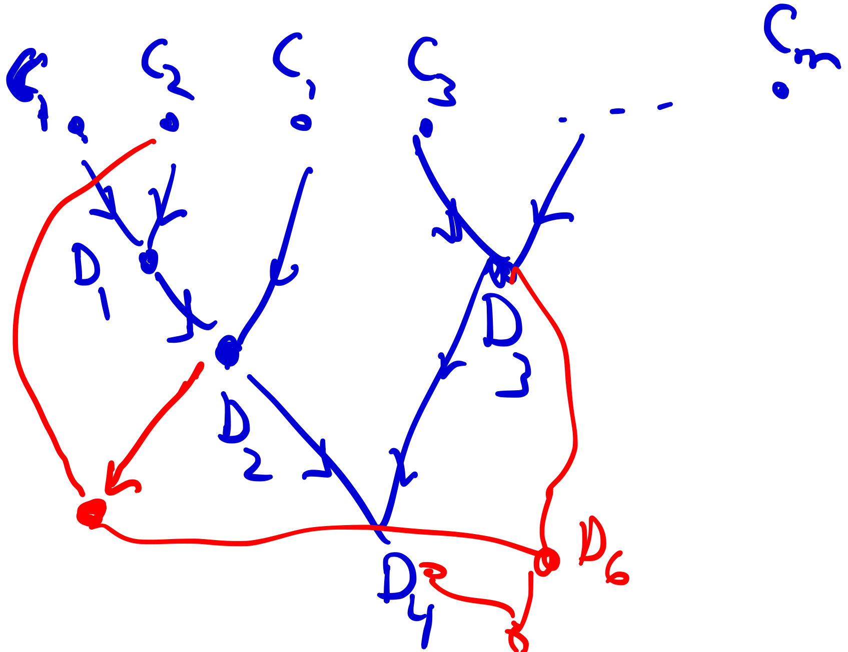
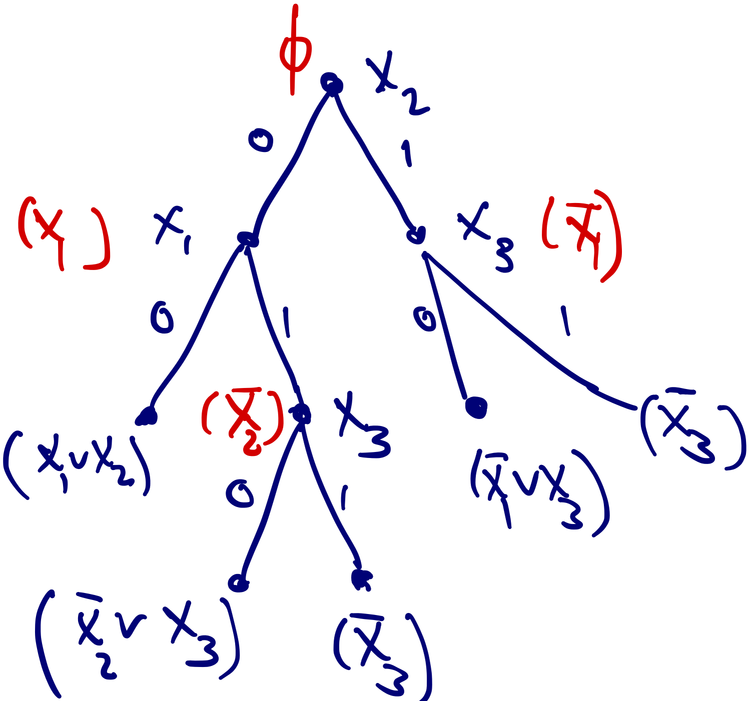
General [Dag] vs Tree Resolution

Tree: each derived clause is used at most once



DPLL = Tree Resolution

$$(x_1 \vee x_2)(\bar{x}_1 \vee x_3)(\bar{x}_2 \vee x_3)(\bar{x}_3)$$



Resolution LBs

Tree Resolution
Regular Resolution – Tseitin
general Resolution – Haken '85
Ben-Sasson, Wigderson ⟷ size vs width

Urquhart
Chvatal Szemeredi
⋮

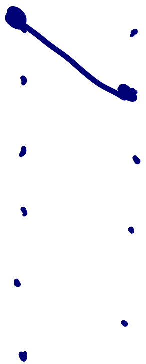
Hard Examples for Resolution

(1) $\neg PHP^{n}_{n-1}$ variables $P_{i,j}$ $i \in [n]$, $j \in [n-1]$

Clauses (1) Pigeon clauses

$$\left(P_{i,1} \vee \dots \vee P_{i,n-1} \right) \quad \forall i \in [n]$$

n=6



(2) Hole Clauses

$$\left(\neg P_{i_1,j} \vee \neg P_{i_2,j} \right) \quad \forall i_1, i_2 \in [n],\ i_1 \neq i_2,\ \forall j \in [n-1]$$

clauses $O(n^3)$

(2) Random KCNF formulas $(K=3)$
(m, n)

$f \sim \mathcal{U}(m,n)$: pick m 3-clauses over $x_1 \dots x_n$

$$\binom{n}{3} 8$$

$m > 20n \Rightarrow f \sim \mathcal{U}(m,n)$ unsat whp

<u>Thm</u> whp $f \sim \mathcal{U}(20n, n)$
f requires $\exp(\Omega(n))$ size Res refutations

Methods

1. Restriction Method
   a. apply a restriction which sets some of the variables to 0/1 s.t. under restriction, resulting proof is narrow
   b. wide clause Lemma: any Res ref of F_n requires a wide clause
2. Ben-Sasson-Wig
   a. If 3CNF f over n vars has size S Res ref, then it has one of width $\sqrt{n \log S}$

CSC 2429 - Proof Complexity
& applications

Intro: See Lecture slides
from Proof Complexity
tutorial

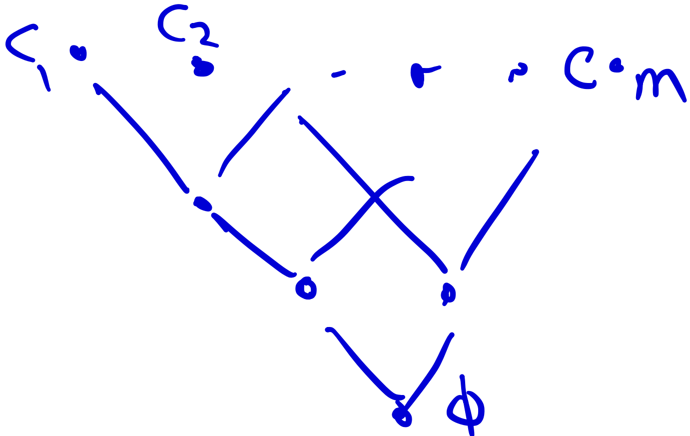
Resolution

proof system for proving UNSAT of CNF formulas

$f = C_1 \wedge C_2 \wedge \ldots \wedge C_m$

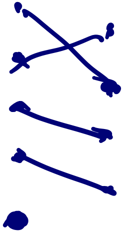
Rule (Resolution)

$$\frac{(x_1 \vee C) \quad (\bar{x}_1 \vee D)}{(C \vee D)}$$



proof size = # of clauses in the proof

Restriction Method for PHP^n_{n-1} LBs



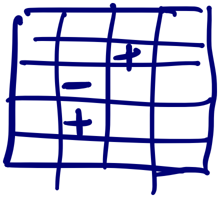
Defn a critical truth assignment α
map $n-1$ pigeons to $n-1$ holes (1-1, onto)
leave remaining pigeon out

$$n \cdot (n-1)!$$

we will write a clause as a matrix

$n-1$

n

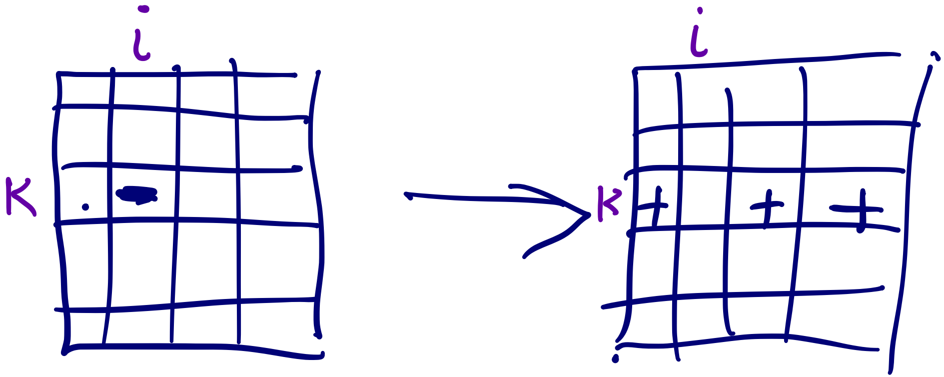


$$P_{23} \vee \overline{P}_{32} \vee \overline{P}_{42}$$

Conversion to Monotone:

Let P be a Res ref. for PHP^n_{n-1}.

