Lecture 11 Feasible Interpolation Oct 8

Goal: Prove size lower bounds for Cutting Planes proofs

Considering "split" unsatisfiable CNF formulas

$$F = A(x,y) \wedge B(x,z)$$

"partial"

Associated "interpolation function" $f_F : \{0,1\}^n \to \{0,1,*\}$

$$f_F(x) = \begin{cases} 1 & \exists y : A(x,y) = 1 \\ 0 & \exists z : B(x,z) = 1 \\ * & \text{o/w} \end{cases}$$

Note: Because of variable partitioning, f_F is a well-defined (partial) function.

Complexity of refuting F ~ complexity of computing f_F.

Do this by considering associated search problems

Search(F) := Given assignment, output false clause

For $f : \{0,1\}^n \to \{0,1,*\}$

Karchmer-Wigderson (KW) Game

$KW(f)$:= Two inputs: $x \in f^{-1}(1)$, $y \in f^{-1}(0)$. Goal: find an $i \in [n]$ s.t. $x_i \neq y_i$.

$$\begin{tikzcd} \text{Proof for } F \arrow[d, shift right] & & \text{Small circuit for } f_F \arrow[d, shift left] \\ \text{Prover Strategy Search}(F) \arrow[u, shift right] \arrow[rr, "(*)"] & & \text{Protocol for } KW(f_F) \arrow[u, shift left, "(\#)"] \arrow[ll, bend left, "\times"] \end{tikzcd}$$

Today: Prove two theorems

Oct 8

Thm 1 (*) For any unsat CNF formula $F = A(x,y) \wedge B(x,z)$

$$D_{Res}(F) \geq \text{Communication Complexity of } KW(f_F)$$
$$CC(KW(f_F))$$

If all occurrences of the x variables in $A(x,y)$ are positive then

$$D_{Res}(F) \geq CC(mKW(f_F))$$

Key to proving good lower bounds via this technique.

Aside: $mKW(f_F)$?

If $f: \{0,1\}^n \to \{0,1,*\}$ is a monotone function,
i.e.
if there exists a 0-1 assignment to all $*$s s.t.

if $x_i \leq y_i$ for all i $\quad f(x) \leq f(y)$

then define

mKW(f): Given $x \in f^{-1}(1), y \in f^{-1}(0)$, find $i \in [n]$
s.t. $x_i = 1$ and $y_i = 0$.

ex) $f: \{0,1\}^n \to \{0,1\}$ and monotone,

can't happen

$x \in f^{-1}(1), y \in f^{-1}(0)$ s.t. $\forall i: x_i = 1$ then $y_i = 1$
$\Rightarrow x_i \leq y_i$

$\Rightarrow \underset{1}{\underset{\shortparallel}{f(x)}} \leq \underset{0}{\underset{\shortparallel}{f(y)}}$ cont!

Thm 2 (#) For any partial function Oct 8

$f: \{0,1\}^n \to \{0,1,*\}$,

$$CC(KW(f)) = \text{min depth of any boolean circuit computing } f$$

If f is monotone

$$CC(mKW(f)) = \text{min depth of any monotone boolean ckt computing } f$$

NO NOT GATES, only $\wedge, \vee$

Thm 1 (#) For any unsat CNF formula $F = A(x,y) \wedge B(x,z)$

$$D_{Res}(F) \geq \text{Communication Complexity of } KW(f_F)$$
$$CC(KW(f_F))$$

Proof of Thm 1

Let π be any resolution proof of F. We give a comm. protocol for $KW(f_F)$ with complexity at most the depth of π.

Alice gets $u \in f_F^{-1}(1)$, $f(u)=1 \Leftrightarrow A(u,y)$ is satisfiable.

Alice picks any q^u s.t. $A(u,q^u)=1$.

Bob gets $v \in f_F^{-1}(0)$, $f(v)=0 \Leftrightarrow B(v,z)$ is sat.

$\therefore$ Bob picks r^v s.t. $B(v,r^v)=1$.

Goal: Find $i \in [n]$ s.t. $u_i \neq v_i$.

Alice and Bob walk down Π from the root clause, $\bot$, maintain the following invariant:

(*) Both assignments $(\overset{x}{u}, \overset{y}{q^u}, \overset{z}{r^v}), (\overset{x}{v}, \overset{y}{q^u}, \overset{z}{r^v})$ falsify the current clause.

Initially, they're at $\bot$, so (*) holds!

Next, suppose $\dfrac{C \vee w \qquad \bar{w} \vee D}{C \vee D}$ they are at clause $C \vee D$

derived from $C \vee w$, $\bar{w} \vee D$.

(1) If w is a y-variable (in $A(x,y)$), let $w = y_i$. Alice sends q^u_i to Bob, they go to whatever input clause is false.

(2) If w is a z-variable (in $B(x,z)$), let $w = z_i$, now Bob speaks! (symmetric)

(3) If w is an x-var, let $w = x_i$.

Bob sends v_i to Alice — if $u_i \neq v_i$ then done! If $u_i = v_i$, then they both go to the input clause to this step that is falsified.

