LECTURE 5

Recall again Ben-Sasson & Wigderson

For F CNF formula over n variables it holds that

$$L_R(F \vdash 0) = \exp\left(\Omega\left(\frac{(W(F\vdash 0) - W(F))^2}{n}\right)\right) \quad (1)$$

For restricted case of tree-like resolution got much stronger bound

$$L_T(F \vdash 0) \geq 2^{(W(F\vdash 0) - W(F))} \quad (2)$$

NATURAL QUESTION: Can we improve bound for general resolution from (1) to sth like (2)?

Suppose that F is k-CNF. Then (1) says that if $W(F\vdash 0) = \omega(\sqrt{n \log n})$ then $L_R(F\vdash 0)$ grows super polynomially

Today / Exhibit F s. t. k-CNF

Thm [BG01]
$$\begin{cases} L_R(F\vdash 0) = \text{poly}(n) \\ W(F\vdash 0) = \Theta(\sqrt{n}) \end{cases}$$

So bound in (1) is at least (almost) optimal

Corollary

General resolution is exponentially stronger than tree-like resolution.

There are better separations known (e.g. [BIW04]) but this one we get "for free"

Use CNF formulas encoding ordering principles:

"If $S = \{e_1, \ldots, e_n\}$ is a finite set of (partially or totally) ordered elements, then S has a minimal element."

Our CNFs will encode the negation of this (to be unsatisfiable).

x_{ij} should be interpreted as "$e_i < e_j$"

(a) $\overline{x_{ij}} \vee \overline{x_{ji}}$ $\quad i \neq j \in [n]$ $\quad$ antisymmetry

(b) $\overline{x_{ij}} \vee \overline{x_{jk}} \vee x_{ik}$ $\quad i \neq j \neq k \neq i \in [n]$ $\quad$ transitivity

(c) $\bigvee_{i \neq j} x_{ij}$ $\quad j \in [n]$ $\quad$ no min element

(d) $x_{ij} \vee x_{ji}$ $\quad i \neq j \in [n]$ $\quad$ totality

(a) + (b) + (c) Partial ordering principle POP_n

(a) + (b) + (c) + (d) Linear ordering principle LOP_n

(Have different names in the literature)

POP_n and LOP_n both have

- $\Theta(n^2)$ variables
- $\Theta(n^3)$ clauses

Conjectured hard for resolution by [Krishnamurthy '85]

Proven easy by [Stålmarck '96]

We do slightly modified proof by [Bonet & Galesi '99, '01]
conference → '99, journal → '01

<u>**Lemma**</u> [Sti 96] There are resolution refutations $\pi : POP_n \vdash 0$ in length poly(n) [and hence of $LOP_{(n)}$ too]

Let us write

$$C_m(j) = \bigvee_{i=1, i \neq j}^{m} x_{ij}$$ "one of $e_1, \dots, e_m$ is less than e_j"

$$A(i,j,k) = \bar{x}_{ij} \vee \bar{x}_{jk} \vee x_{ik}$$ "transitivity $e_i < e_j \wedge e_j < e_k \to e_i < e_k$"

$$B(i,j) = \bar{x}_{ij} \vee \bar{x}_{ji}$$ "antisymmetry $e_i < e_j \to e_j \not< e_i$"

<u>Idea</u> Inductive approach

$$POP_2 = C_2(1) \wedge C_2(2) \wedge B(1,2)$$

$$= x_{21} \wedge x_{12} \wedge (\bar{x}_{12} \vee \bar{x}_{21})$$

Easy ~~to~~ refute.

