Formally Verified Conditions for Regulatiry of Interval Matrices

Ioana Paşca

INRIA Sophia Antipolis

Calculemus at CICM, 2010

Interval arithmetic

Tool used to handle inaccuracies in computations.

$$-\pi * \sqrt{2} \approx -3.14 * 1.41 = -4.4274$$

$$[-3.15, -3.14] * [1.41, 1.42] = [-4.473, -4.4274]$$

If we know the bounds on the input data we can compute the bounds on the result.

Interval arithmetic, more formally

Definition

interval := closed, bounded, connected, nonempty subset of $\mathbb{R}$

$$\boldsymbol{x} := [\underline{x}, \overline{x}] = \{\tilde{x} \in \mathbb{R} \mid \underline{x} \leq \tilde{x} \leq \overline{x}\}, \quad \text{where } \underline{x}, \overline{x} \in \mathbb{R}, \underline{x} \leq \overline{x}$$

Notation $\mathbb{IR}$ – set of intervals

Classification

- thin interval $\underline{x} = \overline{x}$
- thick interval $\underline{x} < \overline{x}$

Interval arithmetic, more formally

Definition

interval := closed, bounded, connected, nonempty subset of $\mathbb{R}$

$$x := [\underline{x}, \overline{x}] = \{\tilde{x} \in \mathbb{R} \mid \underline{x} \leq \tilde{x} \leq \overline{x}\}, \quad \text{where } \underline{x}, \overline{x} \in \mathbb{R}, \underline{x} \leq \overline{x}$$

Notation $\mathbb{IR}$ – set of intervals

Classification

- thin interval $\underline{x} = \overline{x}$
- thick interval $\underline{x} < \overline{x}$

Associated real quantities

- midpoint $x_c := \frac{\underline{x}+\overline{x}}{2}$
- radius $\Delta_x := \frac{\overline{x}-\underline{x}}{2}$

$$x = [x_c - \Delta_x, x_c + \Delta_x]$$

Basic interval operations

$$x + z := \Box\{\tilde{x} + \tilde{z} \mid \tilde{x} \in x, \tilde{z} \in z\}$$

Basic interval operations

$$x + z := \square\{\tilde{x} + \tilde{z} \mid \tilde{x} \in x, \tilde{z} \in z\} = \{\tilde{x} + \tilde{z} \mid \tilde{x} \in x, \tilde{z} \in z\} =$$

$$= [\underline{x} + \underline{z}, \overline{x} + \overline{z}]$$

Basic interval operations

$$x + z := \square\{\tilde{x} + \tilde{z} \mid \tilde{x} \in x, \tilde{z} \in z\} = \{\tilde{x} + \tilde{z} \mid \tilde{x} \in x, \tilde{z} \in z\} =$$

$$= [\underline{x} + \underline{z}, \overline{x} + \overline{z}]$$

do the same for opposite and multiplication

Rounded interval arithmetic

Usage

- in theory: $[\underline{x}, \overline{x}]$ with $\underline{x}, \overline{x} \in \mathbb{R}$
- in practice: $[\underline{x}, \overline{x}]$ with $\underline{x}, \overline{x} \in M$,
  where M is a machine representable subset of $\mathbb{R}$

Outward rounding

$$\Diamond x := [\nabla \underline{x}, \Delta \overline{x}]$$

Rounded interval arithmetic

Usage

- in theory: $[\underline{x}, \overline{x}]$ with $\underline{x}, \overline{x} \in \mathbb{R}$
- in practice: $[\underline{x}, \overline{x}]$ with $\underline{x}, \overline{x} \in M$,
  where M is a machine representable subset of $\mathbb{R}$

