Satisfiability Checking

26 Summary III

Prof. Dr. Erika Ábrahám

RWTH Aachen University
Informatik 2
LuFG Theory of Hybrid Systems

WS 22/23

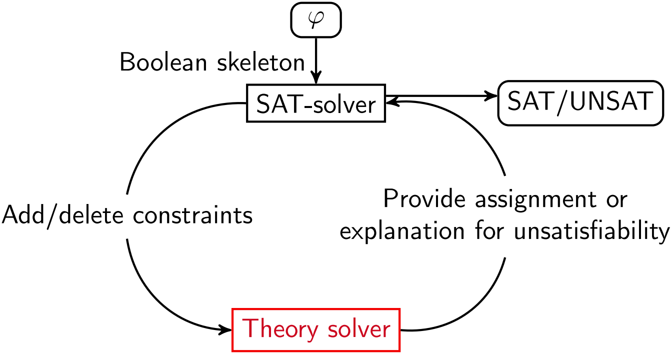
Non-linear real arithmetic

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

$$
\begin{array}{lll}
p & := const \mid x \mid (p+p) \mid (p \cdot p) & \text{polynomials} \\
c & := p < 0 \mid p = 0 \mid p > 0 & \text{(polynomial) constraints} \\
\varphi & := c \mid (\varphi \wedge \varphi) \mid \neg\varphi & \text{QFNRA formulas}
\end{array}
$$

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

Connection to SMT



Solves $\begin{pmatrix} p_1 & \sim_1 & 0 \\ & \vdots & \\ p_m & \sim_m & 0 \end{pmatrix}$ where $\begin{array}{ll} p_i \in \mathbb{Q}[x_1, \ldots, x_n], & \\ \sim_i \in \{<, \leq, =, \neq, \geq, >\} \end{array}$ for $1 \leq i \leq m$.

1. Interval constraint propagation
2. Subtropical satisfiability
3. Virtual substitution
4. Cylindrical algebraic decomposition

Basis: Interval arithmetic

- Step 1: Partially extend real arithmetic operations to $\mathbb{R} \cup \{-\infty, +\infty\}$.
- Step 2: Extend real arithmetic operations to intervals.

Definition (Interval arithmetic)

Assume real intervals $A = [\underline{A}, \overline{A}]$ and $B = [\underline{B}, \overline{B}]$.

$$
\begin{aligned}
A + B &= [\underline{A} + \underline{B}; \overline{A} + \overline{B}] \\
A - B &= [\underline{A} - \overline{B}; \overline{A} - \underline{B}] \\
A \cdot B &= [min(\underline{A} \cdot \underline{B}, \underline{A} \cdot \overline{B}, \overline{A} \cdot \underline{B}, \overline{A} \cdot \overline{B}); max(\underline{A} \cdot \underline{B}, \underline{A} \cdot \overline{B}, \overline{A} \cdot \underline{B}, \overline{A} \cdot \overline{B})] \\
A^2 &= (A \cdot A) \cap [0; +\infty) \\
A \div B &= A \cdot \frac{1}{B} = A \cdot [\frac{1}{\overline{B}}; \frac{1}{\underline{B}}] \text{ if } 0 \notin B \textit{ (extended interval division if } 0 \in B\textit{)}
\end{aligned}
$$

