Utilisation et certification de l'arithmétique des modèles de Taylor dans un assistant de preuves

Francisco Cháves

Sous la direction de Marc Daumas et Nathalie Revol
Laboratoire de l'Informatique du Parallélisme
Arénaire - LIP - UMR 5668 CNRS - ENS Lyon - INRIA - UCBL

28-9-2007

Motivation

- Des erreurs logicielles ont entraîné
  - la destruction du premier vol d'Ariane 5 ;
  - la défaillance du système de défense anti-missile Patriot ;
  - les surdoses de radiation au Panama ION.

- Les méthodes formelles permettent de certifier les logiciels, mais ...
  - il faut une connaissance poussée des méthodes formelles ;
  - les interfaces manquent de convivialité.

Méthodes formelles invisibles

- Méthodes formelles invisibles de Tiwari, Shankar et Rushby.
  - outils d'analyse formelle : model checkers, assistants de preuves, ...
  - invisibles : l'interaction avec l'utilisateur est cachée ou réduite.

- Preuves vérifiées par ordinateur basées sur l'arithmétique d'intervalles, de Muñoz et al. :
  - calcul numérique fiable : arithmétique d'intervalles ;
  - preuves vérifiées par ordinateur : assistant de preuves.

PVS . . .

Prototype Verification System est un langage de spécification, avec des outils de développement et un assistant de preuves intégrés :

- le langage de spécification est basé sur la logique classique typée d'ordre supérieur ;
- l'assistant de preuves offre un ensemble de commandes de preuve (règles et stratégies) dans le cadre du calcul de séquents.

PVS le langage . . .

example1: THEORY
BEGIN

x, y, z, w: VAR real

associative_mult: AXIOM
$x \times (y \times z) = (x \times y) \times z$

foo: LEMMA
$x \times y \times (z \times w) =$
$x \times (y \times z) \times w$

END example1

PVS assistant de preuves

```
foo :
|-----
{1} FORALL (w, x, y, z : real) : x * y * (z * w)
= x * (y * z) * w
Rule?
```

PVS assistant de preuves

```
foo :
|-----
{1} FORALL (w, x, y, z : real) : x * y * (z * w)
= x * (y * z) * w
Rule?(skolem! )
```

```
this simplifies to :
foo :
|-----
{1} x!1 * y!1 * (z!1 * w!1) = x!1 * (y!1 * z!1)
* w!1
Rule?
```

PVS assistant de preuves

```
foo :
|-----
{1} FORALL (w, x, y, z : real) : x * y * (z * w)
= x * (y * z) * w
Rule?(skolem! )
```

```
this simplifies to :
foo :
|-----
{1} x!1 * y!1 * (z!1 * w!1) = x!1 * (y!1 * z!1)
* w!1
Rule? (rewrite "associative_mult")
```

```
Rewriting using associative_mult, matching in *,
Q.E.D.
```

Introduction à l'arithmétique d'intervalles

Un intervalle I est un couple $[a, b]$ qui représente l'ensemble $\{x | a \leq x \leq b\}$.
On définit les opérations suivantes :

- $[a, b] + [a', b'] = [a + a', b + b']$,
- $[a, b] - [a', b'] = [a - b', b - a']$,
- $c \cdot [a, b] = [c \cdot a, c \cdot b]$ si $c \geq 0$,
- $[a, b] \cdot [a', b'] = [\min\{aa', ab', ba', bb'\}, \max\{aa', ab', ba', bb'\}]$,
- etc.

Propriétés

Lorsque l'on travaille avec un assistant de preuves, on associe des propriétés aux opérations.
Pour $x \in [a, b]$, $y \in [a', b']$ et $c \in \mathbb{R}$:

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

Ces propriétés ont été vérifiées en PVS par Muñoz et al.

Décorrélation des variables . . .

. . . c'est un problème inhérent à l'arithmétique d'intervalles.

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

s'évalue en arithmétique d'intervalles

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

Le théorème de Taylor-Lagrange a été utilisé pour remédier à ce problème par :

- Berz & Makino dans COSY ;
- Nedialkov dans VNODE ;
- Muñoz et al., en association avec un assistant de preuves ;
- Zumkeller en Coq ;
- . . .

