Algebraic and Semi-Algebraic Reasoning For Formal Methods

Lecture 4 - Applications of Gröbner Bases and Sum of Squares.

Sriram Sankaranarayanan

Operations on Varieties

- Algebraic Variety V
  - Representation: Gröbner basis of the ideal $\mathsf{Id}(V)$.
- Intersection of varieties:
  - $V_1 \cap V_2$ – Groebner$(G_1 \cup G_2)$
  - Why do we need to compute Gröbner basis again?
- Union of varieties:
  - $V_1 \cup V_2$ – $G_1 \otimes G_2$ or $\langle G_1 \rangle \cap \langle G_2 \rangle$.

Unions of Varieties

Two ways of computing intersections:

$$\mathsf{Var}(\langle f_1, \dots, f_j \rangle) \cup \mathsf{Var}(\langle g_1, \dots, g_k \rangle)$$
$$= \mathsf{Var}(\langle f_1 g_1, f_1 g_2, \dots, f_j g_k \rangle)$$
$$= \mathsf{Var}(\langle f_1, \dots, f_j \rangle \cap \langle g_1, \dots, g_k \rangle)$$

- How do we compute ideal intersections?
- Which one is better?

Trick Let t be a *fresh variable*.

$$\langle f_1, \ldots, f_j \rangle \cap \langle g_1, \ldots, g_k \rangle =$$
$$\langle tf_1, \ldots, tf_j, (1-t)g_1, \ldots, (1-t)g_k \rangle \cap K[\vec{x}]$$

- Prove that this computes ideal intersection
- Eliminate the variable t.
  - We will see how to do so soon.

Ideal Products

Let $p \in \langle f_1, \ldots, f_j \rangle \cap \langle g_1, \ldots, g_k \rangle$ then $p \in \langle f_1 g_1, f_1 g_2, \ldots, f_j g_k \rangle$?

- Not necessarily!
- However, $p^2 \in \langle f_1 g_1, f_1 g_2, \ldots, f_j g_k \rangle$?.

If $p \in \langle f_1 g_1, f_1 g_2, \ldots, f_j g_k \rangle$, is $p \in \langle f_1, \ldots, f_j \rangle \cap \langle g_1, \ldots, g_k \rangle$?

Inclusion Checking

- Algebraic Varieties: V_1, V_2.
- Check if $V_1 \subseteq V_2$.
    - Let $\langle G_1 \rangle, \langle G_2 \rangle$ be the Gröbner bases.

- If $V_1 \subseteq V_2$ then $\langle G_2 \rangle \subseteq \langle G_1 \rangle$.
- Each gen. in G_2 reduces to 0 under reduction by G_1?

Image Computation

- Image computation:
    - Assertion $\varphi : g_1(\vec{x}) = 0 \ \wedge \ \cdots \ \wedge \ g_m(\vec{x}) = 0$
    - Transition relation $\rho : \ p_1(\vec{x}, \vec{x}') = 0 \ \wedge \ \cdots \ p_m(\vec{x}, \vec{x}') = 0.$
    - Post-Condition: $(\exists \ \vec{x}_0) \ \varphi[\vec{x}_0] \wedge \ \rho[\vec{x}_0, \vec{x}]$

Elimination Theory

Let $I : \langle p_1, \dots, p_m \rangle$ be an ideal in $K[x_1, \dots, x_n, y_1, \dots, y_m]$.

- Compute Gröbner basis G under an *elimination order*

Elimination Theory

Let $I : \langle p_1, \dots, p_m \rangle$ be an ideal in $K[x_1, \dots, x_n, y_1, \dots, y_m]$.

- Compute Gröbner basis G under an *elimination order*
  - Eg., lexicographic ordering: $x_1 > \dots > x_n > y_1 > \dots > y_m$

Elimination Theory

Let $I : \langle p_1, \dots, p_m \rangle$ be an ideal in $K[x_1, \dots, x_n, y_1, \dots, y_m]$.

- Compute Gröbner basis G under an *elimination order*
  - Eg., lexicographic ordering: $x_1 > \dots > x_n > y_1 > \dots > y_m$
- Take all polynomials involving $y_1, \dots, y_m$:

Elimination Theory

Let $I : \langle p_1, \dots, p_m \rangle$ be an ideal in $K[x_1, \dots, x_n, y_1, \dots, y_m]$.

