Satisfiability Checking

Cylindrical Algebraic Decomposition

Prof. Dr. Erika Ábrahám

RWTH Aachen University
Informatik 2
LuFG Theory of Hybrid Systems

WS 19/20

Reminder: Non-linear real arithmetic (NRA)

Syntax

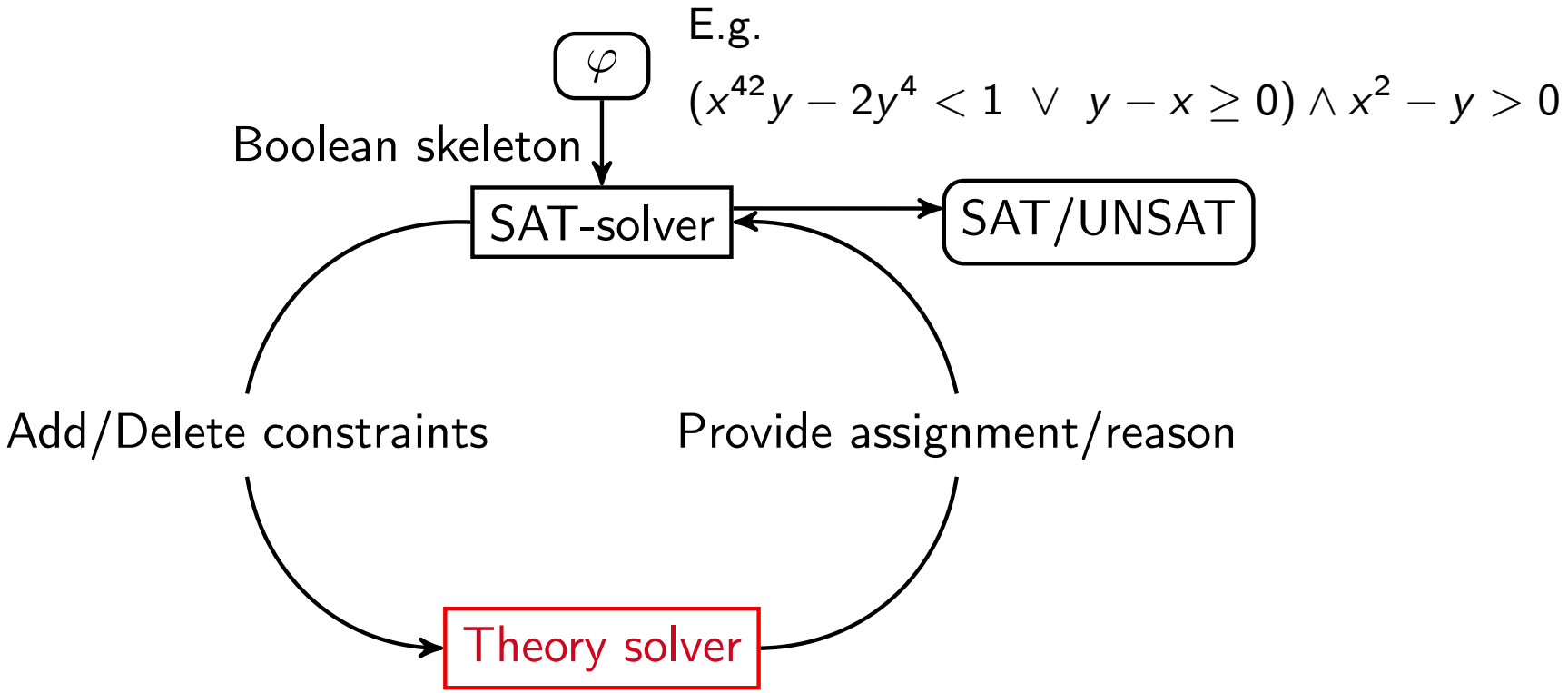
$$\begin{array}{rrcccccccc} \text{Polynomials: } & p & ::= & 0 & \mid & 1 & \mid & x & \mid & p+p \mid p-p \mid (p \cdot p) \\ \text{Constraints: } & c & ::= & p=0 & \mid & p<0 & \mid & p>0 & & \\ \text{Formulas: } & \varphi & ::= & c & \mid & \neg\varphi & \mid & \varphi \wedge \varphi & \mid & \exists x \varphi \end{array}$$

where x is a variable.

- Normal form: $p = a_1 x_1^{e_{\mathbf{1},1}} \cdots x_n^{e_{n,\mathbf{1}}} + \cdots + a_k x_1^{e_{\mathbf{1},k}} \cdots x_n^{e_{n,k}}$
- $\deg(p) := \max_{1 \leq j \leq k}(\sum_{i=1}^{n} e_{i,j})$ degree of p
- φ is non-linear if there is a polynomial p in φ with $\deg(p) > 1$.

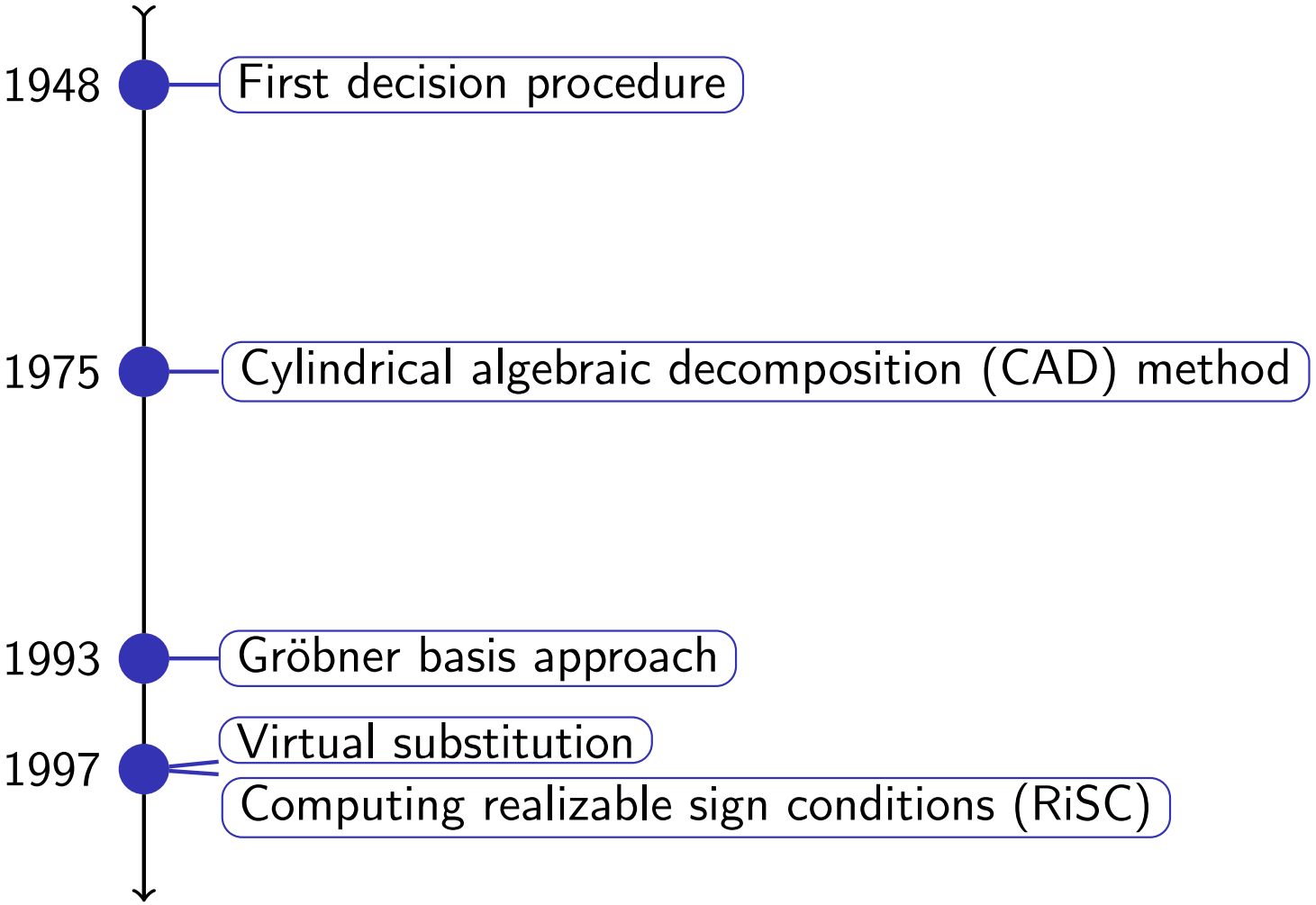
  Linear real arithmetic (LRA): $\deg(p) \leq 1$ for all polynomials p in φ.
- Syntactic sugar: $\leq$, $\geq$, $\neq$, $\forall$, $\vee$, $\rightarrow$, $\ldots$
- Though CAD can be applied to general NRA formulas, for simplicity, we consider only the satisfiability check of quantifier-free formulas (existential fragment of NRA).