In each clause, replace any negated literal $\neg P_{ik}$ by $\{P_{\ell k} \mid \ell \neq i\}$



<u>Claim</u> This translation is <u>sound</u> wrt all cta's

Restrictions:

set some pigeons 1-1, onto way to some holes

$$P_{ij} \to 1$$

$$P_{ij'} \to 0 \quad \forall j' \neq j$$

$$P_{i'j} \to 0 \quad \forall i' \neq i$$

Defn Let a (monotone) clause C be called fat if it contains $\geq \frac{n^3}{10}$ literals greedily choose restriction of this type to set all fat clauses to 1.

S

F

- On average, setting a single P_{ij} will set $\frac{F \cdot n^2}{10\,(n)(n-1)} \geq F/10$
- Pick any P_{ij} that achieves at least the avg
  set $P_{ij} \to 1$, $P_{i'j} \to 0$ $P_{ij'} \to 0$
- Apply this restriction to whole refutation
  will end up with a monotone Ref of $\neg PHP^{n-1}_{n-2}$, where # of wide clauses is $\leq 9F/10 \leq 9S/10$

- apply argument $\log_{10/9} S$ times then guaranteed to have set all wide clauses to 1.
- Left with a Res ref. (monotone) of $\neg PHP^{n'}_{n'-1}$ where

$$n' \geq n - \log_{\frac{10}{9}} S$$

for $S < 2^{n/20}$ $\quad n' > .671\, n$

This contradicts the following

<u>wide Clause lemma</u>

Any monotone Res Ref of $\neg PHP^{n}_{n-1}$ must have a clause with $\geq 2n^2/9$ literals.

$$\frac{2(n')^2}{9} > \frac{n^2}{10}$$

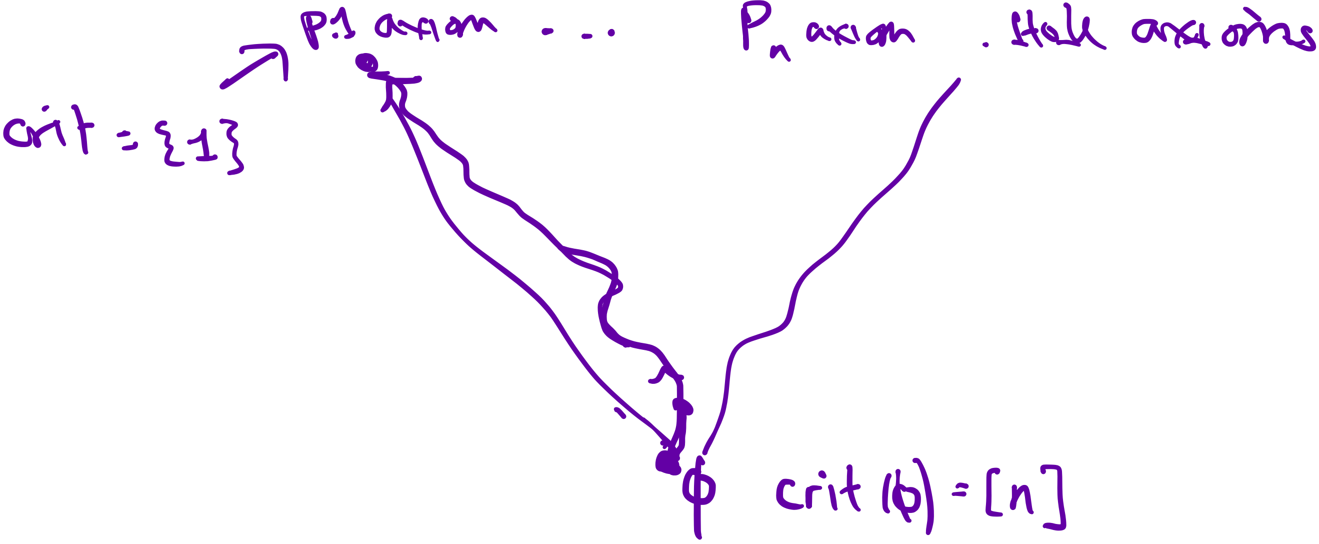
Proof of Wide Clause Lemma

Fix a proof P of PHP^n_{n-1}

For every clause/matrix C in P,

let $\quad crit(C) = \{ i \mid \exists$ i-cta α falsifying $C \}$

all of the cta's flow thru a unique path in P, from root clause to a pigeon axiom

