

Certification of inequalities involving transcendental functions: combining SDP and max-plus approximation

Xavier ALLAMIGEON¹, Stéphane GAUBERT², Victor MAGRON³ and Benjamin WERNER⁴

Abstract—We consider the problem of certifying an inequality of the form $f(x) \geq 0, \forall x \in K$, where f is a multivariate transcendental function, and K is a compact semialgebraic set. We introduce a certification method, combining semialgebraic optimization and max-plus approximation. We assume that f is given by a syntactic tree, the constituents of which involve semialgebraic operations as well as some transcendental functions like \cos, \sin, \exp , etc. We bound some of these constituents by suprema or infima of quadratic forms (max-plus approximation method, initially introduced in optimal control), leading to semialgebraic optimization problems which we solve by semidefinite relaxations. The max-plus approximation is iteratively refined and combined with branch and bound techniques to reduce the relaxation gap. Illustrative examples of application of this algorithm are provided, explaining how we solved tight inequalities issued from the Flyspeck project (one of the main purposes of which is to certify numerical inequalities used in the proof of the Kepler conjecture by Thomas Hales).

Index Terms—Polynomial Optimization Problems, Certification, Semidefinite Programming, Transcendental Functions, Branch and Bound, Semialgebraic Relaxations, Sum of Squares, Flyspeck Project, Non-linear Inequalities, Quadratic Cuts, Max-plus approximation.

I. INTRODUCTION

Inequalities involving transcendental and semialgebraic functions: Given a multivariate transcendental real function $f : \mathbb{R}^n \rightarrow \mathbb{R}$ and a compact semialgebraic set $K \in \mathbb{R}^n$, we consider the following optimization problem:

$$f^* := \inf_{x \in K} f(x) , \quad (I.1)$$

The goal is to find the global minimum f^* and a global minimizer x^* . We shall also search for certificates to assess that:

$$\forall x \in K, \quad f(x) \geq 0 . \quad (I.2)$$

A special case of Problem (I.1) is semialgebraic optimization. Then, $f = f_{sa}$ belongs to the algebra \mathcal{A} of semialgebraic functions which extends multivariate polynomials by allowing arbitrary composition of $(\cdot)^p, (\cdot)^{\frac{1}{p}} (p \in \mathbb{N}_0), |\cdot|, +, -, \times, /, \sup(\cdot, \cdot), \inf(\cdot, \cdot)$:

$$f_{sa}^* := \inf_{x \in K} f_{sa}(x) . \quad (I.3)$$

The research leading to these results has received funding from the European Union's 7th Framework Programme under grant agreement nr. 243847 (ForMath).

¹INRIA and CMAP, École Polytechnique, Palaiseau, France, Xavier.Allamigeon at inria.fr

²INRIA and CMAP, École Polytechnique, Palaiseau, France, Stéphane.Gaubert at inria.fr

³INRIA and LIX, École Polytechnique, Palaiseau, France, magron at lix.polytechnique.fr

⁴INRIA and LIX, École Polytechnique, Palaiseau, France, benjamin.werner at polytechnique.edu

Furthermore, when $f = f_{pop}$ is a multivariate polynomial and $K = K_{pop}$ is given by finitely many polynomial inequalities, Problem (I.3) matches the Polynomial Optimization problem (POP):

$$f_{pop}^* := \inf_{x \in K_{pop}} f_{pop}(x) . \quad (I.4)$$

Motivations: Our ultimate motivation is to automatically verify inequalities occurring in the proof of Kepler conjecture by Thomas Hales [14]. The formal verification of Kepler's conjecture is an ambitious goal addressed by the Flyspeck project [13]. Flyspeck is a large-scale effort needing to tackle various mathematical tools. One particular difficulty is that Hales' proof relies on hundreds of inequalities, and checking them requires non-trivial computations. Because of the limited computing power available inside the proof assistants, it is essential to devise optimized algorithms that: (1) verify these inequalities automatically, and (2) produce a *certificate* for each inequality, whose checking is computationally reasonably simple.

There are numerous other applications to the formal assessment of such real inequalities; we can point to several other recent efforts to produce positivity certificates for such problems which can be checked in proof assistants such as Coq [26] [6], HOL-light [17] or MetiTarski [1].

The Flyspeck inequalities typically involve multivariate polynomials with some additional transcendental functions; the aim is thus to compute a lower bound for such expressions. These inequalities are in general tight, and thus challenging for numerical solvers. Computing lower bounds in constrained polynomial optimization problems (POP) is already a difficult problem, which has received much attention. Semidefinite relaxation based methods have been developed in [20] [28]; they can be applied to the more general class of semialgebraic problems [29]. Alternative approaches are based on Bernstein polynomials [36]. The task is obviously more difficult in presence of transcendental functions. Other methods of choice, not restricted to polynomials, include global optimization by interval methods (see e.g. [15]), branch and bound methods with Taylor models [9] [5].

In what follows, we will consider the following running example taken from Hales' proof:

Example 1.1 (Lemma₉₉₂₂₆₉₉₀₂₈ Flyspeck): Let $K, \Delta x, l$, and f be defined as follows:

- $K := [4; 6.3504]^3 \times [6.3504; 8] \times [4; 6.3504]^2$
- $\Delta x := x_1 x_4 (-x_1 + x_2 + x_3 - x_4 + x_5 + x_6) + x_2 x_5 (x_1 - x_2 + x_3 + x_4 - x_5 + x_6) + x_3 x_6 (x_1 + x_2 - x_3 + x_4 + x_5 - x_6) - x_2 x_3 x_4 - x_1 x_3 x_5 - x_1 x_2 x_6 - x_4 x_5 x_6$

- $l(x) := -\frac{\pi}{2} + 1.6294 - 0.2213(\sqrt{x_2} + \sqrt{x_3} + \sqrt{x_5} + \sqrt{x_6} - 8.0) + 0.913(\sqrt{x_4} - 2.52) + 0.728(\sqrt{x_1} - 2.0)$
- $f(x) := l(x) + \arctan \frac{\partial_4 \Delta x}{\sqrt{4x_1 \Delta x}}$

Then, $\forall x \in K, f(x) \geq 0$.

