$\boxed{\text{RESOLUTION}}$

Last time we saw

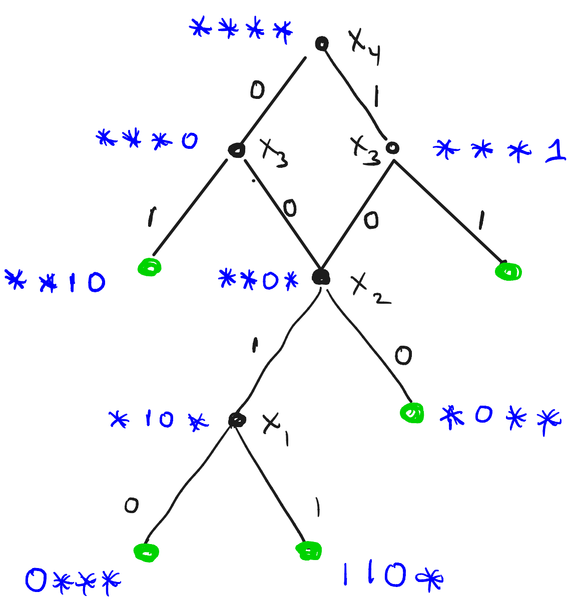
- RES is SOUND & COMPLETE

- tree-RES refutation Π for f $\approx$ Decision tree for solving search_f

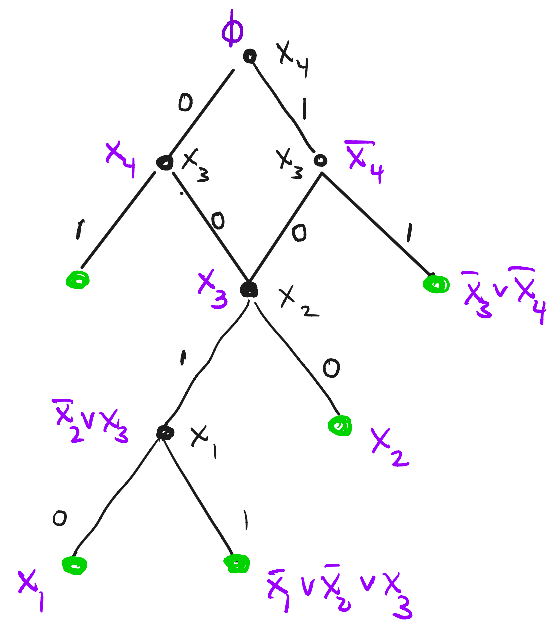
- (DAG)-RES refutation Π for f $\approx$ Prover/Delayer DAGs (or RES-DAGs) for solving search_f

Ex 2 $\boxed{\text{Prover-Delayer Example}}$

$$f = x_1 \wedge x_2 \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_3) \wedge (\bar{x}_3 \vee x_4) \wedge (\bar{x}_3 \vee \bar{x}_4)$$



Prover-Delayer game



Res Refutation

Today:

1. Resolution Lower Bounds

2. Frege Systems

Resolution Lower Bounds via Width

I. Width LBs $\longrightarrow$ Size LBs via restriction argument

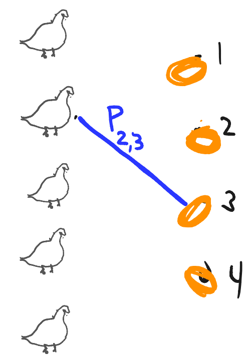
or general size-width tradeoff

II. Width LBs : via expansion of clause-variable graph of F

Propositional Pigeonhole Principle

$$PHP_n^{n+1}: \underbrace{\bigwedge_{i=1}^{n+1} \left(P_{i,1} \vee P_{i,2} \vee \dots \vee P_{i,n}\right)}_{\text{Pigeon clauses}} \wedge \underbrace{\bigwedge_{\substack{i_1, i_2 \le n+1 \\ j \le n}} \left(\overline{P_{i_1,j}} \vee \overline{P_{i_2,j}}\right)}_{\text{Hole clauses (one-to-one)}}$$

$$\wedge \underbrace{\bigwedge_{\substack{i \\ j_1 \neq j_2}} \left(\overline{P_{i,j_1}} \vee \overline{P_{i,j_2}}\right)}_{\text{functional}} \wedge \underbrace{\bigwedge_{j=1}^{n} \left(P_{1,j} \vee P_{2,j} \vee \dots \vee P_{n+1,j}\right)}_{\text{onto}}$$

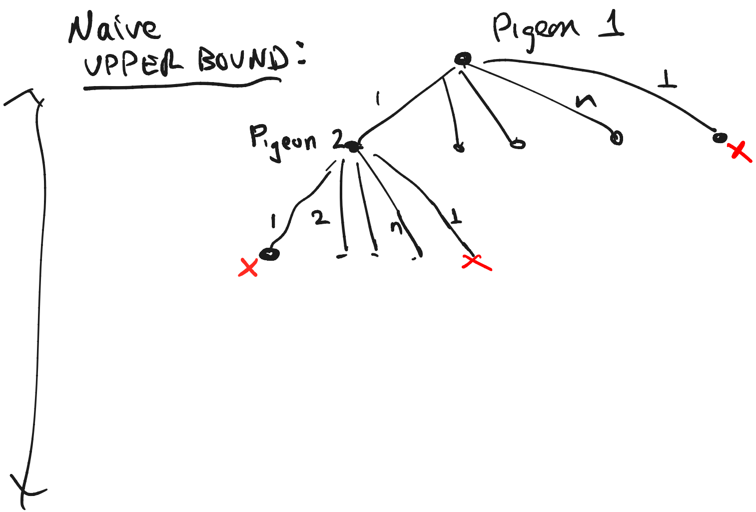


Res Lower Bounds for PHP : Warmup Tree-Resolution

Show any decision tree for search_{PHP} requires size $2^{\Omega(n)}$

Q: Is this tight for tree-like Resolution?