From POP_n, derive POP_{n-1}.
By induction POP_{n-1} easy to refute.
So POP_n also easy to refute

Structure of resolution refutation becomes

$C_n(1)$ $C_n(2)$ ... $C_n(n-1)$ $C_n(n)$
$C_{n-1}(1)$ $C_{n-1}(2)$ ... $C_{n-1}(n-1)$
⋮
$C_2(1)$ $C_2(2)$
0

Intuitively, refutation argues:
"If $S_n = \{e_1, e_2, \ldots, e_{n-1}, e_n\}$ is ordered but does not have minimal element, then $S_{n-1} = \{e_1, e_2, \ldots, e_{n-1}\}$ is also ordered and does not have minimal element"

~~For k=n,~~ We know $C_n(1), C_n(2), \ldots, C_n(n)$ since these are axioms. Show how to derive $C_{n-1}(1), C_{n-1}(2), \ldots, C_{n-1}(n-1)$ from this (works for any $k \leadsto k-1$, not just $n \leadsto n-1$)

Fix some $j \in [n-1]$ and show how to derive $C_{n-1}(j)$

(1) Perform following steps, all resolving over $x_{n,j}$

(1) $$\frac{C_n(j) \qquad A(1,n,j)}{C_{n-1}(j) \vee \overline{x}_{1,n}}$$

$$\left(\frac{\bigvee_{i=1, i \neq j}^{n} x_{i,j} \qquad \overline{x}_{1,n} \vee \overline{x}_{n,j} \vee x_{1,j}}{\bigvee_{i=1, i \neq j}^{n-1} x_{i,j} \vee \overline{x}_{1,n}} \right)$$

(2) $$\frac{C_n(j) \qquad A(2,n,j)}{C_{n-1}(j) \vee \overline{x}_{2,n}}$$

⋮

($j-1$) $$\frac{C_n(j) \qquad A(j-1,n,j)}{C_{n-1}(j) \vee \overline{x}_{j-1,n}}$$

(j) $$\frac{C_n(j) \qquad B(j,n)}{C_{n-1}(j) \vee \overline{x}_{j,n}}$$

"If all $\{e_1, \ldots, e_{n-1}\}$ are $\geq e_j$ then $e_i \nless e_n$" This is seen since $e_n < e_j$ (the only alternative left) $e_i < e_n$ would yield $e_i < e_j$ by transitivity which is a contradiction.

⋮

($n-1$) $$\frac{C_n(j) \qquad A(n-1,n,j)}{C_{n-1}(j) \vee \overline{x}_{n-1,n}}$$

(2) Now resolve over variables $x_{1,n}, x_{2,n}, \ldots, x_{n-1,n}$ as follows

Some e_i must be $< e_n$ ...

But if $C_{n-j}(j)$ holds, that element is not e_1...

$$\frac{C_n(n) \qquad C_{n-1}(j) \vee \overline{x}_{1,n}}{C_{n-1}(j) \vee \bigvee_{\ell=2}^{n-1} x_{\ell,n}}$$

$$\frac{C_{n-1}(j) \vee \bigvee_{\ell=2}^{n-1} x_{\ell,n} \qquad C_{n-1}(j) \vee \overline{x}_{2,n}}{C_{n-1}(j) \vee \bigvee_{\ell=3}^{n-1} x_{\ell,n}}$$

... And not e_2 ...

$$\vdots$$

... And not e_{n-2} ...

$$\frac{C_{n-1}(j) \vee \bigvee_{\ell=n-2}^{n-1} x_{\ell,n} \qquad C_{n-1}(j) \vee \overline{x}_{n-2,n}}{C_{n-1}(j) \vee x_{n-1,n} \qquad C_{n-1}(j) \vee \overline{x}_{n-1,}}$$

$$\frac{}{C_{n-1}(j)}$$

But this shows that for any $j = 1, \ldots, n-1$, we can derive $C_{n-1}(j)$, which is exactly what we need for the induction.

CLAIM Putting everything together, this gives a refutation of POP_n in length $\mathrm{poly}(n)$

Proof Left to the reader to verify this

QUESTION What is the (clause) space of this refutation?

Left to the reader to figure out good way of doing it space-efficiently.

