Lecture 5 Sep 17

Thm (Part (2) of earlier) If F is any unsat. CNF then

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

"width gap" $\gg \sqrt{n}$

Proof Proved last ti

Claim 1 If $w_{Res}(F \upharpoonright x=b) \leq k-1$ and $w_{Res}(F \upharpoonright x=1-b) \leq k$ then $w_{Res}(F) \leq k$.

Let π be our optimal resolution proof for F.

Say a clause C is wide if C has at least k literals (k chosen later).

Let

$$a = \left(1 - \frac{k}{2n}\right)^{-1} \quad \left(\geq e^{k/2n} \text{ since } \tfrac{k}{2n} < 1\right)$$

Claim 2 If F can be refuted by a proof using at most a^b wide clauses, then

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

Pf. Induction on n, b. Let S be the # of wide clauses in the proof $S \leq a^b$.

If $b=0$, $|S| \leq 1 \Rightarrow \bot \in F$, $w_{Res}(F) \leq w(F)$

Since all of the wide clauses have $\geq k$ literals, by averaging there is a literal ℓ that occurs in

$\hookrightarrow x$ or $\bar{x}$

$$\frac{k}{2n} s$$

of the wide clauses.

- If we set $\ell = 1$, then we're left with a refutation of

$$F \restriction \ell = 1 \quad \text{with at most} \quad \left(1 - \frac{k}{2n}\right) s \quad \text{wide clauses.}$$

$$\left(1 - \frac{k}{2n}\right) s \leq a^{-1} a^{b} \leq a^{b-1}.$$

So induction on $b \Rightarrow w_{Res}(F \restriction \ell = 1) \leq w(F) + k + b - 1$

- If $\ell = 0$, then we're left with a refutation of

$$F \restriction \ell = 0, \text{ with } \leq n-1 \text{ variables.}$$

So, induction on $n \Rightarrow w_{Res}(F \restriction \ell = 0) \leq w(F) + k + b$

By Claim 1, $w_{Res}(F) \leq w(F) + k + b$. $\square$

Choose b s.t. $|\pi| = a^b$. Then

$$b = \frac{\ln |\pi|}{\ln a} = \frac{\ln S_{Res}(F)}{\ln a} \leq \frac{2n \ln S_{Res}(F)}{k}.$$

Applying Claim 2

$$w_{Res}(F) \le w(F) + K + \underbrace{\frac{2n \ln S_{Res}(F)}{K}}.$$

Optimizing for K, we get $K = \sqrt{2n \ln S_{Res}(F)}$.

$\square$

Is the size-width relationship tight? Yes

[Bonet - Galesi 99] Exhibited a formula with

$$w(F) = O(1), \quad w_{Res}(F) = \sqrt{n}, \quad S_{Res}(F) \le n^{O(1)}.$$

Other Hard Examples for Resolution

- Tseitin tautologies
- Random CNF formulas

Tseitin Tautologies

Let $G = (V, E)$ be a graph with $|V|$ odd.

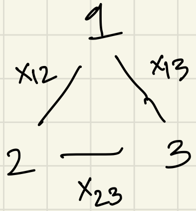
The Tseitin tautology Tsei_G is an unsatisfiable CNF formula with

Variables: For every edge $uv \in E$ add variable x_{uv}

Constraints: For every vertex $u \in V$ add constraint

XOR/ mod 2 sum $\rightarrow$ $\bigoplus_{uv \in E} x_{uv} = 1$

ex)



$G = K_3$

$x_{12} \oplus x_{13} = 1$

$x_{12} \oplus x_{23} = 1$

$x_{13} \oplus x_{23} = 1$

Add up all equations $0 = 1$.

