Guaranteed Proofs Using Interval Arithmetic
Marc Daumas, Guillaume Melquiond, César Muñoz

To cite this version:
Marc Daumas, Guillaume Melquiond, César Muñoz. Guaranteed Proofs Using Interval Arithmetic. 17th IEEE Symposium on Computer Arithmetic, 2005, Cape Cod, Massachusetts, United States. pp.188-195, 10.1109/ARITH.2005.25. hal-00164621

HAL Id: hal-00164621
https://hal.archives-ouvertes.fr/hal-00164621
Submitted on 22 Jul 2007

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Guaranteed Proofs Using Interval Arithmetic

Marc Daumas, Guillaume Melquiond, and César Muñoz

Abstract

This paper presents a set of tools for mechanical reasoning of numerical bounds using interval arithmetic. The tools implement two techniques for reducing decorrelation: interval splitting and Taylor’s series expansions. Although the tools are designed for the proof assistant system PVS, expertise on PVS is not required. The ultimate goal of the tools is to provide guaranteed proofs of numerical properties with a minimal human-theorem prover interaction.

1 Introduction

Deadly and disastrous failures [4, 7, 12] confirm the shared belief that the traditional peer-review process is not sufficient to guarantee correctness of published proofs and software [11]. Despite this belief, mechanical theorem provers and proof assistants are not widely used in the applied mathematics community. Part of the problem is the lack of user friendly interfaces that result on steep learning curves. This paper presents a set of tools for mechanical reasoning of numerical bounds using interval arithmetic. The goal is to provide guaranteed formal proofs of numerical properties with a minimum effort.

Interval arithmetic has been used for decades as a standard tool for numerical analysis on engineering applications [8, 15]. In interval arithmetic, operations are evaluated on range of numbers rather than on real numbers. Formally, an interval $x = [a, b]$ is the set of real numbers between $a$ and $b$, i.e.,

$$[a, b] = \{ x \mid a \leq x \leq b \}.$$  

where $\times = \{ +, -, \times, \div \}$. This property is fundamental to interval arithmetic. It guarantees that the evaluation of an expression using interval arithmetic is a correct approximation of the exact real value.

Interval arithmetic is sub-distributive, i.e., $x \times (y + z) \subseteq x \times y + x \times z$. In the general case, the inclusion is strict. This may have surprising effects, for instance $x - x$ is, in general, different from the interval $0$, e.g., $[0, 1] - [0, 1] \neq [-1, 1]$. This effect is also called decorrelation and it is due to the fact that interval identity is lost in interval arithmetic.

Consider the function $f(x) = x \times (1 - x)$. A simple analysis reveals that $f$ reaches its maximum at $x = \frac{1}{2}$ with $f\left(\frac{1}{2}\right) = \frac{1}{4}$. If $x \in [0, 1]$, the minimums are reached at the bounds with $f(0) = f(1) = 0$. Hence,

$$\forall x \in [0, 1] : x \times (1 - x) \in \left[0, \frac{1}{4}\right].$$  

On the other hand, the interval expression $x \times (1 - x)$, where $x = [0, 1]$, evaluates to $[0, 1]$. The inclusion property guarantees that $[0, 1]$ is a correct approximation of $f(x)$, for $x \in \mathbb{R}$. However, as this example shows, it may not be the best one:

$$\left[0, \frac{1}{4}\right] \subset [0, 1].$$  

1In the case of division, it is assumed that $0 \not\in y$. 

---

* M. Daumas (Marc.Daumas@ens-lyon.fr) and G. Melquiond (Guillaume.Melquiond@ens-lyon.fr) are with the LIP Computer Science Laboratory, UMR 5668 CNRS–ENS Lyon–INRIA, France. César Muñoz (munoz@nianet.org) is with the National Institute of Aerospace, 144 Research Drive, Hampton, VA, USA. This work was partially supported by the National Aeronautics and Space Administration under NASA Cooperative Agreement NCC-1-02043, by the French National Center for Scientific Research under CNRS PICS grant 2533, and by the Department of the Development and the Department of the Industrial Relations (DirDRI) of the INRIA.
There are a few techniques to reduce the effect of decorrelation. They usually require arithmetic manipulations of the interval expressions and a fine analysis of the interval variables. For example, an expert will probably note that \( f(x) \) is equivalent to \( 1 - (x - \frac{1}{2})^2 \), and that the corresponding interval expression \( 1 - (x - \frac{1}{2})^2 \) does not suffer from decorrelation. The proof that a particular numerical expression satisfies some given bounds is not necessarily difficult, but it can be cumbersome, tedious, and, definitively, error prone.

