Satisfiability Checking

18 Interval constraint propagation I

Prof. Dr. Erika Ábrahám

RWTH Aachen University
Informatik 2
LuFG Theory of Hybrid Systems

WS 22/23

18 Interval constraint propagation I

1. Interval arithmetic
2. Contraction I

$x^2 = y \qquad x \in [-1, 1]$

$\Downarrow$

$y \in [0, 1]$

Next lecture:

Contraction II

The global ICP algorithm

Non-linear real arithmetic

We consider input formulae φ from the theory of quantifier-free nonlinear real arithmetic (QFNRA):

just Polynomials with constraints (<,=) and formulas (ϕ ∧ ϕ ,¬ϕ).

常数 变量

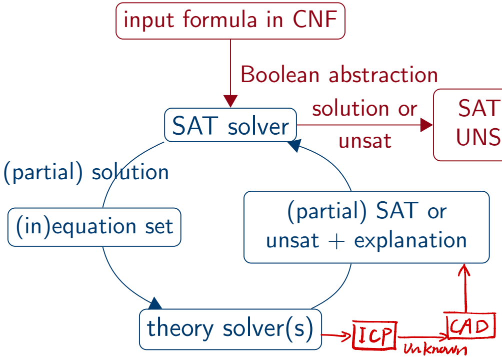
$$
\begin{array}{lll}
p & := & const \mid x \mid (p+p) \mid (p-p) \mid (p \cdot p) \\
c & := & p < 0 \mid p = 0 \\
\varphi & := & c \mid (\varphi \wedge \varphi) \mid \neg\varphi
\end{array}
$$

polynomials
(polynomial) constraints
QFNRA formulas

where constants *const* and variables x take real values from $\mathbb{R}$.

- Best known methods for checking the satisfiability of QFNRA formulas have exponential complexity → hard to solve
- Approaches we learn for solving QFNRA:
  - Interval constraint propagation (ICP) incomplete
  - Subtropical satisfiability incomplete
  - Virtual substitution (VS) incomplete
  - Cylindrical algebraic decomposition (CAD) complete

Interval constraint propagation (ICP) in SMT



Remember: the theory solvers needs to check sets/conjunctions of theory constraints only (in contrast to arbitrary Boolean combinations)

We first use interval constraint propagation (ICP) in a theory solver module:

- Incomplete: ICP always terminates but it might return "unknown" → later we extend it with a backend implementing a complete procedure.
- Relatively cheap reduction of the search space: Even if the answer is "unknown", ICP might still be helpful because it returns a smaller search space (a set of subsets of the original search space) without loosing any solution.

Intervals

For simplicity, in the following we consider only weak interval bounds.

Definition (Interval)

- An interval $A = [\underline{A}; \overline{A}]$ with
  - lower bound $\underline{A} \in \mathbb{R} \cup \{-\infty\}$ and
  - upper bound $\overline{A} \in \mathbb{R} \cup \{+\infty\}$,

  denotes the closed connected set

  $$\boxed{[\![A]\!] = \{v \in \mathbb{R} \mid \underline{A} \leq v \leq \overline{A}\}}$$

  where $-\infty \leq v \leq +\infty$ for all real numbers $v \in \mathbb{R}$.
- We denote by $\mathbb{I}$ the set of all intervals.
- We call A bounded iff $[\![A]\!]$ is bounded (i.e. $\underline{A} \neq -\infty$ and $\overline{A} \neq +\infty$), and unbounded otherwise.
- An interval $A = [\underline{A}; \overline{A}]$ is empty iff $[\![A]\!] = \emptyset$ (i.e. $\underline{A} > \overline{A}$.)

Notation

- For point intervals $[v; v]$ for some $v \in \mathbb{R}$ we also write v.
- The only closed connected subset of $\mathbb{R}$ with a non-unique interval representation is the empty set; we use $[1; 0]$ for its representation.

  An interval is empty iff its width is negative 空集统一用[1;0]表示
- To simplify notation, we always use brackets "[" and "]", even for unbounded intervals like $[0, +\infty]$. Realize that it does not mean that $+\infty$ is included in the interval. $= [0, +\infty)$

Intervals and boxes

Definition (Interval diameter)

The width/diameter $D(A) \in \mathbb{R} \cup \{+\infty\}$ of an interval $A = [\underline{A}; \overline{A}] \in \mathbb{I}$ is $D(A) = +\infty$ if A is unbounded and $D(A) = \overline{A} - \underline{A}$ otherwise.

Q: What is the width of a point interval?
A: 0

Q: If we know the width of an interval, how can we determine whether the interval is empty?
A: An interval is empty iff its width is negative.

Definition (Interval box)

An n-dimensional box is a cross product $A_1 \times \ldots \times A_n \in \mathbb{I}^n$ of n intervals.

Interval arithmetic

For set operations, we define for all $A = [\underline{A}; \overline{A}] \in \mathbb{I}$ and $B = [\underline{B}; \overline{B}] \in \mathbb{I}$:

- $A = \emptyset$ iff $\underline{A} > \overline{A}$

  (i.e. $A = \emptyset$ iff $[\![A]\!] = \emptyset$)

- $A \cap B =$

$$\begin{cases} [1;0] & \textit{if } A = \emptyset \vee B = \emptyset \vee \underline{B} > \overline{A} \vee \underline{A} > \overline{B} \\ [\max\{\underline{A}, \underline{B}\}, \min\{\overline{A}, \overline{B}\}] & \end{cases}$$

即A,B没有交集

两者下界取较大值,
上界取较小值

(i.e. $[\![A \cap B]\!] = [\![A]\!] \cap [\![B]\!]$)

Interval arithmetic

- We extend real arithmetic operations to intervals. Besides the interval-adaptations $+, -, \cdot : \mathbb{I} \times \mathbb{I} \to \mathbb{I}$ of the QFNRA operators $+, -, \cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, we will also need division $\div : \mathbb{I} \times \mathbb{I} \to \mathbb{I}$ as the inverse of the multiplication, and square and square root operations $\cdot^2$, $\pm\sqrt{\cdot} : \mathbb{I} \to \mathbb{I}$ (we will see later why).

  Arithmetic operations on intervals will be exact:

$$op\,A = \{op\, a \,|\, a \in [\![A]\!]\} \qquad A\; op\; B = \{a\; op\; b \,|\, a \in [\![A]\!] \wedge b \in [\![B]\!]\}$$

- Given an interval domain for each variable, polynomials can now be evaluated to an interval value.

  However, the interval evaluation of polynomials will be in general over-approximative (due to different occurrences of the same variable).
- The approach introduced in this lecture can be naturally extended to further operators like *sin*, *cos*, *exp*,. . . .

Computing with infinity

We first partially extend the operations $+, -, \cdot, \div : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ from $\mathbb{R}$ to $\mathbb{R} \cup \{-\infty, +\infty\}$ as follows. Let $a, b \in \mathbb{R}$. The following tables define the extensions, where rows constain the first and columns the second operands.

Addition $+$	$-\infty$	b	$+\infty$
$-\infty$	$-\infty$	$-\infty$	
a	$-\infty$	$a+b$	$+\infty$
$+\infty$		$+\infty$	$+\infty$

Subtraction $-$	$-\infty$	b	$+\infty$
$-\infty$		$-\infty$	$-\infty$
a	$+\infty$	$a-b$	$-\infty$
$+\infty$	$+\infty$	$+\infty$	

Multiplication $\cdot$	$-\infty$	$-\infty < b < 0$	0	$0 < b < \infty$	$+\infty$
$-\infty$	$+\infty$	$+\infty$	0	$-\infty$	$-\infty$
$-\infty < a < 0$	$+\infty$	$a \cdot b$	0	$a \cdot b$	$-\infty$
0	0	0	0	0	0
$0 < a < \infty$	$-\infty$	$a \cdot b$	0	$a \cdot b$	$+\infty$
$+\infty$	$-\infty$	$-\infty$	0	$+\infty$	$+\infty$

Division $\div$	$-\infty$	$-\infty < b < 0$	0	$0 < b < \infty$	$+\infty$
a	0	$a \div b$		$a \div b$	0

Note: The above tables define the arithmetic operations only partially (e.g., division is not defined for infinite nominator). The undefined cases (for which a meaningful definition cannot be given) will not be needed.

Now we are ready to extend the real arithmetic operations to (possibly unbounded) intervals. For each operator, we first look at some examples before we give a general definition.

Let in the following $A = [\underline{A}; \overline{A}] \in \mathbb{I}$ and $B = [\underline{B}; \overline{B}] \in \mathbb{I}$.

