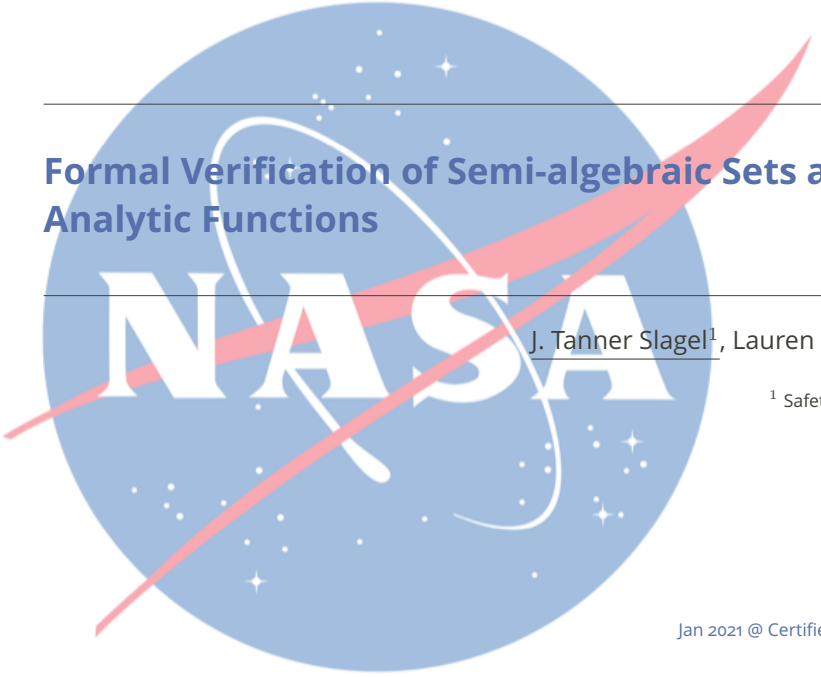


Formal Verification of Semi-algebraic Sets and Real Analytic Functions

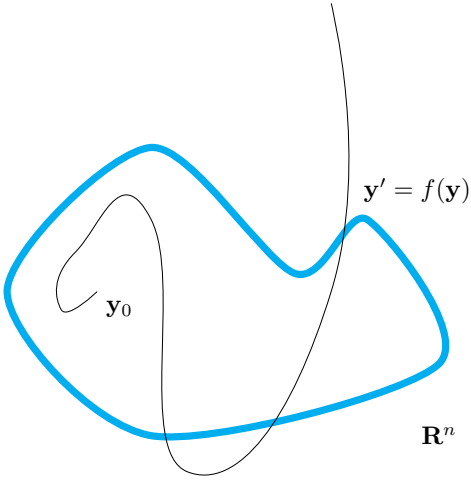
J. Tanner Slagel[1], Lauren White[2], Aaron M. Dutle[1]

[1] Safety Critical Avionics Systems Branch
NASA Langley
j.tanner.slagel@nasa.gov
aaron.m.dutle@nasa.gov

[2] Department of Mathematics
Kansas State University
laurenmwhite@ksu.edu

Jan 2021 @ Certified Programs and Proofs (CPP) 2021

Motivation



- Hybrid system: a dynamical system that exhibits both continuous and discrete dynamic behavior
- Differential dynamic Logic (DDL): logic for specifying and verifying hybrid systems
- Goal: implement DDL in the Prototype Verification System (PVS). This requires:
  - Multivariate polynomials and semi-algebraic (SA) sets
  - Real analytic functions
  - Behavior of real analytic functions on boundary of SA sets.

j.tanner.slagel@nasa.gov

Outline

- Motivation
- Formalization of Semi-algebraic Sets
  - Multivariate polynomials
  - Semi-algebraic sets
- Formalization of Real Analytic Functions
  - Real analytic vs. smooth
- Formalization of Real Analytic Functions with SA Sets
  - Behavior on the boundary
  - Replacing real analytic with smooth
- Conclusions and Future Work

j.tanner.slagel@nasa.gov

Outline

- Motivation
- Formalization of Semi-algebraic Sets
  - Multivariate polynomials
  - Semi-algebraic sets
- Formalization of Real Analytic Functions
  - Real analytic vs. smooth
- Formalization of Real Analytic Functions with SA Sets
  - Behavior on the boundary
  - Replacing real analytic with smooth
- Conclusions and Future Work

j.tanner.slagel@nasa.gov

Multivariate Polynomials

- Primitive monomial:

$$\mathbf{X}^{\boldsymbol{\alpha}} := X_0^{\alpha_0} \cdots X_{m-1}^{\alpha_{m-1}}$$

  - $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \ldots \alpha_{m-1}) \in \mathbb{N}^m$
  - $m \in \mathbb{N}$
- Monomial:

$$c\mathbf{X}^{\boldsymbol{\alpha}}$$

  - $c \in \mathbb{R}$
  - $\mathbf{X}$ primitive monomial
- Multivariate polynomial:

$$p = \sum_{k=0}^{n} c_k \mathbf{X}^{\boldsymbol{\alpha}(k)}$$

  - $n \in \mathbb{N}$
  - $c_k \in \mathbb{R}$, $\boldsymbol{\alpha}(k) \in \mathbb{N}^m$ for each $k \in \mathbb{N}_{\leq n}$

j.tanner.slagel@nasa.gov

Formalization of Multivariate Polynomials

- Monomial:
  - Record datatype

```
monomial: TYPE =
  [# C := real, alpha := list[nat] #]
```

  - Instantiation

```
m = (# C := c, alpha := L #)
```

    - "`'`" field accessor, i.e., `m'alpha = L`
- Multivariate polynomial:
  - Datatype

```
MultPoly: TYPE = list[monomial]
```

  - Instantiation

```
p1: MultPoly = (: (# C:=1, alpha:=(: 2 :) #),
  (# C:=1, alpha:=(: 1 :) #) :)
```


j.tanner.slagel@nasa.gov

Representation

Consider:

$$p_1 = X_0^2 + X_0$$

$$p_2 = X_0 + X_0^2$$

$$p_3 = X_0 X_1^0 + X_0^2$$

$$p_4 = X_0 + 3X_0^2 + (-2)X_0^2$$

$$p_5 = X_0 + X_0^2 + 0X_0^3$$

```
p1: MultPoly := (: (# C:=1,
alpha:=(: 2 :) #)
  (# C:=1, alpha:=(: 1 :) #) :)

p2: MultPoly := (: (# C:=1,
alpha:=(: 1 :) #)
  (# C:=1, alpha:=(: 2 :) #) :)

p3: MultPoly := (: (# C:=1,
alpha:=(: 1, 0 :) #)
  (# C:=1, alpha:=(: 2 :) #) :)

                    ⋮
```


j.tanner.slagel@nasa.gov

Representation

Consider:

$$p_1 = X_0^2 + X_0$$

$$p_2 = X_0 + X_0^2$$

$$p_3 = X_0 X_1^0 + X_0^2$$

$$p_4 = X_0 + 3X_0^2 + (-2)X_0^2$$

$$p_5 = X_0 + X_0^2 + 0X_0^3$$

```
p1: MultPoly = (: (# C: = 1,
alpha: = (: 2 :) #)
  (# C: = 1, alpha: = (: 1 :) #) :)

p2: MultPoly = (: (# C: = 1,
alpha: = (: 1 :) #)
  (# C: = 1, alpha: = (: 2 :) #) :)

p3: MultPoly = (: (# C: = 1,
alpha: = (: 1, 0 :) #)
  (# C: = 1, alpha: = (: 2 :) #) :)

⋮
```

Not unique when viewed as functions (under evaluation)

j.tanner.slagel@nasa.gov

Standard Form

A multivariate polynomial is in Standard Form when:

1. `lifted?(p)/lift(p)`: Each monomial in polynomial is same dimension:

$$\exists m \in \mathbb{N} \text{ s.t. } \dim(\boldsymbol{\alpha}(k)) = m \forall k \in \mathbb{N}_{\leq n}$$

$$\exists n_0 \in \mathbb{N}_{\leq n} \text{ s.t. } \boldsymbol{\alpha}_m(n_0) > 0$$

2. `simplified?(p)/simplify(p)`: No primitive monomial appears more than once:

$$\forall i \neq j \in \mathbb{N}_{\leq n}, \boldsymbol{\alpha}(i) \neq \boldsymbol{\alpha}(j)$$

