Guaranteed Proofs Using Interval Arithmetic

Marc Daumas, Guillaume Melquiond, César Muñoz

Arénaire, LIP, ENS Lyon
National Institute of Aerospace

June 28th 2005

Proving mathematical inequalities

- A plane flying at 250 knots and with a bank angle of 35° has a turn rate of at least 3° each second:

$$\frac{3\pi}{180} \leq \frac{g}{v} \tan\left(\frac{35\pi}{180}\right),$$

where $g = 9.8 m/s^2$ and $v = 250 \frac{514}{1000} m/s$.

Proving mathematical inequalities

- A plane flying at 250 knots and with a bank angle of 35° has a turn rate of at least 3° each second:

$$\frac{3\pi}{180} \leq \frac{g}{v} \tan\left(\frac{35\pi}{180}\right),$$

where $g = 9.8 m/s^2$ and $v = 250 \frac{514}{1000} m/s$.

- This inequality is trivially true:

$$\frac{3\pi}{180} \approx 0.052 \quad \text{and} \quad \frac{g}{v}\tan(\frac{35\pi}{180}) \approx 0.053.$$

But how to prove it formally yet simply?

Proving mathematical inequalities

- Let $\underline{\pi}$ and $\overline{\pi}$ be two rational approximations of π such that $\underline{\pi} \leq \pi \leq \overline{\pi}$. Since tan is monotonous on $[0, \frac{\pi}{2}[$, the inequality is implied by $\frac{3\overline{\pi}}{180} \leq \frac{g}{v} \tan(\frac{35\underline{\pi}}{180})$.
- Let $\underline{\tan}$ be a closed rational function $\mathbb{Q} \to \mathbb{Q}$ such that $\underline{\tan}(x) \leq \tan(x)$. The inequality is then implied by $\frac{3\overline{\pi}}{180} \leq \frac{g}{v} \underline{\tan}(\frac{35\underline{\pi}}{180})$.

Proving mathematical inequalities

- Let $\underline{\pi}$ and $\overline{\pi}$ be two rational approximations of π such that $\underline{\pi} \leq \pi \leq \overline{\pi}$. Since tan is monotonous on $[0, \frac{\pi}{2}[$, the inequality is implied by $\frac{3\overline{\pi}}{180} \leq \frac{g}{v} \tan(\frac{35\underline{\pi}}{180})$.
- Let $\underline{\tan}$ be a closed rational function $\mathbb{Q} \to \mathbb{Q}$ such that $\underline{\tan}(x) \leq \tan(x)$. The inequality is then implied by $\frac{3\overline{\pi}}{180} \leq \frac{g}{v}\underline{\tan}(\frac{35\underline{\pi}}{180})$.
- Both members of this new inequality can be computed exactly through rational arithmetic and then compared. It can be done formally and automatically.

Plan

Rational interval arithmetic

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

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

Rational interval arithmetic

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

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

- Arithmetic operators:
  - $\mathbf{x} + \mathbf{y} = [\underline{x} + \underline{y}, \overline{x} + \overline{y}]$,
  - $\mathbf{x} - \mathbf{y} = [\underline{x} - \overline{y}, \overline{x} - \underline{y}]$,
  - $\mathbf{x} \times \mathbf{y} = [\mathrm{min}\{\underline{x}\underline{y}, \underline{x}\overline{y}, \overline{x}\underline{y}, \overline{x}\overline{y}\}, \mathrm{max}\{\underline{x}\underline{y}, \underline{x}\overline{y}, \overline{x}\underline{y}, \overline{x}\overline{y}\}]$,
  - $\mathbf{x} \div \mathbf{y} = \mathbf{x} \times [\frac{1}{\overline{y}}, \frac{1}{\underline{y}}]$, if $\underline{y}\overline{y} > 0$.

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

Containment property and proofs

- If $x \in \mathbf{x}$ and $y \in \mathbf{y}$ then
  - $x \diamond y \in \mathbf{x} \diamond \mathbf{y}$, where $\diamond \in \{+, -, \times, \div\}$,
  - $-x \in -\mathbf{x}$,
  - $|x| \in |\mathbf{x}|$,
  - $x^n \in \mathbf{x}^n$.

