arXiv:1507.03331v7 [cs.NA] 25 Nov 2016

A

Certified Roundoff Error Bounds Using Semidefinite Programming

VICTOR MAGRON, CNRS Verimag
GEORGE CONSTANTINIDES, Imperial College London
ALASTAIR DONALDSON, Imperial College London

Roundoff errors cannot be avoided when implementing numerical programs with finite precision. The ability to reason about rounding is especially important if one wants to explore a range of potential representations, for instance for FPGAs or custom hardware implementations. This problem becomes challenging when the program does not employ solely linear operations, and non-linearities are inherent to many interesting computational problems in real-world applications.

Existing solutions to reasoning possibly lead to either inaccurate bounds or high analysis time in the presence of nonlinear correlations between variables. Furthermore, while it is easy to implement a straightforward method such as interval arithmetic, sophisticated techniques are less straightforward to implement in a formal setting. Thus there is a need for methods which output certificates that can be formally validated inside a proof assistant.

We present a framework to provide upper bounds on absolute roundoff errors of floating-point nonlinear programs. This framework is based on optimization techniques employing semidefinite programming and sums of squares certificates, which can be checked inside the Coq theorem prover to provide formal roundoff error bounds for polynomial programs. Our tool covers a wide range of nonlinear programs, including polynomials and transcendental operations as well as conditional statements. We illustrate the efficiency and precision of this tool on non-trivial programs coming from biology, optimization and space control. Our tool produces more accurate error bounds for 23 % of all programs and yields better performance in 66 % of all programs.

CCS Concepts: •**Design and analysis of algorithms** → **Approximation algorithms analysis;** *Numeric approximation algorithms;* **Mathematical optimization;** *Continuous optimization;* Semidefinite programming; Convex optimization; •**Logic** → **Automated reasoning;**

Additional Key Words and Phrases: correlation sparsity pattern, floating-point arithmetic, formal verification, polynomial optimization, proof assistant, roundoff error, semidefinite programming, transcendental functions.

ACM Reference Format:
Victor Magron, George Constantinides and Alastair Donaldson, 2016. Certified Roundoff Error Bounds Using Semidefinite Programming. *ACM Trans. Math. Softw.* V, N, Article A (January YYYY), 32 pages.
DOI: http://dx.doi.org/10.1145/0000000.0000000

1. INTRODUCTION

Constructing numerical programs which perform accurate computation turns out to be difficult, due to finite numerical precision of implementations such as floating-point or fixed-point representations. Finite-precision numbers induce roundoff errors, and knowledge of

This work was partly funded by the Engineering and Physical Sciences Research Council (EPSRC) "Challenging Engineering" Grant (EP/I020457/1, EP/K034448/1, EP/K015168/1), Royal Academy of Engineering, Imagination Technologies and European Research Council (ERC) "STATOR" Grant Agreement nr. 306595.
Author's addresses: V. Magron, CNRS Verimag, 700 avenue Centrale, 38401 Saint-Martin d'Hères FRANCE; G. Constantinides, Imperial College London, London SW7 2AZ, UK; A. Donaldson, Imperial College London, London SW7 2AZ, UK.
Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© YYYY ACM. 0098-3500/YYYY/01-ARTA $15.00
DOI: http://dx.doi.org/10.1145/0000000.0000000

the range of these roundoff errors is required to fulfill safety criteria of critical programs, as typically arising in modern embedded systems such as aircraft controllers. Such a knowledge can be used in general for developing accurate numerical software, but is also particularly relevant when considering migration of algorithms onto hardware (e.g. FPGAs). The advantage of architectures based on FPGAs is that they allow more flexible choices in number representations, rather than limiting the choice between IEEE standard single or double precision. Indeed, in this case, we benefit from a more flexible number representation while still ensuring guaranteed bounds on the program output.

To obtain lower bounds on roundoff errors, one can rely on testing approaches, such as meta-heuristic search [Borges et al. 2012] or under-approximation tools (e.g. `s3fp` [Chiang et al. 2014]). Here, we are interested in efficiently handling the complementary over-approximation problem, namely to obtain precise upper bounds on the error. This problem boils down to finding tight abstractions of linearities or non-linearities while being able to bound the resulting approximations in an efficient way. For computer programs consisting of linear operations, automatic error analysis can be obtained with well-studied optimization techniques based on SAT/SMT solvers [Haller et al. 2012] and affine arithmetic [Delmas et al. 2009]. However, non-linear operations are key to many interesting computational problems arising in physics, biology, controller implementations and global optimization. Recently, two promising frameworks have been designed to provide upper bounds for roundoff errors of nonlinear programs. The corresponding algorithms rely on Taylor-interval methods [Solovyev et al. 2015], implemented in the `FPTaylor` tool, and on combining SMT with interval arithmetic [Darulova and Kuncak 2014], implemented in the `Rosa` real compiler.

The complexity of the mathematics underlying techniques for nonlinear reasoning, and the intricacies associated with constructing an efficient implementation, are such that a means for independent formal validation of results is particularly desirable. The `Rosa` tool is based on theoretical results that should provide sound over-approximations of error bounds. While `Rosa` relies on an SMT solver capable of generating unsatisfiability proof witnesses (thus allowing independent soundness checking), it does not formally verify these certificates inside a proof assistant. To the best of our knowledge, `FPTaylor` and GAPPA are the only academic software tools that can produce formal proof certificates. For `FPTaylor`, this is based on the framework developed in [Solovyev and Hales 2013] to verify nonlinear inequalities in HOL-LIGHT [Harrison 1996] using Taylor-interval methods. However, most of computation performed in the informal optimization procedure ends up being redone inside the HOL-LIGHT proof assistant, yielding a formal verification which may be computationally demanding.

The aim of this work is to provide a formal framework to perform automated precision analysis of computer programs that manipulate finite-precision data using nonlinear operators. For such programs, guarantees can be provided with certified programming techniques. Semidefinite programming (SDP) is relevant to a wide range of mathematical fields, including combinatorial optimization, control theory and matrix completion. In 2001, Lasserre introduced a hierarchy of SDP relaxations [Lasserre 2001] for approximating polynomial infima. Our method to bound the error is a decision procedure based on a specialized variant of the Lasserre hierarchy [Lasserre 2006]. The procedure relies on SDP to provide sparse sum-of-squares decompositions of nonnegative polynomials. Our framework handles polynomial program analysis (involving the operations $+, \times, -$) as well as extensions to the more general class of semialgebraic and transcendental programs (involving $\sqrt{\cdot}, /, \min, \max, \arctan, \exp$), following the approximation scheme described in [Magron et al. 2015a].

1.1. Overview of our Method

We present an overview of our method and of the capabilities of related techniques, using an example. Consider a program implementing the following polynomial expression f:

$$
\begin{aligned}
f(\mathbf{x}) := & \; x_2 \times x_5 + x_3 \times x_6 - x_2 \times x_3 - x_5 \times x_6 \\
& + x_1 \times (-x_1 + x_2 + x_3 - x_4 + x_5 + x_6) ,
\end{aligned}
$$

where the six-variable vector $\mathbf{x} := (x_1, x_2, x_3, x_4, x_5, x_6)$ is the input of the program. For this example, assume that the set $\mathbf{X}$ of possible input values is a product of closed intervals: $\mathbf{X} = [4.00, 6.36]^6$. This function f together with the set $\mathbf{X}$ appear in many inequalities arising from the the proof of the Kepler Conjecture [Hales 2006], yielding challenging global optimization problems.

The polynomial expression f is obtained by performing 15 basic operations (1 negation, 3 subtractions, 6 additions and 5 multiplications). When executing this program with a set of floating-point numbers $\hat{\mathbf{x}} := (\hat{x}_1, \hat{x}_2, \hat{x}_3, \hat{x}_4, \hat{x}_5, \hat{x}_6) \in \mathbf{X}$, one actually computes a floating-point result $\hat{f}$, where all operations $+, -, \times$ are replaced by the respectively associated floating-point operations $\oplus, \ominus, \otimes$. The results of these operations comply with IEEE 754 standard arithmetic [IEEE 2008] (see relevant background in Section 2.1). Here, for the sake of clarity, we do not consider real input variables but we do it later on while performing detailed comparison (see Section 4). For instance, (in the absence of underflow) one can write $\hat{x}_2 \otimes \hat{x}_5 = (x_2 \times x_5)(1 + e_1)$, by introducing an error variable e_1 such that $-\epsilon \leq e_1 \leq \epsilon$, where the bound ϵ is the machine precision (e.g. $\epsilon = 2^{-24}$ for single precision). One would like to bound the absolute roundoff error $|r(\mathbf{x}, \mathbf{e})| := |\hat{f}(\mathbf{x}, \mathbf{e}) - f(\mathbf{x})|$ over all possible input variables $\mathbf{x} \in \mathbf{X}$ and error variable $e_1, \ldots, e_{15} \in [-\epsilon, \epsilon]$. Let us define $\mathbf{E} := [-\epsilon, \epsilon]^{15}$ and $\mathbf{K} := \mathbf{X} \times \mathbf{E}$. Then our bound problem can be cast as finding the maximum $r^\star$ of $| \; r \; |$ over $\mathbf{K}$, yielding the following nonlinear optimization problem:

$$
\begin{aligned}
r^\star := & \max_{(\mathbf{x}, \mathbf{e}) \in \mathbf{K}} |r(\mathbf{x}, \mathbf{e})| \\
= & \; \max\{- \min_{(\mathbf{x}, \mathbf{e}) \in \mathbf{K}} r(\mathbf{x}, \mathbf{e}), \max_{(\mathbf{x}, \mathbf{e}) \in \mathbf{K}} r(\mathbf{x}, \mathbf{e})\} \; ,
\end{aligned} \tag{1}
$$

One can directly try to solve these two polynomial optimization problems using classical SDP relaxations [Lasserre 2001]. As in [Solovyev et al. 2015], one can also decompose the error term r as the sum of a term $l(\mathbf{x}, \mathbf{e})$, which is affine w.r.t. $\mathbf{e}$, and a nonlinear term $h(\mathbf{x}, \mathbf{e}) := r(\mathbf{x}, \mathbf{e}) - l(\mathbf{x}, \mathbf{e})$. Then the triangular inequality yields:

$$
r^\star \leq \max_{(\mathbf{x}, \mathbf{e}) \in \mathbf{K}} |l(\mathbf{x}, \mathbf{e})| + \max_{(\mathbf{x}, \mathbf{e}) \in \mathbf{K}} |h(\mathbf{x}, \mathbf{e})| \; . \tag{2}
$$

It follows for this example that $l(\mathbf{x}, \mathbf{e}) = x_2 x_5 e_1 + x_3 x_6 e_2 + (x_2 x_5 + x_3 x_6) e_3 + \cdots + f(\mathbf{x}) e_{15} = \sum_{i=1}^{15} s_i(\mathbf{x}) e_i$, with $s_1(\mathbf{x}) := x_2 x_5, s_2(\mathbf{x}) := x_3 x_6, \ldots, s_{15}(\mathbf{x}) := f(\mathbf{x})$. The *Symbolic Taylor Expansions* method [Solovyev et al. 2015] consists of using a simple branch and bound algorithm based on interval arithmetic to compute a rigorous interval enclosure of each polynomial s_i, $i = 1, \ldots, 15$, over $\mathbf{X}$ and finally obtain an upper bound of $|l| + |h|$ over $\mathbf{K}$. In contrast, our method uses sparse semidefinite relaxations for polynomial optimization (derived from [Lasserre 2006]) to bound l and basic interval arithmetic as in [Solovyev et al. 2015] to bound $|h|$ (i.e. we use interval arithmetic to bound second-order error terms in the multivariate Taylor expansion of r w.r.t. $\mathbf{e}$).

The following comparison results have been obtained on an Intel Core i7-5600U CPU (2.60 GHz). All execution times have been computed by averaging over five runs.

— A direct attempt to solve the two polynomial problems occurring in Equation (1) fails as the SDP solver (in our case SDPA [Yamashita et al. 2010]) runs out of memory.

— Using our method implemented in the `Real2Float` tool, one obtains an upper bound of 760ϵ for $|l|+|h|$ over $\mathbf{K}$ in 0.15 seconds. This bound is provided together with a certificate which can be formally checked inside the COQ proof assistant in 0.20 seconds.
— After normalizing the polynomial expression and using basic interval arithmetic, one obtains 8 times more quickly a coarser bound of 922ϵ.
— Symbolic Taylor expansions implemented in `FPTaylor` [Solovyev et al. 2015] provide a more precise bound of 721ϵ, but the analysis time is 28 times slower than with our implementation. Formal verification of this bound inside the HOL-LIGHT proof assistant takes 27.7 seconds, which is 139 times slower than proof checking with `Real2Float` inside COQ. One can obtain an even more precise bound of 528ϵ (but 37 times slower than with our implementation) by turning on the improved rounding model of `FPTaylor` and limiting the number of branch and bound iterations to 10000. The drawback of this bound is that it cannot be formally verified.
— Finally, a sligthly coarser bound of 762ϵ is obtained with the `Rosa` real compiler [Darulova and Kuncak 2014], but the analysis is 19 times slower than with our implementation and we cannot get formal verification of this bound.

1.2. Related Works

SMT solvers allow analysis of programs with various semantics or specifications but are limited for the manipulation of problems involving nonlinear arithmetic. Several solvers, including Z3 [De Moura and Bjørner 2008], provide partial support for the IEEE floating-point standard [Rümmer and Wahl 2010]. They suffer from a lack of scalability when used for roundoff error analysis in isolation (as emphasized in [Darulova and Kuncak 2014]), but can be integrated into existing frameworks, e.g. FPHILE [Paganelli and Ahrendt 2013]. The procedure in [Gao et al. 2013] can solve SMT problems over the real numbers, using interval constraint propagation, but has not yet been applied to quantification of roundoff error.

The `Rosa` tool [Darulova and Kuncak 2014] provides a way to compile functional SCALA programs involving semialgebraic functions and conditional statements. The tool uses affine arithmetic to provide sound over-approximations of roundoff errors, allowing for generation of finite precision implementations which fulfill the required precision given as input by the user. This tool thus relies on abstract interpration but bounds of the affine expressions are provided through an optimization procedure based on SMT. In our case, we use the same rounding model but provide approximations which are affine w.r.t. the additional error variables and nonlinear w.r.t. the input variables. Instead of using SMT, we bound the resulting expressions with optimization techniques based on semidefinite programming.
Abstract interpretation [Cousot and Cousot 1977] has been extensively used in the context of static analysis to provide sound over-approximations, called *abstractions*, of the sets of values taken by program variables. The effects of variable assignments, guards and conditional branching statements are handled with several domain specific operators (e.g. inclusion, meet and join). Well studied abstract domains include intervals [Moore 1962] as well as more complicated frameworks based on affine arithmetic [Stolfi and de Figueiredo 2003], octogons [Miné 2006], zonotopes [Ghorbal et al. 2010], polyhedra [Chen et al. 2008], interval polyhedra [Chen et al. 2009], some of them being implemented inside a tool called APRON [Jeannet and Miné 2009]. Abstract domains provide sound over-approximations of program expressions, and allow upper bounds on roundoff error to be computed. The GAPPA tool [Daumas and Melquiond 2010] relies on interval abstract domains with an extension to affine domains [Linderman et al. 2010], to reason about roundoff errors. As demonstrated in [Solovyev et al. 2015], the bounds obtained inside GAPPA are often coarser than other methods. Formal guarantees can be provided as GAPPA benefits from an interface with COQ while making use of interval libraries [Melquiond 2012] relying on formalized floating-points [Boldo and Melquiond 2011]. The static analysis commercial tool FLUCTUAT (with a free academic version) relies on affine abstract domains [Blanchet et al. 2003] and

Table I. Comparison of roundoff error tools w.r.t. expressiveness.

Feature	Real2Float	Rosa	FPTaylor	GAPPA	FLUCTUAT
Basic FP operations/formats	√	√	√	√	√
Special values ($\pm\infty$, NaN)				√	√
Improved rounding model			√	√	√
Input uncertainties	√	√	√	√	√
Transcendental functions	√		√		
Discontinuity errors	√	√			√
Proof certificates	√		√	√	

techniques which are very similar to the ones in Rosa, including interval subdivision. This tool does not perform optimization but uses forward computation to analyze floating-point programs written in C. Furthermore, FLUCTUAT also has a procedure for discontinuity errors [Ghorbal et al. 2010]. The GAPPA and FLUCTUAT tools use a different rounding model (also available as an option inside FPTaylor) based on a piecewise constant absolute error bound. This is more precise than the simple rounding model used in our framework but requires (possibly) extensive use of a branch and bound algorithm as each interval has to be subdivided in intervals $[2^n, 2^{n+1}]$ for several values of the integer n. In [Solovyev et al. 2015], the authors provide a table (Table 1) comparing relevant features of FPTaylor with three other tools (Rosa, GAPPA and FLUCTUAT), performing roundoff error estimation. In a similar fashion, we summarize the main features related to our tool Real2Float and the same four above-mentioned tools used for our further benchmark comparisons w.r.t. their expressiveness in Table I.

Computing sound bounds of nonlinear expressions is mandatory to perform formal analysis of finite precision implementations and can be performed with various optimization tools. In the polynomial case, alternative approaches to semidefinite relaxations are based on decomposition in the multivariate Bernstein basis. Formal verification of bounds obtained with this decomposition has been investigated by Munõz and Narkawicz [Muñoz and Narkawicz 2013] in the PVS theorem prover. We are not aware of any work based on these techniques which can quantify roundoff errors. Another decomposition of nonnegative polynomials into SOS certificates consists in using the Krivine-Handelman [Krivine 1964; Handelman 1988] representation and boils down to solving linear programming (LP) relaxations. In our case, we use a different representation, leading to solve SDP relaxations. The Krivine-Handelman representation has been used in [Boland and Constantinides 2010] to compute roundoff error bounds. LP relaxations often provide coarser bounds than SDP relaxations and it has been proven in [Lasserre 2009] that generically finite convergence does not occur for convex problems, with the exception of the linear case. The work in [Roux 2015] focuses on formalization of roundoff errors bounds related to positive definiteness verification. Branch and bound methods with Taylor models [Berz and Makino 2009] are not restricted to polynomial systems and have been formalized [Solovyev and Hales 2013] to solve nonlinear inequalities occurring in the proof of Kepler Conjecture. Symbolic Taylor Expansions [Solovyev et al. 2015] have been implemented in the FPTaylor tool to compute formal bounds of roundoff errors for programs involving both polynomial and transcendental functions.