This paper presents a set of tools that support mechanical proof checking of numerical bounds using interval arithmetic. The tools implement two techniques to reduce decorrelation. The first technique is based on interval splitting. The second technique is based on Taylor’s series expansions. The tools are designed for the verification system PVS,\(^2\) which is developed by SRI International [16]. However, minimal PVS expertise is required to use our tools as most of the technical burden of proving properties in a proof assistant system is hidden from the user. A C++ library generates proof obligations and proof scripts, in the form of PVS files, for a given numerical problem. The files are processed by PVS in batch mode and a summary of the status of the proofs is printed. User interaction with the theorem prover is minimized. This approach is usually referred as invisible formal methods [21].

The rest of this paper is organized as follows. Section 2 presents an overview of the PVS interval arithmetic library. The usage of the library is illustrated with the toy example \( x \times (1 - x) \in [0, 1] \) for \( x \in [0, 1] \). This example is reused in Section 3 to show how the precision can be improved by a simple interval splitting technique. Section 4 motivates a Taylor’s series expansion technique with an example taken from a critical aeronautical application. That technique guarantees that an implemented polynomial approximation is close to about one unit in the last place (ulp) of the exact transcendental function. The relative error is exactly bounded by \( 1.36 \times 10^{-6} \). Section 5 presents the C++ library that generates the proof obligations and proof scripts of the examples in sections 3 and 4.

### 2 A PVS Library for Interval Arithmetic

The Prototype Verification System (PVS) [16] is a mechanical proof checker that provides a strongly typed specification language and a theorem prover for higher-order logic. PVS developments are organized in theories. A theory is a collection of mathematical and logical objects such as function definitions, variable declarations, axioms, and lemmas.


The library Interval is a set of PVS theories defining rational interval arithmetic. The library provides a set of proof strategies that automate interval reasoning, specially with respect to decorrelation effects.

Listing 1 shows a few definitions from the PVS theory `Interval`. Dots are used to simplify the presentation and hide some technical parts. Comments start with the symbol `#` and extend to the end of the line. The theory defines the type `Interval` and mathematical variables \( x, y \) of type `real` (real numbers), \( X, Y \) of type `Interval`, and \( n \) of type `nat` (natural numbers).

Intervals are stored as pairs of real numbers \([|x, y|]\). For instance, the PVS object \([|0, 1|]\) represents the interval \([0, 1]\). If \( X \) is a PVS interval, \( \text{lb}(X) \) is the lower bound and \( \text{ub}(X) \) is the upper bound of \( X \). The propositions \( x \in X \) and \( x \subseteq y \) are written \( x \#\# X \) and \( X \ll Y \), respectively. Furthermore, the proposition \( X > x \) states that all values in \( X \) are strictly greater than \( x \); similarly for \( X \geq x \), \( X < x \), and \( X \leq x \).

The four basic interval operations are defined as in [9]:

\[
\begin{align*}
  x + y &= \left[ \frac{x+y}{2}, \frac{x+y}{2} \right] \\
  x - y &= \left[ \frac{x-y}{2}, \frac{x-y}{2} \right] \\
  x \times y &= \left[ \min\{|xy|, |xy|, |xy|, |xy|\}, \\
  \max\{|xy|, |xy|, |xy|, |xy|\} \right] \\
  x \div y &= x \times \left[ \frac{1}{y}, \frac{1}{y} \right], \quad \text{if } y \neq 0.
\end{align*}
\]

We also define negative, absolute value, square, and power functions as follows:

\[
\begin{align*}
  -x &= [-x, -x], \\
  |x| &= \left\{ \begin{array}{ll}
  \min\{|x|, |x|\}, & \text{if } x \geq 0, \\
  \max\{|x|, |x|\}, & \text{if } x < 0.
\end{array} \right. \\
  x^n &= \left\{ \begin{array}{ll}
  [1], & \text{if } n \geq 0, \\
  [x^n, x^n], & \text{if } x \geq 0 \text{ or odd}(n), \\
  [0, \max\{x^n, x^n\}], & \text{otherwise}.
\end{array} \right.
\end{align*}
\]

