Propositional Proof Systems - Overview/Introduction

Resolution
Frege systems
extended Frege/extended Resolution
Cutting planes (integer linear inequalities on all variables)
Nullstellensatz/Polynomial calculus (polynomials over finite fields)
Stranger proof systems
Abstract proof systems

Goal of a proof system is to prove tautologies.

Example

Language: Variables $x_1, y, z_1, z_2, x_1, x_2, y, z_2$

that map over $\{T, F\}$

Funct: $\land, \lor, \rightarrow$

Unary negation

Formulas: $x_1 \rightarrow \neg p \rightarrow (p \lor y) \land (\neg y)$

$p \rightarrow (p \lor -p) \rightarrow p$

$\neg (p \lor -p)$

is a Tautology

Truth table assignment

$p \lor -p$ is a Tautology if $\neg (p \lor -p)$ is not satisfiable

Pf: $q$ is satisfiable if $q$ is true under some truth assignment

$q$ is false under some truth assignment

$q$ is satisfiable if $q$ is false under some truth assignment

$q$ is not a tautology

I.e.: Showing $q$ is a tautology is same as showing $\neg q$ is not satisfiable.

Thus, Taut is $\text{NP}$ complete
How do show Ψ is sound? 
(5) Try all truth asssignment. 
(6) Give a proof.

Define Frege system (in language 0, V, →) Ψ.

Axion One: Any formula of the form

\[ \psi \rightarrow (\phi \rightarrow \psi) \]
\[ (\psi \rightarrow \phi) \rightarrow ((\psi \rightarrow \phi) \rightarrow (\phi \rightarrow \phi)) \]
\[ (\phi \rightarrow \phi) \rightarrow (\psi \rightarrow (\phi \rightarrow \phi)) \]
\[ \psi \rightarrow \phi \]

Only rule of inference: Modus Ponens

\[ \frac{\psi \quad \psi \rightarrow \phi}{\phi} \]

Define \( \Gamma \rightarrow \psi \) if \( \exists \phi \vdash \phi \rightarrow \psi \), etc.

Then \( \Gamma \rightarrow \psi \) is sound if \( \Gamma \) is complete.

Also implicitly sound and complete.

Then if \( \psi \rightarrow \phi \) is a tautology, then \( \psi \) has a \( \Gamma \rightarrow \phi \) proof of size \( \leq 2^{\lvert \psi \rvert} \).

Define \( \lvert \psi \rvert \) = number of symbols of \( \psi \)

size of \( \Gamma \rightarrow \phi \) = \( \sum \lvert \psi \rvert \), \( \psi \) a line in \( \Gamma \)

Proof another.

Key property of \( \Gamma \):

1. Soundness/completeness.
2. Polynomial time verifiability.

If poly time procedure which gives \( \Gamma \rightarrow \phi \) determine \( \Gamma \vdash \phi \rightarrow \phi \)
**Defn.** An abstract proof system is a polynomial-time function $f : \{0,1\}^* \to \text{TAUT}$. 

**Discuss.** For an abstract proof system $f$, $\text{ZFC}$ is a "redundant system." Theorem [Cook-Reckhow ’79]: $\exists \text{ a polynomially bounded srs f ист NP=co\text{NP}}$. 

Theorem: Let $f, g$ be abstract proof systems.

- $f$ simulates $g$ if $\forall P, \exists P' \subseteq P, |P'| \leq p(|P|)$ and $f(P') = y$.
- $f$ is polynomial if $\forall P, |P| \leq p(|P|)$.
- $f$ is polynomial if $\exists g, f$ simulates $g$.
- $f$ is polynomial if $\forall g, f$ simulates $g$ and $f$ does not simulate $g$.

For some polynomial $p$,

$$f \circ \text{polynomially bounded if } \forall P, |P| \leq p(|P|) \Rightarrow f(P) = y.$$
Pf (Easy). Note TAUT is coNP-complete.

\( \text{Pf: TAUT} \in \text{coNP by defn.} \)

\( \text{if } \text{NP} = \text{coNP} \text{, then } \text{TAUT} \in \text{coNP} \text{ by defn.} \)

\( \text{iff SAT } \leq_{T} \text{ TAUT since SAT } \in \text{NP} \text{.} \)

\( \Leftrightarrow \text{if NP coNP, TAUT } \in \text{NP. So, \exists Q \in \text{Ptime}, poly} \)

\( \text{up Q } \in \text{TAUT it } \exists x \in (\{0,1\}^{*}) \text{ Q(x, Q).} \)

\( \text{Define } f \text{ by } f(\langle x, Q \rangle ) = \begin{cases} Q & \text{if } Q(x, y) \\ x = \chi, \neg Q \end{cases} \)

\( \text{Given poly-size } c_{Q} \text{ in A, } \forall Q \in \text{TAUT it } \exists x \in (\{0,1\}^{*}) \text{ A(P) is Q.} \)

\( \text{Given a NP-defination of TAUT.} \)

\( \text{Corollary: If no poly UID gives correct, then } P \neq \text{NP.} \)

\( \text{Known: Res, CP, NS, PC not poly ID's} \)

\( \text{F, cF not even.} \)

Best known lower bound to F:

- Let \( T \) alternate \( \varphi(x, \chi) \)
  \[ + \]
  \( \text{Let } Q_{n} \in \text{ T} \)
  \( \forall \text{in } \inf \theta_{Q_{n}} \)
  \( \text{so } |Q_{n}| = \theta(n) \)

Then if \( P \neq Q \), the \( |Q| = \Omega(n) \) \( \rightarrow |P| > c \cdot n^{2} \)

\( \text{Pf: Fix } P \neq Q. \)

For \( \forall m \), define \( y_{i} \) to be actively under \( P \)

\( \text{If } \exists \varphi_{n} \text{, such that } \varphi_{n} \text{ is not actively used, clone } \varphi_{n} \text{.} \)

Form P' by replacing every such \( y_{i} \) in P with F.

P' is still in NP, but its last move is not a test move.
Extended Frp

extension rule: \( x \rightarrow y \rightarrow z \) \( (x \rightarrow y) \cdot (y \rightarrow z) \)

Def: \( y_0 \ldots \ y_n \)

end \( y_i \) - axiom or

inferrable \( \text{by MP} \)

\( x \rightarrow y \) when \( x \) not used in \( y_i \), any \( y_j \), for

\( y_i \).

