Algebraic and Semi-Algebraic Reasoning For Formal Methods

Lecture 5 - Sum of Squares Programming.

Sriram Sankaranarayanan

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 $p(x_1, \dots, x_n)$ can be written:

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

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: 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.

Checking SOS

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

Output: Is $p = \sigma_1^2 + \dots + \sigma_k^2$ 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.

Checking Sum of Squares : Idea

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

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

$$\begin{array}{c|ccccc} & x^2y & xy & x & y & 1 \\ \hline x^2y & 1 & 0 & 0 & 0 & 0 \\ xy & 0 & -2 & 0 & 0 & 0 \\ x & 0 & 0 & 1 & -1 & 0 \\ y & 0 & 0 & -1 & 2 & 0 \\ 1 & 0 & 0 & 0 & 0 & 9 \end{array}$$

Q is not a psd matrix.

Basic Idea.

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

Constraint Problem

Let $p = \sum_{\alpha \in \mathbb{N}^n} c_\alpha \vec{x}^\alpha$.

- $M(p)$: set of monomials in p.
- Choose a monomial basis $\mu(\vec{x}) = [\beta_1, \ldots, \beta_k]$.
  - Every $\alpha \in M(p)$ can be written as the sum of two monomials in the basis.
- Let Q be an unknown *positive semi-definite matrix* that we seek.
- *Question:* What are the constraints on Q?

Constraint Problem (continued)

For every monomial $\alpha \in M(p)$, let

$$C(\alpha) = \{(i, j) \mid \beta_i + \beta_j = \alpha\}$$

Each monomial imposes a constraint on the entries of Q:

$$\sum_{(i,j) \in C(\alpha)} Q_{i,j} = c_\alpha$$

- Linear equality involving entries of Q.

Constraint Problem (continued)

$$
\begin{array}{rl}
\text{find} & Q \in \mathbb{R}^{|\mu|\times|\mu|} \\
\text{s.t.} & \\
& \vdots \\
& (C_\alpha, Q) = c_\alpha \quad \leftarrow \text{ linear equations over entries of } Q \\
& \vdots \\
& Q \succeq 0 \qquad\quad \leftarrow \text{ PSD constraint}
\end{array}
$$

This is called a semi-definite programming problem (SDP).

Semi-Definite Programming

- Trace inner product:
  - $(A, B) = \mathsf{tr}(A \times B) = \sum_i \sum_j A_{i,j} B_{i,j}$.

SDP Problem: Decision Variable $X \in \mathbb{R}^{n \times n}$.

$$
\begin{aligned}
\min \quad & (C, X) \\
& (A_1, X) = b_1 \\
& \vdots \\
& (A_m, X) = b_m \\
& X \succeq 0
\end{aligned}
$$

Semi-Definite Programming

Semidefinite Programming, S. Boyd and L. Vandenberghe, SIAM REVIEW Vol. 38, No. 1, pp. 49-95, March 1996.

- Lots of applications of SDPs,
  - Engineering design problems
  - Data Analysis Problems
  - Approximation Algorithms
- Properties of SDPs,
- Techniques for Efficient Solution.

Semi-Definite Programming: Primal vs. Dual Forms

$$
\begin{aligned}
\min \quad & (C, X) \\
\text{s.t.} \quad & (A_1, X) = b_1 \\
& \vdots \\
& (A_m, X) = b_m \\
& X \succeq 0
\end{aligned}
$$

$$
\begin{aligned}
\min \quad & \sum_{j=1}^{m} b_j x_j \\
\text{s.t.} \quad & C + \sum_{j=1}^{m} x_i A_i \ \succeq \ 0
\end{aligned}
$$

Note: both forms are interchangable.

SDP : Solution

$$\begin{aligned} \min \quad & (C, X) \\ \text{s.t.} \quad & (A_1, X) = b_1 \\ & \vdots \\ & (A_m, X) = b_m \\ & X \succeq 0 \end{aligned}$$

- Infeasible
- Unbounded
- Feasible and Optimal
  - Symmetric PSD matrix X.
  - X satisfies the constraints.
  - Minimizes the objective.

Solving SDPs

- Interior point methods.
- Basic Idea: Use a barrier function.
- **TODO** Illustrate what barrier functions are and how interior point methods work.

Solving SDPs: Convergence

- Requires strict feasibility.
  - There exists a solution $X \succ 0$ satisfying constraints.
- Guaranteed to get a solution that is within $\epsilon > 0$ distance of optimal solution.
  - Time complexity in problem size and $\log(\frac{1}{\epsilon})$.
  - Arithmetic operations are typically $O(1)$.

SDP Numerics

SDPs are typically solved using floating point arithmetic.

- Some extended precision solvers such as SDPA.