1.3. Contributions

Our key contributions can be summarized as follows:

— We present an optimization algorithm providing sound over-approximations for roundoff errors of floating-point nonlinear programs. This algorithm is based on sparse sums of squares programming [Lasserre 2006]. In comparison with other methods, our algorithm allows us to obtain tighter upper bounds, while overcoming scalability and numerical issues inherent in SDP solvers [Todd 2001]. Our algorithm can currently handle programs implementing polynomial functions, but also involving non-polynomial components, in-

cluding either semialgebraic or transcendental operations (e.g. $/, \sqrt{}, \arctan, \exp$), as well as conditional statements. Programs containing iterative or while loops are not currently supported.

— Our framework is fully implemented in the `Real2Float` tool. Among several features, the tool can optionally perform formal verification of roundoff error bounds for polynomial programs, inside the COQ proof assistant [Coq 2016]. The most recent software release of `Real2Float` provides OCAML [OCaml 2015] and COQ libraries and is freely available.[1] Our implementation tool is built on top of the `NLCertify` verification system [Magron 2014]. Precision and efficiency of the tool are evaluated on several benchmarks coming from the existing literature. Numerical experiments demonstrate that our method competes well with recent approaches relying on Taylor-interval approximations [Solovyev et al. 2015] or combining SMT solvers with affine arithmetic [Darulova and Kuncak 2014]. We also compared our tool with GAPPA [Daumas and Melquiond 2010] and FLUCTUAT [Delmas et al. 2009].

The paper is organized as follows. In Section 2, we present mandatory background on roundoff errors due to finite precision arithmetic before describing our nonlinear program semantics (Section 2.1). Then we recall how to perform certified polynomial optimization based on semidefinite programming (Section 2.2) and how to obtain formal bounds while checking the certificates inside the COQ proof assistant (Section 2.3). Section 3 contains the main contribution of the paper, namely how to compute tight over-approximations for roundoff errors of nonlinear programs with sparse semidefinite relaxations. Finally, Section 4 is devoted to the evaluation of our nonlinear verification tool `Real2Float` on benchmarks arising from control systems, optimization, physics and biology, as well as comparisons with the tools `FPTaylor`, `Rosa`, GAPPA and FLUCTUAT.

2. PRELIMINARIES

2.1. Program Semantics and Floating-point Numbers

We support conditional code without procedure calls or loops. Despite these restrictions, we can consider a wide range of nonlinear programs while assuming that important numerical calculations can be expressed in a loop-free manner. Our programs are encoded in an ML-like language:

```
let box_prog     x1 ... xn = [(a1, b1); ... ; (an, bn)];;
let obj_prog     x1 ... xn = [(f(x), ϵReal2Float)];;
let cstr_prog    x1 ... xn = [g1(x); ... ; gk(x)];;
let uncert_prog  x1 ... xn = [u1; ... ; un];;
```

Here, the first line encodes interval floating-point bound constraints for input variables, namely $\mathbf{x} := (x_1, \dots, x_n) \in [a_1, b_1] \times \cdots \times [a_n, b_n]$. The second line provides the function $f(\mathbf{x})$ as well as the total roundoff error bound $\epsilon_{\texttt{Real2Float}}$. Then, one encodes polynomial nonnegativity constraints over the input variables, namely $g_1(\mathbf{x}) \geq 0, \dots, g_k(\mathbf{x}) \geq 0$. Finally, the last line allows the user to specify a numerical constant u_i to associate a given uncertainty to the variable x_i, for each $i = 1, \dots, n$.

The type of numerical constants is denoted by `C`. In our current implementation, the user can choose either 64 bit floating-point or arbitrary-size rational numbers. This type `C` is used for the terms $\epsilon_{\texttt{Real2Float}}$, $u_1, \dots, u_n$, $a_1, \dots, a_n$, $b_1, \dots, b_n$. The inductive type of polynomial expressions with coefficients in `C` is `pExprC` defined as follows:

```
type pexprC = Pc of C | Px of positive
| Psub of pexprC * pexprC | Pneg of pexprC
| Padd of pexprC * pexprC
```

[1] forge.ocamlcore.org/frs/?group_id=351

```
| Pmul of pexprC * pexprC
```

The constructor `Px` takes a positive integer as argument to represent either an input or local variable. The inductive type `nlexpr` of nonlinear expressions (such as $f(\mathbf{x})$) is defined as follows:

```
type nlexpr =
| Pol of pexprC | Neg of nlexpr
| Add of nlexpr * nlexpr
| Mul of nlexpr * nlexpr
| Sub of nlexpr * nlexpr
| Div of nlexpr * nlexpr | Sqrt of nlexpr
| Transc of transc * nlexpr
| IfThenElse of pexprC * nlexpr * nlexpr
| Let of positive * nlexpr * nlexpr
```

The type `transc` corresponds to a *dictionary* $\mathcal{D}$ of special functions. In our case $\mathcal{D} := \{\exp, \log, \cos, \sin, \tan, \arccos, \arcsin, \arctan\}$. For instance, the term `Transc (exp,` $f(\mathbf{x})$`)` represents the program implementing $\exp(f(\mathbf{x}))$.

Given a polynomial expression p and two nonlinear expressions f and g, the term `IfThenElse(`$p(\mathbf{x})$`,` $f(\mathbf{x})$`,` $g(\mathbf{x})$`)` represents the conditional program implementing the expression[2] **if** $(p(\mathbf{x}) \geq 0)$ $f(\mathbf{x})$ **else** $g(\mathbf{x})$. The constructor **Let** allows us to define local variables in an ML fashion, e.g. **let** $t_1 = 331.4 + 0.6 * T$ **in** $-t_1 * v/((t_1 + u) * (t_1 + u))$ (part of the *doppler1* program considered in Section 4).

Finally, one obtains rounded nonlinear expressions using a recursive procedure `round`, defined according to Equation (3) and Equation (4). Rounded expressions are supported inside conditions. When an uncertainty u_i is specified for an input variable x_i, the corresponding rounded expression is given by $x_i\,(1 + e)$, with $\mid e \mid \leq u_i$, the uncertainty u_i being a relative error.

We adopt the standard practice [Higham 2002] to approximate a real number x with its closest floating-point representation $\hat{x} = x(1+e)$, with $|e|$ is less than the machine precision ϵ. In the sequel, we neglect both overflow and denormal range values. The operator $\hat{\ }$ is called the rounding operator and can be selected among rounding to nearest, rounding toward zero (resp. $\pm\infty$). In the sequel, we assume rounding to nearest. The scientific notation of a binary (resp. decimal) floating-point number $\hat{x}$ is a triple (s, sig, exp) consisting of a sign bit s, a *significand* $sig \in [1, 2)$ (resp. $[1, 10)$) and an *exponent* exp, yielding numerical evaluation $(-1)^s\, sig\, 2^{exp}$ (resp. $(-1)^s\, sig\, 10^{exp}$).

The value of ϵ actually gives the upper bound on the relative floating-point error and is equal to $2^{-\text{prec}}$, where prec is called the *precision*, referring to the number of significand bits used. For single precision floating-point, one has prec = 24. For double (resp. quadruple) precision, one has prec = 53 (resp. prec = 113). Let $\mathbb{R}$ denote the set of real numbers and $\mathbb{F}$ the set of binary floating-point numbers.

For each real-valued operation $\texttt{bop}_{\mathbb{R}} \in \{+, -, \times, /\}$, the result of the corresponding floating-point operation $\texttt{bop}_{\mathbb{F}} \in \{\oplus, \ominus, \otimes, \oslash\}$ satisfies the following when complying with IEEE 754 standard arithmetic [IEEE 2008] (without overflow, underflow and denormal occurrences):

$$\texttt{bop}_{\mathbb{F}}\,(\hat{x}, \hat{y}) = \texttt{bop}_{\mathbb{R}}\,(\hat{x}, \hat{y})\,(1 + e) \ , \quad \mid e \mid \leq \epsilon = 2^{-\text{prec}} \ . \tag{3}$$

Other operations include special functions taken from $\mathcal{D}$, containing the unary functions tan, arctan, cos, arccos, sin, arcsin, exp, log, $(\cdot)^r$ with $r \in \mathbb{R} \setminus \{0\}$. For $f_{\mathbb{R}} \in \mathcal{D}$, the corresponding

[2]Our general framework could theoretically handle nested if statements. However, our current implementation is limited to programs involving single top level conditional statements

floating-point evaluation satisfies

$$f_{\mathbb{F}}(\hat{x}) = f_{\mathbb{R}}(\hat{x})(1+e) \ , \quad | e | \leq \epsilon(f_{\mathbb{R}}) \ . \tag{4}$$

The value of the relative error bound $\epsilon(f_{\mathbb{R}})$ differs from the machine precision ϵ in Equation (3) and has to be properly adjusted on a per-operator basis. We refer the interested reader to [Bingham and Leslie-Hurd 2014] for relative error bound verification of transcendental functions (see also [Harrison 2000] for formalization in HOL-LIGHT).

2.2. SDP Relaxations for Polynomial Optimization

The sums of squares method involves approximation of polynomial inequality constraints by sums of squares (SOS) equality constraints. Here we recall mandatory background about SOS. We apply this method in Section 3 to solve the problems of Equation (1) when the nonlinear function r is a polynomial. In the sequel, let us denote by n the number of initial variables of the polynomial optimization problem and by k the number of optimization constraints.

2.2.1. Sums of squares certificates and SDP. First we recall basic facts about generation of SOS certificates for polynomial optimization, using semidefinite programming, which can be found in texts such as [Lasserre 2001]. Denote by $\mathbb{R}[\mathbf{x}]$ the vector space of polynomials and by $\mathbb{R}_{2d}[\mathbf{x}]$ the restriction of $\mathbb{R}[\mathbf{x}]$ to polynomials of degree at most $2d$. Let us define the set of SOS polynomials:

$$\Sigma[\mathbf{x}] := \Big\{ \sum_i q_i^2, \ \text{with } q_i \in \mathbb{R}[\mathbf{x}] \Big\} \ , \tag{5}$$

as well as its restriction $\Sigma_{2d}[\mathbf{x}] := \Sigma[\mathbf{x}] \bigcap \mathbb{R}_{2d}[\mathbf{x}]$ to polynomials of degree at most $2d$. For instance, the following bivariate polynomial $\sigma(\mathbf{x}) := 1 + (x_1^2 - x_2^2)^2$ lies in $\Sigma_4[\mathbf{x}] \subseteq \mathbb{R}_4[\mathbf{x}]$.

Optimization methods based on SOS use the implication $r \in \Sigma[\mathbf{x}] \implies \forall \mathbf{x} \in \mathbb{R}^n$, $r(\mathbf{x}) \geq 0$, i.e. the inclusion of $\Sigma[\mathbf{x}]$ in the set of nonnegative polynomials.

The underlying reason for using SOS polynomials is that optimizing over positive polynomials is NP Hard [Laurent 2009]. Thus, one would like to replace such positivity constraints by more tractable ones, and in particular the SOS decompositions admitted by positive polynomials provide a suitable alternative: when fixing the degree of such decompositions, the resulting relaxed problem becomes more tractable.

Given $r \in \mathbb{R}[\mathbf{x}]$, one considers the following polynomial minimization problem:

$$r^* := \inf_{\mathbf{x} \in \mathbb{R}^n} \{ r(\mathbf{x}) \ : \ \mathbf{x} \in \mathbf{K} \} \ , \tag{6}$$

where the set of constraints $\mathbf{K} \subseteq \mathbb{R}^n$ is defined by

$$\mathbf{K} := \{ \mathbf{x} \in \mathbb{R}^n : g_1(\mathbf{x}) \geq 0, \dots, g_k(\mathbf{x}) \geq 0 \} \ ,$$

for polynomial functions $g_1, \dots, g_k$. The set $\mathbf{K}$ is called a *basic semialgebraic* set. Membership of semialgebraic sets is ensured by satisfying conjunctions of polynomial nonnegativity constraints.

Remark 2.1. When the input variables satisfy interval constraints $\mathbf{x} \in [a_1, b_1] \times \cdots \times [a_n, b_n]$ then one can easily show that there exists some integer $M > 0$ such that $M - \sum_{i=1}^n x_i^2 \geq 0$. In the sequel, we assume that this nonnegativity constraint appears explicitly in the definition of $\mathbf{K}$. Such an assumption is mandatory to prove the convergence of semidefinite relaxations recalled in Theorem 2.3.

In general, the objective function r and the set of constraints $\mathbf{K}$ can be nonconvex, which makes Problem (6) difficult to solve in practice. One can rewrite Problem (6) as the equiv-

alent maximization problem:

$$r^* := \sup_{\mu \in \mathbb{R}} \{ \mu \, : \, r(\mathbf{x}) - \mu \geq 0 \, , \; \forall \mathbf{x} \in \mathbf{K} \, \} \, . \tag{7}$$

Now we outline how to handle the nonnegativity constraint $r - \mu \geq 0$. Given a nonnegative polynomial $p \in \mathbb{R}[\mathbf{x}]$, the existence of an SOS decomposition $p = \sum_i q_i^2$ valid over $\mathbb{R}^n$, is equivalent to the existence of a symmetric real matrix $\mathbf{Q}$, a solution of the following linear matrix feasibility problem:

$$r(\mathbf{x}) = \mathbf{m}_d(\mathbf{x})^\intercal \, \mathbf{Q} \, \mathbf{m}_d(\mathbf{x}) \, , \quad \forall \mathbf{x} \in \mathbb{R}^n, \tag{8}$$

where $\mathbf{m}_d(\mathbf{x}) := (1, x_1, \ldots, x_n, x_1^2, x_1 x_2, \ldots, x_n^d)$ and the matrix $\mathbf{Q}$ has only nonnegative eigenvalues. Such a matrix $\mathbf{Q}$ is called *positive semidefinite*. The vector $\mathbf{m}_d$ (resp. matrix $\mathbf{Q}$) has a size (resp. dimension) equal to $s_n^d := \binom{n+d}{d}$. Problem (8) can be handled with semidefinite programming (SDP) solvers, such as MOSEK [Andersen and Andersen 2000] or SDPA [Yamashita et al. 2010] (see [Vandenberghe and Boyd 1994] for specific background about SDP). Then, one computes the "LDL" decomposition $\mathbf{Q} = \mathbf{L}^\intercal \mathbf{D} \mathbf{L}$ (a variant of the classical Cholesky decomposition), where $\mathbf{L}$ is a lower triangular matrix and $\mathbf{D}$ is a diagonal matrix. Finally, one obtains $r(\mathbf{x}) = (\mathbf{L} \, \mathbf{m}_d(\mathbf{x}))^\intercal \, \mathbf{D} \, (\mathbf{L} \, \mathbf{m}_d(\mathbf{x})) = \sum_{i=0}^{s_n^d} q_i(\mathbf{x})^2$. Such a decomposition is called a sums of squares (SOS) *certificate*.

Example 2.2. Let us define $r(\mathbf{x}) := \frac{1}{4} + x_1^4 - 2x_1^2 x_2^2 + x_2^4$. With $\mathbf{m}_2(\mathbf{x}) = (1, x_1, x_2, x_1^2, x_1 x_2, x_2^2)$, one solves the linear matrix feasibility problem $r(\mathbf{x}) = \mathbf{m}_2(\mathbf{x})^\intercal \, \mathbf{Q} \, \mathbf{m}_2(\mathbf{x})$. One can show that the solution writes $\mathbf{Q} = \mathbf{L}^\intercal \mathbf{D} \mathbf{L}$ for a 6×6 matrix $\mathbf{L}$ and a diagonal matrix $\mathbf{D}$ with entries $(\frac{1}{2}, 0, 0, 1, 0, 0)$, yielding the SOS decomposition: $r(\mathbf{x}) = (\frac{1}{2})^2 + (x_1^2 - x_2^2)^2$. This is enough to prove that p is nonnegative.

2.2.2. Dense SDP relaxations for polynomial optimization. In order to solve our goal problem (Problem (1)), we are trying to solve Problem (6), recast as Problem (7). We first explain how to obtain tractable approximations of this difficult problem. Define $g_0 := 1$. The hierarchy of SDP relaxations developed by Lasserre [Lasserre 2001] provides lower bounds of r^*, through solving the optimization problems $(\mathbf{P}_d)$:

$$(\mathbf{P}_d) : \begin{cases} p_d^\star := \sup\limits_{\sigma_j, \mu} \;\; \mu \;\; , \\ \qquad\quad \text{s.t.} \;\; r(\mathbf{x}) - \mu = \sum_{j=0}^{k} \sigma_j(\mathbf{x}) g_j(\mathbf{x}) \, , \forall \mathbf{x} \, , \\ \qquad\qquad\;\; \mu \in \mathbb{R} \, , \sigma_j \in \Sigma[\mathbf{x}] \, , \qquad j = 0, \ldots, k \, , \\ \qquad\qquad\;\; \deg(\sigma_j g_j) \leq 2d, \qquad j = 0, \ldots, k \, . \end{cases}$$

One can solve $(\mathbf{P}_d)$ with SDP optimization to find a tuple $(\mu, \sigma_0, \ldots, \sigma_k)$ which enables a proof that $g_1(\mathbf{x}) \geq 0 \wedge \cdots \wedge g_k(\mathbf{x}) \geq 0 \implies r(\mathbf{x}) - \mu \geq 0$.

The next theorem is a consequence of the assumption mentioned in Remark 2.1.

THEOREM 2.3 (LASSERRE [LASSERRE 2001]). *Let $p_d^\star$ be the optimal value of the SDP relaxation $(\mathbf{P}_d)$. Then, the sequence of optimal values $(p_d^\star)_{d \in \mathbb{N}}$ is nondecreasing and converges to $r^\star$.*

The number of SDP variables (i.e. the number of variables of the semidefinite relaxation $(\mathbf{P}_d)$) grows polynomially with the integer d, called the *relaxation order*. Indeed, at a fixed number of variables n, the relaxation $(\mathbf{P}_d)$ involves $O((2d)^n)$ SDP variables and $(k+1)$ linear matrix inequalities (LMIs) of size $O(d^n)$. When d increases, then more accurate lower bounds of $r^\star$ can be obtained, at an increasing computational cost. At a fixed

d, the relaxation $(\mathbf{P}_d)$ involves $O(n^{2d})$ SDP variables and $(d+1)$ linear matrix inequalities (LMIs) of size $O(n^d)$.

Example 2.4. Consider the polynomial f mentioned in Section 1: $f(\mathbf{x}) := x_2x_5 + x_3x_6 - x_2x_3 - x_5x_6 + x_1(-x_1 + x_2 + x_3 - x_4 + x_5 + x_6)$ and the set $\mathbf{K} := [4, 6.36]^6$. The set $\mathbf{K}$ can be equivalently rewritten as:

$$\mathbf{K} := \{ \mathbf{x} \in \mathbb{R}^n \, : \, g_1(\mathbf{x}) \geq 0, \dots, g_7(\mathbf{x}) \geq 0 \},$$

with $g_i(\mathbf{x}) := (6.36 - x_i)(x_i - 4)$ for each $i = 1, \dots, 6$ and $g_7(\mathbf{x}) := 243 - \sum_{i=0}^6 x_i^2$. Here the constant $M = 243$ is chosen so that $M \geq 6 \times 6.36^2$ and the assumption in Remark 2.1 is fulfilled. The number of initial variables of the optimization problem $r^* := \inf_{\mathbf{x} \in \mathbb{R}^n} \{ f(\mathbf{x}) : \mathbf{x} \in \mathbf{K} \}$ is $n = 6$ and the number of optimization constraints is $k = 7$. For $d = 1$, the dense SDP relaxation $(\mathbf{P}_1)$ involves $\binom{n+2d}{2d} = \binom{6+2}{2} = 28$ variables and provides a lower bound $p_1^\star = 20.755$ for r^*. The dense SDP relaxation $(\mathbf{P}_2)$ involves $\binom{6+4}{4} = 210$ variables and provides a tighter lower bound of $p_2^\star = 20.8608$ for r^*.

2.2.3. Exploiting sparsity. Here we recall how to exploit the structured sparsity of the problem to replace one SDP problem $(\mathbf{P}_d)$ by an SDP problem $(\mathbf{S}_d)$ of size $O(\kappa^{2d})$ where κ is the average size of the maximal cliques of the correlation sparsity pattern (csp) of the polynomial variables (see [Waki et al. 2006; Lasserre 2006] for more details). We now present these notions as well as the formulation of sparse SDP relaxations $(\mathbf{S}_d)$.

We denote by $\mathbb{N}^n$ the set of n-tuple of nonnegative integers. The support of a polynomial $r(\mathbf{x}) := \sum_{\boldsymbol{\alpha} \in \mathbb{N}^n} r_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}}$ is defined as $\text{supp}(r) := \{ \boldsymbol{\alpha} \in \mathbb{N}^n \, : \, r_{\boldsymbol{\alpha}} \neq 0 \}$. For instance the support of $r(\mathbf{x}) := \frac{1}{4} + x_1^4 - 2x_1^2x_2^2 + x_2^4$ is $\text{supp}(p) = \{ (0,0), (4,0), (2,2), (0,4) \}$.

Let F_j be the index set of variables which are involved in the polynomial g_j, for each $j = 1, \dots, k$. The correlative sparsity is represented by the $n \times n$ correlation sparsity pattern matrix (csp matrix) $\mathbf{R}$ defined by:

$$\mathbf{R}(i,j) := \begin{cases} 1 & \text{if } i = j \enspace , \\ 1 & \text{if } \exists \boldsymbol{\alpha} \in \text{supp}(f) \text{ such that } \alpha_i, \alpha_j \geq 1 \, , \\ 1 & \text{if } \exists l \in \{1, \dots, k\} \text{ such that } i, j \in F_l \, , \\ 0 & \text{otherwise} \, . \end{cases}$$

We define the undirected csp graph $G(N, E)$ with $N = \{1, \dots, n\}$ and $E = \{\{i,j\} : i, j \in N, \; i < j, \mathbf{R}(i,j) = 1\}$. Then, let $C_1, \dots, C_m \subseteq N$ denote the maximal cliques of $G(N, E)$ and define $n_j := \# C_j$, for each $j = 1, \dots, m$.

Remark 2.5. Assuming that the set $\mathbf{K}$ is as in Remark 2.1, one replaces the constraint $M - \sum_{i=1}^n x_i^2 \geq 0$ by the m redundant additional constraints:

$$g_{k+j} := n_j M^2 - \sum_{i \in C_j} x_i^2 \geq 0 \, , \; j = 1, \dots, m \, , \tag{9}$$

set $k' = k + m$, define the compact semialgebraic set:

$$\mathbf{K}' := \{ \mathbf{x} \in \mathbb{R}^n \, : \, g_1(\mathbf{x}) \geq 0, \dots, g_{k'}(\mathbf{x}) \geq 0 \},$$

and modify Problem (6) into the following optimization problem:

$$r^* := \inf_{\mathbf{x} \in \mathbb{R}^n} \{ r(\mathbf{x}) \, : \, \mathbf{x} \in \mathbf{K}' \} \, . \tag{10}$$

For each $j = 1, \dots, m$, we note $\mathbb{R}_{2d}[\mathbf{x}, C_j]$ the set of polynomials of $\mathbb{R}_{2d}[\mathbf{x}]$ which involve the variables $(x_i)_{i \in C_j}$. We denote $\Sigma[\mathbf{x}, C_j] := \Sigma[\mathbf{x}] \bigcap \mathbb{R}_{2d}[\mathbf{x}, C_j]$. Similarly, we define $\Sigma[\mathbf{x}, F_j]$, for each $j = 1, \dots, k'$. The following program is the sparse variant of the SDP program

$(\mathbf{P}_d)$:

$$(\mathbf{S}_d): \begin{cases} r_d^\star := \sup\limits_{\mu,\sigma_j} \ \mu \ , \\ \qquad \text{s.t.} \ r(\mathbf{x}) - \mu = \sum_{j=0}^{k'} \sigma_j(\mathbf{x}) g_j(\mathbf{x}) \,, \ \forall \mathbf{x} \,, \\ \qquad \mu \in \mathbb{R} \,, \ \sigma_0 \in \sum_{j=1}^{m} \Sigma[\mathbf{x}, C_j] \,, \\ \qquad \sigma_j \in \Sigma[\mathbf{x}, F_j] \,, \ j = 1, \ldots, k' \,, \\ \qquad \deg(\sigma_j g_j) \leq 2d \,, \ j = 0, \ldots, k' \,, \end{cases}$$

where $\sigma_0 \in \sum_{j=1}^{m} \Sigma[\mathbf{x}, C_j]$ if and only if there exist $\sigma^1 \in \Sigma[\mathbf{x}, C_1], \ldots, \sigma^m \in \Sigma[\mathbf{x}, C_m]$ such that $\sigma_0(\mathbf{x}) = \sum_{j=1}^{m} \sigma^j(\mathbf{x})$, for all $\mathbf{x} \in \mathbb{R}^n$.

The number of SDP variables of the relaxation $(\mathbf{S}_d)$ is $\sum_{j=1}^{m} \binom{n_j+2d}{2d}$. At fixed d, it yields an SDP problem with $O(\kappa^{2d})$ variables, where $\kappa := \frac{1}{m} \sum_{j=1}^{m} n_j$ is the average size of the cliques $C_1, \ldots, C_m$. Moreover, the cliques $C_1, \ldots, C_m$ satisfy the running intersection property:

Definition 2.6 (*RIP*). Let $m \in \mathbb{N}_0$ and $I_1, \ldots, I_m$ be subsets of $\{1, \ldots, n\}$. We say that $I_1, \ldots, I_m$ satisfy the running intersection property (RIP) when for all $i = 1, \ldots, m$, there exists an integer $l < i$ such that $I_i \cap (\cup_{j<i} I_j) \subseteq I_l$.

This RIP property together with the assumption mentioned in Remark 2.5 allow us to state the sparse variant of Theorem 2.3:

THEOREM 2.7 (LASSERRE [LASSERRE 2006, THEOREM 3.6]). *Let $r_d^\star$ be the optimal value of the sparse SDP relaxation $(\mathbf{S}_d)$. Then the sequence $(r_d^\star)_{d\in\mathbb{N}}$ is nondecreasing and converges to $r^\star$.*

The interested reader can find more details in [Waki et al. 2006] about additional ways to exploit sparsity in order to derive analogous sparse SDP relaxations. We illustrate the benefits of the SDP relaxations $(\mathbf{S}_d)$ with the following example:

Example 2.8. Consider the polynomial f mentioned in Section 1: $f(\mathbf{x}) := x_2 x_5 + x_3 x_6 - x_2 x_3 - x_5 x_6 + x_1(-x_1 + x_2 + x_3 - x_4 + x_5 + x_6)$. Here, $n = 6, d = 2, N = \{1, \ldots, 6\}$. The 6×6 correlative sparsity matrix $\mathbf{R}$ is:

$$\mathbf{R} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

The csp graph G associated to $\mathbf{R}$ is depicted in Figure 1. The maximal cliques of G are $C_1 := \{1, 4\}$, $C_2 := \{1, 2, 3\}$, $C_3 := \{1, 2, 5\}$, $C_4 := \{1, 5, 6\}$ and $C_5 := \{1, 3, 6\}$. For $d = 2$, the dense SDP relaxation $(\mathbf{P}_2)$ involves $\binom{6+4}{4} = 210$ variables against $\binom{2+4}{4} + 4\binom{3+4}{4} = 155$ for the sparse variant $(\mathbf{S}_2)$. The dense SDP relaxation $(\mathbf{P}_3)$ involves 924 variables against 364 for the sparse variant $(\mathbf{S}_3)$. This difference becomes significant while considering that the time complexity of semidefinite programming is polynomial w.r.t. the number of variables with an exponent greater than 3 (see [Ben-Tal and Nemirovski 2001, Chapter 4] for more details).

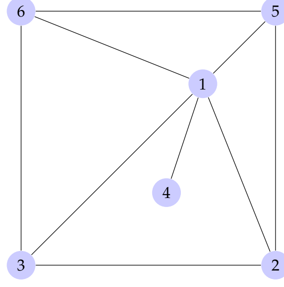


Fig. 1. Correlative sparsity pattern graph for the variables of f from Example 2.8.

2.3. Computer Proofs for Polynomial Optimization

Here, we briefly recall some existing features of the Coq proof assistant to handle formal polynomial optimization, when using SDP relaxations. The advantage of such relaxations is that they provide SOS certificates, which can be formally checked *a posteriori*. For more details on Coq, we recommend the documentation available in [Bertot and Castéran 2004]. Given a polynomial r and a set of constraints $\mathbf{K}$, one can obtain a lower bound on r by solving any instance of Problem $(\mathbf{P}_d)$. Then, one can verify formally the correctness of the lower bound $r_d^\star$, using the SOS certificate output $\sigma_0, \dots, \sigma_k$. Indeed it is enough to prove the polynomial equality $r(\mathbf{x}) - r_d^\star = \sum_{j=0}^k \sigma_j(\mathbf{x}) g_j(\mathbf{x})$ inside Coq. Such equalities can be efficiently proved using Coq's ring tactic [Grégoire and Mahboubi 2005] via the mechanism of computational reflection [Boutin 1997]. Any polynomial of type `pexprC` (see Section 2.1) can be normalized to a unique polynomial of type `polC` (see [Grégoire and Mahboubi 2005] for more details on the constructors of this type). For the sake of clarity, let us consider the unconstrained case, i.e. $\mathbf{K} = \mathbb{R}^n$. One encodes an SOS certificate $\sigma_0(\mathbf{x}) = \sum_{i=1}^m q_i^2$ with the sequence of polynomials $[q_1; \dots; q_m]$, each q_i being of type `polC` . To prove the equality $r = \sigma_0$, our version of the ring tactic normalizes both r and the sequence $[q_1; \dots; q_m]$ and compares the two normalization results. This mechanism is illustrated in Figure 2 with the polynomial $r(\mathbf{x}) := \frac{1}{4} + x_1^4 - 2x_1^2 x_2^2 + x_2^4$ (see Example 2.2) being encoded by `r` and the polynomials $1/2$ and $x_1^2 - x_2^2$ being encoded respectively by $\mathtt{q_1}$ and $\mathtt{q_2}$.

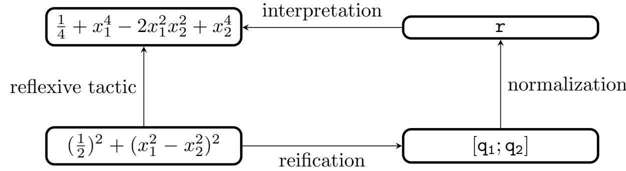


Fig. 2. An illustration of computational reflection.

In the general case, this computational step is done through a `checker_sos` procedure which returns a Boolean value. If this value is true, one applies a correctness lemma, whose conclusion yields the nonnegativity of $r - r_d^\star$ over $\mathbf{K}$. In practice, the SDP solvers are implemented in floating-point arithmetic, thus the above equality between $r - r_d^\star$ and the SOS certificate does not hold. However, following Remark 2.1, each variable lies in a closed interval, thus one can bound the remainder polynomial $\epsilon(\mathbf{x}) := r(\mathbf{x}) - r_d^\star - \sum_{j=0}^k \sigma_j(\mathbf{x}) g_j(\mathbf{x})$ using basic interval arithmetic, so that the lower bound $\epsilon^\star$ of ϵ yields the valid inequality: $\forall \mathbf{x} \in \mathbf{K}, r(\mathbf{x}) \geq r_d^\star + \epsilon^\star$. For more explanation, we refer the interested reader to the formal

Input: input variables $\mathbf{x}$, input constraints $\mathbf{X}$, nonlinear expression f, rounded expression $\hat{f}$, error variables $\mathbf{e}$, error constraints $\mathbf{E}$, relaxation order d
Output: interval enclosure I_d of the error $\hat{f} - f$ over $\mathbf{K} := \mathbf{X} \times \mathbf{E}$
1: Define the absolute error $r(\mathbf{x}, \mathbf{e}) := \hat{f}(\mathbf{x}, \mathbf{e}) - f(\mathbf{x})$
2: Compute $l(\mathbf{x}, \mathbf{e}) := r(\mathbf{x}, 0) + \sum_{j=1}^{m} \frac{\partial r(\mathbf{x},\mathbf{e})}{\partial e_j}(\mathbf{x}, 0)\, e_j$
3: Define $h := r - l$
4: Compute bounds for h: $I^h :=$ `ia_bound`$(h, \mathbf{K})$
5: Compute bounds for l: $I_d^l :=$ `sdp_bound`$(l, \mathbf{K}, d)$
6: **return** $I_d := I_d^l + I^h$

Fig. 3. `bound`: our algorithm to compute roundoff errors bounds of nonlinear programs.

framework [Magron et al. 2015b, Section 2.3]. Note that this formal verification remains valid when considering the sparse variant ($\mathbf{S}_d$).

3. GUARANTEED ROUNDOFF ERROR BOUNDS USING SDP RELAXATIONS

In this section, we present our new algorithm, relying on sparse SDP relaxations, to bound roundoff errors of nonlinear programs. After stating our general algorithm (Section 3.1), we detail how this procedure can handle polynomial programs (Section 3.2). Extensions to the non-polynomial case, including conditional statements, are presented in Section 3.3.

3.1. The General Optimization Framework

Here we consider a given program that implements a nonlinear transcendental expression f with input variables $\mathbf{x}$ satisfying a set of constraints $\mathbf{X}$. We assume that $\mathbf{X}$ is included in a box (i.e. a product of closed intervals) $[\mathbf{a}, \mathbf{b}] := [a_1, b_1] \times \cdots \times [a_n, b_n]$ and that $\mathbf{X}$ is encoded as follows:

$$\mathbf{X} := \{ \mathbf{x} \in \mathbb{R}^n \, : \, g_1(\mathbf{x}) \geq 0, \ldots, g_k(\mathbf{x}) \geq 0 \} \,,$$

for polynomial functions $g_1, \ldots, g_k$. Then, we denote by $\hat{f}(\mathbf{x}, \mathbf{e})$ the rounded expression of f after applying the `round` procedure (see Section 2.1), introducing additional error variables $\mathbf{e}$.

The algorithm `bound`, depicted in Figure 3, takes as input $\mathbf{x}$, $\mathbf{X}$, f, $\hat{f}$, $\mathbf{e}$ as well as the set $\mathbf{E}$ of bound constraints over $\mathbf{e}$. Here we assume that our program implementing f does not involve conditional statements (this case will be discussed later in Section 3.3). For a given machine ϵ, one has $\mathbf{E} := [-\epsilon, \epsilon]^m$, with m being the number of error variables. This algorithm actually relies on the sparse SDP optimization procedure ($\mathbf{S}_d$) (see Section 2.2 for more details), thus `bound` also takes as input a relaxation order $d \in \mathbb{N}$. The algorithm provides as output an interval enclosure I_d of the error $\hat{f}(\mathbf{x}, \mathbf{e}) - f(\mathbf{x})$ over $\mathbf{K}$. From this interval $I_d := [\underline{f_d}, \overline{f_d}]$, one can compute $f_d := \max\{-\underline{f_d}, \overline{f_d}\}$, which is a sound upper bound of the maximal absolute error $r^\star := \max_{(\mathbf{x},\mathbf{e}) \in \mathbf{K}} \mid \hat{f}(\mathbf{x}, \mathbf{e}) - f(\mathbf{x}) \mid$.

After defining the absolute roundoff error $r := \hat{f} - f$ (Line 1), one decomposes r as the sum of an expression l which is affine w.r.t. the error variable $\mathbf{e}$ and a remainder h. One way to obtain l is to compute the vector of partial derivatives of r w.r.t. $\mathbf{e}$ evaluated at $(\mathbf{x}, 0)$ and finally to take the inner product of this vector and $\mathbf{e}$ (Line 2). Then, the idea is to compute a precise bound of l and a coarse bound of h. The underlying reason is that h involves error term products of degree greater than 2 (e.g. $e_1 e_2$), yielding an interval enclosure I^h of *a priori* much smaller width, compared to the interval enclosure I^l of l. One obtains I^h using the procedure `ia_bound` implementing basic interval arithmetic (Line 4) to bound the remainder of the multivariate Taylor expansion of r w.r.t. $\mathbf{e}$, expressed as a combination of the second-error derivatives (similar as in [Solovyev et al. 2015]). The main algorithm

presented in Figure 3 is very similar to the algorithm of `FPTaylor` [Solovyev et al. 2015], except that SDP based techniques are used instead of the global optimization procedure from [Solovyev et al. 2015]. Note that overflow and denormal are neglected here but one could handle them, as in [Solovyev et al. 2015], by adding additional error variables and discarding the related terms using naive interval arithmetic.