Interval union \( x \cup y \), written in PVS \( X \cup Y \), is defined as the smallest rational interval that contains both \( x \) and \( y \). All these operations are defined such that they satisfy the inclusion property. Indeed, the lemmas shown in Listing 2 are, among many others, provided by the library and formally verified. Free variables are implicitly quantified universally. As we will see, these properties are the basis of the automated support for interval reasoning.
PVS Listing 1 Basic definitions

% interval.pvs
Interval : THEORY
BEGIN

Interval : TYPE = ...

x,y : VAR real
X,Y : VAR Interval
n : VAR nat

+(X,Y): Interval = [|lb(X)+lb(Y),
ub(X)+ub(Y)|]
-(X,Y): Interval = [|lb(X)-ub(Y),
ub(X)-lb(Y)|]
-(X) : Interval = [|-ub(X),
-lb(X)|]
*(X,Y): Interval = ...
/(X,Y): Interval = X * [|1/ub(Y),
1/lb(Y)|]
Abs(X): Interval = ...
Sq(X) : Interval = ...
ˆ( X,n ) : Interval = ...
U(X,Y) : Interval = [|min(lb(X),lb(Y)),
max(ub(X),ub(Y))|]

END Interval

PVS Listing 2 Inclusion properties (I)

... Add_sharp : LEMMA
x # # X AND y # # Y => x+y # # X+Y

Sub_sharp : LEMMA
x # # X AND y # # Y => x-y # # X-Y

Neg_sharp : LEMMA
x # # X => -x # # -X

Mult_sharp : LEMMA
x # # X AND y # # Y => x*y # # X*Y

Zeroless?(X): bool = X > 0 OR X < 0

Div_sharp : LEMMA
Zeroless?(Y) AND
x # # X AND y # # Y => x/y # # X/Y

Abs_sharp : LEMMA
x # # X => abs(x) # # abs(X)

Sq_sharp : LEMMA
x # # X => sq(x) # # sq(X)

Pow_sharp : LEMMA
x # # X => x^n # # X^n

END Interval
The square root and the trigonometric functions are implemented by approximation series. A PVS library of approximations was originally developed by one of the authors for the verification of an algorithm for aircraft conflict detection [14]. It was completed and extended with logarithm, exponential and arc tangent functions by David Lester. The approximation library is part of the NASA Langley PVS libraries.\footnote{Available from http://shemesh.larc.nasa.gov/fm/ftp/larc/PVS-library/pvslib.html.}

The basic idea is to provide for each real function \( f : \mathbb{R} \to \mathbb{R} \), parametric algebraic functions \( \overline{f} : (\mathbb{R}, N) \to \mathbb{R} \) and \( \overline{f} : (\mathbb{R}, N) \to \mathbb{R} \), such that for all \( x, n \)

\[
\begin{align*}
    \frac{f(x, n)}{f(x, n)} & \leq f(x) \leq \frac{f(x, n + 1)}{f(x, n)}, & (1) \\
    \frac{f(x, n + 1)}{f(x, n)} & \leq f(x) \leq \frac{f(x, n)}{f(x, n + 1)}, & (2) \\
    \lim_{n \to \infty} \frac{f(x, n)}{f(x, n)} = f(x) = \lim_{n \to \infty} \frac{f(x, n + 1)}{f(x, n)}. & (4)
\end{align*}
\]

Formula (1) states that \( f \) and \( \overline{f} \) are, respectively, lower and upper bounds of \( f \), and Formulas (2), (3), and (4) state that these bounds can be improved, as much as needed, by increasing the approximation parameter \( n \). Furthermore, we require that \( f \) and \( \overline{f} \) are closed for rational numbers.

For each \( f \), the corresponding parametric interval function \( f \) is defined as follows:

\[
\begin{align*}
    f(x, n) & = \left[ f(x, n), \overline{f}(x, n) \right], \text{ if } f \text{ is increasing,} \\
    f(x, n) & = \left[ \overline{f}(x, n), f(x, n) \right], \text{ if } f \text{ is decreasing.}
\end{align*}
\]

If \( f \) is neither increasing nor decreasing, as in the case of trigonometric functions, \( f \) is defined by case analysis on subintervals that are increasing or decreasing. The parameter \( n \) sets the accuracy of the approximations. In a real numerical problem, this parameter is set in advance by an external program that explores in an efficient way a vast number of values before deciding for the best one. This is one of the functionalities of the C++ library presented in Section 5.

The definitions of the square root and trigonometric interval operations satisfy the inclusion properties in Listing 3. Appropriate preconditions such as \( X \geq 0 \) and \( \tan? (X) \) guarantee that the operations sqrt and tan are well-defined.

Three basic strategies are provided by Interval: sharp, instint, and joint.

---

**PVS Listing 3** Inclusion properties (II)

\[
\begin{align*}
    \text{Sqrt_sharp} & : \text{LEMMA} \\
    & \quad X \geq 0 \text{ AND} \\
    & \quad x \#\# X \Rightarrow \sqrt{x} \#\# \overline{\text{Sqrt}(x, n)} \\
    \text{Sin_sharp} & : \text{LEMMA} \\
    & \quad x \#\# X \Rightarrow \sin(x) \#\# \overline{\text{Sin}(x, n)} \\
    \text{Cos_sharp} & : \text{LEMMA} \\
    & \quad x \#\# X \Rightarrow \cos(x) \#\# \overline{\text{Cos}(x, n)} \\
    \text{Tan_sharp} & : \text{LEMMA} \\
    & \quad \tan? (X) \text{ AND} \\
    & \quad x \#\# X \Rightarrow \tan(x) \#\# \overline{\text{Tan}(x, n)}
\end{align*}
\]

Let \( e(x_1, \ldots, x_n) \) be a real expression with variables \( x_1, \ldots, x_n \), and \( e(x_1, \ldots, x_n) \) be the interval expression corresponding to \( e \) (for a pre-determined approximation parameter), where \( x_i \in x_i, \text{ for } 1 \leq i \leq n \).

- The proof rule sharp automatically discharges goals of the form

\[
x_1 \in x_1, \ldots, x_n \in x_n \\
\frac{e(x_1, \ldots, x_n)}{e(x_1, \ldots, x_n)} \in e(x_1, \ldots, x_n)
\]

using the inclusion lemmas in Listing 2 and Listing 3.

- Let \( y \) be a rational interval. The proof rule instint automatically discharges goals of the form

\[
x_1 \in x_1, \ldots, x_n \in x_n \\
\frac{e(x_1, \ldots, x_n)}{e(x_1, \ldots, x_n)} \in y
\]

by showing that \( e(x_1, \ldots, x_n) \in e(x_1, \ldots, x_n) \) using sharp, and then evaluating the numerical interval expression

\[
e(x_1, \ldots, x_n) \subseteq y.
\]

- The proof rule joint automatically discharges goals of the form

\[
x_1 \in x_1, \ldots, x_n \in x_n \\
\frac{e(x_1, \ldots, x_n)}{e(x_1, \ldots, x_n)} \in y
\]

by showing that

\[
x_1 \in x_1, \ldots, x_i \in x_i', \ldots, x_n \in x_n \\
\frac{e(x_1, \ldots, x_n)}{e(x_1, \ldots, x_n)} \in y
\]

and

\[
x_1 \in x_1, \ldots, x_i \in x_i'', \ldots, x_n \in x_n \\
\frac{e(x_1, \ldots, x_n)}{e(x_1, \ldots, x_n)} \in y
\]

provided that (1) \( x_i = x_i' \cup x_i'' \) and (2) \( x_i' \) and \( x_i'' \) overlap. Appropriate parameters tell the strategy how to select \( x_i, x_i', \text{ and } x_i'' \).
The file fair.pvs, in Listing 4, includes the lemma fair.approx that states 
\[ \forall x \in [0, 1] : x \times (1 - x) \in [0, 1]. \]

**PVS Listing 4** Toy example

```pvs
% fair.pvs
fair : THEORY
BEGIN
fair_approx : LEMMA
FORALL (x:real):
  x ## [0,1] IMPLIES
  x*(1-x) ## [0,1]
%|- fair_approx : PROOF (instint) QED
END fair
```

The PVS theorem prover is generally used in interactive mode. However, batch proving is supported in PVS by the package ProofLite. Proof scripts are written as comments using the special comment symbol %|- . In this case, the interval proof strategy instint is associated to the lemma fair.approx. The file fair.pvs is proof checked in batch mode with the command proveit:

```
$ proveit -package Interval fair.pvs
```

