LECTURE 3

Last time

Proved: Large resolution width

$$\Downarrow$$

Large resolution length

For general resolution

$$W(F \vdash 0) \leq W(F) + \sqrt{8n \ln L(F \vdash 0)}$$

where n = # variables in formula

Today

Use this to prove exponential lower bounds on proof length in resolution

Means SAT solvers based on resolution can't possibly solve these formulas efficiently

Use corollary

$$L(F \vdash 0) \geq \exp\left(\frac{(W(F \vdash 0) - W(F))^2}{8n}\right)$$

Pigeonhole principle

"m pigeons don't fit into n pigeonholes if $m > n$."

x_{ij} = "pigeon i sits in hole j"

PHP^m_n consists of clauses

P^i $\quad \bigvee_{j=1}^{n} x_{ij}$ "pigeon i sits in some hole"

$H_j^{i,i'}$ $\quad \overline{x}_{ij} \vee \overline{x}_{i'j}$ "hole j doesn't hold both pigeons i and i'"

$m > n \Rightarrow$ unsatisfiable

Today focus on hardest case $m = n+1$

(intuitively gets easier for larger m)

THM 2 (Haken '85) (Son of Wolfgang Haken of 4CT-fame)

$$L(PHP^{n+1}_n \vdash 0) = \exp(\Omega(n))$$

PHP^{n+1}_n has # clauses (and size) $\Theta(n^3)$

Want to use BW-machinery.

Two problems:

1) $\exists$ refutations in width $O(n)$
$= O\left(\sqrt{|Vars(PHP^{n+1}_n)|}\right)$

2) Also, width of formula is n

$\Longrightarrow$ Can't get anything interesting

Make formula "sparser"

Consider bipartite graph $G = (U \cup V, E)$

Assume throughout $|U| = m$, $|V| = n$

$N(u)$ = set of NEIGHBOURS of vertex u.

$PHP(G)$ has clauses

$P^u \qquad \bigvee_{v \in N(u)} x_{uv}$

$\cancel{P^v} H_v^{u,u'} \qquad \overline{x}_{uv} \vee \overline{x}_{u'v} \qquad u \neq u', u, u' \in N(v)$

OBSERVATION

If $G' = (U \cup V, E')$ has $E' \supseteq E$, then
$L(PHP(G) \vdash 0) \leq L(PHP(G') \vdash 0)$

<u>Proof</u> Consider ρ setting $x_{uv} = 0$ for all edges $(u,v) \in E' \setminus E$.
Then $PHP(G')\restriction_\rho = PHP(G)$.

In particular, holds for $G' = K_{m,n}$

with $PHP(K_{m,n}) = PHP_n^m$

Suppose G has constant left degree d (≥ 2)

Then $PHP(G)$ is
- d-CNF formula
- with $d(n+1) = \Theta(n)$ variables

$\Rightarrow$ Potentially back in business

If we can find such G with
$\boxed{W(PHP(G) \vdash 0) = \Omega(n)}$ we're done.
Corollary would yield

$$\mathcal{L}(PHP_n^{n+1} \vdash 0) \geq \mathcal{L}(PHP(G) \vdash 0))$$
$$= \exp\left(\frac{(n-d)^2}{d(n+1)}\right)$$
$$= \exp(\Omega(n))$$

since $d = O(1)$

Step back a bit
Why is PHP_n^{n+1} hard?

Because it's almost satisfiable.
Every set of $s \leq n$ pigeons fit perfectly into holes.
No "local argument" can derive contradiction.

Would like to find constant left outdegree graph with similar properties:
(a) sparse graph, but
(b) good connectivity

EXPANDER (Bipartite vertex expander graph) 3:5

$G = (U \cup V, E)$ is a (d, s, e)-expander if

a) left degree d [sparse]

b) $\forall U' \subseteq U$, $|U'| \leq s$ it holds that

$|N(U')| \geq e\,|U'|$ [well-connected]

Maybe draw picture

In fact, want something slightly stronger

UNIQUE-NEIGHBOUR EXPANDER

$G = (U \cup V, E)$ is a (d,s,e)-unique-neighbour expander (or sometimes BOUNDARY EXPANDER) if

a) left degree d

b) $\forall U' \subseteq U$, $|U'| \leq s$ it holds that

$$|\partial U'| \geq e\,|U'| \quad \text{where}$$

$$v \in \partial U' \text{ if } |N(v) \cap U'| = 1.$$

PROPOSITION

Any (d, s, κ)-expander is a $(d, s, 2\kappa - d)$-unique neighbour expander.

