LECTURE 26

Cutting planes proof system

Input: Inconsistent system of 0-1 linear inequalities

Refutation: Derive $0 \geq 1$

Configuration-style proof

At each derivation step

1. DOWNLOAD axiom constraint
2. Apply INFERENCE rule to constraints in memory
3. ERASE constraint

Inference rules

Variable axioms $\dfrac{}{x \geq 0} \qquad \dfrac{}{-x \geq -1}$

Addition $\dfrac{\sum_i a_i x_i \geq A \qquad \sum_i b_i x_i \geq B}{\sum_i (a_i + b_i) x_i \geq A + B}$

Multiplication $\dfrac{\sum_i a_i x_i \geq A}{\sum_i c a_i x_i \geq cA} \quad c \in \mathbb{N}^+$

Division $\dfrac{\sum_i c a_i x_i \geq A}{\sum_i a_i x_i \geq \lceil A/c \rceil}$

Complexity measures:

Length = # constraints in derivation

Line space = max # constraints in memory

What about magnitude of coefficients?

[Buss & Clote '96] building on [Cook, Coullard & Turán '87]

(a) Cutting planes with division only by fixed $k \geq 2$ is as powerful as general cutting planes (up to polynomial factors)

(b) Suppose coefficients and constants have absolute values $\leq B$ and that cutting planes refutes input of length L. Then $\exists$ refutation of length $O(L^3 \log B)$ with coefficients and constants of absolute value $O(L^2 \cdot B \cdot 2^L)$.

So coefficients need not have more than polynomial # bits / exponential magnitude

[Dadush & Tiwari '20] proved analogous result for stabbing planes.

OPEN PROBLEM: Possible to bring this down to logarithmic # bits / polynomial magnitude? Buss & Clote state that this was their goal.

Still remains open!

What would separating formulas look like?

Define CP* as cutting planes, but in any derivation the coefficients and constant terms should have size at most polynomial in size of input — i.e., magnitude = logarithmic # bits

Aside: CP* also defined by requiring integers to have magnitude at most polynomial in input size and exponential in # steps of refutation. Same definition if we insist on polynomial-length refutations. We will define CP* in terms of input.

Can we prove that there is something CP can do efficiently that CP* cannot?

Yes! [dRMNPRV '20]

There are families $\{F_n\}_{n=1}^{\infty}$ of CNF formulas such that
- Cutting planes refutes F_n in (roughly) quadratic length and constant line space simultaneously
- CP* cannot refute F_n in subexponential length and subpolynomial line space simultaneously

MAIN TECHNICAL INGREDIENT
Lifting theorem using equality gadget

HIGH-LEVEL IDEA

CP* IV

Take HORN FORMULA: At most 1 positive literal/clause

Can be refuted by deriving unit clauses z_i in same order in resolution

Make this line-space-efficient in cutting planes by deriving

$$\sum_{i=0}^{n-1} 2^i z_i = \sum_{i=0}^{n-1} 2^i = 2^n - 1$$

(Note that $\sum_i a_i z_i = A$ is syntactic sugar for

$$\sum_i a_i z_i \geq A$$

$$\sum_i -a_i z_i \geq -A \quad)$$

Lift formula F with EQUALITY GADGET

$$EQ(x,y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{o/w} \end{cases} \qquad x, y \in \{0,1\}$$

EXAMPLE

$$C = z_1 \vee \overline{z_2}$$

Then $C[EQ] = C \circ EQ =$

$$\begin{aligned} &(x_1 \vee \overline{y_1} \vee x_2 \vee y_2) \\ \wedge\ &(x_1 \vee \overline{y_1} \vee \overline{x_2} \vee \overline{y_2}) \\ \wedge\ &(\overline{x_1} \vee y_1 \vee x_2 \vee y_2) \\ \wedge\ &(\overline{x_1} \vee y_1 \vee \overline{x_2} \vee \overline{y_2}) \end{aligned}$$

CP* $\overline{V}$

(A) Prove that <u>linear-space-efficient CP-refutation</u> <u>still works</u> for <u>F ∘ EQ</u> if F Horn formula

Derive (in) equalities

$$\sum_{i=0}^{n} 2^i (x_i - y_i) = 0 \qquad (*)$$

Whenever, say, z_k followed from

$$\frac{\begin{array}{l} z_i \\ z_j \end{array}}{\overline{z_i} \vee \overline{z_j} \vee z_k}$$

"decode"

$$x_i = y_i$$
$$x_j = y_j$$

from (*) and apply to

$$(\overline{z_i} \vee \overline{z_j} \vee z_k) \circ EQ$$

to derive

$$x_k = y_k$$

and add to (*). Want to do this length- and space-efficiently

Yields <u>upper bound</u> for <u>general cutting planes</u>.

(B) Suppose there is a short, low-space-efficient refutation π^* in CP* of $F_n \circ EQ$ in length L and low space s

Yields deterministic communication protocol for $Search(F_n) \circ EQ$ in cost

$$\approx s \log L$$

Alice & Bob can evaluate the inequalities and send number — logarithmic # bits

Prove lifting theorem relating communication complexity D^{cc} with decision tree query complexity D^{dt} by

$$D^{cc}(Search(F) \circ EQ) \gtrsim D^{dt}(Search(F))$$

Plug in Horn formulas with large decision tree query cplx — PEBBLING FORMULAS

DONE Right?