After a few seconds, the following message is displayed:

```
Theory totals:
1 formulas, 1 attempted, 1 succeeded
```

3 Sharper Bounds by Interval Splitting

Lemma fair.approx of Section 2.4 is very inaccurate as it bounds \( x \times (1 - x) \), with \( x \in [0, 1] \), by \([0, \frac{1}{2}]\) instead of \([0, \frac{3}{4}]\). This is due to decorrelation on \( x \). In many cases, the easiest way to reduce decorrelation is to divide the input interval in many subintervals and to evaluate the expression on these subintervals separately.

For example, the interval \([0, 1]\) could be evenly divided into 16 intervals \([i/16, (i+1)/16]\). Each arithmetic evaluation is a subset of \([0, \frac{9}{32}]\) that is a little larger than the optimal \([0, \frac{1}{4}]\).

The C++ library presented in Section 5 finds the same degree of accuracy with only 8 intervals:

\[
\begin{array}{cccc}
[0, \frac{1}{4}] & [\frac{1}{4}, \frac{1}{2}] & [\frac{1}{2}, \frac{9}{16}] & [\frac{9}{16}, \frac{3}{4}] \\
[\frac{1}{2}, \frac{3}{4}] & [\frac{3}{4}, \frac{5}{8}] & [\frac{5}{8}, \frac{7}{16}] & [\frac{7}{16}, \frac{1}{2}] \\
\end{array}
\]

Indeed, the PVS file toy.pvs in Listing 5 is automatically generated from the original problem and some extra parameters. In this case, 16 lemmas are necessary to guarantee the required accuracy \([0, \frac{1}{2}]\). Lemmas ToyI0 and ToyI1 prove the case of the subintervals \([0, \frac{1}{4}]\) and \([\frac{1}{4}, \frac{1}{2}]\), respectively, using the proof rule instint. Lemma ToyC1 proves the case of the subinterval \([0, \frac{9}{32}]\) by using the proof rule joint. The strategy shows that \([0, \frac{3}{4}] = [0, \frac{1}{4}] \cup [\frac{1}{4}, \frac{3}{8}]\), and then applies lemmas ToyI0 and ToyI1. The final lemma ToyC7 proves the result on the whole interval \([0, 1]\).

**PVS Listing 5** Toy example (revisited)

```pvs
% toy.pvs
toy : THEORY
BEGIN
  x :VAR real
ToyI0 : LEMMA
  x ## [0,4/16] IMPLIES
  x * (1 - x) ## [0,9/32]
%|- ToyI0 : PROOF (instint) QED
ToyI1 : LEMMA
  x ## [4/16,6/16] IMPLIES
  x * (1 - x) ## [0,9/32]
%|- ToyI1 : PROOF (instint) QED
ToyC1 : LEMMA
  x ## [0,6/16] IMPLIES
  x * (1 - x) ## [0,9/32]
%|- ToyC1 : PROOF
%|- (joint "ToyI0" "ToyI1")
%|- QED
...
ToyC7 : LEMMA
  x ## [0,16/16] IMPLIES
  x * (1 - x) ## [0,9/32]
%|- ToyC7 : PROOF
%|- (joint "ToyC6" "ToyI7")
%|- QED
END toy
```

Proof checking the file toy.pvs in batch mode reports:

```
$ proveit -package Interval toy.pvs
Theory totals:
16 formulas, 16 attempted, 16 succeeded
```

---

4Available from [http://research.nianet.org/~munoz/ProofLite](http://research.nianet.org/~munoz/ProofLite).
4 Taylor’s Series Expansions

Taylor’s Theorem yields the following rule on interval arithmetic. Let $x, a \in \mathbb{X} = (x_0, \ldots, x_n)$ be a list of intervals,

$$
\frac{d^i}{dx^i}(a) \in x_i, \text{ for } 0 \leq i < n, \text{ and } \\
\forall y \in \mathbb{X} : \frac{d^i}{dx^i}(y) \in x_i
$$

This rule is implemented by the strategy $taylor$ in the library Interval. In this section, we show how this rule may be used to reduce decorrelation in a real example.

