Real Number Calculations and Interval Analysis in PVS *

César A. Muñoz
munoz@nianet.org

National Institute of Aerospace @ NASA LaRC

Universidade de Brasilia – Abril 2006

* Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

International Space Station

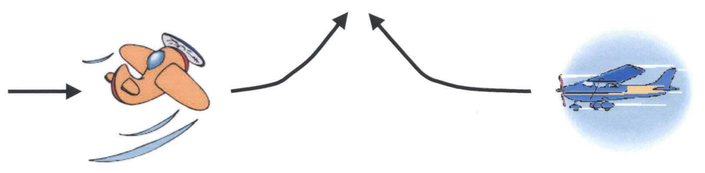
ISS012E22281

Marco Pontes: Crew member of Expedition 13.

Conflict Detection and Resolution

A NASA Application

How to avoid these situations ?



[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Requirements

- Distributed: Responsibility for separation resides on the pilot.
- Pair-wise: Two aircraft (ownship and intruder)
- Tactical: Detection and resolution are based on state information (as opposed to intent information).
- Implicit coordination: No information is exchanged between the aircraft (but aircraft are aware of traffic position and velocity).
- Independent coordination: Resolution are repulsive, but cooperation is not required to keep minimum separation.

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

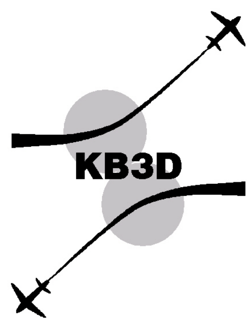
KB3D

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

KB3D is an algorithm designed and verified by the Formal Methods group at NIA-NASA Langley.



Conflict Detection: Problem

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Given the relative 3-D position $\vec{s} = (s_x, s_y, s_z)$ and velocity vector $\vec{v} = (v_x, v_y, v_z)$ of the *ownship* with respect to an *intruder* aircraft, define

$\texttt{cd3d}(s_x, s_y, s_z, v_x, v_y, v_z)\texttt{:bool}$

such that
$\texttt{cd3d}(s_x, s_y, s_z, v_x, v_y, v_z) \equiv$
"There is a predicted conflict within a lookahead time T" $\equiv$

$\exists_{0 \le t < T} (s_x + t v_x)^2 + (s_y + t v_y)^2 < D^2$ and
$(s_z + t v_z)^2 < H^2$

César A. Muñoz
munoz@nianet.org

Conflict Detection (in PVS)

```
cd3d(s_x,s_y,s_z,v_x,v_y,v_z:real) : bool =
  IF  v_x=0 && v_y=0 && s_x^2+s_y^2<D^2 THEN
    s_z^2<H^2 || (v_z s_z<0 && -H<sign(v_z)(T v_z+s_z))
  ELSE
    LET d = 2 s_x v_x s_y v_y+D^2 (v_x^2+v_y^2) - (s_x^2 v_y^2+s_y^2 v_x^2) IN
    IF d>0 THEN
      LET a = v_x^2+v_y^2 IN
      LET b = s_x v_x+s_y v_y IN
      IF v_z = 0 THEN
        s_z^2<H^2 && (D^2>s_x^2+s_y^2 || b≤0) && (d>(a T+b)^2 || a T+b≥0)
      ELSE
        LET t_1 = (-sign(v_z) H-s_z)/v_z IN
        LET t_2 = (sign(v_z) H-s_z)/v_z IN
        (d>(a t_2+b)^2 || a t_2+b≥0) && (d>(a t_1+b)^2 || a t_1+b≤0) &&
        (D^2>s_x^2+s_y^2 || b≤0) && (d>(a T+b)^2 || a T+b≥0) &&
        t_1<T && t_2>0
        ENDIF
    ELSE FALSE
    ENDIF
  ENDIF
```


Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Conflict Detection: Verification