3. `allnonzero?(p)/allnonzero(p)`:

$$\forall k \in \mathbb{N}_{\leq n}, c_k \neq 0$$

4. `is_sorted?(p)/mv_sort(p)`: monomial terms are ordered by Graded Lexicographic Order

j.tanner.slagel@nasa.gov

Graded Lexicographical Order

Graded Lexicographical Order, $\mathbf{X}^{\boldsymbol{\alpha}(0)} < \mathbf{X}^{\boldsymbol{\alpha}(1)}$ when:

1. Degree of $\mathbf{X}^{\boldsymbol{\alpha}(0)}$ is less than degree of $\mathbf{X}^{\boldsymbol{\alpha}(1)}$, i.e.,

$$\deg\left(\mathbf{X}^{\boldsymbol{\alpha}(0)}\right) < \deg\left(\mathbf{X}^{\boldsymbol{\alpha}(1)}\right)$$

OR

2. Degree of $\mathbf{X}^{\boldsymbol{\alpha}(0)}$ is the same as $\mathbf{X}^{\boldsymbol{\alpha}(1)}$ and earliest differing exponent is smaller in $\mathbf{X}^{\boldsymbol{\alpha}(0)}$:

$$\deg\left(\mathbf{X}^{\boldsymbol{\alpha}(0)}\right) = \deg\left(\mathbf{X}^{\boldsymbol{\alpha}(1)}\right) \wedge \exists j \in \mathbb{N}_{\leq m-1}\left(\boldsymbol{\alpha}_j\left(0\right) < \boldsymbol{\alpha}_j\left(1\right) \wedge \forall i \in \mathbb{N}_{<j}\ \boldsymbol{\alpha}_i(0) = \boldsymbol{\alpha}_i(1)\right)$$

j.tanner.slagel@nasa.gov

Graded Lexicographical Order

Graded Lexicographical Order, $\mathbf{X}^{\boldsymbol{\alpha}(0)} < \mathbf{X}^{\boldsymbol{\alpha}(1)}$ when:

1. Degree of $\mathbf{X}^{\boldsymbol{\alpha}(0)}$ is less than degree of $\mathbf{X}^{\boldsymbol{\alpha}(1)}$, i.e.,

$$\deg\left(\mathbf{X}^{\boldsymbol{\alpha}(0)}\right) < \deg\left(\mathbf{X}^{\boldsymbol{\alpha}(1)}\right)$$

   OR

2. Degree of $\mathbf{X}^{\boldsymbol{\alpha}(0)}$ is the same as $\mathbf{X}^{\boldsymbol{\alpha}(1)}$ and earliest differing exponent is smaller in $\mathbf{X}^{\boldsymbol{\alpha}(0)}$:

$$\deg\left(\mathbf{X}^{\boldsymbol{\alpha}(0)}\right) = \deg\left(\mathbf{X}^{\boldsymbol{\alpha}(1)}\right) \wedge \exists j \in \mathbb{N}_{\leq m-1}\left(\boldsymbol{\alpha}_j\left(0\right) < \boldsymbol{\alpha}_j\left(1\right) \wedge \forall i \in \mathbb{N}_{<j}\ \boldsymbol{\alpha}_i(0) = \boldsymbol{\alpha}_i(1)\right)$$

Example:

$$X_1X_2,\ X_0^2X_1^2,\ X_0^2X_1^1X_0^1,\ X_0^4.$$

j.tanner.slagel@nasa.gov

Example of Standard Form

$$p(X_0, X_1, X_2) = X_0X_1X_2 + 5X_0^0X_1 - 3X_0^0X_1^1 + 7X_0^1X_2^2$$

j.tanner.slagel@nasa.gov

Example of Standard Form

$$p(X_0, X_1, X_2) = X_0X_1X_2 + 5X_0^0X_1 - 3X_0^0X_1^1 + 7X_0^1X_2^2$$

Lift

$$p(X_0, X_1, X_2) = X_0X_1X_2 + 5X_0^0X_1X_2^0 - 3X_0^0X_1^1X_2^0 + 7X_0^1X_1^0X_2^2$$

j.tanner.slagel@nasa.gov

Example of Standard Form

$$p(X_0, X_1, X_2) = X_0X_1X_2 + 5X_0^0X_1 - 3X_0^0X_1^1 + 7X_0^1X_2^2$$

Lift

$$p(X_0, X_1, X_2) = X_0X_1X_2 + 5X_0^0X_1X_2^0 - 3X_0^0X_1^1X_2^0 + 7X_0^1X_1^0X_2^2$$

Sort

$$p(X_0, X_1, X_2) = 5X_0^0X_1X_2^0 - 3X_0^0X_1^1X_2^0 + 7X_0^1X_1^0X_2^2 + X_0X_1X_2$$

j.tanner.slagel@nasa.gov

Example of Standard Form

$$p(X_0, X_1, X_2) = X_0 X_1 X_2 + 5X_0^0 X_1 - 3X_0^0 X_1^1 + 7X_0^1 X_2^2$$

Lift

$$p(X_0, X_1, X_2) = X_0 X_1 X_2 + 5X_0^0 X_1 X_2^0 - 3X_0^0 X_1^1 X_2^0 + 7X_0^1 X_1^0 X_2^2$$

Sort

$$p(X_0, X_1, X_2) = 5X_0^0 X_1 X_2^0 - 3X_0^0 X_1^1 X_2^0 + 7X_0^1 X_1^0 X_2^2 + X_0 X_1 X_2$$

Simplify

$$p(X_0, X_1, X_2) = 2X_0^0 X_1 X_2^0 + 7X_0^1 X_1^0 X_2^2 + X_0 X_1 X_2$$

j.tanner.slagel@nasa.gov

Example of Standard Form

$$p(X_0, X_1, X_2) = X_0X_1X_2 + 5X_0^0X_1 - 3X_0^0X_1^1 + 7X_0^1X_2^2$$

Lift

$$p(X_0, X_1, X_2) = X_0X_1X_2 + 5X_0^0X_1X_2^0 - 3X_0^0X_1^1X_2^0 + 7X_0^1X_1^0X_2^2$$

Sort

$$p(X_0, X_1, X_2) = 5X_0^0X_1X_2^0 - 3X_0^0X_1^1X_2^0 + 7X_0^1X_1^0X_2^2 + X_0X_1X_2$$

Simplify

$$p(X_0, X_1, X_2) = 2X_0^0X_1X_2^0 + 7X_0^1X_1^0X_2^2 + X_0X_1X_2$$

Formalization required showing

```
lifted?(mv_sort(lift(p)))
sorted?(allnonzero(sorted(lift(p))))
```

etc.

j.tanner.slagel@nasa.gov

Uniqueness of standard form

Theorem

Given a function σ that returns the standard form of a polynomial as in Definition 7, and p_1, p_2 polynomial expressions of the form (4),

$$\sigma(p_1) = \sigma(p_2)$$

if and only if for all $\mathbf{x} \in \mathbb{R}^m$,

$$p_1(\mathbf{x}) = p_2(\mathbf{x}).$$

```
standard_form_is_unique:  THEOREM
FORALL (p,q:  MultPoly):
  mv_standard_form(p) = mv_standard_form(q)
    IFF
  FORALL ((x:list[real] | length(x) >= max(max_length(p), max_length(q)))):
  full_eval(p)(x)  =  full_eval(q)(x)
```


j.tanner.slagel@nasa.gov

Semi-algebraic Sets

- Atomic polynomial formula:

$$p \triangleright 0$$

  - p is a polynomial in $\mathbb{R}[\mathbf{X}]$, $\mathbf{X} := X_0, \cdots, X_{m-1}$
  - $\triangleright \in \{\geq, >, \leq, <\}$
- Quantifier free polynomial formula:

$$\varphi = \bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} p_{ij} \triangleright 0, \text{ where } \triangleright \in \{\geq, >, \leq, <\}$$

- Semi-algebraic set:
  and a subset S of $\mathbb{R}^m$ is a *semi-algebraic set*, if there is a quantifier free polynomial formula φ such that

$$S = \{\mathbf{x} \in \mathbb{R}^m \mid \varphi(\mathbf{x}) \text{ is true}\}$$

j.tanner.slagel@nasa.gov

Formalization of Semi-algebraic Sets

- Atomic polynomial formula:

```
atomic_poly:  TYPE =
  [# poly:(mv_standard_form?)  ineq:INEQ #]
```

with

```
INEQ: TYPE = { ff:  [real,real -> bool] |
  (ff =  <= ) OR (ff =  >= ) OR
  (ff =  < ) OR (ff =  > ) }
```

- Quantifier free polynomial formula:
  - A conjunction of atomic polynomial formulas

