2 > 0$.

Now, observe that $\omega_i > 0$ since for $1 \le i \le k$, $\omega_i := g(\xi_i) > 0$ by assumption, and for $1 \le i \le \frac{n-k}{2}$, $\omega_{k+2i-1} = \omega_{k+2i} := 2(\lambda_i + \Re(\gamma_i)) > 0$. Therefore h is a positive weighted sum of n squares of polynomials of degree $< n$ with real coefficients.

Finally, as the polynomials u_i are linearly independent over $\mathbb{C}$ and $u_{k+2i-1} = \overline{u_{k+2i}}$, the real polynomials

$$u_1, \ldots, u_k, \Re(u_{k+2}), \Im(u_{k+2}), \ldots, \Re(u_n), \Im(u_n)$$

are also linearly independent. This implies that the real polynomials $h_1, \ldots, h_n$ are also linearly independent over $\mathbb{R}$ (and in particular non-zero). □

We fix the following notation for the rest of the paper:

Notation 2.3. We set $S^n(\mathbb{R})$ for the set of symmetric matrices in $\mathbb{R}^{n\times n}$ and $S^n_+(\mathbb{R})$ for its cone of symmetric positive semidefinite matrices. We equip $S^n(\mathbb{R})$ with the Frobenius inner product $\langle A, B\rangle = \mathrm{trace}(A\,B)$, $\forall A, B \in S^n(\mathbb{R})$, which induces the Frobenius norm $\|\cdot\|$. The 2-norm on the coefficients of polynomials in $\mathbb{R}[x]$ is also denoted by $\|\cdot\|$. For $m \in \mathbb{N}_0$ we set $\mathbb{R}[x]_m$ for the set of polynomials of degree bounded by m. Finally, $\mathbf{x} = [1, x, \ldots, x^{n-1}]^T$ is the column vector of monomials of degree $< n$.

Note that for any polynomial $p = \sum_{i=0}^{d} p_i x^i$, one has

$$\begin{aligned} \|p\, f\| \le \sum_{i=0}^{d} \|p_i x^i f\| \ &\le\ \sum_{i=0}^{d} |p_i|\, \|x^i f\| \\ \le \sum_{i=0}^{d} \|p\|\, \|f\| \ &\le\ (d+1)\|p\|\, \|f\|. \end{aligned} \tag{8}$$

As a first corollary of Proposition 2.2, we have:

Corollary 2.4. *Let $f, g \in \mathbb{R}[x]$ with f of degree n with simple roots ξ_i, $1 \le i \le n$, and g of degree $< n$ that is strictly positive on the real roots $\xi_1, \dots, \xi_k$ of f. Then, there exists a pair $(Q, q) \in S^n(\mathbb{R}) \times \mathbb{R}[x]_{n-2}$ with Q* positive definite *such that $g = \mathbf{x}^T Q \mathbf{x} + q\, f$.*
In particular $Q \in \operatorname{Int}(S^n_+(\mathbb{R}))$, where Int *denotes interior.*

Proof. For fixed $\lambda_i > |g(\xi_i)|$, $1 \le i \le \frac{n-k}{2}$, let H be the coefficient matrix of the polynomials $h_1, \dots, h_n$ of Proposition 2.2 in the monomial basis $1, x, \dots, x^{n-1}$, so that

$$[h_1, \dots, h_n] = \mathbf{x}^T H. \tag{9}$$

The matrix H is invertible since $h_1, \dots, h_n$ are linearly independent. Let Δ be the diagonal matrix

$$\Delta = \operatorname{diag}(\omega_1, \dots, \omega_n). \tag{10}$$

Then (7) rewrites as

$$h = \mathbf{x}^T H \Delta H^T \mathbf{x} = \mathbf{x}^T Q\, \mathbf{x} \tag{11}$$

where $Q := H\Delta H^T$ is positive definite since H is invertible and $\omega_i > 0$ for $1 \le i \le n$. Also, as $h \equiv g \mod f$ and $\deg(h) \le 2n-2$, there exists $q \in \mathbb{R}[x]_{n-2}$ such that $g = h + q\, f$.
Finally $Q \in \operatorname{Int}(S^n_+(\mathbb{R}))$ since $\det(Q) > 0$. ☐

Note that when $\lambda_i = |g(\xi_{k+2i})|$, which is the case in Parrilo's polynomial (5), $h_{k+2i} = 0$ and therefore these polynomials h_i, $1 \le i \le n$, are not linearly independent. This means that Parrilo's polynomial (5) lies in the border of the cone $S^n_+(\mathbb{R})$. What we were able to do in Proposition 2.2 is to modify Parrilo's construction in order to obtain a polynomial h in the interior of this cone. This gives room to perturb it a little in order to get a rational polynomial with the same characteristics, and yields the particular version of our main theorem when g is strictly positive on all the real roots of a squarefree polynomial f.

To describe this construction, we introduce the following ingredients.

Notation 2.5. Let $p = p_0 + p_1 x + \cdots + p_{2n-2} x^{2n-2} \in \mathbb{R}[x]$. We define the affine space

$$\mathcal{Q}_p = \{Q \in S^n(\mathbb{R}) \ :\ \mathbf{x}^T Q\, \mathbf{x} = p\},$$

and the symmetric matrix

$$Q_p = \begin{bmatrix} p_0 & \frac{p_1}{2} & \frac{p_2}{3} & \cdots & \frac{p_{n-2}}{n-1} & \frac{p_{n-1}}{n} \\ \frac{p_1}{2} & \frac{p_2}{3} & & \iddots & \frac{p_{n-1}}{n} & \frac{p_n}{n-1} \\ \frac{p_2}{3} & & \iddots & \iddots & \iddots & \vdots \\ \vdots & \iddots & \iddots & \iddots & \iddots & \frac{p_{2n-4}}{3} \\ \frac{p_{n-2}}{n+1} & \frac{p_{n-1}}{n} & \iddots & & \frac{p_{2n-4}}{3} & \frac{p_{2n-3}}{2} \\ \frac{p_{n-1}}{n} & \frac{p_n}{n-1} & \cdots & \frac{p_{2n-4}}{3} & \frac{p_{2n-3}}{2} & p_{2n-2} \end{bmatrix}, \tag{12}$$

which satisfies

$$\mathbf{x}^T Q_p \mathbf{x} = \sum_{k=0}^{2n-2} p_k x^k = p, \tag{13}$$

and therefore $Q_p \in \mathcal{Q}_p$.

We note for further use that we have

$$\|Q_p\| = \Big(\sum_{k=0}^{2n-2} s_k \Big(\frac{p_k}{s_k}\Big)^2\Big)^{1/2} \le \Big(\sum_{k=0}^{2n-2} p_k^2\Big)^{1/2} = \|p\|, \tag{14}$$

where

$$s_k = s_{2n-2-k} = k+1, \quad 0 \le k \le n-1, \tag{15}$$

denotes the number of entries in each of the $2n-1$ antidiagonals of Q_p.