Always be unsatisfiable when $|V|$ is odd (handshaking)

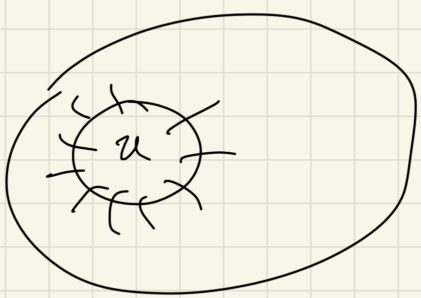
"Resolution cannot count, even mod 2"

Thm [Urquhardt 87] when G is an expander graph then Tsei_G requires exponential length.

Defn If $G = (V, E)$ is a graph then the (edge) expansion of G is

$$\exp(G) := \min_{U \subseteq V} \left\{ |E(U, V \setminus U)| : \frac{|V|}{3} \le |U| \le \frac{2|V|}{3} \right\}$$

where $E(U, V \setminus U) :=$ {edges crossing from U to $V \setminus U$}



G is an expander graph if $\exp(G)$ is "large".

Expander graphs := very "well connected" –

cannot break G into disconnected pieces by only cutting few edges.

ex) Complete graph clearly has $\exp(G) \approx \Theta(n^2)$.
$= O(|V|)$

Q. Do sparse (i.e. few edges) expanders exist?

A. Yes! (Concrete examples are hard to describe...)

Random graph (adding each edge with prob. p) are expanders with very high probability.

Exercise $\quad w_{Res}(Tsei_G) \geq \exp(G)$ (Hint. What is $\mu(\cdot)$? Try with $G = K_n$.

Thm The complete graph K_n has

$\exp(K_n) = \Theta(n^2)$, so

$$S_{Res}(Tsei_{K_n}) \geq 2^{\Omega\left(\frac{(\overbrace{w_{Res}(Tsei)}^{\Theta(n^2)} - \overbrace{\mu(F)}^{O(n)})^2}{n^2}\right)} = 2^{\Omega(n^2)}.$$

Random k-CNF

Let $\mathcal{F}(m,n,k)$ be the probability distribution over width-k CNF formulas obtained by sampling m clauses of width k with replacement uniformly random.

Each single width-k clause is chosen uniformly from n variables with probability

$$\frac{1}{\binom{n}{k} 2^k}$$

Q. For fixed n, k, for which m is $F \sim \mathcal{F}(m,n,k)$ unsat. w.h.p.?

Let $z \in \{0,1\}^n$ be a fixed assignment.

If I sample a random clause, what is the likelihood it will be satisfied?

$$\Pr_{C \sim \mathcal{F}(1,n,k)} [C \text{ satisfied by } z] = 1 - \frac{1}{2^k}$$

$$\Pr_{F \sim \mathcal{F}(m,n,k)} [F \text{ satisfied by } z] = \left(1 - \frac{1}{2^k}\right)^m$$

$$\leq \exp\left(-\frac{m}{2^k}\right).$$

$$\Pr[\exists z \text{ satisfying } F] \leq 2^n \exp\left(-\frac{m}{2^k}\right) \quad \text{(union bound)}$$

$\frac{m}{n} \gg \frac{2^k}{\log(e)}$ then $\nearrow$ will tend to 0.

Choosing m "near" to this threshold, then resolution will require long refutations.

<u>Thm</u> [Chvátal–Szemeredi 88, BKPS 98]

If $F \sim \mathcal{F}(m,n,k)$ where $m \le n^{k/2}$ then

$$S_{Res}(F) := 2^{\Omega(m^{O(1)})} \quad \text{w.h.p.}$$

"Almost all" random K-CNFs are hard for resolution.

<u>Hard Exercise</u> Prove if $F \sim \mathcal{F}(m,n,3)$, $m \le n^{3/2-\varepsilon}$, then

$$w_{Res}(F) = \Omega\left(\left(\frac{m}{n}\right)^{-2/(1-\varepsilon)} n\right) \quad \text{w.h.p.}$$

$$= \Omega(n).$$

↳ Plug width lower bd into width-size relation then you can deduce size lower bounds.

Next time:

Algorithms!