Then if \( P \) is \( \text{Frp} / y_i \) of \( m \) lines

\( P' \), et if \( y_i \) of \( O(m+1p^2) \) symbols.

Pf (Sketch): formulas

(a) Enumerate all \( x \) in \( P \) which are active in \( y_i \) - axiom

of \( P \). (Explain) - e. g. given as a law

\( x_1 \ldots x_{m'} \) \( m' \) = \( O(m) \), or as a diagram

hence if an axiom or a line of \( P \)

or \( u \),

selfish of the

last line of \( P \)

\( \text{CNP} \).

(b) For each selfish all \( x \) in \( P \) of \( m \) lines

\( y_i \) or \( y_i \) or \( y_i \) or \( y_i \) (say)

et.

(c) For each line \( x_i \) in \( P \)


\( y_i \rightarrow y_i \). (C. i) Axiom

\( \text{CNP} \).

(c. ii) MP \( y_i \rightarrow y_i \), \( y_i \rightarrow y_i \).

\( y_i \rightarrow y_i \).

\( O(m) \) symbols.
Example 1

(b) \( \chi_{\varphi \rightarrow (\varphi \lor \psi)} \Leftrightarrow \chi_{\varphi} \rightarrow \chi_{\varphi \lor \psi} \)

(axiom)

(c) \( \chi_{\varphi} \rightarrow \chi_{\varphi \lor \chi_{\psi}} \)

(a) \rightarrow (b) \rightarrow (c) \rightarrow \chi_{\varphi \rightarrow (\varphi \lor \psi)}

\( \therefore \chi_{\varphi \rightarrow (\varphi \lor \psi)} \)

Tautology of size \( O(1) \)
Hence has a proof of size \( O(1) \) by completion

3 uses of MP.

Example 2

\( \varphi \rightarrow \psi \)

(c) \( \chi_{\varphi} \quad \text{ind hyp} \)

(b) \( \chi_{\varphi \rightarrow \psi} \quad \text{ind hyp} \)

(a) \( \chi_{\varphi \rightarrow \psi} \Leftrightarrow (\chi_{\varphi} \rightarrow \chi_{\psi}) \quad \text{extension} \)

\( \chi_{\varphi \rightarrow \psi} \rightarrow (c) \rightarrow \chi_{\varphi} \rightarrow \psi_{\chi} \)

Tautology of size \( O(1) \)
2 uses of MP

1 more use of MP
(a) For \( y_n \) close \( y \)

\[ O(\log n) \text{ steps, } O(\log n) \text{ symbols}. \]

\[ \text{Method: For each subformula } \varphi \text{ of } y_n, \text{ make } \]

\[ \varphi \to y \]

(work from smallest formula to do longest)

(\text{for each formula closest to } \varphi)

\[ \varphi \to \underline{\varphi} \]

[CR'79] Theorem \( \text{PHP}^{n+1}, \text{for any size of symbol}. \)

**Proof** let \( n \geq 2 \) \( \text{PHP}^{n+1} \) the following hold:

\[ \text{PHP}^{n+1}(x) \equiv \bigwedge_{i=1}^{n} \bigvee_{j=1}^{n} \bigwedge_{i \neq j} x_{ij} \wedge \neg \bigwedge_{i \neq j} x_{ij} \]

**Proof (Sketch)**

Introduce new variables \( x_{ij} \) for \( 1 \leq i \leq n; 1 \leq j \leq n \)

So that

\[ x_{ij} \text{ is just } x_{ij}. \]

So, add \( x_{ij} \) for \( x_{ij} \in T_n \)

For \( x_{ij} \) and \( x_{ij} \)

\[ \to \text{PHP}^{n+1}(x) \to \text{PHP}^{n+1}(x) \]

\[ \text{for } \log n \text{ proof of size } \log n \]

The fact \( \text{PHP}^{n+1}(x) \to \to \text{PHP}^{n+1}(x) \)

From \( \to \) \( \text{PHP}^{n+1}(x) \to \text{PHP}^{n+1}(x) \)

and hence \( \text{PHP}^{n+1}(x) \)


\( x_{ij}^{e-1} = x_{ij}^{e} \lor (x_{i,j}^{e} \land x_{e+1,j}^{e}) \)

Get:

\[ \text{LHS-\text{PHP}}_{e}^{L_{1}}(x^{e}) \rightarrow \text{LHS-\text{PHP}}_{e-1}^{L_{1}}(x^{e-1}) \]

\[ \text{RHS-\text{PHP}}_{e}^{L_{1}}(x^{e}) \rightarrow \text{RHS-\text{PHP}}_{e-1}^{L_{1}}(x^{e}) \]

Thus:

\[ \text{PHP}_{e}^{L_{1}}(x^{e}) \rightarrow \text{PHP}_{e-1}^{L_{1}}(x^{e-1}) \]

qed...

\textbf{Theorem [Bun]} \quad \exists \text{poly} \text{ PHP}_{n}^{n+1}(x).

\textbf{Pf} \quad \text{approx. - closeen.}

\textbf{Theorem [Bun, Jan 18, 2014]} \quad \exists \text{poly} \text{ PHP}_{n}^{n+1}(x).

\textbf{Pf} \quad \text{We mimic the proof of [Cook-Reckhow 79].}

\textbf{Define:} \quad \phi_{i,j}^{e} \text{ by:}

\[ \text{Ex } l = 0, 1, \ldots, n \]

\[ \text{Et } f : [n+1] \rightarrow [n] \text{ (potentially be assumed to violate the PHP}_{n}^{n+1} \text{.)} \]

Define a directed graph \( G^{e} \) by
$G^k$: bipartite on $[n+1] \cup \{n\}$, directed.

For $f(i) = j$ $G$ has an edge $(i, 0) \rightarrow (j, 1)$.

And for $j > 1$, $j \leq n$ $G$ has an edge $(j, 0) \rightarrow (j+1, 0)$.

$\phi_{ij} \iff \exists \text{a path in } G^k \text{ from } i \text{ to } j$.

(for $i \leq n+1$, $j \leq n$)

More generally define

Reach $^{G^k}_{\leq m}$ $(x, y)$ : $\text{path in } G^k \text{ from } (x, y) \text{ to } (x, y) + G^k$.