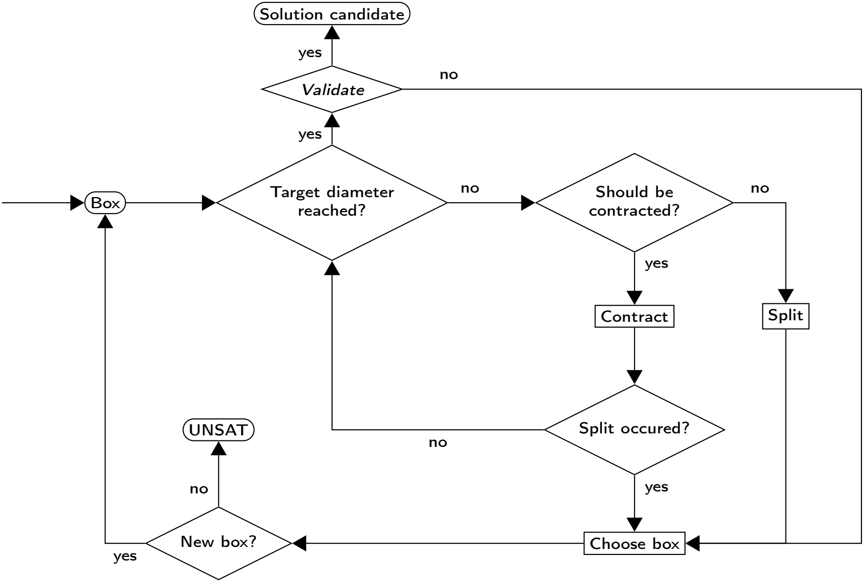
Interval constraint propagation (ICP)

- Incomplete but cheap method.
- Basic idea:
  Start with a list containing a single initial box (value domain).
  Use the input constraints to contract a non-empty box from the list.
  If no contraction possible, split a non-empty box.
- Termination: all boxes are empty (UNSAT) or there is a sufficiently small non-empty box (possibly SAT).

First contraction approach: Interval arithmetic

Second contraction approach: Interval Newton method

Algorithm overview



Contraction I: Preprocessing

Apply to all constraints:

$$e_1 \sim e_2$$

$$\downarrow$$

$$r_1 \cdot m_1 + \ldots + r_k \cdot m_k \sim e_{linear}$$

coefficients from $\mathbb{Q}$

non-linear monomials

add fresh variables h_i, $i = 1, \ldots, k$, with initial domain from $h_i = e_{linear} - \frac{1}{r_i} \sum_{j \in \{1,\ldots,i-1,i+1,\ldots,k\}} r_j m_j$ via interval arithmetic

$$\downarrow$$

$$r_1 \cdot h_1 + \ldots + r_k \cdot h_k \sim e_{linear}$$

$$h_i - m_i = 0,\ i = 1, \ldots, k$$

Contraction I: Method

Choose contraction candidate (c, x)

constraint c

variable x in c with current interval doma

transform c to $x \sim e$, where e does not contain x

possible due to preprocessing

Replace in e all variables by their bounds and evalute via interval arithmetic

Result: a set of intervals

Launch a new search branch for each B from the result,
with contracted x domain according to $\sim$:

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

Contraction II: Preprocessing

Apply to all inequalities:

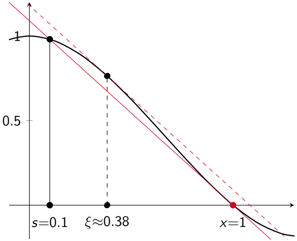
$$e_1 \sim e_2 \xrightarrow{} \quad h - (e_1 - e_2) = 0 \qquad h \sim 0$$

add fresh variable h with initial domain from $h = e_1 - e_2$ via interval arithmetic

Contraction II: Method

Inequations: $h \sim 0$ as in the first method.
Equations: $f(x) = 0$ (f a polynomial), we handled only the univariate case

- Input:
  - interval A
  - univariate polynomial constraint $f(x) = 0$
  - sample point $s \in A$
- Output: contracted interval $A_{new} = A \cap (s - \frac{f(s)}{f'(A)})$
  ($f'(x)$: first derivative of $f(x)$)



Heuristics to choose CCs

- Relative contraction

$$gain_{rel} = \frac{D_{old} - D_{new}}{D_{old}} = 1 - \frac{D_{new}}{D_{old}}$$

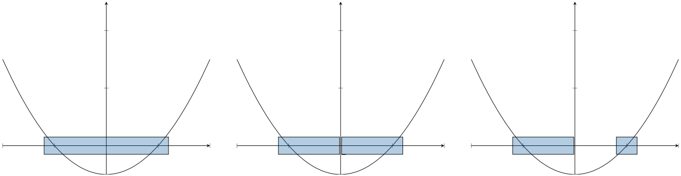
  is in general not predictable.

