# Cylindrical Algebraic Decompositions

Christoph-Simon Senjak

Lehr- und Forschungseinheit für Theoretische Informatik
Institut für Informatik
Ludwig-Maximilians-Universität München
Oettingenstr.67, 80538 München

PUMA Workshop 1. Oktober 2013

# Foreword

- This talk bases on the work of Assia Mahboubi, especially "Implementing the cylindrical algebraic decomposition within the Coq system", Math. Struct. in Comp. Science (2007), vol. 17, pp. 99–127.
- Furthermore on S. Basu, R. Pollack, M. Roy, "Algorithms in Real Algebraic Geometry", Second edition, Springer-Verlag Berlin Heidelberg, 2006
- Some definitions are slightly shortened and not every detail is given.
- I am responsible for any mistake in this talk.

# Real Closed Fields

- Discrete Real Closed Fields:
  - Axioms of commutative unit ring
  - Unary predicate $P$, "positivity", $x < y :\Leftrightarrow \neg P(x - y)$.
  - $P(1)$, $\neg P(0)$, $\neg P(-x) \wedge \neg P(x) \rightarrow x = 0$
  - $P(x) \wedge P(y) \rightarrow P(x + y) \wedge P(x \cdot y)$, $P(x + y) \rightarrow P(x) \vee P(y)$
  - Intermediate value Theorem: For all $f(x) = a_n x^n + \ldots + a_0$ the axiom $f(u) < 0 < f(v) \wedge u < v \rightarrow \exists_x . u < x < v \wedge f(x) = 0$
  - $P(x) \vee \neg P(x)$
- Theorem (Palmgren): The theory of discrete real closed fields is intuitionistically equivalent to the classical theory of real closed fields.

# Motivation

- Common problem: Simple inequalities which are left implicit in pen-and-paper proofs are hard to show in proof checkers: $\forall_{x_1,v_0,v_1 \in \mathbb{R}}. x_1 \geq v_1 + 1 \Rightarrow x_0 \geq v_0 \Rightarrow x_1 x_0 + x_1 > v_0 + v_1 v_0 + v_1$
- Theorem (Tarski): The theory of real closed fields is decidable. Important special case for applications:
- Theorem (Quantifier Elimination):
  - $\mathcal{L}$ language of ordered fields
  - $\Phi(Y)$ $\mathcal{L}$-formula with coefficients from an ordered subring $D$ of an ordered field $R$
  - $\Rightarrow$ exists $\Psi(Y)$ with coefficients in $D$, such that $\forall_{y \in R^k}. \Psi(y) \leftrightarrow \Phi(y)$
- Using CAD to find such formulae.

# Algebraic and semi-algebraic sets

- $\mathcal{P} \subseteq R[X_1, \ldots X_n]$ finite $\Rightarrow Z(\mathcal{P}) := \{x \in R^n \mid \bigwedge_{P \in \mathcal{P}} P(x) = 0\}$ called the **set of zeroes**.
- $S \subseteq \mathbb{R}^n$ is called **algebraic**, if it is a set of zeroes.
- The set of **semi-algebraic subsets** of $R^k$ is the smallest set containing all algebraic sets and all sets defined by polynomial inequalities, and is closed under complementation, finite union and finite intersection.
- Let $S \subseteq R^k$, $T \subseteq R^l$ be semi-algebraic sets. $f : S \to T$ is called a **semi-algebraic function** if its graph is a semi-algebraic subset of $R^{k+l}$

- Theorem (Tarski-Seidenberg): A projection of a semi-algebraic set from dimension $n$ to $n-1$ remains semi-algebraic.
- We are mainly interested in **sign conditions**, sets on which the sign of a polynomial is invariant.
- Idea: Successively eliminate the semi-algebraic sets down to the one-dimensional case. Solve the one-dimensional case, then lift up again.
- CADs give conditions for the elimination and lifting part.

# Univariate Case - 1

- An **isolating list** for polynomials $P_1, \ldots, P_n \in \mathbb{Q}[X]$ is a list of rational points and open intervals with rational bounds, containing exactly one zero of one of the $P_i$.
- Cauchy bounds: $P = \sum_{i=p}^{q} a_i X^i$, $p > q$, $a_p a_q \neq 0$.

  $C(P) := \sum_{i=q}^{p} \frac{|a_i|}{|a_p|}$, $c(P) := \sum_{i=q}^{p} \frac{|a_i|}{|a_q|}$ $\Rightarrow$ the absolute value of all nonzero roots of $P$ are inside $]c(P); C(P)[$.
- **Bernstein polynomials** $B_{p,i}(c,d) = \binom{p}{i} \frac{(X-c)^i (d-X)^{p-i}}{(d-c)^p}$ form a basis of polynomials of degree $\leq p$. Number of sign-changes of coefficients $(b_i)_i$ in this basis give info about the number of roots in $]c,d[$: $0 \Leftrightarrow$ no root, 1 and $P(c)P(d) < 0 \Leftrightarrow$ exactly one root.

