Non-linear Real Arithmetic: Cylindrical Algebraic Decomposition

Prof. Dr. Erika Ábrahám and Ulrich Loup

January 23, 2012

Repetition: non-linear real arithmetic (NRA)

Syntax

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

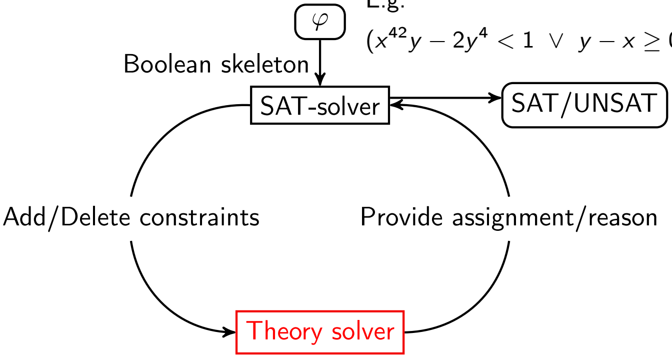
where x is a variable.

- $p = a_1 x_1^{e_{1,1}} \cdots x_n^{e_{n,1}} + \cdots + a_k x_1^{e_{1,k}} \cdots x_n^{e_{n,k}}$,
  $\deg(p) := \max_{1\leq j\leq k}(\sum_{i=1}^{n} e_{i,j})$ degree of p
- φ 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.
- NRA mainly used in the SMT context to differentiate from LRA.
- Here: NRA indicates that non-linear constraints are not forbidden.

Recall: connection to SMT

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



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

Repetition: NRA solving history

- 1948 — First decision procedure [T48]
- 1975 — Cylindrical algebraic decomposition (CAD) method [C75]
- 1993 — Gröbner basis approach [W93]
- 1997 — Virtual substitution [W97]
- 1997 — Computing realizable sign conditions (RiSC) [BPR97]

Outline

1. Preliminaries
2. Cylindrical Algebraic Decomposition
3. CAD Construction
4. Technical Remarks

Outline

1 Preliminaries

2 Cylindrical Algebraic Decomposition

3 CAD Construction

4 Technical Remarks

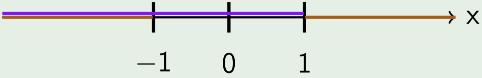
NRA solution space (12)

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

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

Example (one-dimensional)

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



$$=]-\infty, -1[$$

Example (two-dimensional)

Sign-invariance

Sign of a polynomial

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

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

Sign invariant set = solution set

Given $p_i \in \mathbb{Z}[x_1, \ldots, x_n]$, $n \in \mathbb{N}$, $\sim_i \in \{<, =, >\}$ for $1 \leq i \leq m$, then

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

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

Sign-invariant regions

Region

$R \in \mathbb{R}^n$ is called a region if

$$R \neq (A \cap R) \cup (B \cap R)$$

with $A \cap R \neq \emptyset$ and $B \cap R \neq \emptyset$ for all open, $\emptyset \neq A, B \subseteq \mathbb{R}^n$ with $A \cap B = \emptyset$.

Example

- For $a, b \in \mathbb{R}$, $]a, b[$, $\{a\}$, are regions, and $R \times R'$ for regions R, R'.

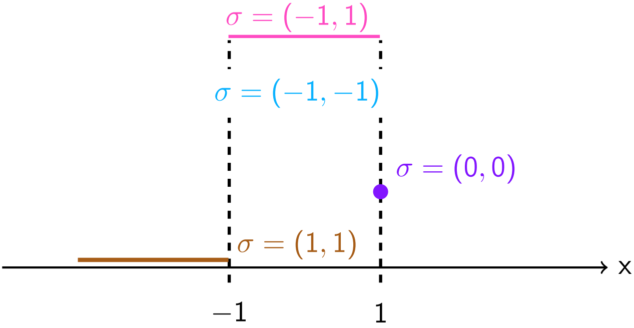
Remarks

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 maximal regions.
- $\mathbb{R}^n$ can be decomposed into maximal sign-invariant regions.

Example: sign-invariant regions

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



Outline

1 Preliminaries

2 Cylindrical Algebraic Decomposition

3 CAD Construction

4 Technical Remarks

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 $n \geq 2$.