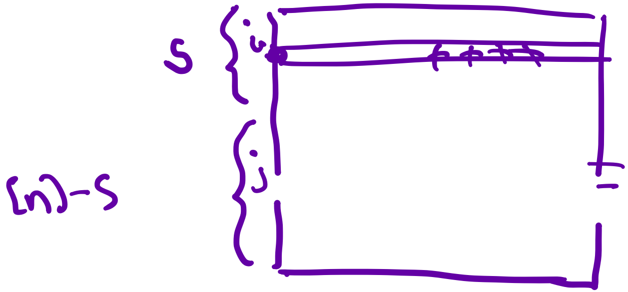


By soundness, if C_1 C_2 derive C_3

then $\text{crit}(C_1) \cup \text{crit}(C_2) \supseteq \text{crit}(C_3)$

so $\exists$ C^* s.t. $\frac{n}{3} \leq |\underbrace{\text{crit}(C^*)}_{S \subseteq [n]}| \leq \frac{2n}{3}$

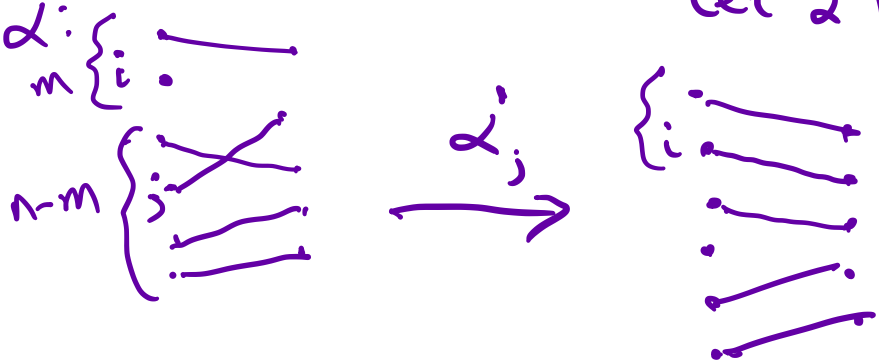
<u>Claim</u> C^* is wide. $|S| = m$, $S = \mathrm{cnt}(C^*)$



Fix $i \in S$.

We want to show that there must be $\geq (n-m)$ †'s in row i

Let α be an i-cta falsifying C^*



if $j \to \ell_j$ then map $i \to \ell_j$

So $P_{i\ell_j}$ must occur in C^*

Do same argument for all $i \in S$

So C^* has $\geq (n-m)\cdot m$ t's altogether

Since $\frac{n}{3} \leq m \leq \frac{2n}{3}$

$$(n-m)(m) \geq \frac{2n^2}{9}$$

$\blacksquare$

Ben-Sasson - Wigderson

Size-width tradeoff Thms for Resolution

Thm. Let f be a kCNF, n vars

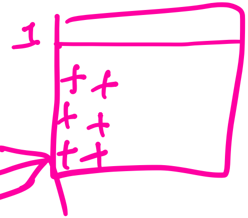
① If f has a tree Res proof of size S, then f has a Res ref of width $\log_2 S$

② If f has a (general) Res proof of size S, then f has a Res ref of width $O(\sqrt{n \log S})$

(proof next lecture!)

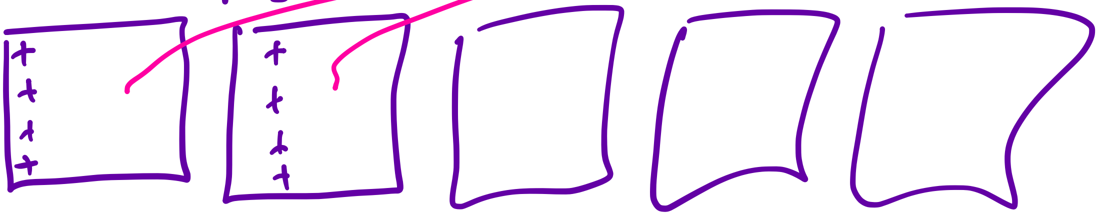
UPPER BOUNDS for PHP in Resolution

Nicer combinatorial view



Monotone Resolution (just for PHP)

Start with pigeon axioms



Single rule:

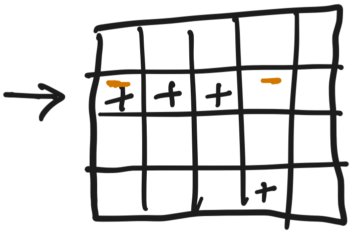
Pick a row i, pick 2 prev. derived matrices

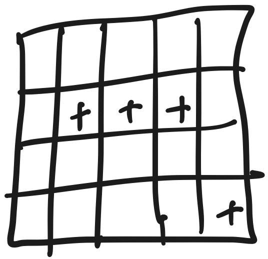
Take the intersection of +'s in row i

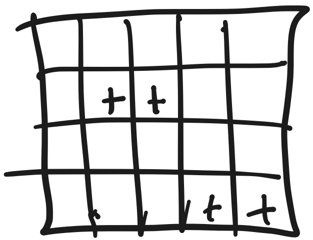
+ the union of all other +'s

Claim: Monotone Res is equiv to general Res

① Simulating Monotone Rule by Res rule (use hole axioms)