Rappel : théorème de Taylor

Soit f une fonction $(n+1)$ fois continûment dérivable entre x_0 et x,

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

où $\xi \in [x_0, x]$.

Rappel : théorème de Taylor

Soit f une fonction $(n+1)$ fois continûment dérivable entre x_0 et x,

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

où $\xi \in [x_0, x]$.

Soit f une fonction $(n+1)$ fois continûment dérivable à l'intérieur de I,

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

où $x \in I, x_0 \in I$.

Exemple : réduction de la décorrélation . . .

En supposant que les modèles de Taylor aient déjà été définis,

$$\sin x - x \quad \text{avec} \quad x \in \left[-\frac{1}{10}, \frac{1}{10}\right]$$

peut être représenté par le modèle de Taylor d'ordre 3

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

Plan de l'exposé

Modèles de Taylor

Les modèles de Taylor ont été définis par Lanford (1980), développés par Eckmann, Koch et Wittwer (1984) et popularisés par Berz et Makino à partir de 1990.

Une fonction f est représentée par un couple (p, I), appelé modèle de Taylor de f d'ordre N, tel que $f(x) = p(x) + r$, $r \in I$.

- $p(x)$ partie polynomiale de degré fixé N,
- $x \in J$, le plus souvent $J = [0, 1]$ ou $J = [-1, 1]$,
- $r \in I$ le reste intervalle.

Propriétés des modèles de Taylor

- Réduction de la décorrélation des variables ;
- intégration : opération naturelle sur les modèles de Taylor que l'on peut utiliser pour la résolution d'EDO ;
- facilité de traitement des fonctions sin, cos, exp et des fonctions analytiques en général ;
- construction incrémentale des dérivées par opérations et composition : inutile de calculer explicitement les dérivées.

Addition de deux modèles de Taylor

Soient $A = (p(x), I)$ et $B = (q(x), I')$, $r \in I$, $s \in I'$ des modèles de Taylor pour f et g, la somme

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

a pour modèle de Taylor associé
$(p(x) + q(x), I + I')$.

Multiplication de deux modèles de Taylor (1/2)

Soient $A = (p(x), I)$ et $B = (q(x), I')$, $r \in I$, $s \in I'$ des modèles de Taylor d'ordre N pour f et g, le produit

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

pourrait avoir pour modèle de Taylor
$(p(x) \cdot q(x), p(J) \cdot I' + q(J) \cdot I + I \cdot I')$
où $x \in J$.

Multiplication . . . (tronquée) (2/2)

Soient $A = (p(x), I)$ et $B = (q(x), I')$, $r \in I$, $s \in I'$ des modèles de Taylor d'ordre N pour f et g, et soit $t = \text{trunc}(p \cdot q, N)$, le produit

$$\begin{aligned} & f(x) \cdot g(x) \\ =& t(x) + (p \cdot q - t)(x) + p(x) \cdot s + q(x) \cdot r + r \cdot s \end{aligned}$$

a pour modèle de Taylor d'ordre N
$(t(x), (pq - t)(J) + p(J) \cdot I' + q(J) \cdot I + I \cdot I')$.

Exponentielle

Soit f une fonction représentée par le modèle de Taylor $(p(x), I)$, $r \in I$

$$\exp(f(x)) = \exp(p(x)) \cdot \exp(r)$$
$$= \exp(p(x)) + \exp(p(x)) \cdot (\exp(r) - 1)$$

$$\exp(p(0)) \cdot \exp(p(x) - p(0))$$

(intervalle)

approximation
+ erreur (intervalle)

$$\sum_{i=0}^{N} \frac{1}{i!}(p(x) - p(0))^i + \sum_{i=N+1}^{\infty} \frac{1}{i!}(p(x) - p(0))^i$$

partie polynomiale tronquée
+ reste de la troncature (intervalle)

reste de Lagrange (intervalle)

Arc-tangente

On rencontre un problème de décorrélation des variables pour le reste de Lagrange de atan, dû principalement au terme $\frac{f^{(N+1)}(x)}{(N+1)!}$.

$$\text{atan}^{(5)}(x) = \frac{384x^4}{(1+x^2)^5} - \frac{282x^2}{(1+x^2)^4} + \frac{24}{(1+x^2)^3}$$

$$\frac{\text{atan}^{(5)}([-1,1])}{5!} = \left[\frac{-19}{8}, \frac{17}{5}\right] \backsimeq [-2.375, 3.4]$$

Le reste est $\backsimeq [-0.079102, 0.2]$.