We now describe the orthogonal projection from $S^n(\mathbb{R})$ on $\mathcal{Q}_p$ for the Frobenius norm, in a more convenient matrix formulation for the univariate case than in [10, Prop.7], and prove it for sake of completeness.

Lemma 2.6. *The map*

$$\pi_p : S^n(\mathbb{R}) \longrightarrow \mathcal{Q}_p \quad , \quad Q \longmapsto Q - Q_{\mathbf{x}^T Q \mathbf{x} - p}$$

is the orthogonal projection onto the affine space $\mathcal{Q}_p$ for the norm $\|\cdot\|$.

Proof. Let $Q \in S^n(\mathbb{R})$. By (13), we have:

$$\mathbf{x}^T \pi_p(Q)\, \mathbf{x} = \mathbf{x}^T Q \mathbf{x} - (\mathbf{x}^T Q \mathbf{x} - p) = p,$$

and thus $\pi_p(Q) \in \mathcal{Q}_p$.

To prove that $\pi_p(Q)$ is the orthogonal projection of Q on $\mathcal{Q}_p$, we show that $Q - \pi_p(Q)$ is orthogonal to $\mathcal{Q}_p$:
We first observe that for any $Q \in S^n(\mathbb{R})$,

$$\mathbf{x}^T Q \mathbf{x} = \sum_{k=0}^{2n-2} \Big(\sum_{i+j=k+2} Q_{i,j}\Big) x^k = \sum_{k=0}^{2n-2} \langle Q, H_k \rangle x^k,$$

where for $0 \leq k \leq 2n-2$, $H_k \in S^n(\mathbb{R})$ is the Hankel matrix such that $(H_k)_{i,j} = 1$ if $i+j = k+2$ and 0 otherwise, $1 \leq i, j \leq n$. This shows that the affine space $\mathcal{Q}_p$ is defined by the equations

$$\langle Q, H_k \rangle - p_k = 0, \quad k = 0, \dots, 2n-2,$$

which implies that the vector space $\mathcal{Q}_p^{\perp}$ orthogonal to $\mathcal{Q}_p$ is spanned by $(H_k)_{0 \leq k \leq 2n-2}$.
On another hand we can easily verify from its definition that

$$Q_p = \sum_{k=0}^{2n-2} \frac{p_k}{s_k} H_k,$$

where s_k is defined in (15). Therefore,

$$Q - \pi_p(Q) = Q_{\mathbf{x}^T Q \mathbf{x} - p} = \sum_{k=0}^{2n-2} \big(\langle Q, H_k \rangle - \frac{p_k}{s_k}\big) H_k,$$

which shows that $Q - \pi_p(Q)$ is a linear combination of $(H_k)_{0 \leq k \leq 2n-2}$, and thus orthogonal to $\mathcal{Q}_p$. □

We are going to use this projection to compute a rational sum of squares modulo f for a polynomial g strictly positive at the real roots of f.

Proposition 2.7. *Let $f \in \mathbb{Q}[x]$ be a non-zero squarefree polynomial and $g \in \mathbb{Q}[x]$ be such that g is strictly positive on all the real roots of f. Then there exist polynomials $h_i \in \mathbb{Q}[x]$ of degree $< n$ and positive weights $\omega_i \in \mathbb{Q}_+$, $1 \leq i \leq n$, such that*

$$h := \sum_{i=1}^{n} \omega_i h_i^2 \quad \textit{satisfies} \quad h \equiv g \mod f.$$

Proof. There is a natural proof of this proposition which makes use of the fact that the set

$$\{(A, b) \in S^n(\mathbb{R}) \times \mathbb{R}[x]_{n-2} : \, g = \mathbf{x}^T A \mathbf{x} + b\, f\}$$

is a real affine space which in the case that $f, g \in \mathbb{Q}[x]$ is defined by a rational basis and a rational particular point. This approach follows the proof of the analogous result for the global case mentioned as *image representation* in [10, Section 3.2].

Here, we give the proof that uses the orthogonal projection π_p defined in Definition 2.5, as done for the global case in the *kernel representation* in [10, Section 3.1].

Without loss of generality we can assume that $\deg(g) < n$ by replacing it by its remainder modulo f.

Let (Q^*, q^*) be given by Corollary 2.4, i.e. $g = \mathbf{x}^T Q^* \mathbf{x} + q^* f$ and $Q^* \in \mathrm{Int}(S_+^n(\mathbb{R}))$, and let $\sigma > 0$ be the smallest eigenvalue of Q^*, which is the distance of Q^* to the set of singular matrices, so that the open ball centered at Q^* and of radius σ is contained in $S_+^n(\mathbb{R})$.

Take a rational approximation $(\overline{Q}, q) \in S^n(\mathbb{Q}) \times \mathbb{Q}[x]_{n-2}$ such that

$$\|\overline{Q} - Q^*\| < \frac{\sigma}{2} \quad \text{and} \quad \|q - q^*\| < \frac{\sigma}{2(n-1)\|f\|}. \tag{16}$$

The problem is that most surely, $\mathbf{x}^T \overline{Q} \mathbf{x} + q\, f \neq g$.

Let $e := \mathbf{x}^T \overline{Q} \mathbf{x} + qf - g$ be the error polynomial, and define

$$Q := \pi_{g-qf}(\overline{Q}) = \overline{Q} - Q_e \in S^n(\mathbb{Q}),$$

which is the orthogonal projection of $\overline{Q}$ on $\mathcal{Q}_{g-qf}$ according to Lemma 2.6. Then $Q \in \mathcal{Q}_{g-qf}$, i.e. $\mathbf{x}^T Q \mathbf{x} + qf = g$.

Next we prove that $Q \in \mathrm{Int}(S_+(\mathbb{Q}))$ by proving that $\|Q - Q^*\| < \sigma$. We have

$$\begin{aligned}
\|Q - Q^*\| &\leq \|\pi_{g-q\,f}(\overline{Q}) - \pi_{g-q\,f}(Q^*)\| + \|\pi_{g-q\,f}(Q^*) - Q^*\| \\
&\leq \|\pi_{g-q\,f}(\overline{Q}) - \pi_{g-q\,f}(Q^*)\| + \|\pi_{g-q\,f}(Q^*) - \pi_{g-q^*\,f}(Q^*)\| \\
&\leq \|\overline{Q} - Q^*\| + \|Q^* - Q_{\mathbf{x}^T Q^* \mathbf{x} - (g - q\,f)} - \big(Q^* - Q_{\mathbf{x}^T Q^* \mathbf{x} - (g - q^*\,f)}\| \\
&\leq \|\overline{Q} - Q^*\| + \|Q_{(q^* - q)\,f}\|,
\end{aligned}$$

since $\mathbf{x}^T Q^* \mathbf{x} + q^* g = g$ implies $Q^* = \pi_{g-q^* f}(Q^*)$.