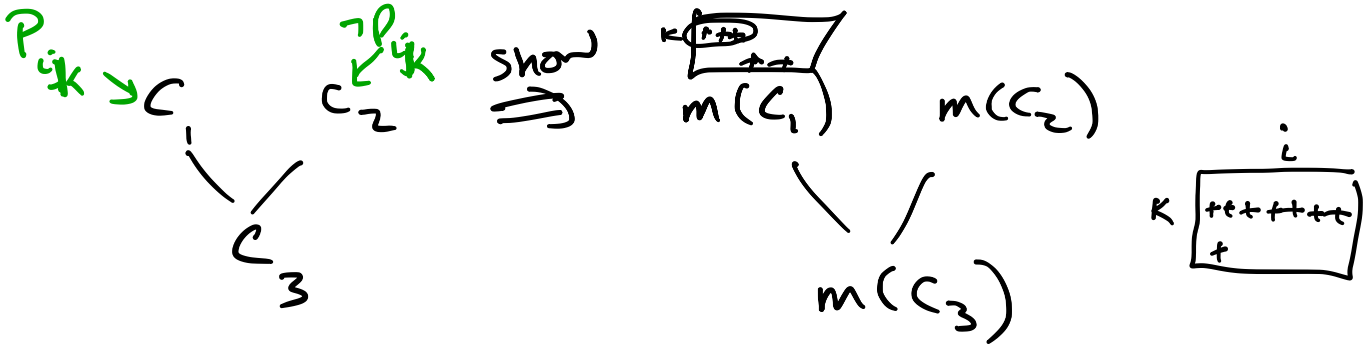






② Simulating Resolution by Monotone Res

we will convert the whole proof to monotone; then show how to use monotone rule on the monotone clauses

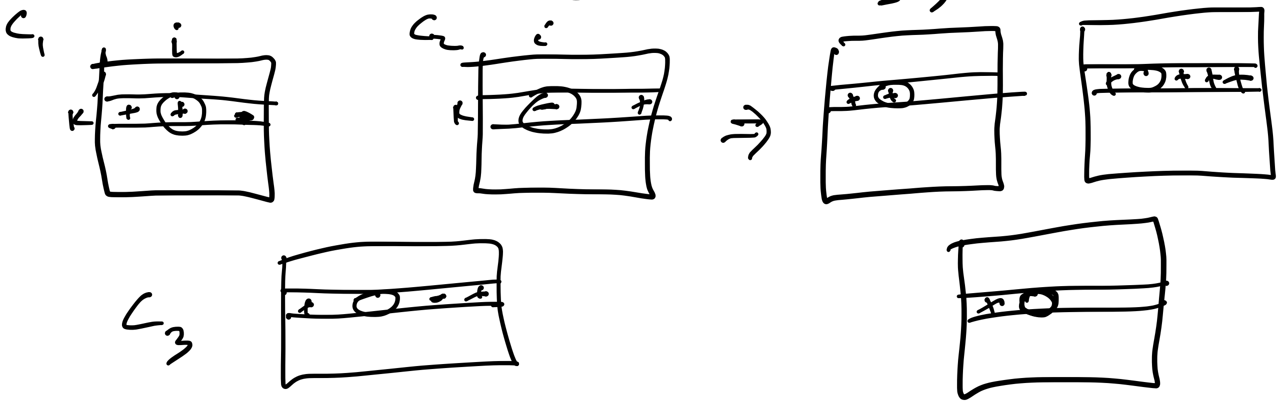


Case 1 If $m(C_2)$ has a + in position P_{ik}, then it has +'s everywhere in row k so $m(C_3)$ is just $m(C_1)$ [or has more +'s]

Case 2 $m(C_2)$ does not have a $+$ in position p_{ik}

then let C_3' be the clause obtained by applying monotone rule to $m(C_1)$, $m(C_2)$ using row k.

