Most resolution length lower bounds can be proven via Ben-Sasson & Wigderson size-width relation

- Prove strong lower bound on $W(F \vdash \bot)$
- Use

$$\boxed{L(F \vdash) = \exp\left(\Omega\left(\frac{(W(F \vdash \bot) - W(F))^2}{|Vars(F)|}\right)\right)}$$

Width lower bounds (and also lower bounds on other cplx measures) can be proven via graph expansion

High-level idea: Given CNF formula F over variables X, create bipartite CLAUSE-VARIABLE INCIDENCE GRAPH (CVIG) with $G(F)$

- Left vertex set = clauses C
- Right vertex set = variables x
- Edge between C and x if x or $\bar{x}$ occurs in C

Want to show that if $G(F)$ well-connected, then F hard

DEF (BIPARTITE BOUNDARY EXPANDER)

Bipartite graph $G = (U \cup V, E)$ is a bipartite (s, δ)-BOUNDARY EXPANDER if $\forall U' \subseteq U, |U'| \leq s$, it holds that $|\partial(U')| \geq \delta |U'|$, where the BOUNDARY $\partial(U') = \{v \in V : |N(v) \cap U'| = 1\}$ consists of all vertices on right-hand side V with unique neighbour in U' on left-hand side

Problem: Often there is higher level structure that is not exactly captured by CNF encoding

Ex For Tseitin formula, think of clauses

$$\left\{\begin{array}{l} x \vee y \vee z \\ x \vee \bar{y} \vee \bar{z} \\ \bar{x} \vee y \vee \bar{z} \\ \bar{x} \vee \bar{y} \vee z \end{array}\right\} \text{ as single constraint } x \oplus y \oplus z = 1$$

Ex For PHP, we only studied assignments corresponding to matchings, so hole axioms $\bar{x}_{i,j} \vee \bar{x}_{i',j}$ never really played a part in the argument

Want to allow "generalized CVIG" that captures combinatorial structure behind CNF formula

Given formula $\mathcal{F}$ over variables V, we choose

① Partition $\mathcal{F} = E \cup \bigcup_{i=1}^{m} F_i$

E and F_i are disjoint sets of clauses that should be satisfiable

② Division $V = \bigcup_{i=1}^{n} V_i$

V_i and V_j need not be disjoint

$\boxed{\text{OVERLAP}}$ $ol(\mathcal{V}) = \max_x \left|\{ V_i \in \mathcal{V} : x \in V_i \}\right|$

Overlap will be small constant for us

Today it will be $= 1$

Generalized CVIG for $(\mathcal{F}, \mathcal{V})_{\mathcal{E}}$

- Left vertex set $\mathcal{U} = \{F_1, F_2, \ldots, F_m\}$
- Right vertex set $\mathcal{V} = \{V_1, V_2, \ldots, V_n\}$
- Edge (F_i, V_j) if $\mathrm{Vars}(F_i) \cap V_j \neq \emptyset$

Special clause set $\mathcal{E}$ not part of graph, but "filters" with truth value assignments used in lower bound arguments

Describe two-person game between Adversary and Satisfier played on $(\mathcal{F}, \mathcal{V})_{\mathcal{E}}$

Good Satisfier strategy = resolution width lower bound

DEF (RESOLUTION EDGE GAME)

Fix $(\mathcal{F}, \mathcal{V})_{\mathcal{E}}$-graph for CNF formula $\mathcal{F}$ over variables $\mathcal{V}$. RESOLUTION EDGE GAME on edge (F_i, V_j) with respect to filtering set $\mathcal{E}$:

(1) Adversary chooses total assignment α s.t. $\alpha(\mathcal{E}) = T$

(2) Satisfier modifies α on V_j to get α'

(3) Satisfier wins if $\alpha'(F_i \wedge \mathcal{E}) = T$

Satisfier wins resolution edge game on (F_i, V_j) if has winning strategy

Satisfier wins resolution edge game on $(\mathcal{F}, \mathcal{V})_{\mathcal{E}}$ if wins on all edges in graph

DEF (RESOLUTION EXPANDER)

$(\mathcal{F}, \mathcal{V})_{\mathcal{E}}$-graph is $(s, \delta, \mathcal{E})$-RESOLUTION EXPANDER if

- $(\mathcal{F}, \mathcal{V})_{\mathcal{E}}$ graph is (s, δ)-boundary expander
- Satisfier wins resolution edge game on $(\mathcal{F}, \mathcal{V})_{\mathcal{E}}$.

<u>Note</u> <u>expansion</u> measured in terms of <u>vertices</u> in $(\mathcal{F}, V)_E$ - graph. Every vertex can correspond to many clauses or variables

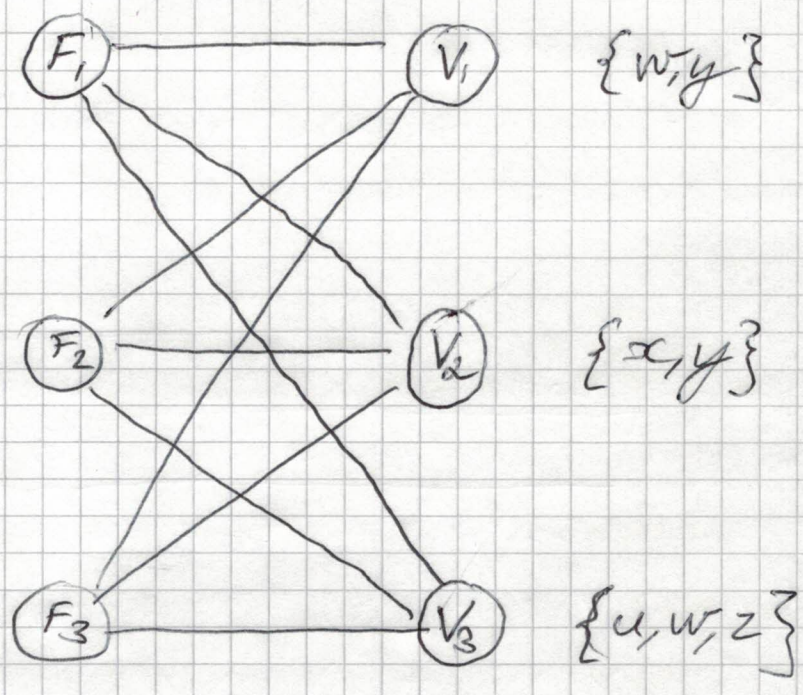
$\forall \mathcal{F}' \subseteq \mathcal{F} \setminus \{E\}$ s.t. $|\mathcal{F}'| = \#\text{subsets } F_i \in \mathcal{F}' \leq s$
in holds that $|\partial(\mathcal{F}')| = \#\text{unique neighbors } V_j \geq \delta |\mathcal{F}'|$

<u>Ex</u>

$w \vee x \vee y$
$\bar{u} \vee x$
$u \vee \bar{x}$

$x \vee \bar{y}$
$x \vee \bar{z}$
$\bar{x} \vee y \vee z$

$x \vee y$
$x \vee z$
$\bar{x} \vee \bar{y} \vee \bar{z}$



$$\mathcal{E} = \{\bar{y} \vee z\}$$

<u>Edge (F_1, V_1)</u> Adversary wins. Play any total assignment α_1 extending $\rho_1 = \{u \mapsto \bot, x \mapsto \top, y \mapsto \bot\}$
Flipping w or y cannot satisfy $u \vee \bar{x}$

<u>Edge (F_1, V_2)</u> Adversary again wins by playing any extension α_2 of $\rho_2 = \{u \mapsto \bot, w \mapsto \bot, y \mapsto \bot, z \mapsto \bot\}$
Satisfier cannot flip y because of $\mathcal{E}$
But $F_2 \restriction_{\{\bar{y}, \bar{z}\}} = x \wedge \bar{x}$

<u>Edge (F_2, V_2)</u> Satisfier wins. Given any α_3 s.t. $\alpha_3(\mathcal{E}) = T$, set $\alpha'(x) = \alpha_3(y \vee z)$ and leave other variables unchanged

Say that CNF formula $\mathcal{F}$ over variables V ADMITS AN $(s, \delta, \mathcal{E})$-RESOLUTION EXPANDER if there is a partition of the clauses $\mathcal{F} = \mathcal{E} \cup \bigcup_{j=1}^{m} F_j$ and division of the variables $V = \bigcup_{j=1}^{n} V_j$ such that the resulting $(\mathcal{F}, V)_{\mathcal{E}}$-graph is an $(s, \delta, \mathcal{E})$-resolution expander.

Then this is sufficient to prove resolution width lower bounds

<u>THEOREM (ESSENTIALLY [BW01], BUT FORMULATED AS IN [AIN20])</u>
If a CNF formula $\mathcal{F}$ admits an $(s, \delta, \mathcal{E})$-resolution expander with overlap ℓ, then $\boxed{W(\mathcal{F} \vdash \bot) > \frac{\delta s}{2\ell}}$

What we want to do now:
(a) Prove this theorem
(b) Show how PHP and Tseitin lower bounds immediately follow

For the proof, define "progress measure" $\mu : \{\text{clauses}\} \to \mathbb{N}_0$ that assesses how hard it is to derive a clause

PROPERTY A: For axiom clause $A \in \mathcal{F}$ $\mu(A) = O(1)$
PROPERTY B: For $\frac{C \vee x \quad D \vee \bar{x}}{C \vee D}$ $\boxed{\mu(C \vee D) \leq \mu(C \vee x) + \mu(D \vee \bar{x})}$
PROPERTY C: For empty clause $\bot$ $\mu(\bot) > s$.

From this, immediately get:

CLAIM D

In any resolution refutation $\pi : \mathcal{F} \vdash \bot$ there is a clause $C \in \pi$ with $\mu(C) \in (s/2, s]$

The theorem then follows from combining this with:

CLAIM E

Any clause C with $\mu(C) = \sigma \leq s$ has width $W(C) \geq \delta\sigma / \ell$

Now, let's fill in details

Sets of clauses F imply clause C, $F \models C$, if $\alpha(F) = T$ implies $\alpha(C) = T$

Given $(\mathcal{F}, V)_E$ - graph, define

$$\boxed{\mu(C) = \min\{ |\mathcal{F}'| : \wedge_{F \in \mathcal{F}'} F \wedge E \models C \}}$$

i.e., size of smallest collection of clause sets F_i on left-hand side that together with E imply C

Let us verify properties

(A) $A \in \mathcal{F}$ means $A \in E \Rightarrow \mu(A) = 0$

$A \in F_i \Rightarrow \mu(A) \leq 1$

(B) Suppose $\left.\begin{array}{l} \mathcal{F}_1 \wedge E \models C \vee x \\ \mathcal{F}_2 \wedge E \models D \vee \bar{x} \end{array}\right\}$ so $\mu(C \vee D) \leq \mu(C \vee x) + \mu(D \vee \bar{x})$

Then $(\mathcal{F}_1 \wedge \mathcal{F}_2) \wedge E \models C \vee D$

(c) Suppose $\mu(\perp) \leq s$. Then $\exists \mathcal{F}' \subseteq \mathcal{F}, |\mathcal{F}'| \leq s$, such that $\bigwedge_{F \in \mathcal{F}'} F \wedge E \models \perp$, i.e., $\bigwedge_{F \in \mathcal{F}'} F \wedge E$ is unsatisfiable. We show for any $\mathcal{F}' \subseteq \mathcal{F}$, $|\mathcal{F}'| = s$, that $\bigwedge_{F \in \mathcal{F}'} F \wedge E$ is satisfiable, so $\mu(\perp) > s$. Fix any such $\mathcal{F}', |\mathcal{F}'| = s$

WLB VII

By expansion $|\partial(\mathcal{F}')| \geq \delta |\mathcal{F}'| > 0$.
i.e., $\exists$ right vertex set V_s and left vertex set F_s (possibly after relabelling) such that V_s unique neighbour of F_s, i.e.

$$V_s \in N(F_s) \setminus N\left(\bigcup_{j=1}^{s-1} F_j\right)$$

By the same argument, find

$$V_{s-1} \in N(F_{s-1}) \setminus N\left(\bigcup_{j=1}^{s-2} F_j\right)$$

$$V_{s-2} \in N(F_{s-2}) \setminus N\left(\bigcup_{j=1}^{s-3} F_j\right)$$

etcetera – referred to as PEELING ARGUMENT
For $i = 1, 2, \ldots, s$

$$\boxed{V_i \in N(F_i) \setminus N\left(\bigcup_{j=1}^{i-1} F_j\right)}$$

V_i is not a neighbour of any F_j for $j < i$.

Now take any α_0 s.t. $\alpha_0(E) = T$ (which exists, since E should be satisfiable. Play Satisfier strategy on $F_1 \leftrightarrow V_1$ if needed to get α_1 s.t. $\alpha_1(F_1 \wedge E) = T$.
Now play Satisfier strategy on $F_2 \leftrightarrow V_2$ if needed to get α_2 s.t. $\alpha_2(F_2 \wedge E_2) = T$. But note that $V_2 \cap Vars(F_1) = \emptyset$, so $\alpha_2(F_1) = \alpha_1(F_1) = T$ and $\alpha_2(F_1 \wedge F_2 \wedge E) = T$

By induction, for $F_i \longleftrightarrow V_i$ have α_{i-1} s.t. $\alpha_{i-1}(\bigwedge_{j=1}^{i-1} F_j \wedge E) = T$ and playing Satisfier strategy on $F_i \longleftrightarrow V_i$ yields α_i satisfying $\bigwedge_{j=1}^{i} F_j \wedge E$. This shows that $\bigwedge_{j=1}^{s} F_j \wedge E$ satisfiable as claimed.

It remains to prove Claim E, i.e., that $\mu(C) = \sigma \leq s$ implies $W(C) \geq \delta\sigma/\ell$.

Fix $\mathcal{F}_C \subseteq \mathcal{F}$ witnessing that $\mu(C) = |\mathcal{F}_C| = \sigma$

Then $\bigwedge_{F \in \mathcal{F}_C} \wedge E \models C$ $\quad (\dagger)$

but for all $\mathcal{F}' \subsetneq \mathcal{F}_C$ it holds that

$$\bigwedge_{F \in \mathcal{F}'} \wedge E \not\models C \qquad (\ddagger)$$

Claim E now follows from another claim

CLAIM F For all $V \in \partial(\mathcal{F}_C)$ it holds that $V \cap Vars(C) \neq \emptyset$

Given claim F, since every variable x occurs in at most ℓ sets V, we get $W(C) \geq |\partial(\mathcal{F}_C)|/\ell \geq$
$\geq \delta\sigma/\ell$

<u>Proof of Claim F</u> Fix $V \in \partial(\mathcal{F}_C)$ and its unique neighbour $F_V \in \mathcal{F}_C$. By $(\ddagger)$ there exists α s.t. $\alpha(\bigwedge_{F \in \mathcal{F}_C \setminus \{F_V\}} F \wedge E) = T$ but $\alpha(C) = \bot$

Satisfier strategy on $F_V \longleftrightarrow V$ yields α' such that $\alpha'(\bigwedge_{F \in \mathcal{F}_C} \wedge E) = T$. If $V \cap Vars(C) = \emptyset$, then $\alpha'(C) = \bot$, but that contradicts $(\dagger)$.

Now we can get width lower bounds (and hence length lower bounds) for Tseitin formulas and pigeonhole principle formulas

TSEITIN FORMULAS

Bounded-degree undirected graph $G = (V, E)$
Charge function $\chi : V \to \{0,1\}$ such that $\sum_{v \in V} \chi(v)$ odd number

$PARITY_{v,\chi}$ = Clauses encoding $\sum_{e \ni v} x_e \equiv \chi(v) \pmod 2$
$Ts(G,\chi) = \bigwedge_{v \in V} PARITY_{v,\chi}$

Modifying our notion of edge expander slightly (only makes them easier to find)

DEF G is an (s,δ)-EDGE EXPANDER if $\forall V' \subseteq V$, $|V'| \le s$ it holds that $|\mathcal{E}(V', V \setminus V')| \ge \delta |V'|$, where $\mathcal{E}(U,W) = \{(u,w) \in E \mid u \in U, w \in W\}$

THEOREM If G is an (s,δ)-edge expander and χ is odd, then $W(Ts(G,\chi) \vdash \bot) > \delta s / 2$.

Proof sketch Left vertex sets $F_v := PARITY_{v,\chi}$. $E = \emptyset$. Every variable x_e, $e \in E$ forms singleton set $V_e = \{x_e\}$, so overlap $ol(V^\circ) = 1$

If G is (s,δ)-edge expander, then $(\mathcal{F}, V)_E$ is resolution expander with same parameters — $\partial(F')$ are precisely edges leaving vertex set. Satisfier can win on any $F_v \leftrightarrow x_e$ by flipping x_e to satisfy parity $\boxtimes$

PIGEONHOLE PRINCIPLE FORMULAS

WLB X

Define formulas over general bipartite graphs $G = (\mathcal{U} \cup V, E)$

PIGEON AXIOMS	$\bigvee_{v \in N(u)} x_{u,v}$	$u \in \mathcal{U}$
HOLE AXIOMS	$\overline{x}_{u,v} \vee \overline{x}_{u',v}$	$v \in V$, $u \neq u' \in N(v)$
FUNCTIONALITY AXIOMS	$\overline{x}_{u,v} \vee \overline{x}_{u,v'}$	$u \in \mathcal{U}$, $v \neq v' \in N(u)$
ONTO AXIOMS	$\bigvee_{u \in N(v)} x_{u,v}$	$v \in V$

Conjunction of all clauses yields formula $\boxed{\text{Onto-FPHP}(G)}$

PHP formulas from before are $\text{Onto-FPHP}(K_{n+1,n})$

Let $\rho_G = \{ x_{u,v} \mapsto \bot \mid u \in \mathcal{U}, v \in V, (u,v) \notin E \}$

Then $\text{Onto-FPHP}(K_{n+1,n}) \restriction_{\rho_G} = \text{Onto-FPHP}(G)$

So sufficient to prove lower bounds for constant-left-degree graphs — # variables $\Theta(n)$

- For every pigeon u, pick uniformly and independently at random d holes for d suitable constant (≈ 5 or so)
- For any isolated hole v, pick one pigeon u_v

Yields bipartite (s, δ)-boundary expander for $\delta > 0$ and $s = \Omega(n)$ with matching from V to $\mathcal{U}$

THEOREM If $G = (U \dot\cup V, E)$ is bipartite (s, δ)-boundary expander with full matching of V into U*, then $W(\text{Onto-FPHP}(G) \vdash \bot) > \delta s/2$

(*) Condition can be significantly relaxed, but we keep it for purposes of exposition

Proof sketch Construct $(\mathcal{F}, \mathcal{V})_E$-graph as follows

- Left sets $F_u = \{ \bigvee_{v \in N(u)} x_{u,v} \}$
- right sets $V_v = \{ x_{u,v} \mid u \in N(v) \}$
  so $\mathrm{ol}(\mathcal{V}) = 1$
- filtering set $\mathcal{E}$ = all hole axioms, functionality axioms, and onto axioms

If G is (s, δ)-boundary expander, then $(\mathcal{F}, \mathcal{V})_E$ resolution expander with same parameters.

Graphs are easily verified to be isomorphic

Suppose Adversary and Satisfier play on edge (F_u, V_v). Then α is full matching of V into U, since filtering set satisfied.

If $\alpha(F_u) = T$, Satisfier does nothing

Otherwise, change α on V_v so that

$\alpha(x_{u,v}) = T$ $\alpha(x_{u',v}) = \bot$ for $u' \neq u$.

This is new full matching of V into U, so filtering set satisfied $\boxtimes$

Since Onto-FPHP(G) has $\Theta(n)$ variables if G has constant left degree, linear width lower bound $\Rightarrow$ exponential length lower bound

By restriction argument, exponential lower bound holds for $\mathcal{K}_{n+1,n}$ for all PHP flavours for resolution.

Most resolution length lower bounds can be established with size-width relation — but not all

Note that for k-clique formulas the resolution width is k, so get nothing for range of parameters we are interested in ($\ll \sqrt{n}$)