By (14) and (8) we have

$$\|Q_{(q^*-q)\,f}\| \leq \|(q^* - q)\,f\| \leq (n-1)\|q^* - q\|\,\|f\|$$

since $\deg(q^* - q) \leq 2n - 2$. Finally, by (16), we conclude

$$\|Q - Q^*\| < \frac{\sigma}{2} + (n-1)\frac{\sigma}{2(n-1)\|f\|}\,\|f\| = \sigma.$$

This implies that $Q \in \mathrm{Int}(S_+^n(\mathbb{R}))$, i.e. $h = \mathbf{x}^T Q\,\mathbf{x}$ is a rational positive weighted sum of squares. □

Example 2.8. We now consider a toy example to illustrate our construction. This is a toy example because in this case we know the roots of f and use that knowledge, as in the proof or our existential theorem. Let $f = x^3 - 2 = (x - 2^{1/3})(x - 2^{1/3}\omega)(x - 2^{1/3}\overline{\omega})$, where $\omega = e^{2\pi \mathbf{i}/3}$, and $g = x$, which is strictly positive on $2^{1/3}$. Set $\xi_1 = 2^{1/3}$, $\xi_2 = 2^{1/3}\omega$ and $\xi_3 = \overline{\xi_2}$.

Parrilo's construction (5) gives in this case the following real polynomial, which is congruent to g modulo f and a sum of 2 squares:

$$g(\xi_1)\underbrace{u_1(x)}_{\in \mathbb{R}[x]}{}^2 + \underbrace{\Big(\sqrt{g(\xi_2)}u_2(x) + \sqrt{g(\xi_3)}u_3(x)\Big)^2}_{\in \mathbb{R}[x]} \;=\; \mathbf{x}^T Q^*\,\mathbf{x}$$

where

$$Q^* = \begin{bmatrix} \frac{2\sqrt[3]{2}}{9} & \frac{2}{9} & -\frac{\sqrt[3]{4}}{18} \\ \frac{2}{9} & \frac{\sqrt[3]{4}}{18} & -\frac{\sqrt[3]{2}}{18} \\ -\frac{\sqrt[3]{4}}{18} & -\frac{\sqrt[3]{2}}{18} & \frac{5}{18} \end{bmatrix}.$$

Note that Q^* is a rank 2 positive semidefinite matrix, which therefore lies in the border of the cone of positive semidefinite matrices.

Now, if we take $\lambda := 2|g(\xi_2)| = 2 \cdot 2^{1/3}$ in our construction (6), we get $h^* = \mathbf{x}^T Q^* \mathbf{x}$ where

$$Q^* = \begin{bmatrix} \frac{4\sqrt[3]{2}}{9} & \frac{1}{9} & -\frac{\sqrt[3]{4}}{9} \\ \frac{1}{9} & \frac{2\sqrt[3]{4}}{9} & -\frac{\sqrt[3]{2}}{9} \\ -\frac{\sqrt[3]{4}}{9} & -\frac{\sqrt[3]{2}}{9} & \frac{7}{18} \end{bmatrix}$$

is a (rank 3) definite positive matrix with smallest eigenvalue $\sigma \sim 0.2239$, and

$$g = \mathbf{x}^T Q^* \mathbf{x} + q^* f \quad \text{for} \quad q^* = -\frac{7}{18}x + \frac{2\sqrt[3]{2}}{9}.$$

Here, if we take the following rational approximations of Q^* and q^* (rounding to two significant digits)

$$\overline{Q} = \begin{bmatrix} 0.6 & 0.1 & -0.2 \\ 0.1 & 0.4 & -0.1 \\ -0.2 & -0.1 & 0.4 \end{bmatrix} \quad \text{and} \quad q = -0.4x + 0.3$$

we get that $\|Q^* - \overline{Q}\| \cong 0.0923$ and $\|q^* - q\| \cong 0.0229$. Thus, we have $\|Q^* - \overline{Q}\| < \frac{\sigma}{2} \cong 0.112$ and $\|q^* - q\| < \frac{\sigma}{2(n-1)\|f\|} \cong 0.025$ respectively, satisfying both of the bounds given in (16) required in the proof of Proposition 2.7. We have $\mathbf{x}^T \overline{Q}\, \mathbf{x} + q\, f = 0.1x^3 + x \neq g$, with error

$$e = \mathbf{x}^T \overline{Q}\, \mathbf{x} + q\, f - g = 0.1x^3.$$

Compute the orthogonal projection of $\overline{Q}$ on $\mathcal{Q}_{g-qf}$:

$$Q = \pi_{g-qf}(\overline{Q}) = \overline{Q} - Q_e = \begin{bmatrix} 0.6 & 0.1 & -0.2 \\ 0.1 & 0.4 & -0.15 \\ -0.2 & -0.15 & 0.4 \end{bmatrix}$$

so that $\mathbf{x}^T \overline{Q}\, \mathbf{x} - \mathbf{x}^T Q\, \mathbf{x} = e$ and Q is still a definite positive matrix. Then matrix $Q \in S^3(\mathbb{Q})$ satisfies

$$h := \mathbf{x}^T Q\, \mathbf{x} = \mathbf{x}^T \overline{Q}\, \mathbf{x} - e = g - q\, f \equiv g \mod f,$$

and h is a sum of squares of rational polynomials, which we can obtain for example using the exact LU-decomposition of Q as follows:

$$h = \frac{3}{5}\left(1 + \frac{1}{6}x - \frac{1}{3}x^2\right)^2 + \frac{23}{60}\left(x - \frac{7}{23}x^2\right)^2 + \frac{137}{460}x^4.$$

2.2. **The general case.** In this subsection we generalize the results of the previous section to the case when f is non-necessarily squarefree and g is non-negative on all the real roots of f (but might vanish on some of them), as long as $\gcd(f, g)$ and $f/\gcd(f, g)$ are relatively prime, in order to obtain our main theorem.

We will need the following auxiliary results, namely Hensel lemma and Chinese remainder theorem.

Lemma 2.9. *Let $p, g \in \mathbb{Q}[x]$ with p irreducible in $\mathbb{Q}[x]$ which does not divide g. Assume that there exists $\overline{h}_1, \dots, \overline{h}_N \in \mathbb{Q}[x]$ and $\omega_1 \dots, \omega_N \in \mathbb{Q}_+$ for some $N \in \mathbb{N}$ with $\deg(\overline{h}_i) < \deg(p)$ such that*

$$g \equiv \sum_{i=1}^{N} \omega_i \overline{h}_i^2 \mod p.$$

Then for any fixed $e \in \mathbb{N}$, $e \geq 1$, there exist $h_1, \dots, h_N \in \mathbb{Q}[x]$ with $\deg(h_i) < e \cdot \deg(p)$ such that

$$g \equiv \sum_{i=1}^{N} \omega_i h_i^2 \mod p^e.$$

Proof. We show that it suffices to perform Hensel lifting on one of the polynomials $\overline{h}_i$. Since $p \in \mathbb{Q}[x]$ is irreducible and does not divide g, one of the $\overline{h}_i$ at least is not divisible by p, and w.l.o.g. we assume that it is $\overline{h}_1$.