- Heuristics: use weights $W_k^{(ij)} \in [0; 1]$ to estimate

$$W_{k+1}^{(ij)} = W_k^{(ij)} + \alpha(gain_{rel,k+1}^{(ij)} - W_k^{(ij)})$$

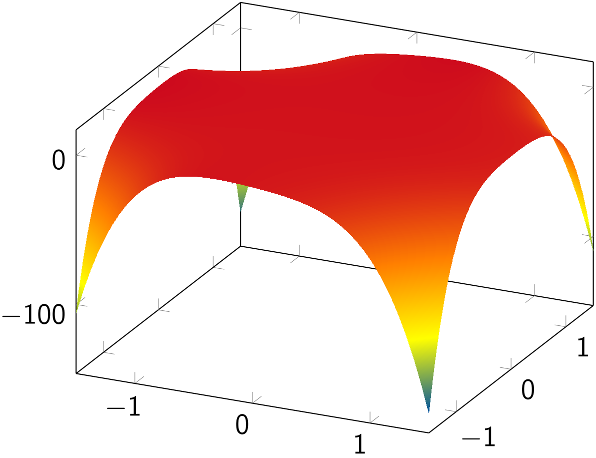
Further aspects

- Assure termination: When the weight of all CCs is below the threshold we do not make progress $\rightarrow$ split the box.



- Handle linear constraints separately
- Store search tree for incrementality and explanations

Intuition



$$f(x,y) = y + 2xy^3 - 3x^2y^2 - x^3 - 4x^4y^4$$

Solving equations

1. Assure $p(1, \ldots, 1) < 0$

2. Find x_+ with $p(x_+) > 0$ for $v \in \mathit{frame}^+(p)$ by solving

$$n^T v > b \wedge \bigwedge_{u \in \mathit{frame}(p) \setminus \{v\}} n^T u < b$$

and find $a \in \{2, 4, 8, \ldots\}$ with $p(a^{n^T}) > 0$

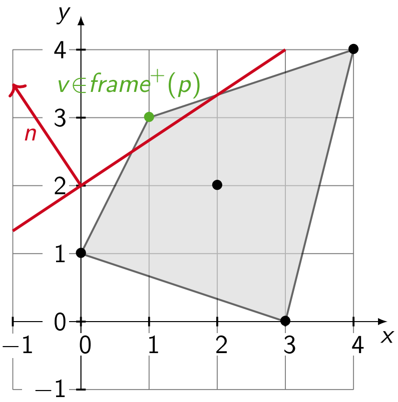
Incomplete!

3. Construct univariate p^* encoding p

on the line from $(-1, \ldots, -1)$ to x_+

Find root $p^*(t_0) = 0$

Transform t_0 to x_0 with $p(x_0) = 0$



Virtual substitution method

- Quantifier elimination, here only existential fragment

$$\exists x_1.\ldots.\exists x_n.\varphi_n \quad \equiv \quad \exists x_1.\ldots.\exists x_{n-1}.\varphi_{n-1}$$

- Restriction: x_n at most quadratic in φ_n
- Basic idea:
  - solution equation
  - $\rightsquigarrow$ finitely many test candidates $T \subset \mathbb{R}$
  - $\rightsquigarrow$ virtually substitute test candidates for x_n:

$$\exists x_1.\ldots.\exists x_n.\varphi_n \quad \equiv \quad \exists x_1.\ldots.\exists x_{n-1}.\bigvee_{t\in T}\varphi_n[t /\!/ x_n]$$

