Lecture 3 More on Resolution!

Sep 10

$F :=$ unsatisfiable CNF formula

$= C_1 \wedge C_2 \wedge \cdots \wedge C_m$, each C_i is a <u>clause</u> (OR of lits)

Resolution Refutation of F is a list of clauses

$\underbrace{D_1, \ldots, D_m}_{F}, \underbrace{D_{m+1}, \ldots, D_s}$ $= \bot$ ← empty clause

All other clauses are obtained from earlier clauses by the resolution rule

$$\frac{A \vee x \qquad B \vee \bar{x}}{A \vee B} \qquad (\nexists y : y \in A,\ \bar{y} \in B)$$

ex) $x_1 \wedge (\bar{x}_1 \vee x_2) \wedge (\bar{x}_2 \vee x_3) \wedge \bar{x}_3$

$$\frac{\dfrac{x_1 \qquad \bar{x}_1 \vee x_2}{x_2} \qquad \dfrac{\bar{x}_2 \vee x_3 \qquad \bar{x}_3}{\bar{x}_2}}{\bot}$$

<u>Defn</u> A resolution refutation is tree-like if the graph underlying the refutation is a tree.

(i.e. every derived clause is used at most once.)

- Tree-like resolution can be exponentially weaker than general resolution, but, it is still complete.

Complexity Measures of Refutations

Sep 10

$F :=$ unsat CNF, on n variables

$S_{Res}(F) :=$ min # of clauses in any resolution ref. of F ("size")

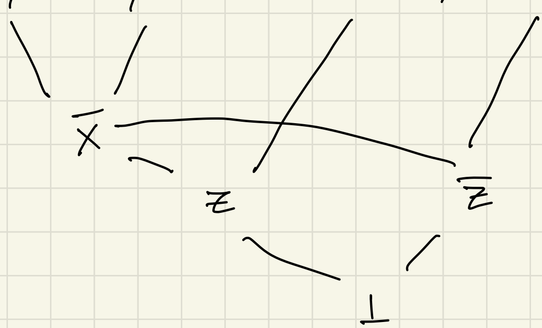
$S^{T}_{Res}(F) :=$ ———————— tree-like res. ref of F

$D_{Res}(F) :=$ min depth of any resolution ref. of F

ex) DAG likeproof

$w(F) = 2$

$F = y \wedge (\bar{y} \vee \bar{x}) \wedge (x \vee z) \wedge (x \vee \bar{z})$



$w(F) :=$ $\underbrace{\text{width}}_{\#\text{ of lits}}$ of the largest clause in F

$w_{Res}(F) :=$ minimum width of any resolution refutation of F.

Assumes F is minimally unsat, i.e. if we delete a clause it is SAT (safe assumption)

- $w(F) \le w_{Res}(F) \le D_{Res}(F) \le n$
- $S_{Res}(F) \le S^{T}_{Res}(F) \le 2^{D_{Res}(F)(\pm 1)}$
  - $S_{Res}(F) \le |\{\#\text{ of clauses of width} \le w_{Res}(F)\}|$

$$\leq \sum_{i=0}^{w} 2^i \binom{n}{i} \approx n^{O(w_{Res}(F))}$$

In particular, if $w_{Res}(F) = O(1)$ then F has a polynomial-size proof!

<u>Thm</u> [Haken 85] Any resolution refutation of PHP_n^{n+1} requires length $2^{\Omega(n)}$.

PHP_n^{n+1} = defined on $(n+1)n$ variables

$$x_{ij} \qquad i \in [n+1], j \in [n]$$

$$x_{ij} = 1 \iff \text{Pigeon } i \text{ mapped to hole } j$$

<u>Clauses:</u> $\bigvee_{j=1}^{n} x_{ij}$ for all $i \in [n+1]$

$\overline{x_{ij}} \vee \overline{x_{kj}}$ for all $i \neq k \in [n+1]$, $j \in [n]$.

<u>Proof</u> Two steps

(1) Any "proof" of PHP_n^{n+1} requires a wide clause $\geq \Omega(n^2)$

(2) There is a partial restriction $\rho \in \{0,1,*\}^{(n+1)n}$ such that

- $\underbrace{PHP_n^{n+1} \restriction \rho}_{\text{restricted}} = PHP_m^{m+1}$

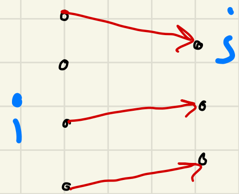
$C \restriction \rho$:= plug ρ into

- <u>All</u> wide clauses will be satisfied by ρ in the proof.

Defn An assignment $\alpha \in \{0,1\}^{(n+1)n}$ is i-critical if the only clause falsified in PHP^{n+1}_n is

$$\bigvee_{j=1}^{n} x_{ij}$$

Sep 10



2-critical

Defn If C is a clause over x_{ij} vars, let C^+ be the clause obtained by replacing every negative literal $\overline{x_{ij}}$ with

$$\bigvee_{k \neq j} x_{ik}.$$

Let π be a resolution proof of PHP^{n+1}_n, let

$$\pi^+ = \{C^+ \mid C \in \pi\}. \qquad \text{"relativization"}$$

Claim π^+ contains a clause C^+ with $w(C^+) \geq \frac{n^2}{9}$.

Proof For any clause C, define

$$\text{Crit}(C) := \{ i \in [n+1] : C(\alpha) = 0 \text{ for an } i\text{-crit assign } \alpha \}$$

$$\mu(C) := |\text{Crit}(C)|$$

If C is a clause of PHP^{n+1}_n,

- $\mu(C) = 0$ if C is a "hole" clause
- $\mu(C) = 1$ if C is a "pigeon" clause

$\mu(C) \leq 1$

$\mu(\bot) = n+1$

If $A = Res(B, C)$ $\qquad \dfrac{B \quad C}{A}$

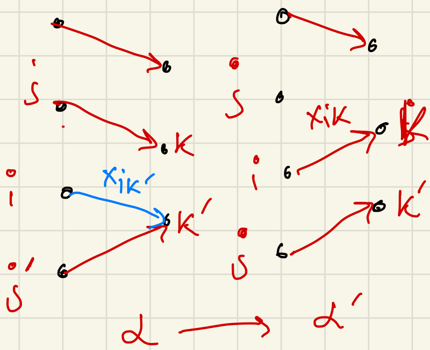
(*) $\mu(A) \leq \mu(B) + \mu(C)$

$A(\alpha) = 0$ for i-crit α, then either $B(\alpha) = 0$ or $C(\alpha) = 0$!

$\therefore$ Let C be any clause in the proof π with

$$\frac{n}{3} < \mu(C) \leq \frac{2n}{3} \quad \text{(uses subadditivity).}$$

Let $i \in Crit(C)$, $j \notin Crit(C)$.



Let α be i-crit, s.t. $C(\alpha) = 0$

Go from α to α' which is j-critical by setting

$x_{ik} = 1 \qquad x_{jk} = 0$

But $C(\alpha') = 1$ — so x_{ik} appears in C^+!

Apply the same argument to all $i \in Crit(C)$, $j \notin Crit(C)$ then

$$w(C^+) \geq \mu(C)(n - \mu(C)) \geq n^2/9. \qquad \square$$

Aside: example of CNF formula F with small resolution proofs but large tree-like resolution proofs?

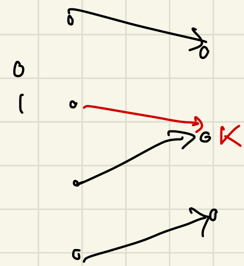
Answer: Q3 any Horn formula that is unsatisfiable has a polynomial-size Res. ref.

C^+ – obtained from C by replacing

$$\overline{x_{ij}} \longrightarrow \bigvee_{j \neq k} x_{ik}$$

<u>Fact</u> If α is a i-critical assignment for some i, then

$$C(\alpha) = C^+(\alpha)$$



$C(\alpha) = 1$ why is $C^+(\alpha) = 1$?

$C^+(\alpha) = 1$

$x_{ik} = 1 \in C^+$

↪ C contained $\overline{x_{ij}}$ for some $j \neq k$

α is i-critical $\Rightarrow$ i not mapped $(\overline{x_{ij}} = 1)$

or

j-critical $\Rightarrow$

Horn := every clause has ≤ 1 positive literal

e.g. $\overline{x_1} \vee \overline{x_2} \vee x_3 \to y_3 \oplus z_3$ $\qquad \overline{x_1} \vee \overline{x_4}$ $\qquad x_5$

$S^T_{Res}(F \circ XOR) \geq 2^{d_{Res}(F)}$.

Exercise: There is a Horn formula requiring large depth!

<u>Defn</u> If C is a clause over x_{ij} vars, let C^+ be the clause obtained by replacing every negative literal $\overline{x_{ij}}$ with

$$\bigvee_{k \neq j} x_{ik}.$$

Let Π be a resolution proof of PHP^{n+1}_n, let

$$\Pi^+ = \{C^+ \mid C \in \Pi\}.$$ "relativization"

<u>Claim</u> Π^+ contains a clause C^+ with $w(C^+) \geq \frac{n^2}{9}$.

Today: How do we kill all the wide clauses?

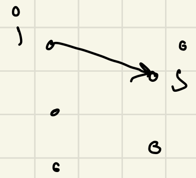
Notice all clauses C^+ are ORs of positive literals. So, restricting <u>any</u> variable in C^+ to 1 will kill the clause.

Say a clause C in the proof Π is <u>wide</u> if $w(C^+) \geq \varepsilon n^2$ (choose ε later).

Since every wide clause has an ε-fraction of the variables, by averaging there is some literal x_{ij}

occurring in $\geq \varepsilon S$ of the wide clauses (where S is the # of wide clauses).

- Pick x_{ij}, set $x_{ij} = 1$, set $x_{ik} = 0$ for all $k \neq j$.
- After this restriction we're left with PHP^{n}_{n-1}, and the restricted proof is a refutation of the new instance.



How many times until all wide clauses are gone?

- After d restrictions, we have $(1-\varepsilon)^d S$ wide clauses remaining. To kill all wide clauses, we need

$$(1-\varepsilon)^d S \leq e^{-d\varepsilon} S < 1.$$

$$\Rightarrow \ln S < d\varepsilon \iff \frac{\ln S}{\varepsilon} < d$$

Choose $d = \ln S / \varepsilon$. After d restrictions, we have a proof of of PHP^{n+1-d}_{n-d} with no wide clauses. By the Claim, there is a clause of width

$$\frac{(n-d)^2}{9} \geq \frac{(n - \ln S/\varepsilon)^2}{9}$$

So, if $(n-d)^2/9 \geq \varepsilon n^2$ we have a contradiction. Towards this, assume $S \leq e^{\frac{\varepsilon n}{4}}$, then

$$\frac{(n-d)^2}{9} \geq \frac{(n - n/4)^2}{9} = \frac{n^2}{16}$$

Then, if $\varepsilon < 1/16$ we have a contradiction. $\therefore$ $S \geq e^{\varepsilon n/4}$.

$\square$

Width-size tradeoffs [Ben-Sasson - Wigderson 01] Sep 16

Thm For any unsat CNF F, we have

(1) $S^{T}_{Res}(F) \geq 2^{w_{Res}(F) - w(F)}$

(2) $S_{Res}(F) \geq 2^{\frac{(w_{Res}(F) - w(F))^2}{16n}}$

"width gap is $\omega(\sqrt{n})$ then lower bds"

↳ cannot naively be applied to get PHP lower bds

Pf (1)

Prove by induction on b (integer parameter) and n (# vars) that if

$$S^{T}_{Res}(F) \leq 2^{b}$$

then $w_{Res}(F) \leq b + w(F)$.