Avec des degrés plus élevés, le problème s'amplifie.

Séries alternées

Une série alternée est une série réelle dont les termes décroissant vers 0 en valeur absolue sont alternativement positifs et négatifs.

Théorème

Soit (a_n) *une suite positive* $(\forall(n : \mathbb{N}).\ a_n > 0)$, *décroissante* $(a_{n+1} <= a_n)$ *qui converge vers* 0. *Alors la série alternée* $\sum (-1)^n a_n$ *converge, et le reste partiel*

$$R_n = \sum_{k=n+1}^{+\infty} (-1)^k a_k \quad \textit{vérifie} \quad |R_n| \leq a_{n+1} \textit{ pour tout } n \in \mathbb{N}.$$

Nous avons implanté une théorie des séries alternées en PVS.

Arc-tangente

Soit f une fonction représentée par le modèle de Taylor $(p(x), I)$, $r \in I$.

$$\begin{aligned}\operatorname{atan}(f(x)) &= \operatorname{atan}(p(x) + r) \\ &= \underbrace{\operatorname{atan}(p(x))}_{\text{partie polynomiale tronquée}} + \underbrace{\operatorname{atan}(p(x) + r) - \operatorname{atan}(p(x))}_{\text{(intervalle)}}\end{aligned}$$

$$\underbrace{\operatorname{atan}(p(x) - p(0))}_{\sum_{i=0}^{N} \frac{(-1)^i}{2i+1}(p(x)-p(0))^{2i+1}} + \underbrace{\operatorname{atan}(p(x)) - \operatorname{atan}(p(x) - p(0))}_{\text{(intervalle)}}$$

$$\sum_{i=0}^{N} \frac{(-1)^i}{2i+1}(p(x)-p(0))^{2i+1} + \sum_{i=N+1}^{\infty} \frac{(-1)^i}{2i+1}(p(x)-p(0))^{i}$$

partie polynomiale tronquée
$+$ reste de la troncature (intervalle)

reste (intervalle)
à l'aide du théorème

Propriété d'inclusion

Principe fondamental de l'arithmétique d'intervalles : « Tu ne mentiras point ».
Pour passer du calcul aux théorèmes :

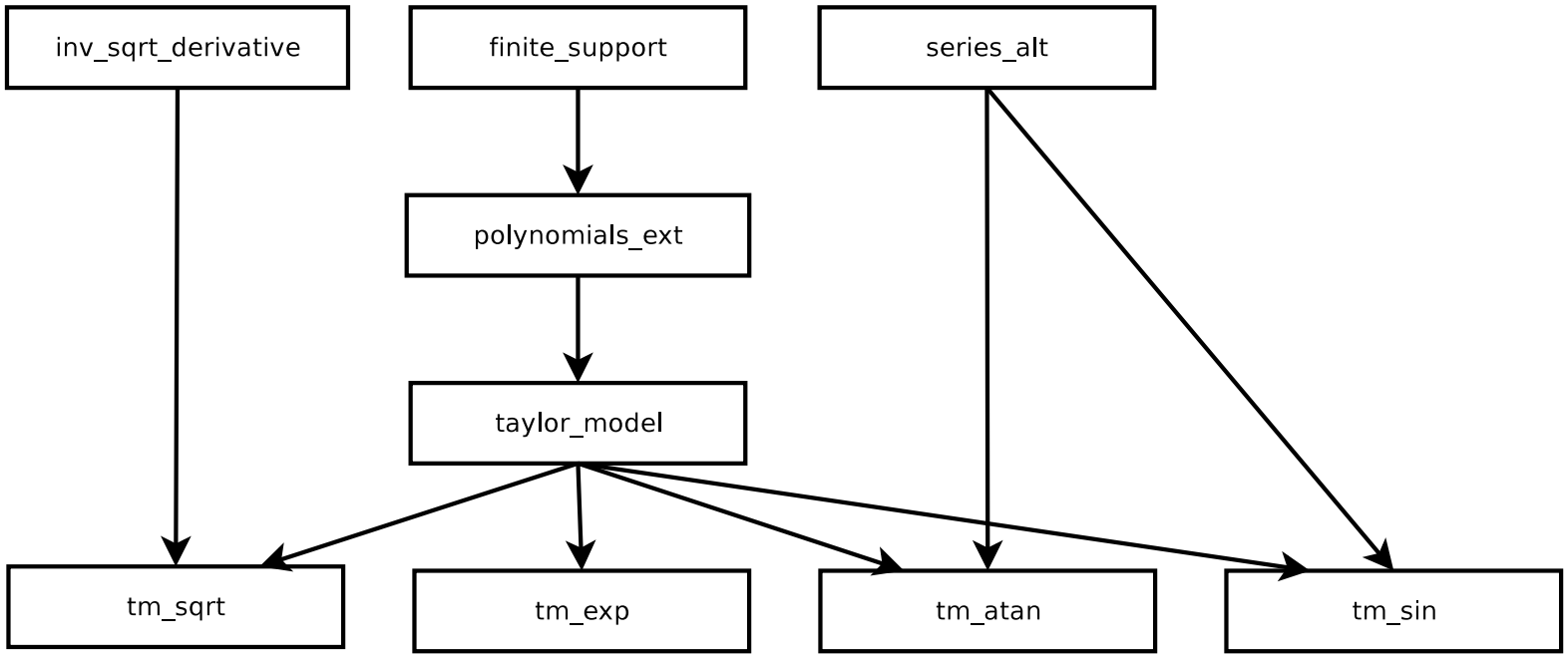
$$\text{containment}(f, t) = \forall x \in J.f(x) - t`P(x) \in t`I$$