Define

$$\overline{g} = \frac{g}{\omega_1} \quad \text{for} \quad N = 1 \quad \text{and} \quad \overline{g} := \frac{g - \sum_{i=2}^{N} \omega_i \overline{h}_i^2}{\omega_1} \in \mathbb{Q}[x] \quad \text{for} \quad N > 1.$$

Then $\overline{g} \equiv \overline{h}_1^2 \mod p$, and we define the following Newton iteration starting from $h_1^{(0)} := \overline{h}_1$:

(17)
$$h_1^{(k+1)} \equiv \frac{1}{2}\Big(h_1^{(k)} + \frac{\overline{g}}{h_1^{(k)}}\Big) \equiv \frac{1}{2}\Big(h_1^{(k)} + s_1^{(k)}\,\overline{g}\Big) \mod p^{2^{k+1}} \quad \text{for } k \geq 0,$$

where $s_1^{(k)} \in \mathbb{Q}[x]$ is defined by $s_1^{(k)}\,h_1^{(k)} \equiv 1 \mod p^{2^{k+1}}$.

First note that this sequence is well defined in $\mathbb{Q}[x]$ since by induction,

$$h_1^{(k)} \equiv \frac{1}{2}\Big(h_1^{(0)} + \frac{\big(h_1^{(0)}\big)^2}{h_1^{(0)}}\Big) \equiv h_1^{(0)} \mod p,$$

and therefore $h_1^{(k)}$ is prime to the irreducible polynomial p since $h_1^{(0)}$ is, and hence invertible modulo $p^{2^{k+1}}$.

We now prove by induction that $\big(h_1^{(k)}\big)^2 \equiv \overline{g} \mod p^{2^k}$:

First, from (17) we derive

$$h_1^{(k)}\,h_1^{(k+1)} \equiv \frac{1}{2}\Big(\big(h_1^{(k)}\big)^2 + \overline{g}\Big) \mod p^{2^{k+1}}. \tag{18}$$

Now, by the inductive hypothesis, $\big(h_1^{(k)}\big)^2 \equiv \overline{g} \mod p^{2^k}$ implies that

$$\begin{aligned} h_1^{(k+1)} &\equiv \frac{1}{2}\Big(h_1^{(k)} + s_1^{(k)}\,\big(h_1^{(k)}\big)^2\Big) \mod p^{2^k} \\ &\equiv \frac{1}{2}\Big(h_1^{(k)} + h_1^{(k)}\Big) \equiv h_1^{(k)} \mod p^{2^k}. \end{aligned}$$

Therefore, $h_1^{(k)} = h_1^{(k+1)} + t\,p^{2^k}$ for some $t \in \mathbb{Q}[x]$ and from (18),

$$\begin{aligned}\big(h_1^{(k+1)} + t\,p^{2^k}\big)h_1^{(k+1)} &\equiv \frac{1}{2}\Big(\big(h_1^{(k+1)} + t\,p^{2^k}\big)^2 + \overline{g}\Big) \mod p^{2^{k+1}} \\ &\equiv \frac{1}{2}\Big(\big(h_1^{(k+1)}\big)^2 + 2t\,p^{2^k}h_1^{(k+1)} + \overline{g}\Big) \mod p^{2^{k+1}}\end{aligned}$$

and we can cancel $t\,p^{2^k}h_1^{(k+1)}$ from both sides. We conclude

$$\big(h_1^{(k+1)}\big)^2 \equiv \frac{1}{2}\Big(\big(h_1^{(k+1)}\big)^2 + \overline{g}\Big) \mod p^{2^{k+1}}$$

which implies

$$\big(h_1^{(k+1)}\big)^2 \equiv \overline{g} \mod p^{2^{k+1}}.$$

Going back to the definition of $\overline{g}$,

$$g = \omega_1\overline{g} + \sum_{i=2}^{N}\omega_i\overline{h}_i^2 \equiv \omega_1\big(h_1^{(k)}\big)^2 + \sum_{i=2}^{N}\omega_i\overline{h}_i^2 \mod p^{2^k}.$$

Finally, if we choose k such that $2^{k-1} < e \leq 2^k$ and define $h_1 := h_1^{(k)} \mod p^e$, $h_i := \overline{h}_i$ for $2 \leq i \leq N$ and $\omega_1, \dots, \omega_N$ unchanged then we get the sum of squares decomposition of g modulo p^e with the desired degree bounds.

∎

Lemma 2.10. *Let $f_1, \dots, f_r \in \mathbb{Q}[x]$ with $\gcd(f_i, f_j) = 1$ for $1 \leq i < j \leq r$. Assume that $g \in \mathbb{Q}[x]$ satisfies*

$$g \equiv \sum_{j=1}^{N_i}\omega_{i,j}h_{i,j}^2 \mod f_i, \quad 1 \leq i \leq r,$$

for some $N_i \in \mathbb{N}$, $h_{i,j} \in \mathbb{Q}[x]$ with $\deg(h_{i,j}) < \deg f_i$ and $\omega_{i,j} \in \mathbb{Q}_+$, for $1 \leq j \leq N_i$. Then there exist $N \in \mathbb{N}$, $h_1, \dots, h_N \in \mathbb{Q}[x]$ and $\omega_1, \dots, \omega_N \in \mathbb{Q}_+$ such that

$$g \equiv \sum_{i=1}^{N}\omega_i h_i^2 \mod \Big(\prod_{i=1}^{r} f_i\Big).$$

Furthermore, $\deg(h_i) < \sum_{i=1}^{r}\deg(f_i)$ for $1 \leq i \leq N$.

Proof. The usual Chinese remainder theorem for a system

$$g \equiv g_i \mod f_i,\ 1 \leq i \leq r,$$

admits the solution (c.f. [14, Algorithm 5.4])

$$g \equiv s_1 f^{(1)}g_1 + \cdots + s_r f^{(r)}g_r \mod f$$

where $f := \prod_{i=1}^{r} f_i$, $f^{(i)} := \prod_{j\neq i} f_j$ and s_i is defined by $s_i f^{(i)} + t_i f_i = 1$ for $1 \leq i \leq r$.

On another side, notice that

$$s_i f^{(i)} \equiv (s_i f^{(i)})^2 \mod f,\ 1 \leq i \leq r,$$

since $s_i f^{(i)} \equiv 1 \mod f_i$ and $s_i f^{(i)} \equiv 0 \mod f_j$ for $j \neq i$. Then

$$g \equiv (s_1 f^{(1)})^2 g_1 + \cdots + (s_r f^{(r)})^2 g_r \mod f.$$

In our setting, since $g_i := \sum_{j=1}^{N_i} \omega_{i,j} h_{i,j}^2$ we get

$$\begin{aligned} g &\equiv \sum_{i=1}^{r} (s_i f^{(i)})^2 \Big(\sum_{j=1}^{N_i} \omega_{i,j} h_{i,j}^2 \Big) \mod f \\ &\equiv \sum_{i=1}^{r} \sum_{j=1}^{N_i} \omega_{i,j} (s_i f^{(i)} h_{i,j})^2 \mod f. \end{aligned}$$

We get $N := \sum_{i=1}^{r} N_i$ and reduce $s_i f^{(i)} h_{i,j}$ modulo f to achieve the desired degree bounds in the SOS decomposition. □

We are now able to prove the full version of our theorem. We repeat the statement here for the reader's convenience.