Then $C_3' \subseteq m(C_3)$



High level:

If $m(C_1)$ says some pigeon in $S_1 \cup S$ goes to k
and $m(C_2)$ " " " $S_2 \cup S$ goes to k

where S_1, S_2 disjoint, then
we must have some pigeon in S going to k
(otherwise not 1-1)

UPPER BOUNDS $\neg PHP^m_n$

[Buss-Pitassi]

① Res UB $\sim 2^{\sqrt{n}}$ uses $m \sim 2^{\sqrt{n}}$

[Maciel, Pitassi, Woods]

② Let f be any UNSAT formula over $x_1, \ldots x_n$

Form f' by adding to f all clauses $y \leftrightarrow t$ where t is a conjunction of k literals, y is a new var

$$y \leftrightarrow x_1 \wedge x_2 \wedge x_3$$

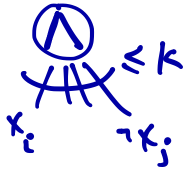
Let new f' be called f + width-k axioms

We will show $\neg PHP^{2n}_n$ + width-$\log n$ axioms has quasi-poly size Res refutations

* Res proofs of f + width-k axioms $\equiv$ Res(k) proofs of f

Res(k) : like Resolution but instead of clauses, lines are disjunctions of fan-in $\leq k$ conjunctions

$(t_1 \vee t_2 \vee \ldots \vee t_\ell)$, each t_i :



Nearly Matching Lower Bounds:

$\neg PHP^m_n$: requires $2^{\Omega(\sqrt{n})}$ size Resolution proofs for any m

[Raz, Pitassi]

[Raz]

[Razborov1], [Razborov2]