Outward rounding

$$\Diamond x := [\nabla \underline{x}, \Delta \overline{x}]$$

Example

$$[-3.15, -3.14] * [1.41, 1.42] = [-4.473, -4.4274]$$

M : decimal numbers with 2 digits

$$[-3.15, -3.14] *^{\Diamond} [1.41, 1.42] = [-4.48, -4.42]$$

Issues with rounded arithmetic

Rounded arithmetic

$$x +^{\Diamond} z = \Diamond[\underline{x} + \underline{z}, \overline{x} + \overline{z}]$$

$$\{\tilde{x} + \tilde{z} \mid \tilde{x} \in x, \tilde{z} \in z\} \subseteq x +^{\Diamond} z$$

Ideal arithmetic

$$\{\tilde{x} + \tilde{z} \mid \tilde{x} \in x, \tilde{z} \in z\} = x + z$$

Interval arithmetic in proof assistants

Nature of interval methods

- interval arithmetic was born to safely deal with errors

Usage

- interval arithmetic appears in critical software
- certified computation

Formalizations

- Coq, PVS, Isabelle
- focus on computation efficiency and automation of techniques

Computation driven formalizations

- basic operations
- elementary functions
- techniques to increase accuracy
- rounded interval arithmetic
- automated procedures to compute and prove bounds for expressions
- computations by external tools

Formalizing more “theoretical” results

Formalizing more “theoretical” results

- solving systems of linear equations with interval coefficients

Exercise

Consider the following system:

$$\begin{cases} [1,2]x_1 & + & [2,4]x_2 & = [-1,1] \\ [2,4]x_1 & + & [1,2]x_2 & = [1,2] \end{cases}$$

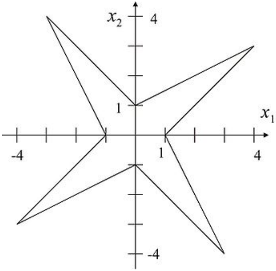
Find a box that contains all pairs $(x_1, x_2) \in \mathbb{R}^2$ that satisfy the equations for some choice of coefficients in their respective intervals.

- correctness of methods for solving these systems is based on more involved theoretical results
- application: robot movement

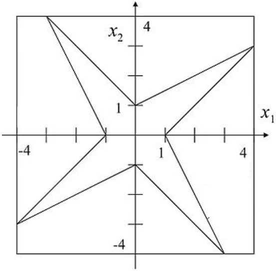
Two steps:

1. checking regularity of the associated interval matrix
2. computing bounds of the solution set

exact solution



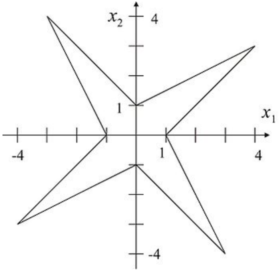
bounds for the solution set



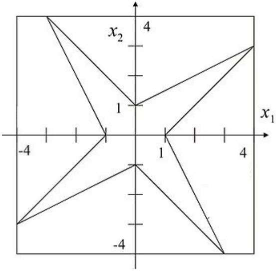
Two steps:

1. checking regularity of the associated interval matrix
2. computing bounds of the solution set

exact solution



bounds for the solution set



Definition

$$A = [A_{ij}]_{m \times n},\ A_{ij} \in \mathbb{IR}$$

Example

$$A = \begin{pmatrix} [1,2] & [2,4] \\ [2,4] & [1,2] \end{pmatrix}$$

Characterization

$$A = \{\tilde{A} \in M(\mathbb{R})_{m \times n} \mid \tilde{A}_{ij} \in A_{ij}\}$$

$$\begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix} \in A$$

Associated real matrices

$$A_c := [(A_{ij})_c]$$

$$A_c = \begin{pmatrix} 1.5 & 3 \\ 3 & 1.5 \end{pmatrix}$$

$$\Delta_A := [\Delta_{A_{ij}}]$$

$$\Delta_A = \begin{pmatrix} 0.5 & 1 \\ 1 & 0.5 \end{pmatrix}$$

Operations on interval matrices

Addition

$$A + B := \square\{\tilde{A} + \tilde{B} \mid \tilde{A} \in A, \tilde{B} \in B\}$$

Operations on interval matrices

Addition

$$A + B := \square\{\tilde{A} + \tilde{B} \mid \tilde{A} \in A, \tilde{B} \in B\} = \{\tilde{A} + \tilde{B} \mid \tilde{A} \in A, \tilde{B} \in B\}$$

$$(A + B)_{ij} = A_{ij} + B_{ij}$$

An interval matrix A is called regular iff $\forall \tilde{A} \in A, \det \tilde{A} \neq 0$

and it is called singular otherwise ($\exists \tilde{A}, \tilde{A} \in A \wedge \det \tilde{A} = 0$).