Theorem. *Let $f \in \mathbb{Q}[x]$ be a non-zero polynomial of degree n and $g \in \mathbb{Q}[x]$ be such that $\gcd(f, g)$ and $f/\gcd(f, g)$ are relatively prime. Assume that g is non-negative on all the real roots of f. Then there exist polynomials $h_i \in \mathbb{Q}[x]$ of degree $< n$ and positive weights $\omega_i \in \mathbb{Q}_+$, $1 \leq i \leq N$ for some $N \in \mathbb{N}$, such that*

$$h := \sum_{i=1}^{N} \omega_i h_i^2 \quad \textit{satisfies} \quad h \equiv g \mod f.$$

Proof. First assume that $\gcd(f, g) = 1$. Note that therefore, the assumption that g is non-negative on the real roots of f implies that g is strictly positive on the real roots of f.

W.l.o.g. we can assume that f is monic. Suppose f has the following decomposition over $\mathbb{Q}$ into powers of irreducible factors in $\mathbb{Q}[x]$

$$f = p_1^{e_1} \cdots p_r^{e_r}$$

where p_i are distinct monic irreducible polynomials in $\mathbb{Q}[x]$, $e_i \in \mathbb{N}$ for $1 \leq i \leq r$, and $\sum_{i=1}^{r} e_i \deg(p_i) = n$.

Fix $i \in \{1, \ldots, r\}$. Since g is strictly positive on the real roots of the irreducible polynomial p_i, we can apply Proposition 2.7 to p_i and g, which shows the existence of $\overline{h}_{i,j} \in \mathbb{Q}[x]$ of degree $< N_i := \deg(p_i)$ and $\omega_{i,j} \in \mathbb{Q}_+$ for $1 \leq i \leq N_i$, such that

$$g \equiv \sum_{j=1}^{N_i} \omega_{i,j} \overline{h}_{i,j}^2 \mod p_i.$$

Next we apply Lemma 2.9 with $p = p_i$ and $e = e_i$ to show the existence of $h_{i,j} \in \mathbb{Q}[x]$ of degree $< e_i \deg(p_i)$, $1 \le i \le N_i$, such that

$$g \equiv \sum_{j=1}^{N_i} \omega_{i,j}\, h_{i,j}^2 \mod p_i^{e_i}. \tag{19}$$

Finally we apply Lemma 2.10 with $f_i = p_i^{e_i}$ for $1 \le i \le r$ to combine the congruences in (19) and obtain $N \in \mathbb{N}$, $h, h_1, \ldots, h_N \in \mathbb{Q}[x]$ and $\omega_1, \ldots, \omega_N \in \mathbb{Q}_+$ such that

$$h := \sum_{i=1}^{N} \omega_i\, h_i^2 \quad \text{satisfies} \quad h \equiv g \mod f.$$

Furthermore, $\deg(h_i) < \sum_{i=1}^{r} e_i \deg(p_i) = n$ for $1 \le i \le N$. This proves the claim for an arbitrary polynomial f with $\gcd(f, g) = 1$.

Assume now that $d := \gcd(f, g) \neq 1$. We show that under our assumption $\gcd(f/d, d) = 1$, there is a polynomial $b \in \mathbb{Q}[x]$ relatively prime to f/d which satisfies that $b\, d^2 \equiv g \mod f$ and therefore b is strictly positive on the roots of f/d:

The assumption implies that $\gcd(f/d, g) = 1$, and therefore g is strictly positive on all the real roots of f/d. Since $\gcd(f/d, d^2) = 1$ as well, there exist $s, t \in \mathbb{Q}[x]$ s.t.

$$1 = s \cdot \frac{f}{d} + t \cdot d^2.$$

This implies in particular $\gcd(f/d, t) = 1$ and that

$$g = s \cdot \frac{g}{d} \cdot f + (tg) \cdot d^2. \tag{20}$$

We set $b := tg$. Then b and f/d are relatively prime since t and f/d, and g and f/d are. Therefore b is striclty positive on all the real roots of f/d because for any such root ξ, $d(\xi) \neq 0$, $b(\xi) \neq 0$ and $b(\xi)d^2(\xi) = g(\xi) \ge 0$.

Finally, (20) implies that $b\, d^2 \equiv g \mod f$.

We then apply our previous construction to b and f/d: There exist $\overline{h}_i \in \mathbb{Q}[x]$ of degree $< n - \deg(d)$ and $\omega_i \in \mathbb{Q}_+$, $1 \le i \le N$, such that

$$\overline{h} := \sum_{i=1}^{N} \omega_i \overline{h}_i^2 \quad \text{satisfies} \quad \overline{h} \equiv b \mod \frac{f}{d}.$$

Therefore,

$$d^2\, \overline{h} = \sum_{i=1}^{N} \omega_i\, (d\, \overline{h}_i)^2 \quad \text{and} \quad d^2 \overline{h} \equiv b\, d^2 \mod f.$$

Since $b\, d^2 \equiv g \mod f$ we conclude that

$$d^2 \overline{h} \equiv g \mod f.$$

We note that $\deg(d\,\overline{h}_i) < n$, thus $h := d^2\overline{h}$, $h_i := d\,\overline{h}_i$ and ω_i, $1 \le i \le N$, satisfy the claim of the theorem. $\square$

Example 2.11. Let us again consider a toy example to show how it works when $\gcd(f,g) \neq 1$ and f is not squarefree.

Consider $f = x(x^3-2)^2$ and $g = x^3$. Here $d = \gcd(f,g) = x$ and $f/d = (x^3-2)^2$ are relatively prime, so we are in the assumptions of our theorem.

In this case, as $g/d^2 = x$ is already a polynomial, we can take $tg = g/d^2 = x$.

(1) Find rational SOS for $g/d^2 = x$ modulo (x^3-2) (see Example 2.8):

$$x \equiv \frac{3}{5}\left(1+\frac{1}{6}x-\frac{1}{3}x^2\right)^2 + \frac{23}{60}\left(x-\frac{7}{23}x^2\right)^2 + \frac{137}{460}x^4 \mod (x^3-2).$$

(2) Apply Hensel lifting to find rational SOS for $g/d^2 = x$ modulo $(x^3-2)^2$ (note that we lift only the last term):

$$\begin{aligned} x \equiv{}& \frac{3}{5}\left(1+\frac{1}{6}x-\frac{1}{3}x^2\right)^2 + \frac{23}{60}\left(x-\frac{7}{23}x^2\right)^2 \\ &+ \frac{137}{460}\left(\frac{-46}{137}x^5+\frac{69}{274}x^4+\frac{229}{137}x^2-\frac{69}{137}x\right)^2 \mod (x^3-2)^2, \end{aligned}$$

i.e. $x \equiv \omega_1\overline{h}_1^2 + \omega_2\overline{h}_2^2 + \omega_3\overline{h}_3^2 \mod f/d = (x^3-2)^2$.