Construction of the set of test candidates T

Given: constraint $p \sim 0$, $\quad p = ax^2 + bx + c$, $\quad \sim \in \{=, <, >, \leq, \geq, \neq\}$

p is constant in $x \rightsquigarrow$ potential solution interval $(-\infty, \infty)$

Roots of p in x if not constant:

Linear in x :	$x_0 = -\frac{c}{b}$	, if	$a = 0 \land b \neq 0$
Quadratic in x :	$x_1 = \frac{-b+\sqrt{b^2-4ac}}{2a}$	, if	$a \neq 0 \land b^2 - 4ac \geq 0$
	$x_2 = \frac{-b-\sqrt{b^2-4ac}}{2a}$	, if	$a \neq 0 \land b^2 - 4ac > 0$

Potential solution intervals:

constraint	potential solution intervals ($0 \leq i,\ j \leq 2,\ i \neq j$)				
$p = 0$		$[x_i,\ x_i]$			$(-\infty,\ \infty)$
$p < 0 \quad p > 0 \quad p \neq 0$	$(-\infty,\ x_i)$		$(x_i,\ x_j)$	$(x_i,\ \infty)$	$(-\infty,\ \infty)$
$p \leq 0 \quad p \geq 0$	$(-\infty,\ x_i]$		$[x_i,\ x_j]$	$[x_i,\ \infty)$	$(-\infty,\ \infty)$

Construction of the set of test candidates T

constraints	potential solution intervals $(0 \leq i,\ j \leq 2,\ i \neq j)$				
$p = 0$		$[x_i,\ x_i]$			$(-\infty,\ \infty)$
$p < 0 \quad p > 0 \quad p \neq 0$	$(-\infty,\ x_i)$		$(x_i,\ x_j)$	$(x_i,\ \infty)$	$(-\infty,\ \infty)$
$p \leq 0 \quad p \geq 0$	$(-\infty,\ x_i]$		$[x_i,\ x_j]$	$[x_i,\ \infty)$	$(-\infty,\ \infty)$

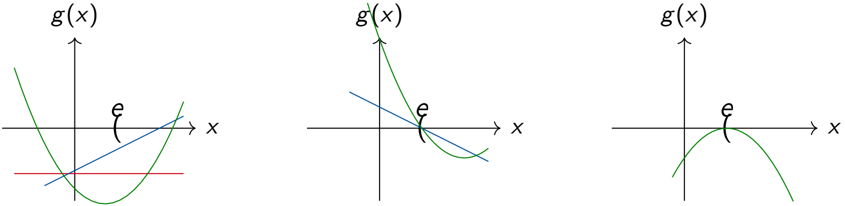
Test candidates: smallest values from each potential solution interval:

- $p = 0,\ p \leq 0,\ p \geq 0$
  1. Roots of the polynomial p
  2. $-\infty$ $(:=$ sufficiently small value)

- $p < 0,\ p > 0,\ p \neq 0$
  1. Roots of the polynomial p plus an infinitesimal ϵ
  2. $-\infty$

Virtual substitution of a variable by a test candidate

Example: $(g(x) < 0)[e + \epsilon /\!\!/ x]$



Case 1 Case 2 Case 3

Result:

$$\underbrace{g[e/\!\!/x] < 0}_{\text{Case 1}} \vee \underbrace{g[e/\!\!/x] = 0 \wedge g'[e/\!\!/x] < 0}_{\text{Case 2}} \vee \underbrace{g[e/\!\!/x] = 0 \wedge g'[e/\!\!/x] = 0 \wedge g''[e/\!\!/x] < 0}_{\text{Case 3}}$$

26 Summary III

Cylindrical algebraic decomposition

Cells are...