UPPER BOUNDS: PHP^{n+1}_{n}

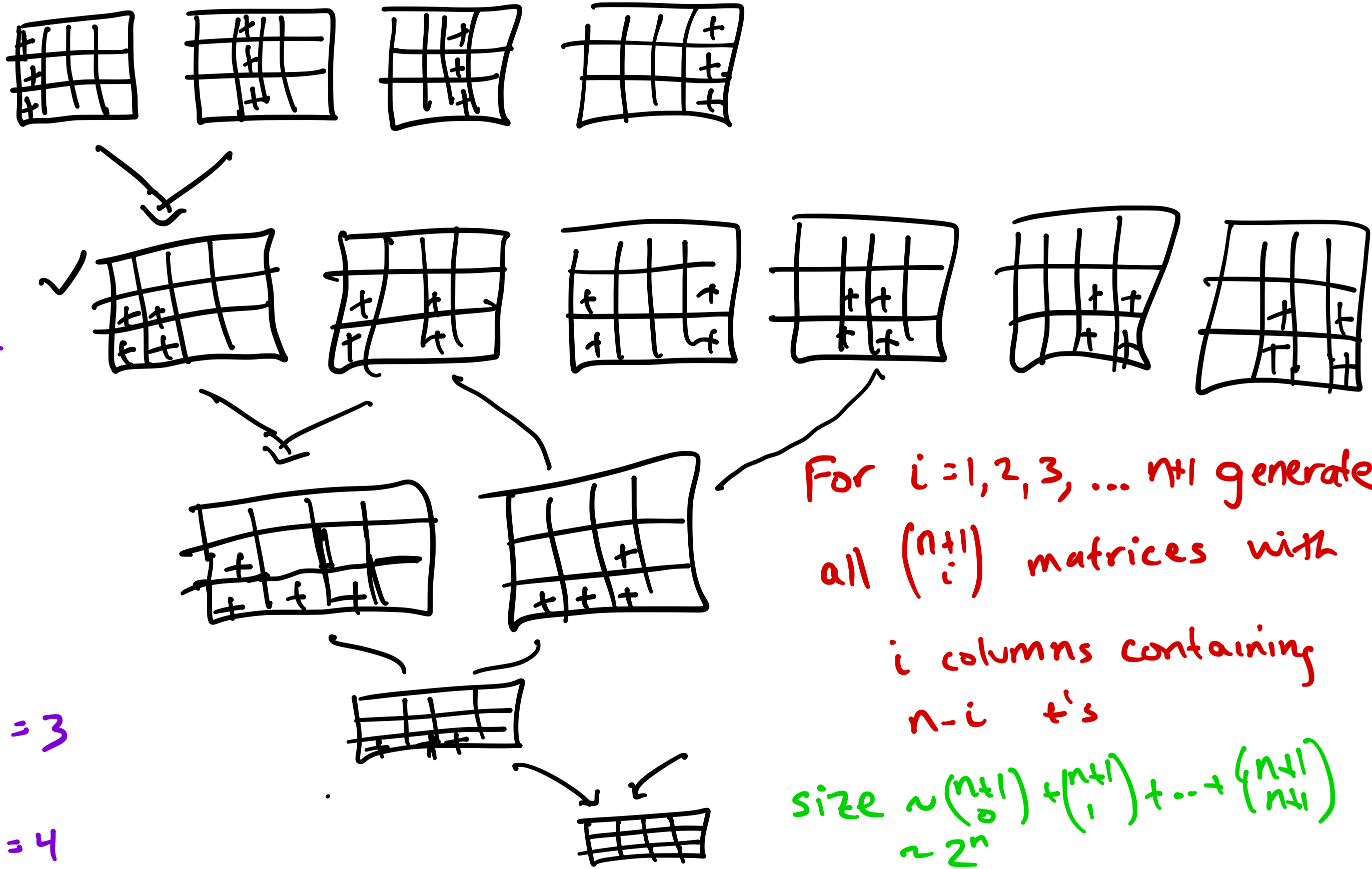
Example $n+1 = 4$
$n = 3$

i=1

i=2

i=3

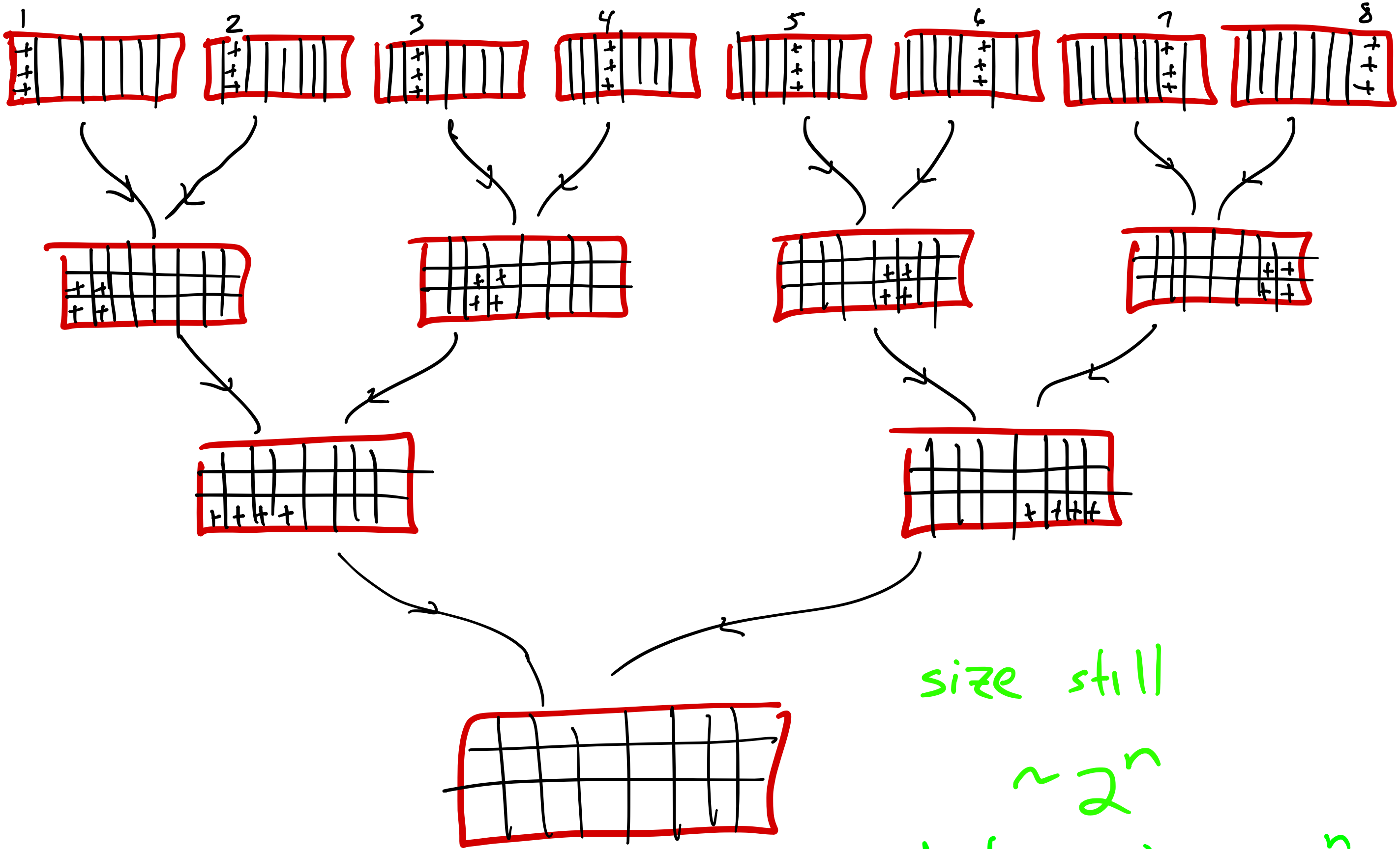
i=4



For $i = 1, 2, 3, \ldots n+1$ generate all $\binom{n+1}{i}$ matrices with i columns containing $n-i$ +'s

size $\sim \binom{n+1}{0} + \binom{n+1}{1} + \ldots + \binom{n+1}{n+1}$
$\sim 2^n$