- Correctness: THEOREM
  $\forall\ \vec{s}, \vec{v}.$
  $\mathtt{cd3d}(\vec{s}, \vec{v}) \implies$
  $\exists_{0 \le t < T}.\ (s_x + tv_x)^2 + (s_y + tv_y)^2 < D^2\ \wedge\ (s_z + tv_z)^2 < H^2.$

- Completeness: THEOREM
  $\forall\ \vec{s}, \vec{v}.$
  $(\exists_{0 \le t < T}.\ (s_x + tv_x)^2 + (s_y + tv_y)^2 < D^2\ \wedge\ (s_z + tv_z)^2 < H^2) \implies$
  $\mathtt{cd3d}(\vec{s}, \vec{v}).$

- Both theorems were formally verified using a mechanical theorem prover.

Example 1.*

- The turn rate of an aircraft flying at v knots and with a bank angle of ϕ is given by the formula

$$\dot{\theta}(\phi, v) = g \tan(\phi)/v,$$

where $g = 9.8$ m/s^2.

- What is $\dot{\theta}(35^o, 250knots)$?

*Taken from *Formal verification of conflict detection algorithms*, C. Muñoz, R. Butler, V. Carreño, and G. Dowek, 2003.

In Java ...

```
class thetadot {

  static final double g = 9.8;

  static double thetadot(double phi,double v) {
    return 1000*g*Math.tan(phi*Math.PI/180.0)/(514*v);
  }

  public static void main(String argv[]) {
    double phi = 35;
    double v   = 250;
    System.out.println("thetadot("+phi+","+v+") = "+
                       thetadot(phi,v));
  }
}
```

```
$ java thetadot
thetadot(35.0,250.0) = 0.05340104182455374
```


Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

In PVS . . .

```
thetadot : THEORY
BEGIN
  g : posreal = 9.8

  thetadot (phi:real,v:posreal) : real =
    1000*g*tan(phi*pi/180)/(514*v)

  phi : posreal = 35
  v   : posreal = 250

  thetadot_35_250 : axiom
    0.053 <= thetadot(phi,v) AND
    thetadot(phi,v) <= 0.054

END thetadot
```


[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Example 2.[¶]

- Given the following definition:

$$
\begin{aligned}
a_0 &= 11/2 \\
a_1 &= 61/11 \\
a_{n+2} &= 111 - \frac{1130 - 3000/a_n}{a_{n+1}}
\end{aligned}
$$

- What is a_{20} ?

[¶] Taken from *Arithmétique des ordinateurs, J.-M. Muller, 1989.*

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

In Java . . .

```
class mya {

  static double a(int n) {
    if (n==0)
      return 11/2.0;
    if (n==1)
      return 61/11.0;
    return 111 - (1130 - 3000/a(n-2))/a(n-1);
  }

  public static void main(String[] argv) {
    for (int i=0;i<=20;i++)
      System.out.println("a("+i+") = "+a(i));
  }
}
```

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

$a_0 \ldots a_{20}$

```
$ java mya
a(0)  = 5.5
a(2)  = 5.5901639344262435
a(4)  = 5.674648620514802
a(6)  = 5.74912092113604
a(8)  = 5.81131466923334
a(10) = 5.861078484508624
a(12) = 5.935956716634138
a(14) = 15.413043180845833
a(16) = 97.13715118465481
a(18) = 99.98953968869486
a(20) = 99.99996275956511
```

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

In PVS ...

```
mya : THEORY
BEGIN

    a(n:nat) : RECURSIVE posreal =
      if    n = 0 then 11/2
      elsif n = 1 then 61/11
      else  111 - (1130 - 3000/a(n-2))/a(n-1)
      endif
      MEASURE n

    a20_axiom : axiom
      99 <= a(20) AND a(20) <= 100

    a20_lemma : lemma
      a(20) <= 6
    %|- a20_lemma : PROOF (eval-formula) QED

END mva
```

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

How to Proof this Simple Lemma ?

```
    g   : posreal = 9.8
    phi : posreal = 35
    v   : posreal = 250

    td_35_250 : lemma
      0.053 <= 1000*g*tan(phi*pi/180)/(514*v)

%|- td_35_250 : PROOF ( ... ) QED
```

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

A Simple Lemma ?

- There are no variables. How hard could this be ?

```
  tr_35 : lemma
    3*pi/180 <= tr(35*pi/180)
%|- tr_35 : PROOF
%|- First note that that tan is increasing.
%|- Furthermore, π/6  <  35π/180. Moreover, ...
%|- QED
```


A Mechanical Proof

- Assume $\underline{\pi}, \overline{\pi}, \underline{\tan}, \overline{\tan}$, lower and upper bounds of π and tan, respectively.
- Goal:

$$\vdash \; 3\pi/180 \; \leq \; v\tan(35\pi/180)/g.$$

- *Proof*:
  1. $\vdash \; 3\pi/180 \; \leq \; 3\overline{\pi}/180$, because $\overline{\pi}$ is an upper bound.
  2. $\vdash \; v\underline{\tan}(35\underline{\pi}/180)/g \; \leq \; v\tan(35\pi/180)/g$, because $\underline{\tan}$ and $\underline{\pi}$ are lower bounds.
  3. $\vdash \; 3\overline{\pi}/180 \; \leq \; v\underline{\tan}(35\underline{\pi}/180)/g$, by simple calculation.

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Issues

1. What are the requirements for $\underline{f}$ and $\overline{f}$?
2. How to use $\underline{f}$ and $\overline{f}$ in a systematic way?
3. How to automate those proofs in PVS ?

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Issue 1: $\underline{f}$ and $\overline{f}$

The functions $\underline{f} : (\mathbb{R}, \mathbb{N}) \rightarrow \mathbb{R}$ and $\overline{f} : (\mathbb{R}, \mathbb{N}) \rightarrow \mathbb{R}$ are closed under $\mathbb{Q}$ such that

$$\begin{aligned} \underline{f}(x,n) \;\leq\; & f(x) \;\leq\; \overline{f}(x,n), & (1)\\ \underline{f}(x,n) \;\leq\; & \underline{f}(x,n+1), & (2)\\ \overline{f}(x,n+1) \;\leq\; & \overline{f}(x,n), & (3)\\ \lim_{n\rightarrow\infty} \underline{f}(x,n) \;=\; & f(x) \;=\; \lim_{n\rightarrow\infty} \overline{f}(x,n), & (4) \end{aligned}$$

where n is an approximation parameter.

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Solution Issue 1: Rational Lower Bounds

We have defined $\underline{f}$ and $\overline{f}$ for $f \in \{\sin, \cos, \tan, \pi, \mathrm{atan}, \sqrt{}, \exp, \ln\}$ and formally verified (in PVS) that they satisfy (1)-(4).

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Sine, Cosine

$$\begin{aligned}
\underline{\sin}(x,n) &= \sum_{i=1}^{2n} (-1)^{i-1} \frac{x^{2i-1}}{(2i-1)!}, \\
\overline{\sin}(x,n) &= \sum_{i=1}^{2n+1} (-1)^{i-1} \frac{x^{2i-1}}{(2i-1)!}, \\
\underline{\cos}(x,n) &= 1 + \sum_{i=1}^{2n+1} (-1)^{i} \frac{x^{2i}}{(2i)!}, \\
\overline{\cos}(x,n) &= 1 + \sum_{i=1}^{2(n+1)} (-1)^{i} \frac{x^{2i}}{(2i)!}.
\end{aligned}$$

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Logarithm $(1 < x \leq 2)$

For $-1 < x \leq 1$, we use the alternating series for natural logarithm:

$$\ln(x+1) \;=\; \sum_{i=1}^{\infty}(-1)^{i+1}\frac{x^i}{i}.$$

Therefore, we define

$$\underline{\ln}(x,n) \;=\; \sum_{i=1}^{2n}(-1)^{i+1}\frac{(x-1)^i}{i}, \quad \text{if } 1 < x \leq 2,$$

$$\overline{\ln}(x,n) \;=\; \sum_{i=1}^{2n+1}(-1)^{i+1}\frac{(x-1)^i}{i}, \quad \text{if } 1 < x \leq 2.$$

[a]Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Logarithm $(0 < x \leq 1)$

Using properties of the natural logarithm function, we obtain

$$\underline{\ln}(1,n) \;=\; \overline{\ln}(1,n) \;=\; 0,$$

$$\underline{\ln}(x,n) \;=\; -\underline{\ln}(\frac{1}{x},n), \quad \text{if } 0 < x < 1,$$

$$\overline{\ln}(x,n) \;=\; -\overline{\ln}(\frac{1}{x},n), \quad \text{if } 0 < x < 1.$$

Real Number Calculations and Interval Analysis in PVS [a]

[a]Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Logarithm $(2 < x)$

We observe that

$$\exists(m{:}\mathbb{N}, y{:}(1\ldots2]) : \ln(x) = m\ln(2) + \ln(y).$$

Hence,

$$\begin{array}{rcll} \underline{\ln}(x,n) & = & m\ \underline{\ln}(2,n) + \underline{\ln}(y,n), & \text{if } x > 2, \\ \overline{\ln}(x,n) & = & m\ \overline{\ln}(2,n) + \overline{\ln}(y,n), & \text{if } x > 2. \end{array}$$

Furthermore, $\surd$, tan, π, atan, exp, ...

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Issue 2: $\overline{f}$ or $\underline{f}$?

Note that

$$y + f(x) \quad \le \quad y + \overline{f}(x,n),$$

but

$$y - f(x) \quad \le \quad y - \underline{f}(x,n).$$

In general,

$$\begin{array}{rcll} k \times f(x) & \le & k \times F(x,n), & \text{where} \\ F & = & \overline{f} & \text{if } k \ge 0, \\ F & = & \underline{f} & \text{otherwise.} \end{array}$$

To chose the appropriate F, we first have to decide whether k is positive or negative.

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

A Difficult Decision Problem

$$\frac{k}{f(x)} \leq \frac{k}{F(x,n)}.$$

Which bound $F = \overline{f}$ or $F = \underline{f}$ is appropriate in this case ?

Solution Issue 2: Rational Interval Arithmetic

- Let $\underline{\mathbf{x}}, \overline{\mathbf{x}}$ be in $\mathbb{Q}$,

$$\mathbf{x} \;=\; [\underline{\mathbf{x}}, \overline{\mathbf{x}}] \;=\; \{x \mid \underline{\mathbf{x}} \leq x \leq \overline{\mathbf{x}}\}.$$

- Interval basic operations are defined such that they satisfy the inclusion property: If $x \in \mathbf{x}$ and $y \in \mathbf{y}$ then

$$\begin{aligned} x \otimes y &\in \mathbf{x} \otimes \mathbf{y}, \quad \text{where } \otimes \in \{+, -, \times, \div\}, \\ -x &\in -\mathbf{x}, \\ |x| &\in |\mathbf{x}|, \quad \text{and} \\ x^n &\in \mathbf{x}^n. \end{aligned}$$

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

From Real Functions to Interval Functions

- For each f, a parametric interval function $[\mathbf{f}]_n$ is defined as follows:

$$
\begin{array}{lcll}
[\mathbf{f}(\mathbf{x})]_n & = & [\underline{f}(\underline{\mathbf{x}}, n), \overline{f}(\overline{\mathbf{x}}, n)], & \text{if } f \text{ is increasing,} \\
[\mathbf{f}(\mathbf{x})]_n & = & [\underline{f}(\overline{\mathbf{x}}, n), \overline{f}(\underline{\mathbf{x}}, n)], & \text{if } f \text{ is decreasing.}
\end{array}
$$

- If f is neither increasing nor decreasing, e.g., sin and cos, $[\mathbf{f}]_n$ is defined by case analysis on increasing and decreasing ranges.