3.2. Polynomial Programs

We first describe our `sdp_bound` optimization algorithm when implementing polynomial programs. In this case, `sdp_bound` calls an auxiliary procedure `sdp_poly`. The bound of l is provided through solving two sparse SDP instances of Problem ($\mathbf{S}_d$), at relaxation order d. We now give more explanation about the `sdp_poly` procedure.

We can map each input variable x_i to the integer i, for all $i = 1, \ldots, n$, as well as each error variable e_j to $n + j$, for all $j = 1, \ldots, m$. Then, define the sets $C_1 := \{1, \ldots, n, n + 1\}, \ldots, C_m := \{1, \ldots, n, n+m\}$. Here, we take advantage of the correlation sparsity pattern of l by using m distinct sets of cardinality $n+1$ rather than a single one of cardinality $n+m$, i.e. the total number of variables. After writing $l(\mathbf{x}, \mathbf{e}) = r(\mathbf{x}, 0) + \sum_{j=1}^{m} \frac{\partial r(\mathbf{x},\mathbf{e})}{\partial e_j}(\mathbf{x}, 0)\, e_j$ and noticing that $r(\mathbf{x}, 0) = \hat{f}(\mathbf{x}, 0) - f(\mathbf{x}) = 0$, one can scale the optimization problems by writing

$$l(\mathbf{x}, \mathbf{e}) = \sum_{j=1}^{m} s_j(\mathbf{x}) e_j = \epsilon \sum_{j=1}^{m} s_j(\mathbf{x}) \frac{e_j}{\epsilon} \,, \tag{11}$$

with $s_j(\mathbf{x}) := \frac{\partial r(\mathbf{x},\mathbf{e})}{\partial e_j}(\mathbf{x}, 0)$, for all $j = 1, \ldots, m$. Replacing $\mathbf{e}$ by $\mathbf{e}/\epsilon$ leads to computing an interval enclosure of l/ϵ over $\mathbf{K}' := \mathbf{X} \times [-1, 1]^m$. Recall that from Remark 2.1, there exists an integer $M > 0$ such that $M - \sum_{i=1}^{n} x_i^2 \geq 0$, as the input variables satisfy box constraints. Moreover, to fulfil the assumption of Remark 2.5, one encodes $\mathbf{K}'$ as follows:

$$\begin{aligned} \mathbf{K}' := \{\, (\mathbf{x}, \mathbf{e}) \in \mathbb{R}^{n+m} \ :\ & g_1(\mathbf{x}) \geq 0, \ldots, g_k(\mathbf{x}) \geq 0 \,, \\ & g_{k+1}(\mathbf{x}, e_1) \geq 0, \ldots, g_{k+m}(\mathbf{x}, e_m) \geq 0 \,\} \,, \end{aligned}$$

with $g_{k+j}(\mathbf{x}, e_j) := M + 1 - \sum_{i=1}^{n} x_i^2 - e_j^2$, for all $j = 1, \ldots, m$. The index set of variables involved in g_j is $F_j := N = \{1, \ldots, n\}$ for all $j = 1, \ldots, k$. The index set of variables involved in g_{k+j} is $F_{k+j} := C_j$ for all $j = 1, \ldots, m$.

Then, one can compute a lower bound of the minimum of $l'(\mathbf{x}, \mathbf{e}) := l(\mathbf{x}, \mathbf{e})/\epsilon = \sum_{j=1}^{m} s_j(\mathbf{x}) e_j$ over $\mathbf{K}'$ by solving the following optimization problem:

$$\begin{aligned} \underline{l'_d} := \sup_{\mu, \sigma_j} \ & \mu \,, \\ \text{s.t.} \ & l' - \mu = \sigma_0 + \textstyle\sum_{j=1}^{k+m} \sigma_j g_j \,, \\ & \mu \in \mathbb{R} \,,\ \sigma_0 \in \textstyle\sum_{j=1}^{m} \Sigma[(\mathbf{x}, \mathbf{e}), C_j] \,, \\ & \sigma_j \in \Sigma[(\mathbf{x}, \mathbf{e}), F_j] \,,\ j = 1, \ldots, k + m \,, \\ & \deg(\sigma_j g_j) \leq 2d \,,\ j = 1, \ldots, k + m \,. \end{aligned} \tag{12}$$

A feasible solution of Problem (12) ensures the existence of $\sigma^1 \in \Sigma[(\mathbf{x}, e_1)], \ldots, \sigma^m \in \Sigma[(\mathbf{x}, e_m)]$ such that $\sigma_0 = \sum_{j=0}^{m} \sigma^j$, allowing the following reformulation:

$$\begin{aligned} \underline{l'_d} := \sup_{\mu, \sigma_j} \ & \mu \,, \\ \text{s.t.} \ & l' - \mu = \textstyle\sum_{j=1}^{m} \sigma^j + \sum_{j=1}^{k+m} \sigma_j g_j \,, \\ & \mu \in \mathbb{R} \,,\ \sigma_j \in \Sigma[\mathbf{x}] \,,\ j = 1, \ldots, m \,, \\ & \sigma^j \in \Sigma[(\mathbf{x}, e_j)] \,, \deg(\sigma^j) \leq 2d \,,\ j = 1, \ldots, m \,, \\ & \deg(\sigma_j g_j) \leq 2d \,,\ j = 1, \ldots, k + m \,. \end{aligned} \tag{13}$$

An upper bound $\overline{l'_d}$ can be obtained by replacing sup with inf and $l' - \mu$ by $\mu - l'$ in Problem (13). Our optimization procedure `sdp_poly` computes the lower bound $\underline{l'_d}$ as well as an upper bound $\overline{l'_d}$ of l' over $\mathbf{K}'$ then returns the interval $I^l_d := [\epsilon \, \underline{l'_d}, \epsilon \, \overline{l'_d}]$, which is a sound enclosure of the values of l over $\mathbf{K}$.

We emphasize two advantages of the decomposition $r := l + h$ and more precisely of the linear dependency of l w.r.t. $\mathbf{e}$: scalability and robustness to SDP numerical issues. First, no computation is required to determine the correlation sparsity pattern of l, by comparison to the general case. Thus, it becomes much easier to handle the optimization of l with the sparse SDP Problem (13) rather than with the corresponding instance of the dense relaxation $(\mathbf{P}_d)$. While the latter involves $\binom{n+m+2d}{2d}$ SDP variables, the former involves only $m \binom{n+1+2d}{2d}$ variables, ensuring the scalability of our framework. In addition, the linear dependency of l w.r.t. $\mathbf{e}$ allows us to scale the error variables and optimize over a set of variables lying in $\mathbf{K}' := \mathbf{X} \times [-1, 1]^m$. It ensures that the range of input variables does not significantly differ from the range of error variables. This condition is mandatory while considering SDP relaxations because most SDP solvers (e.g. Mosek [Andersen and Andersen 2000]) are implemented using double precision floating-point. It is impossible to optimize l over $\mathbf{K}$ (rather than l' over $\mathbf{K}'$) when the maximal value ϵ of error variables is less than 2^{-53}, due to the fact that SDP solvers would treat each error variable term as 0, and consequently l as the zero polynomial. Thus, this decomposition insures our framework against numerical issues related to finite-precision implementation of SDP solvers.

Let us define the interval enclosure $I^l := [\underline{l}, \overline{l}]$, with $\underline{l} := \inf_{(\mathbf{x},\mathbf{e})\in\mathbf{K}} l(\mathbf{x}, \mathbf{e})$ and $\overline{l} := \sup_{(\mathbf{x},\mathbf{e})\in\mathbf{K}} l(\mathbf{x}, \mathbf{e})$. The next lemma states that one can approximate I^l as closely as desired using the `sdp_poly` procedure.

Lemma 3.1 (Convergence of the `sdp_poly` procedure). *Let I^l_d be the interval enclosure returned by the procedure* `sdp_poly`$(l, \mathbf{K}, d)$. *The sequence $(I^l_d)_{d\in\mathbb{N}}$ converges to I^l.*

Proof. It is sufficient to show the similar convergence result for $l' = l/\epsilon$, as it implies the convergence for l by a scaling argument. The sets $C_1, \dots, C_m$ satisfy the RIP property (see Definition 2.6). Moreover, the encoding of $\mathbf{K}'$ satisfies the assumption mentioned in Remark 2.5. Thus, Theorem 2.7 implies that the sequence of lower bounds $(\underline{l'_d})_{d\in\mathbb{N}}$ converges to $\underline{l'} := \inf_{(\mathbf{x},\mathbf{e})\in\mathbf{K}'} l'(\mathbf{x}, \mathbf{e})$. Similarly, the sequence of upper bounds converge to $\overline{l'}$, yielding the desired result. □

Lemma 3.1 guarantees asymptotic convergence to the exact enclosure of l when the relaxation order d tends to infinity. However, it is more reasonable in practice to keep this order as small as possible to obtain tractable SDP relaxations. Hence, we generically solve each instance of Problem (13) at the minimal relaxation order, that is $d_0 := \max\{\lceil \deg l/2 \rceil), \max_{1\leq j\leq k+m}\{\lceil \deg(g_j)/2 \rceil)\}\}$.

3.3. Non-polynomial and Conditional Programs

Other classes of programs do not only involve polynomials but also semialgebraic and transcendental functions as well as conditional statements. Such programs are of particular interest as they often occur in real-world applications such as biology modeling, space control or global optimization. We present how the general optimization procedure `sdp_bound` can be extended to these nonlinear programs.

3.3.1. Semialgebraic programs. Here we assume that the function l is semialgebraic, that is it involves non-polynomial components such as divisions or square roots. Following [Lasserre and Putinar 2010], we explain how to transform the optimization problem $\inf_{(\mathbf{x},\mathbf{e})\in\mathbf{K}} l(\mathbf{x}, \mathbf{e})$

Input: input variables $\mathbf{y}$, input constraints $\mathbf{K}$, semialgebraic expression f
Output: variables $\mathbf{y}_{\text{poly}}$, constraints $\mathbf{K}_{\text{poly}}$, polynomial expression f_{poly}

1: $I :=$ `ia_bound`$(f, \mathbf{K})$
2: **if** $f =$ `Pol` (p) **then** $\mathbf{y}_{\text{poly}} := \mathbf{y}$, $\mathbf{K}_{\text{poly}} := \mathbf{K}$, $f_{\text{poly}} := p$
3: **else if** $f =$ `Div` (g, h) **then**
4: $\quad \mathbf{y}_g, \mathbf{K}_g, g_{\text{poly}} :=$ `lift`$(\mathbf{y}, \mathbf{K}, g)$
5: $\quad \mathbf{y}_h, \mathbf{K}_h, h_{\text{poly}} :=$ `lift`$(\mathbf{y}, \mathbf{K}, h)$
6: $\quad \mathbf{y}_{\text{poly}} := (\mathbf{y}_g, \mathbf{y}_h, x) \qquad f_{\text{poly}} := x$
7: $\quad \mathbf{K}_{\text{poly}} := \{\mathbf{y}_{\text{poly}} \in \mathbf{K}_g \times \mathbf{K}_h \times I : x h_{\text{poly}} = g_{\text{poly}}\}$
8: **else if** $f =$ `Sqrt` (g) **then**
9: $\quad \mathbf{y}_g, \mathbf{K}_g, g_{\text{poly}} :=$ `lift`$(\mathbf{y}, \mathbf{K}, g)$
10: $\quad \mathbf{y}_{\text{poly}} := (\mathbf{y}_g, x) \qquad f_{\text{poly}} := x$
11: $\quad \mathbf{K}_{\text{poly}} := \{\mathbf{y}_{\text{poly}} \in \mathbf{K}_g \times I : x^2 = g_{\text{poly}}\}$
12: ...
13: **end**
14: **return** $\mathbf{y}_{\text{poly}}, \mathbf{K}_{\text{poly}}, f_{\text{poly}}$

Fig. 4. `lift`: a recursive procedure to reduce semialgebraic problems to polynomial problems.

into a polynomial optimization problem, then use the sparse SDP program (13). One way to perform this reformulation consists of introducing lifting variables to represent non-polynomial operations. We first illustrate the extension to semialgebraic programs with an example.

Example 3.2. Let us consider the program implementing the rational function $f : [0, 1] \to \mathbb{R}$ defined by $f(x_1) := \frac{x_1}{1+x_1}$. Applying the rounding procedure (with machine ϵ) yields $\hat{f}(x_1, \mathbf{e}) := \frac{x_1(1+e_2)}{(1+x_1)(1+e_1)}$ and the decomposition $r(x_1, \mathbf{e}) := \hat{f}(x_1, \mathbf{e}) - f(x_1) = l(x_1, \mathbf{e}) + h(x_1, \mathbf{e}) = s_1(x_1)e_1 + s_2(x_1)e_2 + h(x_1, \mathbf{e})$. One has $s_1(x_1) = \frac{\partial r(x_1, \mathbf{e})}{\partial e_1}(x_1, 0) = -\frac{x_1}{1+x_1}$ and $s_2(x_1) = -s_1(x_1)$.

Let $\mathbf{K} := [0, 1] \times [-\epsilon, \epsilon]^2$. One introduces a lifting variable $x_2 := \frac{x_1}{1+x_1}$ to handle the division operator and encode the equality constraint $p(\mathbf{x}) := x_2(1 + x_1) - x_1 = 0$ with the two inequality constraints $p(\mathbf{x}) \geq 0$ and $-p(\mathbf{x}) \geq 0$. To ensure the compactness assumption, one bounds x_2 within $I := [0, 1/2]$, using basic interval arithmetic.

Let $\mathbf{K}_{\text{poly}} := \{(\mathbf{x}, \mathbf{e}) \in [0, 1] \times I \times [\epsilon, \epsilon]^2 : p(\mathbf{x}) \geq 0\,, \ -p(\mathbf{x}) \geq 0\}$. Then the rational optimization problem involving l is equivalent to $\inf_{(\mathbf{x},\mathbf{e}) \in \mathbf{K}_{\text{poly}}} x_2(-e_1 + e_2)$, a polynomial optimization problem that we can handle with the `sdp_poly` procedure, described in Section 3.2.

In the semialgebraic case, `sdp_bound` calls an auxiliary procedure `sdp_sa`. Given input variables $\mathbf{y} := (\mathbf{x}, \mathbf{e})$, input constraints $\mathbf{K} := \mathbf{X} \times \mathbf{E}$ and a semialgebraic function l, `sdp_sa` first applies a recursive procedure `lift` which returns variables $\mathbf{y}_{\text{poly}}$, constraints $\mathbf{K}_{\text{poly}}$ and a polynomial f_{poly} such that the interval enclosure I^l of $l(\mathbf{y})$ over $\mathbf{K}$ is equal to the interval enclosure of the polynomial $l_{\text{poly}}(\mathbf{y}_{\text{poly}})$ over $\mathbf{K}_{\text{poly}}$. Calling `sdp_sa` yields the interval enclosure $I_d^l :=$ `sdp_poly`$(l_{\text{poly}}, \mathbf{K}_{\text{poly}}, d)$. We detail the lifting procedure `lift` in Figure 4 for the constructors `Pol`(Line 2), `Div` (Line 3) and `Sqrt` (Line 8). The interval I obtained through the `ia_bound` procedure (Line (1)) allows us to constrain the additional variable x to ensure the assumption of Remark 2.5. For the sake of consistency, we omit the other cases (`Neg`, `Add`, `Mul` and `Sub`) where the procedure is straightforward. For a similar procedure in the context of global optimization, we refer the interested reader to [Magron 2013, Chapter 2]. The set of variables $\mathbf{y}_{\text{poly}}$ can be decomposed as $(\mathbf{x}_{\text{poly}}, \mathbf{e})$, where $\mathbf{x}_{\text{poly}}$ gathers input variables with lifting variables and has a cardinality equal to n_{poly}. Then, one easily shows

that the sets $\{1,\dots,n_{\text{poly}},e_1\}$,...,$\{1,\dots,n_{\text{poly}},e_m\}$ satisfy the RIP, thus ensuring to solve efficiently the corresponding instances of Problem (13).

3.3.2. Transcendental programs. The above lifting procedure allows an exact representation of the graph of a semialgebraic function with polynomials involving additional (lifting) variables. We consider a procedure to approximate transcendental functions with semialgebraic functions. Here we assume that the function l is transcendental, i.e. involves univariate non-semialgebraic components such as exp or sin. We use the method presented in [Magron et al. 2015a], based on maxplus approximation of semiconvex transcendental functions by quadratic functions. This idea comes from optimal control [McEneaney 2006] and was developed further to represent the value function by a "maxplus linear combination", which is a supremum of quadratic polynomials at given points x_i. Given a set of points (x_i), we approximate from above and from below every transcendental function $f_{\mathbb{R}}$ by infima and suprema of finitely many quadratic polynomials $(f_{x_i}^-)$ and $(f_{x_i}^+)$. Hence, we reduce the problem to semialgebraic optimization problems. We can interpret this method in a geometrical way by thinking of it in terms of "quadratic cuts", since quadratic inequalities are added to approximate the graph of a transcendental function.

For each univariate transcendental function $f_{\mathbb{R}}$ in our dictionary set $\mathcal{D}$, one assumes that $f_{\mathbb{R}}$ is twice differentiable, so that the univariate function $g := f_{\mathbb{R}} + \frac{\gamma}{2}|\cdot|^2$ is convex on I for large enough $\gamma > 0$ (for more details, see the reference [McEneaney 2006]). It follows that there exists a constant $\gamma \leq \sup_{x\in I} -f''_{\mathbb{R}}(x)$ such that for all $x_i \in I$:

$$\begin{aligned} \forall x \in I, \quad f_{\mathbb{R}}(x) \geq f_{x_i}^-(x)\,, \\ \text{with } f_{x_i}^- := -\frac{\gamma}{2}(x-x_i)^2 + f'_{\mathbb{R}}(x_i)(x-x_i) + f_{\mathbb{R}}(x_i)\,, \end{aligned} \tag{14}$$

implying that for all $x \in I$, $f_{\mathbb{R}}(x) \geq \max_{x_i\in I} f_{x_i}^-(x)$. Similarly, one obtains an upper-approximation $\min_{x_i\in I} f_{x_i}^+(x)$. Figure 5 provides such approximations for the function $f_{\mathbb{R}}(x) := \log(1+\exp(x))$ on the interval $I := [-8, 8]$.

