RESOLUTION

Last time we saw

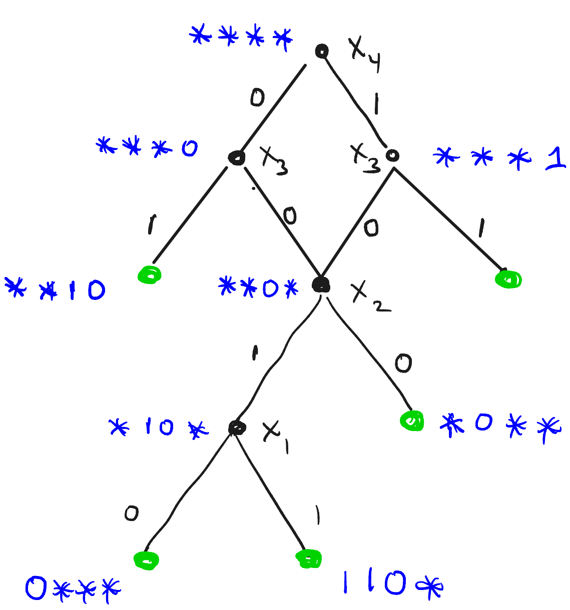
- RES is SOUND + COMPLETE

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

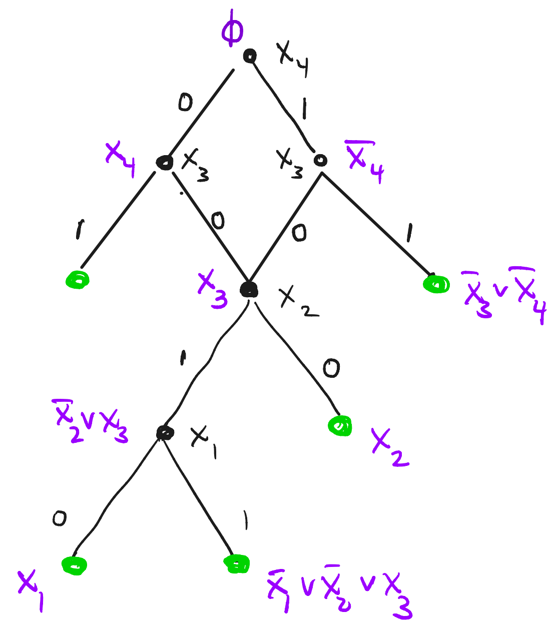
- (DAG)-RES refutation Π for f $\approx$ Prover/Delayer DAGs (or RES-DAGs) for solving Search_f

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

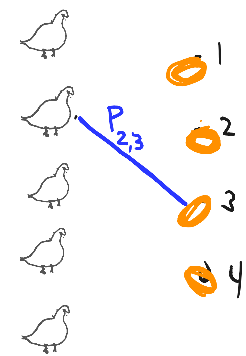
I. Width LBs $\longrightarrow$ Size LBs via restriction argument
or general size-width tradeoff

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

Propositional Pigeonhole Principle

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

$$\wedge \underbrace{\bigwedge_{\substack{i_1, i_2 \le n+1 \\ j \le n}} \left(\overline{P}_{i,j} \vee \overline{P}_{i,j}\right)}_{\text{functional}} \wedge \underbrace{\bigwedge_{j=1}^{n} \left(P_{1,j} \vee P_{2,j} \vee \dots \vee P_{n+1,j}\right)}_{\text{onto}}$$

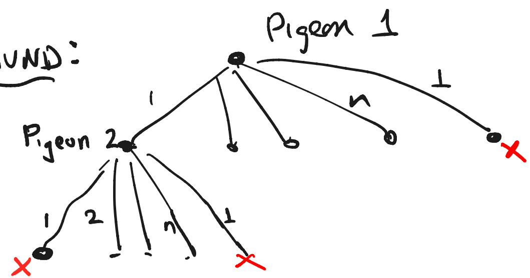


Res Lower Bounds for PHP: Warmup Tree-Resolution

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:

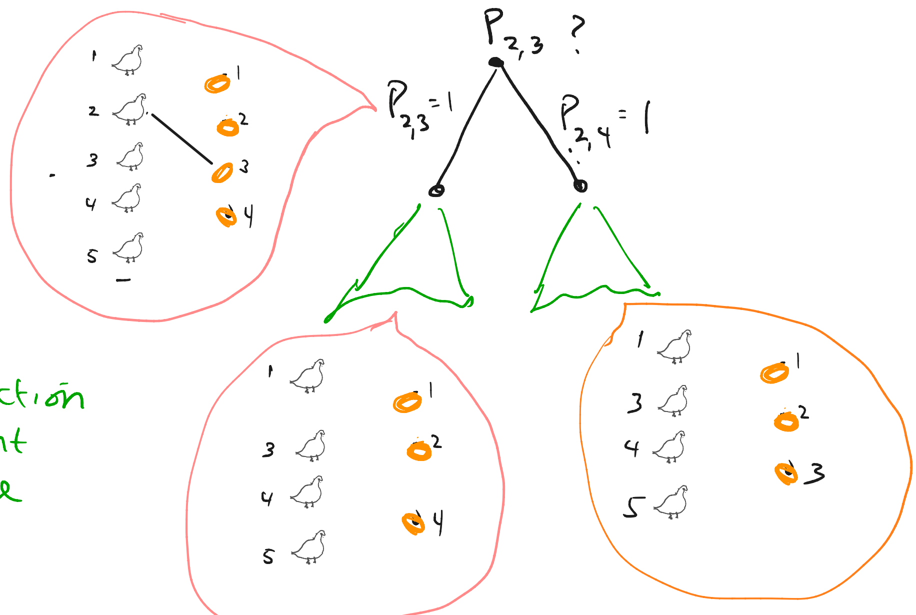
Show Res DAG (Prover Delayer) can solve search in size $2^{O(n)}$

Res Lower Bounds for PHP : Warmup Tree-Resolution

Theorem

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

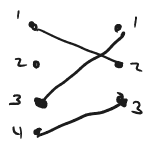
To Prove Theorem: Prove by induction on n that any decision tree for $\text{Search}_{PHP^{n+1}_n}$ that gives correct answers for all cta's has size 2^n.



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

RES LOWER BOUNDS FOR PHP (The general case)

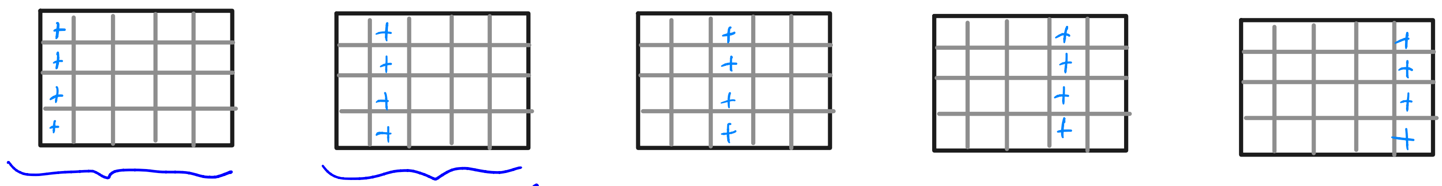
Critical Truth Assignments: $n-1$ of the n pigeons mapped 1-1 to the $n-1$ holes and the leftover pigeon unmapped.



← 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



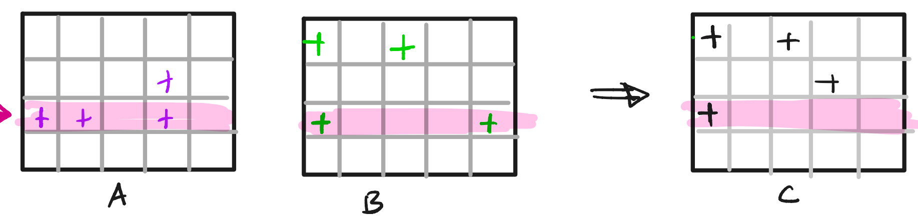
$P_{11} \vee P_{12} \vee \dots \vee P_{1n}$ $\quad$ $P_{21} \vee P_{22} \vee \dots \vee P_{2n}$

$n+1$ Pigeon Axioms

(No hole axioms)

Monotone Rule:

pick a hole (row) j

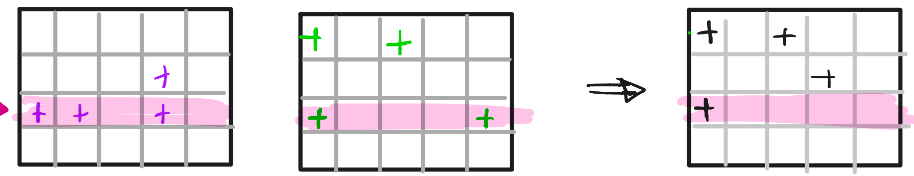


<u>Lemma</u> Any size-s RES refutation of PHP^m_n can be transformed into a monotone refutation of size $O(s)$, and vice-versa.

Monotone Transformation of PHP

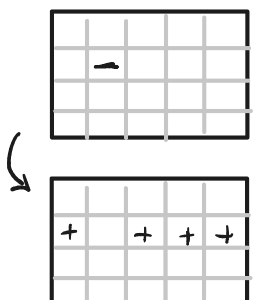
Monotone Rule:

pick a hole (row) j



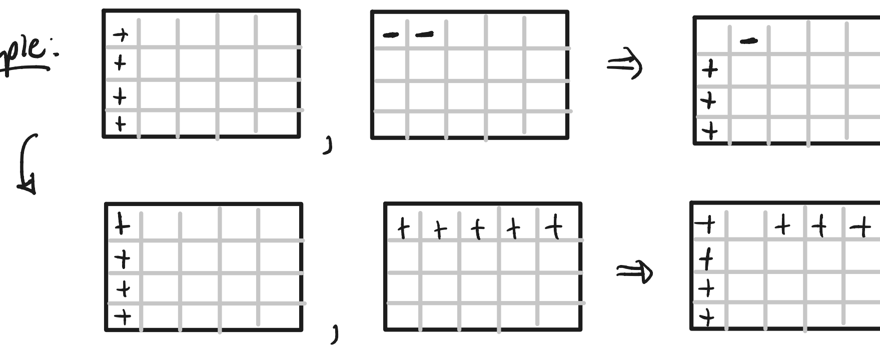
A B C

1. Convert each clause to monotone clause



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

Example:



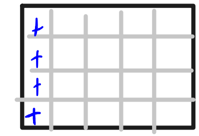
$\therefore$ Suffices to prove LB for monotone refutations

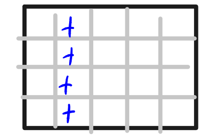
Playing With Monotone Refutations

UB strategy:

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

n clauses

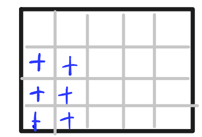




...

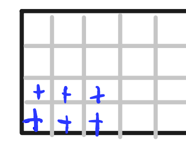
1. Remove hole n : generate all $(n-1) \times 2$ subrectangles on holes $1 \ldots n-1$

$\binom{n}{2}$ clauses



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

$\binom{n}{3}$ clauses



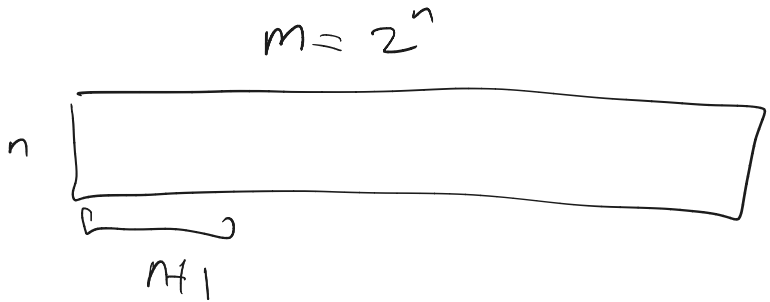
$\vdots$

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

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

n : Remove hole 1 : generate empty clause

$\binom{n}{0}$ clauses

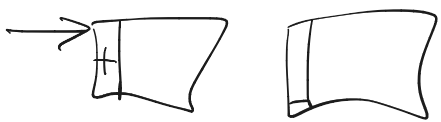


Conj

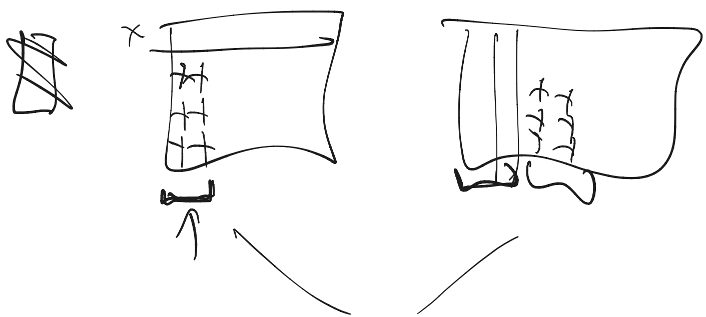
$2^{\#\text{holes}}$

$=$ Res

compl.