# Univariate Case - 2

To calculate an isolating list:

- Begin with the interval given by the cauchy bounds.
- Using the Bernstein-Basis, check if one or zero or more zeroes.
- If more zeroes, split the interval in two intervals and proceed with them.
- $\Rightarrow$ end up with a list of intervals that contain exactly one root, that is, an isolating list.

# Cylindrical Decompositions

are sequences $\mathcal{S}_1, \ldots, \mathcal{S}_k$ where each $\mathcal{S}_i$ is a finite partition of $R^i$ into semi-algebraic subsets, the **cells of level** $i$. Furthermore:

- Each $S \in \mathcal{S}_1$ is either a point or an open interval.
- For every $S \in \mathcal{S}_i$ there are continuous semi-algebraic $\xi_{S,1} < \ldots < \xi_{S,\ell_S} : S \to R$ such that $S \times R \subseteq R^{i+1}$ is the disjoint union of cells of $\mathcal{S}_{i+1}$ which are
  - either the graph of one of the $\xi_{S,j}$ for $j = 1, \ldots, \ell_S$:
    $$\{(x', x_{j+1}) \in S \times R \mid x_{j+1} = \xi_{S,j}(x')\}$$
  - or a band of $S \times R$ bounded from below and from above by the graphs of t he functions $\xi_{S,j}$ and $\xi_{S,j+1}$ for $j = 0, \ldots, \ell_S$, where we take $\xi_{S,0} := -\infty, \xi_{S,\ell_S+1} := \infty$:
    $$\{(x', x_{j+1}) \in S \times R \mid \xi_{S,j}(x') < x_{j+1} < \xi_{S,j+1}(x')\}$$
- A cylindrical decomposition is **adapted** to polynoms $T_1, \ldots, T_\ell$, if on every top cell, the sign of every $T_i$ is invariant.

# Elimination

- From our polynomials $P_1, \ldots, P_i$, generate (possibly more) polynomials $Q_1, \ldots, Q_j$ that do not contain one of the variables, using a projection operator.
- Some uniformity properties must hold, so the relevant properties of the polynomials over the cells can be checked with arbitrary elements. The polynomials $Q_i$ should have a constant sign over every cell.
- The $Q_i$ contain truncations and **subresultants** of the $P_i$ and their derivatives. Subresultant computation is expensive.

# Lifting

- Generate a tree of **isolating parallelepipeds**, lists $(\mathcal{T}_1, I_1), \ldots, (\mathcal{T}_k, I_k)$ where
  - $\mathcal{T}_i \in \mathbb{Q}[X_1, \ldots, X_i]$
  - $I_1$ is open interval with rational endpoints or rational singleton containint the root $z_1$ of $\mathcal{T}_1$, and no other root of $\mathcal{T}_1$, $I_2$ is open interval with rational endpoints or rational singleton containing the root $z_2$ of $\mathcal{T}_2(z_1, X_2)$ and no other root of $\mathcal{T}_2(z_1, X_2)$, etc.

# Example - 1

- Consider $P = X^2 + Y^2 - 1$ (which describes the unit circle).
- After eliminating $Y$, we get $X^2 - 1$. One possible isolating list (with sign conditions and representants) is
  $(]-\infty; -1[, \{-2\}, +)$, $(\{-1\}, \{-1\}, 0)$, $(]-1; 1[, \{0\}, -)$, $(\{1\}, (]\frac{1}{2}, \frac{3}{2}[), 0)$, $(]1; \infty[, \{2\}, +)$
  where we assume that 1 is not known exactly, and only described by the isolating interval.

# Example - 2

- Lifting yields:
  - $P(-2, Y) = Y^2 + 3$, which has a constant positive sign $\Rightarrow$ $\{(x, y) \mid x < -1, y \in \mathbb{R}\}$ is a cell. Similar for above 2, $\{(x, y) \mid x > 1, y \in \mathbb{R}\}$ is a cell.
  - $P(-1, Y) = Y^2$ has a single root 0, the cells are the two half-lines $\{(x, y) \mid x = -1, y \gtrless 0\}$, and $\{(-1, 0)\}$.
  - $P(0, Y) = Y^2 - 1$: There are five cells $\{(x, y) \mid y < -\sqrt{1 - x^2}\}$, $\{(x, y) \mid y = -\sqrt{1 - x^2}\}$, $\{(x, y) \mid -\sqrt{1 - x^2} < y < \sqrt{1 - x^2}\}$, $\{(x, y) \mid y = \sqrt{1 - x^2}\}$, $\{(x, y) \mid y > \sqrt{1 - x^2}\}$.
  - Above the interval $((]\frac{1}{2}, \frac{3}{2}[), 0)$, the algorithm does not know the exact value of the root (1). So it has to stick with the abstract relation that some $z$ is the only root of $X^2 + 1$, and consider $P(z, Y) = Y^2 + (z^2 + 1)$.

# Example - 3

- We get 13 cells: