

Proofs, beliefs and algorithms through the lens of sums of squares

Boaz Barak
Harvard

Pablo Parrilo
MIT

David Steurer
IAS/Cornell

Pravesh Kothari
Princeton/IAS

<http://www.boazbarak.org/sos>

<http://www.sumofsquares.org>

ADMINISTRATIVE ISSUES

Instructors: Boaz Barak (Harvard) and Pablo Parrilo (MIT)

Web site: <http://www.boazbarak.org/sos>

Join Piazza if you haven't already!

Times and locations: Fridays 10am-1pm *See Google calendar!*

MIT: 5-234 (55 Mass Ave) **Harvard:** MD-221 (33 Oxford St)

Will poll re make-up lectures

What you need to do:

- Show up
- Do reading before each lecture
- Do exercises (informally, collaboration is fine)
- Participate in Piazza and class discussion
- Can post about homeworks (use "spoiler alerts")

TWO MOST BEAUTIFUL WORDS IN THE ENGLISH LANGUAGE:

LINEAR

CONVEX

THE WORLD IS A CRUEL PLACE

Non-linearity and non-convexity abound...

Optimization: Discrete problems (e.g., constraint-satisfaction, integer programming)

Learning: Non convex objectives (e.g., neural networks)

Control: Non linear systems (e.g., everything)

CAN'T SOLVE IN GENERAL..

..TAILORED ALGORITHMS/HEURISTICS FOR SPECIAL CASES

OUR FOCUS: A GENERAL FRAMEWORK

Sum of Squares semidefinite program [Shor'87,Parrilo'00,Lasserre'01]:

- Applicable to any* non-linear problem.
- Sometimes works, sometimes doesn't
(always works if you give it enough time)
- Often as good as best-known tailor made algorithm.
- Even when it **fails**, state can be interpreted as **partial knowledge**.

SUM OF SQUARES:
AN ABBREVIATED HISTORY

DUAL TASKS:

Search/Decision:

Compute $\min_{x \in \Omega} f(x)$

(or $\operatorname{argmin}_{x \in \Omega} f(x)$)

Refutation:

Certify $f(x) \geq \alpha$

for all $x \in \Omega$

Turn of 20th century: $\Omega = \mathbb{R}^n$, $f = \text{polynomial}$

Minkowski 1890's: If $f(x) \geq 0 \forall x \in \mathbb{R}^n$ are there poly's p_1, \dots, p_m s.t.

$$f = p_1^2 + \dots + p_m^2 ?$$

Hilbert 1896: **No!** Moreover, characterize when this happens.

(Motzkin 1966: $f(x) = x^2 + y^2x^4 + y^4 - 3x^2y^2$)

Hilbert's 17th problem (1900): Are there rational functions r_1, \dots, r_m s.t.

$$f = r_1^2 + \dots + r_m^2 ?$$

Artin (1927): Yes!

Stengle (1964), Krivine (1974): Generalize to many f 's, arbitrary varieties Ω

Known as **Positivstellensatz**

QUANTITATIVE VERSIONS*

PROOFS

Vorobjev-Grigoriev'99:

Measure complexity by max degree d

Grigoriev'01: $d = \Omega(n)$ for 3XOR,
Knapsack

ALGORITHMS

N.Shor'87: $n^{O(d)}$ time alg for
finding restricted degree d Psatz
proofs.

Parrilo'00, Lasserre'01:
 $n^{O(d)}$ time alg for general proofs

TYPICAL QUESTIONS: If $\min f(x) = \alpha^*$

What's the smallest d^* s.t. $\Vdash_{d^*} f \geq \alpha^*$?

For given d what's the largest α^d s.t. $\Vdash_d f \geq \alpha^d$?

If $\alpha^d < \alpha^*$ can we still get **partial information** about $x^* = \operatorname{argmin} f(x)$?

* Counting numbers, not bits (ignoring numerical precision issues)