Proof

Left to the reader.

The lower bound follows from combining two lemmas

LEMMA A

For a (d, s, e)-unique-neighbour expander, $e \geq 1$, it holds that $W(PHP(G) \vdash 0) \geq s \cdot e/2$

LEMMA B

There is a $c > 1$ such that for all n large enough there are graphs $G = (U \cup V, E)$, $|U| = n+1$, $|V| = n$, that are $(5, n/c, 1)$-unique-neighbour expanders

Proof sketch for Lemma B.

Can be done constructively, but we won't go there. Instead use probabilistic method to prove existence of $(5, n/c, 3)$-expanders.

For all $u \in U$, pick 5 neighbours in V uniformly and independently at random among all $\binom{n}{5}$ subsets.

For the right c, such a graph is an expander with overwhelming probability. This is proven by showing that all sets $U' \subseteq U$ of size $\leq s$ are expanding ~~with~~ almost surely.

And the probability couldn't be large (indeed, couldn't be > 0) unless such expanders exist. So they do exist.

Helpful facts for the calculations

① Union bound: $Pr[A \cup B] \leq Pr[A] + Pr[B]$

② $$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{ne}{k}\right)^k$$

③ If $m > n$ then $$\frac{\binom{n}{k}}{\binom{m}{k}} < \left(\frac{n}{m}\right)^k$$

There are also explicit constructions, e.g. by ~~Capalbo–Vadhan~~
Capalbo–Reingold–Vadhan–Wigderson STOC '02
But note that we don't need explicitness – we just use the expander inside the proof, so non-explicitness is perfectly OK.

PROOF STRATEGY FOR LEMMA 4

Given any $\pi = \{D_1, D_2, \ldots, D_L\}$ define measure $\mu : \{\text{clauses}\} \to \mathbb{N}$ of "progress" such that

(i) $\mu(\text{axioms}) \leq 1$

(ii) $\mu(\text{final empty clause } 0) \geq$ large

(iii) μ only increases gradually, so there must exist some $D_i \in \pi$ with medium-sized measure $\mu(D_i)$

(iv) Such a D_i must contain many literals (because of expansion), so $W(D)$ large
$\Rightarrow W(\pi)$ large (for any π)

~~IMPLEMENTATION~~

Let $\mathcal{H}$ denote all hole axioms on form

$$\overline{x}_{u,v} \vee \overline{x}_{u',v} \quad \text{for } u,u' \in N(v)$$

Let $$P^u = \bigvee_{v \in N(u)} x_{u,v}$$

Define
$$\mu(D) = \min \left\{ |\mathcal{U}'| : \mathcal{H} \wedge \bigwedge_{u \in \mathcal{U}'} P^u \vDash D \right\}$$

(i) $C \in \mathcal{H} \Rightarrow \mu(C) = 0$
$C = P^u \Rightarrow \mu(C) = 1$

(ii) $\mu(0) > s$

Any set $\mathcal{U}'$ of s pigeons fit into $|\partial \mathcal{U}'| \geq |\mathcal{U}'|$ distinct holes. Follows by

HALL'S MARRIAGE THEOREM
~~If~~ ~~For~~ $G = (\mathcal{U}' \cup V', E')$ it holds that there is a matching of $\mathcal{U}'$ into V' if and only if $\forall\ \mathcal{U}^* \subseteq \mathcal{U}'$ we have $|N(\mathcal{U}^*)| \geq |\mathcal{U}^*|$

This means that for all $\mathcal{U}'$ ~~of~~ size $\leq s$ $\mathcal{H} \wedge \bigwedge_{u \in \mathcal{U}'} P^u$ is satisfiable, so $\mathcal{H} \wedge \bigwedge_{u \in \mathcal{U}'} P^u \nvDash 0$.