Interval arithmetic: Addition

Example (Interval addition)

$[-1;5] + [1;4] = [0;9]$

$[-2;3] + 4 = [-2;3] + \underbrace{[4;4]}_{4} = [2;7]$

Definition (Interval addition)

$$A + B = \begin{cases} [\underline{A} + \underline{B} \,;\, \overline{A} + \overline{B}] & \textit{if } A \neq \emptyset \textit{ and } B \neq \emptyset \\ [1;0] & \textit{otherwise} \end{cases}$$

Interval arithmetic: Subtraction

Example (Interval subtraction)

$[-1;5] - [1;4] = [-5;4]$
$[-2;3] - 4 = [-2;3] - [4;4] = [-6;-1]$

Definition (Interval subtraction)

$$A - B = \begin{cases} [\underline{A} - \overline{B}\,;\, \overline{A} - \underline{B}] & \textit{if } A \neq \emptyset \textit{ and } B \neq \emptyset \\ [1;0] & \textit{otherwise} \end{cases}$$

We can also define unary minus as syntactic sugar:

Definition (Unary interval minus)

We define $-A = 0 - A$.

Interval arithmetic: Multiplication

Example (Interval multiplication)

$[-1;5] \cdot [1;4] = [-4;20]$
$[-2;3] \cdot 4 = [-2;3] \cdot [4;4] = [-8;12]$

Definition (Interval multiplication)

$$A \cdot B = \begin{cases} [\mathit{min}(\underline{A} \cdot \underline{B}, \underline{A} \cdot \overline{B}, \overline{A} \cdot \underline{B}, \overline{A} \cdot \overline{B}) \;;\; \mathit{max}(\underline{A} \cdot \underline{B}, \underline{A} \cdot \overline{B}, \overline{A} \cdot \underline{B}, \overline{A} \cdot \overline{B})] \\ \qquad \text{if } A \neq \emptyset \text{ and } B \neq \emptyset \\ [1;0] \quad \text{otherwise} \end{cases}$$

Interval arithmetic: Multiplication

Example (Interval square)

Special case: Squaring an interval can only result in positive values.
$[-1;5]^2 = [0;25]$

Definition (Interval square)

$A^2 = (A \cdot A) \cap [0;+\infty)$ for non-empty $A = [\underline{A};\overline{A}] \in \mathbb{I}$ and $A^2 = [1;0]$ otherwise.

e.g. $[-1;5]^2 = ([-1;5] \cdot [-1;5]) \cap [0;+\infty) = [-5;25] \cap [0,+\infty) = [0;25]$

Example (Interval square root)

$x^2 = y$
$\Rightarrow x = \pm\sqrt{y}$

$\pm\sqrt{[0;4]} = [-2;2]$ $\quad \pm\sqrt{[-4;4]} = [-2;2]$ $\quad \pm\sqrt{[1;4]} = [-2;-1] \cup [1;2]$

Definition (Interval square root)

A只能取正数

$$\pm\sqrt{A} = \begin{cases} \left[-\sqrt{\overline{A}}; +\sqrt{\overline{A}}\right] & \text{if } \underline{A} \le 0 \le \overline{A} \text{ (with } \sqrt{+\infty} = +\infty) \\ \left[-\sqrt{\overline{A}}, -\sqrt{\underline{A}}\right] \cup \left[\sqrt{\underline{A}}, \sqrt{\overline{A}}\right] & \text{if } 0 < \underline{A} \le \overline{A} \\ [1;0] & \text{otherwise} \end{cases}$$

These can be generalised to arbitrary powers A^k and roots $\sqrt[k]{A}$.

Interval arithmetic: Division

Example (Interval division for $0 \notin B$)

$[2;3] \div [4;5] = [2;3] \cdot \frac{1}{[4;5]} = [2;3] \cdot [\frac{1}{5}; \frac{1}{4}] = [\frac{2}{5}; \frac{3}{4}]$

Definition (Interval division for $0 \notin B$)

$$A \div B = \begin{cases} [1;0] & \text{if } A = \emptyset \text{ or } B = \emptyset \\ A \cdot \frac{1}{B} = A \cdot [\frac{1}{\overline{B}}; \frac{1}{\underline{B}}] & \text{if } A \neq \emptyset \text{ and } B \neq \emptyset \text{ and } 0 \notin B. \end{cases}$$

B不包含 0

Interval arithmetic: Division

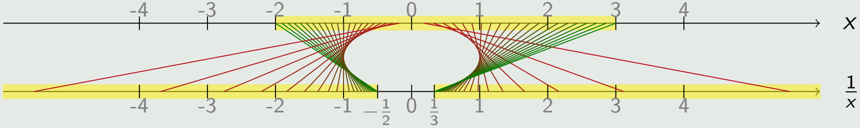
Problem: B may contain 0, but division by 0 is not defined

Example (Interval division for $0 \in B$)

B 包含 0

If $0 \in B$ then the previous definition does not work correctly:
$\frac{1}{[-2;3]} = [\frac{1}{3}; -\frac{1}{2}] \rightarrow$ invalid bounds

How should $\frac{1}{[-2;3]}$ be defined?



We observe: $\frac{1}{[-2;3]} = [-\infty; -\frac{1}{2}] \cup [\frac{1}{3}; +\infty]$!
Note: Result may be disconnected!

Interval arithmetic: Division

Definition (Interval division $A \div B$ for $0 \in B$)

The following table defines the result of $A \div B$ for $A \neq \emptyset$ and $0 \in B$; rows define case distinctions on A, columns on B:

$A \div B$	$B = [0;0]$	$\underline{B} < \overline{B} = 0$	$\underline{B} < 0 < \overline{B}$	$0 = \underline{B} < \overline{B}$
$A = [0;0]$	$[1;0]$	$[0;0]$	$[0;0]$	$[0;0]$
$\underline{A} < \overline{A} = 0$	$[1;0]$	$[0;+\infty]$	$[-\infty;+\infty]$	$[-\infty;0]$
$\underline{A} < 0 < \overline{A}$	$[1;0]$	$[-\infty;+\infty]$	$[-\infty;+\infty]$	$[-\infty;+\infty]$
$0 = \underline{A} < \overline{A}$	$[1;0]$	$[-\infty;0]$	$[-\infty;+\infty]$	$[0;+\infty]$
$\overline{A} < 0$	$[1;0]$	$[\overline{A}/\underline{B};+\infty]$	$[-\infty;\overline{A}/\overline{B}] \cup [\overline{A}/\underline{B};+\infty]$	$[-\infty;\overline{A}/\overline{B}]$
$0 < \underline{A}$	$[1;0]$	$[-\infty;\underline{A}/\underline{B}]$	$[-\infty;\underline{A}/\underline{B}] \cup [\underline{A}/\overline{B};+\infty]$	$[\underline{A}/\overline{B};+\infty]$

18 Interval constraint propagation I

1. Interval arithmetic
2. Contraction I

Next lecture:

- Contraction II
- The global ICP algorithm

How to strengthen bounds using interval arithmetic

- Now we can compute with intervals.
- The input of ICP (as a theory solver in an SMT solver) is
  - a set C of QFNRA constraints in n ordered variables $x_1, \ldots, x_n$ and
  - an initial box $B = A_1 \times \ldots \times A_n$ (interval domains A_i for the variables x_i in the constraints).
- Our goal is to decide whether the initial box B contains a common satisfying solution for the constraints in C.
- Let us first have a look at how we can make the initial box B smaller without loosing any solutions.

  This bound strengthening is done via iterative contraction.
- We learn two different contraction methods.

Contraction I: Preprocessing

- The first contraction method requires that for each $c \in C$ and each variable x in c, we can bring c to an equivalent form $x \sim e$ with $\sim \in \{<, \leq, =, \geq, >\}$, where x does not appear in e.
- This is doable for linear constraints (only addition operations), and also for equations with only multiplication operations if we allow division and root operations in e.
- We need some preprocessing (done for each constraint one time, when ICP receives it) to satisfy this requirement.