The function

$$
r(\phi) = \frac{a}{1 + (1 - f)^2 \tan^2 \phi},
$$

where $a$ and $f$ are constants defined by WGS84, appears in the implementation of aircraft navigation algorithms. Indeed, $r(\phi)$ is used to translate aircraft geodesic coordinates, as calculated by global positioning systems, to Cartesian coordinates used, for example, by geometric conflict detection and resolution algorithms [3].

For efficiency reasons, one may want to approximate the function $r(\phi)$ by polynomial

$$
\hat{r}(\phi) = \frac{4439091}{4} + (\phi_0^2 - \phi_0^2) \times \\
\phantom{\frac{4439091}{4}} \frac{9023647}{4} + (\phi_0^2 - \phi_0^2) \times \\
\phantom{\frac{4439091}{4}} \frac{13868737}{64} + (\phi_0^2 - \phi_0^2) \times \\
\phantom{\frac{4439091}{4}} \frac{13233647}{2048} + (\phi_0^2 - \phi_0^2) \times \\
\phantom{\frac{4439091}{4}} \frac{1898597}{16384} + (\phi_0^2 - \phi_0^2) \times \\
\phantom{\frac{4439091}{4}} \frac{6661427}{131072},
$$

where $\phi_0 = 715/512 \approx 80\pi/180$ and $\phi \in [0, \phi_0]$, as the latitude is assumed to be between 0 and 80°.

The coefficients of the polynomial approximation and $\phi_0^2$ are stored exactly using IEEE single precision. Thus, the objective is to show that

$$
e(\phi) = r(\phi) - \hat{r}(\phi),
$$

is bounded by $1.36 \times 10^{-6}$, i.e., about an ulp of the exact value.

Let $r(\Phi), \hat{r}(\Phi)$, and $e(\Phi)$ be the interval expressions corresponding to $r(\phi), \hat{r}(\phi)$, and $e(\phi)$, respectively, and $\Phi$ be an interval such that $\phi \in \Phi \subseteq [0, \phi_0]$. Decorrelation on $e(\Phi)$ yields that for any interval $\Phi$, $e(\Phi)$ is wider than the sum of the width of intervals $r(\Phi)$ and $\hat{r}(\Phi)$. Therefore, the splitting technique presented in the previous section would require more than $\phi_0/\text{ulp}$ subintervals to verify that $e(\Phi)$ is no wider than one ulp. No proof assistant can guarantee such a large number of lemmas in a reasonable time.

To reduce decorrelation, we use Taylor’s series expansion with $x = \phi, n = 1, a$ equal to the midpoint of $\Phi, x = \Phi, x_0 = e([a])$, and $x_n = e(\Phi)$, where $e'$ is the interval function corresponding to the first derivative of $e$. We get

$$
e(\phi) \leq e(a) + (\Phi - a)e'(\Phi),
$$

as both (1) $e(a) \in e([a])$ and (2) $\forall \Phi : e'(\Phi) \leq e'(\Phi)$ trivially hold. Decorrelation on Formula (5) is reduced to first order with respect to the original $e(\Phi)$.

Further reduction of decorrelation could be obtained by increasing the order of the Taylor series expansion, e.g., the second order expansion yields

$$
e(\phi) \leq e(a) + (\Phi - a)e'(\Phi) + \frac{(\Phi - a)^2}{2} e''(\Phi).
$$

However, note that $\hat{r}(\phi)$ is a least square approximation of $r(\phi)$ on Chebyshev’s polynomials [18] and $r(\phi)$ is a relatively smooth function. Therefore, the first order expansion, along with interval splitting, is sufficient in this case to show the required accuracy.

Listing 6 illustrates the PVS definitions used in this example. As a convention in PVS, real functions are written in lowercase, and interval functions are written in uppercase. In particular, $r, \hat{r}, e,$ and $\hat{e}$ correspond to $r, \hat{r}, e,$ and $\hat{e}$, respectively, whereas $\mathbb{R}, \hat{\mathbb{R}},$ and $E$ correspond to $r, \hat{r},$ and $e$, respectively. PVS is a strongly typed language where every function has to be well-defined. The user-defined type $\Phi$ rules out values $\Phi$ where every function has to be well-defined. The empty interval acts as an exceptional value in cases where the real function is undefined.

