CSE 599S Proof Complexity & Applications

Lecture 14 — 18 Nov 2020

- Presentation papers
  - See e-mail - papers listed are just samples
  - arrange time to talk with me about potential paper if you would like
  - 25 min talk week of Dec 14-18.
  - send me ranked preferences (1-3)

Cutting Planes — Sherali-Adams — Sum-of-Squares

PC, IR, Resolution

F $\quad (h_1 \geq 0, \ldots, h_m \geq 0)$

$(\ell_{C_1} \geq 0, \ldots, \ell_{C_m} \geq 0)$

$x \vee \bar{y} \vee z$ dual var

$\ell_C \quad x + y + z - 1 \geq 0$

$\ell_{C_i} \quad x + (1-y) + z - 1 \geq 0$

Derivation that $h \geq 0$

SA: $g_0 + \sum_i g_i \ell_{C_i} \equiv_I h$ ← multilinear reduction

each $g_i = \sum a_j J_{P_i N_i}$ $\quad a_j > 0$

non-neg juntas

Finding SA proofs

LP deg d ⇒ time $n^{O(d)}$

SoS: $q_0 + \sum_i q_i \ell_{C_i} \equiv_I h$

each q_i is a sum of squares

$q_i = \sum_j p_j^2$

Find SoS proofs

Semi-definite program SDP

deg d size of SDP $\binom{n}{\leq d}$ $n^{O(d)}$

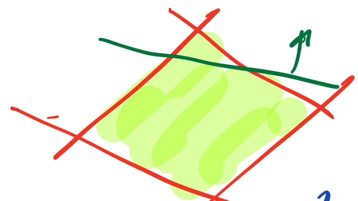
SDPs. vs LPs.

LP

$\min c^T \cdot x$ objective fn

$$\boxed{\begin{matrix} Ax=b \\ x\geq 0 \end{matrix}}$$

polytope



polytope

SDP

view 1:

$\min c^T \cdot x$

$Ax=b$

$x \geq 0$

$\rightarrow$ each x_i is an inner product

X

$$\begin{pmatrix} x_{11} & \cdots \\ \cdots & \cdots \end{pmatrix}$$

$$\times$$

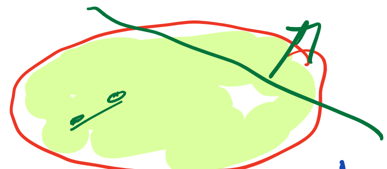
$(x_{11}, \ldots, x_{nn})$

$\min c^T \cdot X$

$$\boxed{AX=b}$$

$$\boxed{X \succeq 0}$$

positive definite constraint



ellipsoid

X is ~~square~~ symmetric, square matrix

all eigenvalues are real

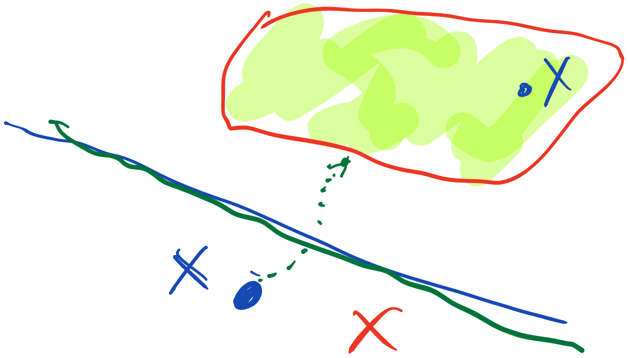
all eigenvalues ≥ 0

A

$y^T X y \geq 0$

$\forall y$

Khachian's Ellipsoid Method for LP also "works" for SDPs.



Convex region

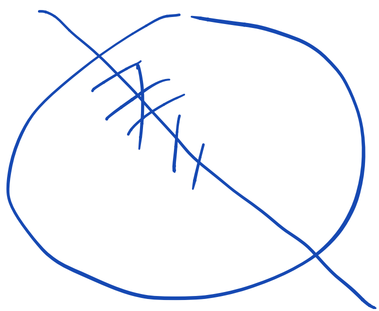
enough for first alg.

For LP immediate
ellipsoid trickier.

Can find deg d SOS proof in time $n^{O(d)}$

Optimization MAXCUT

(G, w)



max total weight of edges crossing the cut

NP-hard

Best LP $\frac{1}{2}$ approx

Best known .878 approx
given by an SDP
SOS degree 2

Beyond SOS: Positivstellensatz

$h_1 \geq 0, \dots, h_m \geq 0$

$h \geq 0$ on K.

SOS

$$\boxed{q_0 + \sum q_i h_i \equiv_I h}$$

q_i is SOS

if $h_1 \geq 0$ and $h_2 \geq 0$

Then $h_1 h_2 \geq 0$

Positivstellensatz

$$\boxed{q_0 + \sum_{S \subseteq [m]} q_S \prod_{i \in S} h_i \equiv_I h.}$$

q_S is SOS

don't count S s.t. $q_S = 0$

Algorithm?

Dynamic version of Positivstellensatz:
Positivstellensatz Calculus

Can Derive h means $h \geq 0$

Rules:

Axioms:

$$\frac{}{1} \quad \text{trivial}$$

$$\frac{}{h_i} \quad \text{input axiom}$$

Inference.

$$\frac{f}{\text{multilinear}(f)} \quad \text{multilin}$$

$$\frac{f, g}{af + bg} \quad \text{(linear combo)} \quad a, b \geq 0$$

$$\frac{f, g}{f + g}$$

$$\frac{f}{x \cdot f}$$ (1, trivial)

$$\frac{f}{p^2 \cdot f}$$ p poly

so far get SOS

$$\frac{f, g}{f \cdot g}$$ Multiplicat rule.

