Inner approximated reachability analysis

Eric Goubault, Michel Kieffer, Olivier Mullier and Sylvie Putot

LIX & L2S - CNRS - Supélec - Univ Paris-Sud

November 24th, 2015

Reachability of dynamical systems - central to program analysis, control theory

- Outer approximation: safety proof (but "false alarms" ?)
- Inner approximation: property falsification
- Combined inner and outer approximations: indication of the precision of estimates

In this talk

- Inner approximation of $f : \mathbb{R}^n \to \mathbb{R}^p$ using:
  - modal intervals and Kaucher arithmetic ($f : \mathbb{R}^n \to \mathbb{R}$)
  - generalized mean value theorem
  - zonotopes for Jacobian outer approximation ($f : \mathbb{R}^n \to \mathbb{R}^p$)
- Applications to numerical schemes and dynamical systems analysis

This can also be applied to outer-approximation (although we have already the "usual" zonotopic approximation, that we recap a bit ; and to invariant calculations.

Related work

Outer approximation has become classical

Intervals, zonotopes, support functions, ellipsoids etc.

Inner approximation is much more difficult

- Linear case [Kurzhanski-Varaiya HSCC 2000, Althoff et al. CDC 2007, Kanade et al. CAV 2009]
- Simulation-based local inner approximations [Nghiem et al. HSCC 2010]
- Box bisections [Goldsztejn-Jaulin Reliable Computing 2010, Mullier-Goubault-Kieffer-Putot RC 2013]
- Parallelepipeds [Goldsztejn-Hayes SCAN 2006]
- Order 0 generalized affine forms [Goubault-Putot SAS 2007]

Intervals, outer and inner approximations

Intervals: closed connected subsets of $\mathbb{R}$, noted $[x] \in \mathbb{I}$

We would like to compute $\text{range}(f, [x]) = \{f(x), x \in [x]\}$.

Outer (or over) approximation

- An *outer approximating extension* of $f : \mathbb{R}^n \to \mathbb{R}$ over intervals is $[f] : \mathbb{I}^n \to \mathbb{I}$ such that

$$\forall [x] \in \mathbb{I}^n, \text{range}(f, [x]) \subseteq [z] = [f]([x])$$

- Natural interval extension: replacing real by interval operations in function f.

Example: the extension of $f(x) = x^2 - x$ on $[2, 3]$ is $[f]([2, 3]) = [2, 3]^2 - [2, 3] = [1, 7]$, and can be interpreted as

$$(\forall x \in [2, 3])\,(\exists z \in [1, 7])\,(f(x) = z).$$

Inner (or under) approximation

An interval inner approximation $[z] \in \mathbb{I}$ satisfies $[z] \subseteq \text{range}(f, [x])$ of the range of f over $[x]$, can be interpreted as

$$(\forall z \in [z])\,(\exists x \in [x])\,(f(x) = z).$$

Generalized intervals for outer and inner approximations

Generalized intervals

- Intervals whose bounds are not ordered $\mathbf{K} = \{[a, b],\ a \in \mathbb{R}, b \in \mathbb{R}\}$
- Called proper if $a \leq b$, else improper

Definition (Following Goldsztejn et al. 2005)

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a continuous function and $[x] \in \mathbf{K}^n$, decomposed in $[x]_{\mathcal{A}} \in \mathbf{I}^p$ and $[x]_{\mathcal{E}} \in (\text{dual } \mathbf{I})^q$ with $p + q = n$. A generalized interval $[z] \in \mathbf{K}$ is $(f, [x])$-interpretable if

$$(\forall x_{\mathcal{A}} \in [x]_{\mathcal{A}})\,(Q_z z \in \text{pro }[z])\,(\exists x_{\mathcal{E}} \in \text{pro }[x]_{\mathcal{E}}), (f(x) = z)$$

where $Q_z = \exists$ if $[z]$ is proper, and $Q_z = \forall$ if $[z]$ is improper.

- When all intervals are proper, we get classical interval computation and an outer approximation of range$(f, \mathbf{x})$

$$(\forall x \in [x])\,(\exists z \in [z])\,(f(x) = z).$$

- When all intervals are improper, we get an inner approximation of range$(f, [x])$

$$(\forall z \in \text{pro }[z])\,(\exists x \in \text{pro }[x])\,(f(x) = z).$$

Kaucher arithmetic [Kaucher 1980] on generalized intervals

Kaucher addition extends addition on classical intervals:
$[x] + [y] = [\underline{x} + \underline{y}, \overline{x} + \overline{y}]$ and $[x] - [y] = [\underline{x} - \overline{y}, \overline{x} - \underline{y}]$.

Kaucher multiplication

Let $\mathcal{P} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \geqslant 0 \wedge \overline{x} \geqslant 0\}$, $-\mathcal{P} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \leqslant 0 \wedge \overline{x} \leqslant 0\}$,
$\mathcal{Z} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \leqslant 0 \leqslant \overline{x}\}$, and dual $\mathcal{Z} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \geqslant 0 \geqslant \overline{x}\}$.

$[x] \times [y]$	$[y] \in \mathcal{P}$	$\mathcal{Z}$	$-\mathcal{P}$	dual$\mathcal{Z}$
$[x] \in \mathcal{P}$	$[\underline{x}\underline{y}, \overline{x}\overline{y}]$	$[\overline{x}\underline{y}, \overline{x}\overline{y}]$	$[\overline{x}\underline{y}, \underline{x}\overline{y}]$	$[\underline{x}\underline{y}, \underline{x}\overline{y}]$
$\mathcal{Z}$	$[\underline{x}\overline{y}, \overline{x}\overline{y}]$	$[\min(\underline{x}\overline{y}, \overline{x}\underline{y}), \max(\underline{x}\underline{y}, \overline{x}\overline{y})]$	$[\overline{x}\underline{y}, \underline{x}\underline{y}]$	0
$-\mathcal{P}$	$[\underline{x}\overline{y}, \overline{x}\underline{y}]$	$[\underline{x}\overline{y}, \underline{x}\underline{y}]$	$[\overline{x}\overline{y}, \underline{x}\underline{y}]$	$[\overline{x}\overline{y}, \overline{x}\underline{y}]$
dual$\mathcal{Z}$	$[\underline{x}\underline{y}, \overline{x}\underline{y}]$	0	$[\overline{x}\overline{y}, \underline{x}\overline{y}]$	$[\max(\underline{x}\underline{y}, \overline{x}\overline{y}), \min(\underline{x}\overline{y}, \overline{x}\underline{y})]$

Interpretation of Kaucher arithmetic, Goldsztejn et al. 2005

Let $f : \mathbb{R}^n \to \mathbb{R}$ be given by an arithmetic expression with single occurrences of variables. Then for $[x] \in \mathbf{K}^n$, $f([x])$, computed using Kaucher arithmetic, is $(f, [x])$-interpretable.

UNIVERSITÉ PARIS-SACLAY

Kaucher arithmetic [Kaucher 1980] on generalized intervals

Kaucher addition extends addition on classical intervals:
$[x] + [y] = [\underline{x} + \underline{y}, \overline{x} + \overline{y}]$ and $[x] - [y] = [\underline{x} - \overline{y}, \overline{x} - \underline{y}]$.

Kaucher multiplication

Let $\mathcal{P} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \geqslant 0 \wedge \overline{x} \geqslant 0\}$, $-\mathcal{P} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \leqslant 0 \wedge \overline{x} \leqslant 0\}$,
$\mathcal{Z} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \leqslant 0 \leqslant \overline{x}\}$, and dual $\mathcal{Z} = \{[x] = [\underline{x}, \overline{x}],\ \underline{x} \geqslant 0 \geqslant \overline{x}\}$.

$[x] \times [y]$	$[y] \in \mathcal{P}$	$\mathcal{Z}$	$-\mathcal{P}$	dual$\mathcal{Z}$
$[x] \in \mathcal{P}$	$[\underline{x}\underline{y}, \overline{x}\overline{y}]$	$[\overline{x}\underline{y}, \overline{x}\overline{y}]$	$[\overline{x}\underline{y}, \underline{x}\overline{y}]$	$[\underline{x}\underline{y}, \underline{x}\overline{y}]$
$\mathcal{Z}$	$[\underline{x}\overline{y}, \overline{x}\overline{y}]$	$[\min(\underline{x}\overline{y}, \overline{x}\underline{y}), \max(\underline{x}\underline{y}, \overline{x}\overline{y})]$	$[\overline{x}\underline{y}, \underline{x}\underline{y}]$	0
$-\mathcal{P}$	$[\underline{x}\overline{y}, \overline{x}\underline{y}]$	$[\underline{x}\overline{y}, \underline{x}\underline{y}]$	$[\overline{x}\overline{y}, \underline{x}\underline{y}]$	$[\overline{x}\overline{y}, \overline{x}\underline{y}]$
dual$\mathcal{Z}$	$[\underline{x}\underline{y}, \overline{x}\underline{y}]$	0	$[\overline{x}\overline{y}, \underline{x}\overline{y}]$	$[\max(\underline{x}\underline{y}, \overline{x}\overline{y}), \min(\underline{x}\overline{y}, \overline{x}\underline{y})]$

Interpretation of Kaucher arithmetic, Goldsztejn et al. 2005

Let $f : \mathbb{R}^n \to \mathbb{R}$ be given by an arithmetic expression with single occurrences of variables. Then for $[x] \in \mathbf{K}^n$, $f([x])$, computed using Kaucher arithmetic, is $(f, [x])$-interpretable.

Example: $[z] = [x] \times [y] = 0$ when $[x] \in \mathcal{Z}$ and $[y] \in$ dual $\mathcal{Z}$

Example: Kaucher multiplication

Example (Interpretation of the Kaucher multiplication in the case $\mathcal{Z} \times$ dual $\mathcal{Z}$)

$[z] = [x] \times [y] = 0$ when $[x] \in \mathcal{Z} = \{[x],\ \underline{x} \leqslant 0 \leqslant \overline{x}\}$ (e.g. [-5,4]) and
$[y] \in$ dual $\mathcal{Z} = \{[x],\ \underline{x} \geqslant 0 \geqslant \overline{x}\}$ (e.g. [1,-1]).

Definition (reminder)

Let $f : \mathbb{R}^n \to \mathbb{R}$ and $[x] \in \mathbf{K}^n$, which we can decompose in $[x]_{\mathcal{A}} \in \mathbf{I}^p$ and $[x]_{\mathcal{E}} \in (\text{dual } \mathbf{I})^q$ with $p + q = n$. A generalized interval $[z] \in \mathbf{K}$ is $(f, [x])$-interpretable if

$$(\forall x_{\mathcal{A}} \in [x]_{\mathcal{A}})\,(Q_z z \in \text{pro } [z])\,(\exists x_{\mathcal{E}} \in \text{pro } [x]_{\mathcal{E}}), (f(x) = z)$$

where $Q_z = \exists$ if $[z]$ is proper, and $Q_z = \forall$ otherwise.

Example: Kaucher multiplication

Example (Interpretation of the Kaucher multiplication in the case $\mathcal{Z} \times$ dual $\mathcal{Z}$)

$[z] = [x] \times [y] = 0$ when $[x] \in \mathcal{Z} = \{[x],\ \underline{x} \leqslant 0 \leqslant \overline{x}\}$ (e.g. [-5,4]) and $[y] \in$ dual $\mathcal{Z} = \{[x],\ \underline{x} \geqslant 0 \geqslant \overline{x}\}$ (e.g. [1,-1]).

Definition (reminder)

Let $f : \mathbb{R}^2 \to \mathbb{R}$ and $[x] \in \mathbf{I}$ and $[y] \in (\text{dual } \mathbf{I})$. A generalized interval $[z] \in \mathbf{K}$ is $(f, [x] \times [y])$-interpretable if

$$(\forall x \in [x])\,(Q_z z \in \text{pro } [z])\,(\exists y \in [y]), (f(x,y) = x \times y = z)$$

where $Q_z = \exists$ if $[z]$ is proper, and $Q_z = \forall$ otherwise.

Example: Kaucher multiplication

Example (Interpretation of the Kaucher multiplication in the case $\mathcal{Z} \times$ dual $\mathcal{Z}$)

$[z] = [x] \times [y] = 0$ when $[x] \in \mathcal{Z} = \{[x],\ \underline{x} \leqslant 0 \leqslant \overline{x}\}$ (e.g. [-5,4]) and $[y] \in$ dual $\mathcal{Z} = \{[x],\ \underline{x} \geqslant 0 \geqslant \overline{x}\}$ (e.g. [1,-1]).

Definition (reminder)

Let $f : \mathbb{R}^2 \to \mathbb{R}$ and $[x] \in \mathbf{I}$ and $[y] \in (\text{dual } \mathbf{I})$. A generalized interval $[z] \in \mathbf{K}$ is $(f, [x] \times [y])$-interpretable if

$$(\forall x \in [x])\,(\forall z \in \text{pro } [z])\,(\exists y \in [y]),(f(x,y) = x \times y = z)$$

where $Q_z = \exists$ if $[z]$ is proper, and $Q_z = \forall$ otherwise.

Let us suppose $[z]$ improper:

- computing $[z] = [x] \times [y]$ consists in finding $[z]$ such that $\forall x \in [x]$, $\forall z \in$ pro $[z]$, $\exists y \in$ pro $[y]$, $z = x \times y$;
- instanciating the property for $0 \in [x]$, we get $\forall z \in$ pro $[z]$, $(\exists y \in$ pro $[y])$ $z = 0$. Thus $[z]$ is necessarily 0.

Limitations of Kaucher and interval arithmetic

Kaucher arithmetic defines a generalized interval natural extension :

- Interpretable as outer approximation when all intervals are proper (interval arithmetic), but may be insufficiently accurate because of *dependency problem*
- Interpretable as inner approximation when all intervals are proper and f is given by an arithmetic expression *with single occurences of variables*

Example (dependency problem in outer approximation)

Let $f(x) = x - x$, then $[f]([-1,1]) = [-1,1] - [-1,1] = [-2,2]$

Example (single-occurence limitation in inner approximation)

Let $f(x) = x^2 - x$, we want an inner approximation of $\text{range}(f,[2,3])$. But due to the two occurrences of x, $f([3,2])$ with Kaucher arithmetic is not $(f,[x])$-interpretable.