    ```
    meeting  TYPE =list[atomic_poly]
    ```

  - A disjunction of these conjunctions

    ```
    joining:  TYPE =list[meeting]
    ```

  - Example, for atomic polynomial formulas a, b, c, d:

$$(a \wedge b) \vee (c \wedge d)$$

```
(:  (:  a, b :), (:  c, d :)  :)
```


j.tanner.slagel@nasa.gov

Formalization of Semi-algebraic Sets

- **Semi-algebraic set:** An SA set $S(\varphi)$ defined by φ is then specified in PVS by

```
semi_alg(j:joining)(n:nat | n >= meet_max(j)):
  set[VectorN(n)] =
  { x:VectorN(n) | join(j)(x) },
```

Formalization of Semi-algebraic Sets

- **Semi-algebraic set:** An SA set $S(\varphi)$ defined by φ is then specified in PVS by

```
semi_alg(j:joining)(n:nat | n >= meet_max(j)):
  set[VectorN(n)] =
  { x:VectorN(n) | join(j)(x) },
```

Theorem

For two Semi-algebraic sets S_1 and S_2, the following properties hold:

1. *The union $S_1 \cup S_2$ is an Semi-algebraic set.*
2. *The intersection $S_1 \cap S_2$ is an Semi-algebraic set.*
3. *The compliment S_1^{c} is an Semi-algebraic set.*

j.tanner.slagel@nasa.gov

Formalization of Semi-algebraic Sets

- **Semi-algebraic set:** An SA set $S(\varphi)$ defined by φ is then specified in PVS by

```
semi_alg(j:joining)(n:nat | n >= meet_max(j)):
  set[VectorN(n)] =
  { x:VectorN(n) | join(j)(x) },
```

Theorem

For two Semi-algebraic sets S_1 and S_2, the following properties hold:

1. *The union $S_1 \cup S_2$ is an Semi-algebraic set.*
2. *The intersection $S_1 \cap S_2$ is an Semi-algebraic set.*
3. *The compliment S_1^c is an Semi-algebraic set.*

Note: proving this theorem in PVS required writing the disjunctive normal form for

- The disjunction of two joining expressions
- The conjunction of two joining expressions
- The complement of two joining expressions

j.tanner.slagel@nasa.gov

Formalization of Semi-algebraic Sets

- **Semi-algebraic set:** An SA set $S(\varphi)$ defined by φ is then specified in PVS by

```
semi_alg(j:joining)(n:nat | n >= meet_max(j)):
  set[VectorN(n)] =
  { x:VectorN(n) | join(j)(x) },
```

Theorem

For two Semi-algebraic sets S_1 and S_2, the following properties hold:

1. *The union $S_1 \cup S_2$ is an Semi-algebraic set.*
2. *The intersection $S_1 \cap S_2$ is an Semi-algebraic set.*
3. *The compliment S_1^c is an Semi-algebraic set.*

Note: proving this theorem in PVS required writing the disjunctive normal form for

- The disjunction of two joining expressions Easy, concatenation of lists
- The conjunction of two joining expressions
- The complement of two joining expressions

j.tanner.slagel@nasa.gov

Formalization of Semi-algebraic Sets

- **Semi-algebraic set:** An SA set $S(\varphi)$ defined by φ is then specified in PVS by

```
semi_alg(j:joining)(n:nat | n >= meet_max(j)):
  set[VectorN(n)] =
  { x:VectorN(n) | join(j)(x) },
```

Theorem

For two Semi-algebraic sets S_1 and S_2, the following properties hold:

1. *The union $S_1 \cup S_2$ is an Semi-algebraic set.*
2. *The intersection $S_1 \cap S_2$ is an Semi-algebraic set.*
3. *The compliment S_1^c is an Semi-algebraic set.*

Note: proving this theorem in PVS required writing the disjunctive normal form for

- The disjunction of two joining expressions Easy, concatenation of lists
- The conjunction of two joining expressions
- The complement of two joining expressions Easy, “flip" inequality in atomic polynomials

j.tanner.slagel@nasa.gov

Formalization of Semi-algebraic Sets

- **Semi-algebraic set:** An SA set $S(\varphi)$ defined by φ is then specified in PVS by

```
semi_alg(j:joining)(n:nat | n >= meet_max(j)):
  set[VectorN(n)] =
  { x:VectorN(n) | join(j)(x) },
```

Theorem

For two Semi-algebraic sets S_1 and S_2, the following properties hold:

1. *The union $S_1 \cup S_2$ is an Semi-algebraic set.*
2. *The intersection $S_1 \cap S_2$ is an Semi-algebraic set.*
3. *The compliment S_1^c is an Semi-algebraic set.*

Note: proving this theorem in PVS required writing the disjunctive normal form for

- The disjunction of two joining expressions Easy, concatenation of lists
- The conjunction of two joining expressions Distributing conjunction across many disjunctions
- The complement of two joining expressions Easy, “flip" inequality in atomic polynomials

j.tanner.slagel@nasa.gov

Conjunction of joining expressions

Disjunctive normal form of a conjunction of joining expression with an atomic polynomial:

$$\left(\bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} p_{ij} \triangleright 0 \right) \wedge (q \triangleright 0) = \bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i+1} w_{ij}$$

where

$$w_{i,j} = \begin{cases} p_{i,j} & j \leq J_i \\ q & j = J_i + 1 \end{cases}$$

j.tanner.slagel@nasa.gov

Conjunction of joining expressions

Disjunctive normal form of a conjunction of joining expression with an atomic polynomial:

$$\left(\bigvee_{i=1}^{I}\bigwedge_{j=1}^{J_i} p_{ij} \triangleright 0\right) \wedge (q \triangleright 0) = \bigvee_{i=1}^{I}\bigwedge_{j=1}^{J_i+1} w_{ij}$$

where

$$w_{i,j} = \begin{cases} p_{i,j} & j \leq J_i \\ q & j = J_i + 1 \end{cases}$$

Conjunction of joining expressions:

```
cap_join(j1,j2:joining):  RECURSIVE joining =
  IF j1 = null THEN null
  ELSIF j2 = null THEN null
  ELSE append(append_to_each(car(j1),j2),
  cap_join(cdr(j1),j2))
  ENDIF
  MEASURE length(j1).
```


j.tanner.slagel@nasa.gov

Outline

- Motivation
- Formalization of Semi-algebraic Sets
  - Multivariate polynomials
  - Semi-algebraic sets
- Formalization of Real Analytic Functions
  - Real analytic vs. smooth
- Formalization of Real Analytic Functions with SA Sets
  - Behavior on the boundary
  - Replacing real analytic with smooth
- Conclusions and Future Work

j.tanner.slagel@nasa.gov

Real Analytic Functions

Function $f : \mathbb{R} \to \mathbb{R}$ is real analytic at $c_0 \in D$:

$$\exists \{a_k\}_{k=0}^{\infty},\, r \in \mathbb{R}_{>0} \text{ s.t. } f(x) = \sum_{k=0}^{\infty} a_k \left(x - c_0\right)^k \qquad \forall x \in (c_0 - r, c_0 + r)\,.$$

Sequence $\{a_k\}$ and real number r are defined by the predicate

```
analytic_parts?(c0:real,f:[real->real]) (M:posreal, ak:sequence[real]):
bool =
  FORALL(x:real| abs(x-c0) < M):
  convergent?(powerseries(ak)(x-c0)) AND
  f(x) = inf_sum(powerseq(ak,x-c0)),
```


j.tanner.slagel@nasa.gov

Real Analytic Functions

Function $f : \mathbb{R} \to \mathbb{R}$ is real analytic at $c_0 \in D$:

$$\exists \{a_k\}_{k=0}^{\infty},\, r \in \mathbb{R}_{>0} \text{ s.t. } f(x) = \sum_{k=0}^{\infty} a_k \left(x - c_0\right)^k \qquad \forall x \in (c_0 - r, c_0 + r)\,.$$

Sequence $\{a_k\}$ and real number r are defined by the predicate

```
analytic_parts?(c0:real,f:[real->real]) (M:posreal, ak:sequence[real]):
bool =
  FORALL(x:real| abs(x-c0) < M):
  convergent?(powerseries(ak)(x-c0)) AND
  f(x) = inf_sum(powerseq(ak,x-c0)),

analytic?(c0:real)(f:[real -> real]):  bool =
  EXISTS(r:posreal, ak:sequence[real]):
  analytic_parts?(c0,f)(r,ak).
```


j.tanner.slagel@nasa.gov

Formally verified properties of real analytic functions

The following properties of real analytic function where shown:

- Sum of two analytic functions is analytic
- Constant multiple of an analytic function is analytic
- Product of two analytic functions is analytic:

$$(f \cdot g)(x) = \sum_{k=0}^{\infty} \mathit{conv}(k, a, b)(x - c_0)^k$$

where

$$\mathit{conv}(k, a, b) = \sum_{i=0}^{k} a_i b_{k-1}$$

- non-negative power of analytic function is analytic

j.tanner.slagel@nasa.gov

Smooth vs. Analytic

For real functions, analytic is a stronger condition than smooth (infinity differentiable) :

$$sm(x) = \begin{cases} e^{-1/x}\sin(1/x) & x > 0 \\ 0 & x \leq 0. \end{cases}$$

$$\lim_{x \to 0} sm^{(n)}(x) = 0,$$

was challenging.

j.tanner.slagel@nasa.gov

Smooth vs. Analytic

For real functions, analytic is a stronger condition than smooth (infinity differentiable) :

$$sm(x) = \begin{cases} e^{-1/x}\sin(1/x) & x > 0 \\ 0 & x \leq 0. \end{cases}$$

sm is smooth: For every $n \in \mathbb{N}$

$$sm^{(n)}(x) = \begin{cases} \frac{e^{-1/x}(p_n(x)\sin(1/x)+q_n(x)\cos(1/x))}{x^{2n}} & x > 0 \\ 0 & x \leq 0. \end{cases}$$

For some polynomials p_n and q_n. NASALib does not have L'Hôpital's rule, therefore

$$\lim_{x\to 0} sm^{(n)}(x) = 0,$$

was challenging.

j.tanner.slagel@nasa.gov

Smooth not analytic continued

For real functions, analytic is a stronger condition than smooth (infinity differentiable) :

$$sm(x) = \begin{cases} e^{-1/x}\sin(1/x) & x > 0 \\ 0 & x \leq 0. \end{cases}$$

sm is not analytic at zero. If it was there is some M such that for $x \in (-M, M)$,

$$sm(x) = \sum_{k=1}^{\infty} \frac{sm^{(k)}(0)}{k!} x^k = 0$$

j.tanner.slagel@nasa.gov

Smooth not analytic continued

For real functions, analytic is a stronger condition than smooth (infinity differentiable) :

$$sm(x) = \begin{cases} e^{-1/x}\sin(1/x) & x > 0 \\ 0 & x \leq 0. \end{cases}$$

sm is not analytic at zero. If it was there is some M such that for $x \in (-M, M)$,

$$sm(x) = \sum_{k=1}^{\infty} \frac{sm^{(k)}(0)}{k!} x^k = 0$$

Choose $x_n = \frac{2}{\pi(4n+1)}$, $sm(x_n) \neq 0$

j.tanner.slagel@nasa.gov

Outline

- Motivation
- Formalization of Semi-algebraic Sets
  - Multivariate polynomials
  - Semi-algebraic sets
- Formalization of Real Analytic Functions
  - Real analytic vs. smooth
- Formalization of Real Analytic Functions with SA Sets
  - Behavior on the boundary
  - Replacing real analytic with smooth
- Conclusions and Future Work

j.tanner.slagel@nasa.gov

Semi-algebraic Sets and Real Analytic Functions

Lemma

For a function $f : D \to \mathbb{R}^n$, real analytic at a point $c_0 \in \mathbb{R}$, the following statements are true

1. *For any monomial $m : \mathbb{R}^n \to \mathbb{R}$. the composition $m \circ f$ is real analytic.*
2. *Furthermore, for any polynomial $p : \mathbb{R}^n \to R$, the composition $p \circ f$ is real analytic.*