Reminder: Connection to SMT

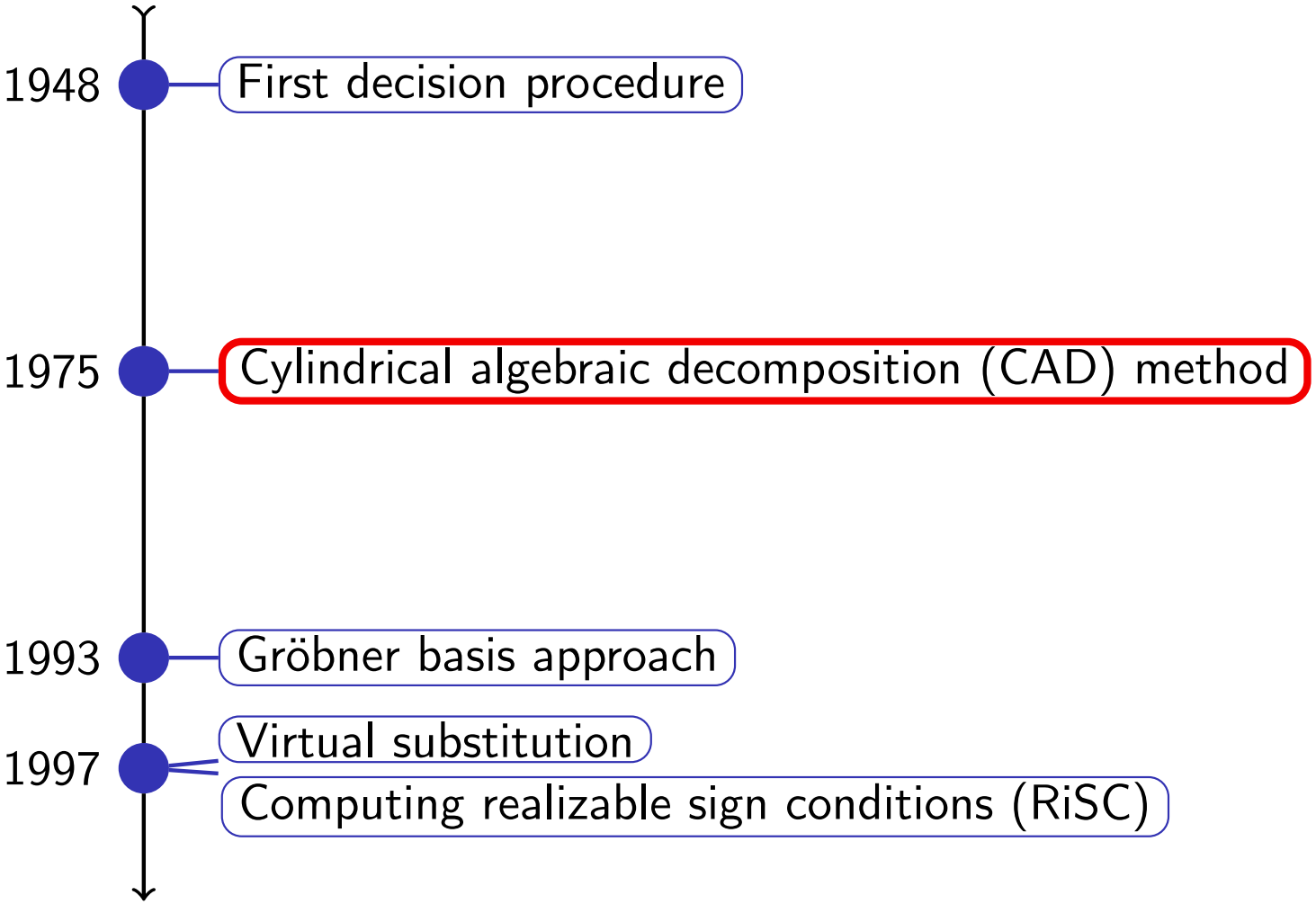


Solves $\begin{pmatrix} p_1 & \sim_1 & 0 \\ & \vdots & \\ p_m & \sim_m & 0 \end{pmatrix}$ where $\begin{array}{l} p_i \in \mathbb{Z}[x_1, \ldots, x_n], \\ \sim_i \ \in \{<, =, >\} \end{array}$ for $1 \leq i \leq m$.

Reminder: NRA solving history



Reminder: NRA solving history



Outline

Outline

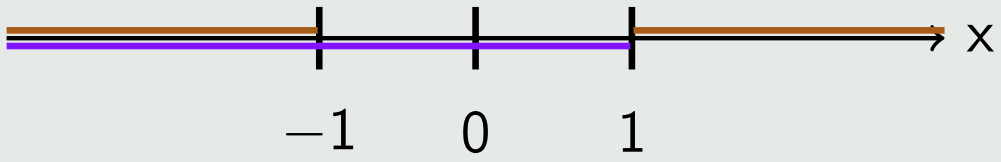
NRA solution space (1)

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

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

Example (one-dimensional)

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



$= (-\infty, -1)$

NRA solution space (2)

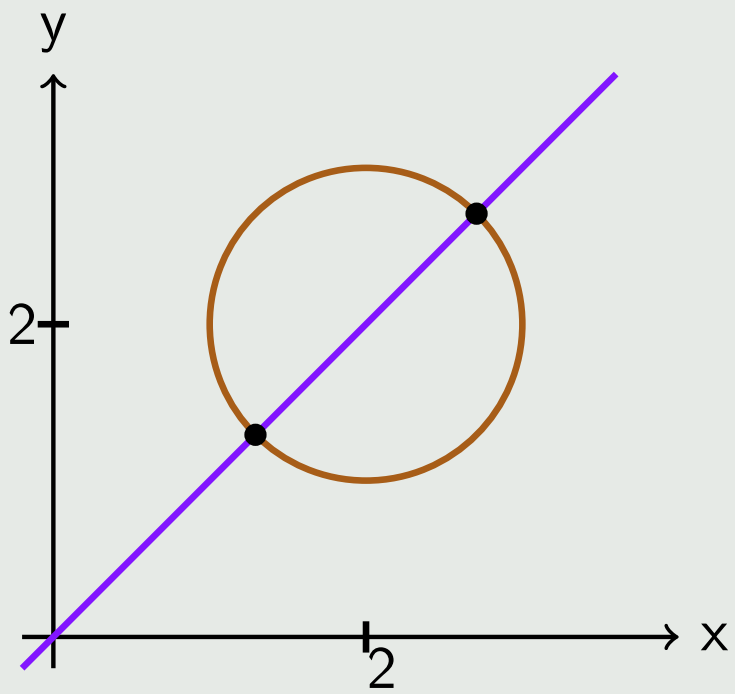
Solution set: $\mathcal{S}\begin{pmatrix} p_1 \sim_1 0 \\ \vdots \\ p_m \sim_m 0 \end{pmatrix} = \{a \in \mathbb{R}^n \mid p_i(a) \sim_i 0, 1 \leq i \leq m\},$

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

Example (two-dimensional)

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

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



Regions

Region

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

Example

- For $a, b \in \mathbb{R}$, the sets $(a, b) \subseteq \mathbb{R}$ and $\{a\} \subseteq \mathbb{R}$ are regions of $\mathbb{R}$.
- If R and R' are regions of $\mathbb{R}$ then $R \times R'$ is a region of $\mathbb{R}^2$.

Sign-invariant regions

Sign of a polynomial

Given a polynomial $p \in \mathbb{Z}[x_1, \ldots, x_n]$, $a \in \mathbb{R}^n$,

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

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

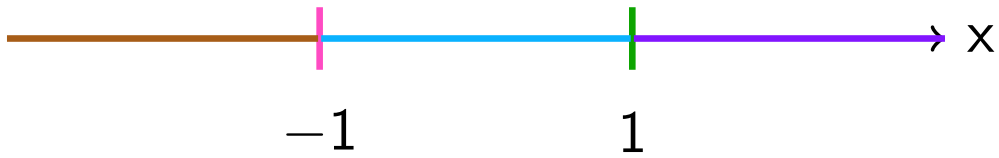
Example: Sign-invariant regions

$P = (x^2 - 1,\ 1 - x)$

$$\operatorname{sgn}(x^2-1) = \begin{cases} 1 & \text{for } x \in (-\infty,-1) \cup (1,\infty) \\ 0 & \text{for } x \in [1,1] \cup [-1,-1] \\ -1 & \text{for } x \in (-1,1) \end{cases}$$

$$\operatorname{sgn}(1-x) = \begin{cases} 1 & \text{for } x \in (-\infty,1) \\ 0 & \text{for } x \in [1,1] \\ -1 & \text{for } x \in (1,\infty) \end{cases}$$

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



Sign-invariance

Solution sets are sign-invariant sets

Given $P = (p_1, \ldots, p_m) \in \mathbb{Z}[x_1, \ldots, x_n]^m$, $\sim_i \in \{<, =, >\}$ for $1 \leq i \leq m$, then

$$\mathcal{S}\begin{pmatrix} p_1 \sim_1 0 \\ \vdots \\ p_m \sim_m 0 \end{pmatrix} = \mathcal{S}\begin{pmatrix} \operatorname{sgn}(p_1) = \sigma_1 \\ \vdots \\ \operatorname{sgn}(p_m) = \sigma_m \end{pmatrix} =: \mathcal{S}_\sigma(P)$$

with $\sigma = (\sigma_1, \ldots, \sigma_m)$ and $\sigma_i = \begin{cases} -1 & \text{if } \sim_i \text{ is } < \\ 0 & \text{if } \sim_i \text{ is } = \\ 1 & \text{if } \sim_i \text{ is } > \end{cases}$.

Let $P \in \mathbb{Z}[x_1, \ldots, x_n]^m$ and $\sigma \in \{-1, 0, 1\}^m$.

- $\mathcal{S}_\sigma(P)$ can be decomposed into finitely many P-sign-invariant regions.
- $\mathbb{R}^n$ can be decomposed into finitely many P-sign-invariant regions.

Non-trivial roots

The sign of a polynomial changes only at its roots.

Remark

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

Non-trivial roots

The sign of a polynomial changes only at its roots.

Remark

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

Example

- $x^3 - 6x^2 + 11x - 6$ has rational roots: 1, 2 and 3.

Non-trivial roots

The sign of a polynomial changes only at its roots.

Remark

A polynomial $p \in \mathbb{Z}[x]$ 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 $\sqrt{2}$.

Non-trivial roots

The sign of a polynomial changes only at its roots.

Remark

A polynomial $p \in \mathbb{Z}[x]$ 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.

