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

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

\[
\text{D}_{\text{Res}}(F) \geq CC(\text{kw}(f_F)) = \text{min depth of boolean circuit for } f_F
\]

If all \( x \) vars occurred positively in \( A \), then

\[
\text{D}_{\text{Res}}(F) \geq CC(\text{mkw}(f_F)) = \text{min depth of a monotone boolean circuit for } f_F
\]

Today:

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

\[
\text{S}_{\text{cp}}(F) \geq \text{min size of any real monotone circuit computing } f_F
\]

“Real” monotone computation?
Regular monotone boolean circuits only allow \( \land \) (AND) and \( \lor \) (OR) gates to compute boolean functions.

Real monotone circuits allow any real function

\[
\psi : IR \rightarrow IR \quad \text{or} \quad \psi : IR \times IR \rightarrow IR
\]

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

\[ x_1, x_2, y_1, y_2 \in IR, \quad x_1 \leq x_2, \quad y_1 \leq y_2 \quad \text{then} \]

\[ \psi(x_1) \leq \psi(x_2), \quad \psi(x_1, y_1) \leq \psi(x_2, y_2). \]

Consider \( \text{MAj}_3 : \{0,1\}^3 \rightarrow \{0,1\} \)

\[
\text{MAj}_3(x) = 1 \quad \text{iff} \quad \exists \text{ 2 input bits are 1.}
\]

**Monotone Boolean Ckt**

**Real Monotone Ckt**

\[
\begin{array}{c@{\quad}c}
\text{x = 110} & \text{\( \geq 2 \)} \quad \text{output 1 if input is} \quad \text{\( \geq 2 \), 0 o/w.}
\end{array}
\]

**Monotone in it's input if** \( x \leq y \) **then** \( \geq 2(x) \leq \geq 2(y) \)!
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 \(d(x), \beta(y) \in \mathbb{R}\), referee responds with 1 if \(d(x) \geq \beta(y)\), 0 if \(d(x) < \beta(y)\).

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

[Iturbes- Pudlak 17] [Fleming- Pankratov- Pitassi- Robere 17]

We're going to prove the interpolation theorem directly.

**Defn** A real monotone circuit \(C\) computing \(f \colon \{0,1\}^n \to \{0,1\}\) is given by a sequence of functions

\[ g_1, g_2, \ldots, g_s \]

such that

- \(g_s = f\)
- For each \(i\), either \(g_i = x_i\) for some \(i \in [n]\), or \(g_i = \varphi(g_{i^+})\)
where \( \psi : \mathbb{R} \to \mathbb{R} \) is monotone, \( j < i \)

or

\[
\begin{align*}
g_j^i &= \psi(g_j, g_k) \\
\psi : \mathbb{R} \times \mathbb{R} &\to \mathbb{R} \text{ monotone, } j, k < i.
\end{align*}
\]

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

\[
\text{Scp}(F) \geq \min \text{ size of any real monotone circuit computing } f_F
\]

**Pf** Goal: give an algorithm computing \( f_F \), given a CP proof \( \Pi \) of \( F \).

**Plan** Go through \( \Pi \), replace each inequality

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

with two inequalities

\[
b(y) \geq D_0 \quad \quad c(z) \geq D_1
\]

s.t.

\[
D_0 + D_1 \geq D - a(x)
\]

for any input \( x \in \{0, 1\}^n \), assigned to \( x \)-vars.
If we can do this then we are done! The last inequality is

\[ 0 \geq 1 \]

will be replaced with

\[ 0 \geq D_0 \quad 0 \geq D_1 \]

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 \( \geq 1 \).

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!

\[ \text{ex} \quad a(x) + b(y) \geq 0 \]

\[ a(\alpha) + b(y) \geq 0 \]

So, set \( D_0 := 0 - a(\alpha) \)

\[ b(y) \geq D_0 = 0 - a(\alpha). \quad 0 \geq 0 \]

**Linear Combination**

Let’s suppose the inequality \( I \) is obtained by taking a non-negative linear combo of

(Note: The notes on the next page have been edited since lecture)
\[ I_1 = a_1(x) + b_1(y) + c_1(z) \geq G_1, \quad I_2 = a_2(x) + b_2(y) + c_2(z) \geq G_2 \]

Induction, \( I_1 \) and \( I_2 \) can be split into

\[
\begin{align*}
I_1 & & I_2 \\
b(y) & \geq 0 & b'(y) & \geq D' \\
c(z) & \geq E & c'(z) & \geq E'
\end{align*}
\]

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

Split \( I \) by defining

\[
\begin{align*}
r b(y) + s b'(y) & \geq rD + sD' \\
r c(z) + s c'(z) & \geq rE + sE'
\end{align*}
\]

Observe that

\[
rD + sD' + rE + sE' \\
= r(D+E) + s(D'E')
\]

By induction we have

\[
D + E \geq G_1 - a_1(x) \quad D' + E' \geq G_2 - a_2(x)
\]

The RHS of \( I = rI_1 + sI_2 \) is \( rG_1 + sG_2 \), so

\[
r(D+E) + s(D'+E') \geq r(G_1 - a_1(x)) + s(G_2 - a_2(x))
\]

as desired.
Rounding Rule

Consider $I$ obtained by dividing and rounding $I'$.

\[
I' := a(x) + b(y) + c(z) \geq 0
\]

and

\[
I := \frac{1}{d} (a(x) + b(y) + c(z)) \geq \left\lfloor \frac{D}{d} \right\rfloor
\]

Splitting $I'$ by induction:

\[
b(y) \geq D_0 \quad \rightarrow \quad \frac{1}{d} b(y) \geq \left\lfloor \frac{D_0}{d} \right\rfloor
\]

\[
c(z) \geq D_1 \quad \rightarrow \quad \frac{1}{d} c(z) \geq \left\lfloor \frac{D_1}{d} \right\rfloor
\]

apply division by $d$ in parallel!

WTS that $\left\lfloor \frac{D_0}{d} \right\rfloor + \left\lfloor \frac{D_1}{d} \right\rfloor \geq \left\lfloor \frac{D}{d} \right\rfloor - \frac{a(x)}{d}

\[
\left\lfloor \frac{D_0}{d} \right\rfloor + \left\lfloor \frac{D_1}{d} \right\rfloor \geq \left\lfloor \frac{D_0 + D_1}{d} \right\rfloor
\]

(induction) $\Rightarrow \left\lfloor \frac{D - a(x)}{d} \right\rfloor = \left\lfloor \frac{D}{d} \right\rfloor - \frac{a(x)}{d}$
Algorithm: Given $F$ and $d_{0,1}^n$ to $x$-variables and CP proof of $F$

- Plug in $d$ to all lines of the proof
- Inductively split every line of the proof, by above arguments
- Examine $O \geq D_0$, $O \geq D_1$. 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.

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

**Thm** [Raz 85]

Let $f$ be any monotone function on $(2^i)$ 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
\( \Omega(k) \) 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 \( F = \text{Clique}(x, y) \land \text{Colour}(x, z) \) from last class!

Any interpolant \( f_F \) will compute the function in the previous theorems!

Cor: Cutting Planes proofs of
\[ F = \text{Clique}^k_n(x, y) \land \text{Colour}^k_n(x, z) \]
require \( n \Omega(k) \) size.

Proofs of ckt lbs in [Pudlák 97] - possible presentation topic!
Next: Algebraic proof systems!