A library of Taylor Models for PVS automatic proof checker

Francisco José Cháves and **Marc Daumas**

LIP Computer Science Laboratory

UMR 5668 CNRS - ENS Lyon - INRIA

email: Francisco.Jose.Chaves.Alonso@ENS-Lyon.fr

LP2A Laboratory

EA 3679 UPVD

email: Marc.Daumas@Univ-Perp.fr

Outline

- Introduction
  - Prior art
  - Interval arithmetic
  - Taylor theorem
- Taylor models
- A toy example
- Conclusions

Introduction

- Software failures occur repeatedly
  - Patriot missile defense system
  - Ariane 501 flight destruction
  - Panama ION overdose of radiation
- Formal methods are a way to certify software
  - Developments require expertise
  - We lack more user-friendly interfaces

Prior art

- Invisible formal methods by Tiwary, Shankar and Rushby
- Guaranteed Proofs Using Interval Arithmetic by Daumas, Melquiond and Muñoz. http://research.nianet.org/ munoz/Interval/
  - Interval splitting
  - Taylor's series expansions

PVS ...

Prototype Verification System is a specification language integrated with support tools and a theorem prover.

- The specification language is based on classical, typed higher-order logic.
- The theorem prover provides a collection of proof commands (rules and strategies) within a sequent calculus framework
- http://pvs.csl.sri.com
  http://shemesh.larc.nasa.gov/fm/fm-pvs.html

Interval arithmetic

An interval I is a pair $[a, b]$ that represents the set $\{x | a \leq x \leq b\}$ with the following operations:

- $[a, b] + [a', b'] = [a + a', b + b']$,
- $[a, b] - [a', b'] = [a - b', b - a']$,
- $c \cdot [a, b] = [c \cdot a, c \cdot b]$ for $c \geq 0$,
- $[a, b] \cdot [a', b'] =$
  $[\min\{aa', ab', ba', bb'\}, \max\{aa', ab', ba', bb'\}]$,
- and many more (see for example the PVS library)

Interval arithmetic

Working with automatic proof checkers, we convert operations into properties, $x \in [a, b]$, $y \in [a', b']$ and $c \in \mathbb{R}$:

- $x + y \in [a, b] + [a', b']$,
- $x - y \in [a, b] - [a', b']$,
- $c \cdot x \in c \cdot [a, b]$,
- $x \cdot y \in [a, b] \cdot [a', b']$.

Applications

Interval Arithmetic as well as Taylor models can be used for

- Self validation of arithmetic properties
  - Optimization.
  - Solution of systems of equations.
  - Parameter estimation.
  - . . . (see for examples the book by Jaulin et al.)
- Bounds on round-off errors
  - Forward error analysis

Decorrelation . . .

. . . is a problem intrinsic to interval arithmetic.

$$x - x \in [0, 0] \text{ with } x \in [0, 1]$$

is computed as

$$[0, 1] - [0, 1] = [-1, 1]$$

Taylor theorem has been used by Daumas et al. to reduce decorrelation, associated with a theorem prover (automation recently added).

An example about decorrelation . . .

Assuming you know what Taylor models are,

$$\sin x - x \text{ with } x \in [-1/10, 1/10]$$

is replaced using Taylor models of degree 3 by

$$\frac{x^3}{3!} + r \qquad r \in [-1/12000000, 1/12000000]$$

Taylor theorem (real)

Let f be (n+1) times continuously derivable between x_0 and x,

$$f(x) = f(x_0) + (x - x_0)f'(x_0) + \frac{(x - x_0)^2}{2!}f''(x_0) + \cdots + \frac{(x - x_0)^n}{n!}f^{(n)}(x_0) + \frac{(x - x_0)^{n+1}}{(n+1)!}f^{(n+1)}(x_0 + (x - x_0)\theta)$$

where $0 < \theta < 1$

Taylor theorem (interval)