Want to prove lower bound on width
Will prove this for LOP_n.
Except this is not a k-CNF

Standard trick

Can transform any CNF formula F to equivalent 3-CNF formula, which we will denote $\widetilde{F}$, by using extension variables

Suppose $F = C_1 \wedge C_2 \wedge \cdots \wedge C_m$
m clauses over n variables
For every C_j
- If $W(C_j) \leq 3$, leave as is, let $\widetilde{C}_j = C_j$
- Else, for $C_j = a_1 \vee a_2 \vee \cdots \vee a_w$

  let $\widetilde{C}_j$ be the clauses

$$\overline{y}_{0,j}$$
$$y_{0,j} \vee a_1 \vee \overline{y}_{1,j}$$
$$y_{1,j} \vee a_2 \vee \overline{y}_{2,j}$$
$$\vdots$$
$$y_{w-1,j} \vee a_w \vee \overline{y}_{w,j}$$
$$y_{w,j}$$

Let $\widetilde{F} = \bigwedge_{C \in F} \widetilde{C}$. Clearly a 3-CNF

Say that $\widetilde{F}$ is the 3-CNF VERSION of F.

Proposition 1

$\tilde{F}$ is unsatisfiable if and only if F is unsatisfiable

Proof Exercise.

Proposition 2

If F has m clauses over n variables and $\pi : F \vdash 0$ is a (general) resolution refutation, then there is a (general) resolution refutation $\tilde{\pi} : \tilde{F} \vdash 0$ s.t. $L(\tilde{\pi}) \leq L(\pi) + O(mn)$

Proof Also exercise

That is, $\tilde{F}$ is "not harder than" F.

We will study $\widetilde{LOP_n}$. Easy to verify

still $\Theta(n^2)$ variables
still $\Theta(n^3)$ clauses

Will prove

Lemma 3 $W(\widetilde{LOP_n} \vdash 0) = \Omega(n)$

From this the [BG01]- thm follows

Plugging in the width bound in [BW01] for tree-like resolution, we get

$$L_T(\widetilde{LOP_n} \vdash 0) = \exp(\Omega(n))$$

which yields the exponential separation between general and tree-like resolution in the corollary

Easiest to think about LOP_n and then just set extension variables in $\widetilde{LOP}_n$ in "the right way"

In what follows
$$\alpha : Vars(LOP_n) \to \{0,1\}$$
$$\beta : Vars(\widetilde{LOP}_n) \to \{0,1\}$$

<u>DEF</u> 4 A CRITICAL ASSIGNMENT α for LOP_n is an assignment defining a total (a.k.a. linear) ordering on $\{e_1, \ldots, e_n\}$

i.e. $\alpha(x_{ij}) = 1$ iff $e_i < e_j$ according to this ordering.

α is j-CRITICAL if e_j is the (unique) minimal element.

If α is j-critical, then
$$\alpha\left(\bigvee_{i \neq j} x_{ij}\right) = \alpha(C_j) = 0$$
$$\alpha(LOP_n \setminus \{C_j\}) = 1$$

<u>DEF</u> 5 A j-CRITICAL ASSIGNMENT β for $\widetilde{LOP}_n$ is an assignment s.t.

1) β restricted to subdomain $Vars(LOP_n)$ is j-critical for LOP_n

2) $\beta(\widetilde{LOP}_n \setminus \widetilde{C}_j) = 1$

3) $\beta(\widetilde{C}_j) = 0$

<u>Proposition 6</u> Any j-critical assignment α for LOP_n can be extended to a j-critical assignment β for $\widetilde{LOP}_n$

Proof For every $k \neq j$, set the extension variables $y_{i,k}$ so that $\tilde{C}_k$ becomes true.

E.g. find min i^* s.t. $\alpha(x_{i^*k}) = 1$ (exists since $\alpha(C_k) = 1$)

Set $\beta(y_{ik}) = 0$ for $i < i^*$

$\beta(y_{ik}) = 1$ for $i \geq i^*$

So we can keep thinking about LOP_n if we just make sure to be careful with the extension variables.