Extended Inclusion Property

- If $x \in \mathbf{x}$, then $f(x) \in [\mathbf{f}(\mathbf{x})]_n$, for all $n \in \mathbb{N}$.

- We have defined $[\mathbf{f}(\mathbf{x})]_n$ for $f \in \{\text{sin}, \text{cos}, \text{tan}, \pi, \text{atan}, \sqrt{}, \text{exp}, \text{ln}\}$ and formally verified (in PVS) the inclusion property for each interval operation.

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Inclusion Theorem

- Let e be a real expression on variables $x_1, \ldots x_m$, and let $\mathbf{x_1}, \ldots, \mathbf{x_m}$ be interval values such that $x_i \in \mathbf{x_i}$, for $1 \leq i \leq m$, then

$$e(x_1, \ldots, x_m) \in [\mathbf{e}(\mathbf{x_1}, \ldots, \mathbf{x_m})]_n,$$

  where $[e]_n$ is the interval expression corresponding to e.
- *Proof*: Structural induction on e.

César A. Muñoz
munoz@nianet.org

General (Incomplete) Method

- Goal:

$$x_1 \in \mathbf{x_1}, \ldots, x_m \in \mathbf{x_m} \ \vdash \ e(x_1, \ldots, x_m) \ \diamond \ k,$$

  where $\diamond \in \{<, \leq, >, \geq\}$.
- *Proof*:
  1. Derive:

$$x_1 \in \mathbf{x_1}, \ldots, x_m \in \mathbf{x_m} \ \vdash \ e(x_1, \ldots, x_m) \in [\mathbf{e}(\mathbf{x_1}, \ldots, \mathbf{x_m})]_n,$$

     for a given n, using the Inclusion Theorem.
  2. Check by simple calculation:

$$\vdash \ [\mathbf{e}(\mathbf{x_1}, \ldots, \mathbf{x_m})]_n \ \diamond \ k.$$

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Issue 3: Automation

The Sources of Incompleteness:

- Which n ?
- Interval arithmetic is sub-distributive:

$$\mathbf{x} \times (\mathbf{y} + \mathbf{z}) \subseteq \mathbf{x} \times \mathbf{y} + \mathbf{x} \times \mathbf{z}.$$

  Decorrelation effect:
  - $\mathbf{x} - \mathbf{x}$ is not necessarily $\mathbf{0}$,
  - $\mathbf{x} \div \mathbf{x}$ is not necessarily $\mathbf{1}$,
  - $\mathbf{x} \geq 0$ and $\mathbf{x} \leq 0$ may be both false.
- Interval computations yield correct approximations, but not necessarily good ones.

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Solution Issue 3: Pragmatism

- Which n ? A configurable parameter with a default value, e.g., 3 suffices in most of our applications.
- Implementation of rewriting strategies to rearrange and simplify expressions: factorized expressions have fewer decorrelation.

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Interval Splitting

The approximation error of the union of the parts is less than the approximation error of the whole:

Let $\mathbf{x} = \bigcup_{1 \leq i \leq n} \mathbf{x_i}$,

$$\frac{\forall_{1 \leq i \leq n} : \; x \in \mathbf{x_i} \; \vdash \; e(x) \in \mathbf{z}}{x \in \mathbf{x} \; \vdash \; e(x) \in \mathbf{z}}$$

Remark: $\mathbf{z} \subseteq [\mathbf{e}(\mathbf{x})]_n$.

Implementation: An interval $\mathbf{x}$ is evenly split using a user-provided parameter.