2



$2^{\sqrt{n}}$ pieces

$2^{\tilde{O}(\sqrt{n})}$

PHP LOWER BOUND FOR MONOTONE REFUTATIONS

Theorem Any monotone refutation of PHP_n^{n+1} 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 $PHP_{n'}^{n'+1}$, where $n' = \Theta(n)$ and width of every clause in $\Pi|_\rho$ is small — Lemma 1

2. (Wide Clause Lemma): Any monotone refutation of $PHP_{n'}^{n'+1}$ 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 $T(\Pi)|_\rho$ 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 $T(\Pi)$ 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 $C_1, C_2 \rightarrow C_3$ then

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

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

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

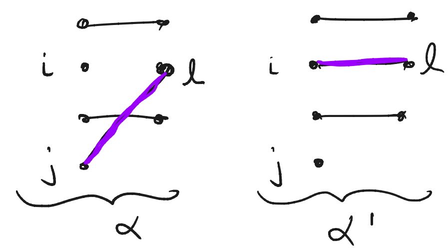
Let complexity$(C^*) = m$. Then $|C^*| \geq (n-m)(m)$

Let S be a minimal set of pigeon clauses that implies C, $|S| = m$.
We will show: $\forall i \in S$ C^* contains at least $(n-m)$ distinct variables $P_{i,j}$

(since $|S| = m$ this implies $|C^*| \geq (n-m)(m)$)

Let α be an i-cta falsifying C^*

for each $j \notin S$ consider the cta α_j obtained by "replacing" i with j:



α falsifies C^* but α' satisfies C^*.

$\therefore$ since C^* is monotone, P_{il} must occur in C^*

Resolution Lower Bounds

① Width LBs $\rightarrow$ 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

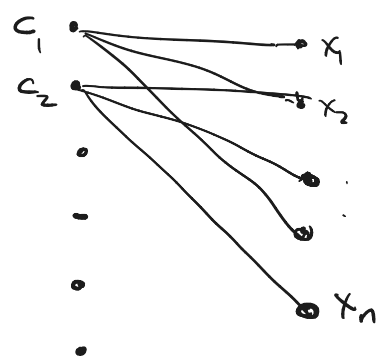
Resolution Lower Bounds for random KSAT

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

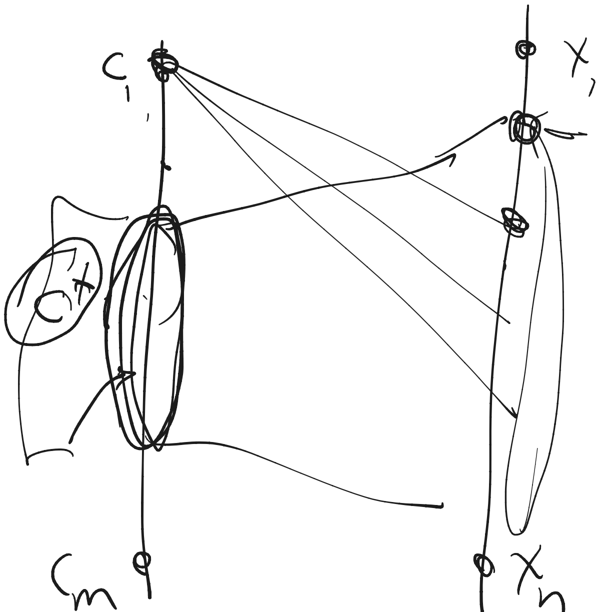
   Follows directly from fact that clause-variable graph is a good boundary expander whp.

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

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

How to prove width LBs from expansion of F

$F = C_1 \wedge \dots \wedge C_m$ kCNF



Claim

If G_F has $(\frac{\alpha}{3}, O(1))$ boundary expansion, then Res-width$(F) = \Omega(n)$.