Contrary to the approach described in [19], we do not have to generate a new Taylor approximation for each subrange. By using an interval-based Taylor expansion, the same expression can be reused for all the subranges. We do not suffer from the Taylor coefficients being irrational numbers, they are simply given by interval expressions involving rational functions. Relying on rational interval arithmetic leads to conceptually simpler proofs: one single global Taylor expansion has to be validated, and the proofs for all the subranges simply consist in an interval instantiation of this expansion.

5 A C++ Library for Real Applications

The splitting technique presented in Section 3 is implemented by an external library written in C++. Given a nu-

---

PVS Listing 6 Functions $R$, $\hat{r}$, and $E$ in PVS

\begin{verbatim}
a : real = 6378137 
f : real = 1000000000/298257223563 
uf2 : real = sq(1 - f) 
maxsq : real = 511225/262144 

Phi : TYPE = {x: real | x ## [0,715/512]} 

r(phi:Phi) : real = a / sqrt(1 + uf2 * sq(tan(phi))) 
R(PHI:Interval) : Interval = a / Sqrt(1 + uf2 * Sq(Tan(PHI,4)),7) 

hat_r(phi:Phi) : real = (4439091/4) + (maxsq - sq(phi)) * ( 
  (9023647/4) + (maxsq - sq(phi)) * ( 
    (13868737/64) + (maxsq - sq(phi)) * ( 
      (13233647/2048) + (maxsq - sq(phi)) * ( 
        (-1898597/16384) + (maxsq - sq(phi)) * 
          (-6661427/131072)))) 

hat_R(PHI:Interval) : Interval = (4439091/4) + (maxsq - Sq(PHI)) * ( 
  (9023647/4) + (maxsq - Sq(PHI)) * ( 
    (13868737/64) + (maxsq - Sq(PHI)) * ( 
      (13233647/2048) + (maxsq - Sq(PHI)) * ( 
        (-1898597/16384) + (maxsq - Sq(PHI)) * 
          (-6661427/131072)))) 


e(phi:Phi) : real = r(phi) - hat_r(phi) 
E(PHI:Interval) : Interval = R(PHI) - hat_R(PHI) 
\end{verbatim}

merical problem, the library finds an appropriate subinterval division and generates proof obligations, in the form of lemmas, and proof guarantees, in the form of proof scripts, that yield a required accuracy. Lemmas and proofs are grouped in files such that they can be processed in parallel by PVS. The library also sets, as needed, the approximation parameters of the square root and trigonometric functions. The splitting technique applied to Formula (5) starts with 100,000 subintervals to guarantee that the relative error is bounded by $1.36 \times 10^{-6}$. The trigonometric functions must be approximated to the $4$th term and the square root to the $7$th term. In total 9,935 intervals were considered. For each interval, 3 lemmas and their respective proof scripts were automatically generated by the C++ library. As expected, the final lemma in this development reads:

$$\text{PHI} : \text{Interval} = [|0,715/512|]$$

RI : LEMMA

FORALL (phi:real) :
phi #\# PHI =\= e(phi) / r(phi) #\# 
[|-136/1000000000,136/1000000000|]$

6 Conclusion and Perspective

The examples presented in Sections 3 and 4 could have been handled in HOL-light\(^6\) using one of the tools presented in [6]. According to Sturm’s theorem [10, p. 434] that development is more efficient on these specific examples but it is limited to problems that can ultimately be approximated by polynomial functions. On the other hand, the techniques presented here can seamlessly guarantee rational approximations or even arbitrary programmed approximations as long as they are piecewise continuously differentiable (for the developments of Section 4).

In summary, the tools allow users to state and formally verify numerical properties in PVS with a minimal interaction with the theorem prover. No PVS expertise is required in most cases.

Research is conducted to study the feasibility of enhancing the prototypes with some of the following features:

- Floating point arithmetic rather than rational arithmetic as developed in [2].
- Use of high speed multiple precision techniques.
- Implementation of latest developments on Taylor’s models [13], and mix Taylor’s models and floating point arithmetic [17].

The tools are currently being used to check numerical properties of aircraft navigation algorithms developed at the National Institute of Aerospace (NIA).7

Acknowledgment

Proofs of Sections 4 and 5 were checked on high performance clusters set up and maintained by the Reso research project of the LIP computer science laboratory.

References


7The PVS library Interval described in this paper is available from http://research.nianet.org/~munoz/Interval.