# CSE 599S Proof Complexity & Applications

**Lecture 16:** 25 Nov 2020

## Interpolation

Craig's Interpolation Theorem

$\phi$ vars $x, y$
$\psi$ vars $x, z$ $\Rightarrow$ $\exists\ \theta$ in vars $x$ s.t.
$\phi \to \psi$ $\qquad \phi \to \theta \to \psi$

---

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

$F$ unsat $\Rightarrow$ on any input $x = \vec{\alpha}$ either $A(\vec{\alpha}, y)$ or $B(\vec{\alpha}, z)$ is unsat.

We say that any function

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

is an <u>interpolant</u> for $F$

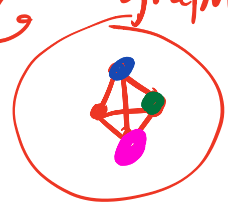
why is it an interpolant like Craig's Thm

"$F$ unsat" $\equiv$ $A(x,y) \to \neg B(x,z)$

By defn $\quad A(x,y) \to C(x)$
$\qquad\qquad C(x) \to \neg B(x,z)$

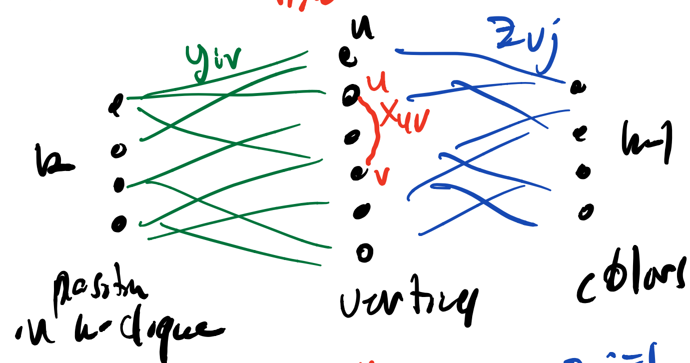
ex Formulas of this form:

$G$ a graph



if $G$ has a $k$-clique $]\ A$
then it doesn't have a $(k-1)$-coloring. $]\ \neg B$

CLIQUE-COLOR$_{n,k}$




$y_{iv}=1$ iff if $v$ is $i^{th}$ vertex in a k-clique

$\binom{n}{2}$ vars $x_{uv}$ edges of graph

$z_{vj}=1$ iff color of $v$ is $j$

$A(x,y)$ • $y_{i1} \vee \cdots \vee y_{in}$ $\forall i \in [k]$

x is positive • $\bar{y}_{iu} \vee \bar{y}_{i'v} \vee x_{uv}$ $i \neq i'$, $u \neq v$

$\boxed{\bullet\ \bar{y}_{iu} \vee \bar{y}_{iv}}$ not necessary $i$, $u \neq v$

$B(x,z)$ • $z_{u1} \vee z_{u2} \vee \cdots z_{uk-1}$ $\forall u \in [n]$

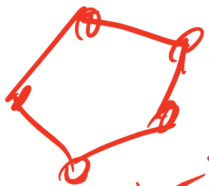
x is negative • $\bar{z}_{uj} \vee \bar{z}_{vj} \vee \bar{x}_{uv}$ $u \neq v$, $j$

$\boxed{\bullet\ \bar{z}_{uj} \vee \bar{z}_{uj'} \quad u,\ j \neq j'}$ not necessary

unsat because $PHP^{k}_{k-1}$ is unsat.

# Interpolant for Clique-Color

$$C(x) = \begin{cases} 1 & \text{if graph given by } x \text{ has a } k\text{-clique} \\ 0 & \text{if graph is } (k-1)\text{-colorable} \\ * & \end{cases}$$



$k=3$

---

We will show that proofs systems Resolution, Cutting Planes have a form of feasible interpolation

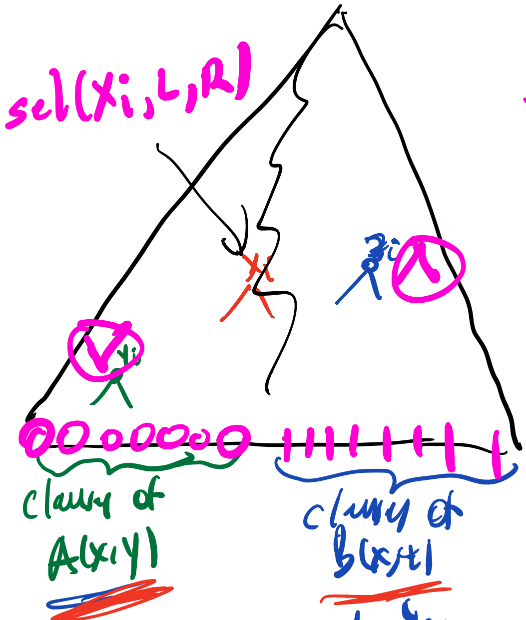
small refutation of $F = A(x,y) \wedge B(x,z)$ $\Rightarrow$ small circuit for interpolant of $F$