For part 1, this was done using the recursion, for a monomial $m : \mathbb{R}^n \to \mathbb{R}$ and $f : \mathbb{R} \to \mathbb{R}^n$,

$$m \circ f(x) = (\hat{m} \circ \hat{f}(x)) \cdot (c(f_0(x))^k)$$

1. c is coefficient of the monomial m
2. f_0 original function f projected on first entry
3. $\hat{m} : \mathbb{R}^{n-1} \to \mathbb{R}$ original monomial m projected on the last $n-1$ entries
4. $\hat{f} : \mathbb{R} \to \mathbb{R}^{n-1}$ original function f projected on the last $n-1$ entries

j.tanner.slagel@nasa.gov

Clean Exit

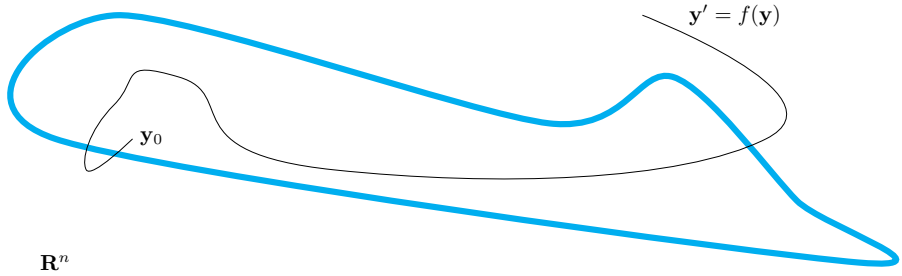
Theorem

For a connected $D \subset \mathbb{R}$, a function $f : D \to \mathbb{R}^n$, that is real analytic on D, a SA set $S(\varphi)$, and a $x_0 \in \mathbb{R}$ such that $f(x_0) \in S(\varphi)$. Then one of the following cases is true

1. $f(x) \in S(\varphi)$ *for all* $x \geq x_0$,
2. *for* $x^* = \inf\{x \in D | x > x_0, f(x) \notin S(\varphi)\}$, $f(x^*) \notin S(\varphi)$, *and there exists an* ϵ *such that* $f(x^* + t) \in S(\varphi)$ *for all* $0 < t < \epsilon$, *or*
3. *for* $x^* = \inf\{x \in D | x > x_0, f(x) \notin S(\varphi)\}$, *there exists an* ϵ *such that* $f(x^* + t) \notin S(\varphi)$ *for all* $0 < t < \epsilon$.

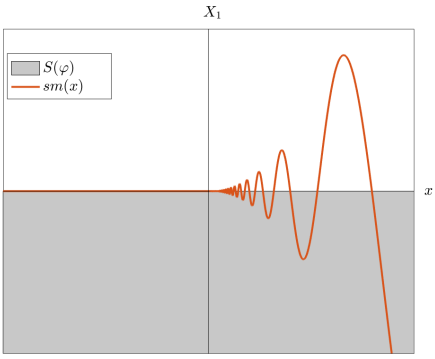
j.tanner.slagel@nasa.gov

Clean Exit continued



j.tanner.slagel@nasa.gov

Smooth is not strong enough




```
not_clean_exit:  LEMMA
  inf({xx:real |
  NOT SA((:  sm(xx) :))}) = 0
  AND
  EXISTS(xn,yn:sequence[real]):
    convergence(xn,0) AND
    convergence(yn,0) AND
    FORALL(i:nat):
      SA((:  sm(xn(i)) :))  AND
      xn(i) > 0 AND
      NOT SA((:  sm(yn(i)) :)  )  AND
      yn(i) > 0
```


j.tanner.slagel@nasa.gov

Outline

- Motivation
- Formalization of Semi-algebraic Sets
  - Multivariate polynomials
  - Semi-algebraic sets
- Formalization of Real Analytic Functions
  - Real analytic vs. smooth
- Formalization of Real Analytic Functions with SA Sets
  - Behavior on the boundary
  - Replacing real analytic with smooth
- Conclusions and Future Work

j.tanner.slagel@nasa.gov

Conclusion and Future Work

In PVS, formalized:

- Multivariate polynomials and semi-algebraic sets
- Real analytic functions
- Behavior of real analytic functions on boundary of semi-algebraic sets

Future work:

- Multivariate polynomials over arbitrary ring
- Allow conditional statement PVS atomic polynomial formula
- Theory of differential equations in PVS (when is the solution real analytic?)

j.tanner.slagel@nasa.gov

Conclusion and Future Work

In PVS, formalized:

- Multivariate polynomials and semi-algebraic sets
- Real analytic functions
- Behavior of real analytic functions on boundary of semi-algebraic sets

Future work:

- Multivariate polynomials over arbitrary ring
- Allow conditional statement PVS atomic polynomial formula
- Theory of differential equations in PVS (when is the solution real analytic?)

Thanks for listening! Questions?

j.tanner.slagel@nasa.gov