Naive UPPER BOUND:



ht $O(n)$

fanout $O(n)$ so $n^n \sim 2^{n \lg n}$

Exercise:

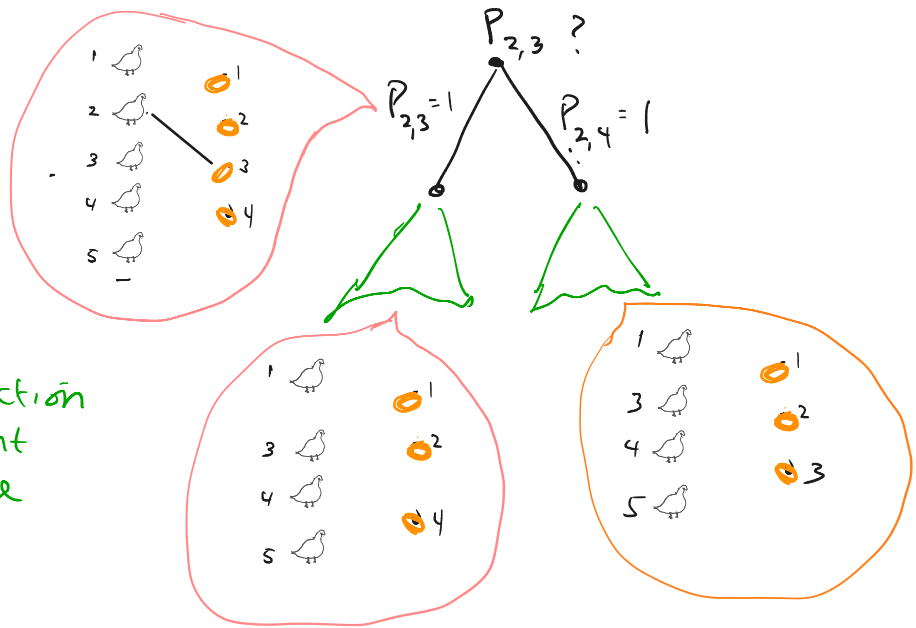
Show Res DAG (Van Gelder) can solve search in size $2^{O(n)}$

Res Lower Bounds for PHP: Warmup Tree-Resolution

Theorem

Any decision tree solving $\text{search}_{PHP_n^{n+1}}$ requires $2^{\Omega(n)}$ size.

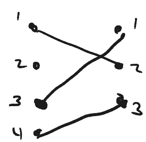
To Prove Theorem: Prove by induction on n that any decision tree for $\text{Search}_{PHP_n^{n+1}}$ that gives correct answers for all cta's has size 2^n.



By induction left and right subtrees have size 2^{n-1}

RES LOWER BOUNDS FOR PHP (The general case)

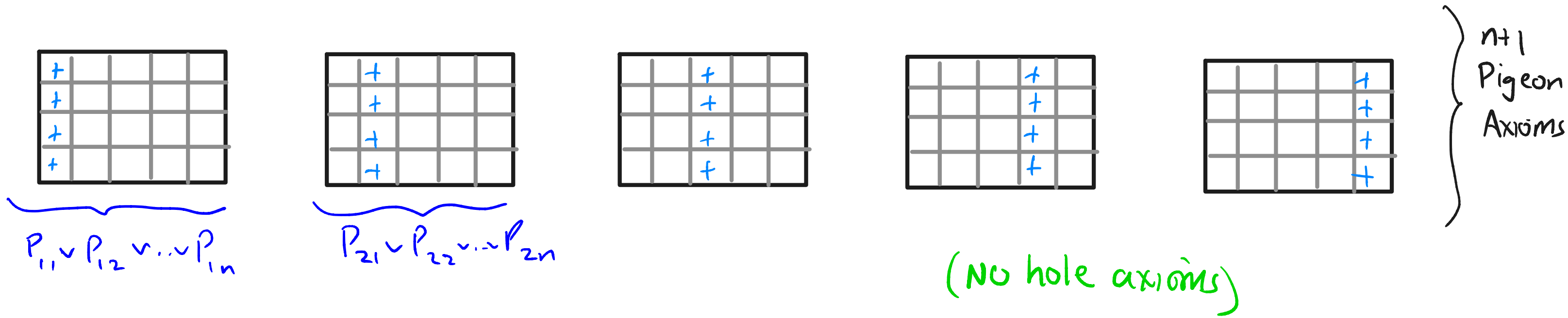
Critical Truth Assignments: $n-1$ of the n pigeons mapped 1-1 to the $n-1$ holes and the leftover pigeon unmapped.



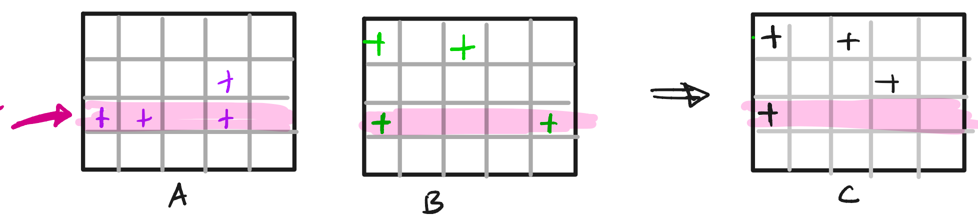
← this is a 2-cta since pigeon 2 unmapped

First we will transform RES refutations of PHP into a nice combinatorial form.

Monotone Transformation of PHP^{n+1}_n



Monotone Rule: pick a hole (row) j

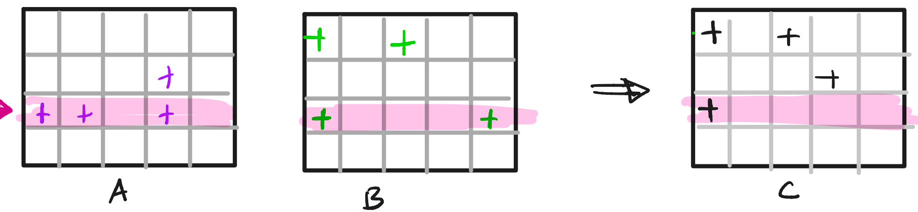


Lemma Any size-S RES refutation of PHP^m_n can be transformed into a monotone refutation of size $O(S)$, and vice-versa.

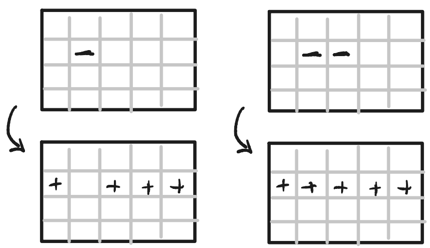
Monotone Transformation of PHP

Monotone Rule:

pick a hole (row) j

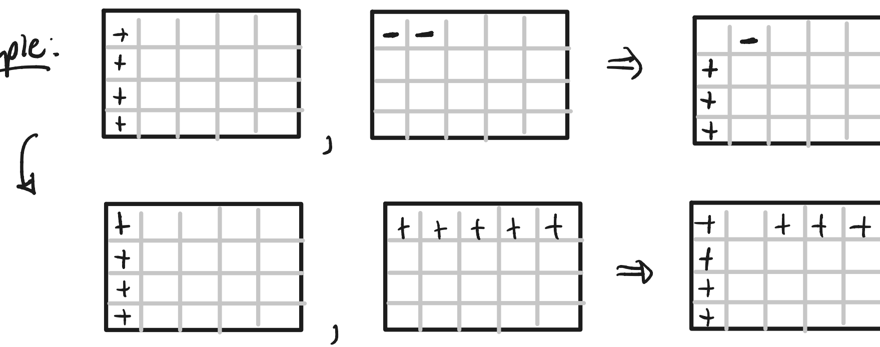


1. Convert each clause to monotone clause



2. Show any RES step in Π can be simulated by monotone rules in Π_{monotone}

Example:



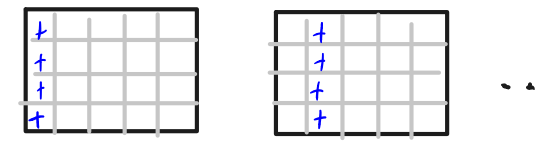
$\therefore$ Suffices to prove LB for monotone refutations

Playing With Monotone Refutations

UB strategy:

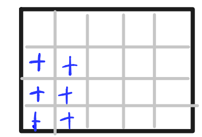
0. start with all $n \times 1$ all-$+$ subrectangles

n clauses



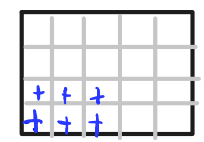
1. Remove hole n : generate all $(n-1) \times 2$ subrectangles on holes $1 \ldots n-1$

$\binom{n}{2}$ clauses



2. Remove hole $n-1$: generate all $(n-2) \times 2$ subrectangles on holes $1 \ldots n-2$

$\binom{n}{3}$ clauses



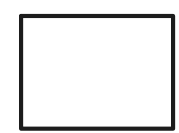
⋮

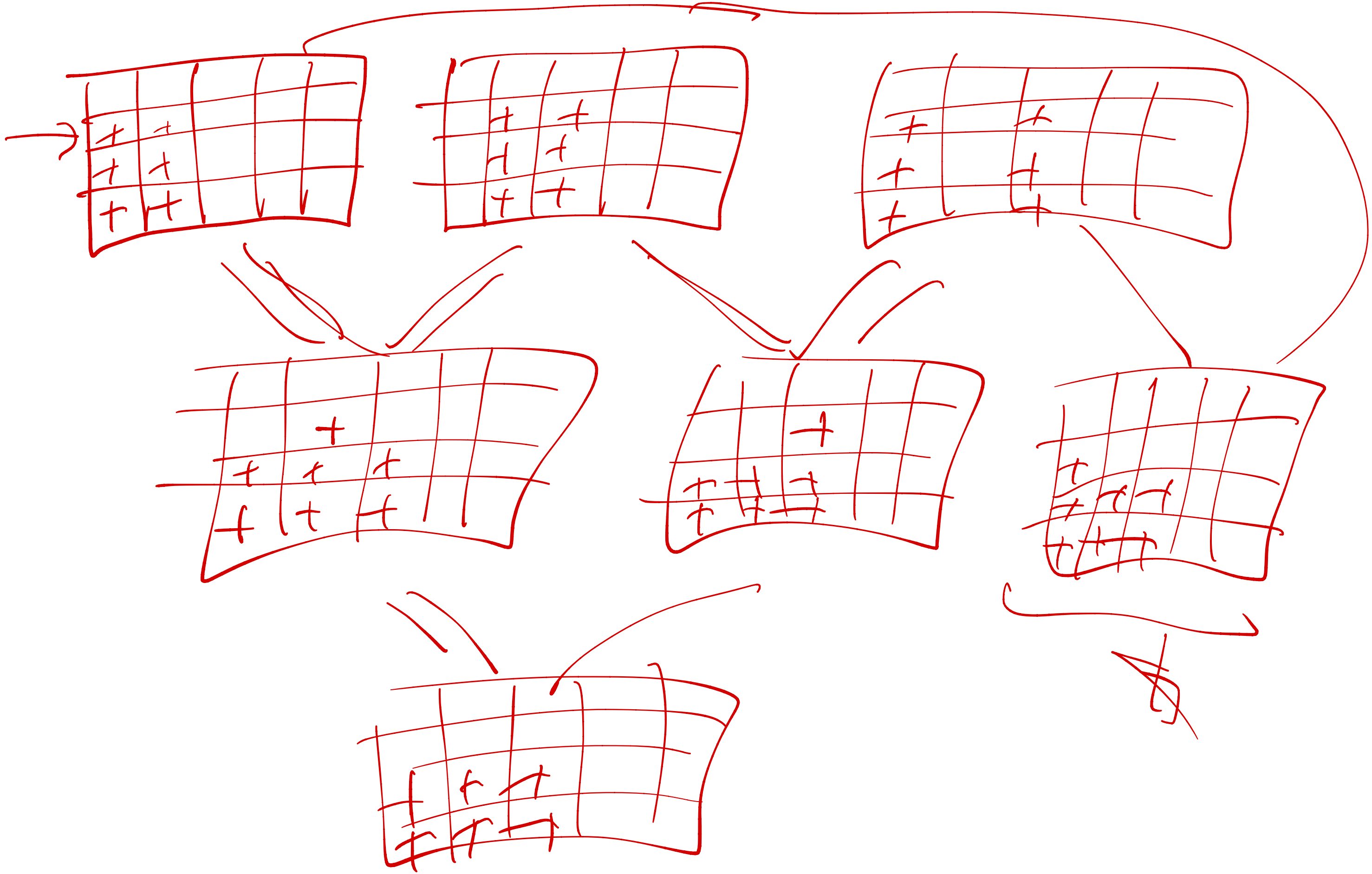
$n-1$. Remove hole 2 : generate all $1 \times n$ subrectangles on holes $\underline{1}$

$\binom{n}{n-1}$

n : Remove hole 1 : generate empty clause

$\binom{n}{0}$ clauses





PHP Lower Bound for Monotone Refutations

Theorem Any monotone refutation of PHP^{n+1}_n requires size $\exp(\Omega(n))$

PLAN:

0. Assume Π is monotone refutation of size S.

1. apply a random restriction ρ to Π so that $\Pi|_\rho$ is still a monotone refutation of $PHP^{n'+1}_{n'}$, where $n' = O(n)$ and width of every clause in $\Pi|_\rho$ is small — Lemma 1

2. (Wide Clause Lemma): Any monotone refutation of $PHP^{n'+1}_{n'}$ requires large width. $\#$ — Lemma 2

Lemma 1 Assume Π has size $S < 2^{n/20}$. Then $\exists$ 1-1 partial restriction ρ mapping εn pigeons to holes such that $\text{width}(\Pi|_\rho) \leq n^2/10$

Proof Let $t = n^2/10$. Define a wide clause as one of width $\geq t$.

- Apply a restriction ρ such that $\mathcal{T}(\Pi)|_\rho$ has width $\leq t$:

  On average setting a single variable $P_{i,j}$ to 1 will set $\geq S/10$ wide clauses to 1.

  Pick P_{ij} achieving at least the avg & set it to 1, & set $P_{i,j'} = 0 \; \forall j' \neq i$, $P_{i',j} = 0 \; \forall i' \neq i$

  Left with $\leq 9S/10$ wide clauses.

  Repeat iteratively $\log_{10/9} S$ times to set all wide clauses in $\mathcal{T}(\Pi)$ to 1.

- Left with a sound refutation of $PHP^{n'}_{n'-1}$ of width $< t = n^2/10$ where $n' \geq n - \underbrace{\log_{10/9} S}_{\varepsilon n} > .67n$

Lemma 2 (wide clause lemma for PHP)

Any monotone Res refutation of PHP_n^{n+1} has width $\geq 2n^2/9$.

Pf Let the complexity of a (monotone) clause C be the minimum number of clauses in PHP_n^{n+1} that implies C on all cta's

Complexity(pigeon-clause) = 1

Complexity(final empty clause) = $n+1$

By soundness, if $C_1, C_2 \to C_3$ then

$$\text{complexity}(C_3) \leq \text{complexity}(C_1) + \text{complexity}(C_2)$$

$\therefore \exists\, C^*$ in $\pi(\Pi)$ such that $\frac{n}{3} \leq \text{complexity}(C^*) \leq \frac{2n}{3}$

we will show: $\text{width}(C^*) \geq 2n^2/9$

Lemma 2 (wide clause lemma for PHP)

Any monotone Res refutation of PHP_n^{n+1} has width $\geq 2n^2/9$.

C^* = complex clause, $S \subseteq [n+1]$ = min subset of Pigeon clauses that implies C^*

IDEA: $\forall i$, all i-cta's satisfy all Pigeon-j clauses $j \neq i$

- so if $i \in S$, there must exist at least one i-cta α that falsifies C^*.
- and if $i \notin S$, then all i-cta's satisfy C^*

Using sensitivity of C^* wrt i-cta's, we will argue width$(C^*) = \Omega(n^2)$

Lemma 2 Any monotone Res refutation of PHP_n^{n+1} has width $\geq 2n^2/9$

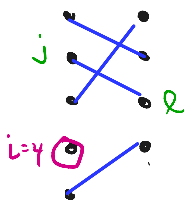
C^* = complex clause, $S \subseteq [n+1]$ = min subset of Pigeon clauses that implies C^*

IDEA: $\forall i$, all i-cta's satisfy all Pigeon-j clauses $j \neq i$

- so if $i \in S$, there must exist at least one i-cta α that falsifies C^*.
- and if $i \notin S$, then all i-cta's satisfy C^*

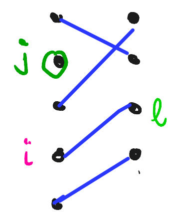
Let $i \in S$, α i-cta falsifying C^*:

α:



Let $j \notin S$. Let α_j be j-cta obtained from α by "toggling":

α_j:



Lemma 2 Any monotone Res refutation of PHP_n^{n+1} has width $\geq 2n^2/9$

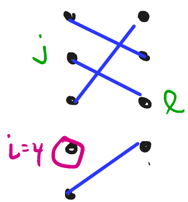
C^* = complex clause, $S \subseteq [n+1]$: min subset of Pigeon clauses that implies C^* $|S| = m$

IDEA : $\forall i$, all i-cta's satisfy all Pigeon-j clauses $j \neq i$

- so if $i \in S$, there must exist at least one i-cta α that falsifies C^*.
- and if $i \notin S$, then all i-cta's satisfy C^*

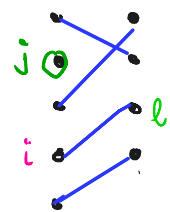
Let $i \in S$, α i-cta falsifying C^*:

α_i:



$\forall j \notin S$. Let α_j be j-cta obtained from α by "toggling":

α_j:



$\Rightarrow$ By monotonicity $P_{i,\ell}$ must occur in C^*

$\Rightarrow$ Running over all $j \notin S$ C^* must contain all vars $P_{i,\ell'}$ $\leftarrow n-m$

$\Rightarrow$ Running over all $i \in S$ C^* must contain $(n-m)\cdot n$ variables $\leftarrow m\cdot(n-m)$

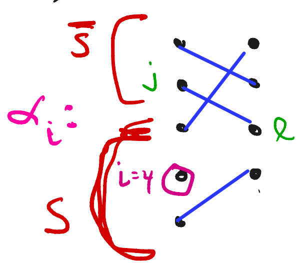
Lemma 2 Any monotone Res refutation of PHP^{n+1}_{n} has width $\geq 2n^2/9$

C^* = complex clause, $S \subseteq [n+1]$: min subset of Pigeon clauses that implies C^* $|S| = m$

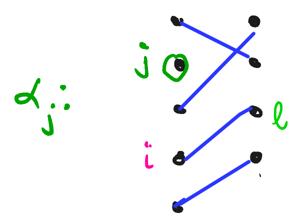
IDEA: $\forall i$, all i-cta's satisfy all Pigeon-j clauses $j \neq i$

- so if $i \in S$, there must exist at least one i-cta α that falsifies C^*.
- and if $i \notin S$, then all i-cta's satisfy C^*

Let $i \in S$, α i-cta falsifying C^*:



$\forall j \notin S$. Let α_j be j-cta obtained from α by "toggling":



$\Rightarrow$ By monotonicity $P_{i,\ell}$ must occur in C^*

$\Rightarrow$ Running over all $j \notin S$ C^* must contain all vars $P_{j,\ell'}$ $\leftarrow n-m$

$\Rightarrow$ Running over all $i \in S$ C^* must contain $(n-m)\cdot n$ variables $\leftarrow m\cdot(n-m)$

Resolution Lower Bounds

① Width LBs → Size LBs via restriction argument
or general size-width tradeoff

A second way to reduce size LBs to width LBs:
Ben-Sasson-Wigderson Size-Width Tradeoff for Resolution

Theorem [BW01] Let F be unsat kCNF on n vars. Then

1. $\text{Tree-Res-Size}(F) \geq 2^{\text{Res-Width}(F) - k}$

2. $\text{Res-Size}(F) \geq 2^{\Omega(\text{Res-width}(F) - k)^2/n}$

gives exponential Lower Bounds for many UNSAT formulas simply by expansion

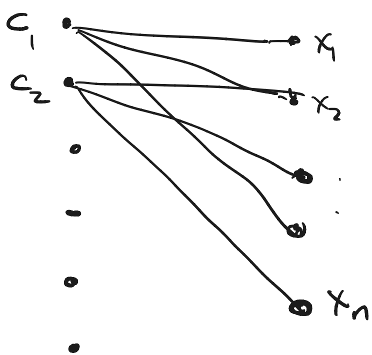
Resolution Lower Bounds for random KSAT

Theorem [BW01] Let F be unsat KCNF on n vars. Then

1. $\text{Tree-Res-Size}(F) \geq 2^{\text{Res-width}(F) - k}$

2. $\text{Res-Size}(F) \geq 2^{\Omega(\text{Res-width}(F) - k)^2 / n}$

$f \sim \mathcal{F}(\Delta, n, k)$: pick $m = \Delta n$ clauses of width k. For $\Delta > 0$ suff large, whp $f \sim \mathcal{F}(\Delta, n, k)$ UNSAT



1. For $f \sim \mathcal{F}(\Delta, n, k)$ any Resolution dag requires Linear width

   Follows directly from fact that clause-variable graph is a good boundary expander whp.

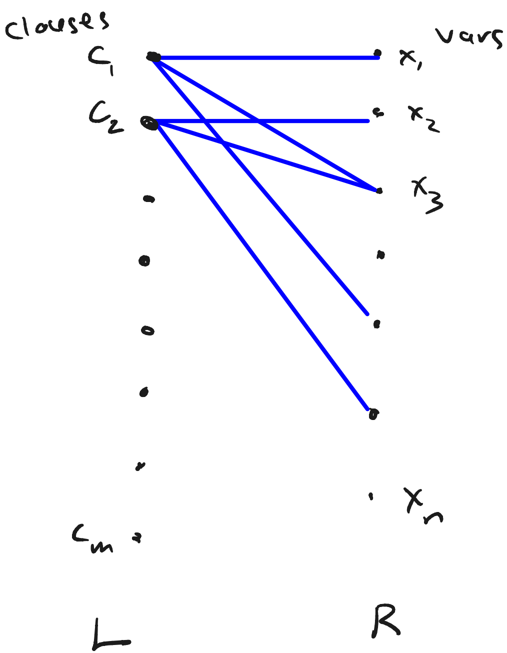
2. Ben-Sasson, Wigderson: Small size $\Rightarrow$ small width

   s $\quad\quad$ $\sqrt{n \log s}$

Proving Lower Bounds from Expansion

Let $F = C_1 \wedge C_2 \wedge \cdots \wedge C_m$

Clause-Variable graph G_F:



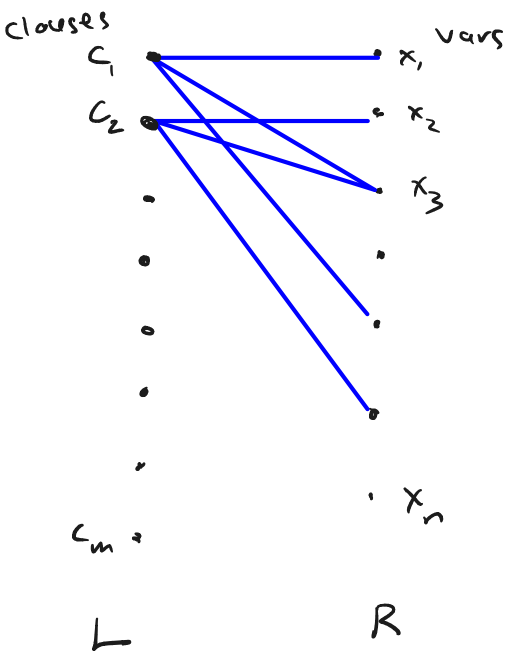
<u>Defn</u> G_F has (ε, δ)-expansion if $\forall S \subseteq L$, $|S| \leq \varepsilon n$, $|N(S)| \geq \delta \cdot |S|$

<u>Defn</u> G_F has (ε, δ)-boundary expansion if $\forall S \subseteq L$, $|S| \leq \varepsilon n$, $|\#\text{unique nbrs in } N(S)| \geq \delta \cdot |S|$

Proving Lower Bounds from Expansion

Let $F = C_1 \wedge C_2 \wedge \cdots \wedge C_m$

Clause-Variable graph $\mathcal{G}_F$:



Defn $\mathcal{G}_F$ has (ε, δ)-expansion if $\forall S \subseteq L$, $|S| \le \varepsilon n$, $|N(S)| \ge \delta \cdot |S|$

Defn $\mathcal{G}_F$ has (ε, δ)-boundary expansion if $\forall S \subseteq L$, $|S| \le \varepsilon n$, $|\#\text{unique nbrs in } N(S)| \ge \delta \cdot |S|$

Claim Let $\mathcal{G}$ have degree d, expansion e then b = boundary expansion $\ge 2e - d$

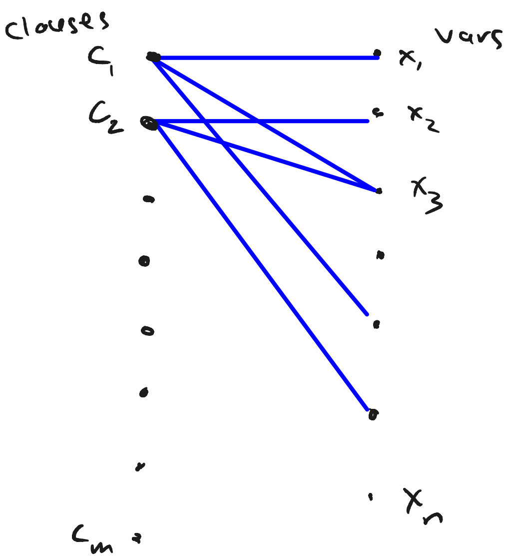
$$e \cdot |S| \le b \cdot |S| + \frac{d|S| - b|S|}{2}$$

$$b \ge 2e - d$$

Proving Lower Bounds from Expansion

Let $F = C_1 \wedge C_2 \wedge \dots \wedge C_m$

Clause-Variable graph G_F:



Claim: Let $0<\varepsilon<1$

If G_F has $(\varepsilon, O(1))$-boundary expansion, then $\text{RES-WIDTH}(F) = \Omega(n)$

Pf: Let C^* be first clause in refutation derived from $\geq \frac{n}{8}$ initial clauses.

$\therefore$ C^* derived from $\leq \frac{n}{4}$ " "

Let $S \subseteq [m]$, $\frac{n}{8} \leq |S| \leq \frac{n}{4}$ be clauses minimally implying C^*

All boundary vars of $\{C_i \mid i \in S\}$ must occur in C^*

$\therefore$ By boundary expansion, $\text{width}(C^*) = \Omega(n)$

Resolution Lower Bounds

Methods

① Width LBs $\longrightarrow$ Size LBs via restriction argument

or general size-width tradeoff

Width LBs : via expansion of clause-variable graph of F

② Feasible Interpolation $\longleftarrow$ we will discuss next class

RES UPPER BOUNDS FOR PHP^m_n

0. PHP^{m}_n : tree-like Res : $2^{\Theta(n^2)}$
   Res : $2^{\Theta(n)}$

1. The previous Resolution Lower bound still gives similar lower bound for the weak PHP, PHP^m_n, $m = n^2$

2. [Buss-P] show polysize Res refutations of PHP^m_n, $m \sim 2^{\sqrt{n}}$
   [Raz] proves near matching Res lower bound

3. [Maciel-P-Woods] : quasipoly size Res(polylog n) refutations of PHP^m_n, $m = 2n$
   (see also Paris-Wilkie-Woods)

OPEN Q's

1. Are there <u>polysize</u> Res(polylog n) refutations of PHP_n^{2n} ?

   or polysize Bounded-depth refutations of weak PHP ?

   Best Lower bounds : superpoly for Res$(\sqrt{\log n})$, PHP_n^{2n}

   Motivation : Res LBs for "NP $\not\subset$ P/poly"

Extra Slides (Not Covered)

Size S Res Refutations of PHP^m_n for $n < \frac{\log m \log S}{\log\log S}$ [Buss-P]

Let Pigeons $= [m]$, holes $= [n]$

Loop: Divide pigeons $[m]$ into blocks of size $\log S + 1$

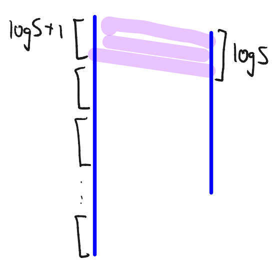
Case 1 Some block of pigeons maps to first $\log S$ holes.
If so, refute in size $\sim S$ and HALT

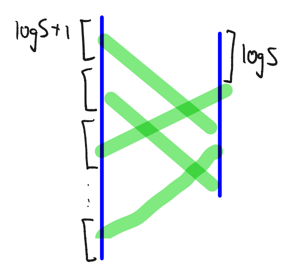
Case 2 Otherwise let each block of pigeons be a "super-pigeon" $P_{a,j} = \bigvee_{i \in Block(a)} P_{i,j}$

Each superpigeon maps to one of the last $n - \log S$ holes

So $|\text{superpigeons}| \approx \frac{m}{\log S}$ $\quad |\text{holes}| = n - \log S$

Repeat Loop with $\frac{m}{\log S}$ (super)pigeons, $n - \log S$ holes





Size S Res Refutations of PHP^m_n for $n < \frac{\log m \log S}{\log\log S}$

Let Pigeons $= [m]$, holes $= [n]$

Loop: Divide pigeons $[m]$ into blocks of size $\log S + 1$

Case 1 Some block of pigeons maps to first $\log S$ holes.
If so, refute in size $\sim S$ and HALT

Case 2 Otherwise Let each block of pigeons be a "super-pigeon" $P_{a,j} = \bigvee_{i \in Block(a)} P_{i,j}$

Each superpigeon maps to one of the last $n - \log S$ holes

so $|\text{superpigeons}| \approx \frac{m}{\log S}$ $\quad |\text{holes}| = n - \log S$

Repeat Loop with $\frac{m}{\log S}$ (super)pigeons, $n - \log S$ holes

Analysis: after $\frac{n}{\log S}$ iterations, need $m \geq 0$:

Set $n = \frac{\log m \log S}{\log\log S}$

$$\frac{m}{(\log S + 1)^{\frac{n}{\log S}}} \simeq \frac{\log m^{\frac{\log m}{\log\log m}}}{(\log S)^{\frac{n}{\log S}}} = \frac{\log m^{\frac{\log m}{\log\log m}}}{\log m^{\frac{\log\log S}{\log S}\frac{n}{\log\log m}}} = \frac{\log m^{\frac{\log m}{\log\log m}}}{\log m^{\frac{\log m}{\log\log m}}} = 1$$

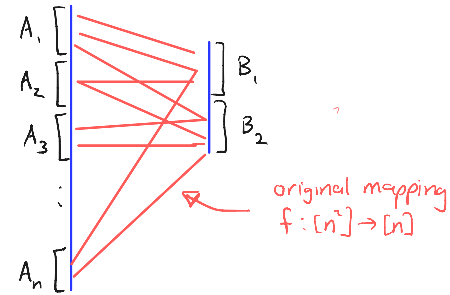
setting $S \cong \log m$ $\quad n = \frac{(\log m)^2}{\log\log m}$ $\quad$ so $m \sim 2^{\sqrt{n}}$, and proof of size $2^{O(\sqrt{n})}$

Quasi-poly Size Res(polylog n) Refutations of $PHP^{n^2}_n$

$\boxed{\text{Step 1}}$ (Reduce range) Let $A = [n^2]$, $B = [n]$

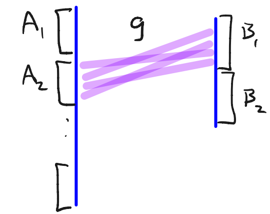
Partition A into n blocks $A_1, \dots, A_n$ each size n

Partition B into 2 blocks B_1, B_2 each size $\frac{n}{2}$



Case 1: Some A_i maps all pigeons in A_i to B_1

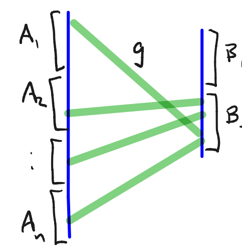
Then we have injective map $g: \underbrace{A_i}_{n} \to \underbrace{B_1}_{\frac{n}{2}}$



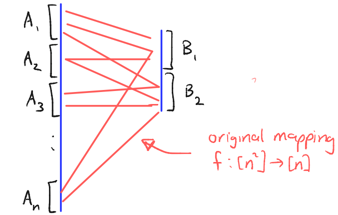
Case 2: $\forall i$ some pigeon in A_i maps to B_2

Then we have an injective map g from $[n]$ to B_2

$[n]$ = "superpigeons" Superpigeon $P_{r,s} = \bigvee_{\text{pigeons } i \text{ in } A_r} P_{i,\frac{n}{2}+s}$



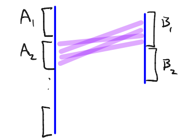
Quasi-poly Size Res(polylog n) Refutations of $PHP_n^{n^2}$



$\boxed{\text{Step 1}}$ (Reduce range) Let $A=[n^2]$, $B=[n]$

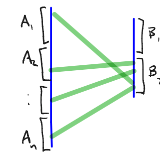
Partition A into n blocks $A_1,\dots,A_n$ each size n

Partition B into 2 blocks B_1, B_2 each size $\frac{n}{2}$



Case 1: Some A_i maps all pigeons in A_i to B_1: $g:\underbrace{A_i}_{n}\to\underbrace{B_1}_{\frac{n}{2}}$

Case 2: $\forall i$ some pigeon in A_i maps to B_2: $g:\underset{\text{superpigeons}}{[n]}\to B_2$



$\boxed{\text{Step 2}}$ (Amplify pigeons $n\to n^2$)

Define $h:[n^2]\to[\frac{n}{2}]$ by : $h(i)=k$ iff $\exists j\in[n]$ s.t. $f(i)=j$ and $g(j)=k$

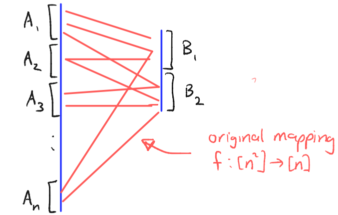
(h is injective, assuming both f, g are injective)

After steps ① + ② we have gone from injective $f:[n^2]\to[n]$ to injective $h:[n^2]\to[\frac{n}{2}]$

Repeat Steps ① + ② to obtain sequence of injective functions

$f_0:[n^2]\to[n]$, $f_1:[n^2]\to[\frac{n}{2}]$, $f_2:[n^2]\to[\frac{n}{4}]$, ... $f_{\log n}:[n^2]\to[1]$ ← #

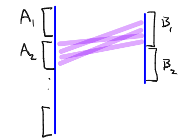
Quasi-poly Size Res(polylog n) Refutations of $PHP^{n^2}_n$



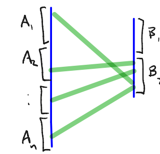
$\boxed{\text{Step 1}}$ (Reduce range) Let $A=[n^2]$, $B=[n]$

Partition A into n blocks $A_1,\dots,A_n$ each size n

Partition B into 2 blocks B_1, B_2 each size $\frac{n}{2}$



Case 1: Some A_i maps all pigeons in A_i to B_1: $g: \underbrace{A_i}_{n} \to \underbrace{B_1}_{\frac{n}{2}}$



Case 2: $\forall i$ some pigeon in A_i maps to B_2: $g: \underset{\text{superpigeons}}{[n]} \longrightarrow B_2$

$\boxed{\text{Step 2}}$ (Amplify pigeons $n \to n^2$)

Define $h: [n^2] \to [\frac{n}{2}]$ by: $h(i)=k$ iff $\exists j \in [n]$ s.t. $f(i)=j$ and $g(j)=k$

(h is injective, assuming both f, g are injective)

Complexity of Refutation

* At each iteration, each "super-pigeon" is a polylog n-width DNF, size quasipoly(n)

  So proof starts with axioms $PHP^{n^2}_n(f)$

  Step 1: Derive axioms $PHP^{n}_{\frac{n}{2}}(g)$ where vars $Q_{ij} \in$ polylog n-DNF

  Step 2: Derive axioms $PHP^{n^2}_{\frac{n}{2}}(h)$ (where vars $\in$ PolylognDNF) from $PHP^{n^2}_n(f)$, $PHP^{n}_{\frac{n}{2}}(g)$