Contribution: In this paper, we present a certification framework, combining Lasserre SDP relaxations of semialgebraic problems with max-plus approximation by quadratic functions.

The idea of max-plus approximation comes from optimal control: it was originally introduced by Fleming and McEneaney [11], and developed by several authors [3], [12], [23], [24], [31], to represent the value function by a “max-plus linear combination”, which is a supremum of certain basis functions, like quadratic forms. When applied to the present context, this idea leads to approximate from above and from below every transcendental function appearing in the description of the problem by infima and suprema of finitely many quadratic forms. In that way, we are reduced to a converging sequence of semialgebraic problems. A geometrical way to interpret the method is to think of it in terms of “quadratic cuts”: quadratic inequalities are successively added to approximate the graph of a transcendental function.

The proposed method (Figure 2) may be summarized as follows. Let f be a function and K a box issued from a Flyspeck inequality, so f belongs to the set of transcendental functions obtained by composition of semialgebraic functions with \arctan , \arccos , \arcsin , \exp , \log , $|\cdot|$, $(\cdot)^{\frac{1}{p}}$ ($p \in \mathbb{N}_0$), $+$, $-$, \times , $/$, $\sup(\cdot, \cdot)$, $\inf(\cdot, \cdot)$. We alternate steps of approximation, in which an additional quadratic function is added to the representation, and optimization steps, in which an SDP relaxation from Lasserre hierarchy is solved. The information on the location of the optimum inferred from this relaxation is then used to refine dynamically the quadratic approximation. In this way, at each step of the algorithm, we refine the following inequalities

$$f^* \geq f_{sa}^* \geq f_{pop}^* , \quad (I.5)$$

where f^* is the optimal value of the original problem f_{sa}^* the optimal value of its current semialgebraic approximation, and f_{pop}^* the optimal value of the SDP relaxation which we solve. The lower estimate f_{pop}^* does converge to f^* . This follows from a theorem of Lasserre (convergence of moment SDP relaxations) and from the consistency of max-plus approximation, see Theorem 3.3.

Max-plus approximation has attracted interest because it may attenuate the “curse of dimensionality” for some structured problems [25]. Indeed, the estimate of [12] shows that the number of quadratic terms needed to reach an ϵ -approximation of a function of d variables is of order $\epsilon^{-d/2}$, where d is the dimension. Hence, max-plus approximations can be applied to fixed, small dimensional sub-expressions of complex high dimensional expressions, in a curse of dimensionality free way. In particular, in the Flyspeck inequalities involve generally 6 variables, but only univariate transcendental functions, so $d = 1$.

An alternative, more standard approach, is to approximate transcendental functions by polynomials of a sufficiently high degree, and to apply SDP relaxations to the polynomial problems obtained in this way. Further experiments presented in [4] indicate that this method is not always scalable. Another alternative approach, which is quite effective on Flyspeck type inequalities, is to run branch and bound type algorithms with interval arithmetics. However, in some instances, this leads to certifying an exponential number of interval arithmetics computations. Thus, it is of interest to investigate hybrid methods such as the present one, in order to obtain more concise certificates.

An important issue, for the practical efficiency of the method, is the simultaneous tuning of the precision of the max-plus approximation and of the orders of semidefinite relaxation. How to perform optimally this tuning is still not well understood. However, we present experimental results, both for some elementary examples as well as non-linear inequalities issued from the Flyspeck project, giving some indication that certain hard subclasses of problems (sum of arctan of correlated functions in many variables) can be solved in a scalable way.

To solve the POP instances, several solvers are available as Gloptipoly [18] or Kojima sparse refinement of the hierarchy of SDP relaxations [33], implemented in the SparsePOP solver [34]. These solvers are interfaced with several SDP solvers (e.g. SeDuMi [32], CSDP [7], SDPA [35]).

The paper is organized as follows. In Section II, we recall the definition and properties of Lasserre relaxations of polynomial problems, together with reformulations by Lasserre and Putinar of semialgebraic problems classes. The max-plus approximation, and the main algorithm are presented in Section III. In Section IV, we show how the algorithm can be combined with standard domain subdivision methods, to reduce the relaxation gap. Numerical results are presented in Section V.

II. NOTATION AND PRELIMINARY RESULTS

Let $\mathbb{R}_d[X]$ be the vector space of real forms in n variables of degree d and $\mathbb{R}[X]$ the set of multivariate polynomials in n variables. We also define the cone $\Sigma_d[X]$ of sums of squares of degree at most $2d$.

A. Constrained Polynomial Optimization Problems and SOS

We consider the general constrained polynomial optimization problem (POP):

$$f_{pop}^* := \inf_{x \in K_{pop}} f_{pop}(x), \quad (II.1)$$

where $f_{pop} : \mathbb{R}^n \rightarrow \mathbb{R}$ is a d -degree multivariate polynomial, K_{pop} is a compact set defined by polynomial inequalities $g_1(x) \geq 0, \dots, g_m(x) \geq 0$ with $g_i(x) : \mathbb{R}^n \rightarrow \mathbb{R}$ being a real-valued polynomial of degree $w_i, i = 1, \dots, m$. We call K_{pop} the feasible set of Problem (II.1). Let $g_0 := 1$. We introduce the k -truncated quadratic module $M_k(K_{pop}) \subset$

$\mathbb{R}_{2k}[X]$ associated with g_1, \dots, g_m :

$$M_k(K_{\text{pop}}) = \left\{ \sum_{j=0}^m \sigma_j(x) g_j(x) : \sigma_j \in \Sigma_{k-\lceil w_j/2 \rceil}[X] \right\}$$

Let $k \geq k_0 := \max(\lceil d/2 \rceil, \max_{0 \leq j \leq m} \{\lceil w_j/2 \rceil\})$ and consider the following hierarchy of semidefinite relaxations:

$$Q_k : \begin{cases} \sup_{\mu, \sigma_0, \dots, \sigma_m} \mu \\ f_{\text{pop}}(x) - \mu \in M_k(K_{\text{pop}}), \end{cases}$$

and denote by $\sup(Q_k)$ its optimal value.