Containment property and proofs

- If $x \in \mathbf{x}$ and $y \in \mathbf{y}$ then
  - $x \diamond y \in \mathbf{x} \diamond \mathbf{y}$, where $\diamond \in \{+, -, \times, \div\}$,
  - $-x \in -\mathbf{x}$,
  - $|x| \in |\mathbf{x}|$,
  - $x^n \in \mathbf{x}^n$.

- 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

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

  where $\mathbf{e}$ is the interval expression corresponding to e.

Containment property and proofs

- If $x \in \mathbf{x}$ and $y \in \mathbf{y}$ then
  - $x \diamond y \in \mathbf{x} \diamond \mathbf{y}$, where $\diamond \in \{+, -, \times, \div\}$,
  - $-x \in -\mathbf{x}$,
  - $|x| \in |\mathbf{x}|$,
  - $x^n \in \mathbf{x}^n$.
- 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

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

  where $\mathbf{e}$ is the interval expression corresponding to e.

Thanks to the containment property, intervals can be used as proofs of inequalities. Because the bounds are exact rational numbers, a proof assistant easily computes them and it can automatically generate the related proofs.

Bounding algebraic and transcendental functions

Special functions are bounded by parametric functions $\mathbb{Q} \times \mathbb{N} \to \mathbb{Q}$.

- Sine:
  - $\underline{\sin}(x, n) = \sum_{i=1}^{2n} (-1)^{i-1} \frac{x^{2i-1}}{(2i-1)!}$
  - $\overline{\sin}(x, n) = \sum_{i=1}^{2n+1} (-1)^{i-1} \frac{x^{2i-1}}{(2i-1)!}$
- Square root:
  - $\overline{\text{sqrt}}(x, 0) = x + 1$
  - $\overline{\text{sqrt}}(x, n+1) = \frac{1}{2}(y + \frac{x}{y})$, where $y = \overline{\text{sqrt}}(x, n)$
  - $\underline{\text{sqrt}}(x, n) = \frac{x}{\overline{\text{sqrt}}(x,n)}$
- Furthermore, cos, atan, exp, log, ...

Once again, proof generation amounts to doing exact computations on rational numbers.

Proofs by approximation

- The National Institute of Aerospace and NASA Langley intend to prove the safety of algorithms for airplane collision avoidance. They do not use numerical tools to this end.
- What is wrong with numerical tools?

Proofs by approximation

- The National Institute of Aerospace and NASA Langley intend to prove the safety of algorithms for airplane collision avoidance. They do not use numerical tools to this end.
- What is wrong with numerical tools?
  Nothing. But they do not provide enough formal guarantees when verifying safety critical systems:

```
> 3 * Pi / 180 <= 9.8 * tan(35 * Pi / 180) / (250 * 0.514);
```

$$\frac{1}{60}\pi \leq 0.07626459144 \tan\left(\frac{7}{36}\pi\right)$$

```
> evalf(%); evalb(%);
```

$$0.05235987758 \leq 0.05340104182$$

true

(Maple 9.5)

Numerical proofs in PVS

Instead of numerical tools, NIA and NASA use PVS, a proof assistant. `http://pvs.csl.sri.com/`

Proofs are constructed by applying strategies to transform the hypotheses and goals of theorems until they match each other. For proofs by approximation, the assistant will formally guarantee the correctness of the computations.

Numerical proofs in PVS

Instead of numerical tools, NIA and NASA use PVS, a proof assistant. `http://pvs.csl.sri.com/`

Proofs are constructed by applying strategies to transform the hypotheses and goals of theorems until they match each other. For proofs by approximation, the assistant will formally guarantee the correctness of the computations.

Our strategy `numerical` does a proof by approximation: it applies interval arithmetic theorems to certify an inequality. The proof assistant will formally guarantee the correctness of the computations.

Examples of PVS and the `numerical` strategy

```
  |-------
{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.
```

Intervals and decorrelation

- Let $\mathbf{x}$ be $[0, 1]$,
$$\mathbf{x} \times (1 - \mathbf{x}) = [0, 1].$$
However,
$$\forall x \in \mathbf{x} : \; x \cdot (1 - x) \in [0, \tfrac{1}{4}].$$
- The multiple occurrences of an interval are not correlated, hence an overestimation of the final result.
- In particular, if $\mathbf{x}$ is not a singleton,
  - $\mathbf{x} - \mathbf{x} \neq \mathbf{0}$,
  - $\mathbf{x} \div \mathbf{x} \neq \mathbf{1}$.

