Cutting planes proof system

<u>Input</u>: Inconsistent system of 0-1 linear inequalities
<u>Refutation</u>: 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

<u>Inference rules</u>

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

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

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

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

<u>Complexity measures</u>:
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

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 of CNF formulas $\{F_n\}_{n=1}^{\infty}$ 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

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

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

<u>EXAMPLE</u>

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

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

$$(x_1 \vee \overline{y}_1 \vee x_2 \vee y_2)$$
$$\wedge (x_1 \vee \overline{y}_1 \vee \overline{x}_2 \vee \overline{y}_2)$$
$$\wedge (\overline{x}_1 \vee y_1 \vee x_2 \vee y_2)$$
$$\wedge (\overline{x}_1 \vee y_1 \vee \overline{x}_2 \vee \overline{y}_2)$$

CP* V

(A) Prove that line-space-efficient CP refutation still works for $F \circ EQ$ 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

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

"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 π^* 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

$$\approx s \log L$$

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

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

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

DONE

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)