Satisfiability Checking

24 The cylindrical algebraic decomposition method I

Prof. Dr. Erika Ábrahám

RWTH Aachen University
Informatik 2
LuFG Theory of Hybrid Systems

WS 22/23

Reminder: Real arithmetic (NRA)

Syntax

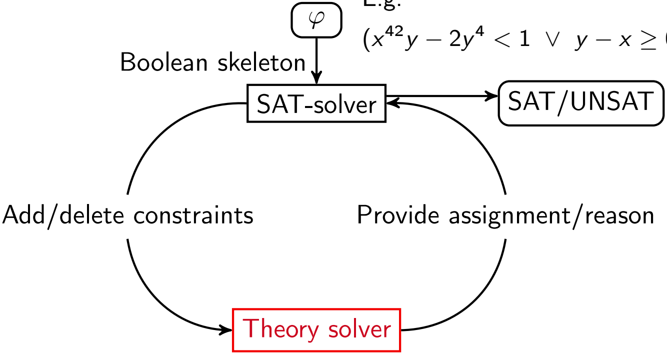
$$\begin{array}{rrcccccccc}
\text{Polynomials:} & p & ::= & const & \mid & x & \mid & (p+p) & \mid & (p \cdot p) \\
\text{Constraints:} & c & ::= & p=0 & \mid & p<0 & \mid & p>0 & & \\
\text{Formulas:} & \varphi & ::= & c & \mid & \neg\varphi & \mid & \varphi \wedge \varphi & \mid & \exists x.\varphi
\end{array}$$

where $const \in \mathbb{Q}$ is a constant and x a real-valued variable.

- Syntactic sugar: $\neq$, $\leq$, $\geq$, $\forall$, $\vee$, $\rightarrow$, $\ldots$
- Normal form: $p = a_1 x_1^{e_{1,1}} \cdots x_n^{e_{1,n}} + \cdots + a_k x_1^{e_{k,1}} \cdots x_n^{e_{k,n}}$
  第一个term, 其中包含X1, ...Xn　第k个term, 其中包含X1, ...Xn
- $\deg(p) := \max_{i\in\{1,\ldots,k\}}(\sum_{j=1}^{n} e_{i,j})$ degree of p
  对每个term, degree等于其中所有变量的幂指数求和　多项式的degree等于degree最大的term
- Though CAD can be applied to general NRA formulas, for simplicity, here we consider only the satisfiability check of quantifier-free formulas (existential fragment of NRA).

Reminder: Connection to SMT

E.g.
$(x^{42}y - 2y^4 < 1 \ \lor \ y - x \geq 0) \land x^2 - y > 0$



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

1. What is a cylindrical algebraic decomposition?
2. Computing cylindrical algebraic decompositions for $\mathbb{R}$
3. Computing cylindrical algebraic decompositions for $\mathbb{R}^n$ (next lecture)

NRA solution space (1)

解集

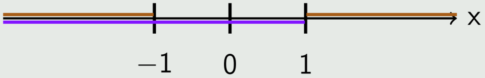
Solution set: $\mathcal{S}\begin{pmatrix} p_1 \sim_1 0 \\ \vdots \\ p_m \sim_m 0 \end{pmatrix} = \{a \in \mathbb{R}^n \mid p_i(a) \sim_i 0 \textit{ for all } 1 \leq i \leq m\},$

能满足所有constraint的变量取值

where $p_i \in \mathbb{Q}[x_1, \ldots, x_n]$, $\sim_i \in \{\leq, <, =, \neq, >, \geq\}$ for $1 \leq i \leq m$.