Claim: $\phi_{ij}$ has a quadratic time formula.

Reach $^k_{\leq m}$ $(x, y)$ : $\text{path of length } \leq m$.

Reach $^k_{\leq m}$ $(x, y) \iff \forall \text{Reach} ^k_{\leq m-1}$ $\text{(k)}$ $\forall \text{Reach} ^k_{\leq m-2}$ $\text{(k)}$ $\forall \text{Reach} ^k_{\leq m-3}$ $\text{(k)}$ $\forall \text{Reach} ^k_{\leq m-4}$ $\text{(k)}$

Reach $^k_{\leq m}$ $(x, y)$ defined in obvious way.

Claim (2) $\phi_{ij}$ satisfies the equation (5) of page 7 and this can be proved in a size process.
Using poly-sji formulas for Vector Addition,

\[ \text{Count}_i (x_1, \ldots, x_i) \iff \exists i \text{ of the } x_j \text{'s are true.} \]

\[ \text{The show: } \]

\[ \text{Count}_i (Vx_{\bar{L}}, Vx_{\bar{L}_2}, \ldots, Vx_{\bar{L}_n}) \]

\[ \geq n + 1. \]

\[ \text{and if } f : [n+1] \rightarrow [n]. \]

Hence Whence obtain a contradiction.

---

Extended resolution

Substitution

SF primitives e f.

Cutting planes
There is a tree-like, dag-like Frege system \( p \)-simulates a Frege system.

**Proof**

Let \( \psi_0, \psi_1, \ldots, \psi_{n-2}, \psi_{n-1} \) be a Frege.

Let \( A_1, A_2, \ldots, A_n \) be (dag-like) Frege proofs.

If \( \deg_i = \max |A_i| \).

Let \( B_0 = A_0 A_1 A_2 \ldots A_i \) (associated with \( \psi_i \)) \( B_0 = T \) (true).

Claim: There is a tree-like, dag-like Frege proof of \( B_0 \to B_i A_i \) \( \forall i \geq j \), of size \( \deg_i \).

**Proof:** We have \( \psi_i \), \( \psi_{i+1}, \psi_{i+2}, \ldots, \psi_{n-2}, \psi_{n-1} \) as in (i).

- \( \psi_i : (\psi_{i+1} \psi_{i+2} \psi_{i+3}) \to (\psi_{i+4} \psi_{i+5} \psi_{i+6}) \)
- \( \psi_i : (\psi_{i+1} \psi_{i+2} \psi_{i+3}) \to (\psi_{i+4} \psi_{i+5} \psi_{i+6}) \)
- \( \psi_i : (\psi_{i+1} \psi_{i+2} \psi_{i+3}) \to (\psi_{i+4} \psi_{i+5} \psi_{i+6}) \)
- \( \psi_i : (\psi_{i+1} \psi_{i+2} \psi_{i+3}) \to (\psi_{i+4} \psi_{i+5} \psi_{i+6}) \)
- \( \psi_i : (\psi_{i+1} \psi_{i+2} \psi_{i+3}) \to (\psi_{i+4} \psi_{i+5} \psi_{i+6}) \)
- \( \psi_i : (\psi_{i+1} \psi_{i+2} \psi_{i+3}) \to (\psi_{i+4} \psi_{i+5} \psi_{i+6}) \)

Thus we have Frege proofs.

\[ B_i \vdash A_i \] \( B_i \to B_{i+1} (A_i \vdash A_i) \) by (i).

\[ B_{i+1} A_i \to B_{i+2} (A_i \vdash A_i) \) by (i).

\[ B_{i+1} A_i \to B_{i+2} (A_i \vdash A_i) \) by (i).

\[ B_{i+1} A_i \to B_{i+2} (A_i \vdash A_i) \) by (i).

\[ B_{i+1} A_i \to B_{i+2} (A_i \vdash A_i) \) by (ii).

\[ B_{i+1} A_i \to B_{i+2} (A_i \vdash A_i) \) by (ii).

\[ B_{i+1} A_i \to B_{i+2} (A_i \vdash A_i) \) by (ii).

Thus, we can conclude in a tree-like manner.

\[ \psi_i : \psi \to \psi \psi \] (finite case)
Claim: \( B_i \rightarrow A_j \) \( \rightarrow (B_i \rightarrow (A_j \rightarrow A_k)) \rightarrow (B_i \rightarrow A_k) \)

Let's prove each lemma:

**Proof:**

1. Let \( A_{in} \)

   \[ \begin{align*}
   &\text{Proof:} A_{in} \quad (B_i \rightarrow A_{in}) \\
   &\text{Use MP} \quad \text{Get} \quad B_i \rightarrow A_{in}
   \end{align*} \]

2. \( A_{in} \) is derived by MP
   \[ \begin{align*}
   &\text{and} \quad A_{in} \quad \text{of } i, i' \in i
   \end{align*} \]

   \[ \text{Axiom is } A_j \rightarrow A_k \]

   **Final proof of:**

   \[ \begin{align*}
   &B_i \rightarrow A_j \\
   &B_i \rightarrow A_j \\
   &A_{in} (A_j \rightarrow A_k) \rightarrow A_k
   \end{align*} \]

   **Final proof of:**

   \[ \begin{align*}
   &\text{final conclusion of fixed} \text{ axiom}
   \end{align*} \]

To prove Theorem, combine previous claims:

Constant is a tree like \( B_i \rightarrow B_i \)

New \( B_i \) is axiom so finish off with \( B_i \) and MP.

**QED: Theorem**
Topic 2: Substitution. From system

Let \( \varphi = \varphi(x, x) \) be a formula - all occurrences of \( x \)'s indicated.

Let \( \varphi, \psi \) be formulas. The substitution rule allows

\[
\frac{\varphi(x, x)}{\varphi(\psi, \psi)}
\]

Rk: All \( x \)'s replaced "in parallel".

Def: \( sF = F + \) substitution rule.

Note \( sF \) is sound + complete, but not "implicationally complete".

**Example**

Let \( x \neq x \) is not a tautology.

**Theorem** \( sF \) \( \vdash \) \( \varphi \).

**Lemma** If \( sF \) proves \( \varphi \), then \( \varphi \) is in \( \text{core of } F \).

Theorem \( F \vdash (\varphi \land \forall x \varphi_0 \rightarrow (\forall x \varphi_0) \rightarrow (\forall x \varphi_0) \rightarrow \varphi \).