(3) Multiply both sides by $d^2 = x^2$:

$$g \equiv \omega_1(x\overline{h}_1)^2 + \omega_2(x\overline{h}_2)^2 + \omega_3(x\overline{h}_3)^2 \mod f = x(x^3-2)^2.$$

3. Algorithm

In this section, we describe the algorithm announced in the introduction, that computes a certificate of non-negativity of a polynomial $g \in \mathbb{Q}[x]$ on the real roots of another polynomial $f \in \mathbb{Q}[x]$, addressing the algorithmic question in the introduction.

3.1. **Certificate for a strictly positive polynomial.** Here we assume that $f \in \mathbb{Q}[x]$ is a *squarefree* polynomial of degree n, and that g is *strictly positive* on all the real roots of f.

We consider the following optimization problem

$$\begin{array}{ll} \inf & 1 \\ \text{s.t.} & Q \succcurlyeq 0 \\ & q \in \mathbb{R}[x]_{n-2} \\ & g = \mathbf{x}^T Q\,\mathbf{x} + q\,f \end{array} \tag{21}$$

where $\mathbf{x} = [1,\dots,x^{n-1}]^T$ is the vector of monomials of degree $< n$ and $Q \in S^n(\mathbb{R})$. The feasibility set

$$\mathcal{C} = \{(Q,q) \in S^n(\mathbb{R}) \times \mathbb{R}[x]_{n-2} \ :\ Q \succcurlyeq 0,\ g = \mathbf{x}^T Q\,\mathbf{x} + q\,f\}$$

is convex, as the intersection of the linear space

$$\{(Q,q) \in S^n(\mathbb{R}) \times \mathbb{R}[x]_{n-2},\ g - \mathbf{x}^T Q\,\mathbf{x} - q\,f = 0\}$$

with the convex cone $S^n_+(\mathbb{R}) \times \mathbb{R}[x]_{n-2}$.

We solve this convex optimization problem by using a numerical interior point solver, working at a given precision μ. Since the solution returned by such a solver is (an approximation of) an interior point of the face where the objective function reaches its minimum and since the objective function is 1, this yields (a rational approximation of) an interior point (Q^*, q^*) of the convex set $\mathcal{C}$. That is, the numerical solver computes a (rational) approximate solution (Q^*, q^*) of the optimization problem (21), where if the precision μ is good enough, $Q^* \in S^n_+(\mathbb{Q})$ is a positive definite matrix but there will be an error polynomial $\mathbf{x}^T Q^* \mathbf{x} + q^* f - g \neq 0$, although close to 0.

Since (Q^*, q^*) may have a lot of decimals, in order to obtain a rational decomposition of g modulo f of small size, we start by rounding, at a convenient precision $\delta > 0$, $Q^* \in S^n_+(\mathbb{R})$ to a nearby $\overline{Q} \in S^n(\mathbb{Q})$ and $q^* \in \mathbb{R}[x]_{\leq n-2}$ to a nearby rational polynomial $q \in \mathbb{Q}[x]_{\leq n-2}$. We then compute the projection $Q := \pi_{g-q\,f}(\overline{Q}) \in \mathcal{Q}_{g-q\,f}$ which satisfies $g = \mathbf{x}^T Q\,\mathbf{x} + q\,f$. As in the proof of Proposition 2.7, if $\|Q - Q^*\|$ is smaller than the smallest eigenvalue σ of Q^*, then $Q \in S^n_+(\mathbb{Q})$ is a rational positive definite matrix and $g = \mathbf{x}^T Q \mathbf{x} + qf$ gives a rational SOS decomposition of g modulo f, that is $(\mathbf{x}^T Q \mathbf{x}, q)$ is a rational certificate of positivity of g at the real roots of f.

Given the approximate solution (Q^*, q^*) output by the numerical solver, we detail in the following proposition a bound on the rounding precision δ chosen to define $(\overline{Q}, q)$ needed to guarantee that $Q = \pi_{g-qf}(\overline{Q})$ is a positive definite matrix. We assume here that the matrix Q^* output by the solver is positive definite.

Proposition 3.1. *Let $\sigma > 0$ be the smallest eigenvalue of Q^* and assume that $\rho := \|\mathbf{x}^T Q^* \mathbf{x} + q^*\,f - g\| < \sigma$. Set*

$$0 < \delta < \frac{1}{n + (n-1)\sqrt{n}\,\|f\|}(\sigma - \rho).$$

Then, for any rational approximations $(\overline{Q}, q) \in S^n(\mathbb{Q}) \times \mathbb{Q}[x]_{n-2}$ of (Q^*, q^*) such that

$$|\overline{Q}_{i,j} - Q^*_{i,j}| \leq \delta,\ 1 \leq i,j \leq n \quad \text{and} \quad |q_i - q^*_i| \leq \delta,\ 0 \leq i \leq n-2,$$

the symmetric matrix $Q = \pi_{g-qf}(\overline{Q}) \in S^n(\mathbb{Q})$, which satisfies $g = \mathbf{x}^T Q\,\mathbf{x} + q\,f$, is positive definite.

Proof. We have

$$\|\overline{Q} - Q^*\| \leq n\,\delta \quad \text{and} \quad \|q - q^*\| \leq \sqrt{n}\,\delta.$$

Then, the distance between $Q = \pi_{g-q\,f}(\overline{Q})$ and Q^* can be bounded, as in the proof of Proposition 2.7 but with the difference that $Q^* \neq \pi_{g-q^*f}(Q^*)$, as follows:

$$\begin{aligned}\|Q - Q^*\| &\leq \|\pi_{g-q\,f}(\overline{Q}) - \pi_{g-q\,f}(Q^*)\| + \|\pi_{g-q\,f}(Q^*) - \pi_{g-q^*\,f}(Q^*)\| \\ &\quad + \|\pi_{g-q^*\,f}(Q^*) - Q^*\| \\ &\leq \|\overline{Q} - Q^*\| \\ &\quad + \|Q^* - Q_{\mathbf{x}^T Q^*\mathbf{x}-(g-qf)} - (Q^* - Q_{\mathbf{x}^T Q^*\mathbf{x}-(g-q^*f)}\| \\ &\quad + \|Q_{\mathbf{x}^T Q^*\mathbf{x}-(g-q^*\,f)}\| \\ &\leq \|\overline{Q} - Q^*\| + \|Q_{(q^*-q)f}\| + \|Q_{\mathbf{x}^T Q^*\mathbf{x}-(g-q^*\,f)}\|.\end{aligned}$$

Using (14) and (8), as in the proof of Proposition 2.7 we have

$$\|Q_{(q^*-q)\,f}\| \leq (n-1)\|q^* - q\|\,\|f\| \leq (n-1)\sqrt{n}\,\delta\,\|f\|$$

and

$$\|Q_{\mathbf{x}^T Q^*\mathbf{x}-(g-q^*\,f)}\| \leq \|\mathbf{x}^T Q^*\mathbf{x} + q^*\,f - g\| = \rho.$$

As $\|\overline{Q} - Q^*\| \leq n\,\delta$, we deduce that

$$\|Q - Q^*\| \leq (n + (n-1)\sqrt{n}\,\|f\|)\,\delta + \rho < (\sigma - \rho) + \rho = \sigma$$

Therefore Q is positive definite. □

The approximation of σ and the norm ρ of the error polynomial $\mathbf{x}^T Q^*\mathbf{x} + q^* f - g$, which is approximately 0, depend on the precision μ of the solver. If $\rho > \sigma$, we need to increase the precision μ of the numerical solver and compute a new solution (Q^*, q^*).