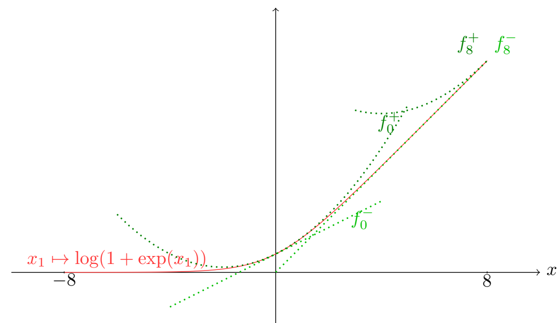


Fig. 5. Semialgebraic Approximations for $x \mapsto \log(1+\exp(x))$: $\max\{f_0^-(x), f_8^-(x)\} \leq \log(1+\exp(x)) \leq \min\{f_0^+(x), f_8^+(x)\}$.

For transcendental programs, our procedure `sdp_bound` calls the auxiliary procedure `sdp_transc`. Given input variables $(\mathbf{x},\mathbf{e})$, constraints $\mathbf{K}$ and a transcendental function l, `sdp_transc` first computes a semialgebraic lower (resp. upper) approximation l^- (resp. l^+) of l over $\mathbf{K}$. For more details in the context of global optimization, we refer the reader to [Magron et al. 2015a]. Then, calling the procedure `sdp_sa` allows us to get interval enclosures of l^- as well as l^+. We illustrate the procedure to handle transcendental programs with an example.

Input: input variables $\mathbf{x}$, input constraints $\mathbf{X}$, nonlinear expression f, rounded expression $\hat{f}$, error variables $\mathbf{e}$, error constraints $\mathbf{E}$, relaxation order d
Output: interval enclosure I_d of the error $\hat{f} - f$ over $\mathbf{K} := \mathbf{X} \times \mathbf{E}$

1: **if** $f =$ `IfThenElse` (p, g, h) **then**
2: $\quad I_d^p :=$ `bound`$(\mathbf{x}, \mathbf{X}, p, \hat{p}, \mathbf{e}, \mathbf{E}, d) = [\underline{p_d}, \overline{p_d}]$
3: $\quad \mathbf{X}_1 := \{\mathbf{x} \in \mathbf{X} : 0 \leq p(\mathbf{x}) \leq -\underline{p_d}\}$
4: $\quad \mathbf{X}_2 := \{\mathbf{x} \in \mathbf{X} : -\overline{p_d} \leq p(\mathbf{x}) \leq 0\}$
5: $\quad \mathbf{X}_3 := \{\mathbf{x} \in \mathbf{X} : 0 \leq p(\mathbf{x})\}$
6: $\quad \mathbf{X}_4 := \{\mathbf{x} \in \mathbf{X} : p(\mathbf{x}) \leq 0\}$
7: $\quad I_d^1 :=$ `bound_nlprog`$(\mathbf{x}, \mathbf{X}_1, g, \hat{h}, \mathbf{e}, \mathbf{E}, d)$
8: $\quad I_d^2 :=$ `bound_nlprog`$(\mathbf{x}, \mathbf{X}_2, h, \hat{g}, \mathbf{e}, \mathbf{E}, d)$
9: $\quad I_d^3 :=$ `bound_nlprog`$(\mathbf{x}, \mathbf{X}_3, g, \hat{g}, \mathbf{e}, \mathbf{E}, d)$
10: $\quad I_d^4 :=$ `bound_nlprog`$(\mathbf{x}, \mathbf{X}_4, h, \hat{h}, \mathbf{e}, \mathbf{E}, d)$
11: $\quad$ **return** $I_d := I_d^1 \cup I_d^2 \cup I_d^3 \cup I_d^4$
12: **else** **return** $I_d :=$ `bound`$(\mathbf{x}, \mathbf{X}, f, \hat{f}, \mathbf{e}, \mathbf{E}, d)$
13: **end**

Fig. 6. `bound_nlprog`: our algorithm to compute roundoff error bounds of programs with conditional statements.

Example 3.3. Let us consider the program implementing the transcendental function $f : [-8, 8] \to \mathbb{R}$ defined by $f(x_1) := \log(1 + \exp(x_1))$. Applying the rounding procedure yields $\hat{f}(x_1, \mathbf{e}) := \log[(1 + \exp(x_1)(1 + e_1))\,(1 + e_2)](1 + e_3)$. Here, $|e_2|$ is bounded by the machine ϵ while $|e_1|$ (resp. $|e_3|$) is bounded with an adjusted absolute error $\epsilon_1 := \epsilon(\exp)$ (resp. $\epsilon_3 := \epsilon(\log)$). Let $\mathbf{K} := [-8, 8] \times [-\epsilon_1, \epsilon_1] \times [-\epsilon, \epsilon] \times [-\epsilon_3, \epsilon_3]$.

One obtains the decomposition $r(x_1, \mathbf{e}) := \hat{f}(x_1, \mathbf{e}) - f(x_1) = l(x_1, \mathbf{e}) + h(x_1, \mathbf{e}) = s_1(x_1)e_1 + s_2(x_1)e_2 + s_3(x_1)e_3 + h(x_1, \mathbf{e})$, with $s_1(x_1) = \frac{\exp(x_1)}{1+\exp(x_1)}$, $s_2(x_1) = 1$ and $s_3(x_1) = \log(1 + \exp(x_1)) = f(x_1)$. Figure 5 provides a lower approximation $s_3^- := \max\{f_0^-, f_8^-\}$ of s_3 as well as an upper approximation $s_3^+ := \min\{f_0^+, f_8^+\}$. One can get similar approximations s_1^- and s_1^+ for s_1. One first obtains (coarse) interval enclosures $I_2 =$ `ia_bound`$(s_1, \mathbf{K})$ and $I_3 =$ `ia_bound`$(s_3, \mathbf{K})$ and one introduces extra variables $x_2 \in I_2$ and $x_3 \in I_3$ to represent s_1 and s_3 respectively. Then, the interval enclosure of l over $\mathbf{K}$ is equal to the interval enclosure of $l_{\text{sa}}(\mathbf{x}, \mathbf{e}) := x_2 e_1 + e_2 + x_3 e_3$ over the set $\mathbf{K}_{\text{sa}} := \{(x_1, \mathbf{e}) \in \mathbf{K}\,, (x_2, x_3) \in I_2 \times I_3\,, s_1^-(x_1) \leq x_2 \leq s_1^+(x_1)\,, s_3^-(x_1) \leq x_3 \leq s_3^+(x_1)\}$.

3.3.3. Programs with conditionals. Finally, we explain how to extend our bounding procedure to nonlinear programs involving conditionals through the recursive algorithm given in Figure 6. The overall procedure is very similar to the one implemented within the `Rosa` tool [Darulova and Kuncak 2014, Section 7, Figure 6]. The `bound_nlprog` algorithm relies on the `bound` procedure (see Figure 3 in Section 3.1) to compute roundoff error bounds of programs implementing transcendental functions (Line 12). From Line 1 to Line 11, the algorithm handles the case when the program implements a function f defined as follows:

$$f(\mathbf{x}) := \begin{cases} g(\mathbf{x}) & \text{if } p(\mathbf{x}) \geq 0, \\ h(\mathbf{x}) & \text{otherwise.} \end{cases}$$

The first branch output is g while the second one is h. More sophisticated conditionals, such as "$p_1(x) \geq 0$ or/and $p_2(x) \geq 0$", are not handled at the moment but one could easily extend the current framework to do so. A preliminary step consists of computing the roundoff error enclosure $I_d^p := [\underline{p_d}, \overline{p_d}]$ (Line 2) for the program implementing the polynomial p. Then the

procedure computes bounds related to the discontinuity error of the branch, that is the maximal value between the four following errors:

— (Line 7) the error obtained while computing the rounded result $\hat{h}$ of the second branch instead of computing the exact result g of the first one, occurring for the set of variables $(\mathbf{x}, \mathbf{e})$ such that $\hat{p}(\mathbf{x}, \mathbf{e}) \leq 0 \leq p(\mathbf{x})$. For scalability and numerical issues, we consider an over-approximation $\mathbf{X}_1$ (Line 3) of this set, where the variables $\mathbf{x}$ satisfy the relaxed constraints $0 \leq p(\mathbf{x}) \leq -\underline{p_d}$. Note that in this case, one has $l(\mathbf{x}, \mathbf{e}) = r(\mathbf{x}, 0) + \sum_{j=1}^{m} \frac{\partial r(\mathbf{x},\mathbf{e})}{\partial e_j}(\mathbf{x}, 0)\, e_j$, with $r(\mathbf{x}, 0) = h(\mathbf{x}) - g(\mathbf{x}) \neq 0$. In general, we expect the magnitude of the partial derivative sum to be very small compared to the one of $r(\mathbf{x}, 0)$.

— (Line 8) the error obtained while computing the rounded result $\hat{g}$ of the first branch instead of computing the exact result h of the second one, occurring for the set of variables $(\mathbf{x}, \mathbf{e})$ such that $p(\mathbf{x}) \leq 0 \leq \hat{p}(\mathbf{x}, \mathbf{e})$. We also consider an over-approximation $\mathbf{X}_2$ (Line 4), where the variables $\mathbf{x}$ satisfy the relaxed constraints $-\overline{p_d} \leq p(\mathbf{x}) \leq 0$.

— (Line 9) the roundoff error corresponding to the program implementation of g.

— (Line 10) the roundoff error corresponding to the program implementation of h.

3.3.4. Simplification of error terms. In addition, our algorithm `bound_nlprog` integrates several features to reduce the number of error variables. First, it memorizes all sub-expressions of the nonlinear expression tree to perform common sub-expressions elimination. We can also simplify error term products, thanks to the following lemma.

LEMMA 3.4 (HIGHAM [HIGHAM 2002, LEMMA 3.3]). *Let ϵ be the machine precision and assume that for a given integer k, one has $\epsilon < \frac{1}{k}$ and $\gamma_k := \frac{k\epsilon}{1-k\epsilon}$. Then, for all $e_1, \ldots, e_k \in [-\epsilon, \epsilon]$, there exists θ_k such that $\prod_{i=1}^{k}(1 + e_i) = 1 + \theta_k$ and $\mid \theta_k \mid \leq \gamma_k$.*

Lemma 3.4 implies that for any k such that $\epsilon < \frac{1}{k}$, one has $\theta_k \leq (k+1)\epsilon$. Our algorithm has an option to automatically derive safe over-approximations of the absolute roundoff error while introducing only one variable e_1 (bounded by $(k+1)\epsilon$) instead of k error variables $e_1, \ldots, e_k$ (bounded by ϵ). The cost of solving the corresponding optimization problem can be significantly reduced but it yields coarser error bounds.

4. EXPERIMENTAL EVALUATION

Now, we present experimental results obtained by applying our general `bound_nlprog` algorithm (see Section 3, Figure 6) to various examples coming from physics, biology, space control and optimization. The `bound_nlprog` algorithm is implemented in an open-source tool called `Real2Float`, built in top of the `NLCertify` nonlinear verification package, relying on OCAML (Version 4.02.1), COQ (Version 8.4pl5) and interfaced with the SDP solver SDPA (Version 7.3.9). The SDP solver output numerical SOS certificates, which are converted into rational SOS using the ZARITH OCAML library (Version 1.2), implementing arithmetic operations over arbitrary-precision integers. For more details about the installation and usage of `Real2Float`, we refer to the dedicated web-page[3] and the setup instructions.[4] All examples are displayed in Appendix A as the corresponding `Real2Float` input text files and satisfy our nonlinear program semantics (see Section 2.1). All results have been obtained on an Intel Core i7-5600U CPU (2.60 GHz). Execution timings have been computed by averaging over five runs.

[3]http://nl-certify.forge.ocamlcore.org/real2float.html

[4]see the `README.md` file in the top level directory

4.1. Benchmark Presentation

For each example, we compared the quality of the roundoff error bounds (Table II) and corresponding execution times (Table III) while running our tool `Real2Float`, `FPTaylor` (version from May 2016 [Solovyev et al. 2015]), `Rosa` (version from May 2014 used in [Darulova and Kuncak 2014]), GAPPA (version 1.2.0 [Daumas and Melquiond 2010]) and FLUCTUAT (version 3.1370 [Delmas et al. 2009]).

To ensure fair comparison, our initial choice was to focus on tools providing certificates and using the same rounding model (`FPTaylor` or `Rosa` which relies on an SMT solver theoretically able to output satisfiability certificates). However, for the sake of completeness, we have also compared `Real2Float` with GAPPA [Daumas and Melquiond 2010] and FLUCTUAT [Delmas et al. 2009]. For all tools, we use default parameters, we use the default number of subdivisions in FLUCTUAT and for GAPPA, we provide the simplest user-provided hints we could think of.

A head-to-head comparison is not straightforward here due to differences in the approaches: GAPPA uses an improved rounding model based on a piecewise constant absolute error bound (see Section 1.2 for more details), and FLUCTUAT does not produce output certificates. We also performed further experiments while turning on the improved rounding model of `FPTaylor` (which is the same as in GAPPA and FLUCTUAT).

A given program implements a nonlinear function $f(\mathbf{x})$, involving variables $\mathbf{x}$ lying in a set $\mathbf{X}$ contained in a box $[\mathbf{a}, \mathbf{b}]$. Applying our rounding model on f yields the nonlinear expression $\hat{f}(\mathbf{x}, \mathbf{e})$, involving additional error variables $\mathbf{e}$ lying in a set $\mathbf{E}$.

At a given semidefinite relaxation order d, our tool computes the upper bound f_d of the absolute roundoff error $\mid f - \hat{f} \mid$ over $\mathbf{K} := \mathbf{X} \times \mathbf{E}$ and verifies that it is less than a requested number $\epsilon^{+}_{\texttt{Real2Float}}$. As we keep the relaxation order d as low as possible to ensure tractable SDP programs, it can happen that $f_d > \epsilon^{+}_{\texttt{Real2Float}}$. The `Real2Float` tool has the default option to perform box subdivisions when the number of initial variables and maximal polynomial degree are both small. When the option is disabled, the solver does not perform subdivisions and outputs the error bound f_d. When enabled, we subdivide a randomly chosen interval of the box $[\mathbf{a}, \mathbf{b}]$ in two halves to obtain two sub-sets $\mathbf{X}_1$ and $\mathbf{X}_2$, fulfilling $\mathbf{X} := \mathbf{X}_1 \cup \mathbf{X}_2$, and apply the `bound_nlprog` algorithm on both sub-sets either until we succeed to certify that $\epsilon^{+}_{\texttt{Real2Float}}$ is a sound upper bound of the roundoff error or until the maximal number of branch and bound iterations is reached. For each benchmark, an error bound $\epsilon_{\texttt{Real2Float}}$ is automatically computed while setting $\epsilon^{+}_{\texttt{Real2Float}} = 0$.

The number $\epsilon_{\texttt{Real2Float}}$ is compared with the upper bounds computed by two other tools implementing simple rounding models: `FPTaylor`, which relies on Taylor Symbolic expansions [Solovyev et al. 2015], and `Rosa`, which relies on SMT and affine arithmetic [Darulova and Kuncak 2014].

For comparison purpose, we also executed each program using random inputs, following the approach used in the `Rosa` paper [Darulova and Kuncak 2014]. Specifically, we executed each program on 10^7 random inputs satisfying the input restrictions. The results from these random samples provide lower bounds on the absolute error. For consistency of comparison, the error bounds computed with `FPTaylor` correspond to the procedure FPT. (a) (see [Solovyev et al. 2015]) using the same simplified rounding model as the one described in Equation 3, also used in `Rosa` [Darulova and Kuncak 2014]. For the sake of further presentation, we identify with a letter (from `a` to `z` and from `α` to `γ`) each of the 30 nonlinear programs. The programs `a-b` and `f-s` are taken from the `Rosa` paper [Darulova and Kuncak 2014] and were used in the `FPTaylor` paper [Solovyev et al. 2015] as well:

— The first 9 programs implement polynomial functions: `a-b` come from physics, `c-e` are derived from expressions involved in the proof of Kepler Conjecture [Hales 2006] and `f-h` implement polynomial approximations of the sine and square root functions. The

Table II. Comparison results of upper and lower bounds for absolute roundoff errors among tools implementing either simple or advanced rounding model. For each model, results of the winning tool are emphasized using **bold fonts**.

		Simple rounding			Improved rounding			
Benchmark	id	Real2Float	Rosa	FPTaylor	FPTaylor	Gappa	Fluctuat	lower bound
Programs involving polynomial functions								
rigidBody1	a	5.33e–13	5.08e–13	**3.87e–13**	**2.95e–13**	**2.95e–13**	3.22e–13	2.28e–13
rigidBody2	b	6.48e–11	6.48e–11	**5.24e–11**	**3.61e–11**	**3.61e–11**	3.65e–11	2.19e–11
kepler0	c	1.18e–13	1.16e–13	**1.05e–13**	**7.47e–14**	1.12e–13	1.26e–13	2.23e–14
kepler1	d	**4.47e–13**	6.49e–13	4.49e–13	**2.87e–13**	4.89e–13	5.57e–13	7.58e–14
kepler2	e	**2.09e–12**	2.89e–12	2.10e–12	**1.58e–12**	2.45e–12	2.90e–12	3.03e–13
sineTaylor	f	**6.03e–16**	9.56e–16	6.75e–16	**4.44e–16**	8.33e–02	6.86e–16	2.85e–16
sineOrder3	g	1.19e–15	1.11e–15	**9.97e–16**	7.95e–16	**7.62e–16**	1.03e–15	3.34e–16
sqroot	h	1.29e–15	8.41e–16	**7.13e–16**	**5.02e–16**	5.37e–16	3.21e–13	4.45e–16
himmilbeau	i	1.43e–12	1.43e–12	**1.32e–12**	**1.01e–12**	**1.01e–12**	**1.01e–12**	1.47e–13
Programs involving semialgebraic functions								
doppler1	j	7.65e–12	4.92e–13	**1.59e–13**	**1.29e–13**	1.82e–13	1.34e–13	7.11e–14
doppler2	k	1.57e–11	1.29e–12	**2.90e–13**	**2.39e–13**	3.23e–13	2.53e–13	1.14e–13
doppler3	l	8.55e–12	2.03e–13	**8.22e–14**	**6.96e–14**	9.29e–14	7.36e–14	4.27e–14
verhulst	m	4.67e–16	6.82e–16	**3.53e–16**	**2.50e–16**	3.18e–16	4.84e–16	2.23e–16
carbonGas	n	2.21e–08	4.64e–08	**1.23e–08**	**7.77e–09**	8.85e–09	1.86e–08	4.11e–09
predPrey	o	2.52e–16	2.94e–16	**1.89e–16**	**1.60e–16**	1.95e–16	2.45e–16	1.47e–16
turbine1	p	2.45e–11	1.25e–13	**2.33e–14**	**1.67e–14**	3.88e–14	6.09e–14	1.07e–14
turbine2	q	2.08e–12	1.76e–13	**3.14e–14**	**2.01e–14**	3.97e–14	8.96e–14	1.43e–14
turbine3	r	1.71e–11	8.50e–14	**1.70e–14**	**9.58e–15**	9.96e+00	4.90e–14	5.33e–15
jetEngine	s	OoM	1.62e–08	**1.50e–11**	**1.03e–11**	1.32e+05	1.82e–11	5.46e–12
Programs implementing polynomial functions with polynomial preconditions								
floudas2_6	t	**5.15e–13**	5.87e–13	7.88e–13	**5.94e–13**	5.98e–13	7.45e–13	4.56e–14
floudas3_3	u	5.81e–13	**4.05e–13**	5.76e–13	4.29e–13	**2.65e–13**	4.32e–13	1.48e–13
floudas3_4	v	2.78e–15	2.56e–15	**2.23e–15**	1.78e–15	**1.23e–15**	2.23e–15	3.80e–16
floudas4_6	w	1.82e–15	1.33e–15	**1.23e–15**	**8.89e–16**	**8.89e–16**	1.12e–15	2.35e–16
floudas4_7	x	**1.06e–14**	1.31e–14	1.80e–14	1.32e–14	**7.44e–15**	1.71e–14	7.31e–15
Programs involving conditional statements								
cav10	y	**2.91e+00**	**2.91e+00**	–	–	–	**1.02e+02**	2.90e+00
perin	z	**2.01e+00**	**2.01e+00**	–	–	–	**4.91e+01**	2.00e+00
Programs implementing transcendental functions								
logexp	α	2.52e–15	–	**2.07e–15**	**1.99e–15**	–	–	1.19e–15
sphere	β	1.53e–14	–	**1.29e–14**	**8.21e–15**	–	–	5.05e–15
hartman3	γ	2.99e–13	–	**1.34e–14**	**4.97e–15**	–	–	1.10e–15
hartman6	δ	5.09e–13	–	**2.55e–14**	**8.19e–15**	–	–	2.20e–15

program `i` is issued from the global optimization literature and implements the problem *Himmilbeau* in [Ali et al. 2005].

— The 10 programs `j-s` implement semialgebraic functions: `j-l` and `p-s` come from physics, `m` and `o` from biology, `n` from control. All these programs are used to compare `FPTaylor` and `Rosa` in [Solovyev et al. 2015].

— The five programs `t-x` come from the global optimization literature and correspond respectively to Problem 2.6, 3.3, 3.4, 4.6 and 4.7 in [Floudas and Pardalos 1990]. We selected them as they typically involve nontrivial polynomial preconditions (i.e. $\mathbf{X}$ is not a simple box but rather a set defined with conjunction of nonlinear polynomial inequalities).

— The two programs `y-z` involve conditional statements and come from the static analysis literature. They correspond to the two respective running examples of [Ghorbal et al. 2010] (Fluctuat's divergence error computation) and [Alexandre Maréchal 2014]. The first program `y` is used in the `Rosa` paper [Darulova and Kuncak 2014] for the analysis of branches discontinuity error.

— The last four programs α-γ involve transcendental functions. The two programs α and β are used in the `FPTaylor` paper [Solovyev et al. 2015] and correspond respectively to the program `logexp` (see Example 3.3) and the program `sphere` taken from NASA World

Wind Java SDK [Nasa 2011]. The 2 programs γ and δ respectively implement the functions coming from the optimization problems *Hartman 3* and *Hartman 6* in [Ali et al. 2005], involving both sums of exponential functions composed with quadratic polynomials.

Tool comparison settings. The five tools `Real2Float`, `Rosa`, `FPTaylor`, GAPPA and FLUCTUAT can handle programs with input variable uncertainties as well as any floating-point precision, but for the sake of conciseness, we only considered to compare their performance on programs implemented in double precision floating-point ($\epsilon = 2^{-53}$). By contrast with preliminary experiments presented in Section 1.1 where we considered floating-point input variables, we run each tool by considering all input variables as real variables, thus we apply the rounding operation to all of them. For the programs involving transcendental functions, we followed the same procedure as in `FPTaylor` while adjusting the precision $\epsilon(f_{\mathbb{R}}) = 1.5\epsilon$ for each special function $f_{\mathbb{R}} \in \{\sin, \cos, \log, \exp\}$. Each univariate transcendental function is approximated from below (resp. from above) using suprema (resp. infima) of linear or quadratic polynomials (see Example 3.3 for the case of program `logexp`).

4.2. Comparison Results

Comparison results for error bound computation are presented in Table II. Among the tools using the simple rounding model (`Real2Float`, `Rosa` and `FPTaylor`), our `Real2Float` tool computes the tightest upper bounds for 7 (resp. 4) out of 30 benchmarks when comparing with `Rosa` and `FPTaylor` (resp. all tools). For all programs `j-s` involving semialgebraic functions and the four programs $\boldsymbol{\alpha}$-$\boldsymbol{\delta}$ involving transcendental functions, `FPTaylor` computes the tightest bounds, when comparing with `Real2Float` and `Rosa`.[5] One current limitation of `Real2Float` is its limited ability to manipulate symbolic expressions, e.g. computing rational function derivatives or yielding reduction to the same denominator. In particular, the analysis of program `s` aborted after running out of memory (meaning of the symbol OoM). The `FPTaylor` tool is better suited to handle programs that exhibit such rational functions and also includes an interface with the MAXIMA computer algebra system [Maxima 2013] to perform symbolic simplifications.

We mention that the interested reader can find more detailed experimental comparisons between the three tools implementing improved rounding models (`FPTaylor`, FLUCTUAT and GAPPA) in [Solovyev et al. 2015, Section 5.2]. Note that `FPTaylor` provides the tightest bounds for 24 out of 30 benchmarks. The GAPPA software provides the tightest bounds for 8 out of 30 benchmarks while being almost always faster than other tools. As emphasized in [Solovyev et al. 2015], GAPPA can sometimes compute more precise bounds with more advanced user-provided hints. Note that FLUCTUAT provides tighter bounds than GAPPA for most rational functions while being always slower. It would be worth implementing the same improved rounding model in `Real2Float` to perform numerical comparisons.

To the best of our knowledge, `Real2Float` is the only academic tool which is able to handle the general class of programs involving either transcendental functions or conditional statements. The `FPTaylor` (resp. `Rosa`) tool does not currently handle conditionals (resp. transcendental functions), as meant by the symbol $-$ in the corresponding column entries. However, an interface bridging the `FPTaylor` and `Rosa` tools would provide each other with the relevant missing features. These error bound comparison results together with their corresponding execution timings (given in Table III) are used to plot the data points shown in Figure 7. For each benchmark identified by `id`, let $t_{\texttt{Real2Float}}$ (in 3rd column of Table III) refer to the execution time of `Real2Float` to obtain the corresponding upper bound $\epsilon_{\texttt{Real2Float}}$ (in 3rd column of Table II).

[5]The running execution times of `Rosa` may change with more recent versions

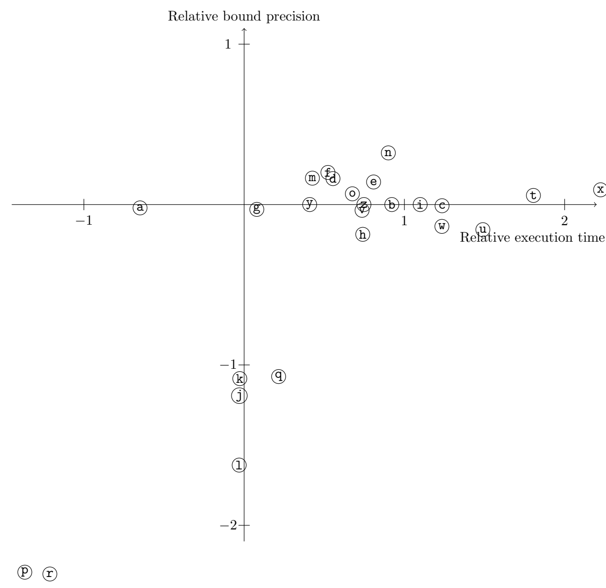
Table III. Comparison of execution times (in seconds) for absolute roundoff error bounds among tools implementing either simple or advanced rounding model. For each model, the winner results are emphasized using **bold fonts**.

		Simple rounding			Improved rounding		
Benchmark	id	Real2Float	Rosa	FPTaylor	FPTaylor	GAPPA	FLUCTUAT
rigidBody1	a	0.58	**0.13**	1.84	0.41	**0.10**	0.29
rigidBody2	b	**0.26**	2.17	3.01	0.46	**0.15**	0.52
kepler0	c	**0.22**	3.78	4.93	6.96	**0.44**	0.70
kepler1	d	17.6	63.1	**9.33**	4.90	0.72	**0.37**
kepler2	e	**16.5**	106	19.1	13.8	**1.58**	2.04
sineTaylor	f	**1.05**	3.50	2.91	**0.11**	0.16	0.55
sineOrder3	g	**0.40**	0.48	1.90	0.40	**0.06**	0.22
sqroot	h	**0.14**	0.77	2.70	0.44	**0.19**	0.40
himmilbeau	i	**0.20**	2.51	3.28	0.49	**0.09**	1.00
doppler1	j	6.80	6.35	**6.13**	1.34	**0.08**	0.77
doppler2	k	6.96	**6.54**	6.88	1.57	**0.08**	0.79
doppler3	l	6.84	**6.37**	9.13	1.50	**0.07**	0.78
verhulst	m	**0.51**	1.36	1.37	0.40	**0.05**	0.25
carbonGas	n	**0.83**	6.59	3.73	0.52	**0.15**	2.03
predPrey	o	**0.87**	4.12	1.78	0.48	**0.04**	5.14
turbine1	p	72.2	**3.09**	4.38	0.53	**0.21**	5.79
turbine2	q	4.72	7.75	**3.25**	0.60	**0.12**	4.76
turbine3	r	74.5	4.57	**3.46**	0.61	**0.20**	5.84
jetEngine	s	OoM	125	**9.79**	3.06	**0.31**	31.2
floudas2_6	t	**2.49**	159	15.9	14.3	**2.35**	26.8
floudas3_3	u	**0.45**	13.9	5.64	13.9	**0.76**	6.41
floudas3_4	v	**0.09**	0.49	1.47	1.27	**0.07**	1.01
floudas4_6	w	**0.07**	1.20	0.91	0.37	**0.05**	1.69
floudas4_7	x	**0.13**	21.8	1.64	0.39	**0.07**	0.53
cav10	y	**0.23**	0.59	−	−	−	1.26
perin	z	**0.49**	2.74	−	−	−	1.19
logexp	α	**1.05**	−	1.10	**0.39**	−	−
sphere	β	**0.05**	−	2.04	**3.69**	−	−
hartman3	γ	**2.02**	−	32.5	**27.8**	−	−
hartman6	δ	**119**	−	364	**259**	−	−

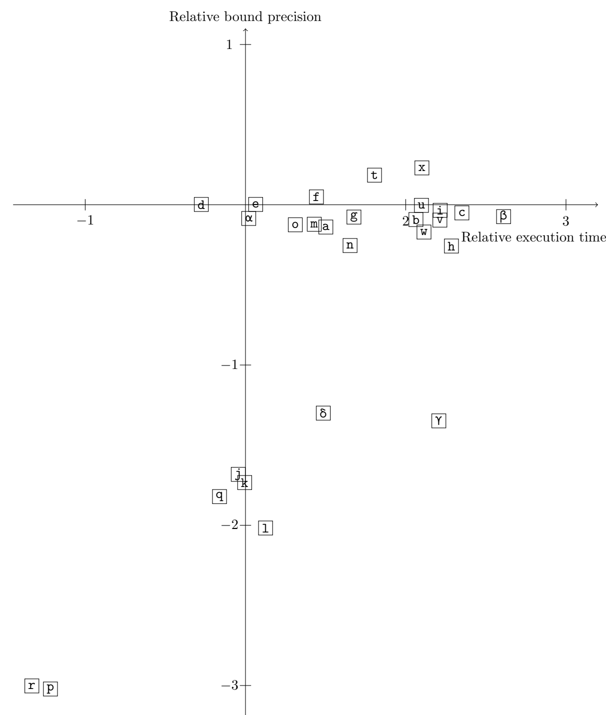
Now, let us define the execution times $t_{\texttt{Rosa}}$, $t_{\texttt{FPTaylor}}$ and the corresponding error bounds $\epsilon_{\texttt{Rosa}}$, $\epsilon_{\texttt{FPTaylor}}$. Then the x-axis coordinate of the point (id) (resp. [id]) displayed in Figure 7(a) (resp. 7(b)) corresponds to the logarithm of the ratio between the execution time of Rosa (resp. FPTaylor) and Real2Float, i.e. $\log \frac{t_{\texttt{Rosa}}}{t_{\texttt{Real2Float}}}$ (resp. $\log \frac{t_{\texttt{FPTaylor}}}{t_{\texttt{Real2Float}}}$). Similarly, the y-axis coordinate of the point (id) (resp. [id]) is $\log \frac{\epsilon_{\texttt{Rosa}}}{\epsilon_{\texttt{Real2Float}}}$ (resp. $\log \frac{\epsilon_{\texttt{FPTaylor}}}{\epsilon_{\texttt{Real2Float}}}$).

The axes of the coordinate system within Figure 7 divide the plane into four quadrants: the nonnegative quadrant $(+,+)$ contains data points referring to programs for which Real2Float computes the tighter bounds in less time, the second one $(+,-)$ contains points referring to programs for which Real2Float is faster but less accurate, the non-positive quadrant $(-,-)$ for which Real2Float is slower and computes coarser bounds and the last one $(-,+)$ for which Real2Float is slower but more accurate.

On the quadrant $(+,-)$ of Figure 7(b), one can see that Real2Float computes bounds which are less accurate than FPTaylor on semialgebraic and transcendental programs, but does so more quickly for most of them. The quadrant $(-,-)$ indicates that Rosa and FPTaylor are more precise and efficient than Real2Float on the three programs p-r. The presence of 18 plots on the nonnegative quadrant $(+,+)$ of Figure 7(a) and Figure 7(b) confirms that Real2Float does not compromise efficiency at the expense of accuracy, in particular for programs implementing polynomials with nontrivial polynomial preconditions.



(a) Comparison with `Rosa`.



(b) Comparison with `FPTaylor`.

Fig. 7. Comparisons of execution times and upper bounds of roundoff errors obtained with `Rosa` and `FPTaylor`, relatively to `Real2Float`.

For each program implementing polynomials, our tool has an option to provide formal guarantees for the corresponding roundoff error bound $\epsilon_{\texttt{Real2Float}}$. Using the formal mechanism described in Section 2.3, `Real2Float` formally checks inside Coq the SOS certificates generated by the SDP solver for interval enclosures of linear error terms l. The `FPTaylor` (resp. Gappa) software has a similar option to provide formal scripts which can be checked inside the Hol-light (resp. Coq) proof assistant, for programs involving polynomial and transcendental functions. For formal verification, our tool is limited compared with `FPTaylor` and Gappa as it cannot handle non-polynomial programs.

Table IV. Comparisons of informal and formal execution times to certify roundoff error bounds obtained with `Real2Float`, `FPTaylor` and Gappa.

		Informal execution time			Formal execution time		
Benchmark	id	`Real2Float`	`FPTaylor`	Gappa	`Real2Float`	`FPTaylor`	Gappa
`rigidBody1`	`a`	0.58	1.84	0.10	0.36	10.2	2.58
`rigidBody2`	`b`	0.26	3.01	0.15	4.81	32.3	4.90
`kepler0`	`c`	0.22	4.93	0.44	0.29	45.5	13.0
`kepler1`	`d`	17.6	9.33	0.72	449	90.5	28.9
`kepler2`	`e`	16.5	19.1	1.58	297	274	59.3
`sineTaylor`	`f`	1.05	2.91	0.16	7.54	42.1	13.6
`sineOrder3`	`g`	0.40	1.90	0.06	0.34	10.4	6.74
`sqroot`	`h`	0.14	2.70	0.19	0.80	16.8	12.9
`himmilbeau`	`i`	0.20	3.28	0.09	0.89	32.2	3.73

Next, we describe the formal proof results obtained while verifying the bounds for the nine polynomial programs `a-i`. Table IV allows us to compare the execution times of `Real2Float`, `FPTaylor` and Gappa required to analyze the nine programs in both informal (i.e. without verification inside Coq or Hol-light) and formal settings. Comparing `Real2Float` with `FPTaylor`, the latter performs better than the former to analyze formally the two programs `d-e` but yields coarser bounds. Our formal procedure is less computationally efficient when the degree (resp. number of variables) of the SOS polynomials grows, as for these two programs. The informal speedup ratio is greater than 3 for the five programs `a`, `c` and `g-i`. The table shows that the speedup ratio in the formal setting is higher than in the informal setting for these five programs. The explanation could be that Coq is inherently faster than Hol-light at checking computations while delegating expensive ones to a virtual machine (being part of Coq's trusted base). Either SOS or Taylor methods could work with the two proof assistants Hol-light and Coq (with natural changes in execution time) and it would be meaningful to compare similar methods in a given proof assistant (SOS techniques in Hol-light or Taylor methods in Coq) but both are not yet fully available. The Gappa tool performs better when analyzing the two programs `d-e`, but is less accurate. This is in contrast with all other programs where the formal verification with `Real2Float` is faster than with Gappa while providing coarser bounds (except program `f` where Gappa yields pessimistic results) Our formal verification framework is a work in progress as it only allows to check correctness of SOS certificates for polynomial programs. The step from formal verification of the step translating the inequality to a statement of explicit syntactic form "$\forall \mathbf{x}, |\texttt{rounded}(f(\mathbf{x})) - f(\mathbf{x})| \leq e$" is missing and requires more software engineering. Thus, the timings presented in Table IV for `Real2Float` do not include formal computation of the symbolic second-order derivatives of r w.r.t. $\mathbf{e}$ as well as the cost of bounding them using formal interval arithmetic.