Eventually they end at a leaf, clause from $A(x,y)$ or $B(x,z)$. We know that

(u, q^u, r^v) satisfies A,
(v, q^u, r^v) satisfies B.

Thus $A \wedge B$ find an i w/ $u_i \neq v_i$, communicate $\leq$ depth(π) bits $\square$

If all occurrences of x-vars in $A(x,y)$ are positive, then we modify the invariant and (3).

Oct 8

(*) Both assignments $(\overset{x}{u}, \overset{y}{q^u}, \overset{z}{r^v}), (\overset{x}{v}, \overset{y}{q^u}, \overset{z}{r^v})$ falsify the current clause.

New (*): $\exists u' \geq u$ s.t. $(u', q^u, r^v), (v, q^u, r^v)$
pointwise ↗ both falsify the current clause.

New Goal: Find $i \in [n]$ s.t. $u_i = 1, v_i = 0$.

Modify (3) as follows:

New (3) $w = x_i$ for some i. Bob sends v_i to Alice.

- If $u_i = 1, v_i = 0$ then halt, output i.
- If $u_i \leq v_i$, then they go to child falsified by v_i.

  If $u_i = v_i$, then no change!

  If $u_i = 0, v_i = 1$, then set $u_i' = 1$, and New (*) is satisfied.

Thm 2 (*) For any partial function $f: \{0,1\}^n \to \{0,1,*\}$, Oct 8

$$CC(KW(f)) = \text{min depth of any boolean circuit computing } f$$

If f is monotone

$$CC(mKW(f)) = \text{min depth of any monotone boolean ckt computing } f$$

NO NOT GATES, only $\wedge, \vee$

Pf of Thm 2

($\leq$) $CC(KW(f)) \leq$ circuit depth of f

Alice gets $u \in f^{-1}(1)$, Bob gets $v \in f^{-1}(0)$

They both (privately) evaluate the circuit C on u and v.

Start at output gate of the circuit C, walk to input variable x_i while maintaining that the current gate g satisfies

$$g(u) \neq g(v).$$

At output gate, $C(u) = f(u) = 1$, $C(v) = f(v) = 0$. ✓

- If $g = h_i \wedge h_j$

$g(u) = 1 \Rightarrow h_i(u) = 1$ and $h_j(u) = 1$

$g(v) = 0 \Rightarrow$ one of $h_i(v), h_j(v) = 0$

So Bob sends the i s.t. $h_i(v) = 0$

- If $g = h_i \vee h_j$

$g(u) = 1 \Rightarrow h_i(u) = 1$ or $h_j(u) = 1$

$g(v) = 0 \Rightarrow h_i(v) = h_j(v) = 0$.

So Alice sends i s.t. $h_i(u) = 1$.

Eventually: they reach an input variable x_i, and by assumption $u_i \neq v_i$.

($\geq$) $CC(KW(f)) \geq$ circuit depth of f.

Short version: Given protocol Π, create boolean ckt for f.

Relabel Alice nodes in Π with $\vee$, Bob nodes with $\wedge$, and leaves where they output x_i, $\overline{x_i}$ with the corresponding variable.

Prove slightly stronger statement:

($\square$) For any $U \subseteq f^{-1}(1)$, $V \subseteq f^{-1}(0)$ let

$$f_{U,V}(x) = \begin{cases} 1 & x \in U \\ 0 & x \in V \\ * & o/w \end{cases}$$

C computes f_{UV}

Then CC of the game for $f_{UV} \geq$ circuit depth of f_{UV}

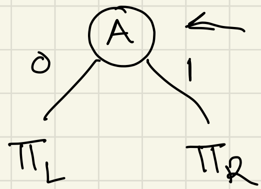
Pf Induction on $d :=$ communication complexity.

Oct 8

If $d=0$, then Alice and Bob know an index i that is different. The circuit is x_i or $\overline{x_i}$.

O/w at depth d: Suppose Alice speaks first

Alice looks at $u \in \mathcal{U}$ and decides what bit to send.



$\leftarrow$ Protocol correct $\mathcal{U} \times \mathcal{V}$

$\mathcal{U}_0 \times \mathcal{V}$ $\quad$ $\mathcal{U}_1 \times \mathcal{V}$ $\quad$ $\mathcal{U} = \mathcal{U}_0 \oplus \mathcal{U}_1$

$\mathcal{U}_0 = \{u : \text{Alice sends } b\}$

Inductively convert Π_L, Π_R to circuits C_L, C_R.
Set

$$C = C_L \vee C_R.$$

$C_L(u) = 1$ if $u \in \mathcal{U}_0$ $\qquad$ $C_R(u) = 1$ if $u \in \mathcal{U}_1$

So on $\mathcal{U}_0 \cup \mathcal{U}_1$ $\qquad$ $C(u) = C_L(u) \vee C_R(u) = 1$

If $C_L(v) = 0$ if $v \in V$ $\qquad$ $C_R(v) = 0$ if $v \in V$

So $\quad C(v) = C_L(v) \vee C_R(v) = 0.$

AND C is correct!

Bob's speaks is a symmetric argument (switch $\wedge$ and $\vee$).

$\square$