Except [Loff & Mukhopadhyay '19] show that such lifting theorem is NOT TRUE for
- equality gadget
- relations/search problems (as opposed to functions)

So instead
- Use equality gadget over non-constant # bits
- Lift Nullstellensatz refutation degree (happens to be = query cplx for pebbling formulas)

A (TOTAL) SEARCH PROBLEM is a relation $S \subseteq \mathcal{I} \times \mathcal{O}$ such that for all $z \in \mathcal{I}$ there exists $o \in \mathcal{O}$ for which $(z, o) \in S$

Think of this as computational task: Given z, find o s.t. $(z, o) \in S$

If $\mathcal{I} = \mathcal{I}^w$ has product structure, and $g : X \times Y \to \mathcal{I}$ is a function (a GADGET), then the COMPOSED/LIFTED SEARCH PROBLEM $S \circ g^n \subseteq (X^n \times Y^n) \times \mathcal{O}$ is the task given $x \in X^n$ and $y \in Y^n$ to find o s.t. $(g^n(x,y), o) \in S$ where

$$g^n(x,y) = (g(x_1,y_1), g(x_2,y_2), \ldots, g(x_n,y_n))$$

Our previous lifting theorems worked for any search problem

Now we have to focus on FALSIFIED CLAUSE SEARCH PROBLEM: Given assignment x to (fixed) unsatisfiable CNF formula F, find clause C falsified by x.

Denote this problem Search(F)

Lifted search problems yield natural communication problems

DETERMINISTIC COMMUNICATION PROTOCOL

Two players Alice with input $x \in X^n$
Bob with input $y \in Y^n$

Protocol tree Π
- Every internal node v labelled by function $f_v^A : X^n \to \{0,1\}$ (Alice speaks) or $f_v^B : Y^n \to \{0,1\}$ (Bob speaks)
- Every internal node has two outgoing edges labelled 0 and 1, respectively
- Input $x \in X^n \times Y^n$ defines path to leaf ℓ_x
- Leaf ℓ_x should be labelled by answer to $S \circ g^n$
- Cost of protocol Π = length of longest path = max # bits communicated
- For problem P, write $D^{cc}(P)$ for minimal cost of any protocol

---

Given any gadget $g : \{0,1\}^q \times \{0,1\}^q \to \{0,1\}$ and CNF formula F, can define

LIFTED FORMULA $F[g]$ or $F \circ g$ by

- replace all literals z_i by CNF encoding of $g(x_{i,1}, \dots, x_{i,q}, y_{i,1}, \dots, y_{i,q})$
- replace all literals $\bar{z}_i$ by CNF encoding of $\neg g(x_{i,1}, \dots, x_{i,q}, y_{i,1}, \dots, y_{i,q})$
- expand all clauses $C \in F$ to CNF in canonical way

OBSERVATION
For any unsatisfiable CNF formula F and any gadget g,

$$D^{cc}(\text{Search}(F \circ g)) \geq D^{cc}(\text{Search}(F) \circ g)$$

We will be interested in the RANK of gadgets

For $g : X \times Y \to \{0,1\}$, the **RANK** of g over the field $\mathbb{F}$, denoted $\text{rank}_{\mathbb{F}}(g)$, is the rank over $\mathbb{F}$ of the matrix with
- rows indexed by $x \in X$
- columns indexed by $y \in Y$
- the cell (x,y) containing $g(x,y)$

EXAMPLE The gadget $EQ^q : \{0,1\}^q \times \{0,1\}^q \to \{0,1\}$ defined by

$$EQ^q(x,y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$$

has $\text{rank}_{\mathbb{F}}(EQ^q) = 2^q$ over any field $\mathbb{F}$

LEMMA [HN 12]
If there is a cutting planes refutation $\Pi : F \vdash \bot$ in length L, line space S, and coefficients and constant terms (absolute values) bounded by B, where F is over n variables, then

$$D^{cc}(\text{Search}(F)) = O(S \cdot (\log B + \log n) \log L)$$

NULLSTELLENSATZ [BIKPP '94]

Given field $\mathbb{F}$

Polynomials $P = \{p_1, \ldots, p_m\}$ over $x_1, \ldots, x_n$

Boolean axioms $x_j^2 - x_j \quad j \in [n]$

a NULLSTELLENSATZ REFUTATION is a sequence of polynomials $q_1, \ldots, q_m, r_1, \ldots, r_n$ s.t. the syntactic equality

$$\sum_{i=1}^{m} q_i p_i + \sum_{j=1}^{n} r_j (x_j^2 - x_j) = 1 \quad (*)$$

holds (after cancellations).

Proof system for CNF formulas by translating clauses

$$C = \bigvee_{z \in P} z \vee \bigvee_{z \in N} \bar{z}$$

to

$$p(C) = \prod_{z \in P} (1 - z) \cdot \prod_{z \in N} z$$

The DEGREE of a Nullstellensatz refutation is the largest total degree of a left-hand side polynomial in $(*)$

$\deg_{NS}^{\mathbb{F}}(F)$ = min NS degree of any refutation of F over $\mathbb{F}$