We can now summarize the certification algorithm for a strictly positive polynomial, in Algorithm 3.1.

3.2. **Certificate for a non-negative polynomial.** We consider now the case where f arbitrary and g non-negative on the real roots of f satisfy the assumption that $\gcd(f, g)$ and $f/\gcd(f, g)$ are relatively prime. We set $d := \gcd(f, g)$.

We closely follow the proof of our main Theorem in Section 2. We first compute $b \in \mathbb{Q}[x]$ relatively prime to f/d such that b is strictly positive on all the real roots of f/d and $b\,d^2 \equiv g \mod f$.

We then compute the irreducible factorization of $f/d = \prod_{i=1}^r p_i^{e_i}$ where the polynomials $p_i \in \mathbb{Q}[x]$ are irreducible, thus with simple roots, and pairwise relatively prime.

We observe that b and p_i are relatively prime, and that b is strictly positive on the real roots of p_i, $1 \leq i \leq r$.

We set b_i to be the remainder of b modulo p_i, $1 \leq i \leq r$, and we apply Algorithm 3.1 to p_i and b_i. We get the rational SOS certificate

$$b_i = \mathbf{x}^T Q_i \mathbf{x} + q_i\,p_i$$

Algorithm 3.1: Rational SOS certificate modulo a squarefree polynomial for a strictly positive polynomial

Input: $f \in \mathbb{Q}[x]_n$ squarefree, $g \in \mathbb{Q}[x]_{n-1}$ such that $g > 0$ at the real roots of f.

(1) $\mu \leftarrow \mu_0$ default precision of the interior point solver.
(2) $(Q^*, q^*) \leftarrow$ solution of the SDP problem (21) by the numerical interior point solver working at precision μ;
(3) $\sigma \leftarrow$ smallest eigenvalue of Q^*;
(4) $\rho \leftarrow \|\mathbf{x}^T Q^* \mathbf{x} + q^* f - g\|$ the 2-norm of the error polynomial;
(5) $\delta \leftarrow \frac{0.99}{n+\sqrt{n(n-1)}\,\|f\|}(\sigma - \rho)$; If $\delta < 0$ then increase precision $\mu \leftarrow 2\,\mu$ and repeat from step (1);
(6) $\overline{Q} \leftarrow$ round Q^* to rational coefficients, with $\lceil \log_{10}(\delta^{-1}) \rceil$ exact digits after decimal point;
(7) $q \leftarrow$ round q^* to rational coefficients, with $\lceil \log_{10}(\delta^{-1}) \rceil$ exact digits after decimal point;
(8) $Q \leftarrow \pi_{g-q\,f}(\overline{Q})$;

Output: $(Q, q) \in S_+^n(\mathbb{Q}) \times \mathbb{Q}[x]_{n-2}$ such that

- $g = \mathbf{x}^T Q \mathbf{x} + q\, f$,
- Q definite positive.

where, setting $n_i := \deg(p_i)$, $Q_i \in S_+^{n_i}(\mathbb{Q})$ is positive definite and $q_i \in \mathbb{Q}[x]_{n_i-2}$. We deduce from it, by LU factorization, a SOS decomposition

$$b_i \equiv \sum_{j=1}^{n_i} \omega_{i,j} \overline{h}_{i,j}^2 \mod p_i,$$

where $\omega_{i,j} \in \mathbb{Q}_+, \overline{h}_{i,j} \in \mathbb{Q}[x]$.

Therefore

$$b \equiv \sum_{j=1}^{n_i} \omega_{i,j} \overline{h}_{i,j}^2 \mod p_i, \quad 1 \le i \le r.$$

By Hensel lifting (Lemma 2.9), we deduce an SOS decomposition of b modulo $p_i^{e_i}$, and by the Chinese Remainder Theorem (Lemma 2.10), we deduce an SOS decomposition of b modulo f/d:

$$b \equiv \sum_{i=1}^{N} \omega_i \overline{h}_i^2 \mod f/d$$

with $\omega_i \in \mathbb{Q}_+, \overline{h}_i \in \mathbb{Q}[x]$. Using that $b\, d^2 \equiv g \mod f$, this gives the following SOS decomposition of g modulo f:

$$g \equiv \sum_{i=1}^{N} \omega_i (d\overline{h}_i)^2 \mod f$$

and we finally compute $q \in \mathbb{Q}[x]$ s.t.

$$g = \sum_{i=1}^{N} \omega_i (d\overline{h}_i)^2 + q\, f.$$

This computation is summarized in Algorithm 3.2.

Algorithm 3.2: Rational SOS certificate for a non-negative polynomial

---

Input: $f \in \mathbb{Q}[x]_n$, $g \in \mathbb{Q}[x]$ such that $g \geq 0$ on the real roots of f and $\gcd(f, g)$ and $f/\gcd(f, g)$ are relatively prime.

(1) $d \leftarrow \gcd(f, g)$;
(2) Compute $b \in \mathbb{Q}[x]$ s.t. b is prime to f/d, strictly positive on the real roots of f/d and $b\, d^2 \equiv g \mod f$.
(3) Compute the factorization $f/d = \prod_{i=1}^{r} p_i^{e_i}$ into irreducible factors in $\mathbb{Q}[x]$;
(4) For each irreducible factor p_i,
    $b_i \leftarrow$ the remainder of b modulo p_i;
    $(Q'_i, q'_i) \leftarrow$ output of Algorithm 3.1 applied to b_i and p_i;
    Compute $\omega_{i,j} \in \mathbb{Q}_+, \overline{h}_{i,j} \in \mathbb{Q}[x]$ such that

$$b_i \equiv \sum_j \omega_{i,j} \overline{h}_{i,j}^2 \mod p_i;$$

    Compute $h_{i,j} \in \mathbb{Q}[x]$ such that

$$b_i \equiv \sum_j \omega_{i,j} h_{i,j}^2 \mod p_i^{e_i}$$

    using Hensel lifting in Lemma 2.9;
(5) Compute $\omega_i \in \mathbb{Q}_+$, $h_i \in \mathbb{Q}[x]$ such that

$$b \equiv \sum_i \omega_i \overline{h}_i^2 \mod f/d$$

    using Chinese Remainder construction in Lemma 2.10;
(6) $h_i \leftarrow d\, \overline{h}_i$;
(7) Compute $q \in \mathbb{Q}[x]$ s.t. $g = \sum_i \omega_i h_i^2 + q\, f$;

Output: $\omega_i \in \mathbb{Q}_+$, $h_i \in \mathbb{Q}[x]$, $q \in \mathbb{Q}[x]$ satisfying

$$g = \sum_i \omega_i h_i^2 + q\, f.$$

3.3. **Example.** We now revisit Example 2.8 to illustrate the symbolic-numeric approach based on Semi-Definite-Programming.