**Proof**

This is the well-known deduction rule, applied \( 2 \) times.

In detail: Apply \( (\forall x \alpha) \rightarrow (\forall x (x \rightarrow \beta)) \rightarrow (x \rightarrow \beta) \)

and \( \alpha \rightarrow (x \rightarrow \beta) \) \( \vdash \)

and use \( \varphi \rightarrow (\forall x \varphi_0) \) at find \( \alpha \), get

\( \varphi \rightarrow \varphi \) if \( \forall x \) size only.
New use \( \mathcal{E}(B \rightarrow C \rightarrow A) \rightarrow B \rightarrow (C \rightarrow A) \) & \text{let } \psi \text{ qf.}

\( (\psi \rightarrow \psi) \rightarrow \ldots \rightarrow (\psi \rightarrow \psi) \rightarrow \psi \)

ged. Lemma.

Discuss on how formalizing the lemma is.

Now set \( \alpha \rightarrow \beta \rightarrow \gamma \rightarrow \zeta \text{ few} \)

\( (\psi \rightarrow \psi) \rightarrow (\psi \rightarrow \psi) \rightarrow (\psi \rightarrow \psi) \rightarrow \psi \)

Sub

\( (\psi \rightarrow \psi) \rightarrow (\psi \rightarrow \psi) \rightarrow (\psi \rightarrow \psi) \rightarrow \psi \)

Sub

\( (\psi \rightarrow \psi) \rightarrow (\psi \rightarrow \psi) \rightarrow (\psi \rightarrow \psi) \rightarrow \psi \)

Sub

\( \psi \rightarrow \psi \) (tautology)

\( (\psi \rightarrow \psi) \rightarrow (\psi \rightarrow \psi) \rightarrow \psi \)

Sub

\( \psi \rightarrow \psi \) (tautology)

\( \psi \rightarrow \psi \) (tautology)

QED Then

Then \( \alpha \rightarrow \beta \rightarrow \gamma \rightarrow \zeta \rightarrow \text{ few} \) \[ \text{[Dovon '85, Kajiček Pulka '89]} \]

Pf \( \text{Let } A_1, A_2, \ldots, A_m \text{ be an } sF \text{-proof of } A \rightarrow A_m \)

Let \( x_1, x_p \) be the \( sF \)-assemblies on all of \( A_1 \rightarrow A_m \)

Goal: Given \( sF \)-proof of \( A_m \)

Suffices (by deduction theorem) to take \( A_m \) as an extra axiom (even though)

and derive a contradiction.
For the $m,...,1$, we introduce new variable $x^*_t$ in $C_t$ by extending and will prove, for $t=m,...,1$,

\[ C_f := \bigvee_{i=1}^{k-1} \neg A_i(x^*_t) \bigvee \bigwedge_{i=1}^{k-1} \neg A_i(x^*_1) \bigvee A_m(x^*_t). \]

Here $A_i(x^*_t)$ means $A_i$ will each $x^*_i$ replaced by $x^*_t$.

Now $C_m$ follow immediately from $A_m$ (as $x^*_m = x^*_1$, $V_i$)

And $C_f$ follows from the fact $A_i$ since is an axiom ($\forall i$)

So it will suffice to gain a poly size (Fagin) proof

\[ C_{f+t} (\text{all extensions} \Rightarrow G_{f+t}) \]

Extension rule $x^*_m \rightarrow x^*_1$ (VI) - box can.

Now suppose $x^*_t$ have been introduced (VI) and $C_{f+t}$ holds.

Case (1): $A_m$ is an axiom. or $A_m$ is inferred by MP,

In this case,

\[ C_{f+t} \land A_{m+t} \rightarrow C_1 \]

and we take $x^*_t \rightarrow x^*_m$ (even, can be the same variable).

Case (2): $C_{f+t}$ is inferred by substitution $B(x_f, x_p) = G$ (4)

For $m \leq t$.

Define, by extension rule (intuition:

\[ x^*_i := \begin{cases} x^*_i & \text{if } x^*_i \neg A_i(x^*_i) \\ \neg \phi_1(x^*_t) & \text{if } \neg (\bigwedge_{i=1}^{k-1} \neg A_i(x^*_1)) \end{cases} \]

More formally:

\[ x^*_t := \left( x^*_i \bigvee x^*_1 \bigvee \bigwedge_{i=1}^{k-1} \neg A_i(x^*_i) \bigvee \phi_1(x^*_t) \bigvee \bigwedge_{i=1}^{k-1} \neg A_i(x^*_i) \right) \]

\[ \bigvee \bigwedge_{i=1}^{k-1} \neg A_i(x^*_i) \bigvee \phi_1(x^*_t) \bigvee \bigwedge_{i=1}^{k-1} \neg A_i(x^*_i) \]
Argue by cases:

Case (1): \( \forall x A_i(x+1) \)

Then \( \forall x A_i(x) \land A_i(x+1) \), so \( C_i \) holds.

Case (2): \( \exists i \exists x \neg A_i(x) \).

Then \( \neg A_i(x) \) by \( C_i \).

Clearly for this \( \neg A_j(x) \) follows.

General proof method for both: Fix \( y_1, y_2 \), fix formula \( D(y) \).

Prove by "突击法" "induction" on the complexity of subformulas \( E(y) \) of \( D(y) \) that

\( \forall x \left( y_1 \rightarrow E(x) \right) \rightarrow \left( E(y_1) \right) \),

Sample Cases: \( E = y \), the theorem.

\( E \in E(y) \neq E(y) \)

Already prove \( \left( y \rightarrow E(x) \right) \rightarrow \left( E(y) \rightarrow E(x) \right) \).

From here \( \left( y \rightarrow E(x) \right) \rightarrow \left( E(y) \rightarrow E(x) \right) \).

Later for \( y \) apply with \( y \rightarrow E(x) \). \( y_1 = x \), \( D = A_i(x) \).

\[ y \rightarrow \cdots \quad y_1 = x \quad y_2 = x \quad D = A_i(x) \]

\[ \forall \]
Claim: \( rF \) simulates \( sF \).

Proof: Suppose \( tF \) simulates \( sF \).

Suppose \( tF \vdash A(x_1, \ldots, x_p) \) for some variables \( x_1, \ldots, x_p \).

Let \( B \vdash A \). Suppose \( \mathcal{D} \vdash tF \rightarrow \neg A \).

Case (i): \( A \) is an axiom.

Case (ii): \( A \) follows by MP from \( A_j, A_j' \) when \( j \neq i \).

Case (iii): \( A \) is \( A_j(x) \) where \( A_j = A_j(x) \) is sub-proof.

Then prove:

(1) \( A_j(x) \) for each \( j = 1, \ldots, p \) (polysubstitution)
(e) For each $i = 1 \cdots p$
\[ x_i \vdash y \vdash A_i(x_i) \rightarrow A_i(y) \]

(c') For each $i = 1 \cdots p$
\[ x_i \vdash y \vdash A_i(x_i) \rightarrow A_i(y) \]

(d) by $x_i \vdash x_i$ and (c), prove
\[ q \rightarrow A_i \]

(d') by $x_i \vdash x_i$ and (c'), prove
\[ \neg q \rightarrow A_i \]

(e) by (d), (d'), prove
\[ q \rightarrow A_i \]

QED.

Let $T$ substitute by
\[ \frac{A(x)}{A(T)} \quad \text{and} \quad \frac{A(x)}{A(t)} \]

Then $T$-sub Frege $p$ simulates $\neg p$. 
Thin sF psi-pula eT

**Proof:** Let $A_1, A_2, \ldots, A_n = A$ be an eF proof of $A$.

Let $B_1, \ldots, B_k$ be the uses of extension rule $\beta$ in order.

- $B_i$: $y_i \leftrightarrow C_i$
- $C_i = C_i(y_{i-1} \ldots y_{i-k})$

$A$ does not involve $y_1 \ldots y_k$. $y_i$'s are distinct.

Let $D_j$ be $(B_2 \land B_3) \ldots \land B_j$ - associated left-to-right.

1. Create an F-proof of $D_k \rightarrow A$ of polynomial size.
   - Proof: Usual construction.

2. Create an F-proof of
   
   $B_k \rightarrow (B_{k-1} \rightarrow \ldots \rightarrow B_2 \rightarrow B \rightarrow A)$.

   **Construction:** Show: $(D_j \rightarrow A) \rightarrow [B_j \rightarrow B_{j+1} \rightarrow \ldots \rightarrow B_2 \rightarrow B \rightarrow A]$

   Using induction on $j$, $j = 1, 2, \ldots k$.

   Newly, $D_{j+1}$ is $D_j \land B_{j+1}$.

   And $(D_j \land B_{j+1}) \rightarrow A \rightarrow B_{j+1} \rightarrow (D_j \rightarrow A)$.

   And $B_j (D_j \rightarrow A) \rightarrow [B_j \rightarrow \ldots \rightarrow A]$

   So $[(D_j \land B_{j+1}) \rightarrow A] \leftrightarrow [(D_j \rightarrow A) \rightarrow [B_j \rightarrow \ldots \rightarrow B \rightarrow A] \rightarrow (B_{j+1} \rightarrow [B_{j+1} \rightarrow B \rightarrow A])$

   Is a tautology (in $D_j$, $B_{j+1}$, $A$) and $B_j \rightarrow [B_{j+1} \rightarrow B \rightarrow A]$

3. Use substitution of $C_k$ for $y_k$ + the MP with $C_k \rightarrow C_k$.

   Repeat $k$ times.

   Discuss an expression of variables!
**Thm e5 p Simulator sT.**

**Pr:** Let $A_1, A_2, \ldots, A_m$ be a sT proof, $A = A_m$.

Let variables $x_1, x_2, \ldots, x_m$ be $x_1, x_2, \ldots, x_m$.

Well introduce (by extension) variable $x_k^k$ for $k = m, m-1, \ldots, 1$.

And will generate (by extension), for each $k$, $\neg A_m \Rightarrow B_k$, where

$$B_k := \bigwedge_{j=1}^k A_j(x^j)$$

when $A_j(x^j)$ means $A_j$ all variables $x_i$ replaced by $x_i^j$.

**Base case:** Let $k = m$. Clearly $x_k^m$ can be introduced and $\neg A_m \Rightarrow B_m$.

**Inductive step:** Let $B_k \Rightarrow B_{k+1}$. Clearly $x_{k+1}$ can be introduced and $\neg A_{k+1} \Rightarrow B_{k+1}$.

Con.(1) $A_k$ is an axiom.

Set $x_k^k \equiv x_k^k$ (i.e., one same variable, no extension).

So then $A_k(x^k)$ is an axiom.

So $B_k \Rightarrow B_{k+1}$ is easy to prove.

Con.(2) $A_k$ introduced by MP. $A_k \Rightarrow A_k$ inferred for $A_i$ and $A_i \Rightarrow A_k$.

Set for $x_i^k < k$. Use $x_i^k \equiv x_i^k$ again.

Then $\neg A_k(x^{k+1}) \Rightarrow \neg A_i \vee \neg (A_i \Rightarrow A_k)$.

And from the $B_{k+1} \Rightarrow B_k$ from the straightforward.

Con.(3) Substitution:

$A_k \equiv A_j(\overline{\varphi})$ when $j \neq k$

and $A_j(\overline{\varphi}) \equiv A_j$ with each $x$ replaced by $\overline{\varphi}$.

End.
Want to define $x^k_i$ by

$$x^k_i = \begin{cases} x_i^{k+1} \text{ if } B_k \text{ true } & \text{ for } j = 1, \ldots, k \\ \phi_i(x^k_0) \text{ o/w.} \end{cases}$$

By extension, we have:

$$x_i^k \leftrightarrow (B_k \land x_i^{k+1}) \lor (\neg B_k \land \phi_i(x^k_0))$$

Now if a Fuzzy point安居.

If $\neg B_k$, then $x_i^k \leftrightarrow \phi_i(x^k_0)$ for all $i$.

For each subformula $C$ of $A_j$,

$$\neg B_k \to \left( C(x^k_0) \to C(\neg \phi) \right)$$

Argue by contradiction of $C$ (as usual)

[Rk: This is also prep. for the variable renaming case.]

[M aggreg. (ψ ⊕ x) → (D(ψ) ⊕ D(x)) be poly symmetric, for $D = D(x)$ any formula.]

Then

$$\neg B_k \land \neg A_m \to \neg A_j(x_i)$$

and $\neg A_j(x^k_i) \lor \neg B_k$, i.e., a contradiction.

Q.E.D.
Theorem 1: Every Frege sentence is SF.

Pf.
Resolution — in to prove completeness

1/ Define literal $x, y, z, \overline{x}, \overline{y}, \overline{z}$, ...

Clause $C$: finds set of literals $x, x \in C$

Meaning: disjunction

Set of clauses $T^*$: meaning: conjunction

Unsatisfied

A set $T$ of clauses is unsatisfiable if $T \vdash \bot$ is a tautology

The empty clause is unsatisfiable

2/ Resolution rule:

\[ \frac{C \cup D}{C \cup D} \]

Pand $(C \cup D) \cup \phi$ is a clause.

Resolution satisfies $\phi$ (empty clim)

Note $T \cup \phi, T' \vdash C$

Suppose $\vdash T' \Rightarrow T'$ is unsatisfiable

$T' \cup C \Rightarrow T' \cup C$

in $\forall x \in T, T' \cup C \Rightarrow T' \cup C$.

Pf easy $\vdash T' \cup C \Rightarrow T' \cup D \vdash T' \cup C \cup D$.

3/ Completion Theorem

(a) If $T$ is unsatisfiable, $T \cup \phi$

(b) If $T \cup C, T \cup C'$

Pf. By Davis-Putnam procedure [DP(\phi)] (or for first order logic?)
Let $T_0 = T$ \\
\text{where } $T_0 = \{D \in T \mid D \text{ does not "clash" with } C \}$

Given some $x \in T_0$ that does not appear in $C$

Split $T_x$ into $T = T_x \cup T_{\bar{x}}$

\begin{align*}
&\text{where } x \in D, \forall D \in T_x \\
&\bar{x} \in D, \forall D \in T_{\bar{x}} \\
&x \in \bar{D}, \forall \bar{D} \in T_x \\
&\bar{x} \in D, \forall D \in T_{\bar{x}}
\end{align*}

For all $D, E \in T_0$, $x \in E \in T_x$

From $D, E$ of a clause

Let $T_{x,1} = T_x \setminus C \cup \bar{T}_{\bar{x}}$

Claim $T_{x,1} \neq C$

PROOF: if not $\exists T \in T_{x,1} \text{ s.t. } T \neq C$, $\exists x \in \{x, \bar{x}\}$

Since $T \not\in C$ (indeed, $T \not\in C$)

\exists x \in E \in T \text{ s.t. } T \in E$

Now flip value of $T(x)$ to $T'(x) = \bar{T}$, $T'$ also w.l.o.g.

\begin{align*}
&\exists D, x \in E \text{ s.t. } T'(x) = \bar{x} \\
&\text{so } x \not\in T' \text{ (since } x \in D) \\
&\text{Now } D, E \text{ do not have a clause variable } x \text{ s.t. } T, T'
\end{align*}

Thus $D, E \in T_{x,1}$. Now $T \not\in D, E \not\neq$

Repeat loop

until all vars are renamed (except $x$ that remains $x$)

$T_m \not\neq \emptyset$ since $T_0 \not\in C$

\text{So claim } $D \in T_m$, $D \in C$ since $D$ has only

\text{clauses that occur in } C

\text{qed}

Rk: The proof is regular (and even oblivious to variable order)

Defn: Regular
Remarks: This proof is especially large in cost. 

Theorem: If \( F \) is satisfiable, \( \exists \) a variable, \( X_i \) of \( \phi \), \( \phi \) is satisfiable. 

Theorem: Any resolution tree of \( \phi \) is satisfiable. 

Let \( \phi \) be a set of clauses. 

**Definition:** \( \phi \) is satisfiable. 

(i) \( \forall x_{ij}, i = 0, 1, \cdots, j = 0, \cdots, n-1 \) \( x_{ij} \) is either true or false. 

(ii) \( \forall (x_{ij}) \), \( \neg x_{ij} \) is true. 

(iii) \( \forall (x_{ij}), \neg x_{ij} \) is true. 

(iv) [Optimal]: \( \forall (x_{ij}) \), \( \neg x_{ij} \) is true. 

(v) [Optimal]: \( \forall (x_{ij}), \neg x_{ij} \) is true. 

(vi) [Optimal]: \( \forall (x_{ij}), \neg x_{ij} \) is false. 

**Proof:** We use the paradigm that a tree-like resolution proof is an explicated decision tree. 

At each node, ask: 

1. Go left or right to the clause that contains the negated form of \( X \). 

2. (If \( \phi \) is satisfiable, get the same answer.) 

3. Go always at a clause that all literals in \( \phi \) are set false by the earlier query answers. 


Input: A satisfiable truth clause. 

Steps: Query truth value of \( \phi \). 

Output: A falsified truth clause.
Defn: size $\subseteq$ of conclusion refutation.

Then a tree-like refutation proof of depth length $h$ and size $S$ gives rise to a
decision tree of the above form, of length $h + \text{size } S$.

As discussed above.

The left subtree of $C$ subsumes $D$ iff CED

Subsumption Rule: \[ \frac{C}{D} \text{ of CED.} \]

Then $T \models \phi$ by a tree-like proof of size $S$

the $T \models \phi$ by a tree-like refutation proof of size $S$

Then $T \models \phi$ by a (tree-like) refutation

proof of a refutation of subproof of size $S$

the $T \models \phi$ by a refutation proof of size $S$

Aff of A. Finish theorem with irregular phrase

$D_x, D_{\bar{x}} (\phi)$

Ex: $E \subseteq X$

$A_x, A_{\bar{x}}$

$A_{\bar{x}}$

Add $x$ to every line between $A_x$ and $D_x$.
Remove the phrase $T$.

Claim: Result is a tree-like refutation.

At $D_x$, is subproof.

Ex: $E', x$

$E', x$

is a valid conclusion refutation (with a unit $x$ in $E'$ or $E$).
Then B. But let the projection be \( C_1, C_2, \ldots, C_n \).

Prove: By induction we assume \( C_i \) is the \( (i-1) \)st element of \( C_i \) such that \( C_i \) is a subset of \( C_i' \) for each \( C_i' \in C_i \).

We construct \( C_i \) as follows:

By induction on \( i \):

If \( C_i \cap C_i' \neq \emptyset \), we denote \( C_i \) as \( C_i' \).

If \( C_i \cup C_i' = C_i' \), \( C_i \) is replaced by \( C_i' \).

If \( \forall x \in C_i \), consider \( \exists C_i' \) such that \( x \notin C_i' \).

Finally, for each \( D_j \), \( C_i \) is replaced by \( D_j \).

Claim: A unique \( C_i \) for the projection, of height \( h \).

And see if you think the regular result of height + see 5.
For each tree $T$, label each node $v$ of the tree with the maximum depth of the minimum subtree rooted at $v$.

At the lower, the clause is selected by an right clause.

Apply previous construction.

Proof:

Let $w$ be the width of a clause.

Width of a variable $\phi$ is $w^{0(1)}$.

The $T \vdash \phi$, the $T \vdash \phi^c$, and $n = w^{0(1)}$.

Proof: Let $\text{Var}(w)^2 = n^{0(1)}$ many clauses.

Let's consider tree-like proofs and their size and relationship with

Thus [CET'96; Benne Pitoni'96]

There is a deterministic algorithm which given a tree $T$, $S$ selects $S$ $T \vdash \phi$ together with a tree-like refutation of size $S$.

Proof: determines that $T$ is unsatisifiable in time $n^{O(1)}$.

Proof: Let $F(S, n) =$ running time of algorithm (TBD) on input $S$ with $n$ variables.
Algorithm: For each of the $2n$ leaf nodes of $T$, repeatedly check if $T_{x=p}$ is unsatisfiable. If none, answer "true", "unknown". If for the first one found, set $x=T$ and call recursively.

Runtime: $F(S, n) = 2n \cdot F(S/2, n) + F(S, n-1)$

We claim $F(S, n) \leq n^{3.5\log n}$.

To prove this, note $F(S, 0) = 1$.

And $n^{3.5\log n} \geq \sum_{i=1}^{n} 2^i F(S/2, i) \leq \sum_{i=1}^{n} 2^i \cdot i^{3.5\log 2} \leq n \cdot 2n^{3.5\log 2}$

or $n \cdot 2n \cdot n^{3.5\log 2} \leq n^{3.5\log 5}$.

Then $|B_S - W_T| = 0$ if width($T$) = $w_0$ and $T \leq \varphi$ is 2-connected.

Then $T$ has a refinement (decomposition) of size width $\leq w_0 + \log 5$.

Proof: the converse of the refit of $T \leq \varphi$ is true.

Suppose $|R_1| < $\frac{1}{2}$.

From $R \times 1_\Phi$:

1. each clause with $\bar{x}$ is removed (the one here!)
2. $x$ is removed from clauses containing it
3. Resolution of $x$ (first occurrence by regularity)
4. It is a refinement of $T_{\bar{x}}$ of size $\frac{1}{2}$. Hence done.
Hence $T_{\geq x}$ has a reduction $R_x$ of width $\leq (w_0 + \log 5) - 1$ by the 3rd hyp.

In $R_x$, union clauses on $\emptyset$ clauses of $T$

or clause $C$ on $C \in T$.

Put the $\geq x$ back in and propagate down
get a reduction $R''_x$ of $x$ of width $\leq (w_0 + \log 5)$.

By 3rd hyp, from $R''_x$, then a clause $R'_x$
of $\emptyset$ of width $\leq (w_0 + \log 5)$

It is become on $\emptyset$ clauses of $T$

and $\emptyset$ clause $C \in T$.

For

New clause $\overline{C} \in S$ from $R''_x$ by

2. Replace every $C$ in $R''_x$ wirh

\[
\frac{R''_x}{\overline{C}}
\]

6. Every all occurrence of $\overline{x}$ is other chain

Width is $\leq (w_0 + \log 5)$

Next, depth $\leq w_0 + O(\sqrt{n \log 5})$ for degenerate

Runtime: $O\left(\frac{n}{\log 5}\right)$ for deg prime.
[CEI '96; Beame-Pitassi '96; BenSasson-Wdowinski '01]

**Definition**
- Width of a clause $= \#$ of literals $\overline{w(C)}$
- Width of a refutation $= \max_{CFR} \overline{w(C)} \overline{w(R)}$

$$\overline{w(T \vdash \phi)} = \min \{ \overline{w(R)} : R \text{ is a refutation of } T \vdash \phi \}$$

(Trivially: $\overline{w(T \vdash \phi)} \geq \min \{ \overline{w(T_0)} : T_0 \models T, T_0 \vdash \phi \}$.)

**Theorem**
- If $\overline{w(T \vdash \phi)} = w$, then $T \vdash \phi$ in $O(w)$ steps ($O(w)$ = # clauses in the refutation).

**Proof**
- There are only $(2w)^w = n^{\overline{w}(w)}$ many clauses of width $\leq w$.

Since $(2w)^w = n^{\overline{w} \log n} = n^{w \log n} = n$.

Let's consider tree-like proofs + their size/width tradeoff.

**Theorem** [CEI; BP]
- There is a deterministic algorithm, which computes $T, S$ s.t. $T \vdash \phi$ with a tree-like proof of size $S$.
Sufficient to have

\[ F(S, n) \geq 2n F(S/2, n) + F(S, n-1) \]

Since \( F(S, 0) = 1 \), need

\[ F(S, n) \geq 2n^2 F(S/2, n) \]

with \( F(S, n) = n^{3 \log 5} \) this is clear

\[ n^{3 \log 5} \geq 2n^2 \cdot n^{3(\log 5) - 3} \]

\[ \text{qed} \]

Theorem [CEY; BSW]: If \( \Gamma \vdash \varphi \) true like, then

\[ w(\Gamma \upharpoonright \varphi) \leq w_0 + \log S \]

where \( w_0 = \max \{ w(C) : \text{CEY} \} \).

**Proof:** Consider the refutation of \( \Gamma \)

tree-like and regular:

\[ \begin{array}{c}
\text{Wlog } |R_1| < S/2 .
\end{array} \]

Form \( R_1, \neg \neg \neg \neg \quad R_2 \).

By induction, \( w(\Gamma_{|x=F}) \leq w_0 + \log (S/2) = (w_0 + \log S) - 1 = k - 1 \).