Cylindrical	$\rightsquigarrow$	... ordered into stack-like cylinders
Algebraic	$\rightsquigarrow$	... defined by real-algebraic formulas
Decomposition	$\rightsquigarrow$	... disjoint and cover $\mathbb{R}^n$

CAD in one dimension for univariate $p(x)$

- Compute Cauchy bound for p: $C = 1 + \max_{i=1,\dots,k-1} \frac{|a_i|}{|a_k|}$
  $\rightsquigarrow$ all real roots of p are within $[-C, C]$

- Compute Sturm sequence for p:

$$
\begin{aligned}
p_0 &= p, \\
p_1 &= p', \\
p_2 &= -rem(p_0, p_1), \quad \dots, \\
p_k &= -rem(p_{k-2}, p_{k-1}) \qquad \text{with } rem(p_{k-1}, p_k) = 0
\end{aligned}
$$

  $\sigma(\cdot)$: number of sign changes (ignoring zeros) in the Sturm sequence
  number of real roots of $p(x)$ in interval $(a, b]$: $\sigma(a) - \sigma(b)$

- Isolate the roots $\xi_1, \dots, \xi_m$ of p by iteratively splitting $[-C, C]$ where needed
- Choose samples $r_0, \dots, r_{2m}$ with

$$r_0 < \xi_1 = r_1 < r_2 < \xi_2 = r_3 < \dots < \xi_m = r_{2m-1} < r_{2m} \,.$$

The CAD in a nutshell

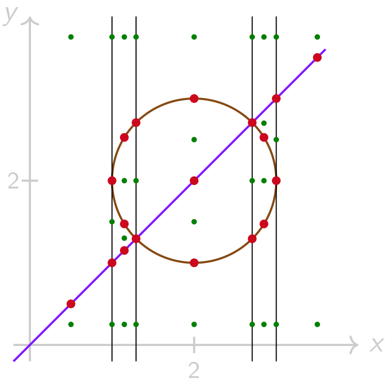
Projection | Construction

$$\begin{tikzcd}[row sep=large]
\rightarrow P_n \subseteq \mathbb{Q}[x_1, \ldots, x_n] \arrow[d, "\text{eliminate } x_n"'] & Z_1 \times \cdots \times Z_n \subseteq \mathbb{R}^n \\
P_{n-1} \subseteq \mathbb{Q}[x_1, \ldots, x_{n-1}] \arrow[d, "\text{eliminate } x_{n-1}"'] & \vdots \arrow[u, "\text{roots of } \{p(z) | p \in P_n, z \in Z_1 \times \cdots \times Z_{n-1}\}"'] \\
\vdots \arrow[d, "\text{eliminate } x_2"'] & Z_1 \times Z_2 \subseteq \mathbb{R}^2 \arrow[u, "\text{roots of } \{p(z) \mid p \in P_3, z \in Z_1 \times Z_2\}"'] \\
P_1 \subseteq \mathbb{Q}[x_1] \arrow[r, bend right, "\text{roots of } P_1"'] & Z_1 \subseteq \mathbb{R} \arrow[u, "\text{roots of } \{p(z) \mid p \in P_2, z \in Z_1\}"']
\end{tikzcd}$$

Samples are: all roots, a sample between each two neighboured roots, one sample below the smallest and one above the largest root

Example: CAD sample construction

$$P = \begin{pmatrix} (x-2)^2 + (y-2)^2 - 1, \\ x - y \end{pmatrix}$$



One-dimensional samples for $\mathrm{proj}(P)$

$\{0, 1, 2 - \frac{\sqrt{2}}{2},\ 2 + \frac{\sqrt{2}}{2},\ 3\}$
$\{-0.5,\ 0.5,\ 1.135,$
$2,\ 2.835,\ 3.5\}$

Extending samples to $\mathbb{R}^2$

- $(2-2)^2 + (y-2)^2 - 1$ yields $(2, 1)$ and $(2, 3)$,
- $(2 - \frac{\sqrt{2}}{2} - 2)^2 + (y-2)^2 - 1$ yields $(2 - \frac{\sqrt{2}}{2},\ 2 + \frac{\sqrt{2}}{2})$ and $(2 - \frac{\sqrt{2}}{2},\ 2 + \frac{\sqrt{2}}{2})$, etc.