Example 3.2. Let $f = x^3 - 2 = (x - 2^{1/3})(x - 2^{1/3}\omega)(x - 2^{1/3}\overline{\omega})$, where $\omega = e^{2\pi \mathbf{i}/3}$, and $g = x$.

By an interior point method for solving the convex optimization program:

$$\begin{array}{ll} \inf & 1 \\ s.t. & Q \in S^3(\mathbb{R}), Q \succcurlyeq 0 \\ & q \in \mathbb{R}[x]_1 \\ & g = \mathbf{x}^t Q \mathbf{x} + qf \end{array}$$

we obtain the matrix Q^* of maximal rank and the polynomial q^*:

$$Q^* \approx \left[\begin{array}{rrr} 0.6176533241 & -0.0017575733 & -0.2261937667 \\ -0.0017575733 & 0.4523875415 & -0.154413329 \\ -0.2261937667 & -0.154413329 & 0.5017575773 \end{array}\right],$$
$$q^* \approx -0.5017575692\, x + 0.308826658.$$

The eigenvalues of Q^* are approximately:

$$0.246491, 0.506204, 0.819104.$$

The norm of the error polynomial is $\rho \approx 1.6024e^{-8}$ so that $\delta \approx 0.0227$ and rounding with $t = 2$ decimal digits yields a positivity certificate. In fact, in this case, rounding with one decimal digit is enough:

$$\overline{Q} = \left[\begin{array}{ccc} 0.6 & 0 & -0.2 \\ 0 & 0.5 & -0.2 \\ -0.2 & -0.2 & 0.5 \end{array}\right] \quad \text{and} \quad q = -0.5\, x + 0.3,$$

with error $e = \mathbf{x}^T \overline{Q} \mathbf{x} + q\, f - g = -0.1x^3 + 0.1x^2$ yield

$$Q = \pi_{g-qf}(\overline{Q}) = \overline{Q} - Q_e = \left[\begin{array}{ccc} \frac{3}{5} & 0 & \frac{-7}{30} \\ 0 & \frac{7}{15} & \frac{-3}{20} \\ \frac{-7}{30} & \frac{-3}{20} & \frac{1}{2} \end{array}\right].$$

It is a positive definite matrix (its eigenvalues are approximately 0.24507, 0.505399, 0.816198) which induces a rational SOS decomposition of g modulo f.

4. Conclusion

In this work,

(1) we showed that a univariate rational polynomial g is strictly positive on all the real roots of a univariate rational squarefree polynomial f if and only if it is a sum of squares of rational univariate polynomials modulo f. To our knowledge, this fact was known for univariate polynomials in the global setting but not in the local setting;
(2) we showed that the usual assumption of g being strictly positive on the real roots of a squarefree polynomial f can be relaxed to $\gcd(f, g)$ and $f/\gcd(f, g)$ relatively prime, which we believe is the best assumption one can obtain;

(3) we produced an algorithm for the local setting, which is the counterpart of known algorithms for the global setting in the strictly positive case, and involves Hensel lifting and Chinese Remainder Theorem in the non squarefree and non-negative case.

Our project is to try to extend our results to the multivariate local setting of polynomials being non-negative on the real zero set of a zero-dimensional ideal. Some of them can be extended mutatis-mutandis but there is still work to be done on the relaxation of the assumptions.

References

[1] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry.* Springer-Verlag, Berlin, 2003. ISBN 3-540-00973-6.

[2] S. Chevillard, J. Harrison, M. Joldeş, and Ch. Lauter. Efficient and accurate computation of upper bounds of approximation errors. *Theoret. Comput. Sci.*, 412(16):1523–1543, 2011.

[3] Feng Guo, Erich L. Kaltofen, and Lihong Zhi. Certificates of impossibility of hilbert-artin representations of a given degree for definite polynomials and functions. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, ISSAC '12, page 195–202, New York, NY, USA, 2012. Association for Computing Machinery.

[4] Erich Kaltofen, Bin Li, Zhengfeng Yang, and Lihong Zhi. Exact certification of global optimality of approximate factorizations via rationalizing sums-of-squares with floating point scalars. In *Proceedings of the Twenty-First International Symposium on Symbolic and Algebraic Computation*, ISSAC '08, page 155–164, New York, NY, USA, 2008. Association for Computing Machinery.

[5] Erich L. Kaltofen, Bin Li, Zhengfeng Yang, and Lihong Zhi. Exact certification in global polynomial optimization via sums-of-squares of rational functions with rational coefficients. *Journal of Symbolic Computation*, 47(1):1–15, 2012.

[6] Edmund Landau. Über die Darstellung definiter Funktionen durch Quadrate. *Math. Ann.*, 62(2):272–285, 1906.

[7] Victor Magron and Mohab Safey El Din. On exact Reznick, Hilbert-Artin and Putinar's representations. *J. Symbolic Comput.*, 107:221–250, 2021.

[8] Victor Magron, Mohab Safey El Din, and Markus Schweighofer. Algorithms for weighted sum of squares decomposition of non-negative univariate polynomials. *Journal of Symbolic Computation*, 93:200–220, 2019.

[9] Pablo A. Parrilo. An explicit construction of distinguished representations of polynomials nonnegative over finite sets. IfA Technical Report AUT02-02, March 2002.

[10] Helfried Peyrl and Pablo A. Parrilo. Computing sum of squares decompositions with rational coefficients. *Theoret. Comput. Sci.*, 409(2):269–281, 2008.

[11] Y. Pourchet. Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques. *Acta Arith.*, 19:89–104, 1971.

[12] Mihai Putinar. Positive polynomials on compact semi-algebraic sets. *Indiana University Mathematics Journal*, 42(3):969–984, 1993.

[13] Claus Scheiderer. Sums of squares of polynomials with rational coefficients. *J. Eur. Math. Soc. (JEMS)*, 18(7):1495–1513, 2016.

[14] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra.* Cambridge University Press, Cambridge, third edition, 2013.

Teresa Krick, Departamento de Matemática & IMAS, Universidad de Buenos Aires & CONICET, Argentina.
Email address: krick@dm.uba.ar

Bernard Mourrain, Aromath, Inria, Université Côte d'Azur, 2004, route des Lucioles, 06902 Sophia Antipolis, France.
Email address: bernard.mourrain@inria.fr

Agnes Szanto, North carolina State University, Department of Mathematics, Campus Box 8205, Raleigh, NC, 27695, USA.
Email address: aszanto@ncsu.edu