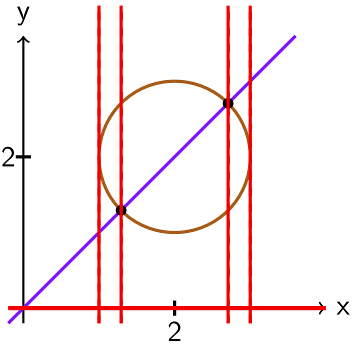
Definition

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

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

- $]2 - \frac{\sqrt{2}}{2}, 2 + \frac{\sqrt{2}}{2}[$
- $\{2 - \frac{\sqrt{2}}{2}\}, \quad \{2 + \frac{\sqrt{2}}{2}\}$
- $]1, 2 - \frac{\sqrt{2}}{2}[\ , \quad]2 + \frac{\sqrt{2}}{2}, 3[$
- $\{1\}, \quad \{3\}$
- $]-\infty, 1[\ , \quad]3, \infty[$

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 maximal P-sign invariant region.
4. If $n > 1$ and $\mathcal{C}'$ is a cylindrical algebraic decomposition of $\mathbb{R}^{n-1}$ such that any $C' \in \mathcal{C}'$ is P-delineable, then for every $C \in \mathcal{C}$ there is a $C' \in \mathcal{C}'$ such that $C \subseteq C' \times \mathbb{R}$ is a maximal P-sign invariant region in $C' \times \mathbb{R}$.

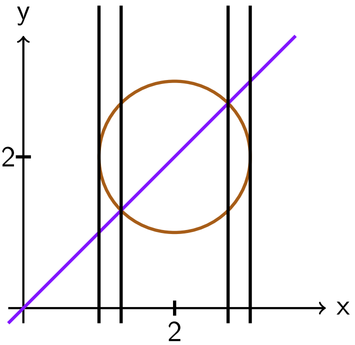
An element $C \in \mathcal{C}$ is called a cell.

Remark

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

Example: CAD with 48 cells

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



P-delineable regions:

- $]2 - \frac{\sqrt{2}}{2}, 2 + \frac{\sqrt{2}}{2}[$
- $\{2 - \frac{\sqrt{2}}{2}\}, \quad \{2 + \frac{\sqrt{2}}{2}\}$
- $]1, 2 - \frac{\sqrt{2}}{2}[\ , \quad]2 + \frac{\sqrt{2}}{2}, 3[$
- $\{1\}, \quad \{3\}$
- $]-\infty, 1[\ , \quad]3, \infty[$

Outline

1 Preliminaries

2 Cylindrical Algebraic Decomposition

3 CAD Construction

4 Technical Remarks

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

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

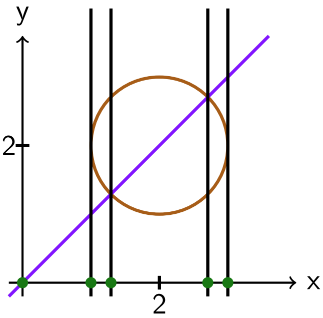
is called a CAD-Projection, if any region $R \subseteq \mathbb{R}^{n-1}$ is $\mathrm{proj}(P)$-sign invariant *iff* R is P-delineable.

Remarks

- Usually, $|\mathrm{proj}(P)| = m' = m^2$. Thus, $m' \in \mathcal{O}(m^{2^{n-1}})$.
- Given a CAD $\mathcal{C}$ for P, then for every cell $C \in \mathcal{C}$ there is a $C' \in \mathcal{C}'$ such that $C' \upharpoonright_{\mathbb{R}^{n-1}} \subseteq C$ is a maximal P-sign invariant region in $C' \times \mathbb{R}$.

Example: CAD projection

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



Projection computed by GiNaCRA ... its real roots

$\mathrm{proj}(P) = \{x^2 - 4x + 3,$	$\{1,\ 3\}$
$-4x + x^2 + \frac{7}{2},$	$\{2 - \frac{\sqrt{2}}{2},\ 2 + \frac{\sqrt{2}}{2}\}$
$x^4 - 8x^3 + 30x^2 - 56x + 49,$	$\{\}$
$x^2 - 4x + 7,$	$\{\}$
$x\}$	$\{0\}$