Theorem 2.1 (Lasserre [20]): The sequence of optimal values $(\sup(Q_k))_{k \geq k_0}$ is non-decreasing. If the quadratic module $M_k(K_{\text{pop}})$ is archimedean, then this sequence converges to f_{pop}^* .

The non-linear inequalities to be proved in the Flyspeck project typically involve a variable x lying in a box $K \subset \mathbb{R}^n$, thus the archimedean condition holds in our case.

B. Semialgebraic Optimization

In this section, we recall how the previous approach can be extended to semialgebraic optimization problems by introducing lifting variables.

Given a semialgebraic function f_{sa} , we consider the problem $f_{\text{sa}}^* = \inf_{x \in K_{\text{sa}}} f_{\text{sa}}(x)$, where $K_{\text{sa}} := \{x \in \mathbb{R}^n : g_1(x) \geq 0, \dots, g_m(x) \geq 0\}$ is a basic semialgebraic set. We suppose that f_{sa} is well-defined and thus has a basic semialgebraic lifting. Then, following the approach described in [21], we can add auxiliary lifting variables z_1, \dots, z_p , and construct polynomials $h_1, \dots, h_s \in \mathbb{R}[x, z_1, \dots, z_p]$ defining the semialgebraic set $K_{\text{pop}} := \{(x, z_1, \dots, z_p) \in \mathbb{R}^{n+p} : x \in K_{\text{sa}}, h_1(x, z) \geq 0, \dots, h_s(x, z) \geq 0\}$, ensuring that $f_{\text{pop}}^* := \inf_{(x,z) \in K_{\text{pop}}} z_p$ is a lower bound of f_{sa}^* .

To ensure that the archimedean condition is preserved, we add bound constraints over the lifting variables. These bounds are computed by solving semialgebraic optimization sub-problems.

Example 2.2 (from Lemma₉₉₂₂₆₉₉₀₂₈ Flyspeck):

Continuing Example 1.1, we consider the function $f_{\text{sa}} := \frac{\partial_4 \Delta x}{\sqrt{4x_1 \Delta x}}$ and the set $K_{\text{sa}} := [4, 6.3504]^3 \times [6.3504, 8] \times [4, 6.3504]^2$. The latter can be equivalently rewritten as

$$K_{\text{sa}} := \{x \in \mathbb{R}^6 : g_1 \geq 0, \dots, g_{12} \geq 0\}$$

where $g_1 := x_1 - 4, g_2 := 6.3504 - x_1, \dots, g_{11} := x_6 - 4, g_{12} := 6.3504 - x_6$.

We introduce two lifting variables z_1 and z_2 , respectively representing the terms $\sqrt{4x_1 \Delta x}$ and $\frac{\partial_4 \Delta x}{\sqrt{4x_1 \Delta x}}$. We also use a lower bound m_1 of $\inf_{x \in K_{\text{sa}}} \sqrt{4x_1 \Delta x}$ and an upper bound M_1 of $\sup_{x \in K_{\text{sa}}} \sqrt{4x_1 \Delta x}$ which can be both computed by solving auxiliary sub-problems.

Now the basic semialgebraic set K_{pop} can be defined as follows:

$$K_{\text{pop}} := \{(x, z_1, z_2) \in \mathbb{R}^{6+2} : x \in K_{\text{sa}}, h_l(x, z_1, z_2) \geq 0, \\ l = 1, \dots, 7\}$$

where the multivariate polynomials h_l are defined by:

$$\begin{aligned} h_1 &:= z_1 - m_1 & h_5 &:= z_1 \\ h_2 &:= M_1 - z_1 & h_6 &:= z_2 z_1 - \partial_4 \Delta x \\ h_3 &:= z_1^2 - 4x_1 \Delta x & h_7 &:= -z_2 z_1 + \partial_4 \Delta x \\ h_4 &:= -z_1^2 + 4x_1 \Delta x \end{aligned}$$

Let $h_0 := 1, \omega_l := \deg h_l, 0 \leq l \leq 7$ and define the quadratic module $M_k(K_{\text{pop}})$ by:

$$M_k(K_{\text{pop}}) = \left\{ \sum_{j=1}^{12} \sigma_j(x) g_j(x) + \sum_{l=0}^7 \theta_l(x) h_l(x) : \right. \\ \left. \sigma_j \in \Sigma_{k-1}[X], 1 \leq j \leq 12, \theta_l \in \Sigma_{k-\lceil \omega_l/2 \rceil}[X], 0 \leq l \leq 7 \right\}$$

Consider the following semidefinite relaxations:

$$Q_k^{\text{sa}} : \begin{cases} \sup_{\mu, \sigma_1, \dots, \sigma_{12}, \theta_0, \dots, \theta_7} \mu \\ z_2 - \mu \in M_k(K_{\text{pop}}) \end{cases}$$

If $k \geq k_0 := \max_{0 \leq l \leq 7} \{\lceil \omega_l/2 \rceil\} = 2$, then as a special case of Theorem 2.1, the sequence $(\sup(Q_k^{\text{sa}}))_{k \geq 2}$ is monotonically non-decreasing and converges to f_{sa}^* . A tight lower bound $m_3 = -0.445$ is obtained at the third relaxation.

III. TRANSCENDENTAL FUNCTIONS UNDERESTIMATORS

In this section, we introduce an algorithm allowing to determine that a multivariate transcendental function is positive (Problem (I.2)). The algorithm relies on an adaptive basic-semialgebraic relaxation, in which approximations of transcendental functions by suprema or infima of quadratic forms are iteratively refined.