Example (one-dimensional)

$$\mathcal{S}\begin{pmatrix} x^2 - 1 > 0 \\ 1 - x > 0 \end{pmatrix}$$



$= (-\infty, -1)$ 即同时满足两个constraint

sign-invariant region

$(-\infty,-1)$ $[-1,-1]$ $(-1,1)$ $[1,1]$ $(1,+\infty)$

NRA solution space (2)

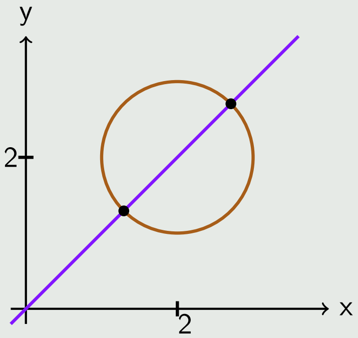
Solution set: $\mathcal{S}\begin{pmatrix} p_1 & \sim_1 & 0 \\ & \vdots & \\ p_m & \sim_m & 0 \end{pmatrix} = \{a \in \mathbb{R}^n \mid p_i(a) \sim_i 0 \textit{ for all } 1 \leq i \leq m\}$,

where $p_i \in \mathbb{Q}[x_1, \ldots, x_n]$, $\sim_i \in \{\leq, <, =, \neq, >, \geq\}$ for $1 \leq i \leq m$.

Example (two-dimensional)

$$\mathcal{S}\begin{pmatrix} (x-2)^2 + \\ (y-2)^2 - 1 = 0 \\ \\ x - y = 0 \end{pmatrix}$$

$$= \left\{\left(2 - \frac{\sqrt{2}}{2}, 2 - \frac{\sqrt{2}}{2}\right), \left(2 + \frac{\sqrt{2}}{2}, 2 + \frac{\sqrt{2}}{2}\right)\right\}$$



Sign-invariant regions

Region

region: 非空, 连续的子集

A region of $\mathbb{R}^n$ is a non-empty, connected subset of $\mathbb{R}^n$.

Example

- For $a, b \in \mathbb{R}$, the set defined by the interval $(a, b) \subseteq \mathbb{R}$ and the point set $\{a\} \subseteq \mathbb{R}$ are regions of $\mathbb{R}$.

  开区间 点..

  1.开区间 2.端点 都是 region

- If R and R' are regions of $\mathbb{R}$ then $R \times R'$ is a region of $\mathbb{R}^2$.

Sign of a polynomial

We define $\mathrm{sgn} : \mathbb{R} \to \{-1, 0, 1\}$ by

$$\mathrm{sgn}(a) \quad := \begin{cases} -1, & a < 0, \\ 0, & a = 0, \\ 1, & a > 0. \end{cases}$$

P: 多项式

P-sign-invariant:多项式的正负保持不变

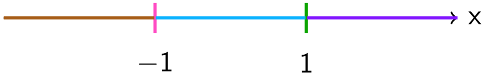
Let $P = \{p_1, \ldots, p_m\} \subset \mathbb{Q}[x_1, \ldots, x_n]$. A region $R \subseteq \mathbb{R}^n$ is P-sign-invariant if $\mathrm{sgn}(p_i(a)) = \mathrm{sgn}(p_i(b))$ for all $i \in \{1, \ldots, m\}$ and $a, b \in R$.

即在变量取值的某一region上, 所有constraint的正负保持不变

Example: Sign-invariant regions

$P = \{x^2 - 1,\ 1 - x\}$

$\mathrm{sgn}(x^2 - 1)$	1	0	-1	0	1
$\mathrm{sgn}(1 - x)$	1	1	1	0	-1

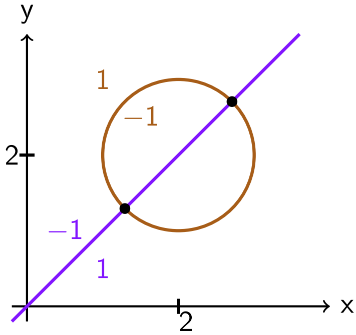


The cylindrical algebraic decomposition method

- decomposes $\mathbb{R}^n$ into finitely many P-sign-invariant regions,
- selects a sample from each region and
- checks whether the constraints are satisfied by any sample.