What if we have a lot more pigeons? $m=8$ $n=3$



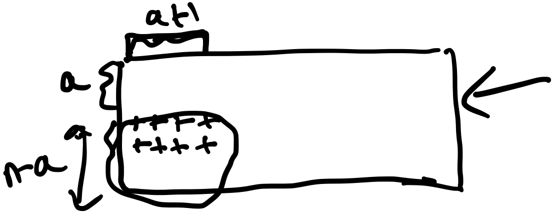
size still

$\sim 2^n$

but now $m = 2^n$

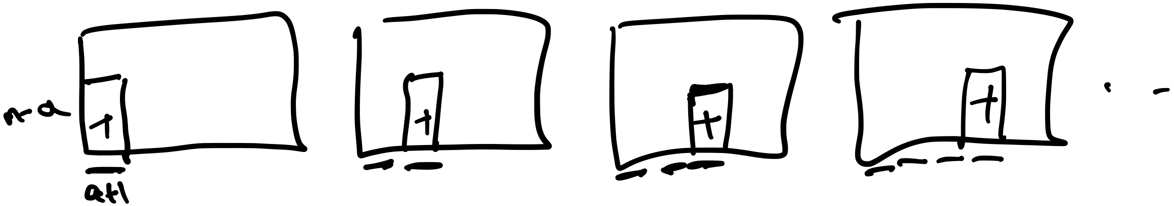
Combining to do better:

1. Split m pigeons into disjoint blocks of size $a+1$
For each block run PHP_a^{a+1} refutation to remove a holes



Left with a metablock of $(n-a)$ by $(a+1)$ $+$'s

Do for each block to get



2 Continue inductively to refute $PHP^{m/(a+1)}_{n-a}$ on these metablocks/metapigeons

set $a \sim \sqrt{n}$

each stage takes $\sim 2^{\sqrt{n}} \cdot 2^{\sqrt{n}}$

# of stages is $\frac{n}{\sqrt{n}} = \sqrt{n}$

So total size is $\sim 2^{O(\sqrt{n})}$!

2nd Upper Bound: $\neg PHP^{2n}_{n}$ + log n-axioms has quasipoly size Resolution proofs [Maciel-P-Woods]

we'll show $\neg PHP^{n^2}_{n}$ (not much harder to do PHP^{2n}_{n})

HIGH LEVEL IDEA: 2 phases

1. Cut the range in half but gap between # pigeons & # holes will lessen

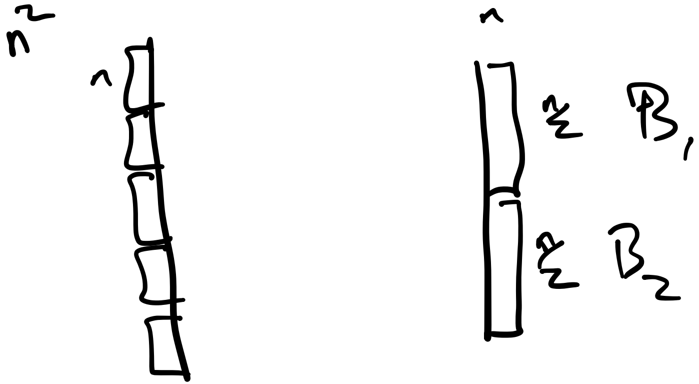
$$\neg PHP^{n^2}_{n} \longrightarrow \neg PHP^{n}_{n/2}$$

2. Amplify gap back to quadratic

$$\neg PHP^{n}_{n/2} \longrightarrow \neg PHP^{n^2}_{n/2}$$

repeat log n times

① $PHP^{n^2}_{n} \Rightarrow PHP^{n}_{n/2}$ (reduce pigeons)



each is an instance of $PHP^{n}_{n/2}$

another $PHP^{n}_{n/2}$ but over meta-pigeons $Q_{a,b}$

either: (a) ∃ a block i s.t. all pigeons in block i map to holes in B_1

(b) ∀ block i ∃ at least one pigeon in i that maps to a hole in B_2

$$Q_{a,b} = \bigvee_{i \text{ in block } a} P_{i,b}$$

(2) $\neg PHP^{n}_{n/2} \to \neg PHP^{n^2}_{n/2}$
(Amplification)

f : original function
$[n^2] \to [n]$

g : new function
$[n] \to [n/2]$

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

Complexity of h:

- If $f(x) = y \iff P_{ij}$ (original vars)
  and $g(x) = y \iff Q_{a,b}$ (each a clause)
  then $h(x) = y$ is an OR of fan-in 2 ANDs
- Iterating $\log n$ times, final h is an OR of fan-in-$\log n$ ANDs