- Compute Gröbner basis G under an *elimination order*
  - Eg., lexicographic ordering: $x_1 > \dots > x_n > y_1 > \dots > y_m$
- Take all polynomials involving $y_1, \dots, y_m$:
  - $\widehat{G} = G \cap K[y_1, \dots, y_m]$

Elimination Theory

Let $I : \langle p_1, \dots, p_m \rangle$ be an ideal in $K[x_1, \dots, x_n, y_1, \dots, y_m]$.

- Compute Gröbner basis G under an *elimination order*
    - Eg., lexicographic ordering: $x_1 > \dots > x_n > y_1 > \dots > y_m$
- Take all polynomials involving $y_1, \dots, y_m$:
    - $\widehat{G} = G \cap K[y_1, \dots, y_m]$
- Claim: $I \cap K[y_1, \dots, y_m] = \langle \widehat{G} \rangle$.

Demonstration

Demo of using abstract interpretation to calculate polynomial invariants.

- Jupyter notebook!

Semi-Algebraic Reasoning

Lagrangian Reasoning for Inequalities

$$
\begin{array}{rcl}
2x - 3y + 4z & \geq & 5 \qquad \leftarrow e_1 \\
3x - 2y + 0z & \geq & 7 \qquad \leftarrow e_2 \\
z & \geq & 3 \qquad \leftarrow e_3 \\
\hline
& & (\Rightarrow) \\
x - y + z & \geq & 3
\end{array}
$$

$$
(x - y + z - 3) = \frac{1}{5}(e_1 + e_2 + e_3)
$$

$$\frac{e \geq 0, \ \lambda \geq 0}{\lambda e \geq 0}$$

$$\frac{e_1 \geq 0, \ e_2 \geq 0}{e_1 + e_2 \geq 0}$$

$$\frac{}{1 \geq 0}$$

Conic Combination

Consider linear inequalities

$$e_1 \geq 0, \dots, e_m \geq 0$$

Conic combination:

$$\lambda_0 + \lambda_1 e_1 + \cdots + \lambda_m e_m \leq 0$$

wherein $\lambda_i \geq 0$.

Farkas' Lemma

$$\varphi: \ e_1 \geq 0 \ \wedge \ e_2 \geq 0 \ \cdots \ \wedge \ e_m \geq 0$$

- φ is unsatisfiable iff $-1 \geq 0$ lies in conic combination.
- If φ is satisfiable: $\varphi \vDash e \geq 0$ iff we can $e = \sum_{i=1}^{m} \lambda_i e_i + \lambda_0$
  - $\lambda_0, \ldots, \lambda_m \geq 0$.
- Foundations of linear programming and duality theory.
  - Reference: V. Chvatal's amazing book on Linear Programming.

Farkas' Lemma in Formal Methods

- Vast literature on using Farkas' Lemma for
    - Invariant Synthesis: Colon + Sank. + Sipma' CAV 2003; Gulwani et al., Tiwari et al.,…
    - Ranking Function Synthesis: Colon + Sipma, Podelski + Rybalchenko, Bradley + Manna, Cook + Rybalchenko + Podelski, …
    - Cost analysis of programs
    - Analysis of probabilistic programs
    - Proof production in linear arithmetic SMT solver: [Reynolds+Tinelli]

Beyond Farkas Lemma

Proving entailment with polynomials:

$$p_1 \geq 0, \cdots, p_m \geq 0 \vDash p \geq 0$$

- $p_1, \ldots, p_m \in \mathbb{R}[x_1, \ldots, x_n]$.
- Entailment over $\mathbb{R}^n$.

Positivstellensatz:

$$p = \sigma_0 + \sigma_1 p_1 + \cdots + \sigma_m p_m$$

where σ_i are *positive polynomials*.

Polynomial Positivity Checking

- Check if a polynomial $p \in \mathbb{R}[x_1, \ldots, x_n]$ is non-negative everywhere.

$$\forall \; x_1, \ldots, x_n \in \mathbb{R}^n, \; p(x_1, \ldots, x_n) \geq 0$$

- Well known to be NP-hard.

  - Positive Definite: $p > 0$ for all $\vec{x} \neq 0$.
  - Positive Semi-Definite: $p \geq 0$ for all $\vec{x}$.