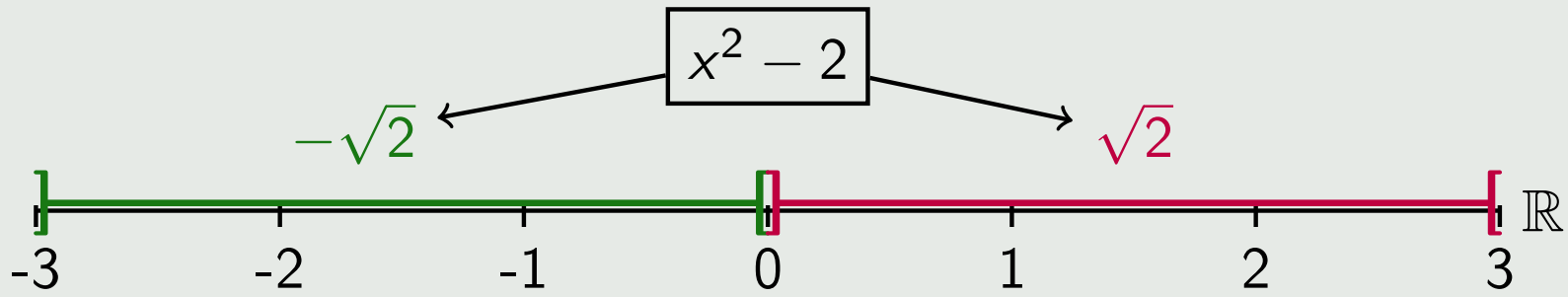
Representing real roots (real algebraic numbers)

Interval representation

$$\Big(\quad \underbrace{p,}\quad \underbrace{(\ l,\quad r\ )}\quad \Big)$$

$\in \mathbb{Z}[x]$ exactly one real root of p in (l, r)

Example



Cylindrical algebraic decomposition: Idea

- Assume a finite set $P \subset \mathbb{Z}[x_1, \ldots, x_n]$ of polynomials in n variables together with a sign condition for each polynomial in P.
- The cylindrical algebraic decomposition (CAD) method produces a decomposition of $\mathbb{R}^n$ into a finite number of P-sign-invariant regions (CAD cells).
- Take an arbitrary element (sample point) from each of the CAD cells.
- If all sign conditions are satisfied for at least one sample point then the problem is satisfiable.
- Otherwise the problem is unsatisfiable.

Outline

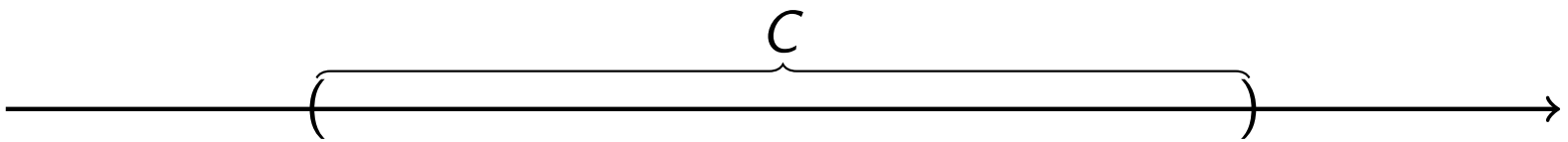
CAD for $\mathbb{R}$

CAD for $\mathbb{R}$

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

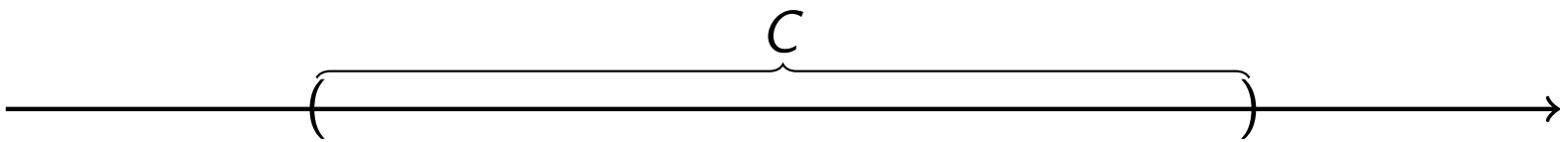
CAD for $\mathbb{R}$

- Assume a set $P = \{p_1 \sim_1 0, \ldots, p_k \sim_k 0\}$ of univariate polynomial constraints with $p_i \in \mathbb{Z}[x]$ and $\sim_i \in \{<, \leq, =, \neq, \geq, >\}$.
- Cauchy bound $\Rightarrow$ Interval $(-C, C)$ containing all real roots of $p_1, \ldots, p_k$.



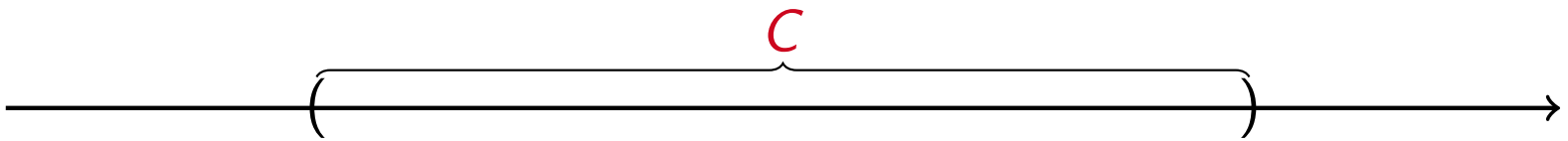
CAD for $\mathbb{R}$

- Assume a set $P = \{p_1 \sim_1 0, \ldots, p_k \sim_k 0\}$ of univariate polynomial constraints with $p_i \in \mathbb{Z}[x]$ and $\sim_i \in \{<, \leq, =, \neq, \geq, >\}$.
- Cauchy bound $\Rightarrow$ Interval $(-C, C)$ containing all real roots of $p_1, \ldots, p_k$.
- Sturm sequence $\Rightarrow$ count the real roots of each p_i in an open interval.



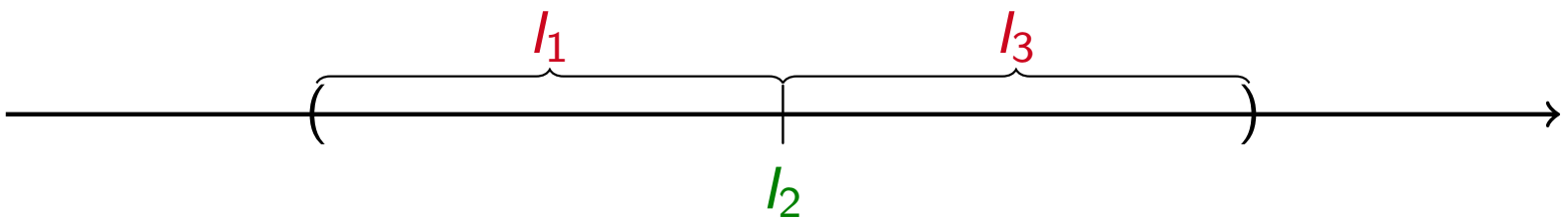
CAD for $\mathbb{R}$

- Assume a set $P = \{p_1 \sim_1 0, \ldots, p_k \sim_k 0\}$ of univariate polynomial constraints with $p_i \in \mathbb{Z}[x]$ and $\sim_i \in \{<, \leq, =, \neq, \geq, >\}$.
- Cauchy bound $\Rightarrow$ Interval $(-C, C)$ containing all real roots of $p_1, \ldots, p_k$.
- Sturm sequence $\Rightarrow$ count the real roots of each p_i in an open interval.
- Split C until each sub-interval I contains at most one real root: for (a, b) choose $a < c < b \rightarrow$ sub-intervals (a, c), $[c, c]$, (c, b)



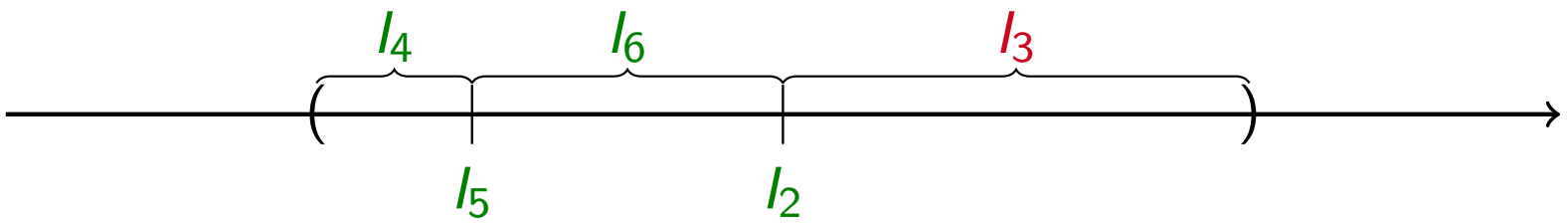
CAD for $\mathbb{R}$

- Assume a set $P = \{p_1 \sim_1 0, \ldots, p_k \sim_k 0\}$ of univariate polynomial constraints with $p_i \in \mathbb{Z}[x]$ and $\sim_i \in \{<, \leq, =, \neq, \geq, >\}$.
- Cauchy bound $\Rightarrow$ Interval $(-C, C)$ containing all real roots of $p_1, \ldots, p_k$.
- Sturm sequence $\Rightarrow$ count the real roots of each p_i in an open interval.
- Split C until each sub-interval I contains at most one real root: for (a, b) choose $a < c < b \rightarrow$ sub-intervals (a, c), $[c, c]$, (c, b)



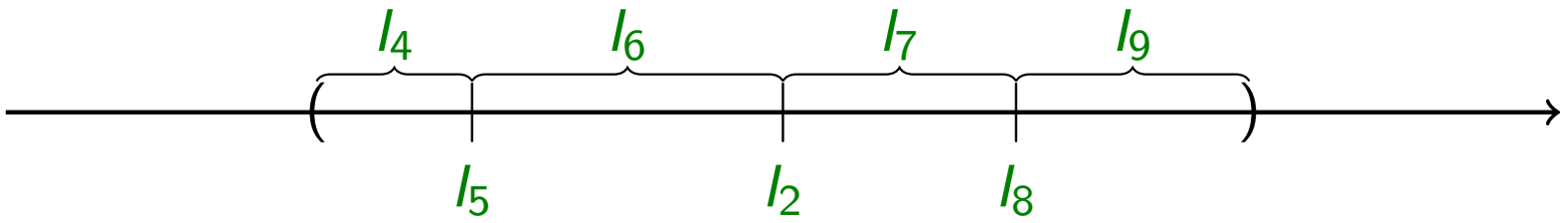
CAD for $\mathbb{R}$

- Assume a set $P = \{p_1 \sim_1 0, \ldots, p_k \sim_k 0\}$ of univariate polynomial constraints with $p_i \in \mathbb{Z}[x]$ and $\sim_i \in \{<, \leq, =, \neq, \geq, >\}$.
- Cauchy bound $\Rightarrow$ Interval $(-C, C)$ containing all real roots of $p_1, \ldots, p_k$.
- Sturm sequence $\Rightarrow$ count the real roots of each p_i in an open interval.
- Split C until each sub-interval I contains at most one real root: for (a, b) choose $a < c < b \rightarrow$ sub-intervals (a, c), $[c, c]$, (c, b)



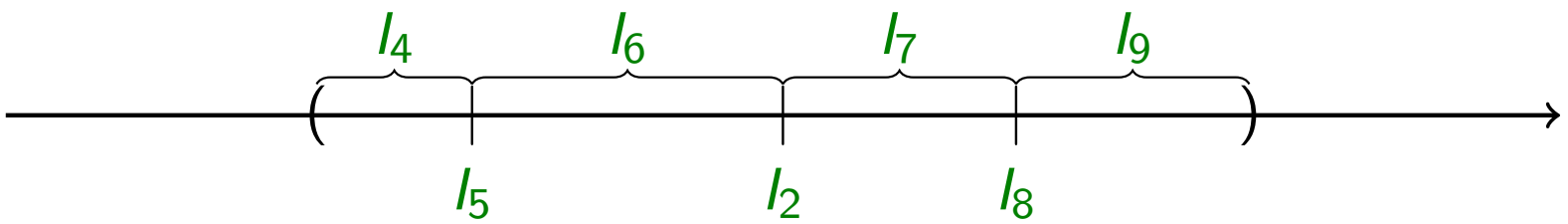
CAD for $\mathbb{R}$

- Assume a set $P = \{p_1 \sim_1 0, \ldots, p_k \sim_k 0\}$ of univariate polynomial constraints with $p_i \in \mathbb{Z}[x]$ and $\sim_i \in \{<, \leq, =, \neq, \geq, >\}$.
- Cauchy bound $\Rightarrow$ Interval $(-C, C)$ containing all real roots of $p_1, \ldots, p_k$.
- Sturm sequence $\Rightarrow$ count the real roots of each p_i in an open interval.
- Split C until each sub-interval I contains at most one real root: for (a, b) choose $a < c < b \rightarrow$ sub-intervals (a, c), $[c, c]$, (c, b)



CAD for $\mathbb{R}$

- Assume a set $P = \{p_1 \sim_1 0, \ldots, p_k \sim_k 0\}$ of univariate polynomial constraints with $p_i \in \mathbb{Z}[x]$ and $\sim_i \in \{<, \leq, =, \neq, \geq, >\}$.
- Cauchy bound $\Rightarrow$ Interval $(-C, C)$ containing all real roots of $p_1, \ldots, p_k$.
- Sturm sequence $\Rightarrow$ count the real roots of each p_i in an open interval.
- Split C until each sub-interval I contains at most one real root: for (a, b) choose $a < c < b \rightarrow$ sub-intervals (a, c), $[c, c]$, (c, b)



CAD for $\mathbb{R}$ with respect to $p_1, \ldots, p_k$:
$[(p_i, I_j), (p_i, I_j)]$ for each I_j containing a real root of a p_i and open intervals between them.

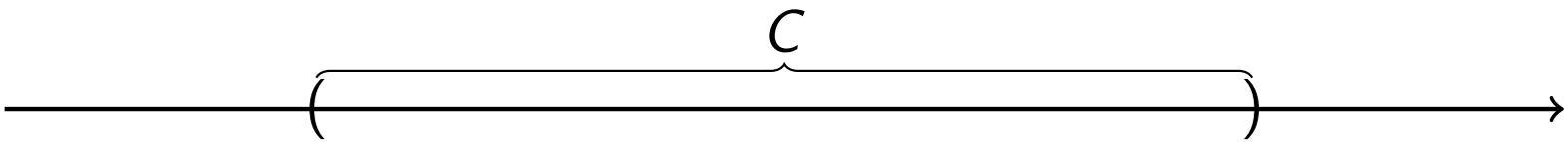
CAD for $\mathbb{R}$: Example

CAD for $\mathbb{R}$: Example

- $\underbrace{x^2 - 2}_{p_1} > 0$

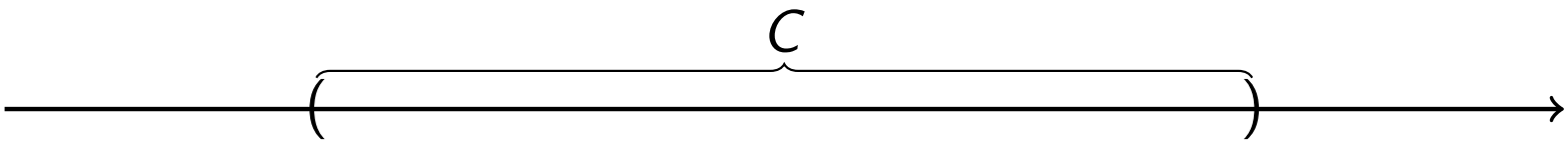
CAD for $\mathbb{R}$: Example

- $\underbrace{x^2 - 2}_{p_1} > 0$
- Cauchy bound: $C = (-3, 3)$



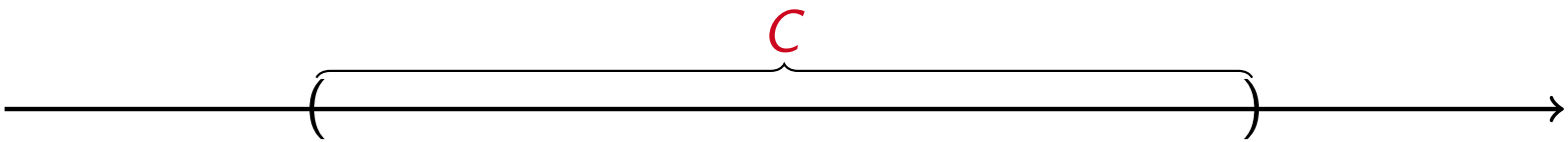
CAD for $\mathbb{R}$: Example

- $\underbrace{x^2 - 2}_{p_1} > 0$
- Cauchy bound: $C = (-3, 3)$
- Sturm sequence $\rightarrow$ Number of real roots in $(-3, 3)$: 2