A. Max-plus Approximation of Semiconvex Functions

Let \mathcal{B} be a set of functions $\mathbb{R}^n \rightarrow \mathbb{R}$, whose elements will be called *max-plus basis functions*. Given a function $f : \mathbb{R}^n \rightarrow \mathbb{R}$, we look for a representation of f as a linear combination of basis functions in the max-plus sense, i.e.,

$$f = \sup_{w \in \mathcal{B}} (a(w) + w) \quad (\text{III.1})$$

where $(a(w))_{w \in \mathcal{B}}$ is a family of elements of $\mathbb{R} \cup \{-\infty\}$ (the ‘‘coefficients’’). The correspondence between the function $x \mapsto f(x)$ and the coefficient function $w \mapsto a(w)$ is a well studied problem, which has appeared in various guises (Moreau conjugacies, generalized Fenchel transforms, Galois correspondences, see [2] for more background).

The idea of max-plus approximation [3], [11], [22] is to choose a space of functions f and a corresponding set \mathcal{B} of basis functions w , and to approximate from below a given f in this space by a finite max-plus linear combination, $f \simeq \sup_{w \in \mathcal{F}} (a(w) + w)$ where $\mathcal{F} \subset \mathcal{B}$ is a finite subset. Note that $\sup_{w \in \mathcal{F}} (a(w) + w)$ is not only an approximation but a valid lower bound of f .

Following [3], [11], for each constant $\gamma \in \mathbb{R}$, we shall consider the family of quadratic functions $\mathcal{B} = \{w_y \mid y \in \mathbb{R}^n\}$ where

$$w_y(x) := -\frac{\gamma}{2} \|x - y\|^2.$$

Recall that a function is γ -semiconvex if and only if the function $x \mapsto \phi(x) + \frac{\gamma}{2}|x|^2$ is convex. Then, it follows from Legendre-Fenchel duality that the space of functions f which can be written as (III.1) is precisely the set of lower semicontinuous γ -semiconvex functions.

The transcendental functions which we consider here are twice continuously differentiable. Hence, their restriction to any bounded convex set is γ -semiconvex for a sufficiently large γ , so that they can be approximated by finite suprema of the form $\sup_{w \in \mathcal{F}} (a(w) + w)$ with $\mathcal{F} \subset \mathcal{B}$. A result of [12] shows that if $N = |\mathcal{F}|$ basis functions are used, then the best approximation error is $O(1/N^{2/n})$ (the error is the sup-norm, over any compact set), provided that the function to be approximated is of class \mathcal{C}^2 . Equivalently, the approximation error is of order $O(h^2)$ where h is a space discretization step. Note that the error of max-plus approximation is of the same order as the one obtained by conventional P_1 finite elements under the same regularity assumption. For the applications considered in this paper, $n = 1$.

In this way, starting from a transcendental univariate elementary function $f \in \mathcal{T}$, such as \arctan , \exp , *etc*, defined on a real bounded interval I , we arrive at a semialgebraic lower bound of f , which is nothing but a supremum of a finite number of quadratic functions.

Example 3.1: Consider the function $f = \arctan$ on an interval $I := [m, M]$. For every point $a \in I$, we can find a constant γ such that

$$\arctan(x) \geq \text{par}_a^-(x) := -\frac{\gamma}{2}(x-a)^2 + f'(a)(x-a) + f(a) .$$

Choosing $\gamma = \sup_{x \in I} -f''(x)$ always work. However, it will be convenient to allow γ to depend on the choice of a to get tighter lower bounds. Choosing a finite subset $A \subset I$, we arrive at an approximation

$$\forall x \in I, \arctan(x) \geq \max_{a \in A} \text{par}_a^-(x) . \quad (\text{III.2})$$

Semialgebraic overestimators $x \mapsto \min_{a \in A} \text{par}_a^+(x)$ can be defined in a similar way.

B. An Adaptive Semialgebraic Approximation Algorithm

We now consider an instance of Problem (I.2). As in Flyspeck inequalities, we assume that K is a box. We assimilate the objective function f with its abstract syntax tree t . We assume that the leaves of t are semialgebraic functions in the set \mathcal{A} , and other nodes are univariate transcendental functions (\arctan , *etc*) or basic operations ($+$, \times , $-$, $/$). For the sake of the simplicity, we suppose that each univariate transcendental function is monotonic.

We first introduce the auxiliary algorithm `samp_approx`, presented in Fig. 1. Given an abstract syntax tree t and a box K , this algorithm computes lower and upper bounds of t over K , and max-plus approximations of t by means of semialgebraic functions. It is also parametrized by a finite sequence of control points used to approximate transcendental functions by means of parabola.

The algorithm `samp_approx` is defined by induction on the abstract syntax tree t . When t is reduced to a leaf,

Input: tree t , box K , SDP relaxation order k , control points sequence $s = x_1, \dots, x_r \in K$

Output: lower bound m , upper bound M , lower tree t^- , upper tree t^+

- 1: **if** $t \in \mathcal{A}$ **then**
- 2: **return** `min_sa` (t, k), `max_sa` (t, k), t, t
- 3: **else if** $r := \text{root}(t) \in \mathcal{T}$ parent of the single child c **then**
- 4: $m_c, M_c, c^-, c^+ := \text{samp_approx}(c, K, k, s)$
- 5: $\text{par}^-, \text{par}^+ := \text{build_par}(r, m_c, M_c, s)$
- 6: $t^-, t^+ := \text{compose}(\text{par}^-, \text{par}^+, c^-, c^+)$
- 7: **return** `min_sa` (t^-, k), `max_sa` (t^+, k), t^-, t^+
- 8: **else if** $\text{bop} := \text{root}(t)$ is a binary operation parent of two children c_1 and c_2 **then**
- 9: $m_{c_i}, M_{c_i}, c_i^-, c_i^+ := \text{samp_approx}(c_i, K, k, s)$ for $i \in \{1, 2\}$
- 10: $t^-, t^+ := \text{compose_bop}(c_1^-, c_1^+, c_2^-, c_2^+)$
- 11: **return** `min_sa` (t^-, k), `max_sa` (t^+, k), t^-, t^+
- 12: **end**

