Real Number Calculations and Interval Analysis in PVS[1]

César A. Muñoz

munoz@nianet.org
http://research.nianet.org/~munoz
National Institute of Aerospace

April 15 2004

---

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

Axiom or Lemma

The turn rate of an aircraft flying at 250 knots and with a bank angle of 35^o is given by the formula:

$$3\pi/180 \leq g \tan(35\pi/180)/v,$$

where $g = 9.8$ m/s^2 and $v = 250$ knt $\times$ 0.514.

The Life of an Axiom

$$\begin{aligned} 3\pi/180 &\approx 0.052, \\ g\tan(35\pi/180)/v &\approx 0.053, \quad \text{and} \\ 0.052 &\leq 0.053. \end{aligned}$$

Therefore,

```
g : posreal = 98/10
v : posreal = 250×514/1000
tr(phi) : real = g×tan(phi)/v

tr_35 : axiom
  3×pi/180 ≤ tr(35×pi/180)
```

The Life of an Axiom

$$\begin{aligned} 3\pi/180 &\approx 0.052, \\ g\tan(35\pi/180)/v &\approx 0.053, \quad \text{and} \\ 0.052 &\leq 0.053. \end{aligned}$$

Therefore,

```
g : posreal = 98/10
v : posreal = 250×514/1000
tr(phi) : real = g×tan(phi)/v

tr_35 : axiom
  3×pi/180 ≤ tr(35×pi/180)
```

The Life of a Lemma

```
tr_35 : lemma
  3×pi/180 ≤ tr(35×pi/180)
```

There are no variables! How difficult could this be ?

- Note that tan is increasing, and
- $\pi/6 < 35\pi/180$.
- Moreover, …

The Life of a Lemma

```
tr_35 : lemma
  3×pi/180 ≤ tr(35×pi/180)
```

There are no variables! How difficult could this be ?

- Note that tan is increasing, and
- $\pi/6 < 35\pi/180$.
- Moreover, . . .

First Step Toward Mechanical Proofs

Given $\underline{\pi}, \underline{\pi}, \underline{\tan}, \overline{\tan}$ algebraic functions such that

- $\underline{\pi} < \pi < \overline{\pi}$, and
- $\underline{\tan}(x) \leq \tan(x) \leq \overline{\tan}(x)$.

The goal:

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

could be discharged in a systematic way.

Proof by Approximations

Goal:

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

1. $\vdash 3\pi/180 < 3\overline{\pi}/180$, using `(grind-reals)`.
2. $\vdash 3\overline{\pi}/180 \leq v\underline{\tan}(35\underline{\pi}/180)/g$, using `(grind)`.
3. $\vdash v\underline{\tan}(35\underline{\pi}/180)/g \leq v\tan(35\pi/180)/g$, using `(grind-reals)`.
4. Finish with `(assert)`.

Issues

- What are the requirements for $\underline{f}$ and $\overline{f}$?
- How to define $\underline{f}$ and $\overline{f}$ for transcendental functions ?
- When to use $\underline{f}$ and $\overline{f}$ in a systematic way?
- How to automate those proofs in PVS ?

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

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

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

Sine, Cosine

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

Square Root, . . .

$$
\begin{array}{rcl}
\overline{\mathrm{sqrt}}(x,0) & = & x+1, \\
\overline{\mathrm{sqrt}}(x,n+1) & = & \frac{1}{2}(y+\frac{x}{y}), \quad \text{where } y=\overline{\mathrm{sqrt}}(x,n), \\
\underline{\mathrm{sqrt}}(x,n) & = & \frac{x}{\overline{\mathrm{sqrt}}(x,n)}.
\end{array}
$$

Furthermore: tangent, arctangent, π, exponential, and logarithm.

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

Note that

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

but

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

Indeed,

$$\begin{aligned} k \times f(x) \quad &\leq \quad k \times \overline{\underline{f}}(x, n), \qquad \text{where} \\ \overline{\underline{f}} \quad &= \quad \overline{f} \quad \text{if } k \geq 0, \\ \overline{\underline{f}} \quad &= \quad \underline{f} \quad \text{otherwise.} \end{aligned}$$

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

Note that

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

but

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

Indeed,

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

Undecidability Problem

$$\begin{aligned} \frac{k}{f(x)} &\leq \frac{k}{\overline{\underline{f}}(x, n)}, \quad \text{where} \\ \overline{\underline{f}} &= ?. \end{aligned}$$

Automation is very difficult as it is, in general, impossible to decide $\underline{f}$ *or* $\overline{f}$.