Example: Sign-invariant regions

$$P = \{(x-2)^2 + (y-2)^2 - 1 = 0, x - y = 0\}$$



Cylindrical algebraic decomposition

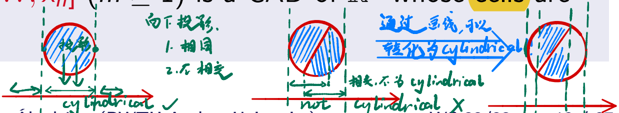
Definition

- A decomposition of $\mathbb{R}^n$ ($n \geq 1$) is a finite set $\mathcal{C}$ of pairwise disjoint regions in $\mathbb{R}^n$ with $\bigcup_{C \in \mathcal{C}} C = \mathbb{R}^n$.

- A decomposition $\mathcal{C}$ of $\mathbb{R}^n$ is semi-algebraic if each $C \in \mathcal{C}$ can be constructed by finite union, intersection and complementation of solution sets of polynomial constraints $p \sim 0$, $p \in \mathbb{Q}[x_1, \ldots, x_n]$.
- A decomposition $\mathcal{C}$ of $\mathbb{R}^n$ is cylindrical if either $n = 1$ or the set of the projections of the regions in $\mathcal{C}$ to the first $n-1$ dimensions is a cylindrical decomposition of $\mathbb{R}^{n-1}$. projection either identical or disjoint
- A cylindrical algebraic decomposition (CAD) of $\mathbb{R}^n$ is a cylindrical and semi-algebraic decomposition of $\mathbb{R}^n$. We call $C \in \mathcal{C}$ a cell.

此时 region 在 X 上的投影
在相同区间内!!!
为 cylindrical!!!

- A CAD for $P \subset \mathbb{Q}[x_1, \ldots, x_n]$ ($m \geq 1$) is a CAD of $\mathbb{R}^n$ whose cells are all P-sign-invariant.

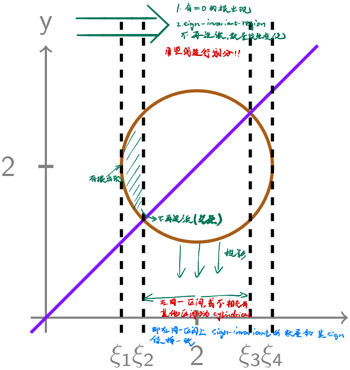


Example: CAD with 47 cells

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

The projected CAD cells in $\mathbb{R}$ are:

$$(-\infty, \xi_1),\ \{\xi_1\},\ (\xi_1, \xi_2),\ \{\xi_2\},\ (\xi_2, \xi_3),\ \{\xi_3\},\ (\xi_3, \xi_4),\ \{\xi_4\},\ (\xi_4, \infty)$$



Reminder

A CAD for P is a

- decomposition of $\mathbb{R}^n$
- which is cylindrical,
- semi-algebraic,
- and its cells are P-sign-invariant.

1. What is a cylindrical algebraic decomposition?
2. Computing cylindrical algebraic decompositions for $\mathbb{R}$
3. Computing cylindrical algebraic decompositions for $\mathbb{R}^n$ (next lecture)

Real roots (zeros) of univariate polynomials

The sign of a polynomial changes only at its (real) roots.

Remark

A polynomial $p \in \mathbb{Q}[x]$ has between 0 and $\deg(p)$ real roots.

Example

- $x^3 - 6x^2 + 11x - 6$ has rational roots: 1, 2 and 3.
- $x^3 - x^2 - 2x + 2$ has one rational and two irrational roots: 1, $-\sqrt{2}$ and $\sqrt{2}$.
- $x^5 - 3x^4 + x^3 - x^2 + 2x - 2$ has only one real root ≈ 2.70312, not representable by radicals.

根基,多用于代数领域, =root

Representing real roots (real algebraic numbers)

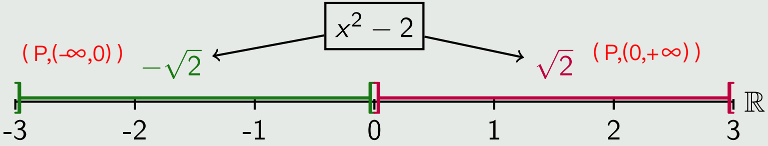
Interval representation

An interval representation (of a real root) is a pair (p, I) of a univariate polynomial p with rational coefficients and a non-empty open interval $I = (\ell, r) \subseteq \mathbb{R}$, $\ell, r \in \mathbb{Q} \cup \{-\infty, \infty\}$ such that I contains exactly one real root of p.

!! open interval !!
如果为closed interval, 则错误

$$\Big(\underbrace{p,}_{\in \mathbb{Q}[x]} \quad \underbrace{(\ell, \; r)}_{\text{exactly one real root of } p \text{ in the interval } (\ell, r)} \Big)$$

Example



Cauchy bound

求出的是所有根的范围

Cauchy bound

Assume a univariate polynomial

$$p = a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x^1 + a_0 x^0 \in \mathbb{Q}[x]$$

with $a_k \neq 0$. If $\xi \in \mathbb{R}$ is a (real) root of p (i.e. $p(\xi) = 0$) then

ai: 常数项a0也包含在内

$$|\xi| \leq 1 + \max_{i=0,\ldots,k-1} \frac{|a_i|}{|a_k|} := C \quad \textit{(called the Cauchy bound of } p\textit{)} .$$

Example

- $x^2 - 1 \quad \rightsquigarrow \quad C = 2$
- $x^2 - 2 \quad \rightsquigarrow \quad C = 3$
- $5 \cdot (x^2 - 2) = 5x^2 - 10 \quad \rightsquigarrow \quad C = 3$
- $(x-3) \cdot (x-5) = x^2 - 8x + 15 \quad \rightsquigarrow \quad C = 16$

$c = 1 + \max\left\{ \frac{|-8|}{|1|}, \frac{|15|}{|1|} \right\} = 16$

Sturm sequence

A Sturm sequence for p allows us to count the real roots of p in an interval.

Sturm's theorem

Assume a square-free (no square factors, i.e., no repeated roots) univariate polynomial $p = a_k x^k + a_{k-1}x^{k-1} + \ldots + a_1 x^1 + a_0 x^0 \in \mathbb{Q}[x]$ with $a_k \neq 0$. For the Sturm sequence $p_0, p_1, \ldots, p_l$ with

- $p_0 = p$
- $p_1 = p'$ (where p' is the derivative of p)
- $p_i = -rem(p_{i-2}, p_{i-1})$ for $i = 2, \ldots, l$ (where rem is the remainder of the polynomial division of p_{i-2} by p_{i-1}) 下一项=负的(第一项÷ 第二项)的余数
- $rem(p_{l-1}, p_l) = 0$ 如果余数=0, 则暂停

let $\sigma(\xi)$ denote the number of sign changes (ignoring zeroes) in the sequence

$$p_0(\xi),\ p_1(\xi),\ p_2(\xi),\ \ldots,\ p_l(\xi)\ .$$

Then for each $a, b \in \mathbb{R}$ with $a < b$, the number of distinct real roots of p in $(a, b]$ is $\sigma(a) - \sigma(b)$.
左开 右闭

Online tools

If you like you can experiment with the online Sturm sequence calculator

`https://planetcalc.com/7719/`

Sturm sequence: Example

$p = x^2 + x + 1$ with Cauchy bound $C = 2$, $p(-2) \neq 0$
$\rightsquigarrow$ all real roots are in $(-2, 2]$

Sturm sequence	values at	
	-2	2
$p_0 = x^2 + x + 1$	$+3$	$+7$
$p_1 = 2x + 1$	-3	$+5$
$p_2 = -\frac{3}{4}$	$-\frac{3}{4}$	$-\frac{3}{4}$
# sign changes $\sigma(\cdot)$	1	1

Thus this polynomial has $1 - 1 = 0$ real roots (in $(-2, 2]$).