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

RES UPPER BOUNDS FOR PHP^m_n

(0.) PHP^{m+1}_n : $2^{\Theta(n)}$

(1.) what about PHP^m_n $m \gg n$?

[Buss-P] show polysize Res refutations of PHP^m_n, $m \sim 2^{\sqrt{n}}$

[Raz] proves matching ~~$2^{\Theta(\sqrt{n})}$ lower bound~~. $2^{\Omega(n^{1/3})}$

(2.) what about slightly stronger proof system?

[Maciel-P-Woods] : quasipoly size Res(polylog n)

(see also Paris-Wilkie-Woods) refutations of PHP^m_n, $m = 2n$

OPEN Q's

1. Are there __polysize__ Res(polylog n) refutations of PHP^{2n}_n ?

   or polysize Bounded-depth refutations of weak PHP ?

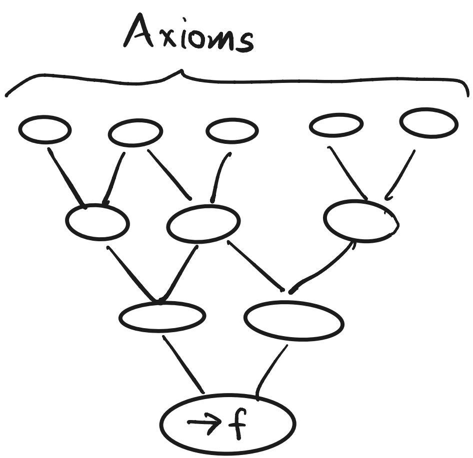
   Best Lower bounds : superpoly for Res($\sqrt{\log n}$), PHP^{2n}_n

   Motivation : Res LBs for "NP ⊄ P/poly"

Frege Proofs : formalized as sequent calculus

Lines are sequents: $\underbrace{A_1, \ldots, A_n}_{\Gamma} \rightarrow \underbrace{B_1, \ldots, B_m}_{\Delta}$

Meaning: $(A_1 \wedge \cdots \wedge A_n)$ implies $(B_1 \vee \cdots \vee B_m)$ $\quad [\, A_1 \wedge \cdots \wedge A_n \supset B_1 \vee \cdots \vee B_m \,]$



Formulation as proof that f is TAUT

Frege Proofs : formalized as sequent calculus

Axiom: $A \to A$

Weakening Rule: $\dfrac{\Gamma \to \Delta}{\Gamma, A \to \Delta, B}$

Logical Rules:

AND-RT $\dfrac{\Gamma \to \Delta, A \qquad \Gamma \to \Delta, B}{\Gamma \to \Delta, A \wedge B}$

AND-LEFT $\dfrac{A, B, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta}$

OR-RT $\dfrac{\Gamma \to \Delta, A, B}{\Gamma \to \Delta, A \vee B}$

OR-LEFT $\dfrac{A, \Gamma \to \Delta, \qquad B, \Gamma \to \Delta}{A \vee B, \Gamma \to \Delta}$

NEG-RT $\dfrac{\Gamma, A \to \Delta}{\Gamma \to \Delta, \neg A}$

NEG-LEFT $\dfrac{\Gamma \to \Delta, A}{\Gamma, \neg A \to \Delta}$

CUT RULE: $\dfrac{A, \Gamma \to \Delta \qquad \Gamma \to \Delta, A}{\Gamma \to \Delta}$

$\mathcal{C}$-Frege: restrict cut formula $A \in \mathcal{C}$

Frege Proofs

A Frege proof of f is a sequence of sequents where each sequent is an axiom, or follows from 1 or 2 previous sequents by a rule, and last line is $\rightarrow f$.

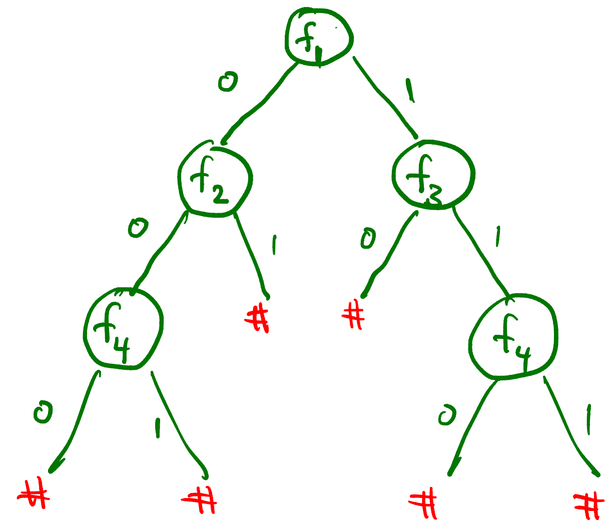
Theorem (Frege Normal Form) Let π be a Frege proof of f. Then there exists another Frege proof π' of f such that:

(1) π' is balanced and tree-like

(2) $|\pi'| \leq \mathrm{poly}(|\pi|)$

Frege Systems: Equivalent Formulation as Prover - Delayer game

Example:



Frege Prover - Liar game:

Liar claims he has a satisfying assignment α for $f = C_1 \wedge C_2 \wedge \ldots \wedge C_m$

Prover queries arbitrary formulas $f_1, \ldots f_q$

game ends when every path has a "truth table" contradiction

Frege Systems: Equivalent Formulation as Prover-Delayer game

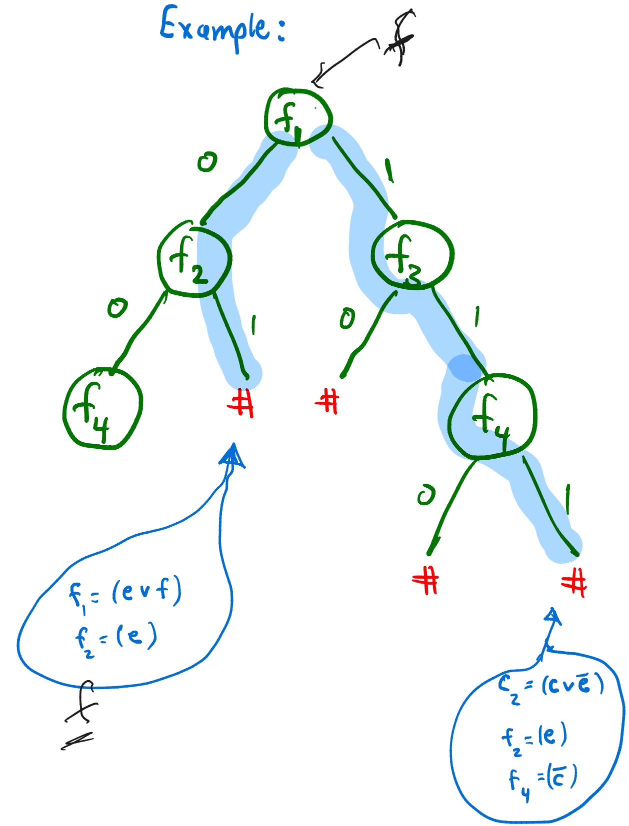
Frege Prover-Liar game:

Liar claims he has a satisfying assignment α for $f = C_1 \wedge C_2 \wedge \ldots \wedge C_m$

Prover queries arbitrary formulas $f_1, \ldots f_q$

game ends when every path has a "truth table" contradiction

Example:



HARD FORMULAS FOR FREGE?

"It is awfully difficult to come up with even candidate hard tautologies -- there is NO such thing as tons of NP-complete problems at our disposal!"

Nearly all statements that can be expressed propositionally are either:

(1) Not true (Not a tautology)

(2) Not known to be true or false

(3) Provably true (and with short Frege proof)

POTENTIALLY HARD FORMULAS ?

① Pigeonhole Principle

$$PHP_n^{n+1} : \bigwedge_{i=1}^{n+1} (P_{i,1} \vee P_{i,2} \vee \cdots \vee P_{i,n}) \wedge \bigwedge_{\substack{i_1, i_2 \le n+1 \\ j \le n}} (\overline{P_{i_1 j}} \vee \overline{P_{i_2 j}})$$

$n = 9$ holes
$n+1 = 10$ pigeons

② other counting Principles (e.g., Tseitin)

③ Random Formulas

④ Existence of pseudo-random generators

⑤ Circuit Lower Bounds $Hard_f(s)$

Conjectured to be hard for Frege

Proof Complexity Zoo