Systems of linear interval equations

A system of linear interval equations with coefficient matrix $A \in M(\mathbb{IR})_{m \times n}$ and right-hand side $b \in \mathbb{IR}^m$ is defined as the family of linear systems of equations

$$\tilde{A}\tilde{x} = \tilde{b} \text{ with } \tilde{A} \in A, \tilde{b} \in b$$

The *solutions set* of such a system is given by:

$$\Sigma(A, b) := \{\tilde{x} \in \mathbb{R}^n \mid \exists \tilde{A} \in A, \exists \tilde{b} \in b \text{ such that } \tilde{A}\tilde{x} = \tilde{b}\}$$

Proof example

Theorem

$$\Sigma(A,b) = \{\tilde{x} \in \mathbb{R}^n \mid A\tilde{x} \cap b \neq \emptyset\}$$

Proof excerpt.

We show: $\{\tilde{x} \in \mathbb{R}^n \mid A\tilde{x} \cap b \neq \emptyset\} \subseteq \Sigma(A,b)$.

Consider $\tilde{x}$ such that $A\tilde{x} \cap b \neq \emptyset$.

Then $A\tilde{x} \cap b$ contains some $\tilde{b} \in \mathbb{R}^m$.

Clearly $\tilde{b} \in b$.

Also, $\tilde{b} \in A\tilde{x}$ and by relation (1), $\tilde{b} = \tilde{A}\tilde{x}$ for some $\tilde{A} \in A$.

Therefore $\tilde{x} \in \Sigma(A,b)$. □

$$A\tilde{x} = \{\tilde{A}\tilde{x} \mid \tilde{A} \in A\} \qquad (1)$$

Setting up the formalization

We need to talk about

- real numbers
- matrices

We use

- Coq standard library Reals
- SSReflect library matrix

Mix SSReflect and standard Coq !

Mix SSREFLECT and COQ

in SSREFLECT

- hierarchy of algebraic structures
- abstract matrices, but operations when elements are from a ring

in COQ's Reals library

- real numbers defined by axioms
- ring structure

Bricks of the formalization

- intervals: definition, operations and properties
- interval matrices: definition, operations and properties
- properties of real matrices
- criteria for regularity of interval matrices

Yet another formalization of intervals

Definition

$$x := [\underline{x}, \overline{x}] = \{\tilde{x} \in \mathbb{R} \mid \underline{x} \leq \tilde{x} \leq \overline{x}\}, \quad \text{where } \underline{x}, \overline{x} \in \mathbb{R}, \underline{x} \leq \overline{x}$$

```
Structure IR: Type := ClosedInt
  { inf: R ; sup: R ; leq_proof: inf ≤b sup }.
```

Intervals as sets

- coerce IR to R → bool

Equality of intervals

```
Lemma eq_intervalP :
  ∀ x z : IR, x = z ↔ inf x = inf z ∧ sup x = sup z.
```

$$x + z = [\underline{x} + \underline{z}, \overline{x} + \overline{z}] = \{\tilde{x} + \tilde{z} \mid \tilde{x} \in x, \tilde{z} \in z\}$$

Addition is

- associative
- commutative $\Rightarrow (\mathbb{IR}, +)$ is a monoid
- neutral element $[0, 0]$

But

$-x + x \neq [0, 0]$, if x is thick $\Rightarrow (\mathbb{IR}, +)$ is NOT a group

$$\Rightarrow (\mathbb{IR}, +, *) \text{ is NOT a ring}$$

Interval matrices

- use SSREFLECT library
- define specific operations on interval matrices, as intervals do not have a ring structure

```
Definition mmul_i (A: 'M[IR]_(m, n)) (x: 'cV[IR]_(n)) :=
    \col_i \big[+IR / 0]_j (A i j) *IR (x j).
```

$$(A * x)_i = \sum_{j=0}^{n-1} A_{ij} x_j$$

- prove specific properties

$$A\tilde{x} = \{\tilde{A}\tilde{x} \mid \tilde{A} \in A\}$$

Results on real matrices

- norm for real matrices
- properties for symmetric and positive definite matrices
- eigenvalues for real matrices
  - Rayleigh quotients
  - Perron Frobenius theorem

Results on real matrices

- norm for real matrices
- properties for symmetric and positive definite matrices
- eigenvalues for real matrices
  - Rayleigh quotients
  - Perron Frobenius theorem

eigenvalues for real matrices:

- roots of the characteristic polynomial
- they can be complex
- Rayleigh quotient: $\frac{x^T A x}{x^T x}$, $x \neq 0$, A – symmetric

$$\forall x \in \mathbb{R}^n, x \neq 0, \lambda_{\text{min}}(A) \leq \frac{x^T A x}{x^T x} \leq \lambda_{\text{max}}(A)$$

spectral radius: $\rho(A) = \max\{|\lambda(A)|\}$

Theorem (Perron Frobenius)

If $A \in \mathbb{R}^{n \times n}$ is nonnegative then the spectral radius $\rho(A)$ is an eigenvalue of A, and there is a real, nonnegative vector $x \neq 0$ with $Ax = \rho(A)x$.

Formalized criteria of regularity

Criterion

A is regular if and only if $\forall \tilde{x} \in \mathbb{R}^n, 0 \in A\tilde{x} \Rightarrow \tilde{x} = 0$.

Criterion

A is regular if and only if $\forall \tilde{x} \in \mathbb{R}^n, |A_c\tilde{x}| \leq \Delta_A|\tilde{x}| \Rightarrow \tilde{x} = 0$.

Formalized criteria of regularity

Criterion

A is regular if and only if $\forall \tilde{x} \in \mathbb{R}^n, 0 \in A\tilde{x} \Rightarrow \tilde{x} = 0$.

Criterion

A is regular if and only if $\forall \tilde{x} \in \mathbb{R}^n, |A_c\tilde{x}| \leq \Delta_A|\tilde{x}| \Rightarrow \tilde{x} = 0$.

Criterion (using positive definiteness)

If the matrix $(A_c^T A_c - \|\Delta_A^T \Delta_A\| I)$ is positive definite for some consistent matrix norm $\|\cdot\|$, then A is regular.

Criterion (using the midpoint inverse)

If the following inequality holds $\rho(|I - RA_c| + |R|\Delta_A) < 1$ for an arbitrary matrix R, then A is regular.

Criterion (using eigenvalues)

If the inequality $\lambda_{max}(\Delta_A^T \Delta_A) < \lambda_{min}(A_c^T A_c)$ holds, then A is regular.

How far from the real world

- adapt results for rounded rounded arithmetic
- treat methods for bounding the solution set
- finish proving the admitted results

leq_proof: inf $\leq_b$ sup

```
Lemma Rle_dec: ∀ r1 r2, {r1 <= r2} + {~ r1 <= r2}.

Definition Rleb r1 r2 :=
  match (Rle_dec r1 r2) with
    | left _ ⇒ true
    | right _ ⇒ false
  end.
```

inf $\leq_b$ sup $\rightsquigarrow$ Rleb inf sup $\rightsquigarrow$ is_true (Rleb inf sup) $\rightsquigarrow$

$\rightsquigarrow$ Rleb inf sup = true

Boolean equality is decidable and therefore proof irrelevant.