Fig. 1. `samp_approx` : recursive semialgebraic max-plus approximation algorithm

i.e. it represents a semialgebraic function of \mathcal{A} , we call the functions `min_sa` and `max_sa` which determine lower and upper bounds using techniques presented in Section II-B. In this case, the tree t provides an exact semialgebraic estimator. If the root of t corresponds to a transcendental function node $r \in \mathcal{T}$ taking a single child c as argument, lower and upper bounds c_m and c_M are recursively obtained, as well as estimators c^- and c^+ . Then we apply the function `build_par` that builds the parabola at the given control points, by using the convexity/semiconvexity properties of r , as explained in Section III-A. An underestimator t^- as well as an overestimator t^+ are determined by composition (so-called `compose` function) of the parabola with c^- and c^+ . Notice that the behaviour of `compose` depends on the monotonicity properties of r . These approximations t^- and t^+ are semialgebraic functions of \mathcal{A} , whence we can also compute their lower and upper bounds using `min_sa` and `max_sa`. The last case occurs when the root of t is a binary operation whose arguments are two children c_1 and c_2 . We can apply recursively `samp_approx` to each child and get semialgebraic underestimators c_1^-, c_2^- and overestimators c_1^+, c_2^+ . Note that when the binary operation is the multiplication or the division, we assume that the estimators of c_1 or c_2 have a constant sign. We have observed that in practice, all the inequalities that we consider in the Flyspeck project satisfy this restriction.

Our main optimization algorithm `samp_optim`, presented in Fig. 2, relies on `samp_approx` and chooses the sequence of control points s dynamically. At the beginning, the set of control points consists of a single point of the box K , chosen so as to minimize the value of the function associated to the tree t among a set of random points (Line 1). Then, at each iteration of the loop from Lines 4 to 10, the algorithm `samp_approx` is called to compute a lower

Input: tree t , box K , $iter_{\max}$ (optional argument)

Output: lower bound m , feasible solution x_{opt}

```

1:  $s := [\text{argmin}(\text{randeval } t)] \quad \triangleright s \in K$ 
2:  $n := 0$ 
3:  $m := -\infty$ 
4: while  $n \leq iter_{\max}$  do
5:   Choose an SDP relaxation order  $k$ 
6:    $m, M, t^-, t^+ := \text{samp\_approx}(t, K, k, s)$ 
7:    $x_{opt} := \text{guess\_argmin}(t^-) \quad \triangleright t^-(x_{opt}) \simeq m$ 
8:    $s := s \cup \{x_{opt}\}$ 
9:    $n := n + 1$ 
10: done
11: return  $m, x_{opt}$ 

```

Fig. 2. `samp_optim`: Semialgebraic max-plus optimization algorithm

bound m of the function t (Line 4). At Line 7, a minimizer candidate x_{opt} of the underestimator tree t^- is computed. It is obtained by projecting a solution x_{sdp} of the SDP relaxation of Section II-B on the coordinates representing the first order moments, following [20, Theorem 4.2]. However, the projection may not belong to K when the relaxation order k is not large enough. This is why tools like SparsePOP use local optimization solver in a post-processing step, providing a point in K which may not be a global minimizer. In any case, x_{opt} is then added to the set of control points (Line 8). Alternatively, if we are only interested in determining whether the infimum of t over K is non-negative (Problem (I.2)), the loop can be stopped as soon as $m \geq 0$.

When we call several times `samp_approx` inside the loop from Lines 4 to 10, we do not need to always compute recursively the underestimators and overestimators as well as bounds of all the nodes and the leaves of the abstract syntax tree. Instead, we “decorate” the tree with interval and semialgebraic values containing these information, based on previous iterations.

Example 3.2 (Lemma₉₉₂₂₆₉₉₀₂₈ Flyspeck): We continue Example 2.2. Since we computed lower and upper bounds (m and M) for $f_{sa} := \frac{\partial_4 \Delta x}{\sqrt{4x_1 \Delta x}}$, we know that the f_{sa} argument of \arctan lies in $I := [m, M]$. We describe three iterations of the algorithm. Fig. 3 illustrates the related semialgebraic underestimators hierarchy.

- 0) Multiple evaluations of f return a set of values and we obtain a first minimizer $guess\ x_1 := \text{argmin}(\text{randeval } f)$ corresponding to the minimal value of the set. $x_1 := (4.8684, 4.0987, 4.0987, 7.8859, 4.0987, 4.0987)$
- 1) We compute $a_1 := f_{sa}(x_1) = 0.3962$, get the equation of par_1^- with `buildpar` and finally compute $m_1 \leq \min_{x \in K} \{l(x) + \text{par}_{a_1}^-(f_{sa}(x))\}$. For $k = 2$, we obtain $m_1 = -0.2816 < 0$ and a new minimizer $x_2 := (4, 6.3504, 6.3504, 6.3504, 6.3504, 6.3504)$.
- 2) $a_2 := f_{sa}(x_2) = -0.4449$, $\text{par}_{a_2}^-$ and $m_2 \leq \min_{x \in K} \{l(x) + \max_{i \in \{1,2\}} \{\text{par}_{a_i}^-(f_{sa}(x))\}\}$. For $k = 2$, we get $m_2 = -0.0442 < 0$ and a new minimizer $x_3 := (4.0121, 4.0650, 4.0650, 6.7455, 4.0650, 4.0650)$.
- 3) $a_3 := f_{sa}(x_3) = 0.1020$, $\text{par}_{a_3}^-$, and $m_3 \leq \min_{x \in K} \{l(x) + \max_{i \in \{1,2,3\}} \{\text{par}_{a_i}^-(f_{sa}(x))\}\}$. For $k =$

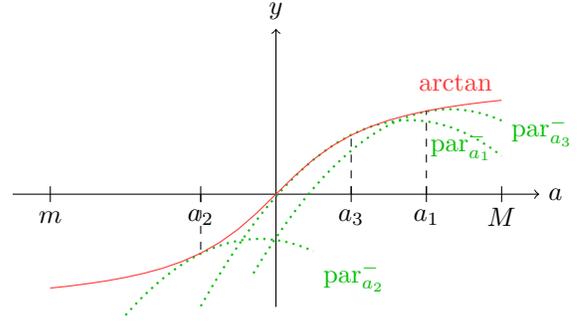


Fig. 3. A hierarchy of Semialgebraic Underestimators for \arctan

2, we obtain $m_3 = -0.0337 < 0$, obtain a new minimizer x_4 .

We denote by t_i^- the underestimator computed at the i^{th} iteration of the algorithm `samp_optim`, and by x_{opt}^i the corresponding minimizer candidate.

Theorem 3.3 (Convergence of `samp_optim`): Assume that at each iteration i , the SDP relaxation order is chosen to be large enough so that x_{opt}^i is a global minimizer of t_i^- . Then every accumulation point of the sequence of $(x_{opt}^i)_i$ is a global minimizer of t over K .

Theorem 3.3 can be proved using the convergence of Lasserre hierarchy of SDP relaxation [20], together with the following lemma:

Lemma 3.4: There exists a positive constant C such that,

$$\forall i \geq 1, \forall x \in K, t(x) - t_i^-(x) \leq Cd(x, S_i)^2, \quad (\text{III.3})$$

where d denotes the euclidean distance and S_i is the set of points $x_{opt}^1, \dots, x_{opt}^i$.

The time complexity of our algorithm strongly depends on the relaxation order k . Indeed, if p is the number of the control points, then the number of moment variables in the SDP problem Q_k is in $O((n+p)^{2k})$, and the size of linear matrix inequalities involved are in $O((n+p)^k)$. The complexity of `samp_optim` is therefore exponential in k . Notice that there are several ways to decrease the size of these matrices. First, symmetries in SDP relaxations for polynomial optimization problems can be exploited to replace one SDP problem Q_k by several smaller SDPs [30]. Notice it is possible only if the multivariate polynomials of the initial problem are invariant under the action of a finite subgroup G of the group $GL_{n+p}(\mathbb{R})$. Furthermore, one can exploit the structured sparsity of the problem to replace one SDP problem Q_k by an SDP problem of size $O(\kappa^{2k})$ where κ is the average size of the maximal cliques correlation pattern of the polynomial variables (see [34]).

IV. REFINING BOUNDS BY DOMAIN SUBDIVISION

A small relaxation order ensures fast computation of the lower bounds but the relaxation gap may remain too high to ensure the convergence of the algorithm. This is particularly critical when we want to certify that a given transcendental

multivariate function is non-negative. In this section, we explain how to reduce the relaxation gap using domain subdivision in order to solve problems of the form (I.2).

Suppose that the algorithm `samp_optim` returns a negative lower bound m and a global minimizer candidate x_c^* . Our approach consists in cutting the initial box K in several boxes $(K_i)_{1 \leq i \leq c}$. We explain the partitioning of K with the following heuristic.

Let $\mathcal{B}_{x_c^*, r}$ be the intersection of the L_∞ -ball of center x_c^* and radius r with the set K . Then, let $f_{x_c^*, r}$ be the quadratic form defined by:

$$\begin{aligned} f_{x_c^*, r} : \mathcal{B}_{x_c^*, r} &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x_c^*) + \mathcal{D}(f)(x_c^*)(x - x_c^*) \\ &\quad + \frac{1}{2}(x - x_c^*)^T \mathcal{D}^2(f)(x_c^*)(x - x_c^*) \\ &\quad + \frac{1}{2}\lambda(x - x_c^*)^2 \end{aligned}$$

with λ given by:

$$\lambda := \min_{x \in \mathcal{B}_{x_c^*, r}} \{\lambda_{\min}(\mathcal{D}^2(f)(x) - \mathcal{D}^2(f)(x_c^*))\} \quad (\text{IV.1})$$

Lemma 4.1: $\forall x \in \mathcal{B}_{x_c^*, r}, f(x) \geq f_{x_c^*, r}$.

To underestimate the value of λ , we determine an interval matrix $\mathcal{D}^2(f) := ([d_{ij}, \bar{d}_{ij}])_{1 \leq i, j \leq n}$ containing coarse bounds of the Hessian difference $(\mathcal{D}^2(f)(x) - \mathcal{D}^2(f)(x_c^*))$ on $\mathcal{B}_{x_c^*, r}$ using interval arithmetic or `samp_approx` with a small number of control points and a low SDP relaxation order. We then apply on $\mathcal{D}^2(f)$ a robust SDP method on interval matrix described by Calafiore and Dabbene in [8], and obtain a lower bound λ' of λ .

By dichotomy and using Lemma 4.1, we can finally compute the L_∞ -ball $\mathcal{B}_{x_c^*, r}$ of maximal radius r such that the underestimator $f_{x_c^*, r}$ is non-negative on $\mathcal{B}_{x_c^*, r}$.

V. RESULTS

We next present the numerical results obtained with our method for both small and medium-sized inequalities taken from the Flyspeck project.

In Tables I and II, the inequalities are indexed by the first four digits of the hash code. We also indicate in subscript the number of variables involved in each inequality. The integer $n_{\mathcal{T}}$ represents the number of transcendental univariate nodes in the corresponding abstract syntax trees. The parameter k_{\max} is the highest SDP relaxation order used to solve the polynomial optimization problems with SparsePOP. We denote by n_{pop} the total number of POP that have to be solved to prove the inequality, and by n_{cuts} the number of domain cuts that are performed during the subdivision algorithm. Finally, m is the lower bound of the function f on K that we obtain with our method, i.e. the minimum of all the computed lower bounds of f among the n_{cut} sub-boxes of K .

The inequalities reported in Table I are similar to the one presented in Example 1.1. They all consist in the addition of the function $x \mapsto \arctan \frac{\partial_4 \Delta x}{\sqrt{4x_1 \Delta x}}$ with an affine function over $\sqrt{x_i}$ ($1 \leq i \leq 6$).