Notation

$x^0 := \bar{x}$, $x^1 := x$

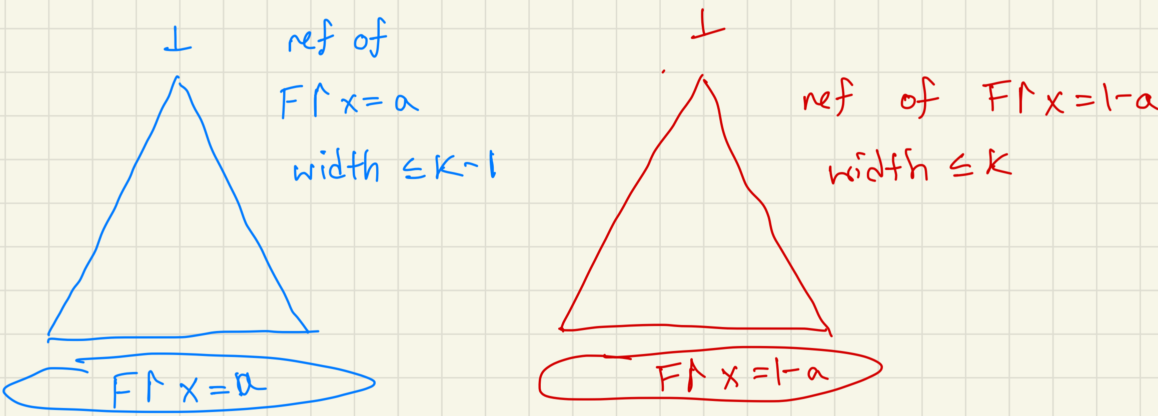
$F \restriction x=a$:= New CNF formula from F by substituting $a \in \{0,1\}$ for x.
So, if $C \in F$ contains x^a we remove C, if $x^{1-a} \in C$ we delete x^{1-a} from the clause.

Claim If $w_{Res}(F \restriction x=a) \leq k$ and

$w_{Res}(F \restriction x=1-a) \leq k-1$ then

$$w_{Res}(F) \leq \max\{k, w(F)\}.$$

Pf of Claim



For simplicity, we assume resolution has the weakening rule

$$\frac{C}{C \vee x} \quad \text{for any } x \notin C.$$

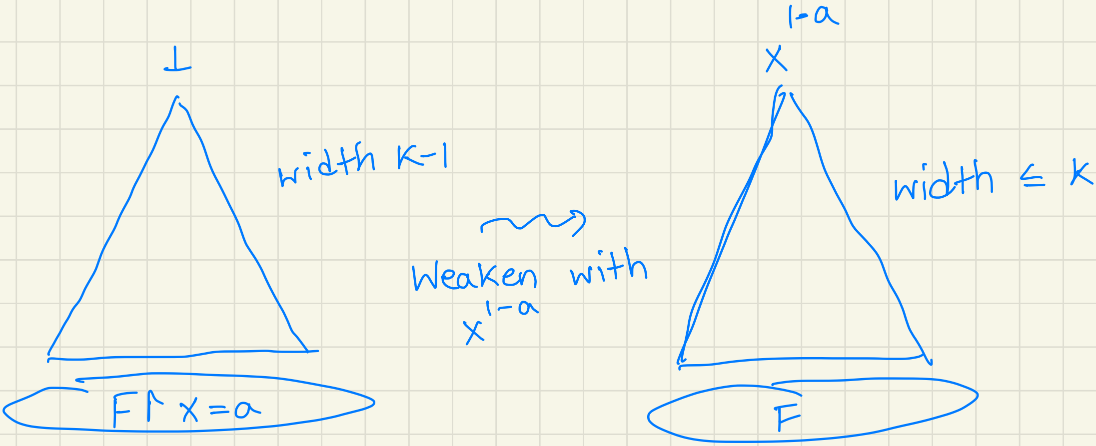
(Note: This just makes the proof cleaner and can be removed.)

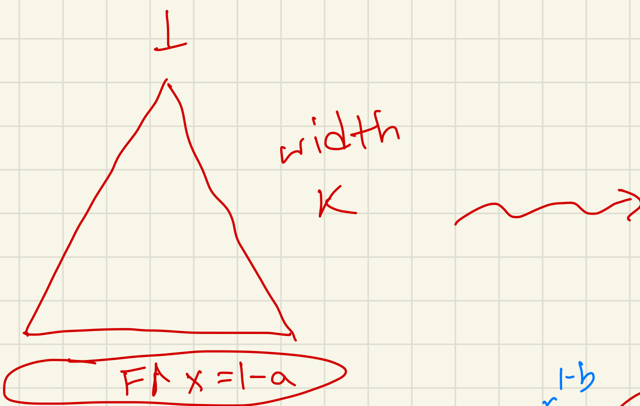
How to combine $\triangle$ and $\triangle$ into a refutation of F?