Sturm sequence: Example

$$p = (x+1)(x+2)(x+3) = x^3 + 6x^2 + 11x + 6,\ C = 12$$

0不需要考虑.(对于 sign change 来说)

Sturm sequence	values at				
	-12	-3	-2	-1	12
$p_0 = x^3 + 6x^2 + 11x + 6$	$-$	0	0	0	$+$
$p_1 = 3x^2 + 12x + 11$	$+$	$+$	$-$	$+$	$+$
$p_2 = \frac{2}{3}x + \frac{4}{3}$	$-$	$-$	0	$+$	$+$
$p_3 = 1$	$+$	$+$	$+$	$+$	$+$
# sign changes $\sigma(\cdot)$	3	2	1	0	0

$$
\begin{array}{llll}
\sigma(-12) & -\sigma(12) & = 3 - 0 = 3 \text{ real roots} & \text{in } (-12, 12] \\
\sigma(-3) & -\sigma(12) & = 2 - 0 = 2 \text{ real roots} & \text{in } (-3, 12] \\
\sigma(-2) & -\sigma(12) & = 1 - 0 = 1 \text{ real root} & \text{in } (-2, 12] \\
\sigma(-1) & -\sigma(12) & = 0 - 0 = 0 \text{ real root} & \text{in } (-1, 12] \\
\sigma(-12) & -\sigma(-1) & = 3 - 0 = 3 \text{ real roots} & \text{in } (-12, -1]
\end{array}
$$

Sturm sequence: Example

$p = (x+1)(x+2)(x+3) = x^3 + 6x^2 + 11x + 6,\ C = 12$

Sturm sequence	values at				
	-12	-3	-2	-1	12
$p_0 = x^3 + 6x^2 + 11x + 6$	$-$	0	0	0	$+$
$p_1 = 3x^2 + 12x + 11$	$+$	$+$	$-$	$+$	$+$
$p_2 = \frac{2}{3}x + \frac{4}{3}$	$-$	$-$	0	$+$	$+$
$p_3 = 1$	$+$	$+$	$+$	$+$	$+$
# sign changes	3	2	1	0	0

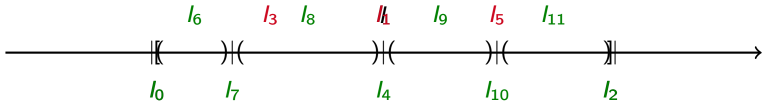
We can count real roots also for right-open intervals:

- $\sigma(-12) - \sigma(12) = 3 - 0 = 3$ real roots in $(-12, 12]$
  得到的结果为左开右闭
  $p(12) > 0 \rightsquigarrow$ there are $3 - 0 = 3$ real roots in $(-12, 12)$
  计算右端值
  将左开右闭 ⇒ open interval
- $\sigma(-12) - \sigma(-1) = 3 - 0 = 3$ real roots in $(-12, -1]$
  $p(-1) = 0 \rightsquigarrow$ there are $3 - 1 = 2$ real roots in $(-12, -1)$

Assume a set $P = \{p_1 \sim_1 0, \ldots, p_k \sim_k 0\}$ of univariate polynomial constraints with $p_i \in \mathbb{Q}[x]$ and $\sim_i \in \{<, \leq, =, \neq, \geq, >\}$.

Real root isolation:

- Cauchy bounds $\rightsquigarrow I = [-C, C]$ contains all real roots of $p_1, \ldots, p_k$.
- Split $\rightsquigarrow [-C, -C], (-C, C), [C, C]$
- Sturm sequence $\rightsquigarrow$ count the real roots of each p_i in each interval.
- Split each sub-interval that contains
  either more then one real root of the same polynomial
  or two different roots of two different polynomials (no check for this introduced here):
  for (a, b) choose $a < c < b \rightarrow$ sub-intervals (a, c), $[c, c]$, (c, b)



CAD for $\mathbb{R}$ with respect to P:

$[(p_i, I_j), (p_i, I_j)]$ for each I_j containing a real root of a p_i and

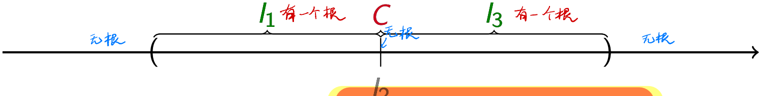
open intervals between them.