Let f be (n+1) times continuously derivable in the interior of I,

$$f(x) \in f(x_0) + (I - x_0)f'(x_0) + \frac{(I - x_0)^2}{2!}f''(x_0) + \cdots + \frac{(I - x_0)^n}{n!}f^{(n)}(x_0) + \frac{(I - x_0)^{n+1}}{(n+1)!}f^{(n+1)}(I)$$

where $x \in I, x_0 \in I$

Outline

- Introduction
  - Prior art
  - Interval arithmetic
  - Taylor theorem
- Taylor models
- A toy example
- Conclusions

Key theories required

To develop Taylor models we have introduced a theory of finite support series and we have extended the theory of polynomials of NASA LaRC.

Taylor models

Taylor models have been introduced by Lanford, developed by Eckmann, Koch and Wittwer. They have been used by Makino, Berz et al, to reduce decorrelation.
A Taylor model is a pair (p, I) associated to each function A such that $A = p(x) + r$, $r \in I$.

- $p(x)$ polynomial part with fixed degree N,
- $x \in J$ usually fixed to $[0, 1]$ or $[-1, 1]$
- $r \in I$ interval part

Properties of Taylor models

- Reduce decorrelation
- Integration is an operation native to Taylor models and can be applied to solve ODEs
- $\sin$, $\cos$, $\exp$ and any analytic function is easily handled with Taylor models.
- No need to develop explicitly the derivative of the function to be studied.

Addition of Taylor models

Let $A = p(x) + r$ and $B = q(x) + s$, $r \in I$, $s \in I'$ be Taylor models, the addition

$$\begin{aligned} & A + B \\ =& p(x) + q(x) + r + s \end{aligned}$$

has the associated Taylor model

$(p(x) + q(x), I + I')$.

Multiplication of Taylor models (1/2)

Let $A = p(x) + r$ an $B = q(x) + s$, $r \in I$, $s \in I'$ be Taylor models, the multiplication

$$
\begin{aligned}
& A \cdot B \\
=& (p(x) + r)(q(x) + s) \\
=& p(x)q(x) + p(x) \cdot s + q(x) \cdot r + r \cdot s
\end{aligned}
$$

almost has the associated Taylor model $(p(x) \cdot q(x), p(J) \cdot I' + q(J) \cdot I + I \cdot I')$

where $x \in J$

Multiplication . . . (truncated) (2/2)

Let $A = p(x) + r$ and $B = q(x) + s$, $r \in I$, $s \in I'$ be Taylor models, and $t = \text{trunc}(p \cdot q, N)$ the multiplication

$$A \cdot B$$

$$= t(x) + (p \cdot q - t)(x) + p(x) \cdot s + q(x) \cdot r + r \cdot s$$

has the associated Taylor model

$$(t(x), (pq - t)(J) + p(J) \cdot I' + q(J) \cdot I + I \cdot I').$$

Inverse

Let $A = p(x) + r$, $r \in I$ be a Taylor model, $q(x) = 1 - \frac{p(x)}{p(0)}$, $t = \text{trunc}(\sum_{i=0}^{N} q^i, N)$, we use the series:

$$\sum_{i=0}^{N} x^i = \frac{1 - x^{N+1}}{1 - x}$$

and the equality:

$$\frac{1}{p(x) + r} = \frac{1}{p(0)} \cdot \frac{p(x)}{p(x) + r} \cdot \frac{1}{1 - \left(1 - \frac{p(x)}{p(0)}\right)}$$

Inverse

To bound the second term, we define the new operator

$$I' = [\frac{1}{1 + \frac{1}{(I/p(J))}}, \frac{1}{1 + \frac{1}{(I/p(J))}}]$$

We cannot use directly

$$\frac{1}{1 + p(J)/I} \text{ nor } \frac{1}{1 + \frac{1}{I/p(J)}}$$

because I can contain 0.

