Semidefinite programming hierarchies for packing and energy minimization (1/4)

David de Laat (TU Delft)

Summer School on Optimization, Interpolation and Modular Forms,
August 24–28, 2020, EPFL

Topics for the four talks

1. **Sums-of-squares hierarchies for polynomial optimization**
2. Moment hierarchies for polynomial optimization
3. Packing problems
4. Energy minimization problems

Polynomial optimization

$$\{p\} \cup Q \subseteq \mathbb{R}[x_1, \dots, x_n] \text{ finite}$$

Polynomial optimization problem:

$$P = \inf \big\{p(x) : x \in S(Q)\big\}$$

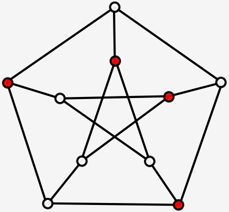
Semialgebraic set:

$$S(Q) = \{x \in \mathbb{R}^n : q(x) \geq 0 \text{ for } q \in Q\}$$

Computing P is NP-hard, even if all polynomials are at most quadratic

Independent set problem

Find a largest independent set in a graph



We can write this as

$$\max\Big\{\sum_{i=1}^{n} x_i : x_i(1-x_i)=0 \text{ for } i=1,\ldots,n,\ x_i+x_j\le 1 \text{ if } i\sim j\Big\}.$$

Sums-of-squares polynomials

Write the problem $P = \inf \{p(x) : x \in S(Q)\}$ as

$$P = \sup \left\{ c \in \mathbb{R} : p(x) - c \geq 0 \text{ for } x \in S(Q) \right\}$$

Quadratic module

$$\mathcal{M}(Q) = \text{cone}\left\{ qs^2 : q \in \{1\} \cup Q,\ s \in \mathbb{R}[x_1, \ldots, x_n] \right\}$$

Truncated quadratic module

$$\mathcal{M}_t(Q) = \text{cone}\left\{ qs^2 : q \in \{1\} \cup Q,\ s \in \mathbb{R}[x_1, \ldots, x_n],\ \deg(qs^2) \leq 2t \right\}$$

The Lasserre hierarchy

$$P_t^{\text{sos}} = \sup \left\{ c \in \mathbb{R} : p - c \in \mathcal{M}_t(Q) \right\}$$

Exercise 1

Show $p \in \mathcal{M}(Q)$ implies $p \geq 0$ on $S(Q)$;

Show $P_t^{\text{sos}} \leq P$ for all t.

Sums-of-squares polynomials

Exercise 2

Let $m(x)$ be a vector whose entries form a basis for the space $\mathbb{R}[x_1, \ldots, x_n]_t$ of polynomials of degree at most t. Then $p \in \mathbb{R}[x_1, \ldots, x_n]_{2t}$ is a sum-of-squares polynomial if and only if there is a positive semidefinite matrix A such that

$$p(x) = m(x)^\mathsf{T} A m(x).$$

Hint: use the Cholesky factorization.

Semidefinite programming

In a semidefinite program we minimize (or maximize) a linear functional over positive semidefinite matrices with linear constraints:

$$\inf \left\{ \langle C, X \rangle : X \in \mathbb{R}^{n \times n},\, X \succeq 0, \langle A_i,\, X \rangle = b_i \text{ for } i = 1, \ldots, m \right\}.$$

Here $\langle C, X \rangle = \mathrm{tr}(C^{\mathsf{T}} X)$ is the trace inner product and $X \succeq 0$ means X is positive semidefinite.

Generalization of linear programming.

Semidefinite programs can be solved in polynomial time (roughly in the size of the problem and $\log(1/\epsilon)$, where $\epsilon > 0$ is the additive error).

Semidefinite programs can be solved efficiently in practice using interior point methods.

Exercise 3
Show P_t^{sos} is a semidefinite program.

What happens as $d \to \infty$?

Definition

$\mathcal{M}(Q)$ is archimedean if for every polynomial p there is a constant $C > 0$ such that $C - p \in \mathcal{M}(Q)$.

Exercise 4

Show $\mathcal{M}(Q)$ is archimedean if and only if there exists a constant $N > 0$ such that

$$N - \sum_{i=1}^{n} x_i^2 \in \mathcal{M}(Q).$$

Hint: For the "if" direction first show $(N + \frac{1}{4}) \pm x_i \in \mathcal{M}(Q)$ for any $i = 1, \ldots, n$. Then extend to the full polynomial ring.

What happens as $d \to \infty$?

Putinar's Theorem (1993)
Suppose $\mathcal{M}(Q)$ is archimedean. If p is strictly positive on $S(Q)$, then $p \in \mathcal{M}(Q)$.

$$P = \sup \left\{ c \in \mathbb{R} : p(x) - c \geq 0 \text{ for } x \in S(Q) \right\}$$

$$P_t^{\text{sos}} = \sup \left\{ c \in \mathbb{R} : p - c \in \mathcal{M}_t(Q) \right\}$$

Asymptotic convergence follows from Putinar's theorem: If $\mathcal{M}(Q)$ is archimedean, then $P_t^{\text{sos}} \to P$ as $t \to \infty$.

Background

In the PhD thesis (2000) of Parrilo SOS and SDP are used to compute the global minimum of a polynomial.

The hierarchy P_t^{sos} introduced by Lasserre in 2001.

In computer science this is used to study approximation algorithms

In quantum information theory there are noncommutative extensions such as the NPA hierarchy (2007).

Is there a contradiction?

Semidefinite programs can be solved in polynomial time (roughly in the size of the problem and $\log(1/\varepsilon)$, where ε is the additive error).

But the independent set problem is NP-hard, and we can write the independent set problem as a polynomial optimization problem of polynomial size.

The value of t for which $P_t^{\mathrm{sos}} = P$ holds depends on the graph and can grow linearly in n (although we will see t does not need to be larger than the independence number).

If t grows linearly in n, the dimension of $\mathbb{R}[x_1, \ldots, x_n]_t$, and thus the size of P_t^{sos}, grows exponentially in n, so there is no contradiction.

Does finite convergence always hold?

The Motzkin polynomial

$$p = x_1^4 x_2^2 + x_1^2 x_2^4 + x_3^6 - 3x_1^2 x_2^2 x_3^2$$

is nonnegative on $\mathbb{R}^3$, which follows from the AM-GM inequality:

$$x_1^2 x_2^2 x_3^2 = \sqrt[3]{(x_1^4 x_2^2)(x_1^2 x_2^4) x_3^6} \leq \frac{x_1^4 x_2^2 + x_1^2 x_2^4 + x_3^6}{3}.$$

It can be shown that p is not a sum-of-squares polynomial. In fact, it can be shown p does not lie in $\mathcal{M}(\{1 - (x_1^2 + x_2^2 + x_3^2)\})$.

This gives an example where $P_t^{\text{sos}} < P$ for all t.

Certificates

Putinar's theorem is an example of a Positivstellensatz.

Hilbert's Nullstellensatz gives a certificate for a polynomial p to be zero at the common zero set of some given polynomials: Write some power of p as an element in the ideal generated by those polynomials.

A Positivstellensatz is a real algebraic version of this: Find a certificate for a polynomial p to be positive on a set.

To find a Nullstellensatz certificate we can use linear algebra, but to find a Positivstellensatz certificate we need optimization.

There are many other Positivstellensatze, but Putinar's theorem is good computationally (SDP) and in practice often gives finite convergence.