At the moment (and in contrast to our method) the `Rosa` tool does not formally verify the output bound provided by the SMT solver, but such a feature could be embedded through an interface with the `smtcoq` framework [Armand et al. 2011]. This latter tool allows the proof witness generated by an SMT solver to be formally (and independently) re-checked

inside COQ. The `smtcoq` framework uses tactics based on *computational reflection* to enable this re-checking to be performed efficiently.

5. CONCLUSION AND PERSPECTIVES

Our verification framework allows us to over-approximate roundoff errors occurring while executing nonlinear programs implemented with finite precision. The framework relies on semidefinite optimization, ensuring certified approximations. Our approach extends to medium-size nonlinear problems, due to automatic detection of the correlation sparsity pattern of input variables and roundoff error variables. Experimental results indicate that the optimization algorithm implemented in our `Real2Float` software package can often produce bounds of quality similar to the ones provided by the competitive solvers `Rosa` and `FPTaylor`, while saving a significant amount of CPU time. In addition, `Real2Float` produces sums of squares certificates which guarantee the correctness of these upper bounds and can can be efficiently verified inside the COQ proof assistant.

This work yields several directions for further research investigation. First, we intend to increase the size of graspable instances by exploiting the SDP relaxations specifically tuned to the case when a program implements the sum of many rational functions [Bugarin et al. 2015]. Symmetry patterns of certain program sub-classes could be tackled with the SDP hierarchies from [Riener et al. 2013]. We could also provide roundoff error bounds for more general programs, involving either finite or infinite conditional loops and additional comparisons with the results described in [Darulova and Kuncak 2016]. A preliminary mandatory step is to be able to generate inductive invariants with SDP relaxations. Another interesting direction would be to apply the method used in [Lasserre 2011] to derive sequences of lower roundoff error bounds together with SDP-based certificates. On the formal proof side, we could benefit from floating-point/interval arithmetic libraries available inside COQ, first to improve the efficiency of the formal polynomial checker, currently relying on exact arithmetic, then to extend the formal verification to non-polynomial programs. The method implemented in `FPTaylor` happens to be efficient and precise to analyze various programs and it would be interesting to design a procedure combining `FPTaylor` with our tool on specific subsets of input constraints. Long-term research perspectives include theoretical study of why/when SOS performs better as well as satisfactory complexity results about SOS certificates (w.r.t. size of polynomials). Finally, we plan to combine this optimization framework with the procedure in [Gao and Constantinides 2015] to improve the automatic reordering of arithmetic expressions, allowing more efficient optimization of FPGA implementations.

NONLINEAR PROGRAM BENCHMARKS

`let box_rigidbody1` $x_1\, x_2\, x_3 = [(-15, 15); (-15, 15); (-15, 15)];;$
`let obj_rigidbody1` $x_1\, x_2\, x_3 = [(-x_1 * x_2 - 2 * x_2 * x_3 - x_1 - x_3,\ 0)];;$

`let box_rigidbody2` $x_1\, x_2\, x_3 = [(-15, 15); (-15, 15); (-15, 15)];;$
`let obj_rigidbody2` $x_1\, x_2\, x_3 =$
$[(2 * x_1 * x_2 * x_3 + 3 * x_3 * x_3 - x_2 * x_1 * x_2 * x_3 + 3 * x_3 * x_3 - x_2, 0)];;$

`let box_kepler0` $x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = [(4, 6.36); (4, 6.36); (4, 6.36); (4, 6.36); (4, 6.36); (4, 6.36)];;$
`let obj_kepler0` $x_1\, x_2\, x_3\, x_4\, x_5\, x_6 =$
$[(x_2 * x_5 + x_3 * x_6 - x_2 * x_3 - x_5 * x_6 + x_1 * (-x_1 + x_2 + x_3 - x_4 + x_5 + x_6),\ 0)];;$

`let box_kepler1` $x_1\, x_2\, x_3\, x_4 = [(4, 6.36); (4, 6.36); (4, 6.36); (4, 6.36)];;$
`let obj_kepler1` $x_1\, x_2\, x_3\, x_4 = [(x_1 * x_4 * (-x_1 + x_2 + x_3 - x_4)$
$+x_2 * (x_1 - x_2 + x_3 + x_4) + x_3 * (x_1 + x_2 - x_3 + x_4)$
$-x_2 * x_3 * x_4 - x_1 * x_3 - x_1 * x_2 - x_4,\ 0)];;$

`let box_kepler2` $x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = [(4, 6.36); (4, 6.36); (4, 6.36); (4, 6.36); (4, 6.36); (4, 6.36)];;$
`let obj_kepler2` $x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = [(x_1 * x_4 * (-x_1 + x_2 + x_3$
$-x_4 + x_5 + x_6) + x_2 * x_5 * (x_1 - x_2 + x_3 + x_4 - x_5 + x_6)$

$+x_3 * x_6 * (x_1 + x_2 - x_3 + x_4 + x_5 - x_6) - x_2 * x_3 * x_4$
$-x_1 * x_3 * x_5 - x_1 * x_2 * x_6 - x_4 * x_5 * x_6,\ 0)];;$

`let box_sineTaylor` $x = [(-1.57079632679, 1.57079632679)];;$
`let obj_sineTaylor` $x = [(x - (x * x * x)/6.0$
$+(x * x * x * x * x)/120.0$
$-(x * x * x * x * x * x * x)/5040.0,\ 0)];;$

`let box_sineOrder3` $z = [(-2, 2)];;$
`let obj_sineOrder3` $z = [(0.954929658551372 * z - 0.12900613773279798 * (z * z * z),\ 0)];;$

`let box_sqroot` $y = [(0, 1)];;$
`let obj_sqroot` $y = [(1.0 + 0.5 * y - 0.125 * y * y + 0.0625 * y * y * y - 0.0390625 * y * y * y * y,\ 0)];;$

`let box_himmilbeau` $x_1\, x_2 = [(-5, 5); (-5, 5)];;$
`let obj_himmilbeau` $x_1\, x_2 = [($
$(x_1 * x_1 + x_2 - 11) * (x_1 * x_1 + x_2 - 11) + (x_1 + x_2 * x_2 - 7) * (x_1 + x_2 * x_2 - 7),\ 0)];;$

`let box_doppler1` $u\ v\ T = [(-100, 100); (20, 20e3); (-30, 50)];;$
`let obj_doppler1` $u\ v\ T = [($`let` $t_1 = 331.4 + 0.6 * T$ `in` $-t_1 * v/((t_1 + u) * (t_1 + u)),\ 0)];;$

`let box_doppler2` $u\ v\ T = [(-125, 125); (15, 25e3); (-40, 60)];;$
`let obj_doppler2` $u\ v\ T = [($`let` $t_1 = 331.4 + 0.6 * T$ `in` $-t_1 * v/((t_1 + u) * (t_1 + u)),\ 0)];;$

`let box_doppler3` $u\ v\ T = [(-30, 120); (320, 20300); (-50, 30)];;$
`let obj_doppler3` $u\ v\ T = [($`let` $t_1 = 331.4 + 0.6 * T$ `in` $-t_1 * v/((t_1 + u) * (t_1 + u)),\ 0)];;$

`let box_verhulst` $x = [(0.1, 0.3)];;$
`let obj_verhulst` $x = [(4 * x/(1 + (x/1.11)),\ 0)];;$

`let box_carbonGas` $v = [(0.1, 0.5)];;$
`let obj_carbonGas` $v = [($`let` $p = 3.5e7$ `in let` $a = 0.401$ `in`
`let` $b = 42.7\text{e-}6$ `in let` $t = 300$ `in let` $n = 1000$ `in`
$(p + a * (n/v) * *2) * (v - n * b) - 1.3806503\text{e-}23 * n * t,\ 0)];;$

`let box_predPrey` $x = [(0.1, 0.3)];;$
`let obj_predPrey` $x = [(4 * x * x/(1 + (x/1.11) * *2),\ 0)];;$

`let box_turbine1` $v\ w\ r = [(-4.5, -0.3); (0.4, 0.9); (3.8, 7.8)];;$
`let obj_turbine1` $v\ w\ r = [(3 + 2/(r * r) - 0.125 * (3 - 2 * v) * (w * w * r * r)/(1 - v) - 4.5, 0)];;$

`let box_turbine2` $v\ w\ r = [(-4.5, -0.3); (0.4, 0.9); (3.8, 7.8)];;$
`let obj_turbine2` $v\ w\ r = [(6 * v - 0.5 * v * (w * w * r * r)/(1 - v) - 2.5, 0)];;$

`let box_turbine3` $v\ w\ r = [(-4.5, -0.3); (0.4, 0.9); (3.8, 7.8)];;$
`let obj_turbine3` $v\ w\ r = [(3 - 2/(r * r) - 0.125 * (1 + 2 * v) * (w * w * r * r)/(1 - v) - 0.5, 0)];;$

`let box_jet` $x_1\, x_2 = [(-5, 5); (-20, 5)];;$
`let obj_jet` $x_1\, x_2 = [($
$x_1 + ((2 * x_1 * ((3 * x_1 * x_1 + 2 * x_2 - x_1)/(x_1 * x_1 + 1))$
$*((3 * x_1 * x_1 + 2 * x_2 - x_1)/(x_1 * x_1 + 1) - 3)$
$+x_1 * x_1 * (4 * ((3 * x_1 * x_1 + 2 * x_2 - x_1)/(x_1 * x_1 + 1)) - 6))$
$*(x_1 * x_1 + 1) + 3 * x_1 * x_1 * ((3 * x_1 * x_1 + 2 * x_2 - x_1)/(x_1 * x_1 + 1))$
$+x_1 * x_1 * x_1 + x_1 + 3 * ((3 * x_1 * x_1 + 2 * x_2 - x_1)/(x_1 * x_1 + 1))), 0)];;$

`let box_floudas2_6` $x_1\, x_2\, x_3\, x_4\, x_5\, x_6\, x_7\, x_8\, x_9\, x_{10} =$
$[(0, 1); (0, 1); (0, 1); (0, 1); (0, 1); (0, 1); (0, 1); (0, 1); (0, 1); (0, 1)];;$
`let cstr_floudas2_6` $x_1\, x_2\, x_3\, x_4\, x_5\, x_6\, x_7\, x_8\, x_9\, x_{10} = [$
$-4 + 2 * x_1 + 6 * x_2 + 1 * x_3 + 0 * x_4 + 3 * x_5 + 3 * x_6 + 2 * x_7 + 6 * x_8 + 2 * x9 + 2 * x_{10};$
$22 - (6 * x_1 - 5 * x_2 + 8 * x_3 - 3 * x_4 + 0 * x_5 + 1 * x_6 + 3 * x_7 + 8 * x_8 + 9 * x9 - 3 * x_{10});$
$-6 - (5 * x_1 + 6 * x_2 + 5 * x_3 + 3 * x_4 + 8 * x_5 - 8 * x_6 + 9 * x_7 + 2 * x_8 + 0 * x9 - 9 * x_{10});$
$-23 - (9 * x_1 + 5 * x_2 + 0 * x_3 - 9 * x_4 + 1 * x_5 - 8 * x_6 + 3 * x_7 - 9 * x_8 - 9 * x9 - 3 * x_{10});$
$-12 - (-8 * x_1 + 7 * x_2 - 4 * x_3 - 5 * x_4 - 9 * x_5 + 1 * x_6 - 7 * x_7 - 1 * x_8 + 3 * x9 - 2 * x_{10})];;$
`let obj_floudas2_6` $x_1\, x_2\, x_3\, x_4\, x_5\, x_6\, x_7\, x_8\, x_9\, x_{10} = [($
$48 * x_1 + 42 * x_2 + 48 * x_3 + 45 * x_4 + 44 * x_5 + 41 * x_6 + 47 * x_7$
$+42 * x_8 + 45 * x9 + 46 * x_{10}$
$-50 * (x_1 * x_1 + x_2 * x_2 + x_3 * x_3 + x_4 * x_4 + x_5 * x_5$
$+x_6 * x_6 + x_7 * x_7 + x_8 * x_8 + x9 * x9 + x_{10} * x_{10}), 0)];;$

`let box_floudas3_3` $x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = [(0, 6); (0, 6); (1, 5); (0, 6); (1, 5); (0, 10)];;$
$-(x_2 - 2) * *2 - (x_3 - 1) * *2 - (x_4 - 4) * *2 - (x_5 - 1) * *2 - (x_6 - 4) * *2,\ 0)];;$

```
let cstr_floudas3_3 x1 x2 x3 x4 x5 x6 =
[(x3 − 3) ∗ ∗2 + x4 − 4; (x5 − 3) ∗ ∗2 + x6 − 4;
2 − x1 + 3 ∗ x2; 2 + x1 − x2; 6 − x1 − x2; x1 + x2 − 2];;
let obj_floudas3_3 x1 x2 x3 x4 x5 x6 = [(−25 ∗ (x1 − 2) ∗ ∗2
−(x2 − 2) ∗ ∗2 − (x3 − 1) ∗ ∗2 − (x4 − 4) ∗ ∗2
−(x5 − 1) ∗ ∗2 − (x6 − 4) ∗ ∗2, 0)];;

let box_floudas3_4 x1 x2 x3 = [(0, 2); (0, 2); (0, 3)];;
let cstr_floudas3_4 x1 x2 x3 = [
4 − x1 − x2 − x3; 6 − 3 ∗ x2 − x3;
−0.75 + 2 ∗ x1 − 2 ∗ x3 + 4 ∗ x1 ∗ x1 − 4 ∗ x1 ∗ x2
+4 ∗ x1 ∗ x3 + 2 ∗ x2 ∗ x2 − 2 ∗ x2 ∗ x3 + 2 ∗ x3 ∗ x3];;
let obj_floudas3_4 x1 x2 x3 = [(−2 ∗ x1 + x2 − x3, 0)];;

let box_floudas4_6 x1 x2 = [(0, 3); (0, 4)];;
let cstr_floudas4_6 x1 x2 = [
2 ∗ x1 ∗ ∗4 − 8 ∗ x1 ∗ ∗3 + 8 ∗ x1 ∗ x1 − x2;
4 ∗ x1 ∗ ∗4 − 32 ∗ x1 ∗ ∗3 + 88 ∗ x1 ∗ x1 − 96 ∗ x1 + 36 − x2];;
let obj_floudas4_6 x1 x2 = [(−x1 − x2, 0)];;

let box_floudas4_7 x1 x2 = [(0, 2); (0, 3)];;
let cstr_floudas4_7 x1 x2 = [−2 ∗ x1 ∗ ∗4 + 2 − x2];;
let obj_floudas4_7 x1 x2 = [(−12 ∗ x1 − 7 ∗ x2 + x2 ∗ x2, 0)];;

let box_cav10 x = [(0, 10)];;
let obj_cav10 x = [( if (x ∗ x − x > 0) then x ∗ 0.1 else x ∗ x + 2, 0)];;

let box_perin x y = [(1, 7); (−2, 7)];;
let cstr_perin x y = [x − 1; y + 2; x − y; 5 − y − x];;
let obj_perin x y = [( if (x ∗ x + y ∗ y ≤ 4) then y ∗ x else 0, 0)];;

let box_logexp x = [(−8, 8)];;
let obj_logexp x = [(log(1 + exp(x)), 0)];;

let box_sphere x r y z = [(−10, 10); (0, 10); (−1.570796, 1.570796); (−3.14159265, 3.14159265)];;
let obj_sphere x r y z = [(x + r ∗ sin(y) ∗ cos(z), 0)];;

let box_hartman3 x1 x2 x3 = [(0, 1); (0, 1); (0, 1)];;
let obj_hartman3 x1 x2 x3 = [(
let e1 = 3.0 ∗ (x1 − 0.3689) ∗ ∗2 + 10.0 ∗ (x2 − 0.117) ∗ ∗2 + 30.0 ∗ (x3 − 0.2673) ∗ ∗2 in
let e2 = 0.1 ∗ (x1 − 0.4699) ∗ ∗2 + 10.0 ∗ (x2 − 0.4387) ∗ ∗2 + 35.0 ∗ (x3 − 0.747) ∗ ∗2 in
let e3 = 3.0 ∗ (x1 − 0.1091) ∗ ∗2 + 10.0 ∗ (x2 − 0.8732) ∗ ∗2 + 30.0 ∗ (x3 − 0.5547) ∗ ∗2 in
let e4 = 0.1 ∗ (x1 − 0.03815) ∗ ∗2 + 10.0 ∗ (x2 − 0.5743) ∗ ∗2 + 35.0 ∗ (x3 − 0.8828) ∗ ∗2 in
−(1.0 ∗ exp(−e1) + 1.2 ∗ exp(−e2) + 3.0 ∗ exp(−e3) + 3.2 ∗ exp(−e4)), 0)];;

let box_hartman6 x1 x2 x3 x4 x5 x6 = [(0, 1); (0, 1); (0, 1); (0, 1); (0, 1); (0, 1)];;
let obj_hartman6 x1 x2 x3 x4 x5 x6 = [(
let e1 = 10.0 ∗ (x1 − 0.1312) ∗ ∗2 + 3.0 ∗ (x2 − 0.1696) ∗ ∗2 + 17. ∗ (x3 − 0.5569) ∗ ∗2 + 3.5 ∗ (x4 − 0.0124) ∗ ∗2
+1.7 ∗ (x5 − 0.8283) ∗ ∗2 + 8.0 ∗ (x6 − 0.5886) ∗ ∗2 in
let e2 = 0.05 ∗ (x1 − 0.2329) ∗ ∗2 + 10 ∗ (x2 − 0.4135) ∗ ∗2 + 17.0 ∗ (x3 − 0.8307) ∗ ∗2 + 0.1 ∗ (x4 − 0.3736) ∗ ∗2
+8.0 ∗ (x5 − 0.1004) ∗ ∗2 + 14.0 ∗ (x6 − 0.9991) ∗ ∗2 in
let e3 = 3.0 ∗ (x1 − 0.2348) ∗ ∗2 + 3.5 ∗ (x2 − 0.1451) ∗ ∗2 + 1.7 ∗ (x3 − 0.3522) ∗ ∗2 + 10.0 ∗ (x4 − 0.2883) ∗ ∗2
+17.0 ∗ (x5 − 0.3047) ∗ ∗2 + 8.0 ∗ (x6 − 0.665) ∗ ∗2 in
let e4 = 17.0 ∗ (x1 − 0.4047) ∗ ∗2 + 8 ∗ (x2 − 0.8828) ∗ ∗2 + 0.05 ∗ (x3 − 0.8732) ∗ ∗2 + 10.0 ∗ (x4 − 0.5743) ∗ ∗2
+0.1 ∗ (x5 − 0.1091) ∗ ∗2 + 14.0 ∗ (x6 − 0.0381) ∗ ∗2 in
−(1.0 ∗ exp(−e1) + 1.2 ∗ exp(−e2) + 3.0 ∗ exp(−e3) + 3.2 ∗ exp(−e4)), 0)];;
```

Acknowledgment

The authors would like to specially acknowledge the precious help of Alexey Solovyev, his excellent feedback and suggestions. They also thank the three referees for helpful comments to improve this paper.