---

**Thm** Let $F(x,y,z) = A(x,y) \wedge B(x,z)$ UNSAT

- If $F$ has a resolution refutation of size $\le S$ $\Rightarrow$ circuit of size $\le 4S$ computing some interpolant for $F$.
- Further if $x$ occurs only positively in $A$ then circuit is <u>monotone</u> (only $\wedge, \vee$ gates, no $\neg$ gates).

**Proof** Consider a resolution refutation of $F$



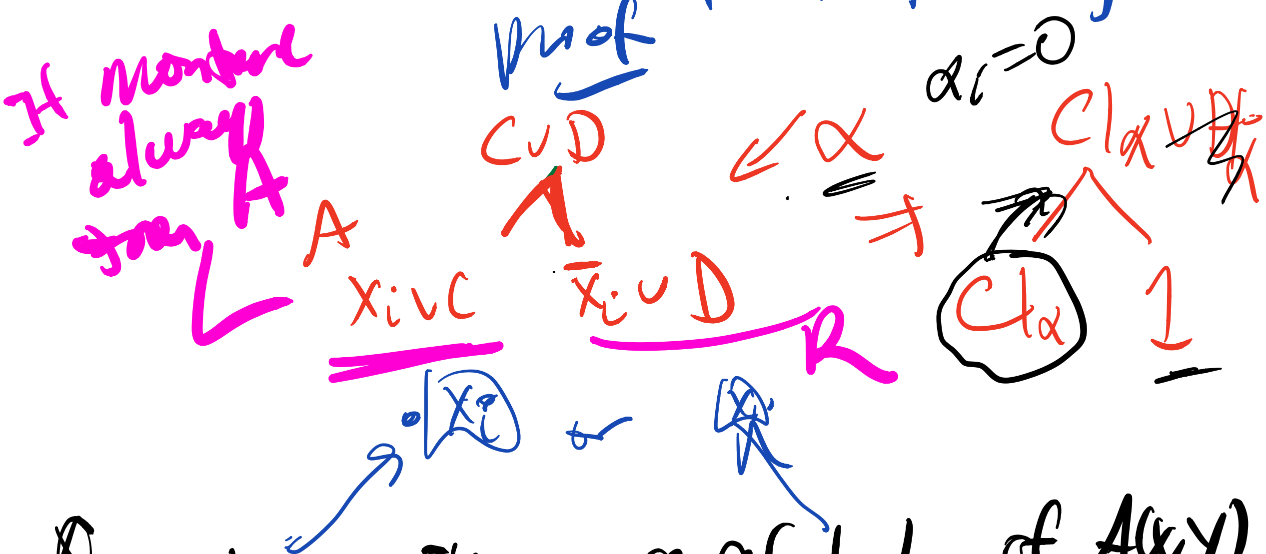

$$\mathrm{sel}(x_i, L, R) = \begin{cases} L & \text{if } x_i = 0 \\ R & \text{if } x_i = 1 \end{cases}$$

$$(x_i \wedge R) \vee (\neg x_i \wedge L)$$

**Claim** This circuit computes an interpolant.

Consider some assignment $\alpha$ to $x$ and how $\alpha$ affects the original proof

$\alpha_i = 0$




⊗ result is either a refutation of $A(x,y)$ or of $B(x,z)$

If proof is a refutation of $B(x,z)$

output is 1 ✓

if proof is a refutation of $A(x,y)$

output is 0 ✓

This meets conditions for interpolant $I$

If $x$ only occurs positively in $A$

replace $sel(x_\varepsilon, L, R)$

by

monotone $(x_i \vee L) \wedge R$

$\uparrow$ 0  $\uparrow$ 0

Thm (Razborov, Alon-Boppana) Any monotone real circuit computing such a function $C$ for $\text{CLIQUECOLOR}_{n,k}$ has size $2^{\Omega(\sqrt{k})}$ where $k$ is $O((n/\log n)^{2/3})$

Pudlak

Cor $\text{CLIQUE-COLOR}$ needs $2^{n^{\Omega(1)}}$ size resolution proofs. ∎

Thm $F = A(x,y) \wedge B(x,z)$ UNSAT, $x$ occurs only positively in $A$

CP refutation of size $S$ $\Rightarrow$ $\exists$ monotone real circuit of size $S + |F| \cdot w(F)$ computing interpolant $C$ for $F$.

all gates fanin $\leq 2$

pairs real # values

$g(a_1, a_2)$

$g(a,b) \geq g(a',b')$ if $a \geq a'$, $b \geq b'$

$g(a) \geq g(a')$ if $a \geq a'$

Proof Idea same as resolution
split each line into two parts
given assignment $x \leftarrow \alpha$

Generic proof line of form

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

$\alpha$:

$b(y) \geq D_0$ $\quad$ $c(z) \geq D_1$ $\quad$ $B(x,z)|_\alpha$

derived from $A(x,y)|_\alpha$ s.t. $D_0 + D_1 \geq D - a(\alpha)$

At end $1 \geq 0$ $\quad$ $b(y)$, $c(z)$ empty $a(\alpha) = 0$

split is $0 \geq D_0$, $0 \geq D_1$

$D_0 + D_1 \geq 1$

either $D_0 \geq 1$ or $D_1 \geq 1$

Inputs $A(x,y)$: $\quad a(x) + b(y) \geq D$

Left $\quad b(y) \geq \underbrace{D - a(\alpha)}_{D_0}$

Right $\quad 0 \geq \underbrace{0}_{D_1}$

$B(x, z)$ Similar —

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

$$\underbrace{0 \geq 0}_{D_0} \qquad \underbrace{\boxed{c(z) \geq D - a(x)}}_{\text{Right}} \quad D_1$$

Rules

- $$\frac{l \geq D}{l' = k l \geq \underbrace{k D}_{D_0', D_1'}} \quad \rightarrow D_0, D_1 \qquad k > 0$$

  $D_0' = k \cdot D_0$

  $D_1' = k \cdot D_1$

- $$\frac{l \geq D, \; m \geq D'}{l_1 + l_2 \geq D + D'}$$

add the $D_0$ and $D_1$ to get the new ones

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

$$\Rightarrow \quad a(x) + b(y) + c(z) \geq \left\lceil \frac{D}{K} \right\rceil$$

$$K \geq 0$$

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

$$D_0 + D_1 \geq D - K\cdot a(x)$$

cp.

$$b(y) \geq \underbrace{\left\lceil \frac{D_0}{K} \right\rceil}_{D_0'} \qquad c(z) \geq \underbrace{\left\lceil \frac{D_1}{K} \right\rceil}_{D_1'}$$

$$D_0' + D_1' = \left\lceil \frac{D_0}{K} \right\rceil + \left\lceil \frac{D_1}{K} \right\rceil \geq \left\lceil \frac{D_0 + D_1}{K} \right\rceil$$

$$= \left\lceil \frac{D - K\,a(\alpha)}{K} \right\rceil$$

$$= \left\lceil \frac{D}{K} - a(\alpha) \right\rceil$$

$$= \left\lceil \frac{D}{K} \right\rceil - a(\alpha)$$

result is ac correct towards of both sides of split

circuit figures whether for last line $D_0 \geq 1$

or $D_1 \geq 1$

It will just compute ( for each split line

$-D_0$

as a function
of $\alpha$

each equate

Note: Can
apply this to
arbitrary formula
of clause length
$\Theta(\log n)$

For arbitrary formulas
eg. Random $\Theta(\log n)$-CNFs?

For any split vars into $Y \cup Z$
disjoint

$F = m$ clauses

$$C_i = C_i^Y \vee C_i^Z$$

add $m$ $X$ vars

$$\underbrace{C_i}_{F} \longmapsto \underbrace{\underbrace{(C_i^Y \vee x_i)}_{A}\ \underbrace{(C_i^Z \vee \bar{x}_i)}_{B}}_{F^{Y,Z}}$$

$F^{Y,Z} \to F$
easy.

Prove $F^{Y,Z}$ is hard for some $Y, Z$
partitioning of vars

use interpolation technique

$2n$ $\quad \dfrac{n}{Y} \quad \dfrac{n}{Z}$