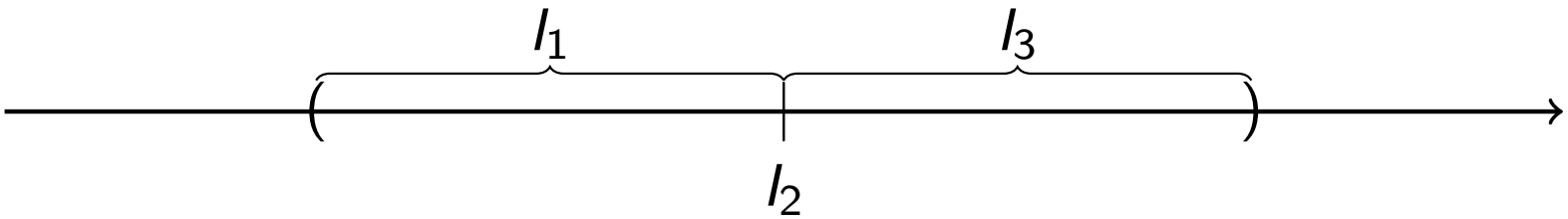
CAD for $\mathbb{R}$: Example

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



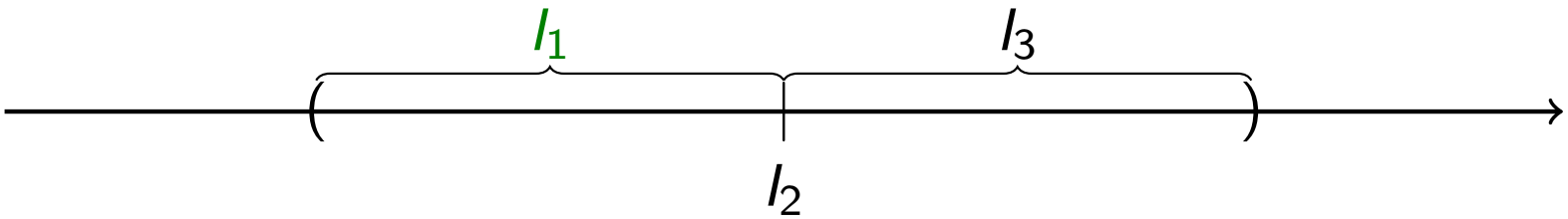
CAD for $\mathbb{R}$: Example

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



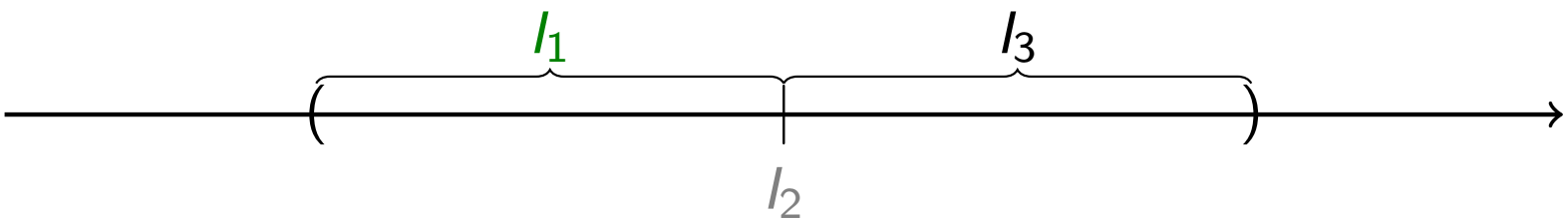
CAD for $\mathbb{R}$: Example

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



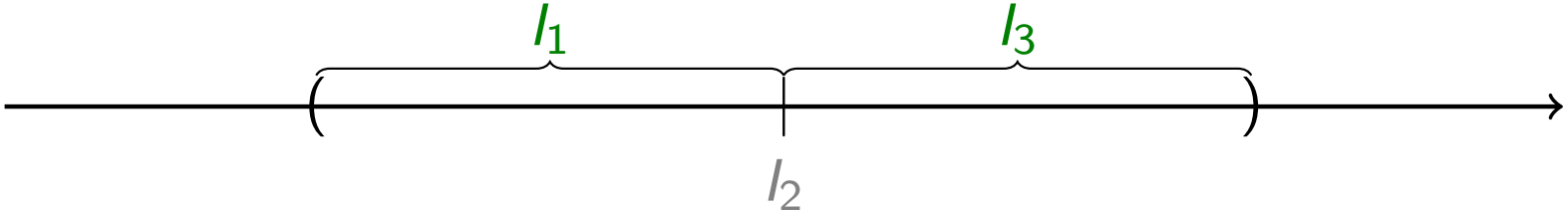
CAD for $\mathbb{R}$: Example

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



CAD for $\mathbb{R}$: Example

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



CAD for $\mathbb{R}$: Example

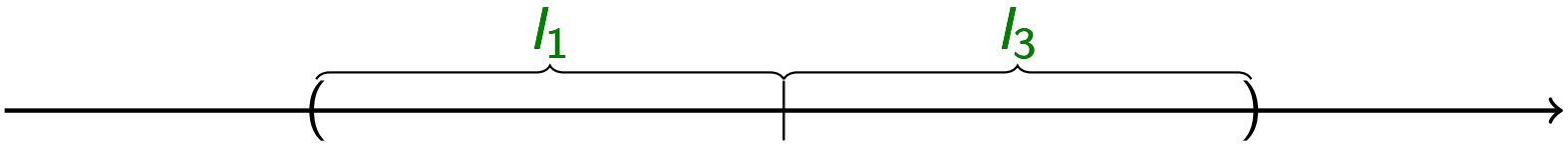
- $\underbrace{x^2 - 2}_{p_1} > 0 \quad (p_1 = x^2 - 2,\ \sigma_1 = 1)$
- $I_1 = (-3, 0),\ I_3 = (0, 3)$
- CAD: $[(p_1, I_1), (p_1, I_1)], \quad [(p_1, I_3), (p_1, I_3)],$
  $(-\infty, (p_1, I_1)), \quad ((p_1, I_1), (p_1, I_3)), \quad ((p_1, I_3), \infty)$

CAD for $\mathbb{R}$: Example

- $\underbrace{x^2 - 2}_{p_1} > 0 \quad (p_1 = x^2 - 2,\ \sigma_1 = 1)$
- $I_1 = (-3, 0),\ I_3 = (0, 3)$
- CAD: $[(p_1, I_1), (p_1, I_1)], \quad [(p_1, I_3), (p_1, I_3)],$
  $(-\infty, (p_1, I_1)), \quad ((p_1, I_1), (p_1, I_3)), \quad ((p_1, I_3), \infty)$
- Take a sample point from each CAD cell and test the sign conditions.

CAD for $\mathbb{R}$: Example

- $\underbrace{x^2 - 2}_{p_1} > 0 \quad (p_1 = x^2 - 2,\ \sigma_1 = 1)$
- $I_1 = (-3, 0),\ I_3 = (0, 3)$
- 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 sign conditions.
- $[(p_1, (-3, 0)), (p_1, (-3, 0))]$: 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 $\mathbb{R}$: Incrementality

CAD for $\mathbb{R}$: Incrementality

- The original method is not incremental.

CAD for $\mathbb{R}$: Incrementality

- The original method is not incremental.
- We achieve incrementality by refining the CAD.

CAD for $\mathbb{R}$: Incrementality

- The original method is not incremental.
- We achieve incrementality by refining the CAD.
- Previous split: $I_1 = (-3, 0)$, $I_2 = [0, 0]$, $I_3 = (0, 3)$

CAD for $\mathbb{R}$: 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: $\underbrace{x^2 - x - 1}_{p_2} > 0$

CAD for $\mathbb{R}$: 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): $C_2 = (-3, 3)$

CAD for $\mathbb{R}$: 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): $C_2 = (-3, 3)$
- Number of real roots in $I_1 = (-3, 0)$: 1

CAD for $\mathbb{R}$: 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): $C_2 = (-3, 3)$
- Number of real roots in $I_1 = (-3, 0)$: 1

  $(p_1, I_1) \neq (p_2, I_1) \Rightarrow$ split

CAD for $\mathbb{R}$: 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): $C_2 = (-3, 3)$
- Number of real roots in $I_1 = (-3, 0)$: 1

  $(p_1, I_1) \neq (p_2, I_1) \Rightarrow$ split
- Number of real roots in $I_2 = [0, 0]$: 0

CAD for $\mathbb{R}$: 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): $C_2 = (-3, 3)$
- Number of real roots in $I_1 = (-3, 0)$: 1

  $(p_1, I_1) \neq (p_2, I_1) \Rightarrow$ split
- Number of real roots in $I_2 = [0, 0]$: 0
- Number of real roots in $I_3 = (0, 3)$: 1

CAD for $\mathbb{R}$: 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): $C_2 = (-3, 3)$
- Number of real roots in $I_1 = (-3, 0)$: 1

  $(p_1, I_1) \neq (p_2, I_1) \Rightarrow$ split
- Number of real roots in $I_2 = [0, 0]$: 0
- Number of real roots in $I_3 = (0, 3)$: 1

  $(p_1, I_3) \neq (p_2, I_3) \Rightarrow$ split

CAD for $\mathbb{R}$: Infeasible subsets

CAD for $\mathbb{R}$: Infeasible subsets

- The original method cannot generate infeasible subsets.

CAD for $\mathbb{R}$: Infeasible subsets

- The original method cannot generate infeasible subsets.
- For $\mathbb{R}$ we collect for each CAD interval one constraint whose sign condition is not satisfied by the interval.

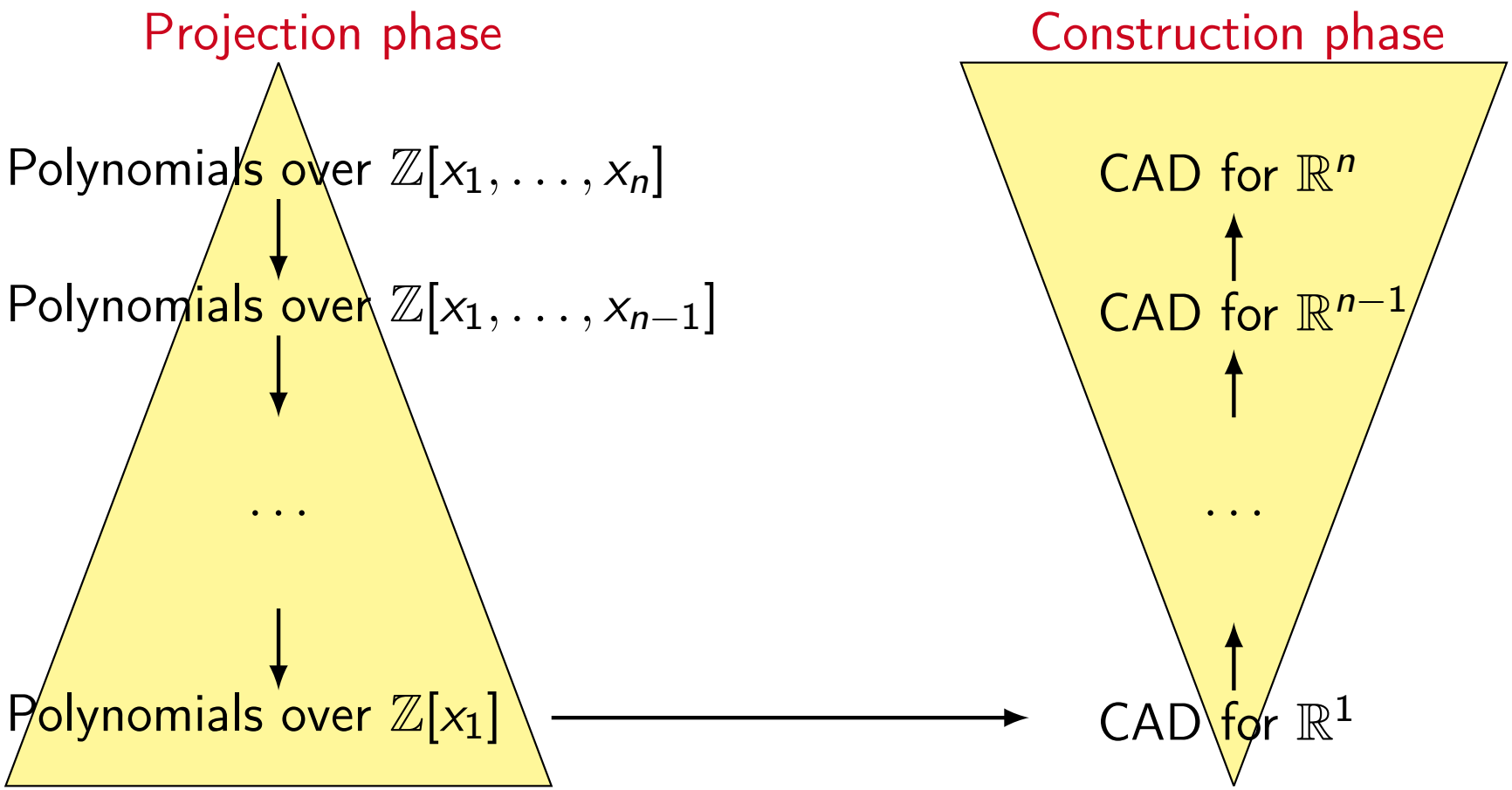
CAD for $\mathbb{R}$: Infeasible subsets

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

Outline

CAD for $\mathbb{R}^n$

A CAD for a set P of polynomials from $\mathbb{Z}[x_1, \ldots, x_n]$ splits $\mathbb{R}^n$ into P-sign-invariant regions.



Delineability

Let $R \subseteq \mathbb{R}^{n-1}$ be a region and $P = (p_1, \ldots, p_m) \in \mathbb{Z}[x_1, \ldots, x_n]^m$, where $m \geq 1$ and $n \geq 2$.

Intuition: If P is delineable on R then the real roots of P vary continuously over R, while maintaining their number and order.

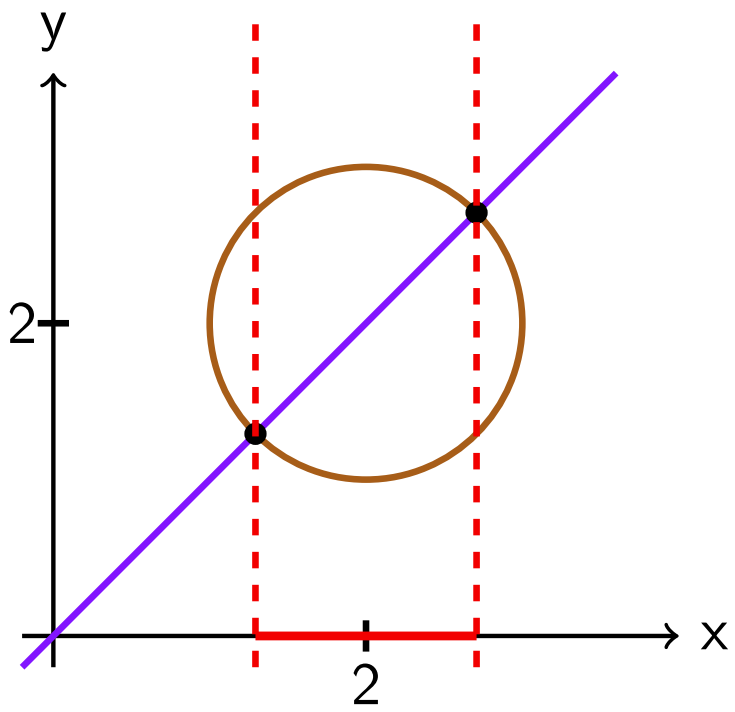
Definition

P is delineable on R if for $1 \leq i, j \leq m$ with $i \neq j$ and for all $a \in R$:

1. the number of roots of $p_i(a)$ is constant,
2. the number of different roots of $p_i(a)$ is constant,
3. the number of common roots of $p_i(a)$ and $p_j(a)$ is constant.

Example: Delineability

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

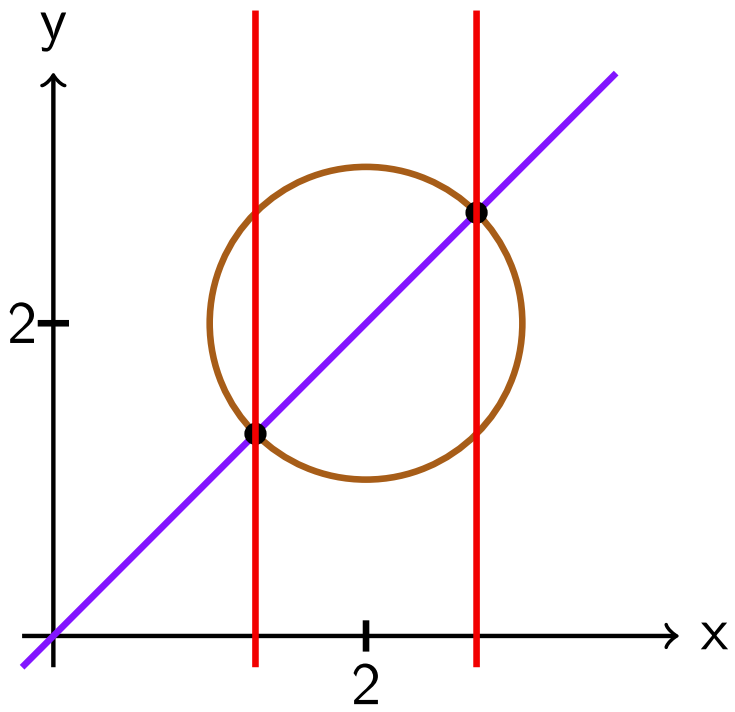


P-delineable regions:

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

Example: Delineability

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

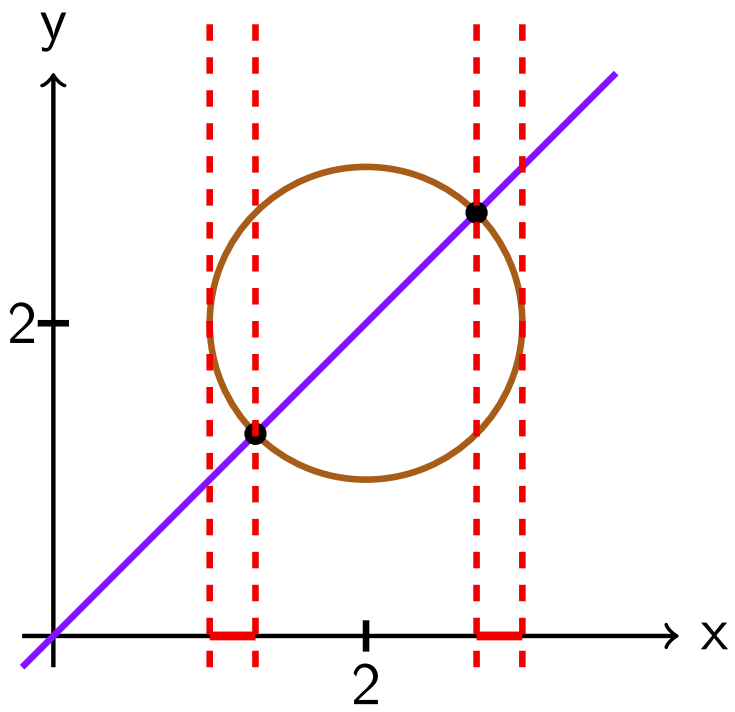


P-delineable regions:

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

Example: Delineability

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

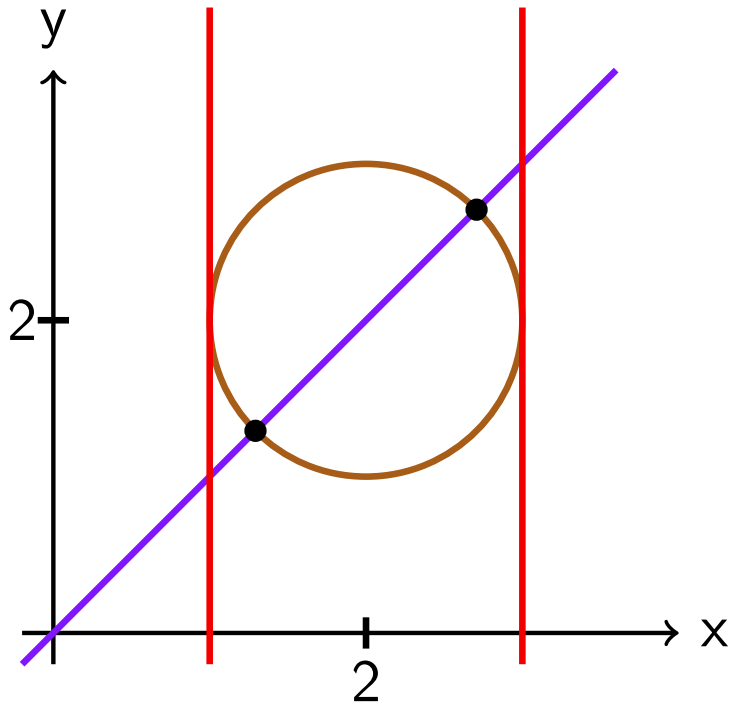


P-delineable regions:

- $(2 - \frac{\sqrt{2}}{2}, 2 + \frac{\sqrt{2}}{2})$
- $\{2 - \frac{\sqrt{2}}{2}\}, \{2 + \frac{\sqrt{2}}{2}\}$
- $(1, 2 - \frac{\sqrt{2}}{2}), (2 + \frac{\sqrt{2}}{2}, 3)$

Example: Delineability

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

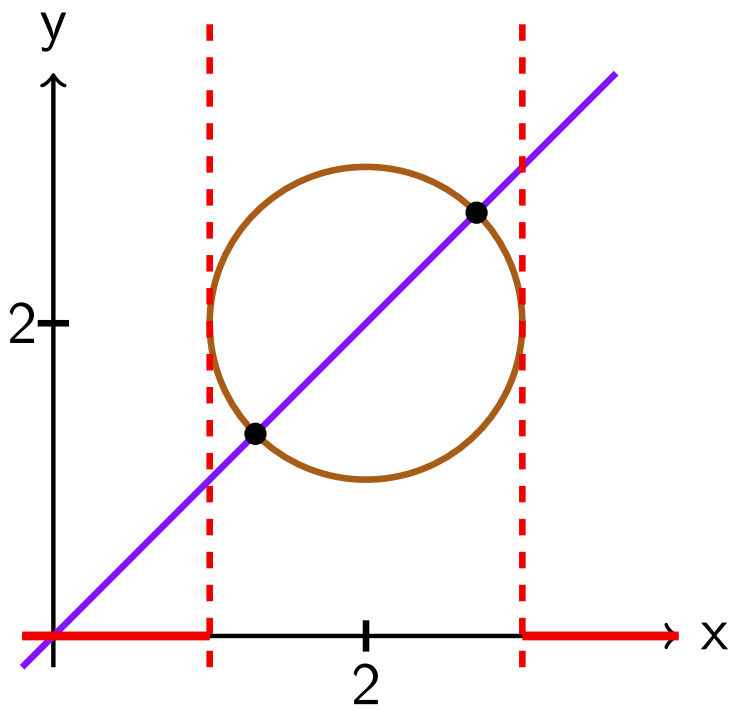


P-delineable regions:

- $(2 - \frac{\sqrt{2}}{2}, 2 + \frac{\sqrt{2}}{2})$
- $\{2 - \frac{\sqrt{2}}{2}\}$, $\{2 + \frac{\sqrt{2}}{2}\}$
- $(1, 2 - \frac{\sqrt{2}}{2})$, $(2 + \frac{\sqrt{2}}{2}, 3)$
- $\{1\}$, $\{3\}$

Example: Delineability

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



P-delineable regions:

- $(2 - \frac{\sqrt{2}}{2}, 2 + \frac{\sqrt{2}}{2})$
- $\{2 - \frac{\sqrt{2}}{2}\}$, $\{2 + \frac{\sqrt{2}}{2}\}$
- $(1, 2 - \frac{\sqrt{2}}{2})$, $(2 + \frac{\sqrt{2}}{2}, 3)$
- $\{1\}$, $\{3\}$
- $(-\infty, 1)$, $(3, \infty)$

Cylindrical algebraic decomposition

Let $P = (p_1, \ldots, p_m) \in \mathbb{Z}[x_1, \ldots, x_n]^m$ and $\mathcal{C} \subseteq 2^{\mathbb{R}^n}$ finite with $m, n \geq 1$.

Definition

$\mathcal{C}$ is called cylindrical algebraic decomposition (CAD) of $\mathbb{R}^n$ for P if the following holds:

1. $\bigcup \mathcal{C} = \mathbb{R}^n$,
2. $C \cap C' = \emptyset$ for all $C, C' \in \mathcal{C}$ with $C \neq C'$,
3. If $n = 1$, then every $C \in \mathcal{C}$ is a P-sign invariant region.
4. If $n > 1$ then there exists a CAD $\mathcal{C}'$ of $\mathbb{R}^{n-1}$ such that for every $C \in \mathcal{C}$ there is a $C' \in \mathcal{C}'$ such that the projection of C to the first $n-1$ dimensions is C'.

An element $C \in \mathcal{C}$ is called a cell.

Cylindrical algebraic decomposition

Let $P = (p_1, \ldots, p_m) \in \mathbb{Z}[x_1, \ldots, x_n]^m$ and $\mathcal{C} \subseteq 2^{\mathbb{R}^n}$ finite with $m, n \geq 1$.

Definition

$\mathcal{C}$ is called cylindrical algebraic decomposition (CAD) of $\mathbb{R}^n$ for P if the following holds:

1. $\bigcup \mathcal{C} = \mathbb{R}^n$,
2. $C \cap C' = \emptyset$ for all $C, C' \in \mathcal{C}$ with $C \neq C'$,
3. If $n = 1$, then every $C \in \mathcal{C}$ is a P-sign invariant region.
4. If $n > 1$ then there exists a CAD $\mathcal{C}'$ of $\mathbb{R}^{n-1}$ such that for every $C \in \mathcal{C}$ there is a $C' \in \mathcal{C}'$ such that the projection of C to the first $n-1$ dimensions is C'.

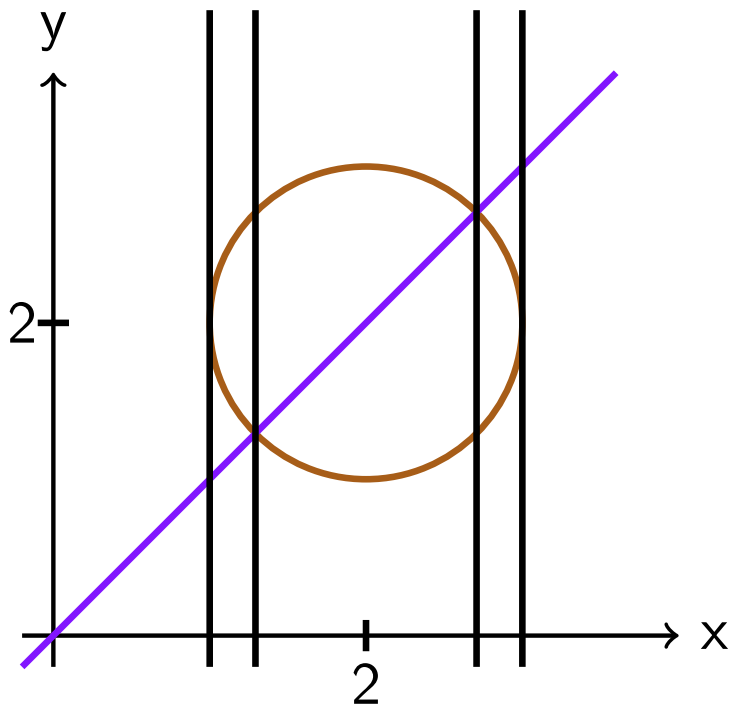
An element $C \in \mathcal{C}$ is called a cell.

Remark

One sample point per cell is sufficient in order to represent a CAD.

Example: CAD with 47 cells

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



P-delineable regions:

- $(2-\frac{\sqrt{2}}{2}, 2+\frac{\sqrt{2}}{2})$
- $\{2-\frac{\sqrt{2}}{2}\}$, $\{2+\frac{\sqrt{2}}{2}\}$
- $(1, 2-\frac{\sqrt{2}}{2})$, $(2+\frac{\sqrt{2}}{2}, 3)$
- $\{1\}$, $\{3\}$
- $(-\infty, 1)$, $(3, \infty)$

CAD projection

Let $P = (p_1, \ldots, p_m) \in \mathbb{Z}[x_1, \ldots, x_n]^m$ where $n \geq 2$ and $m, m' \geq 1$.

Definition

A mapping

$$\text{proj} : 2^{\mathbb{Z}[x_1,\ldots,x_n]} \longrightarrow 2^{\mathbb{Z}[x_1,\ldots,x_{n-1}]}$$

is called a CAD-Projection, if any region $R \subseteq \mathbb{R}^{n-1}$ is $\text{proj}(P)$-sign invariant *iff* R is P-delineable.

CAD projection

Let $P = (p_1, \ldots, p_m) \in \mathbb{Z}[x_1, \ldots, x_n]^m$ where $n \geq 2$ and $m, m' \geq 1$.

Definition

A mapping

$$\text{proj} : 2^{\mathbb{Z}[x_1,\ldots,x_n]} \longrightarrow 2^{\mathbb{Z}[x_1,\ldots,x_{n-1}]}$$

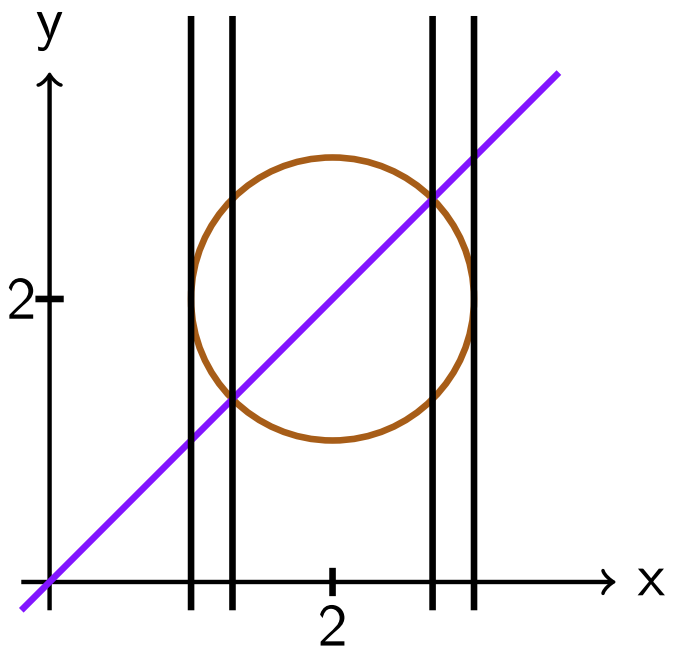
is called a CAD-Projection, if any region $R \subseteq \mathbb{R}^{n-1}$ is $\text{proj}(P)$-sign invariant *iff* R is P-delineable.

Remarks

- Usually, $|\text{proj}(P)| = |P|^2$. Thus, projecting recursively up to the univariate case is in $\mathcal{O}(|P|^{2^{n-1}})$.

Example: CAD projection

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

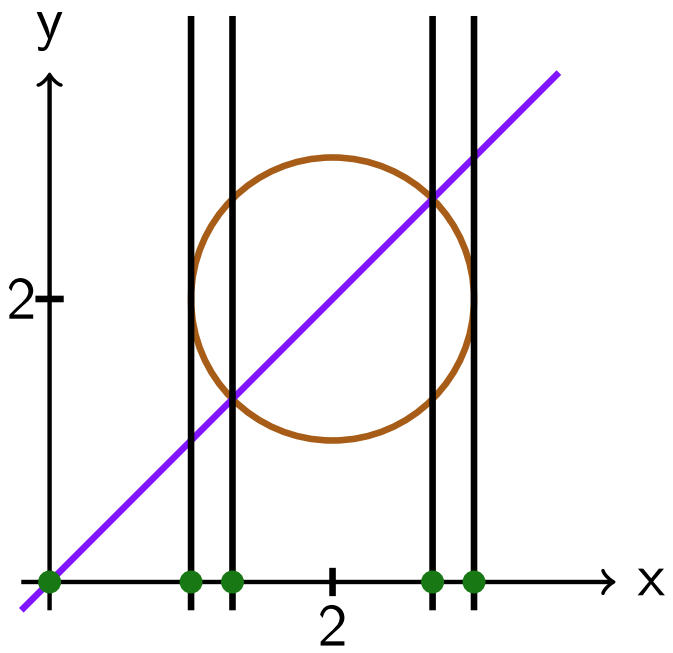


Projection computed by GiNaCRA

$$\begin{aligned} \mathrm{proj}(P) \quad = \quad & \{x^2 - 4x + 3, \\ & -4x + x^2 + \tfrac{7}{2}, \\ & x^4 - 8x^3 + 30x^2 - 56x + 49, \\ & x^2 - 4x + 7, \\ & x\} \end{aligned}$$