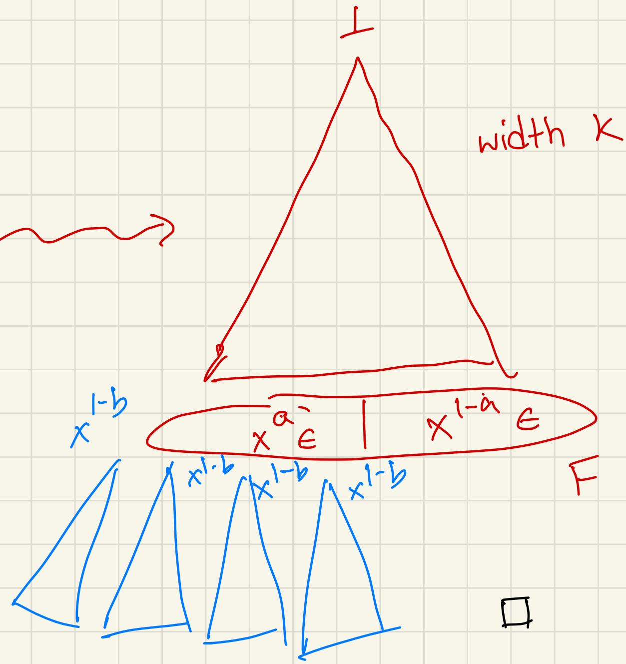
- Let Π_1 be the refutation of $F \upharpoonright x =$, in width $k-1$.
- Let Π_1' be obtained by adding x^{1-a} to every clause in Π_1.
  - Every clause at start of the proof of Π_1' is either a clause in F or a weakening of a clause in F.

$$\frac{x^{1-a} \vee A \vee x \qquad x^{1-a} \vee B \vee \overline{x}}{x^{1-a} \vee A \vee B}$$

- Observe adding x^{1-a} doesn't affect the correctness of any resolution step.







Now substitute the new proof to derive $F\restriction x=1-a$ from F.

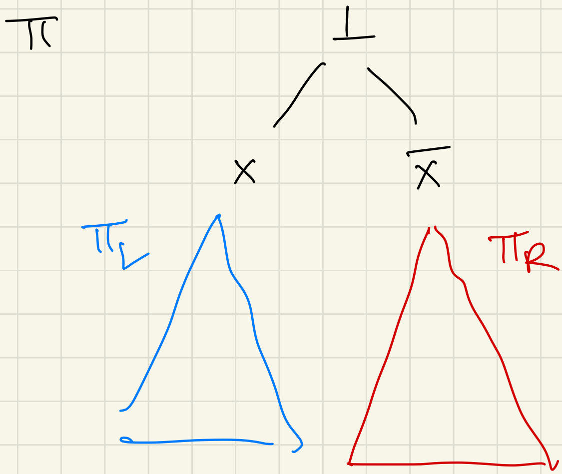
$\square$

(Almost) done!

Let Π be a proof of F, $|\Pi| \le 2^{b}$.

If $b=0$ then $|\Pi| = 1$, means $\bot \in F$ ✓

Otherwise: the last step of Π resolved two literals x and $\bar{x}$.



Size $\leq 2^b$

Assume wlog $|\Pi_L| \leq |\Pi_R|$, so $|\Pi_L| \leq \frac{|\Pi|}{2} \leq 2^{b-1}$.

- Induction on b for Π_L, we get a width $b-1$ proof of $F \upharpoonright x=0$.

- Induction on n for Π_R we get a width b proof of $F \upharpoonright x=1$.

Apply the claim and we are done!

This will <u>massively</u> restructure the proof — low width at cost of doubly-exponential blow-up in size!

Q. Do you <u>have</u> to pay this cost?

(i.e. can we optimize width and size at the same time?)

No!

[Razborov 2016] Doubly-exponential blow-up is necessary for some formulas!

Next time:

(2) $S_{Res}(F) \geq 2^{\frac{(w_{Res}(F) - w(F))^2}{16n}}$.

$x \vee \overline{y}$

$$z_1 \oplus z_2 = (\overline{z_1} \vee \overline{z_2}) \wedge (z_1 \vee z_2)$$

$$\overline{z_1 \oplus z_2} = (z_1 \vee \overline{z_2}) \wedge (\overline{z_1} \vee z_2)$$

$$((z_1 \vee z_2) \wedge (\overline{z_1} \vee \overline{z_2})) \vee ((z_3 \vee \overline{z_4}) \wedge (\overline{z_3} \vee z_4))$$

↳ rewrite in CNF.