A solution: mean-value theorem & affine arithmetic

Affine arithmetic (outer-approximation by zonotopes)

Affine form

For a quantity x :

$$\hat{x} = x_0 + \sum_{i=1}^{n} x_i \varepsilon_i, \quad \text{where } \forall i, x_i \in \mathbb{R} \text{ and } \varepsilon_i \in [-1, 1].$$

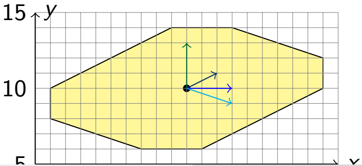
$\hat{x}$ takes its value in $\left[x_0 - \sum_{i=1}^{n} |x_i|, x_0 + \sum_{i=1}^{n} |x_i|\right]$.

Zonotopes (joint range of affine forms)

Several forms for quantities x_i, sharing common noise symbols ε_j:

$$\hat{x}^i = x_0^i + x_1^i \varepsilon_1 + \ldots + x_n^i \varepsilon_n,$$

$$\begin{aligned} \hat{x} &= 20 - 4\varepsilon_1 + 2\varepsilon_3 + 3\varepsilon_4 \\ \hat{y} &= 10 - 2\varepsilon_1 + \varepsilon_2 - \varepsilon_4 \end{aligned}$$



Affine arithmetic (outer-approximation by zonotopes)

Assignment $x := [a, b]$

Centered form using a fresh noise symbol $\varepsilon_{n+1} \in [-1, 1]$,

$$\hat{x} = \frac{(a+b)}{2} + \frac{(b-a)}{2}\,\varepsilon_{n+1}.$$

Affine operations (interpreted exactly; no new noise symbol)

For $\lambda \in \mathbb{R}$, we have

$$\lambda\hat{x} + \hat{y} = (\lambda x_0 + y_0) + \sum_{i=1}^{n}(\lambda x_i + y_i)\varepsilon_i.$$

Multiplication

Possible (simple) version of the multiplication (note the η_1 noise symbol):

$$\hat{x}\hat{y} = x_0 y_0 + \sum_{i=1}^{n}(x_i y_0 + y_i x_0)\,\varepsilon_i + \frac{1}{2}\sum_{1\leqslant i,j\leqslant n} |\, x_i y_j + x_j y_i \,|\, \eta_1.$$

(and similar "linearizations" of non-linear operations)

Generalized mean-value theorem

- To each component $[x]_i$, $i = 1, \ldots, n$ of the input box $[x] \in \mathbf{K}^n$, associate ε_i, by

$$\hat{x}_i(\varepsilon_i) = \frac{\underline{x}_i + \overline{x}_i}{2} + \frac{\overline{x}_i - \underline{x}_i}{2}\varepsilon_i, \text{ where } [x]_i = [\underline{x}_i, \overline{x}_i]$$

- Derive f^ε of the vector $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n)$ from $f : \mathbb{R}^n \to \mathbb{R}$, for some input $[x] \in \mathbf{K}^n$.

Generalized mean-value theorem

Let $f : \mathbb{R}^n \to \mathbb{R}$ be differentiable, $[x] \in \mathbf{K}^n$. Suppose $\left\{ \frac{\partial f^\varepsilon}{\partial \varepsilon_i}(\varepsilon),\ \varepsilon \in [-1, 1]^n \right\} \sqsubseteq [\Delta_i]$.
Then, $\forall (t_1, \ldots, t_n) \in \text{pro } \boldsymbol{\varepsilon} = [-1, 1]^n$,

$$\tilde{f}^\varepsilon([\varepsilon_1], \ldots, [\varepsilon_n]) = f^\varepsilon(t_1, \ldots, t_n) + \sum_{i=1}^{n} [\Delta_i]([\varepsilon_i] - t_i),$$

is $(f, [x])$-interpretable. In particular,

- if $\tilde{f}^\varepsilon([1, -1]^n)$, computed with Kaucher arithmetic, is improper, then pro $\tilde{f}^\varepsilon([1, -1]^n)$ is an inner approximation of $\{f^\varepsilon(\varepsilon),\ \varepsilon \in [-1, 1]^n\} = \text{range}(f, [x])$.
- if $\tilde{f}^\varepsilon([-1, 1]^n)$ is proper, then it is an outer approximation of $\text{range}(f, [x])$.

Generalized affine forms and inner range computation

Generalized affine forms

- The generalized mean-value theorem defines generalized affine forms: for $f : \mathbb{R}^n \to \mathbb{R}$,

$$f^{\varepsilon}(t_1, \ldots, t_n) + \sum_{i=1}^{n} [\Delta_i]([\varepsilon_i] - t_i),$$

  where $\left\{ \frac{\partial f^{\varepsilon}}{\partial \varepsilon_i}(\varepsilon),\ \varepsilon \in [-1, 1]^n \right\} \sqsubseteq [\Delta_i]$.
- We want an inductive computation of these forms on arithmetic expressions

Generalized affine forms

- The generalized mean-value theorem defines generalized affine forms: for $f : \mathbb{R}^n \to \mathbb{R}$,

$$f^\varepsilon(t_1, \ldots, t_n) + \sum_{i=1}^{n} [\Delta_i]([\varepsilon_i] - t_i),$$

  where $\left\{ \frac{\partial f^\varepsilon}{\partial \varepsilon_i}(\varepsilon),\ \varepsilon \in [-1,1]^n \right\} \sqsubseteq [\Delta_i]$.
- We want an inductive computation of these forms on arithmetic expressions

Order 0 forms (SAS 2007)

- The partial derivatives $[\Delta_i]$ are evaluated with intervals
- Example: $f(x) = x^2 - x$, $x \in [2,3]$, thus $f^\varepsilon(\epsilon_1) = (2.5 + 0.5\varepsilon_1)^2 - (2.5 + 0.5\varepsilon_1)$. We get $\tilde{f}^\varepsilon(\varepsilon_1) = 3.75 + [1.5, 2.5]\varepsilon_1$, that can be interpreted as:

$$pro(3.75 + [1.5, 2.5][1, -1]) \subseteq f([-1, 1]) \subseteq 3.75 + [1.5, 2.5][-1, 1]$$

Generalized affine forms and inner range computation

Generalized affine forms

- The generalized mean-value theorem defines generalized affine forms: for $f : \mathbb{R}^n \to \mathbb{R}$,

$$f^{\varepsilon}(t_1, \ldots, t_n) + \sum_{i=1}^{n} [\Delta_i]([\varepsilon_i] - t_i),$$

where $\left\{ \frac{\partial f^{\varepsilon}}{\partial \varepsilon_i}(\varepsilon),\ \varepsilon \in [-1, 1]^n \right\} \sqsubseteq [\Delta_i]$.

- We want an inductive computation of these forms on arithmetic expressions

Order 0 forms (SAS 2007)

- The partial derivatives $[\Delta_i]$ are evaluated with intervals
- Example: $f(x) = x^2 - x$, $x \in [2, 3]$, thus $f^{\varepsilon}(\epsilon_1) = (2.5 + 0.5\varepsilon_1)^2 - (2.5 + 0.5\varepsilon_1)$. We get $\tilde{f}^{\varepsilon}(\varepsilon_1) = 3.75 + [1.5, 2.5]\varepsilon_1$, that can be interpreted as:

$$pro(3.75 + [1.5, -1.5]) \subseteq f([-1, 1]) \subseteq 3.75 + [-2.5, 2.5]$$

Generalized affine forms and inner range computation

Generalized affine forms

- The generalized mean-value theorem defines generalized affine forms: for $f : \mathbb{R}^n \to \mathbb{R}$,

$$f^{\varepsilon}(t_1, \ldots, t_n) + \sum_{i=1}^{n} [\Delta_i]([\varepsilon_i] - t_i),$$

where $\left\{ \frac{\partial f^{\varepsilon}}{\partial \varepsilon_i}(\varepsilon),\ \varepsilon \in [-1,1]^n \right\} \sqsubseteq [\Delta_i]$.

- We want an inductive computation of these forms on arithmetic expressions

Order 0 forms (SAS 2007)

- The partial derivatives $[\Delta_i]$ are evaluated with intervals
- Example: $f(x) = x^2 - x$, $x \in [2,3]$, thus $f^{\varepsilon}(\epsilon_1) = (2.5 + 0.5\varepsilon_1)^2 - (2.5 + 0.5\varepsilon_1)$. We get $\tilde{f}^{\varepsilon}(\varepsilon_1) = 3.75 + [1.5, 2.5]\varepsilon_1$, that can be interpreted as:

$$pro([5.25, 4.25]) \subseteq f([-1,1]) \subseteq [1.25, 6.25]$$

Generalized affine forms and inner range computation

Generalized affine forms

- The generalized mean-value theorem defines generalized affine forms: for $f : \mathbb{R}^n \to \mathbb{R}$,

$$f^{\varepsilon}(t_1, \ldots, t_n) + \sum_{i=1}^{n} [\Delta_i]([\varepsilon_i] - t_i),$$

where $\left\{ \frac{\partial f^{\varepsilon}}{\partial \varepsilon_i}(\varepsilon),\ \varepsilon \in [-1,1]^n \right\} \sqsubseteq [\Delta_i]$.

- We want an inductive computation of these forms on arithmetic expressions

Order 0 forms (SAS 2007)

- The partial derivatives $[\Delta_i]$ are evaluated with intervals
- Example: $f(x) = x^2 - x$, $x \in [2,3]$, thus $f^{\varepsilon}(\epsilon_1) = (2.5 + 0.5\varepsilon_1)^2 - (2.5 + 0.5\varepsilon_1)$. We get $\tilde{f}^{\varepsilon}(\varepsilon_1) = 3.75 + [1.5, 2.5]\varepsilon_1$, that can be interpreted as:

$$[4.25, 5.25] \subseteq f([-1,1]) \subseteq [1.25, 6.25]$$

- Solves the single-occurence limitation but not quite the dependency problem

Generalized affine forms and inner range computation

Generalized affine forms

- The generalized mean-value theorem defines generalized affine forms: for $f : \mathbb{R}^n \to \mathbb{R}$,

$$f^{\varepsilon}(t_1, \ldots, t_n) + \sum_{i=1}^{n} [\Delta_i]([\varepsilon_i] - t_i),$$

where $\left\{ \frac{\partial f^{\varepsilon}}{\partial \varepsilon_i}(\varepsilon),\ \varepsilon \in [-1,1]^n \right\} \sqsubseteq [\Delta_i]$.

- We want an inductive computation of these forms on arithmetic expressions

Here, order 1 generalized affine forms

- Inductive computations with zonotopic outer-approximations of quantities and partial derivatives Δ_i : more precise that order 0
- When computing the inner range of a scalar function as above, we use only the interval range $[\Delta_i]$
- But in general we have $f : \mathbb{R}^n \to \mathbb{R}^p$ and thus vectors of generalized affine forms
- Order 1 forms code some dependency between the components of f or f^{ε} : allows us to define joint inner range (see end of talk)

First-order generalized affine vectors

Definition (first-order generalized vector)

A first-order generalized affine vector for $x = (x_1, \ldots, x_p)$ is a triple $(Z, c, J) \in \mathcal{M}(n+m+1, p) \times \mathbb{R}^p \times (\mathcal{M}(n,p))^{n+m+1}$:

- Column k of $Z = {}^t(Z_0 Z_\varepsilon Z_\eta)$ describes the affine form outer-approximating x_k
- c is the center
- Element $j_{i,k}$ of $J = {}^t(J_0 J_\varepsilon J_\eta)$ describes the affine form outer-approximating $\frac{\partial x^k}{\partial \varepsilon_i}$ (one of the previous Δ_i: column k of J is an affine vector over-approximating $\frac{\partial x}{\partial \varepsilon_i}$)

Property

With matrix notations, a first-order generalized affine vector $(Z, c, J) \in \mathcal{M}(n+m+1, p) \times \mathbb{R}^p \times (\mathcal{M}(n,p))^{n+m+1}$ *abstracts* $f : \mathbb{R}^n \to \mathbb{R}^p$*, if* $c = f^\varepsilon(0)$ *and*

$$(\forall \varepsilon \in [\varepsilon])\,(\exists \eta \in [\eta]), \begin{cases} f^\varepsilon(\varepsilon) = {}^tZ_0 + {}^tZ_\varepsilon \varepsilon + {}^tZ_\eta \eta \\ \frac{\partial f^\varepsilon}{\partial \varepsilon_i}(\varepsilon) = {}^tJ_{i,0} + {}^tJ_{i,\varepsilon}\varepsilon + {}^tJ_{i,\eta}\eta, \forall i = 1, \ldots, n \end{cases} \quad (1)$$

(Z, c, J) defines a simultaneous outer approximation of $f^\varepsilon(\varepsilon)$ and $(\frac{\partial f^\varepsilon}{\partial \varepsilon_i})_i(\varepsilon)$, relying on the same parametrization in the ε and η noise symbols.

École Polytechnique, Université Paris-Saclay

Inductive construction of a sound abstraction: assignment

We now want to inductively build a sound abstraction of any arithmetic expression.

Example: Consider assignments $x_1 := [2,3]$ and $x_2 := [3,4]$.

- The affine forms outer approximating x_1 and x_2 are $\hat{x}_1 = \frac{5}{2} + \frac{1}{2}\varepsilon_1$ and $\hat{x}_2 = \frac{7}{2} + \frac{1}{2}\varepsilon_2$, thus
$$Z = \begin{pmatrix} \frac{5}{2} + \frac{1}{2}\varepsilon_1 & \frac{7}{2} + \frac{1}{2}\varepsilon_2 \end{pmatrix}$$
- The centers are $c = \begin{pmatrix} \frac{5}{2} & \frac{7}{2} \end{pmatrix}$.
- The Jacobian over-approximation is $J = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$

Assignment $f'_{p+1} := [a,b]$ with $a < b$ and corresponding new noise symbol ε_i

If (Z, c, J) abstracts $f : \mathbb{R}^n \to \mathbb{R}^p$, an abstraction of $f' = (f, f'_{p+1} := [a,b]) : \mathbb{R}^n \to \mathbb{R}^{p+1}$ is

$$\begin{cases} Z' & = \begin{pmatrix} Z & \frac{a+b}{2} + \frac{b-a}{2}\varepsilon_i \end{pmatrix} \\ c' & = \begin{pmatrix} c & \frac{a+b}{2} \end{pmatrix} \\ J' & = \begin{pmatrix} & 0 \\ J & \frac{b-a}{2} \\ & 0 \end{pmatrix} \leftarrow i\text{-th line} \end{cases}$$