Propriété d'inclusion

Nous avons implanté en PVS les modèles de Taylor pour

- les opérations arithmétiques ;
- certaines fonctions élémentaires.

Nous avons prouvé que chaque opération ou fonction préserve la propriété d'inclusion.



Plan de l'exposé

Évaluation des modèles de Taylor

Outre la preuve de théories mathématiques, PVS peut les mettre en œuvre et effectuer des calculs, grâce au PVS *ground evaluator* :

- c'est une fonctionnalité expérimentale de PVS 3.x ;
- il extrait du code Common Lisp à partir des spécifications fonctionnelles de PVS et l'évalue ;
- PVSio est une interface alternative et plus conviviale, disponible sur `http://research.nianet.org/~munoz/PVSio`.

Exemple $cosh\left(2 \cdot \frac{x}{1000}\right) \cdot sinh\left(3 \cdot \frac{x}{1000}\right)$

```
example: THEORY
 BEGIN
  IMPORTING tm_exp[5, 5, [[-1, 1]]]
  cosh(x: tm): tm = (1/2) × (exp(x) + exp(-x))
  sinh(x: tm): tm = (1/2) × (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 = cosh(2 × tm_x) × sinh(3 × tm_x)
 END example
```

Exemple

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

Exemple

```
<PVSio> example1‘I ;
==>
(# lb := -19966660037929209080778095595964694170499249884356754248912582792777246825769541627979310535210358464 7/
38763496047478702331322336437004695773022456032565137
27240130672324223395638663643366685812200000000000000
00000000000000,
ub := 19966660037929209080778095595964694170499249884356754248912582792777246825769541627979310535210358464 7/
38763496047478702331322336437004695773022456032565137
27240130672324223395638663643366685812200000000000000
00000000000000 #)
```

Exemple

Le modèle de Taylor d'ordre 5 de

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

avec

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

Plan de l'exposé

Preuve pas à pas

On veut prouver la propriété d'inclusion pour le sinus hyperbolique.

```
sinh(x: real): real =
      (1/2) · (exp(x) − exp(−(x)))
sinh(t: tm): tm =
      (1/2) · (exp(t) − exp(−(t)))

sinh_lem: LEMMA
   containment(λ (x: domIntervalType): sinh(x), sinh(tm_x))
```

Preuve pas à pas

```
sinh_lem :
|-----
{1} containment(LAMBDA (x : domIntervalType) :
        (1 / 2) * (exp(x) - exp(-x)),
        (1 / 2) * (exp(tm_x) - exp(-(tm_x))))
Rule?
```

