Lecture 12: Feasible Interpolation for CP 2 — Oct 14

Last time: Feasible interpolation for Resolution depth by communication protocols.

Thm Let $F = A(x,y) \wedge B(x,z)$ be an unsat. CNF. Then

$$D_{Res}(F) \geq CC(KW(f_F)) = \text{min depth of boolean circuit for } f_F$$

If all x vars occurred positively in A, then

$$D_{Res}(F) \geq CC(mKW(f_F)) = \text{min depth of a monotone boolean circuit for } f_F$$

actually prove lbs!

Today:

Thm Let $F = A(x,y) \wedge B(x,z)$ be an unsatisfiable CNF formula such that every x variable occurs positively in A, then

$$S_{CP}(F) \geq \text{min size of any real monotone circuit computing } f_F$$

"Real" monotone computation?

Regular monotone boolean circuits only allow $\wedge$ (AND) and $\vee$ (OR) gates to compute boolean functions.

Real monotone circuits allow any real function

$$\varphi : \mathbb{R} \to \mathbb{R} \quad \text{or} \quad \psi : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$

that is monotone in their inputs as gates. So, if

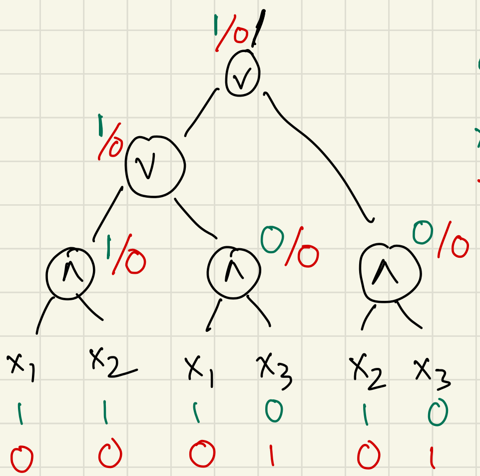
$$x_1, x_2, y_1, y_2 \in \mathbb{R}, \quad x_1 \le x_2, \; y_1 \le y_2 \quad \text{then}$$

$$\varphi(x_1) \le \varphi(x_2), \quad \psi(x_1, y_1) \le \psi(x_2, y_2).$$

ex) Consider $MAJ_3 : \{0,1\}^3 \to \{0,1\}$

$MAJ_3(x) = 1$ iff ≥ 2 input bits are 1.

Monotone Boolean Ckt

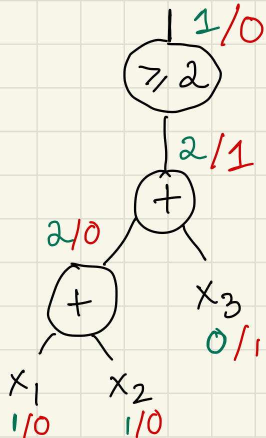


ex)

$x = 110$

$y = 001$

Real Monotone Ckt



$+ :=$ addition over $\mathbb{R}$

$\boxed{\geq 2} :=$ outputs 1 if input is ≥ 2, 0 o/w.

Monotone in it's input

if $x \le y$ then $(\geq 2)(x) \le (\geq 2)(y)$!

We can formalize this interpolation theorem using communication complexity!

Instead, we use a generalization of communication complexity called real communication

In a real comm. protocol Alice and Bob receive bit strings, as usual — but communication is different!

Instead, there is a "referee", Alice and Bob send real numbers to the referee $\alpha(x), \beta(y) \in \mathbb{R}$, referee responds with 1 if $\alpha(x) \geq \beta(y)$, 0 if $\alpha(x) < \beta(y)$.

I won't say more! If you are interested see papers

[Hrubés - Pudlák 17] [Fleming - Pankratov - Pitassi - Robere 17]

We're going to prove the interpolation theorem directly.

<u>Defn</u> A real monotone circuit C computing $f: \{0,1\}^n \to \{0,1\}$ is given by a sequence of functions

$$g_1, g_2, \dots, g_s$$

such that

- $g_s = f$
- For each i, either $g_i = x_i$ for some $i \in [n]$, <u>or</u>

$$g_i = \varphi(g_j)$$

where $\varphi : \mathbb{R} \to \mathbb{R}$ is monotone, $j < i$

<u>or</u>

$$g_i = \varphi(g_j, g_k)$$

$\varphi : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ monotone, $j, k < i$.

<u>Thm</u> Let $F = A(x,y) \wedge B(x,z)$ be an unsatisfiable CNF formula such that every x variable occurs positively in A, then

$$S_{CP}(F) \geq \text{min size of any real monotone circuit computing } f_F$$

<u>Pf</u> Goal: give an algorithm computing f_F, given a CP proof Π of F.

Plan Go through Π, replace each inequality

$$a(x) + b(y) + c(z) \geq D$$

with two inequalities

$$b(y) \geq D_0 \qquad\qquad c(z) \geq D_1$$

s.t.

$$D_0 + D_1 \geq D - a(\alpha)$$

for any input $\alpha \in \{0,1\}^n$, assigned to x-vars.