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Taylor's Theorem on Intervals

The derivative of $f = \frac{df}{dx}$ has one degree less of decorrelation than f.

$$\frac{a \in \mathbf{x} \; \vdash \; \frac{d^i \; f}{dx^i}(a) \in \mathbf{x}_i, \quad \text{for } 0 \leq i < n, \quad \forall_y : \; y \in \mathbf{x} \; \vdash \; \frac{d^n \; f}{dx^n}(y) \in \mathbf{x}_n}{x \in \mathbf{x} \; \vdash \; f(x) \in \Sigma_{k=0}^{n}(\mathbf{x}_k \times (\mathbf{x} - a)^k)/k!}$$

Remark: $\Sigma_{k=0}^{n}(\mathbf{x}_k \times (\mathbf{x} - a)^k)/k! \subseteq [\mathbf{f}(\mathbf{x})]_n$.

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

Taylor's Implementation

- The element a is the midpoint of $\mathbf{x}$.
- $\mathbf{x_i}$ is the interval expression corresponding to $\frac{d^i\ f}{dx^i}(a)$, for $0 \leq i < n$.
- $\mathbf{x_n}$ is the interval expression corresponding to $\frac{d^n\ f}{dx^n}(y)$.

PVS Implementation Issues

- Representation of rational numbers: PVS built-in reals.
  + No special syntax for real expressions.
  - The Inclusion Theorem has to be discharged for every instance.
- Efficient calculations via computational reflection: Ground rational expressions are evaluated in Lisp.

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

The Interval Package (for PVS)

- Publicly available: `http://research.nianet.org/~munoz/Interval`.
- Several strategies, notably
  - `sharp`, which automatically discharges the Inclusion Theorem.
  - `numerical`, which implements splitting.
  - `taylor`, which implements Taylor's technique.

Statistics

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

- 306 lemmas, 10.000 lines of proofs, 1.000 lines of strategy code.
- These numbers do not include the bounding functions which are part of the NASA PVS Library: `http://shemesh.larc.nasa.gov/fm/ftp/larc/PVS-library/pvsl`

Examples

```
g : posreal = 9.8
v : posreal = 250×0.514

tr35: LEMMA 3×π/180 ≤ g×tan(35×π/180)/v
%|- tr35: PROOF (numerical) QED

G(x|x < 1): real = 3×x/2 - ln(1-x)

A_and_S : lemma
  let x = 0.5828 in
    G(x) > 0
%|- A_and_S : PROOF (numerical :defs "G") QED
```

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

More Examples

```
% A fair approximation:

{-1}  x ## [| 0, 1 |]
  |-------
{1}   x * (1 - x) ## [| 0, 1 |]

Rule? (numerical :vars "x")
Q.E.D.

% A better approximation (via splitting):

{-1}  x ## [| 0, 1 |]
  |-------
{1}   x * (1 - x) ## [| 0, 9 / 32 |]

Rule? (numerical :vars ("x" 16))
Q.E.D.
```

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org

More Examples

```
% The best approximation (via Taylor's technique):

X : var Interval
x : var inInterval([|0,1|])

F(X)   : Interval = X*(1-X)
DF(X)  : Interval = 1 - 2*X
D2F(X) : Interval = [| -2 |]

ftaylor : LEMMA
  x*(1-x) ## Taylor2[[|0,1|]](F,DF,D2F)
%|- ftaylor : PROOF (taylor) QED

best : LEMMA
  x*(1-x) ## [| 0,1/4 |]
%|- best : PROOF (numerical :vars "x"
%|-                         :taylor "ftaylor") QED
```


Final Remarks

- All the results are written and formally verified in PVS.
- Strategies provide a pragmatic approach to real exact arithmetic.
- Applications: Verification of aerospace applications.
- Future work: Fewer decorrelation, higher accuracy, floating point numbers, ...

Real Number Calculations and Interval Analysis in PVS [a]

[a] Based on "Real Number Calculations" (TPHOLs 2005) by C. Muñoz and D. Lester, and "Guaranteed Proofs Using Interval Arithmetic" (ARITH 17) by M. Daumas, G. Melquiond, and C. Muñoz.

César A. Muñoz
munoz@nianet.org