CAD for univariate polynomials: Example

- $\underbrace{x^2 - 2}_{p_1} > 0$
- Cauchy bound: $C = (-3, 3)$ contains all real roots of p_1
- Sturm sequence $\rightarrow$ Number of real roots of p_1 in $(-3, 3)$: 2
- Split $(-3, 3)$ into $(-3, 0)$, $[0, 0]$, $(0, 3)$
- Number of real roots of p_1 in $I_1 = (-3, 0)$: 1
- Number of real roots of p_1 in $I_2 = [0, 0]$: 0
- Number of real roots of p_1 in $I_3 = (0, 3)$: 1

strum ⇒ ( ] 根的数量
⇓
计算闭的端点正负
⇓
( ) 根的数量

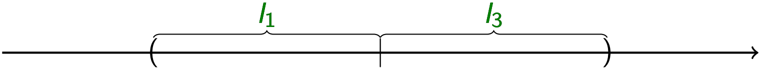
$$\text{CAD: } \left\{ (-\infty, (p_1, I_1)),\ [(p_1, I_1), (p_1, I_1)],\ ((p_1, I_1), (p_1, I_3)),\ [(p_1, I_3), (p_1, I_3)],\ ((p_1, I_3), \infty) \right\}$$



interval的端点可作为 sample point!!!

CAD for univariate polynomials: Example

- $\underbrace{x^2 - 2}_{p_1} > 0$
- $I_1 = (-3, 0)$, $I_3 = (0, 3)$
- CAD: $[(p_1, I_1), (p_1, I_1)]$, $[(p_1, I_3), (p_1, I_3)]$, $(-\infty, (p_1, I_1))$, $((p_1, I_1), (p_1, I_3))$, $((p_1, I_3), \infty)$
- Take a sample point from each CAD cell and test the constraints.
- $[(p_1, (-3, 0)), (p_1, (-3, 0))]$: sample point $(p_1, (-3, 0))$, sign 0
- $[(p_1, (0, 3)), (p_1, (0, 3))]$: sample point $(p_1, (0, 3))$, sign 0
- $(-\infty, (p_1, (-3, 0)))$: sample point -4, sign 1
- $((p_1, (-3, 0)), (p_1, (0, 3)))$: sample point 0, sign -1
- $((p_1, (0, 3)), \infty)$: sample point 4, sign 1



CAD for univariate polynomials: Incrementality

- The original method is not incremental.
- We achieve incrementality by refining the CAD.
- Previous split: $I_1 = (-3, 0)$, $I_2 = [0, 0]$, $I_3 = (0, 3)$
- New constraint: $\underbrace{x^2 - x - 1}_{p_2} > 0$
- Cauchy bound (maximum for p_1 and p_2): $C_2 = (-3, 3)$
  所有根的范围
- Number of real roots of p_2 in $I_1 = (-3, 0)$: 1
  $(p_1, I_1) \neq (p_2, I_1) \Rightarrow$ split
- Number of real roots of p_2 in $I_2 = [0, 0]$: 0
- Number of real roots of p_2 in $I_3 = (0, 3)$: 1
  $(p_1, I_3) \neq (p_2, I_3) \Rightarrow$ split

CAD for univariate polynomials: Infeasible subsets

- The original method cannot generate infeasible subsets.
- For $\mathbb{R}$ we collect for each CAD interval one constraint which is not satisfied by the interval.
- The multivariate case is more involved, but the basic idea is still similar.

1. What is a cylindrical algebraic decomposition?
2. Computing cylindrical algebraic decompositions for $\mathbb{R}$
3. Computing cylindrical algebraic decompositions for $\mathbb{R}^n$ (next lecture)

Learning target

- What is a cylindrical algebraic decomposition for a set of polynomials?
- How to compute it for the univariate case?
- How to compute it for the multivariate case?
- Given a graphical representation of the real roots of some polynomials, how to illustrate their CAD graphically?