If we can do this then we are done! The last inequality is

$$0 \geq 1$$

will be replaced with

$$0 \geq D_0 \qquad\qquad 0 \geq D_1$$

by assumption, $D_0 + D_1 \geq 1$. But both D_0 and D_1 are integers! So one of D_0, D_1 is ≥ 1!

Let's describe the "splitting" procedure

Axioms

Each axiom comes from $A(x,y)$ or $B(x,z)$. So: given $\alpha \in \{0,1\}^n$ assigned to x's, the inequalities are already in the correct form!

ex) $$a(x) + b(y) \geq D$$

$$a(\alpha) + b(y) \geq D$$

So, set $D_0 := D - a(\alpha)$!

$$b(y) \geq D_0 = D - a(\alpha). \qquad 0 \geq 0$$

Linear Combination

(Note: The notes on the next page have been edited since lecture)

Let's suppose the inequality I is obtained by taking a non-negative linear combo of

$I_1 = a_1(x) + b_1(y) + c_1(z) \geq G_1$, $I_2 = a_2(x) + b_2(y) + c_2(z) \geq G_2$

Induction, I_1 and I_2 can be split into

I_1	I_2
$b(y) \geq D$	$b'(y) \geq D'$
$c(z) \geq E$	$c'(z) \geq E'$

So $I = rI_1 + sI_2$, where $r, s \in \mathbb{Z}$, $r, s \geq 0$.

Split I by defining

$$r b(y) + s b'(y) \geq rD + sD'$$

$$r c(z) + s c'(z) \geq rE + sE'$$

Observe that

$$rD + sD' + rE + sE'$$

$$= r(D + E) + s(D' + E')$$

By induction we have

$$D + E \geq G_1 - a_1(\alpha) \qquad D' + E' \geq G_2 - a_2(\alpha)$$

The RHS of $I = rI_1 + sI_2$ is $rG_1 + sG_2$, so

$$r(D + E) + s(D' + E') \geq r(G_1 - a_1(\alpha)) + s(G_2 - a_2(\alpha))$$

as desired.

Rounding Rule

Oct 14

Consider I obtained by dividing and rounding I'.

$$I' := a(x) + b(y) + c(z) \geq D$$

and

$$I := \frac{1}{d}\left(a(x) + b(y) + c(z)\right) \geq \left\lceil \frac{D}{d} \right\rceil$$

Splitting I' by induction:

$$b(y) \geq D_0 \longrightarrow \frac{1}{d} b(y) \geq \left\lceil \frac{D_0}{d} \right\rceil$$

$$c(z) \geq D_1 \longrightarrow \frac{1}{d} c(z) \geq \left\lceil \frac{D_1}{d} \right\rceil$$

apply division by d in parallel!

WTS that $\left\lceil \frac{D_0}{d} \right\rceil + \left\lceil \frac{D_1}{d} \right\rceil \geq \left\lceil \frac{D}{d} \right\rceil - \frac{a(\alpha)}{d}$

$$\left\lceil \frac{D_0}{d} \right\rceil + \left\lceil \frac{D_1}{d} \right\rceil \geq \left\lceil \frac{D_0 + D_1}{d} \right\rceil$$

$$(\text{induction}) \geq \left\lceil \frac{D - a(\alpha)}{d} \right\rceil = \left\lceil \frac{D}{d} \right\rceil - \frac{a(\alpha)}{d} \quad \checkmark$$

Algorithm: Given F and $\alpha \in \{0,1\}^n$ to x-variables and CP proof of F

- Plug in α to all lines of the proof
- Inductively split every line of the proof, by above arguments
- Examine $0 \geq D_0$, $0 \geq D_1$. If $D_0 = 0$ then output 1.

Still have to implement this by a monotone real circuit! All we need to do is calculate D_0, and then apply a threshold.

This can be done inductively using (monotone, real) gates for

- addition
- multiplication by a non-neg. #
- division by a positive #
- rounding.

By a straightforward translation of the above algorithm the proof is complete.

$\square$

To apply this theorem, we use known size lower bounds for real monotone circuits.

Thm [Raz 85]

Let f be any monotone function on $\binom{n}{2}$ variables (i.e. input encodes a graph) s.t.

$f(x) = 1$ if x contains a k-clique

$f(x) = 0$ if x contains a $(k-1)$-colorable graph.

Then any monotone circuit computing f requires $n^{\Omega(k)}$ size.

Note: If we could prove the same theorem for non-monotone circuits, then $P \neq NP$!

Thm [Pudlák 97]

The $n^{\Omega(k)}$ size lower bound for clique holds for real monotone circuits!

Now: Pick $F = \text{Clique}(x, y) \wedge \text{Colour}(x, z)$ from last class!

Any interpolant f_F will compute the function in the previous theorems!

$\therefore$ Cor Cutting Planes proofs of

$$F = \text{Clique}_n^k(x, y) \wedge \text{Colour}_n^k(x, z)$$

require $n^{\Omega(k)}$ size. $\square$

Proofs of ckt lbs in [Pudlák 97] - possible presentation topic!

Next: Algebraic proof systems!