Inverse

$1/A$ has the associated Taylor model

$$\left(\frac{1}{p(0)}t, \frac{1}{p(0)}\left(\sum_{i=0}^{N} q^i - t\right)(J) + \right.$$
$$\left.\frac{1}{p(0)}\left(\frac{q(J)^{N+1}}{1-q(J)} \cdot (1-I') - \left(\sum_{i=0}^{N} q^i(J)\right) \cdot I'\right)\right)$$

Exponential

Let $A = p(x) + r$, $r \in I$ be a Taylor model,

- $q(x) = p(x) - p(0)$,
- $t = \text{trunc}(\sum_{i=0}^{N} \frac{q^i}{i!}, N)$,
- $e_0 = \sum_{i=0}^{N_e} \frac{p(0)^i}{i!}$,
- N_e the order of approximation of exponential
- Exp(e, N_e) a function that bounds $\exp(e)$ in an interval using an approximation of order N_e.

The Taylor model of $\exp(A)$ is:

Exponential

$$
\begin{aligned}
&(e_0 \cdot t, \\
&\quad \left(\sum_{i=0}^{N} \frac{q^i(x)}{i!} - t \right)(J) \\
&\quad + e_0 \cdot ([1] \cup \mathsf{Exp}(q(0), N_e)) \cdot \frac{q(J)^{N+1}}{(N+1)!} \\
&\quad + (\mathsf{Exp}(p(0), N_e) - e_0) \cdot \mathsf{Exp}(q(J), N_e) \\
&\quad + \mathsf{Exp}(p(J), N_e) \cdot (\mathsf{Exp}(I, N_e) - 1))
\end{aligned}
$$

Containment property

Going from evaluation to theorems

$$\text{containment}(f, t) =$$
$$\forall x \in J. f(x) - t`P(x) \in t`I$$

We have proved that each operation preserves the containment property.
taylor_model.pvs and tm_exp.pvs files available from http://perso.ens-lyon.fr/francisco.jose.chaves.alonso/pvs-fi les/

Toy example

In addition to prove mathematical theories PVS can animate them using the PVS *ground evaluator*.

- An experimental feature of PVS 3.x
- Extracts Common Lisp code from PVS functional specifications and evaluates them.
- PVSio an alternative interface to the ground evaluator available from

  http://research.nianet.org/~munoz/PVSio

Toy example $ch\left(2 \cdot \frac{x}{1000}\right) \cdot sh\left(3 \cdot \frac{x}{1000}\right)$

example: THEORY
BEGIN
IMPORTING tm_exp$[5, 5, (\#\text{lb} := -1, \text{ub} := 1\#)]$
ch(x: tm): tm = $(1/2) \times (\exp(x) + \exp(-x))$
sh(x: tm): tm = $(1/2) \times (\exp(x) + -\exp(-x))$
seq_px: fs_type =
λ (n: nat): IF $n = 1$ THEN $1/1000$
ELSE 0 ENDIF
tm_x: tm = ($\#P$:= seq_px, I := $[\![0]\!]\#$)
example1: tm = ch($2 \times$ tm_x) $\times$ sh($3 \times$ tm_x)
END example

Toy example

```
<PVSio> example1‘P(0);
==>
0
<PVSio> example1‘P(1);
==>
3/1000
<PVSio> example1‘P(2);
==>
0
<PVSio> example1‘P(3);
==>
21/2000000000
...
```

Toy example

```
<PVSio> example1‘I;
==>
(# lb := -19966660037929209080778095595964694170499249884356754248912582792777246825769541627979310535210358464 7/
38763496047478702331322336437004695773022456032565137272401306723242233956386636433666858122000000000000000000000000,
ub := 19966660037929209080778095595964694170499249884356754248912582792777246825769541627979310535210358464 7/
38763496047478702331322336437004695773022456032565137272401306723242233956386636433666858122000000000000000000000000 #)
```

Toy example

The Taylor model of degree 5 of

$$ch\left(2 \cdot \frac{x}{1000}\right) \cdot sh\left(3 \cdot \frac{x}{1000}\right)$$
$$= 3 \cdot \frac{x}{1000} + \frac{21}{2} \cdot \left(\frac{x}{1000}\right)^3 + \frac{521}{40} \cdot \left(\frac{x}{1000}\right)^5 + r$$

with

$$r \in 5150892483 \cdot 10^{-28} \cdot [-1, 1]$$

Conclusions

- We have developed a theory for Taylor models in PVS with the operations of addition, negation, multiplication by scalar, multiplication, inverse and exponential.
  Work in progress (sqrt, atan, . . .)
  Work to do (strategies similar to the ones for interval arithmetic)
- We have developed a theory of finite support series and extended the theory of polynomials compatible with the PVS series of NASA LaRC.

Thank you for your attention

http://perso.ens-lyon.fr/francisco.jose.chaves.alonso/
fjchaves@ens-lyon.fr

http://perso.ens-lyon.fr/marc.daumas/
Marc.Daumas@LIRMM.fr
Marc.Daumas@Univ-Perp.fr

Finite support theory

Let $a : \mathbb{N} \to \mathbb{R}$ be a sequence, a has finite support N if

$$\forall n : n > N \Rightarrow a(n) = 0$$

$$\text{finite\_support}(a, N) \Rightarrow \text{finite\_support}(-a, N)$$

$$\text{finite\_support}(a, N) \wedge \text{finite\_support}(b, M) \wedge L \geq \max(N, M) \Rightarrow \text{finite\_support}(a + b, L)$$

$$\ldots$$

More interesting lemmas

We have proved the convergence of a series with finite support:

$$\text{finite\_support}(a, N)$$
$$\Rightarrow \text{convergence}(\text{series}(a), \text{series}(a)(N))$$

A great lemma

We have independently proved the correctness of Cauchy product for series with finite support:

$$\text{finite\_support}(a, N) \wedge \text{finite\_support}(b, M)$$

$$\Rightarrow \left(\sum_{k=0}^{N} a_k\right) \cdot \left(\sum_{k=0}^{M} b_k\right) = \sum_{n=0}^{N+M} \sum_{k=0}^{n} a_k \cdot b_{n-k}$$

Polynomials in PVS

We have demonstrated that the polynomials are power series of finite support sequences:

polynomial$(a, N)(x)$: real $=$ powerseries$(a)(x)(N)$

Multiplication and Power

$$\text{finite\_support}(a, N) \wedge \text{finite\_support}(b, M)$$
$$\Rightarrow \text{polynomial}(a, N)(x) * \text{polynomial}(b, M)(x)$$
$$= \text{polynomial}(\text{cauchy}(a, b), N + M)(x)$$

$$\text{finite\_support}(a, N)$$
$$\Rightarrow \text{polynomial}(a, N)(x)^n =$$
$$\text{polynomial}(\text{pow}(a, n), n * N)(x)$$

Composition of polynomials

We define the composition of polynomials:

```
comp(a : sequence[real], b : sequence[real], d : nat )
  : RECURSIVE sequence[real] =
  IF d = 0 THEN
    (LAMBDA n : IF n = 0 THEN a(0) ELSE 0 ENDIF)
  ELSE
    LET c = (LAMBDA n : IF n = d THEN 0 ELSE a(n) ENDIF)
    IN a(d) * pow(b, d) + comp(c, b, d-1)
  ENDIF
MEASURE d
```

Composition of polynomials

And we prove composition is correct

$$\begin{aligned} &\text{finite\_support}(a, N) \wedge \text{finite\_support}(b, M) \\ \Rightarrow\ &\text{polynomial}(a, N)(\text{polynomial}(b, M)(x)) = \\ &\text{polynomial}(\text{comp}(a, b, N), N * M)(x) \end{aligned}$$