(iii) If $$\frac{D \vee x \quad D' \vee \overline{x}}{D \vee D'}$$ then

$$\mu(D \vee D') \leq \mu(D \vee x) + \mu(D' \vee \overline{x})$$

SUBADDITIVITY W.R.T. RESOLUTION RULE

If $\mathcal{H} \wedge \bigwedge_{u \in \mathcal{U}_1} p^u \models D \vee x$

and $\mathcal{H} \wedge \bigwedge_{u \in \mathcal{U}_2} p^u \models D' \vee \bar{x}$

then $\mathcal{H} \wedge \bigwedge_{u \in \mathcal{U}_1 \cup \mathcal{U}_2} \models D \vee D'$

Hence there must exist $D \in \pi$ with

$$s/2 \leq \mu(D) < s$$

Fix a minimal set $\mathcal{U}'$ (of size $\mu(D)$) such that

$$\mathcal{H} \wedge \bigwedge_{u \in \mathcal{U}'} p^u \models D \qquad (1)$$

<u>CLAIM</u> $\forall v \in \partial \mathcal{U}'$ $\exists$ variable $x_{uv,v}$ in D.

But $|\partial \mathcal{U}'| \geq e|\mathcal{U}'| \geq s \cdot e/2$, since G is a unique-neighbour expander. Hence $W(D) \geq se/2$ follows, which in turn establishes Lemma A.

Proof of CLAIM

By contradiction. Fix $v^* \in \partial \mathcal{U}'$.
Let $u^* \in \mathcal{U}'$ be ~~the~~ a unique neighbour.
Assume that no variable x_{u', v^*} in D.

By the definition of μ

$$\mathcal{H} \wedge \bigwedge_{u \in \mathcal{U}' \setminus \{u^*\}} P^u \nvDash D \qquad (2)$$

($\mathcal{U}'$ had minimal size for this to hold)
This means $\exists\ \alpha$ satisfying $\mathcal{LHS}$ and falsifying D.

W.l.o.g. let $\alpha(x_{u,v^*}) = 0 \quad \forall u \in N(v^*)$

- Cannot falsify $\mathcal{H}$ to set variables to false
- Cannot falsify any P^u, $u \in \mathcal{U}'$, since u^* is unique neighbour of v in $\mathcal{U}'$
- Cannot satisfy D since there are no variables x_{u,v^*} in D.

Now let α^* be as α except $\alpha(x_{u^*,v^*}) = 1$

- $\alpha^*(D) = 0$ still holds for same reasons as above
- $\alpha^*(\mathcal{H}) = 1$ since all other x_{u,v^*} set to 0
- $\alpha^*(P^{u^*}) = 1$

So now $\alpha^*(\mathcal{H} \wedge \bigwedge_{u \in \mathcal{U}'} P^u) = 1$ but $\alpha^*(D) = 0$, contradicting (1). The claim follows. $\square$

G connected, undirected graph; $|V(G)| = n$

$f: V(G) \to \{0,1\}$ has ODD WEIGHT if $\sum_{v \in V(G)} f(v) \equiv 1 \pmod 2$

TSEITIN CONTRADICTION $Ts(G,f)$

G graph, f odd-weight function. Variable x_e for each edge $e \in E(G)$. For each vertex $v \in V(G)$ define clauses $PARITY_v$ encoding

$$PARITY_v = \bigoplus_{e \ni v} x_e \equiv f(v) \pmod 2$$

Then

$$Ts(G,f) = \bigwedge_{v \in V(G)} PARITY_v$$

How to encode parity? Add clauses ruling out all incorrect assignments.

Ex Encode $x \oplus y \oplus z = 1$

For each falsifying assignment, add a clause with opposite signs for all variables (saying that not all variables agree with this assignment)

$x \lor y \lor z$	rules out	$x = y = z = 0$
$\overline{x} \lor \overline{y} \lor z$	–"–	$x = y = 1,\ z = 0$
$\overline{x} \lor y \lor \overline{z}$	–"–	$x = z = 1,\ y = 0$
$x \lor \overline{y} \lor \overline{z}$	–"–	$x = 0,\ y = z = 1$

$\boxed{\text{LEMMA C}}$ If maximal degree of G is d, then $Ts(G,f)$ is a d-CNF with $\leq nd/2$ variables and $\leq n \cdot 2^{d-1}$ clauses.