We want to define set of all variables that "say anything about e_j"

$$V_j = Vars(\tilde{C}_j) \cup \{x_{j,i} \mid i \neq j, i \in [n]\}$$

<u>Proposition 7</u> If D is a clause with $W(D) = w$, then at most $2w$ sets V_j have variables appearing in D.

<u>Proof</u> Every variables appears in at most two different V_j-sets (extension variables only in one).

Want to define a complexity measure or "progress measure" $\mu : \{\text{clauses}\} \to \mathbb{N}$ just as before.

For $I \subseteq [n]$, let $\widetilde{C}_I = \bigwedge_{i \in I} \widetilde{C}_i$

For any clause D, let I_D be a set of minimal size s.t.

<u>All</u> critical assignments to $\widetilde{LOP}_n$ that satisfy $\widetilde{C}_{I_D}$ must also satisfy D.

Let $\mu(D) = |I_D|$

① If D is an axiom $\in \widetilde{C}_j$ then $\mu(D) = 1$

If $D \in \widetilde{LOP}_n \setminus \bigcup_{j \in [n]} \widetilde{C}_j$ then $\mu(D) = 0$

② $\mu(0) = n$, since if $I \neq [n]$, say $j \in [n] \setminus I$, then $\widetilde{LOP}_n \setminus \widetilde{C}_j$ is satisfiable by j-critical assignments

③ μ is subadditive, i.e., if $\dfrac{D \vee x \quad D' \vee \bar{x}}{D \vee D'}$

then $\mu(D \vee D') \leq \mu(D \vee x) + \mu(D' \vee \bar{x})$.

Thus, $\exists$ in any $\pi : \widetilde{LOP}_n \vdash 0$

we can find $D \in \pi$ with

$$n/3 \leq \mu(D) < 2n/3$$

We claim that $W(D) \geq n/6$.

To get a contradiction, suppose not, i.e. $W(D) < n/6$

Fix a minimal set I_D assoc to D by μ

$|I_D| \geq n/3$ since $\mu(D) \geq n/3$

By prop 7 $\exists k \in I_D$ s.t. $V_k \cap Vars(D) = \emptyset$

Pick a k-critical β, i.e. s.t.

$$\beta(\tilde{C}_k) = 0$$
$$\beta(\tilde{C}_j) = 1 \quad \text{for } j \neq k$$
$$\beta(D) = 0$$

Such β exists by minimality of I_D

Consider $\overline{I_D} = [n] \setminus I_D$

$|I_D| \leq 2n/3$ so $|\overline{I_D}| \leq n/3$

Again by prop 7 $\exists \ell \in \overline{I_D}$ s.t. $V_\ell \cap Vars(D) = \emptyset$

<u>Intuition</u> D does not depend in any way on anything related to e_k or e_ℓ, so we can change ordering so that $e_\ell < e_k$ without affecting D. But that will give critical assignment

- satisfying $\tilde{C}_{I_D}$
- falsifying D

which contradicts how I_D chosen in first place

Build β^* corresponding to such reordering in 3 steps from β

① Make ℓ smallest

$$\left.\begin{array}{l}\beta^*(x_{\ell,j}) = 1\\ \beta^*(x_{j,\ell}) = 0\end{array}\right\} \quad \forall j \neq \ell$$

② For all $j \notin \{\ell, k\}$, only change from β is that $x_{\ell j}$ potentially flipped to true — can only help to satisfy $\tilde{C}_j$

(For $\tilde{C}_\ell$ we will get $\beta^*(\tilde{C}_\ell) = 0$ however auxiliary variables are set)

③ Remains to take care of $\tilde{C}_k$

But $\beta^*(x_{\ell,k}) = 1$ so we can set

$$y_{i,k} = 0 \quad \text{for } i < \ell$$
$$y_{i,k} = 1 \quad \text{for } i \geq \ell$$

and make all of $\tilde{C}_k$ true under β^*

So now β^* is a critical assignment satisfying $\tilde{C}_{I_D}$ but falsifying D, contrary to assumption.

Contradiction. The lemma follows.