(Rational) Interval Arithmetic

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

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

$$\begin{aligned}
\mathbf{x} + \mathbf{y} &= [\underline{\mathbf{x}} + \underline{\mathbf{y}}, \overline{\mathbf{x}} + \overline{\mathbf{y}}],\\
\mathbf{x} - \mathbf{y} &= [\underline{\mathbf{x}} - \overline{\mathbf{y}}, \overline{\mathbf{x}} - \underline{\mathbf{y}}],\\
\mathbf{x} \times \mathbf{y} &= [\min\{\underline{\mathbf{x}}\underline{\mathbf{y}}, \underline{\mathbf{x}}\overline{\mathbf{y}}, \overline{\mathbf{x}}\underline{\mathbf{y}}, \overline{\mathbf{x}}\overline{\mathbf{y}}\}, \max\{\underline{\mathbf{x}}\underline{\mathbf{y}}, \underline{\mathbf{x}}\overline{\mathbf{y}}, \overline{\mathbf{x}}\underline{\mathbf{y}}, \overline{\mathbf{x}}\overline{\mathbf{y}}\}],\\
\mathbf{x} \div \mathbf{y} &= \mathbf{x} \times [\frac{1}{\overline{\mathbf{y}}}, \frac{1}{\underline{\mathbf{y}}}], \quad \text{if } \underline{\mathbf{y}}\overline{\mathbf{y}} > 0.
\end{aligned}$$

Furthermore, $-\mathbf{x}, |\mathbf{x}|, \mathbf{x}^n, \ldots$.

Inclusion Property

If $x \in \mathbf{x}$ and $y \in \mathbf{y}$ then

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

Other Functions

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

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

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

Inclusion Theorem: If $x \in \mathbf{x}$, then $f(x) \in [\mathbf{f}(\mathbf{x})]_n$.

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.

Issue 4: Implementation in PVS

The strategy `numerical` solves the sequent

$$x_1 \in \mathbf{x_1}, \ldots, x_m \in \mathbf{x_m} \ \vdash \ e_1(x_1, \ldots, x_m) \diamond k$$

as follows:

1. It shows that

   $$x_1 \in \mathbf{x_1}, \ldots, x_m \in \mathbf{x_m} \ \vdash \ e_1(x_1, \ldots, x_m) \in [\mathbf{e}(\mathbf{x_1}, \ldots, \mathbf{x_m})]_n,$$

   for a given n.
2. It shows that

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

Examples

```
  |-------
{1}  3 × pi / 180 ≤ g × tan(35 × pi / 180) / v

Rule? (numerical)
Evaluating formula using numerical approximations,
Q.E.D.



{-1} x ## [| 0, 2 |]
  |-------
{1}  sqrt(x) + sqrt(3) < 315 / 100

Rule? (numerical :vars "x")

Evaluating formula using numerical approximations,
Q.E.D.
```

Ahh ?

```
{-1} x ## [| 1, 2 |]
  |-------
{1}  x / x ≥ 1

Rule? (numerical :vars "x")
Evaluating formula using numerical approximations,
this simplifies to:
foo :

{-1} x / x - 1 ## [| 1, 2 |] / [| 1, 2 |] - [| 1 |]
{-2} x ## [| 1, 2 |]
  |-------
{1}  [| 1, 2 |] / [| 1, 2 |] ≥ [| 1 |]
```

Sub-distributivity

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

In particular,

- $\mathbf{x} - \mathbf{x}$ is not necessarily $\mathbf{0}$,
- $\mathbf{x} \div \mathbf{x}$ is not necessarily $\mathbf{1}$,
- $\mathbf{x} \geq 0$ or $\mathbf{x} \leq 0$ does not necessarily hold.

Decorrelation

Let $\mathbf{x}$ be $[0,1]$,

$$\mathbf{x} \times (1 - \mathbf{x}) \quad = \quad [0,1].$$

However,

$$\forall x \in \mathbf{x}: \; x(1-x) \in [0, \frac{1}{4}].$$

Remark: $[0,1]$ *is correct but not a very good approximation.*

Interval Splitting

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

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

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

Example

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

Rule? (numerical :vars ("x" 16))
Evaluating formula using numerical approximations,
Q.E.D.

Run time = 22.82 secs.
```

Remark: The interval splitting technique is exponential with respect to number of interval variables.

Taylor's Theorem

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

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

Example

```
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 (instint :taylor "ftaylor") QED
```

So What?

`http://research.nianet.org/~munoz/Interval`

- A sound pocket calculator.
- A library for interval analysis.
- A library for exact arithmetic (not yet!).
- Floating point verification (not yet!)