REFERENCES

Michaël Périn Alexandre Maréchal. 2014. *Three linearization techniques for multivariate polynomials in static analysis using convex polyhedra.* Technical Report TR-2014-7. Verimag Research Report.

M. Montaz Ali, Charoenchai Khompatraporn, and Zelda B. Zabinsky. 2005. A Numerical Evaluation of Several Stochastic Algorithms on Selected Continuous Global Optimization Test Problems. *J. of Global Optimization* 31, 4 (April 2005), 635–672. DOI:http://dx.doi.org/10.1007/s10898-004-9972-2

ErlingD. Andersen and KnudD. Andersen. 2000. The Mosek Interior Point Optimizer for Linear Programming: An Implementation of the Homogeneous Algorithm. In *High Performance Optimization*, Hans Frenk, Kees Roos, Tamás Terlaky, and Shuzhong Zhang (Eds.). Applied Optimization, Vol. 33. Springer US, 197–232. DOI:http://dx.doi.org/10.1007/978-1-4757-3216-0_8

Michael Armand, Germain Faure, Benjamin Grégoire, Chantal Keller, Laurent Théry, and Benjamin Werner. 2011. A Modular Integration of SAT/SMT Solvers to Coq through Proof Witnesses. In *Certified Programs and Proofs*, Jean-Pierre Jouannaud and Zhong Shao (Eds.). Lecture Notes in Computer Science, Vol. 7086. Springer Berlin Heidelberg, 135–150. DOI:http://dx.doi.org/10.1007/978-3-642-25379-9_12

Aharon Ben-Tal and Arkadi Semenovich Nemirovski. 2001. *Lectures on modern convex optimization: analysis, algorithms, and engineering applications*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA.

Y. Bertot and P. Castéran. 2004. *Interactive Theorem Proving and Program Development: Coq'Art: The Calculus of Inductive Constructions*. Springer.

Martin Berz and Kyoko Makino. 2009. Rigorous global search using Taylor models. In *Proceedings of the 2009 conference on Symbolic numeric computation (SNC '09)*. ACM, New York, NY, USA, 11–20.

Jesse Bingham and Joe Leslie-Hurd. 2014. Verifying Relative Error Bounds Using Symbolic Simulation. In *Computer Aided Verification*, Armin Biere and Roderick Bloem (Eds.). Lecture Notes in Computer Science, Vol. 8559. Springer International Publishing, 277–292. DOI:http://dx.doi.org/10.1007/978-3-319-08867-9_18

B. Blanchet, P. Cousot, R. Cousot, J. Feret, L. Mauborgne, A. Miné, D. Monniaux, and X. Rival. 2003. A Static Analyzer for Large Safety-Critical Software. In *Proceedings of the ACM SIGPLAN 2003 Conference on Programming Language Design and Implementation (PLDI'03)*. ACM Press, San Diego, California, USA, 196–207.

David Boland and George A. Constantinides. 2010. Automated Precision Analysis: A Polynomial Algebraic Approach. In *FCCM'10*. 157–164.

S. Boldo and G. Melquiond. 2011. Flocq: A Unified Library for Proving Floating-Point Algorithms in Coq. In *Computer Arithmetic (ARITH), 2011 20th IEEE Symposium on*. 243–252. DOI:http://dx.doi.org/10.1109/ARITH.2011.40

Mateus Borges, Marcelo d'Amorim, Saswat Anand, David Bushnell, and Corina S. Pasareanu. 2012. Symbolic Execution with Interval Solving and Meta-heuristic Search. In *Proceedings of the 2012 IEEE Fifth International Conference on Software Testing, Verification and Validation (ICST '12)*. IEEE Computer Society, Washington, DC, USA, 111–120.

Samuel Boutin. 1997. Using Reflection to Build Efficient and Certified Decision Procedures. In *TACS'97. Springer-Verlag LNCS 1281*. Springer-Verlag, 515–529.

Florian Bugarin, Didier Henrion, and JeanBernard Lasserre. 2015. Minimizing the sum of many rational functions. *Mathematical Programming Computation* (2015), 1–29. http://dx.doi.org/10.1007/s12532-015-0089-z

Liqian Chen, Antoine Miné, and Patrick Cousot. 2008. A Sound Floating-Point Polyhedra Abstract Domain. In *Programming Languages and Systems*, G. Ramalingam (Ed.). Lecture Notes in Computer Science, Vol. 5356. Springer Berlin Heidelberg, 3–18. DOI:http://dx.doi.org/10.1007/978-3-540-89330-1_2

Liqian Chen, Antoine Miné, Ji Wang, and Patrick Cousot. 2009. Interval Polyhedra: An Abstract Domain to Infer Interval Linear Relationships. In *Static Analysis*, Jens Palsberg and Zhendong Su (Eds.). Lecture Notes in Computer Science, Vol. 5673. Springer Berlin Heidelberg, 309–325. DOI:http://dx.doi.org/10.1007/978-3-642-03237-0_21

Wei-Fan Chiang, Ganesh Gopalakrishnan, Zvonimir Rakamaric, and Alexey Solovyev. 2014. Efficient Search for Inputs Causing High Floating-point Errors. In *Proceedings of the 19th ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming (PPoPP '14)*. ACM, New York, NY, USA, 43–52.

Coq 2016. The Coq Proof Assistant. (2016). http://coq.inria.fr/.

P. Cousot and R. Cousot. 1977. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Conference Record of the Fourth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. ACM Press, New York, NY, Los Angeles, California, 238–252.

Eva Darulova and Viktor Kuncak. 2014. Sound Compilation of Reals. In *Proceedings of the 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL '14)*. ACM, New York, NY, USA, 235–248.

Eva Darulova and Viktor Kuncak. 2016. *Towards a Compiler for Reals*. Technical Report. Ecole Polytechnique Federale de Lausanne.

Marc Daumas and Guillaume Melquiond. 2010. Certification of Bounds on Expressions Involving Rounded Operators. *ACM Trans. Math. Softw.* 37, 1, Article 2 (Jan. 2010), 20 pages.

Leonardo De Moura and Nikolaj Bjørner. 2008. Z3: An Efficient SMT Solver. In *Proceedings of the Theory and Practice of Software, 14th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'08/ETAPS'08)*. Springer-Verlag, Berlin, Heidelberg, 337–340. http://dl.acm.org/citation.cfm?id=1792734.1792766

David Delmas, Eric Goubault, Sylvie Putot, Jean Souyris, Karim Tekkal, and Franck Védrine. 2009. Towards an Industrial Use of FLUCTUAT on Safety-Critical Avionics Software. In *Formal Methods for Industrial Critical Systems*, María Alpuente, Byron Cook, and Christophe Joubert (Eds.). Lecture Notes in Computer Science, Vol. 5825. Springer Berlin Heidelberg, 53–69. DOI:http://dx.doi.org/10.1007/978-3-642-04570-7_6

Christodoulos A. Floudas and Panos M. Pardalos. 1990. *A Collection of Test Problems for Constrained Global Optimization Algorithms*. Springer-Verlag New York, Inc., New York, NY, USA.

Sicun Gao, Soonho Kong, and EdmundM. Clarke. 2013. dReal: An SMT Solver for Nonlinear Theories over the Reals. In *Automated Deduction – CADE-24*, MariaPaola Bonacina (Ed.). Lecture Notes in Computer Science, Vol. 7898. Springer Berlin Heidelberg, 208–214. DOI:http://dx.doi.org/10.1007/978-3-642-38574-2_14

Xitong Gao and George A. Constantinides. 2015. Numerical Program Optimization for High-Level Synthesis. In *Proceedings of the 2015 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (FPGA '15)*. ACM, New York, NY, USA, 210–213.

Khalil Ghorbal, Eric Goubault, and Sylvie Putot. 2010. A Logical Product Approach to Zonotope Intersection. In *Computer Aided Verification*, Tayssir Touili, Byron Cook, and Paul Jackson (Eds.). Lecture Notes in Computer Science, Vol. 6174. Springer Berlin Heidelberg, 212–226. DOI:http://dx.doi.org/10.1007/978-3-642-14295-6_22

Benjamin Grégoire and Assia Mahboubi. 2005. Proving Equalities in a Commutative Ring Done Right in Coq. In *TPHOLs (Lecture Notes in Computer Science)*, Joe Hurd and Thomas F. Melham (Eds.), Vol. 3603. Springer, 98–113.

Thomas C. Hales. 2006. Introduction to the Flyspeck Project. In *Mathematics, Algorithms, Proofs (Dagstuhl Seminar Proceedings)*, Thierry Coquand, Henri Lombardi, and Marie-Françoise Roy (Eds.). Dagstuhl, Germany.

Leopold Haller, Alberto Griggio, Martin Brain, and Daniel Kroening. 2012. Deciding Floating-Point Logic with Systematic Abstraction. In *Formal Methods in Computer-Aided Design (FMCAD)*. 131–140.

David Handelman. 1988. Representing polynomials by positive linear functions on compact convex polyhedra. *Pacific J. Math.* 132, 1 (1988), 35–62. http://projecteuclid.org/euclid.pjm/1102689794

John Harrison. 1996. HOL Light: A Tutorial Introduction. In *FMCAD (Lecture Notes in Computer Science)*, Mandayam K. Srivas and Albert John Camilleri (Eds.), Vol. 1166. Springer, 265–269.

John Harrison. 2000. Formal Verification of Floating Point Trigonometric Functions. In *Formal Methods in Computer-Aided Design*, Jr. Hunt, WarrenA. and StevenD. Johnson (Eds.). Lecture Notes in Computer Science, Vol. 1954. Springer Berlin Heidelberg, 254–270. DOI:http://dx.doi.org/10.1007/3-540-40922-X_14

N.J. Higham. 2002. *Accuracy and Stability of Numerical Algorithms: Second Edition*. Society for Industrial and Applied Mathematics. http://books.google.fr/books?id=epilvM5MMxwC

2008. IEEE Standard for Floating-Point Arithmetic. *IEEE Std 754-2008* (Aug 2008), 1–70. DOI:http://dx.doi.org/10.1109/IEEESTD.2008.4610935

Bertrand Jeannet and Antoine Miné. 2009. Apron: A Library of Numerical Abstract Domains for Static Analysis. In *Computer Aided Verification*, Ahmed Bouajjani and Oded Maler (Eds.). Lecture Notes in Computer Science, Vol. 5643. Springer Berlin Heidelberg, 661–667.

Jean-Louis Krivine. 1964. Quelques propriétés des préordres dans les anneaux commutatifs unitaires. *Comptes Rendus de l'Académie des Sciences* 258 (1964), 3417–3418.

J.B. Lasserre. 2009. *Moments, Positive Polynomials and Their Applications*. Imperial College Press. http://books.google.nl/books?id=VY6imTsdIrEC

Jean B. Lasserre. 2001. Global Optimization with Polynomials and the Problem of Moments. *SIAM Journal on Optimization* 11, 3 (2001), 796–817.

Jean B. Lasserre. 2006. Convergent SDP-Relaxations in Polynomial Optimization with Sparsity. *SIAM Journal on Optimization* 17, 3 (2006), 822–843.

Jean B. Lasserre. 2011. A New Look at Nonnegativity on Closed Sets and Polynomial Optimization. 21, 3 (2011), 864–885. DOI:http://dx.doi.org/10.1137/100806990

Jean B. Lasserre and Mihai Putinar. 2010. Positivity and Optimization for Semi-Algebraic Functions. *SIAM Journal on Optimization* 20, 6 (2010), 3364–3383.

Monique Laurent. 2009. Sums of squares, moment matrices and optimization over polynomials. In *Emerging applications of algebraic geometry*. Springer, 157–270.

Michael D. Linderman, Matthew Ho, David L. Dill, Teresa H. Meng, and Garry P. Nolan. 2010. Towards Program Optimization Through Automated Analysis of Numerical Precision. In *Proceedings of the 8th Annual IEEE/ACM International Symposium on Code Generation and Optimization (CGO 10)*. ACM, New York, NY, USA, 230–237.

Victor Magron. 2013. *Formal Proofs for Global Optimization – Templates and Sums of Squares*. Ph.D. Dissertation. Ècole Polytechnique.

Victor Magron. 2014. NLCertify: A Tool for Formal Nonlinear Optimization. In *Mathematical Software – ICMS 2014*, Hoon Hong and Chee Yap (Eds.). Lecture Notes in Computer Science, Vol. 8592. Springer Berlin Heidelberg, 315–320.

Victor Magron, Xavier Allamigeon, Stéphane Gaubert, and Benjamin Werner. 2015a. Certification of real inequalities: templates and sums of squares. *Mathematical Programming* 151, 2 (2015), 477–506. DOI:http://dx.doi.org/10.1007/s10107-014-0834-5

Victor Magron, Xavier Allamigeon, Stéphane Gaubert, and Benjamin Werner. 2015b. Formal proofs for Nonlinear Optimization. *Journal of Formalized Reasoning* 8, 1 (2015), 1–24.

Maxima. 2013. Maxima, a Computer Algebra System. Version 5.30.0. (2013). http://maxima.sourceforge.net/

W. M. McEneaney. 2006. *Max-plus methods for nonlinear control and estimation*. Birkhäuser Boston Inc., Boston, MA. xiv+241 pages.

Guillaume Melquiond. 2012. Floating-point arithmetic in the Coq system. *Information and Computation* 216, 0 (2012), 14 – 23. DOI:http://dx.doi.org/10.1016/j.ic.2011.09.005 Special Issue: 8th Conference on Real Numbers and Computers.

Antoine Miné. 2006. The octagon abstract domain. *Higher-Order and Symbolic Computation* 19, 1 (2006), 31–100. DOI:http://dx.doi.org/10.1007/s10990-006-8609-1

Ramon E. Moore. 1962. *Interval Arithmetic and Automatic Error Analysis in Digital Computing*. Ph.D. Dissertation. Department of Computer Science, Stanford University.

César Muñoz and Anthony Narkawicz. 2013. Formalization of a Representation of Bernstein Polynomials and Applications to Global Optimization. *Journal of Automated Reasoning* 51, 2 (August 2013), 151–196. DOI:http://dx.doi.org/10.1007/s10817-012-9256-3

Nasa 2011. NASA World Wind Java SDK. (2011). http://worldwind.arc.nasa.gov/java/.

OCaml 2015. Objective Caml (OCaml) programming language website. (2015). http://caml.inria.fr/.

Gabriele Paganelli and Wolfgang Ahrendt. 2013. Verifying (In-)Stability in Floating-Point Programs by Increasing Precision, Using SMT Solving. In *15th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2013, Timisoara, Romania, September 23-26, 2013*, Nikolaj Bjørner, Viorel Negru, Tetsuo Ida, Tudor Jebelean, Dana Petcu, Stephen M. Watt, and Daniela Zaharie (Eds.). IEEE Computer Society, 209–216. DOI:http://dx.doi.org/10.1109/SYNASC.2013.35

Cordian Riener, Thorsten Theobald, Lina Jansson Andrén, and Jean B. Lasserre. 2013. Exploiting Symmetries in SDP-Relaxations for Polynomial Optimization. *Mathematics of Operations Research* 38, 1 (2013), 122–141. DOI:http://dx.doi.org/10.1287/moor.1120.0558

Pierre Roux. 2015. Formal Proofs of Rounding Error Bounds. *Journal of Automated Reasoning* (2015), 1–22. DOI:http://dx.doi.org/10.1007/s10817-015-9339-z

Philipp Rümmer and Thomas Wahl. 2010. An SMT-LIB Theory of Binary Floating-Point Arithmetic. In *Informal proceedings of 8th International Workshop on Satisfiability Modulo Theories (SMT) at FLoC, Edinburgh, Scotland*.

Alexey Solovyev and Thomas C. Hales. 2013. Formal Verification of Nonlinear Inequalities with Taylor Interval Approximations. In *NASA Formal Methods, 5th International Symposium, NFM 2013, Moffett Field, CA, USA, May 14-16, 2013. Proceedings (Lecture Notes in Computer Science)*, Guillaume Brat, Neha Rungta, and Arnaud Venet (Eds.), Vol. 7871. Springer, 383–397.

Alexey Solovyev, Charles Jacobsen, Zvonimir Rakamarić, and Ganesh Gopalakrishnan. 2015. Rigorous Estimation of Floating-Point Round-off Errors with Symbolic Taylor Expansions. In *Proceedings of the 20th International Symposium on Formal Methods (FM) (Lecture Notes in Computer Science)*, Nikolaj Bjørner and Frank de Boer (Eds.), Vol. 9109. Springer, 532–550.

J. Stolfi and L.H. de Figueiredo. 2003. An Introduction to Affine Arithmetic. *TEMA Tend. Mat. Apl. Comput.* 4, 3 (2003), 297 – 312.

M.J. Todd. 2001. Semidefinite Optimization. *Acta Numerica* 10 (2001), 515–560.

Lieven Vandenberghe and Stephen Boyd. 1994. Semidefinite Programming. *SIAM Rev.* 38 (1994), 49–95.

Hayato Waki, Sunyoung Kim, Masakazu Kojima, and Masakazu Muramatsu. 2006. Sums of Squares and Semidefinite Programming Relaxations for Polynomial Optimization Problems with Structured Sparsity. *SIAM Journal on Optimization* 17, 1 (2006), 218–242.

Makoto Yamashita, Katsuki Fujisawa, Kazuhide Nakata, Maho Nakata, Mituhiro Fukuda, Kazuhiro Kobayashi, and Kazushige Goto. 2010. *A high-performance software package for semidefinite programs : SDPA7*. Technical Report. Dept. of Information Sciences, Tokyo Institute of Technology, Tokyo, Japan. http://www.optimization-online.org/DB_FILE/2010/01/2531.pdf