Preuve pas à pas

```
sinh_lem :
|-----
{1} containment(LAMBDA (x : domIntervalType) :
        (1 / 2) * (exp(x) - exp(-x)),
        (1 / 2) * (exp(tm_x) - exp(-(tm_x))))
Rule? (rewrite "tm_scal_lem")
```

```
this simplifies to :
sinh_lem :
|-----
[1] containment(LAMBDA (x : domIntervalType) :
(exp(x) - exp(-x)), (exp(tm_x) - exp(-(tm_x))))
Rule?
```

Preuve pas à pas

```
sinh_lem :
|-----
{1} containment(LAMBDA (x : domIntervalType) :
        (1 / 2) * (exp(x) - exp(-x)),
        (1 / 2) * (exp(tm_x) - exp(-(tm_x))))
Rule? (rewrite "tm_scal_lem")
```

```
this simplifies to :
sinh_lem :
|-----
[1] containment(LAMBDA (x : domIntervalType) :
(exp(x) - exp(-x)), (exp(tm_x) - exp(-(tm_x))))
Rule? (rewrite "tm_sub_lem")
```

Preuve pas à pas

```
this yields 2 subgoals :
sinh_lem.1 :
|-----
{1} containment(LAMBDA (x : domIntervalType) :
        exp(-x), exp(-tm_x))
Rule?
```

Preuve pas à pas

```
this yields 2 subgoals :
sinh_lem.1 :
|-----
{1} containment(LAMBDA (x : domIntervalType) :
        exp(-x), exp(-tm_x))
Rule? (rewrite "tm_exp_lem")
```

```
this simplifies to :
sinh_lem.1 :
|-----
[1] containment(LAMBDA (x : domIntervalType) :
        -x,-(tm_x))

Rule?
```

Preuve pas à pas

```
this yields 2 subgoals :
sinh_lem.1 :
|-----
{1} containment(LAMBDA (x : domIntervalType) :
        exp(-x), exp(-tm_x))
Rule? (rewrite "tm_exp_lem")
```

```
this simplifies to :
sinh_lem.1 :
|-----
[1] containment(LAMBDA (x : domIntervalType) :
        -x,-(tm_x))

Rule? (rewrite "tm_neg_lem")
```

Preuve pas à pas

```
this simplifies to :
sinh_lem.1 :
|-----
{1} containment(LAMBDA (x : domIntervalType) :
        x, tm_x)

Rule?
```

Preuve pas à pas

```
this simplifies to :
sinh_lem.1 :
|-----
{1} containment(LAMBDA (x : domIntervalType) :
        x, tm_x)

Rule? (rewrite "tm_x_lem")
```

```
This completes the proof of sinh_lem.1.
sinh_lem.2 :
|-----
{1} containment(LAMBDA (x : domIntervalType) :
        exp(x),exp(tm_x))
Rule?
```

Preuve pas à pas

```
this simplifies to :
sinh_lem.1 :
|-----
{1} containment(LAMBDA (x : domIntervalType) :
        x, tm_x)

Rule? (rewrite "tm_x_lem")
```

```
This completes the proof of sinh_lem.1.
sinh_lem.2 :
|-----
{1} containment(LAMBDA (x : domIntervalType) :
        exp(x),exp(tm_x))
Rule? (rewrite "tm_exp_lem")
```

Preuve pas à pas

```
this simplifies to :
sinh_lem.2 :
|-----
{1} containment(LAMBDA (x : domIntervalType) :
        x, tm_x)
Rule?
```

Preuve pas à pas

```
this simplifies to :
sinh_lem.2 :
|-----
{1} containment(LAMBDA (x : domIntervalType) :
        x, tm_x)
Rule? (rewrite "tm_x_lem")
```

```
This completes the proof of sinh_lem.2.
Q.E.D.
```

Stratégie « containment »

- Les preuves pas à pas sont fastidieuses.