Preprocessing: Example

当一个式子中有多个变量,难以将变量分离时 ⇒ preprocessing

1. $x^2 \cdot y + z = 0 \quad \rightarrow \quad h + z = 0 \wedge h = x^2 \cdot y$

e.g. $\underbrace{x^2 y}_{h_1} + \underbrace{y^2 \cdot x}_{h_2} = 0$

分离x、y困难

$h_1 + h_2 = 0$

$x^2 y = h_1$

$y^2 x = h_2$

2. Now the constraints satisfy the requirements:

$$h + z = 0 \quad \rightarrow \quad h = -z$$
$$\rightarrow \quad z = -h$$

$$h = x^2 \cdot y \quad \rightarrow \quad h = x^2 \cdot y$$
$$\rightarrow \quad x = \pm\sqrt{h \div y}$$
$$\rightarrow \quad y = h \div (x^2)$$

⇒ 此后方便分离出x,y

$x = \pm\sqrt{\frac{h_1}{y}}$

$y = \pm\sqrt{\frac{h_2}{x}}$

Contraction I: Preprocessing

- Set $C' := C$ and $C := \emptyset$.
- Repeat as long as C' is not empty:
  - Take a constraint $e_1 \sim e_2$ with $\sim \in \{<, \leq, =, \geq, >\}$ from C'.
  - Bring $e_1 \sim e_2$ to the normal form $r_1 \cdot m_1 + \ldots + r_k \cdot m_k \sim 0$, where $r_i \in \mathbb{R}$ and m_i are monomials (either 1 or a product of variables) for each $i = 1, \ldots, k$.
  - Replace each non-linear monomial m_i in $r_1 \cdot m_1 + \ldots + r_k \cdot m_k \sim 0$ by a fresh variable h_i and add the result to C.
  - For each newly added variable h_i replacing m_i in the previous step,
    - add an equation $h_i - m_i = 0$ to C, and
    - initialize the bounds of h_i to the interval we get when we substitute the variable bounds in m_i and evaluate the result using interval arithmetic (note: the result will always be a single interval because there is no division or square root in m_i).

Contraction I: Method

- Choose a constraint $c \in C$ and a variable x appearing in c.

  We call such a pair (c, x) a contraction candidate (CC).
- Bring c to a form $x \sim e$, $\sim \in \{<, \leq, =, \geq, >\}$, where e does not contain x. (Note: possible due to preprocessing.)

  y∈[1;11] x∈[3;6]
- Replace all variables in e by their current bounds.

  e.g. y=3x+2 => 3[3; 6] + 2
- Apply interval arithmetic to evaluate the right-hand-side (e with the variables substituted by their bounds) to a union of intervals.

  把式子右边的全部换成interval格式

  e.g. y=3[3; 6] + 2 => [3;3][3;6]+[2;2} =[11;20]
- For each each interval B in that union, derive from the current bound A for x and the computed bound B for e a new bound on x, depending on the type of $\sim$, as follows:

  e.g. y=[11;20]∩ [1;11]=[11;11]

$$
\begin{array}{lll}
x < e & \textit{if } \underline{A} \geq \overline{B} \textit{ then } [1;0] \textit{ else} & [\underline{A}; \min\{\overline{A}, \overline{B}\}] \\
x \leq e & & [\underline{A}; \min\{\overline{A}, \overline{B}\}] \\
x = e & & [\max\{\underline{A}, \underline{B}\}; \min\{\overline{A}, \overline{B}\}] \\
x \geq e & & [\max\{\underline{A}, \underline{B}\}; \overline{A}] \\
x > e & \textit{if } \overline{A} \leq \underline{B} \textit{ then } [1;0] \textit{ else} & [\max\{\underline{A}, \underline{B}\}; \overline{A}]
\end{array}
$$

- Return the union of the derived new bounds.

Contraction I: Method

Example (Contraction)

$x \in [1;3], y \in [1;2], c_1 : y = x, c_2 : y = x^2$

$(c_2, x) : x = \pm\sqrt{y} \to x = \pm\sqrt{[1;2]} = [-\sqrt{2}; -1] \cup [1; \sqrt{2}] \quad \leadsto$

$x \in [1;3] \cap ([-\sqrt{2}; -1] \cup [1; \sqrt{2}]) = [1; \sqrt{2}]$

$(c_1, y) : y = x \to y = [1; \sqrt{2}] \leadsto y \in [1;2] \cap [1; \sqrt{2}] = [1; \sqrt{2}]$

If you like to see a video about ICP:

http://www-sop.inria.fr/coprin/logiciels/ALIAS/Movie/movie_undergraduate.mpg

Learning target

- How are intervals defined?
- How are set operations on intervals defined?
- How are arithmetic operations on intervals defined?

- How can we contract the domain of a variable x for a constraint c if we can x to one side of the constraint?
- How can we contract domains otherwise using the interval Newton method?

- How can we use interval constraint propagation to decide the satisfiability of a set of real-arithmetic constraints (in an incomplete manner)?