TABLE I
RESULTS FOR SMALL-SIZED FLYSPECK INEQUALITIES

Ineq. id	$n_{\mathcal{T}}$	k_{\max}	n_{pop}	n_{cuts}	m	time
9922 ₆	1	2	222	27	3.07×10^{-5}	20 min
3526 ₆	1	2	156	17	4.89×10^{-6}	13 min
6836 ₆	1	2	173	22	4.68×10^{-5}	14 min
6619 ₆	1	2	163	21	4.57×10^{-5}	13 min
3872 ₆	1	2	250	30	7.72×10^{-5}	20 min
3139 ₆	1	2	162	17	1.03×10^{-5}	13 min
4841 ₆	1	2	624	73	2.34×10^{-6}	50 min
3020 ₅	1	3	80	9	2.96×10^{-5}	31 min
3318 ₆	1	3	26	2	3.12×10^{-5}	1.2 h

Table II provides the numerical results obtained on medium-sized Flyspeck inequalities. Inequalities 7394_i ($3 \leq i \leq 5$) are obtained from a same inequality 7394₆ involving six variables, by instantiating some of the variables by a constant value. Inequalities 7726₆ and 7394₆ are both of the form $l(x) + \sum_{i=1}^3 \arctan(q_i(x))$ where l is an affine function over $\sqrt{x_i}$, where $q_1(x) := \frac{\partial_4 \Delta x}{\sqrt{4x_1 \Delta x}}$, $q_2(x) := q_1(x_2, x_1, x_3, x_5, x_4, x_6)$, and $q_3(x) := q_1(x_3, x_1, x_2, x_6, x_4, x_5)$.

TABLE II
RESULTS FOR MEDIUM-SIZE FLYSPECK INEQUALITIES

Ineq. id	$n_{\mathcal{T}}$	k_{\max}	n_{pop}	n_{cuts}	m	time
7726 ₆	3	2	450	70	1.22×10^{-6}	3.4 h
7394 ₃	3	3	1	0	3.44×10^{-5}	11 s
7394 ₄	3	3	47	10	3.55×10^{-5}	26 min
7394 ₅	3	3	290	55	3.55×10^{-5}	12 h

TABLE III
COMPARISON RESULTS FOR RANDOM EXAMPLES

n	samp_approx with $k = 3$		intsolver	
	m	time	m	time
3	0.4581	3.8 s	0.4581	15.5 s
4	0.4157	12.9 s	0.4157	172.1 s
5	0.4746	1 min	0.4746	10.2 min
6	0.4476	4.6 min	0.4476	3.4 h

In Table III, we compared our algorithm with the MATLAB toolbox `intsolver` [27] (based on the Newton interval method [16]) for random inequalities involving two transcendental functions. We denote by n the number of variables, and by m the lower bound that we obtain. The functions that we consider are of the form $x \mapsto \arctan(p(x)) + \arctan(q(x))$, where p is a four-degree polynomial and q is a quadratic form. All variables lie in $[0, 1]$. Both p and q have random coefficients (taken in $[0, 1]$) and are sparse. The results indicate that for such examples, our method may outperform interval arithmetic.

VI. CONCLUSION

We proposed a hybrid method to certify tight non-linear inequalities, combining SDP and approximation of semiconvex functions by suprema of quadratic forms (max-plus basis method, originating from optimal control). The proposed approach bears some similarity with the ‘‘cutting planes’’ proofs

in combinatorial optimization, the cutting planes being now replaced by quadratic inequalities. This allowed us to solve both small and intermediate size inequalities of the Flyspeck project, with a moderate order of SDP relaxation.

Several improvements are possible. The approximation technique used here could be also applied recursively to some semialgebraic subexpressions, in order to reduce the degree of the POP instances.

Finally, we plan to interface the present framework with the Coq proof assistant [10], by exploiting formally certified symbolic-numeric algorithms [19]. We believe that hybrid certification techniques (combinations of formal methods) could be a suitable option to formalize the remaining nonlinear inequalities within reasonable amount of CPU time in order to complete the remaining part of the formal verification of the proof of Kepler conjecture.

ACKNOWLEDGEMENTS

The authors thank the anonymous referees for helpful comments and suggestions to improve this paper.