Semi-Algebraic Entailment Checking

Given $p_1, \dots, p_m, p \in \mathbb{R}[x_1, \dots, x_n]$, check entailment:

$$p_1 \geq 0 \;\wedge\; \cdots \;\wedge p_m \geq 0 \;\vDash\; p \geq 0\,.$$

- Adapt Cylindrical Algebraic Decomposition.

Cylindrical Algebraic Decomposition (CAD)

Given polynomials $p_1, \dots, p_m$ in $\mathbb{R}[x_1, \dots, x_n]$,

- We decompose $\mathbb{R}^n$ into finitely many disjoint cells.
- Each cell is semi-algebraic.
- Each cell is "sign invariant''.
- The decomposition is *cylindrical*.

Cylindrical Decomposition

- Decompose x_n into finitely many points and intervals.

$$\mathbb{R} = (-\infty, a_1) \cup [a_1, a_1] \cup (a_1, a_2) \cup [a_2, a_2] \cup \cdots$$

- For each point/interval, we recursively associate a "stack of regions'' involving $x_1, \ldots, x_{n-1}$.

Cf. Manuel Kauers, How to use a Cylindrical Algebraic Decomposition.
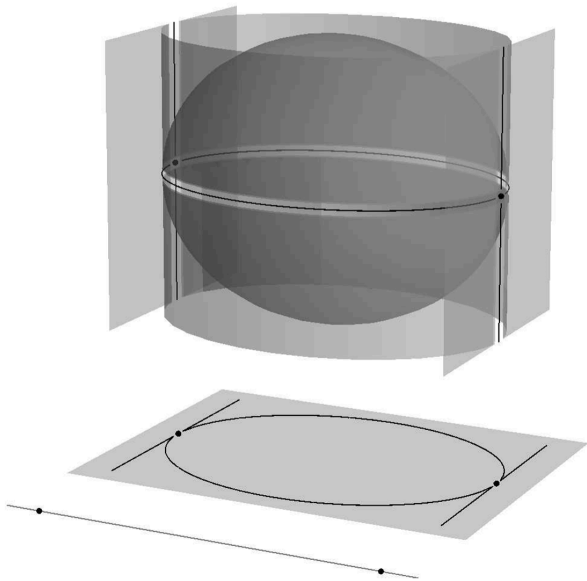
FIGURE 2. cylindrical algebraic decomposition of the unit ball

Cylindrical Algebraic Decomposition: Complexity

- CAD is a very powerful tool for working with semi-algebraic sets.

- However, its complexity is double exponential in number of variables.

  - The full CAD algorithm is not necessary to check if $\exists \vec{x}, p(\vec{x}) < 0$.

Sum Of Squares Techniques

Sum of Squares (SOS)

A polynomial p is *sum of squares* (SOS) iff

$$p = \sigma_1^2 + ... + \sigma_k^2$$

for some $k \geq 0$.

- $\sigma_1, ..., \sigma_k \in \mathbb{R}[x_1, ..., x_n]$.

Positive Polynomials vs. Sum-Of-Squares

If p is SOS then p is a positive semi-definite.

- Is the converse true?

- *Theorem # 1* Any univariate polynomial is positive semi-definite iff it is SOS.

- *Theorem # 2* Any quadratic polynomial is positive semi-definite iff it is SOS.

TODO: Prove these in lecture.

There exists a polynomial that is positive semidefinite but cannot be written as a sum of squares.

Motzkin Polynomial:

$$p = x^4y^2 + x^2y^4 + 1 - 3x^2y^2 \succeq 0$$

- Prove that p is positive semi-definite.
- Prove that p cannot be expressed as SOS.

Quadratic Forms and Sum of Squares

Quadratic polynomial $p(x_1, \ldots, x_n)$ can be written:

$$
\begin{pmatrix} 1 \\ x_1 \\ x_2 \\ \ldots \\ x_n \end{pmatrix}^\top
\begin{pmatrix} Q_{11} & Q_{12} & \cdots & Q_{1,n+1} \\ Q_{21} & Q_{22} & \cdots & Q_{2,n+1} \\ \vdots & & \ddots & \vdots \\ Q_{n+1,1} & Q_{n+1,2} & \cdots & Q_{n+1,n+1} \end{pmatrix}
\begin{pmatrix} 1 \\ x_1 \\ x_2 \\ \ldots \\ x_n \end{pmatrix}
$$

SOS and PSD for Quadratic Forms

A quadratic form $p(\vec{x}) = \vec{x}^\top Q \vec{x}$ is positive semidefinite iff all eigenvalues of Q are non-negative.