Measures deg, size, bitsize

Lower bounds for size of PS calculus even for deg 2 not known

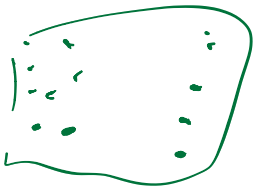
include Lovasz-Schrijver proof system

Lower bounds for tree-like proofs

Communication Complexity

Anup Rao - has textbook

two courses in past few years at UW



Players

Alice

$x \in X$

eg $X = \{0,1\}^n$

Goal
Compute $f(x,y)$

Bob

$y \in Y$

eg. $Y = \{0,1\}^n$

01

0

$f(x,y)$

minimize # of bits sent

Trivial protocol

eg.

x

$f(x,y)$

$n+1$ bits

Q: can get less ?

$EQ(x,y) = 1$ if $x = y$

0 o.w.

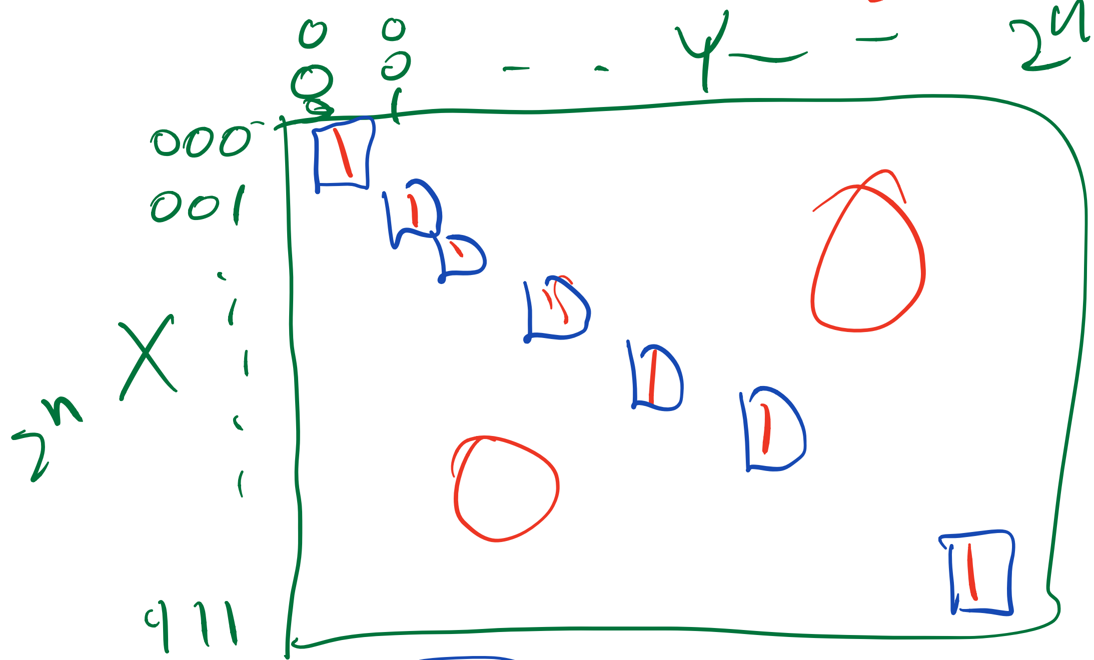
trivial : optimal for EQ

Observation: After each step set of input consistent with transcript is of form

$$\underbrace{A}_{X} \times \underbrace{B}_{Y} \subseteq \underbrace{X \times Y}_{(x,y)}$$

rectangle

$$A \subseteq X, \; B \subseteq Y.$$



$> 2^n$ rectangles

EQ

$C(f) = \#$ of bits

$\Rightarrow > n$ bits of comm

Randomized protocols & error ε.

$C_\varepsilon(f)$

$\Pr[\text{protocol outputs } f(x,y)] \geq 1-\varepsilon$

$C_\varepsilon^{pub}(f)$

shared random string r

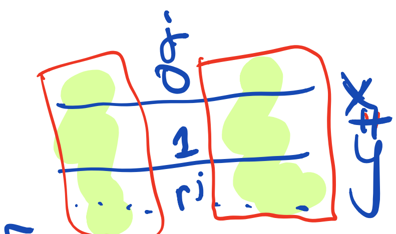
Alice $x \in X$ → Bob $y \in Y$

$\Pi(x,y)$

Claim $C_{1/2^k}^{pub}(EQ) = k+1$

$\Rightarrow C_\varepsilon^{pub}(EQ) = O(\log 1/\varepsilon)$

shared $r_1, \ldots, r_k \in \{0,1\}^n$



random bit

if $x_j \neq y_j$

$\Pr[r^j \cdot x_j \neq r^j \cdot y^j] = 1/2$

if $x \neq y$

$\Pr[r \cdot x = r \cdot y] = 1/2$

Alice x		Bob y
	$r_1 \cdot x \bmod 2 \rightarrow$	
	$r_2 \cdot x \bmod 2 \rightarrow$	
	$\vdots$	
	$r_k \cdot x \bmod 2 \rightarrow$	
	$\leftarrow b$	

if $b=1$ $\left(\begin{array}{c} r_i \cdot x = r_i \cdot y \\ \vdots \\ r_k \cdot x = r_k \cdot y \end{array} \right)$

if $x = y \Rightarrow b = 1$

if $x \neq y \Rightarrow \text{Prob}[b=1] = \frac{1}{2^k}$

<u>Thm</u> $C_\varepsilon(f) \le C_\varepsilon^{pub}(f) + O(\log n)$

<u>Proof idea</u>

Can approx any pub protocol by one with a short r which Alice can flip herself & send to Bob