The CAD sample construction in a nutshell

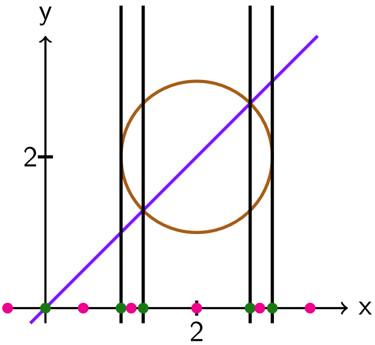
$$
\begin{array}{ccc}
\rightarrow P_n \subseteq \mathbb{Z}[x_1,\dots,x_n] & & Z_1 \times \cdots \times Z_n \subseteq \mathbb{R}^n \\
\Big\downarrow \text{eliminate } x_n & & \Big\uparrow \text{roots of } \{p(z) | p \in P_n, z \in Z_1 \times \cdots \times Z_{n-1}\} \\
P_{n-1} \subseteq \mathbb{Z}[x_1,\dots,x_{n-1}] & & \vdots \\
\Big\downarrow \text{eliminate } x_{n-1} & & \Big\uparrow \text{roots of } \{p(z) \mid p \in P_3, z \in Z_1 \times Z_2\} \\
\vdots & & Z_1 \times Z_2 \subseteq \mathbb{R}^2 \\
\Big\downarrow \text{eliminate } x_2 & & \Big\uparrow \text{roots of } \{p(z) \mid p \in P_2, z \in Z_1\} \\
P_1 \subseteq \mathbb{Z}[x_1] & \xrightarrow{\text{roots of } P_1} & Z_1 \subseteq \mathbb{R}
\end{array}
$$

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

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

Outline

1 Preliminaries

2 Cylindrical Algebraic Decomposition

3 CAD Construction

4 Technical Remarks

Non-trivial roots

Remark

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

- p has between 0 and $\deg(p)$ real roots.

Example

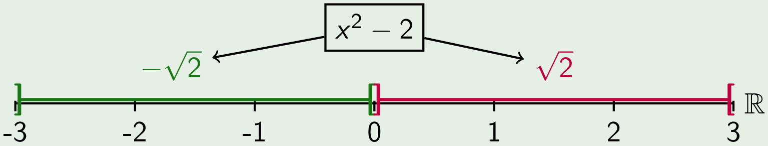
- $x^3 - 6x^2 + 11x - 6$ has rational roots: 1, 2 and 3.
- $x^3 - x^2 - 2x + 2$ has one rational and two irrational roots: 1, $-\sqrt{2}$ and $\sqrt{2}$.
- $x^5 - 3x^4 + x^3 - x^2 + 2x - 2$ has only one real root ≈ 2.70312, not representable by radicals.

Representing a real algebraic number

Interval representation

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

Example



References I

A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, 1948.

G. E. Collins. *Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition*. Springer, Automata Theory and Formal Languages, LNCS 33, 134–183, 1975.

G. E. Collins and H. Hong. *Partial Cylindrical Algebraic Decomposition for Quantifier Elimination*. Academic Press Inc., JSC, 12 (3), 299 – 328, 1991.

V. Weispfenning. *A New Approach to Quantifier Elimination for Real Algebra*. Technical Report MIP-9305, FMI, Universität Passau, D-94030 Passau, Germany, July 1993.

V. Weispfenning. *Quantifier Elimination for Real Algebra – The Quadratic Case and Beyond*. Springer, AAECC, 8 (2), 85–101, 1997.

S. Basu, R. Pollack, and M. F. Roy. *On Computing a Set of Points Meeting Every Semialgebraically Connected Component of a Family of Polynomials on a Variety*. JC, 13 (1), 28–37, 1997.

References II

S. Basu, R. Pollack, and M. F. Roy. *Algorithms in Real Algebraic Geometry*. Springer, 2010.

U. Loup and E. Ábrahám. *GiNaCRA: A C++ Library for Real Algebraic Computations*. In 3rd NASA Formal Methods Symposium (NFM'11), pages 512–517. Volume 6617 of LNCS. Springer-Verlag, 2011.

U. Loup and E. Ábrahám. *I-RiSC: An SMT-Compliant Solver for the Existential Fragment of Real Algebra*. In 4th Int. Conf. on Algebraic Informatics (CAI'11), pages 230–246. Volume 6742 of LNCS. Springer-Verlag, 2011.

S. Feferman. *Tarski's influence on computer science*. Logical Methods in Computer Science, 2006.

A. Dolzmann, T. Sturm, V. Weispfenning. *Real Quantifier Elimination in Practice*. 1997.

Alfred Tarski. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, 1948.

References III

Christopher W. Brown and James H. Davenport. The complexity of quantifier elimination and cylindrical algebraic decomposition. In Dongming Wang, editor, *ISSAC*, pages 54–60. ACM, 2007.

M. O. Rabin. *A simple method for undecidability proofs and some applications*. Logic, Methodology and Philosophy of Science II, 1965.