REFERENCES

- [1] Behzad Akbarpour and Lawrence Charles Paulson. Metitarski: An automatic theorem prover for real-valued special functions. *J. Autom. Reason.*, 44(3):175–205, March 2010.
- [2] M. Akian, S. Gaubert, and V. N. Kolokoltsov. Set coverings and invertibility of functional galois connections. In G. L. Litvinov and V. P. Maslov, editors, *Idempotent Mathematics and Mathematical Physics*, Contemporary Mathematics, pages 19–51. AMS, 2005. math.FA/0403441.
- [3] M. Akian, S. Gaubert, and A. Lakhrouf. The max-plus finite element method for solving deterministic optimal control problems: basic properties and convergence analysis. *SIAM J. Control Optim.*, 47(2):817–848, 2008.
- [4] Xavier Allamigeon, Stéphane Gaubert, Victor Magron, and Benjamin Werner. Certification of bounds of non-linear functions : the templates method, 2013. To appear in the Proceedings of Conferences on Intelligent Computer Mathematics, CICM 2013 Calculemus, Bath.
- [5] Martin Berz and Kyoko Makino. Rigorous global search using taylor models. In *Proceedings of the 2009 conference on Symbolic numeric computation*, SNC '09, pages 11–20, New York, NY, USA, 2009. ACM.
- [6] Frédéric Besson. Fast reflexive arithmetic tactics the linear case and beyond. In *Proceedings of the 2006 international conference on Types for proofs and programs*, TYPES'06, pages 48–62, Berlin, Heidelberg, 2007. Springer-Verlag.
- [7] Brian Borchers. Csdp, a c library for semidefinite programming., 1997.
- [8] G. Calafiore and F. Dabbene. Reduced vertex set result for interval semidefinite optimization problems. *Journal of Optimization Theory and Applications*, 139:17–33, 2008. 10.1007/s10957-008-9423-1.
- [9] Coralía Cartis, Nicholas I. M. Gould, and Philippe L. Toint. Adaptive cubic regularisation methods for unconstrained optimization. part i: motivation, convergence and numerical results. *Math. Program.*, 127(2):245–295, 2011.
- [10] The Coq Proof Assistant. <http://coq.inria.fr/>.
- [11] W. H. Fleming and W. M. McEneaney. A max-plus-based algorithm for a Hamilton-Jacobi-Bellman equation of nonlinear filtering. *SIAM J. Control Optim.*, 38(3):683–710, 2000.
- [12] Stéphane Gaubert, William M. McEneaney, and Zheng Qu. Curse of dimensionality reduction in max-plus based approximation methods: Theoretical estimates and improved pruning algorithms. In *CDC-ECE*, pages 1054–1061. IEEE, 2011.
- [13] Thomas C. Hales. Introduction to the flyspeck project. In Thierry Coquand, Henri Lombardi, and Marie-Françoise Roy, editors, *Mathematics, Algorithms, Proofs*, number 05021 in Dagstuhl Seminar Proceedings, Dagstuhl, Germany, 2006. Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany.
- [14] Thomas C. Hales, John Harrison, Sean McLaughlin, Tobias Nipkow, Steven Obua, and Roland Zumkeller. A revision of the proof of the kepler conjecture. *Discrete & Computational Geometry*, 44(1):1–34, 2010.
- [15] Eldon R. Hansen. Sharpening interval computations. *Reliable Computing*, 12(1):21–34, 2006.
- [16] E.R. Hansen and R.I. Greenberg. An interval newton method. *Applied Mathematics and Computation*, 12(2-3):89 – 98, 1983.
- [17] John Harrison. Verifying nonlinear real formulas via sums of squares. In Klaus Schneider and Jens Brandt, editors, *Proceedings of the 20th International Conference on Theorem Proving in Higher Order Logics, TPHOLS 2007*, volume 4732 of *Lecture Notes in Computer Science*, pages 102–118, Kaiserslautern, Germany, 2007. Springer-Verlag.
- [18] Didier Henrion, Jean-Bernard Lasserre, and Johan Löfberg. GloptiPoly 3: moments, optimization and semidefinite programming. *Optimization Methods and Software*, 24(4-5):pp. 761–779, August 2009.
- [19] 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. *JSC*, 47(1):1–15, jan 2012. In memory of Wenda Wu (1929–2009).
- [20] Jean B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization*, 11(3):796–817, 2001.
- [21] Jean B. Lasserre and Mihai Putinar. Positivity and optimization for semi-algebraic functions. *SIAM Journal on Optimization*, 20(6):3364–3383, 2010.
- [22] W. M. McEneaney. *Max-plus methods for nonlinear control and estimation*. Systems & Control: Foundations & Applications. Birkhäuser Boston Inc., Boston, MA, 2006.
- [23] W. M. McEneaney. A curse-of-dimensionality-free numerical method for solution of certain HJB PDEs. *SIAM J. Control Optim.*, 46(4):1239–1276, 2007.
- [24] W. M. McEneaney, A. Deshpande, and S. Gaubert. Curse-of-complexity attenuation in the curse-of-dimensionality-free method for HJB PDEs. In *Proc. of the 2008 American Control Conference*, pages 4684–4690, Seattle, Washington, USA, June 2008.
- [25] W. M. McEneaney and L. J. Klueber. Convergence rate for a curse-of-dimensionality-free method for a class of HJB PDEs. *SIAM J. Control Optim.*, 48(5):3052–3079, 2009/10.
- [26] David Monniaux and Pierre Corbineau. On the generation of Positivstellensatz witnesses in degenerate cases. In Marko Van Eekelen, Herman Geuvers, Julien Schmaltz, and Freek Wiedijk, editors, *Interactive Theorem Proving (ITP)*, volume 6898 of *Lecture Notes in Computer Science*, pages 249–264. Springer Verlag, August 2011.
- [27] Tiago M. Montanher. Intsolver: An interval based toolbox for global optimization.
- [28] Pablo A. Parrilo and Bernd Sturmfels. *Minimizing polynomial functions*, volume 60 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 83–99. Amer. Math. Soc., Providence, RI, 2003.
- [29] M. Putinar. Positive polynomials on compact semi-algebraic sets. *Indiana University Mathematics Journal*, 42(3):969–984, 1993.
- [30] Cordian Riener, Thorsten Theobald, Lina Jansson Andrén, and Jean B. Lasserre. Exploiting symmetries in sdp-relaxations for polynomial optimization. *CoRR*, abs/1103.0486, 2011.
- [31] Srinivas Sridharan, Mile Gu, Matthew R. James, and William M. McEneaney. Reduced-complexity numerical method for optimal gate synthesis. *Phys. Rev. A*, 82:042319, Oct 2010.
- [32] Jos F. Sturm. Using sedumi 1.02, a matlab toolbox for optimization over symmetric cones, 1998.
- [33] Hayato Waki, Sunyoung Kim, Masakazu Kojima, and Masakazu Mura-matsu. Sums of squares and semidefinite programming relaxations for polynomial optimization problems with structured sparsity. *SIAM Journal on Optimization*, 17:218–242, 2006.
- [34] Hayato Waki, Sunyoung Kim, Masakazu Kojima, Masakazu Mura-matsu, and Hiroshi Sugimoto. Algorithm 883: Sparsepop—a sparse semidefinite programming relaxation of polynomial optimization problems. *ACM Trans. Math. Softw.*, 35(2), 2008.
- [35] M. Yamashita, K. Fujisawa, K. Nakata, M. Nakata, M. Fukuda, K. Kobayashi, and K. Goto. A high-performance software package for semidefinite programs: Sdpa7. Technical report, Dept. of Information Sciences, Tokyo Institute of Technology, Tokyo, Japan, 2010.
- [36] Roland Zumkeller. *Rigorous Global Optimization*. PhD thesis, École Polytechnique, 2008.