Example: CAD projection

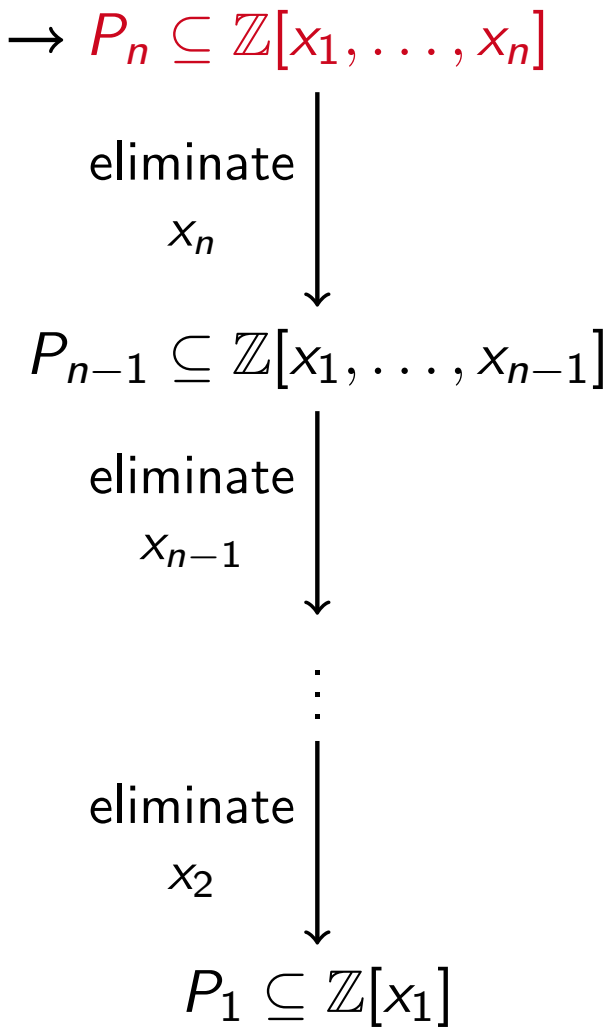
$$P = \begin{pmatrix} (x-2)^2+ \\ (y-2)^2-1, \\ \\ x-y \end{pmatrix}$$



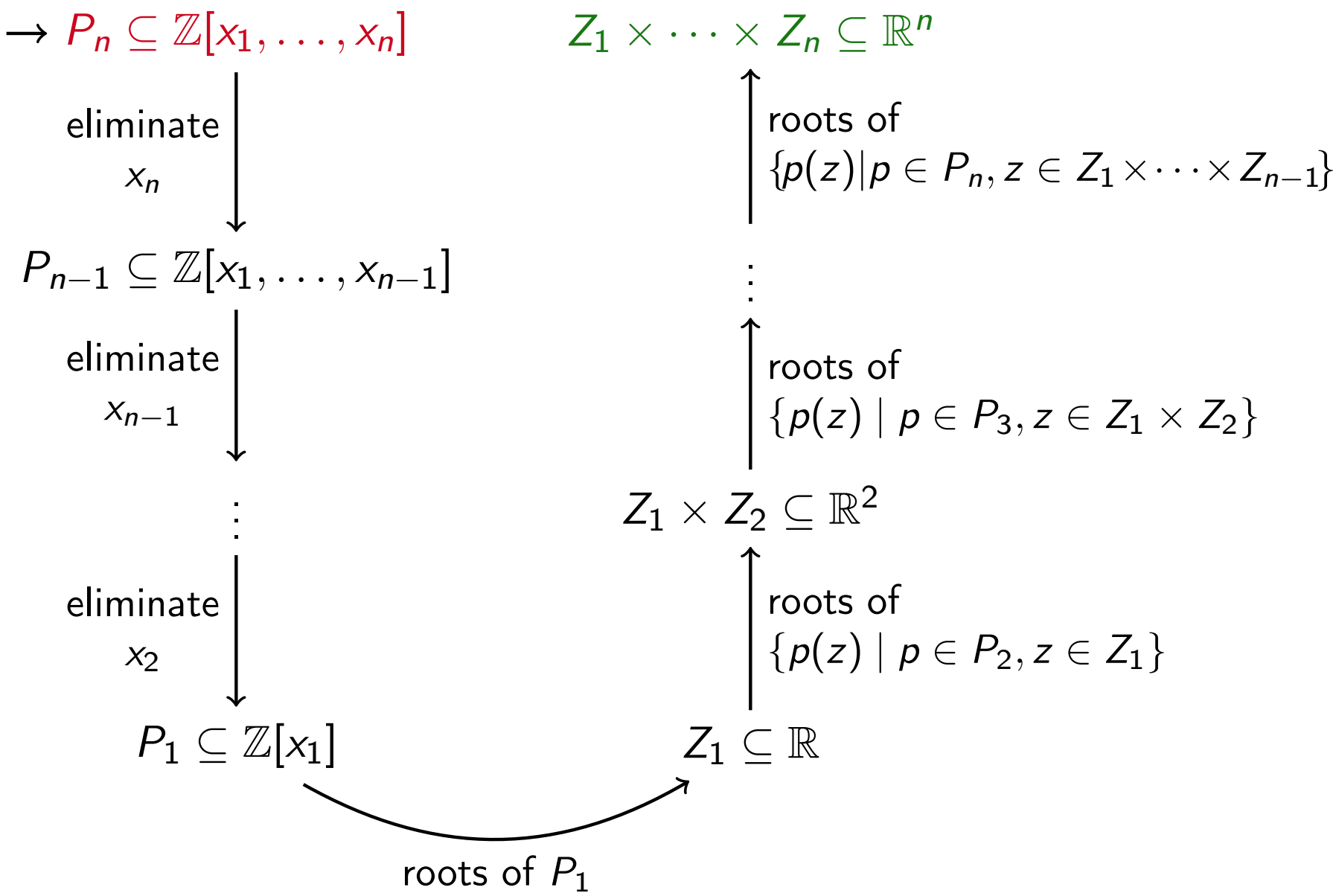
Projection computed by GiNaCRA ... its real roots

$$\begin{aligned} \mathrm{proj}(P) \;=\; \{ & x^2-4x+3, && \{1,\ 3\} \\ & -4x+x^2+\tfrac{7}{2}, && \{2-\tfrac{\sqrt{2}}{2},\ 2+\tfrac{\sqrt{2}}{2}\} \\ & x^4-8x^3+30x^2-56x+49, && \{\} \\ & x^2-4x+7, && \{\} \\ & x\} && \{0\} \end{aligned}$$

The CAD sample construction in a nutshell



The CAD sample construction in a nutshell

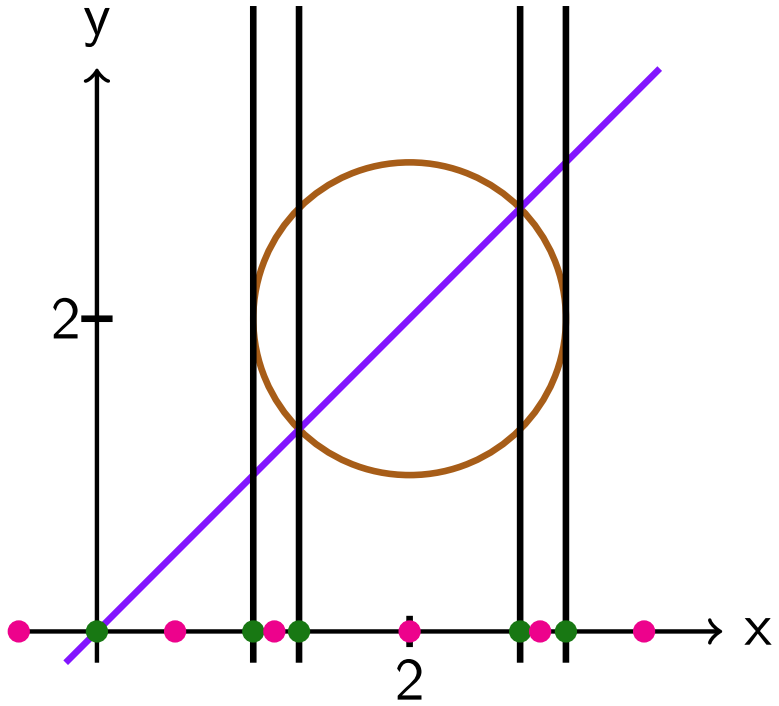


Example: CAD sample construction

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

Samples for $\mathrm{proj}(P)$:

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

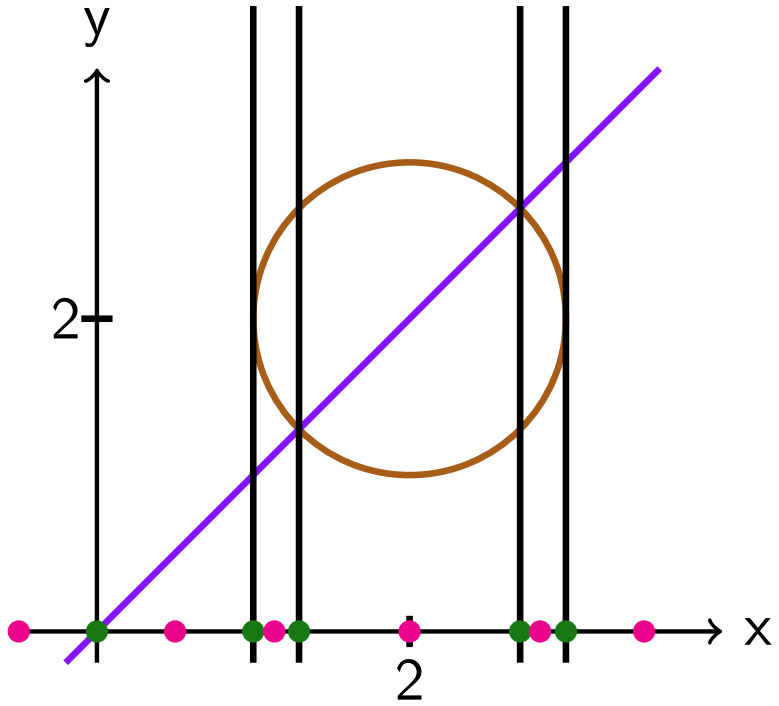


Example: CAD sample construction

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

Samples for $\mathrm{proj}(P)$:

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



Example sample constructions

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