Splitting and Taylor's series

Two additional theorems are used to avoid decorrelation.

- Interval splitting: let $\mathbf{x} = \bigcup_{1 \le i \le n} \mathbf{x_i}$,

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

Splitting and Taylor's series

Two additional theorems are used to avoid decorrelation.

- Interval splitting: let $\mathbf{x} = \bigcup_{1 \le i \le n} \mathbf{x_i}$,

$$\frac{\forall\, 1 \le i \le n:\;\; x \in \mathbf{x_i} \;\vdash\; e(x) \in \mathbf{y}}{x \in \mathbf{x} \;\vdash\; e(x) \in \mathbf{y}}$$

- Taylor's series expansion: if f is n-times differentiable over $\mathbf{x}$,

$$\frac{\begin{array}{c}\forall\, 1 \le i \le n:\;\; a \in \mathbf{x} \;\vdash\; \frac{d^i f}{dx^i}(a) \in \mathbf{y}_i \\ \forall t:\;\; t \in \mathbf{x} \;\vdash\; \frac{d^n f}{dx^n}(t) \in \mathbf{y}_n\end{array}}{x \in \mathbf{x} \;\vdash\; f(x) \in \Sigma_{i=0}^{n}(\mathbf{y}_k \times (\mathbf{x} - a)^i)/i!}$$

An oracle in the form of an auxiliary library

- The speed of PVS is not suitable to search for the approximation order of the elementary functions, the interval splitting, nor the Taylor's expansion order.
- A C++ library providing the same numerical facilities has been implemented. Since it only computes intervals instead of trying to create proofs, it is faster than PVS.
- This library is intended to be used to compute beforehand a set of parameters that will guide PVS to the end of the proof.

Example: bounding a truncation error

- An algorithm relying on the function $r(\phi)$ uses a polynomial approximation $\hat{r}(\phi)$ on $[0, \phi_m]$ with $\phi_m = \frac{715}{512}$

$$
\begin{aligned}
r(\phi) &= \frac{a}{1 + (1-f)^2 \tan^2 \phi} \\
\hat{r}(\phi) &= \frac{4439091}{4} + t \times \left(\frac{9023647}{4} + t \times \ldots \right)
\end{aligned}
$$

$$\text{with } t = \phi_m^2 - \phi^2$$

- In order for the algorithm to be certified, the relative error $\frac{e(\phi)}{r(\phi)} = \frac{r(\phi) - \hat{r}(\phi)}{r(\phi)}$ has to be bounded by 1.36×10^{-7} for any ϕ.

Example: bounding a truncation error

- Sufficient parameters for the proof are:
  - tan approximated to the 4th term, sqrt to the 7th,
  - Taylor's series for $e(\phi)$ expanded to the first order,
  - $[0, \phi_m]$ split into 9935 intervals.
- The final property of the PVS development reads:

```
PHI : Interval = [|0,715/512|]

RI : THEOREM
  ∀ (phi:real) :
    phi ## PHI IMPLIES
    e(phi) / r(phi) ## [|-136/1000000000,136/1000000000|]
```

Conclusion

- Interval arithmetic can be used as a formal foundation for proofs by approximation. Our implementation as a PVS library provides a high level of confidence.

Conclusion

- Interval arithmetic can be used as a formal foundation for proofs by approximation. Our implementation as a PVS library provides a high level of confidence.
- All the PVS strategies are automated. So formally proving a numerical property requires minimal interaction with the proof assistant.

Conclusion

- Interval arithmetic can be used as a formal foundation for proofs by approximation. Our implementation as a PVS library provides a high level of confidence.
- All the PVS strategies are automated. So formally proving a numerical property requires minimal interaction with the proof assistant.
- Interval splitting and Taylor's expansions are not as efficient as Sturm's chains or quantifier elimination, but they apply to a lot more than just polynomials.

Questions?

- E-mail addresses:
  - marc.daumas@ens-lyon.fr
  - guillaume.melquiond@ens-lyon.fr
  - munoz@nianet.org
- PVS library available at
  http://research.nianet.org/~munoz/Interval/