Proof: Suppose $Q\vec{v} = \lambda \vec{v}$, λ must be real and furthermore, $\vec{v}^\top Q \vec{v} = \lambda \vec{v}^\top \vec{v}$.

($\Rightarrow$) Let p be a positive semi-definite polynomial, but Q have a negative eigenvalue $\lambda < 0$. Then $p(\vec{v}) = \lambda \vec{v}^\top \vec{v} < 0$. This is a contradiction.

($\Leftarrow$) Suppose all eigen values of Q are non-negative. Since Q is a symmetric matrix, we can write its spectral decomposition: $Q = \sum_{j=1}^n \lambda_j \vec{v}_j \vec{v}_j^\top$, wherein $\lambda_j \geq 0$ are the eigenvalues. Therefore, $p = \vec{x}^\top Q \vec{x}$ can be written as

$$p = \sum_{j=1}^n \lambda_j \vec{x}^t \vec{v}_j \vec{v}_j^\top \vec{x} = \sum_{j=1}^n (\sqrt{\lambda_j} \vec{v}_j^\top \vec{x})^2$$

Hilbert's Seventeenth Problem

Hilbert's Seventeenth Problem: Can any positive semi-definite
polynomial be written as a sum of squares of rational functions?

$$p = \sum_{j=1}^{k} \frac{\sigma_j^2}{\xi_j^2}$$

- Artin and Schreier'1927: Theory of real-closed fields.

Why SOS?

- Checking if a polynomial is SOS can be made efficient.
    - Reduction to semi-definite programming (convex optimization).
- Positivstellensatz using Sum of Squares.
    - Lasserre Hierarchy.
    - Next lecture.

Checking SOS

Input: $p \in \mathbb{R}[x_1, \dots, x_n]$.

Output: Is $p = \sigma_1^2 + \cdots + \sigma_k^2$ for $\sigma_1, \dots, \sigma_k \in \mathbb{R}[x_1, \dots, x_n]$?

Idea: quadratic forms but lift to a higher dimensional space.

- Originally proposed by N. Shor, 1987 (In Russian).
- Rediscovered by Lasserre'2001 and Parrilo'2003.
    - Global Optimization with Polynomials and the Problem of Moments, Jean B. Lasserre, SIAM J. Opt., 2001.
    - Semidefinite programming relaxations for semialgebraic problems, Pablo Parrilo, Math. Prog. Ser. B, 2003.

Idea Write a non-quadratic polynomial as a quadratic form.

Example $x^4y^2 - 2x^2y^2 + 2y^2 - 2xy + x^2 + 9$

Let $\mu(x,y) = \begin{pmatrix} x^2y \\ xy \\ x \\ y \\ 1 \end{pmatrix}$, Write $p = \mu^\top Q \mu$.

Example (Continued)

$$p = x^4y^2 - 2x^2y^2 + 2y^2 - 2xy + x^2 + 9$$

	x^2y	xy	x	y	1
x^2y	1	0	0	−1	0
xy	0	0	0	0	0
x	0	0	1	−1	0
y	−1	0	−1	2	0
1	0	0	0	0	9

Problem: Q is not unique.

Example: Non-Uniqueness

$$p = x^4y^2 - 2x^2y^2 + 2y^2 - 2xy + x^2 + 9$$

	x^2y	xy	x	y	1
x^2y	1	0	0	0	0
xy	0	−2	0	0	0
x	0	0	1	−1	0
y	0	0	−1	2	0
1	0	0	0	0	9

Q is not a psd matrix.

Basic Idea.

- Fix a vector of monomials $\mu(x_1, \ldots, x_n)$.

- Try to write polynomial p as

    - $p = \mu^\top Q \mu$
    - Q is a positive semidefinite matrix.

- However, there are infinitely many ways of doing so.

    - We need to discover one way to do it!

Next Session

- How to check if a polynomial is SOS?
    - Semi-Definite Programming.
- Positivstellensatz.