LEMMA D For G a connected graph, $Ts(G,f)$ is unsatisfiable iff f has odd weight

Proof of one direction

Suppose $\forall v$ we have $\bigoplus_{e \ni v} x_e \equiv f(v) \pmod 2$

But $\bigoplus_{v \in V(G)} \bigoplus_{e \ni v} x_e$ is even, since each edge is summed over twice

And $\bigoplus_{v \in V(G)} f(v)$ is odd by definition. Contradiction

So $Ts(G,f)$ is unsatisfiable if f has odd weight.

Tseitin contradictions are hard if the underlying graph is expanding. But here we use a slightly different (but related) notion of expansion.

For $S \subseteq V(G)$ a subset of vertices, let $\overline{S} = V(G) \setminus S$. Let $E(S, \overline{S})$ denote all edges connecting some $v \in S$ to some $u \in \overline{S}$

The EDGE EXPANSION of G is

$$h(G) = \min\left\{ \frac{|E(S,S')|}{|S|} : S \subseteq V(G), |S| \leq |\overline{S}| \right\}$$

(also known as the ISOPERIMETRIC NUMBER)

There exist graphs with good edge expansion, i.e. graphs G_n of size $n \to \infty$, maximal degree 3, and $h(G_n) > 0$

Want to prove

$\boxed{\text{LEMMA E}}$ $W(Ts(G,f) \vdash 0) \geq \frac{h(G)}{3} n$

If G has constant maximal degree, we then get

THEOREM 2 (Urquhart '87)
If G is a constant degree graph with positive edge expansion (bounded away from 0) then

$$L(Ts(G,f) \vdash 0) = \exp(\Omega(n))$$

Note that $Ts(G,f)$ also has size $\Theta(n)$ ~~has~~ and has $\Theta(n)$ variables, so this is a truly exponential lower bound and is tight up to constant factors in exponent

Strategy is the same:
- Define cplx measure μ
- $\mu(\text{axioms}) = \text{small}$
- $\mu(0) = \text{large}$
- Find clause with $\mu(D) = \text{medium}$
- Argue ~~μ~~ $W(D) = \text{large}$.

(In fact, Ben-Sasson & Wigderson have a slightly more general technique that unify the lower bounds for PHP_n^{n+1} and $Ts(G,f)$.)

Let $\mu(D) = \min\left\{ |V'| : \bigwedge_{v \in V'} PARITY_v \models D \right\}$

(i) If $C \in Ts(G,f)$ then $C \in PARITY_v$ for some v, so $\mu(C) = 1$

(ii) $\mu(0) = |V(G)| = n$, since for any v^*

$\bigwedge_{v \in V \setminus \{v^*\}} PARITY_v$ is satisfiable.

To see this flip $f(v^*)$. This makes all of formula satisfiable, so $\bigwedge_{v \in V \setminus \{v^*\}} PARITY_v$ is also satisfiable.

(iii) If $\dfrac{D \vee x \quad D' \vee \bar{x}}{D \vee D'}$ then

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

exactly as before.

So in any ~~proof~~ resolution there is some D with $\frac{n}{3} \leq \mu(D) \leq \frac{2n}{3}$

(iv) Need to argue that D is wide

Fix minimal V' s.t.

$$\bigwedge_{v \in V'} PARITY_v \vDash D \qquad (*)$$

We know $$\frac{\mathcal{E}(V', \overline{V'})}{\min(|V'|, |\overline{V'}|)} \geq h(G)$$ and $\min(|V'|, |\overline{V'}|) \geq \frac{n}{3}$

so $$\mathcal{E}(V', \overline{V'}) \geq \frac{h(G)}{3} n$$

We claim that $\forall e \in \mathcal{E}(V', \overline{V'})$ we have $x_e \in Vars(D)$

Suppose not. Consider $e = (v^*, v^{**}) \in \mathcal{E}(V', \overline{V'})$

Since V' was chosen minimal, we have

$$\bigwedge_{v \in V' \setminus \{v^*\}} PARITY_v \nvDash D$$

Fix α setting LHS to true & RHS to false

By assumption, $\alpha(PARITY_{v^*}) = 0$

Flip x_e to get new assignment α'

$$\alpha'\left(\bigwedge_{v \in V'} PARITY_v\right) = 1$$

but since $x_e \notin Vars(D)$ $\quad \alpha'(D) = 0$

This contradicts $(*)$ and lemma E

is proven. Theorem 2 now follows from Ben-Sasson's & Wigderson's general theorem.