Optimal solution need not be rational.

$$\begin{aligned} \max \quad & X_{1,2} \\ \text{s.t.} \quad & X_{1,1} = 1 \\ & X_{2,2} = 2 \\ & X \succeq 0 \end{aligned}$$

- Optimal solution is $\sqrt{2}$.

SDP Numerics (continued)

- SDP solution verification.
  - Check that matrix X is a PSD.
    - Can use Cholesky decomposition.
  - Check that the equality constraints are satisfied.

Cf. Roux, Voronin and Sank. Validating Numerical Semidefinite Programming Solvers for Polynomial Invariants, SAS 2016 and STTT 2018.

Sum of Squares Checking

Given $p \in \mathbb{R}[x_1, \ldots, x_n]$, how do we find the monomials needed for μ?

- Hint: consider maximum degree in each variable.

Newton Polytope: Consider $p = \sum_{\alpha \in \mathbb{N}^n} c_\alpha \vec{x}^\alpha$.

- Collect all monomials as vectors $\alpha \in \mathbb{N}^n$ such that $c_\alpha \neq 0$.
- Compute the convex hull P of the vectors in $\mathbb{N}^n$ corresponding to the monomials.
- Compute all the points in $\frac{1}{2}P$.
- Any monomial $\vec{x}^\beta$ appears in the SOS decomposition of p iff $\beta \in \frac{1}{2}P$.

Proving Entailments

$$(\forall x, y \in \mathbb{R}) \quad x^2 + y^2 \leq 1 \ \wedge \ x + y \leq 0 \ \Rightarrow \ y \leq 1.423$$

Why?

$$(1.423 - y) = \left(\begin{array}{c} 0.765134 \ \ (1 - x^2 - y^2) + \\ 0.4 \quad - (x + y) + \\ 0.6574 - 0.6x + 0.4y + 0.765134(x^2 + y^2) \end{array} \right)$$

Positivstellensatz

Consider entailment over $\mathbb{R}^n$:

$$p_1 \geq 0 \ \wedge \ \cdots \ \wedge \ p_m \geq 0 \ \models \ p \geq 0$$

- One approach is to try to convert to real Nullstellensatz.

Inequalities to Equalities

Consider polynomials over $p \in \mathbb{R}[x_1, \dots, x_n]$.

- Let t be a fresh variable.
- $p \geq 0 \;\Leftrightarrow\; p = t^2$
- $p > 0 \;\Leftrightarrow\; t^2 p = 1$
- $p \neq 0 \;\Leftrightarrow\; tp = 1$

Convert entailment back to equalities.

Real Varieties

Given $p_1, \dots, p_m \in \mathbb{R}[x_1, \dots, x_n]$, define the *real variety* as

$$V = \{\vec{x} \in \mathbb{R}^n \mid \bigwedge_{j=1}^{m} p_j = 0\}$$

- We already saw the importance of algebraic closure.
  - Real variety of $1 + x^2 = 0$.

Theorem $V = \emptyset$ if and only if $1 + \sigma \in \langle p_1, \dots, p_m \rangle$, where σ is SOS.

Positivestellensatz

Let $S = \{\vec{x} \in \mathbb{R}^n \mid p_1(\vec{x}) \geq 0 \ \wedge \ \cdots \ \wedge \ p_m(\vec{x}) \geq 0\}$.

- We wish to show that $p \geq 0$ on S for given p.
- **Important:** We will need S to be compact.

Schmugden's Positivstellensatz

Enrich the set of polynomials

$$Q(S) = \{p_1^{e_1} \cdots p_m^{e_m} \mid e_i \in \{0, 1\}\}$$

Note: $|Q(S)| = 2^m$.

Theorem (Schmugden'1991)

- If $p = \sum_{q \in Q(S)} \sigma_q q$ for SOS polynomials σ_q then $p_1(\vec{x}) \geq 0 \ \wedge \ \cdots \ \wedge \ p_m(\vec{x}) \geq 0 \models p \geq 0$.
- Conversely, if $p_1(\vec{x}) \geq 0 \ \wedge \ \cdots \ \wedge \ p_m(\vec{x}) \geq 0 \models p > 0$ then p can be written as a SOS-combination of polynomials in $Q(S)$.

Putinar's Positivstellensatz

Let $M = \{\sum_{j=1}^{m} \sigma_j p_j + \sigma_0 \mid \sigma_0, \ldots, \sigma_m \text{ SOS}\}$.

- **Archimedean Property:** There exists a K such that

$$x_1^2 + \cdots + x_n^2 \leq K$$

Theorem (Putinar'1993)

- If $p \in M$ then $p_1 \geq 0 \ \wedge \ \cdots \wedge \ p_m \geq 0 \ \models \ p \geq 0$.
- If S compact and M is Archimedean, then $p_1 \geq 0 \ \wedge \ \cdots \ \wedge \ p_m \geq 0 \models p > 0$ then $p \in M$.