Inductive construction of a sound abstraction: affine operations

Example (Consider now $x_3 := 3x_1 - x_2$)

- The outer approx. of quantities x_i are $Z = \begin{pmatrix} \frac{5}{2} + \frac{1}{2}\varepsilon_1 & \frac{7}{2} + \frac{1}{2}\varepsilon_2 & 4 + \frac{3}{2}\varepsilon_1 - \frac{1}{2}\varepsilon_2 \end{pmatrix}$
- The centers are $c = \begin{pmatrix} \frac{5}{2} & \frac{7}{2} & 4 \end{pmatrix}$.
- The Jacobian is $J = \begin{pmatrix} \frac{1}{2} & 0 & \frac{3}{2} \\ 0 & \frac{1}{2} & \frac{-1}{2} \end{pmatrix}$

Affine operations $f' = (f, f'_{p+1} := \lambda_1 f_i + \lambda_2 f_j) : \mathbb{R}^n \to \mathbb{R}^{p+1}$, where $(\lambda_1, \lambda_2) \in \mathbb{R}^2$

$$\begin{cases} Z' = \begin{pmatrix} Z & \lambda_1 \hat{z}_i + \lambda_2 \hat{z}_j \end{pmatrix} \\ c' = \begin{pmatrix} c & \lambda_1 c_i + \lambda_2 c_j \end{pmatrix} \\ J' = \begin{pmatrix} & \lambda_1 \hat{j}_{1,i} + \lambda_2 \hat{j}_{1,j} \\ J & \vdots \\ & \lambda_1 \hat{j}_{n,i} + \lambda_2 \hat{j}_{n,j} \end{pmatrix} \end{cases}$$

Affine operations are exact.

Inductive construction of a sound abstraction: multiplication

Example (Consider now $x_4 := x_1 x_3$)

- Values $\hat{x}_4 = 10 + \frac{23}{4}\varepsilon_1 - \frac{5}{2}\varepsilon_2 + [-\frac{1}{4}, 1] = \frac{83}{8} + \frac{23}{4}\varepsilon_1 - \frac{5}{4}\varepsilon_2 + \frac{5}{8}\eta_1$

$$Z = \begin{pmatrix} \frac{5}{2} + \frac{1}{2}\varepsilon_1 & \frac{7}{2} + \frac{1}{2}\varepsilon_2 & 4 + \frac{3}{2}\varepsilon_1 - \frac{1}{2}\varepsilon_2 & \frac{83}{8} + \frac{23}{4}\varepsilon_1 - \frac{5}{4}\varepsilon_2 + \frac{5}{8}\eta_1 \end{pmatrix}$$

- Center $c = \begin{pmatrix} \frac{5}{2} & \frac{7}{2} & 4 & 10 \end{pmatrix}$.
- Jacobian $\hat{j}_{i4} = \hat{x}_1 \hat{j}_{i3} + \hat{x}_3 \hat{j}_{i1}, i = 1, \ldots, 2$
  $\hat{j}_{14} = (\frac{5}{2} + \frac{1}{2}\varepsilon_1)\frac{3}{2} + (4 + \frac{3}{2}\varepsilon_1 - \frac{1}{2}\varepsilon_2)\frac{1}{2} = \frac{23}{4} + \frac{3}{2}\varepsilon_1 - \frac{1}{4}\varepsilon_2$

$$J = \begin{pmatrix} \frac{1}{2} & 0 & \frac{3}{2} & \frac{23}{4} + \frac{3}{2}\varepsilon_1 - \frac{1}{4}\varepsilon_2 \\ 0 & \frac{1}{2} & \frac{-1}{2} & -\frac{5}{4} - \frac{1}{4}\varepsilon_1 \end{pmatrix}$$

Multiplication $f' = (f, f'_{p+1} := f_i f_j) : \mathbb{R}^n \to \mathbb{R}^{p+1}$

$$\begin{cases} Z' = \begin{pmatrix} Z & \hat{z}_i \hat{z}_j \end{pmatrix} \\ c' = \begin{pmatrix} c & c_i c_j \end{pmatrix} \\ J' = \begin{pmatrix} & \hat{z}_j \hat{j}_{1,i} + \hat{z}_i \hat{j}_{1,j} \\ J & \vdots \\ & \hat{z}_j \hat{j}_{n,i} + \hat{z}_i \hat{j}_{n,j} \end{pmatrix} \end{cases}$$

Interpretation as an inner-approximation

$$Z = \left(\tfrac{5}{2} + \tfrac{1}{2}\varepsilon_1 \quad \tfrac{7}{2} + \tfrac{1}{2}\varepsilon_2 \quad 4 + \tfrac{3}{2}\varepsilon_1 - \tfrac{1}{2}\varepsilon_2 \quad \tfrac{83}{8} + \tfrac{23}{4}\varepsilon_1 - \tfrac{5}{4}\varepsilon_2 + \tfrac{5}{8}\eta_1 \right)$$

$$c = \left(\tfrac{5}{2} \quad \tfrac{7}{2} \quad 4 \quad 10 \right) \quad J = \begin{pmatrix} \frac{1}{2} & 0 & \frac{3}{2} & \frac{23}{4} + \frac{3}{2}\varepsilon_1 - \frac{1}{4}\varepsilon_2 \\ 0 & \frac{1}{2} & \frac{-1}{2} & -\frac{5}{4} - \frac{1}{4}\varepsilon_1 \end{pmatrix}$$

Inner-approximation of the range of $x_3(x_1, x_2)$ and $x_4(x_1, x_2)$ for $(x_1, x_2) \in [2, 3] \times [3, 4]$

$\forall k = 1 \ldots 4, pro(c_k + [\hat{j}_{1k}][1, -1] + [\hat{j}_{2k}][1, -1]) \subseteq [x_k] \subseteq c_k + [\hat{j}_{1k}][-1, 1] + [\hat{j}_{2k}] * [-1, 1])$

- Uses Kaucher multiplication rule $[x] \times [y]$ for $[y] = [1, -1] \in \text{dual } \mathcal{Z}$
- Note that if a jacobian coefficient contains zero, the corresponding multiplication is zero (rule $\mathcal{Z} \times \text{dual } \mathcal{Z} = 0$)
- Exact for x_3 (affine operations only):

$$pro(4 + \frac{3}{2}[1, -1] - \frac{1}{2}[1, -1]) \subseteq range(x_3, [2, 3] \times [3, 4]) \subseteq 4 + \frac{3}{2}[1, -1] - \frac{1}{2}[1, -1]$$

Interpretation as an inner-approximation

$$Z = \begin{pmatrix} \frac{5}{2}+\frac{1}{2}\varepsilon_1 & \frac{7}{2}+\frac{1}{2}\varepsilon_2 & 4+\frac{3}{2}\varepsilon_1-\frac{1}{2}\varepsilon_2 & \frac{83}{8}+\frac{23}{4}\varepsilon_1-\frac{5}{4}\varepsilon_2+\frac{5}{8}\eta_1 \end{pmatrix}$$

$$c = \begin{pmatrix} \frac{5}{2} & \frac{7}{2} & 4 & 10 \end{pmatrix} \quad J = \begin{pmatrix} \frac{1}{2} & 0 & \frac{3}{2} & \frac{23}{4}+\frac{3}{2}\varepsilon_1-\frac{1}{4}\varepsilon_2 \\ 0 & \frac{1}{2} & \frac{-1}{2} & -\frac{5}{4}-\frac{1}{4}\varepsilon_1 \end{pmatrix}$$

Inner-approximation of the range of $x_3(x_1,x_2)$ and $x_4(x_1,x_2)$ for $(x_1,x_2) \in [2,3]\times[3,4]$

$\forall k = 1\ldots4, pro(c_k + [\hat{j}_{1k}][1,-1] + [\hat{j}_{2k}][1,-1]) \subseteq [x_k] \subseteq c_k + [\hat{j}_{1k}][-1,1] + [\hat{j}_{2k}] * [-1,1])$

- Uses Kaucher multiplication rule $[x]\times[y]$ for $[y]=[1,-1] \in$ dual $\mathcal{Z}$
- Note that if a jacobian coefficient contains zero, the corresponding multiplication is zero (rule $\mathcal{Z} \times$ dual $\mathcal{Z} = 0$)
- Exact for x_3 (affine operations only):

$$pro(4+[\frac{3}{2},-\frac{3}{2}]+[\frac{1}{2},-\frac{1}{2}]) \subseteq range(x_3,[2,3]\times[3,4]) \subseteq 4+[-\frac{3}{2},\frac{3}{2}]+[-\frac{1}{2},\frac{1}{2}]$$

Interpretation as an inner-approximation

$$Z = \left(\tfrac{5}{2} + \tfrac{1}{2}\varepsilon_1 \quad \tfrac{7}{2} + \tfrac{1}{2}\varepsilon_2 \quad 4 + \tfrac{3}{2}\varepsilon_1 - \tfrac{1}{2}\varepsilon_2 \quad \tfrac{83}{8} + \tfrac{23}{4}\varepsilon_1 - \tfrac{5}{4}\varepsilon_2 + \tfrac{5}{8}\eta_1 \right)$$

$$c = \left(\tfrac{5}{2} \quad \tfrac{7}{2} \quad 4 \quad 10 \right) \quad J = \begin{pmatrix} \frac{1}{2} & 0 & \frac{3}{2} & \frac{23}{4} + \frac{3}{2}\varepsilon_1 - \frac{1}{4}\varepsilon_2 \\ 0 & \frac{1}{2} & \frac{-1}{2} & -\frac{5}{4} - \frac{1}{4}\varepsilon_1 \end{pmatrix}$$

Inner-approximation of the range of $x_3(x_1, x_2)$ and $x_4(x_1, x_2)$ for $(x_1, x_2) \in [2,3] \times [3,4]$

$\forall k = 1 \dots 4, pro(c_k + [\hat{j}_{1k}][1,-1] + [\hat{j}_{2k}][1,-1]) \subseteq [x_k] \subseteq c_k + [\hat{j}_{1k}][-1,1] + [\hat{j}_{2k}] * [-1,1])$

- Uses Kaucher multiplication rule $[x] \times [y]$ for $[y] = [1,-1] \in$ dual $\mathcal{Z}$
- Note that if a jacobian coefficient contains zero, the corresponding multiplication is zero (rule $\mathcal{Z} \times$ dual $\mathcal{Z} = 0$)
- Exact for x_3 (affine operations only):

$$[2,6] = pro([6,2]) \subseteq range(x_3, [2,3] \times [3,4]) \subseteq [2,6]$$

Interpretation as an inner-approximation

$$Z = \begin{pmatrix} \frac{5}{2} + \frac{1}{2}\varepsilon_1 & \frac{7}{2} + \frac{1}{2}\varepsilon_2 & 4 + \frac{3}{2}\varepsilon_1 - \frac{1}{2}\varepsilon_2 & \frac{83}{8} + \frac{23}{4}\varepsilon_1 - \frac{5}{4}\varepsilon_2 + \frac{5}{8}\eta_1 \end{pmatrix}$$

$$c = \begin{pmatrix} \frac{5}{2} & \frac{7}{2} & 4 & 10 \end{pmatrix} \quad J = \begin{pmatrix} \frac{1}{2} & 0 & \frac{3}{2} & \frac{23}{4} + \frac{3}{2}\varepsilon_1 - \frac{1}{4}\varepsilon_2 \\ 0 & \frac{1}{2} & \frac{-1}{2} & -\frac{5}{4} - \frac{1}{4}\varepsilon_1 \end{pmatrix}$$

Inner-approximation of the range of $x_3(x_1, x_2)$ and $x_4(x_1, x_2)$ for $(x_1, x_2) \in [2,3] \times [3,4]$

$\forall k = 1 \ldots 4,\ pro(c_k + [\hat{j}_{1k}][1,-1] + [\hat{j}_{2k}][1,-1]) \subseteq [x_k] \subseteq c_k + [\hat{j}_{1k}][-1,1] + [\hat{j}_{2k}] * [-1,1])$

- Uses Kaucher multiplication rule $[x] \times [y]$ for $[y] = [1,-1] \in$ dual $\mathcal{Z}$
- Note that if a jacobian coefficient contains zero, the corresponding multiplication is zero (rule $\mathcal{Z} \times$ dual $\mathcal{Z} = 0$)
- Exact for x_3 (affine operations only):

$$[2,6] = pro([6,2]) \subseteq range(x_3, [2,3] \times [3,4]) \subseteq [2,6]$$

- for x_4: $[\hat{j}_{14} = \frac{23}{4} + \frac{3}{2}\varepsilon_1 - \frac{1}{2}\varepsilon_2] \in [4, \frac{15}{2}]$ and $[\hat{j}_{24} = -\frac{5}{4} - \frac{1}{4}\varepsilon_1] \in [-\frac{3}{2}, -1]$:

$$pro(10 + [4, \frac{15}{2}][1,-1] + [-\frac{3}{2}, -1][1,-1]) \subseteq [x_4] \subseteq 10 + [4, \frac{15}{2}][-1,1] + [-\frac{3}{2}, -1][-1,1]$$

Interpretation as an inner-approximation

$$Z = \left(\frac{5}{2} + \frac{1}{2}\varepsilon_1 \quad \frac{7}{2} + \frac{1}{2}\varepsilon_2 \quad 4 + \frac{3}{2}\varepsilon_1 - \frac{1}{2}\varepsilon_2 \quad \frac{83}{8} + \frac{23}{4}\varepsilon_1 - \frac{5}{4}\varepsilon_2 + \frac{5}{8}\eta_1 \right)$$

$$c = \left(\frac{5}{2} \quad \frac{7}{2} \quad 4 \quad 10 \right) \; J = \begin{pmatrix} \frac{1}{2} & 0 & \frac{3}{2} & \frac{23}{4} + \frac{3}{2}\varepsilon_1 - \frac{1}{4}\varepsilon_2 \\ 0 & \frac{1}{2} & \frac{-1}{2} & -\frac{5}{4} - \frac{1}{4}\varepsilon_1 \end{pmatrix}$$

Inner-approximation of the range of $x_3(x_1, x_2)$ and $x_4(x_1, x_2)$ for $(x_1, x_2) \in [2, 3] \times [3, 4]$

$\forall k = 1 \ldots 4$, $pro(c_k + [\hat{j}_{1k}][1, -1] + [\hat{j}_{2k}][1, -1]) \subseteq [x_k] \subseteq c_k + [\hat{j}_{1k}][-1, 1] + [\hat{j}_{2k}] * [-1, 1])$

- Uses Kaucher multiplication rule $[x] \times [y]$ for $[y] = [1, -1] \in$ dual $\mathcal{Z}$
- Note that if a jacobian coefficient contains zero, the corresponding multiplication is zero (rule $\mathcal{Z} \times$ dual $\mathcal{Z} = 0$)
- Exact for x_3 (affine operations only):

$$[2, 6] = pro([6, 2]) \subseteq range(x_3, [2, 3] \times [3, 4]) \subseteq [2, 6]$$

- for x_4: $[\hat{j}_{14} = \frac{23}{4} + \frac{3}{2}\varepsilon_1 - \frac{1}{2}\varepsilon_2] \in [4, \frac{15}{2}]$ and $[\hat{j}_{24} = -\frac{5}{4} - \frac{1}{4}\varepsilon_1] \in [-\frac{3}{2}, -1]$:

$$pro(10 + [4, -4] + [1, -1]) \subseteq [x_4] \subseteq 10 + [-\frac{15}{2}, \frac{15}{2}] + [-\frac{3}{2}, \frac{3}{2}]$$

Interpretation as an inner-approximation

$$Z = \left(\begin{array}{cccc} \frac{5}{2}+\frac{1}{2}\varepsilon_1 & \frac{7}{2}+\frac{1}{2}\varepsilon_2 & 4+\frac{3}{2}\varepsilon_1-\frac{1}{2}\varepsilon_2 & \frac{83}{8}+\frac{23}{4}\varepsilon_1-\frac{5}{4}\varepsilon_2+\frac{5}{8}\eta_1 \end{array} \right)$$

$$c = \left(\begin{array}{cccc} \frac{5}{2} & \frac{7}{2} & 4 & 10 \end{array} \right) \quad J = \left(\begin{array}{cccc} \frac{1}{2} & 0 & \frac{3}{2} & \frac{23}{4}+\frac{3}{2}\varepsilon_1-\frac{1}{4}\varepsilon_2 \\ 0 & \frac{1}{2} & \frac{-1}{2} & -\frac{5}{4}-\frac{1}{4}\varepsilon_1 \end{array} \right)$$

Inner-approximation of the range of $x_3(x_1,x_2)$ and $x_4(x_1,x_2)$ for $(x_1,x_2) \in [2,3]\times[3,4]$

$\forall k = 1 \ldots 4, pro(c_k + [\hat{j}_{1k}][1,-1] + [\hat{j}_{2k}][1,-1]) \subseteq [x_k] \subseteq c_k + [\hat{j}_{1k}][-1,1] + [\hat{j}_{2k}] * [-1,1])$

- Uses Kaucher multiplication rule $[x]\times[y]$ for $[y]=[1,-1] \in$ dual $\mathcal{Z}$
- Note that if a jacobian coefficient contains zero, the corresponding multiplication is zero (rule $\mathcal{Z} \times$ dual $\mathcal{Z} = 0$)
- Exact for x_3 (affine operations only):

$$[2,6] = pro([6,2]) \subseteq range(x_3, [2,3]\times[3,4]) \subseteq [2,6]$$

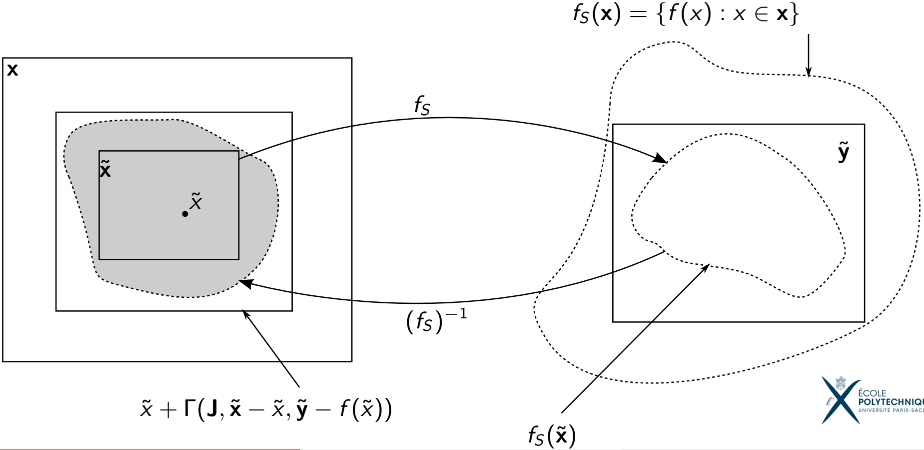
- for x_4: $[\hat{j}_{14} = \frac{23}{4}+\frac{3}{2}\varepsilon_1-\frac{1}{2}\varepsilon_2] \in [4, \frac{15}{2}]$ and $[\hat{j}_{24} = -\frac{5}{4}-\frac{1}{4}\varepsilon_1] \in [-\frac{3}{2},-1]$:

$$[5,15] \subseteq [x_4] \subseteq [1,19]$$

Joint inner range of a vector function

Algorithm to compute a set of boxes proved to be in the image of f:

- Based on input set bisection + a sufficient condition for a box $\tilde{\mathbf{y}}$ to be in range$(f, \mathbf{x})$.
- Only needs an outer approximation of the Jacobian of f
- Goldzstejn-Jaulin 2010 ($f : \mathbb{R}^n \to \mathbb{R}^n$), MGKP 2013 (extension $f : \mathbb{R}^n \to \mathbb{R}^p$)

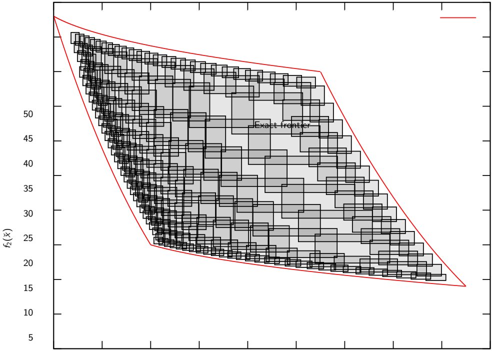


Example

Let $x = (x_1, x_2) \in [2,3] \times [3,4]$ and

$$f(x) = \begin{pmatrix} x_1^3 - 2x_1x_2 \\ x_2^3 - 2x_1x_2 \end{pmatrix}$$

Joint inner range of the corresponding order 1 affine vectors (see paper for computation and inner range of components : costly but rarely needed



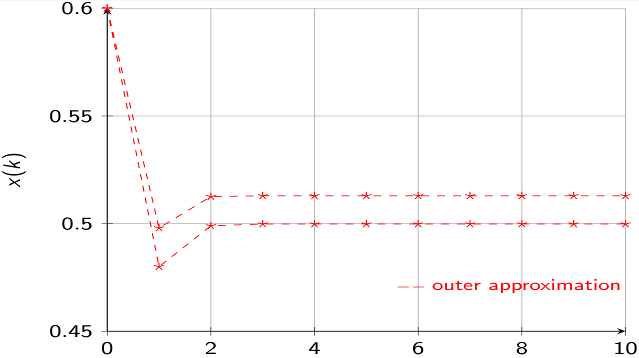
Implementation and experiments

- Order 0 and order 1 affine vectors implemented as an abstract domain in the Apron library for static analysis (`http://apron.cri.ensmp.fr/library`)
  - calls the Taylor1+ abstract domain [Ghorbal-Goubault-Putot 2009, 2010] for zonotopic over-approximation
  - available at `http://www.lix.polytechnique.fr/Labo/Sylvie.Putot/hscc14.html`
  - joint inner approximation as a separate prototype
- Application to the reachability of (discrete) dynamical systems

Example: a Newton algorithm

Consider $x(k+1) = 2x(k) - ax(k)^2$, for $a \in [1.95, 2.]$ and $x(0) = 0.6$, iterated until $|x(k+1) - x(k)| < 5.10^{-4}$. This iteration should converge to $1/a$.

