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 $\dfrac{}{x \geq 0}$ $\dfrac{}{-x \geq -1}$

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

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 & Turan '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 in length $L$. Then $\exists$ refutation in 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. Some 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 sublogarithmic 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 some 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

$$C = z_1 \vee \bar{z}_2$$

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

$$\begin{aligned} & (x_1 \vee \bar{y}_1 \vee x_2 \vee y_2) \\ \wedge\ & (x_1 \vee \bar{y}_1 \vee \bar{x}_2 \vee \bar{y}_2) \\ \wedge\ & (\bar{x}_1 \vee y_1 \vee x_2 \vee y_2) \\ \wedge\ & (\bar{x}_1 \vee y_1 \vee \bar{x}_2 \vee \bar{y}_2) \end{aligned}$$

(A) Prove that line-space-efficient CP-refutation $CP^*_{\overline{V}}$ still works for FO EQ if F Horn formula

Desire (in) equalities

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

Whenever, say, $z_k$ followed from

$$z_i$$
$$z_j$$
$$\overline{z_i} \vee \overline{z_j} \vee z_k$$

"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 upper bound for general cutting planes.

CP* VI

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

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

$$s \log L$$

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

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

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)

$EQ_q : \{0,1\}^q \times \{0,1\}^q \to \{0,1\}$ $\quad EQ_q(x,y) = 1$ iff $x = y$

## MAIN LIFTING THEOREM

Suppose that
- $F$ minimally unsatisfiable CNF formula over $n$ variables
- $\mathbb{F}$ any field
- $g : X \times Y \to \{0,1\}$ any gadget such that

$$\text{rank}_{\mathbb{F}}(g) \geq \frac{6^c n}{\text{Deg}^{\mathbb{F}}_{NS}(F \vdash \bot)}$$

Then

$$D^{cc}(\text{search}(F) \circ g) \geq \text{Deg}^{\mathbb{F}}_{NS}(F \vdash \bot)$$

## UPPER BOUND FOR CP

Suppose that
- $G$ any DAG with constant fan-in & single sink
- $q \in \mathbb{N}^+$, $q = O(\log \log n)$

Then the formula $Peb_G \circ EQ_q$ has
- $O(n \log \log n)$ variables
- $\tilde{O}(n)$ clauses of width $O(\log \log n)$
- cutting planes refutation in simultaneous length $\tilde{O}(n^2)$ and line space $O(1)$

$\tilde{O}(f(n))$ means $O\left(f(n) (\log (f(n)))^k\right)$ for some constant $k$

## LOWER BOUND FOR CP*

Any CP* refutation of $Peb_G \circ EQ_q$ as above in length $L$ and line space $s$ must satisfy

$$s \log L = \Omega(n / \log^2 n)$$

Equality gadget provides a sweet spot:

- Hard for deterministic communication (which can use CP* proofs)
- Easy for randomized and real communication (otherwise we would get hardness for general cutting planes

## SOME OPEN PROBLEMS

1. Size separation for CP vs CP*
2. Line space lower bounds for CP*
3. True length-space trade-offs for CP* that do not apply for CP
4. Direct lower bound proof for parity decision tree query cplx for pebbling formulas

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

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

If $I = I^w$ has product structure, and $g : X \times Y \to I$ is a function (a GADGET), then the COMPOSED/LIFTED SEARCH PROBLEM $S \circ g^n \subseteq (X^n \times Y^n) \times O$ 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 $\Pi$

- 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 $\ell_x$
- Leaf $\ell_x$ should be labelled by answer to $S \circ g^n$
- Cost of protocol $\Pi$ = 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 $P = \{p_1, \dots, p_m\}$ over $x_1, \dots, x_n$

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

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

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

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 $(*)$

$$\mathrm{Deg}_{NS}^{\mathbb{F}}(F \vdash \bot) = \text{min NS degree of any refutation of } F \text{ over } \mathbb{F}$$

Let $\mathcal{P} \in \mathbb{F}[\vec{z}]$ be set of polynomials and $d \in \mathbb{N}^+$

A **d-DESIGN** for $\mathcal{P}$ is a mapping $D$ of polynomials in $\mathbb{F}[\vec{z}]$ of degree $\leq d$ to $\mathbb{F}$ such that

(1) $D$ is linear

(2) $D(1) = 1$

(3) $D(q p_i) = 0$ for all $p_i \in \mathcal{P}$ and all $q$ such that $\mathrm{Deg}(q p_i) \leq d$

(4) $D(z_i^2 q) = D(z_i q)$ for all $q$ s.t. $\mathrm{Deg}(q) \leq d-1$

THEOREM [Buss '98]
Suppose $\mathcal{P} \in \mathbb{F}[\vec{z}]$ is such that $z_i^2 - z_i \in \mathcal{P}$ for all $z_i$. Then $\mathrm{Deg}^{\#}_{NS}(\mathcal{P}+1) > d$ if and only if $\mathcal{P}$ has a $d$-design.

THEOREM [dRMNPRV '20]
For any single-sink DAG $G$ and any field $\mathbb{F}$ it holds that $\mathrm{Deg}^{\#}_{NS}(\mathrm{Peb}_G + 1)$ coincides with the reversible pebbling price of $G$.

Proof sketch Let $V(G) = \{1, 2, \ldots, n\}$
Identify $S \subseteq [n]$ with $z_S = \prod_{i \in S} z_i$.
For fixed $d \in \mathbb{N}^+$, define

$D(z_S) = 1$ is pebble configuration reachable from $\emptyset$ by reversible pebbling in space $\leq d$

$D(z_S) = 0$ otherwise

This is a $d$-design iff reversible pebbling price of $G > d$.

Just for the record, $\boxed{Peb_G}$ is the set of polynomials

- $1 - z_s$ for each source vertex $s$
- $(1 - z_v) \prod_{u \in pred(v)} u$ for non-source vertex $v$ with immediate predecessors $pred(v)$
- $z_t$ for the sink/target vertex $t$
- and also $z_v^2 - z_v$ for all $v$