Nous avons développé avec Muñoz la stratégie « `containment` » pour prouver la propriété d'inclusion de $e(x)$ dans le modèle de Taylor $E(J)$ par récurrence sur la structure de $e(x)$.

```
sinh(x: real): real =
      (1/2) · (exp(x) − exp(−(x)))
sinh(t: tm): tm =
      (1/2) · (exp(t) − exp(−(t)))

sinh_lem: LEMMA
   containment(λ (x: domIntervalType): sinh(x), sinh(tm_x))
%|- sinh_lem : PROOF (containment) QED
```

Stratégie pour certifier des inégalités

Pour un ordre N et un domaine J donnés, la stratégie « `taylormodels` » démontre le séquent

$$x \in J \vdash e(x) \diamond k$$

où $\diamond \in \{<, \leq, >, \geq, \in\}$, en effectuant les pas :

Stratégie pour certifier des inégalités

Pour un ordre N et un domaine J donnés, la stratégie « `taylormodels` » démontre le séquent

$$x \in J \vdash e(x) \diamond k$$

où $\diamond \in \{<, \leq, >, \geq, \in\}$, en effectuant les pas :

1. construction du modèle de Taylor E pour $e(x)$;

Stratégie pour certifier des inégalités

Pour un ordre N et un domaine J donnés, la stratégie « `taylormodels` » démontre le séquent

$$x \in J \vdash e(x) \diamond k$$

où $\diamond \in \{<, \leq, >, \geq, \in\}$, en effectuant les pas :

1. construction du modèle de Taylor E pour $e(x)$;
2. preuve de containment(e, E) donc $e(x) - E\text{`}P(x) \in E\text{`}I$;

Stratégie pour certifier des inégalités

Pour un ordre N et un domaine J donnés, la stratégie « `taylormodels` » démontre le séquent

$$x \in J \vdash e(x) \diamond k$$

où $\diamond \in \{<, \leq, >, \geq, \in\}$, en effectuant les pas :

1. construction du modèle de Taylor E pour $e(x)$;
2. preuve de containment(e, E) donc $e(x) - E\text{`}P(x) \in E\text{`}I$;
3. preuve que le polynôme $E\text{`}P(x) \in E\text{`}P(J)$ donc $e(x) \in E\text{`}P(J) + E\text{`}I$;

Stratégie pour certifier des inégalités

Pour un ordre N et un domaine J donnés, la stratégie « `taylormodels` » démontre le séquent

$$x \in J \vdash e(x) \diamond k$$

où $\diamond \in \{<, \leq, >, \geq, \in\}$, en effectuant les pas :

1. construction du modèle de Taylor E pour $e(x)$;
2. preuve de containment(e, E) donc $e(x) - E\text{`}P(x) \in E\text{`}I$;
3. preuve que le polynôme $E\text{`}P(x) \in E\text{`}P(J)$ donc $e(x) \in E\text{`}P(J) + E\text{`}I$;
4. preuve que $E\text{`}P(J) + E\text{`}I \diamond k$.

Stratégie pour certifier des inégalités

Pour un ordre N et un domaine J donnés, la stratégie « `taylormodels` » démontre le séquent

$$x \in J \vdash e(x) \diamond k$$

où $\diamond \in \{<, \leq, >, \geq, \in\}$, en effectuant les pas :

1. construction du modèle de Taylor E pour $e(x)$;
2. preuve de containment(e, E) donc $e(x) - E\text{`}P(x) \in E\text{`}I$;
3. preuve que le polynôme $E\text{`}P(x) \in E\text{`}P(J)$ donc $e(x) \in E\text{`}P(J) + E\text{`}I$;
4. preuve que $E\text{`}P(J) + E\text{`}I \diamond k$.

En conclusion

$$e(x) \diamond k.$$

Stratégie pour certifier des inégalités

```
myex1: THEORY
 BEGIN

  IMPORTING tm_exp

  x, y: VAR real

  test1: LEMMA
     x ## [[0, 1]] ⟹
       exp(x) − 1 − x − sq(x) ##
         [[−36/100, 12/100]]
  %|- test1 : PROOF (then (skolem!) (taylormodels "x" :order 5)) QED
 END myex1
```

Le “##” signifie “$\in$”.

Plan de l'exposé

Applications

Évaluation d'une fonction élémentaire en arithmétique flottante :

1. approximation de f par un polynôme p dans le domaine J
2. évaluation de p en arithmétique flottante : $\widehat{p(x)}$

Question :

$$|f(x) - \widehat{p(x)}| \leq$$

Applications

Évaluation d'une fonction élémentaire en arithmétique flottante :

1. approximation de f par un polynôme p dans le domaine J
2. évaluation de p en arithmétique flottante : $\widehat{p(x)}$

Question :

$$|f(x) - \widehat{p(x)}| \leq \underbrace{||f - p||_{x \in J}}_{\text{erreur d'approx.}} + \underbrace{|p(x) - \widehat{p(x)}|}_{\text{erreur fp.}}$$

Approximation de la fonction exponentielle

Le contexte est la norme IEEE-754 en simple précision.
L'approximation polynomiale suivante nous a été donnée :

$$p(x) = 1 + x + \frac{524297}{1048576} \cdot x^2 + \frac{349529}{2097152} \cdot x^3$$

pour x dans l'intervalle $[-1/64, 1/64]$.
On nous demande de certifier que

$$|e^x - p(x)| < \frac{1}{2000000000} = 5 \cdot 10^{-10}$$

Ordre	Nb. sous-intervalles	Prouvée	Temps (sec)
3	8	non	89.99
3	9	non	162.98
3	10	non	132.93
3	20	non	433.51
4	8	non	95.92
4	9	oui	172.56
4	10	oui	132.57
5	8	non	103.64
5	9	oui	180.51
5	10	oui	139.47
6	8	non	324.70
6	9	oui	428.22
6	10	oui	419.51

Ordre des modèles de Taylor et nombre de sous-intervalles utilisés pour prouver

$$e^x - p(x) \in \left[-\frac{1}{2000000000}, \frac{1}{2000000000} \right]$$

Applications

- Détection et résolution de conflits aériens :
  - conflit : deux avions s'approchent trop près l'un de l'autre dans l'espace aérien ;
  - résolution : un avion, ou les deux, effectue une manœuvre d'évitement.
- Un algorithme a été proposé (Dowek et al.) et prouvé en PVS. Il représente les positions et les vitesses des avions dans un espace euclidien.
- La fonction arc-tangente est utilisée pour passer de cet espace à la géométrie de la Terre et vice-versa.

Approximation de la fonction arc-tangente

La fonction arc-tangente est approchée par le polynôme

$$q(x) = x - \frac{11184811}{33554432} \cdot x^3 + \frac{13421773}{67108864} \cdot x^5,$$

pour $x \in [-1/30, 1/30]$.
Nous voulons borner l'erreur d'approximation :

$$|\mathrm{atan}(x) - q(x)| \leq \frac{1}{2^i},$$

pour i entre 10 et 26.

	temps (secondes)			
i	Ordre 3	Ordre 4	Ordre 5	Ordre 6
10	5.79	5.57	6.24	34.72
15	6.17	5.51	6.30	34.82
20	5.80	5.58	6.22	34.55
21	5.47	5.58	6.25	34.64
22	5.45	5.53	6.28	34.63
23	5.54	5.54	6.25	34.81
24	5.53	5.56	6.25	35.15
25	5.52	5.63	6.27	34.75
26	6.31	6.37	7.07	34.68

Ordre des modèles de Taylor et temps pour prouver

$$\text{atan}(x) - q(x) \in \left[-\frac{1}{2^i}, \frac{1}{2^i} \right]$$

Conclusions

- Nous avons développé :
  - une théorie des modèles de Taylor en PVS $(+, -, \times, /, \sqrt{}, \exp, \sin, \text{atan} \ldots)$,
  - la propriété d'inclusion pour chaque fonction ;
  - des stratégies pour prouver des propriétés d'inclusion et des inégalités ;
  - une théorie des séries à support fini, des séries alternées et des polynômes compatible avec la bibliothèque PVS des séries du NASA LaRC.
- Nous avons des applications : évaluation des fonctions élémentaires avec arrondi correct en arithmétique flottante ; certification d'expressions utilisées en aéronautique.

Perspectives

- Rendre plus largement disponible l'arithmétique d'intervalles et des modèles de Taylor dans les assistants de preuve (PVS, Isabelle...) ;
- travailler à améliorer l'efficacité pour les modèles de Taylor d'ordre supérieur à 6 ;
- développer d'autres fonctions $(\cos, \tan, \ldots)$;
- automatiser davantage la stratégie pour certifier des inégalités (augmenter l'ordre du modèle de Taylor / diviser le domaine d'entrée) ;
- implanter l'extension des modèles de Taylor au cas multivariable ;
- explorer d'autres bases pour les polynômes comme par exemple Bernstein.

Merci de votre attention.