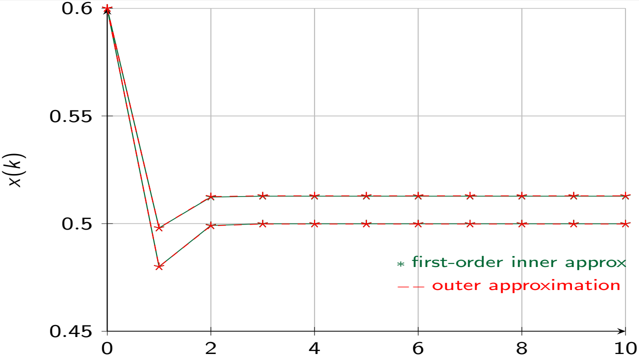
- Outer approximation: the stopping criterion of the loop is always satisfied after 4 iterations ($|x(4) - x(3)| \subseteq [-2.6\,10^{-4}, 2.6\,10^{-4}]$).



Example: a Newton algorithm

Consider $x(k+1) = 2x(k) - ax(k)^2$, for $a \in [1.95, 2.]$ and $x(0) = 0.6$, iterated until $|x(k+1) - x(k)| < 5.\,10^{-4}$. This iteration should converge to $1/a$.

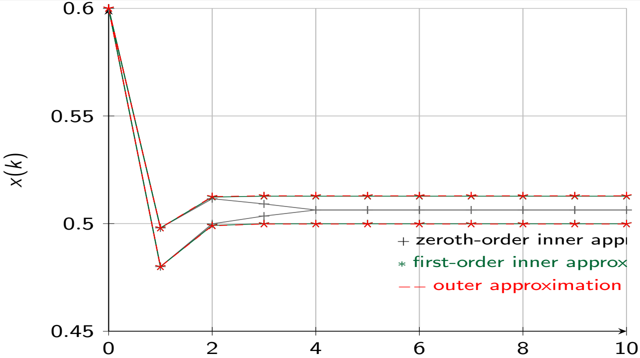
- Outer approximation: the stopping criterion of the loop is always satisfied after 4 iterations ($|x(4) - x(3)| \subseteq [-2.6\,10^{-4}, 2.6\,10^{-4}]$).
- Inner approximation: there exist some inputs for which the criterion is not satisfied for the first 3 iterations (for instance, $[-7.7\,10^{-4}, -4.1\,10^{-4}] \subseteq x(3) - x(2)$).
- When the criterion is satisfied, $[.4999244,\ .5127338] \subseteq x(4) \subseteq [0.499831, 0.512906]$.



Example: a Newton algorithm

Consider $x(k+1) = 2x(k) - ax(k)^2$, for $a \in [1.95, 2.]$ and $x(0) = 0.6$, iterated until $|x(k+1) - x(k)| < 5.\,10^{-4}$. This iteration should converge to $1/a$.

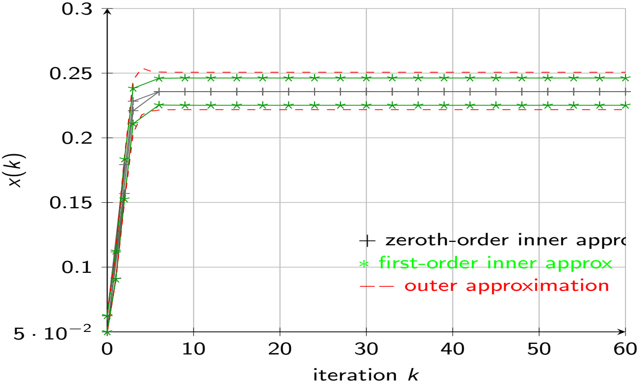
- Outer approximation: the stopping criterion of the loop is always satisfied after 4 iterations ($|x(4) - x(3)| \subseteq [-2.6\,10^{-4}, 2.6\,10^{-4}]$).
- Inner approximation: there exist some inputs for which the criterion is not satisfied for the first 3 iterations (for instance, $[-7.7\,10^{-4}, -4.1\,10^{-4}] \subseteq x(3) - x(2)$).
- When the criterion is satisfied, $[.4999244,\ .5127338] \subseteq x(4) \subseteq [0.499831, 0.512906]$.



Example: good behaviour on this highly non linear Householder iteration

$$x(k+1) = x(k) + x(k)\left(\frac{1}{2}h(k) + \frac{3}{8}h(k)^2\right)$$

with $h(k) = 1 - ax(k)^2$ and $a \in [16, 20]$, starting from $x(0) = [\frac{1}{20}, \frac{1}{16}]$.

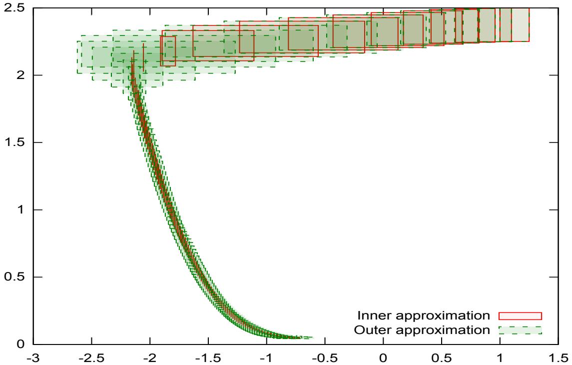


Comparable accuracy of inner and outer approximations, and stability along iterations.

Reachability of discrete dynamical systems: FitzHugh-Nagumo neuron model (100 iterates of Euler time-discretization scheme)

$$\begin{cases} x_1(k+1) = x_1(k) + h\left(x_1(k) - \frac{x_1(k)^3}{3} - x_2(k) + \frac{7}{8}\right) \\ x_2(k+1) = x_2(k) + h\,(0.08(x_1(k) + 0.7 - 0.8x_2(k))) \end{cases}$$

where $h = 0.2$, and $(x_1(0), x_2(0)) = [1, 1.25] \times [2.25, 2.5]$.



Analysis takes 11 sec, $[-.737783, -.716137] \subseteq x_1(100) \subseteq [-.857537, -.595651]$, $[.450016, .506109] \subseteq x_2(100) \subseteq [.429873, .542796]$.

Conclusion and future work

- Inner approximation scheme
  - order of accuracy of outer approximated zonotopes
  - cost remains linear with respect to over-approximated zonotopes
- Reachability analysis of continuous dynamical systems
  - in the paper, indirect method by over approximation of the Jacobian by Taylor Models
  - direct set integration (work in progress)
- Reachability analysis of hybrid systems: interpretation of guard conditions (work in progress)
  - in the paper (HSCC 2014), first ideas for inner approximation of the range of noise symbols in order to satisfy the constraints, instead of the [-1,1] ranges