Lemma: If \( w(\Gamma_{|x=F}) \leq k - 1 \) & \( w(\Gamma_{|x=F} \upharpoonright \varphi) \leq k \), then \( w(\Gamma \upharpoonright \varphi) \leq k \).

**Proof:** From \( R_1(R_{|x=F}) \), add each until clause is either

1. \( \text{CEY} \)
2. \( C \) s.t. \( \text{CEY} \).

Add \( x \) back and percolate down, get \( \Gamma \upharpoonright \varphi \) will width \( k \),

or (7) \( \Gamma \upharpoonright \varphi \) width \( k - 1 \).

Do some \( R_2(R_{|x=F}) \). Give at last a ref. with \( k + 1 \).
For each \( CE \), \( R \)' s.t. \( CE \) \( CE \), reason \( \Gamma \upharpoonright \varphi \) to the

other \( C \).

This yields a valid proof of width \( k \).

**Remark:** Close to the end of the proof.
Theorem [CE1; BS-W]: If \( r \cdot T \prec S \) the
\[
\frac{\omega(T \prec \phi)}{\omega_0 + O(\sqrt{2n \log S})} \leq \frac{\omega_0 \cdot \log S}{\omega_0 + O(\sqrt{2n \log S})}
\]

Proof:
Correct

Cavelley [CE1, BP]: There is an algorithm of deterministic
which when \( T \prec \phi \) correctly determines \( T \) is unsatisfiable.

Proof:
Let \( R \) be a size \( S \) refutation of \( T \). Say \( w_0 \) wlog.
Let \( d = \sqrt{2n \log S} \)

Call a clause \( \text{fat} \) if \( w(c) > 1 \).

\[
a = \frac{1}{1 - \frac{d}{2n}} = (1 - \frac{d}{2n})^{-1}
\]

Idea: Some literal occurs in fraction \( \frac{a}{2n} \) of fat clauses.

Claim: If \( \exists R \) has \( \leq a^b \) fat clauses and is a \( \Omega(n) \) ref.

then \( w(T_1 \phi) \leq \omega_0 + d + b \).

when \( \omega_0 \geq \Omega(\max[w(c), 1]) \)

By induction, \( b = 0 \) is trivially true

End Step

Choose some literal \( c \) in the ref.

Form \( R_{1x=T} \). \( R_{1x=T} \) has \( \leq a^b \) many fat clauses

so \( R_{1x=T} \) has a refutation of width \( \leq \omega_0 + d + b - 1 \)

by induction.

And \( R_{1x=T} \) has a refutation of width \( \leq \omega_0 + d + b \).

Hence, by lemma, \( w(T_1 \phi) \leq \omega_0 + d + b \).

Proof: good claim.

Thus:

\[
\frac{\omega(T_1 \phi)}{\omega_0 + d + \frac{\log S}{\log(1 - \frac{\log S}{2n})}} = \omega_0 + d + \frac{\log S}{\log(1 - \frac{\log S}{2n})} \leq \omega_0 + d + \frac{\log S}{\log \frac{\log S}{2n}} = \omega_0 + d + \sqrt{2n \log S}
\]

\[
= \omega_0 + O(\sqrt{2n \log S}).
\]

QED
Lower bounds for PHP

\[ \text{PHP}_n^{\text{HPP}} - \text{class of with } n \text{ (unfortunately!)} \]

1. \( \forall x, y \in V \quad x \not\sim y \quad V \rightarrow U \quad V = \{1, \ldots, n\} \quad U = \{1, \ldots, n\} \)

2. \( \forall x, y \in V \quad x \not\sim y \quad \forall z \in V \quad z \not\sim y \quad \forall \epsilon_i = x \_i \)

Spanner PHP. \( G \) - bipartite graph on \( V \cup U \), \( E = \epsilon \cup E \_\epsilon \)

1. \( \forall x, y \in V \quad x \not\sim y \quad \forall \epsilon \in E \)

2. \( \forall x, y \in V \quad x \not\sim y \quad (i, j) \in E \)

We'll choose \( G \) to be a "bipartite expander" of a special kind: a \((nH, n, \delta, r, \epsilon)\) \( (\delta = 5, \epsilon = 1) \)

s.t. \( \forall V \subseteq V \), \( |V'| \leq r \), \( \forall V' = \{y \in U : \exists i \in V, (i, j) \in E\} \)

s.t. \( |\epsilon \_V'| \geq \epsilon \cdot |V'| \)

**Theorem**: For some constant \( C \):

Then a random bipartite graph of degree 5 is a \((n + H, n, \delta, \epsilon)\) expander.

Proof: Omitted (the usual counting argument)

**Theorem**: For constant \( k \), \( \text{aw}(G_{PHP\_n^{\text{HPP}}}, 1 - \epsilon) \geq kn \).

**Corollary**: \( G_{PHP\_n^{\text{HPP}}} \mid - \phi \) requires \( S \geq 2^{2n} \).

**Proof**: \( \text{aw}(G_{PHP\_n^{\text{HPP}}} \mid - \epsilon) \leq 2^{2(n \log \epsilon_5 + 5)} + n^2 \leq O(n \log S) \) \( \epsilon \leq \frac{1}{2} \) \( S \gg 2n^2 \).
Proof of Theorem

For $C$ a clause, define

$$
\mu(C) = \min\{N'/1 : \{ST_i : i \in V \setminus \{\text{all literals of } C\}\} \subseteq N'/N\}
$$

For $C$ an initial clause, $\mu(C) \leq 1$

For $C = \emptyset$, $\mu(C) \geq \frac{1}{N} = \frac{1}{r}$

If any $V' \subseteq V$ has $|V'| \geq |V'|/4$ neighbors in $U$, then $N'/N \leq 4$ by Hall's Theorem. Then, if a matching $M$ involving any $V' \subseteq V$, $|V'|/4$, in $ST_{V'}$, then $ST_{V'}$ connected

For $D \subseteq E$, $\mu(C) \leq \mu(D) + \mu(E)$ - subadditivity

Therefore, if $R: GPP^{b,1-n} \rightarrow \emptyset$, $\exists C \in R$ "complex clause"  

such that

$$
\frac{1}{2} \geq \frac{1}{2c} \leq \mu(C) \leq \frac{1}{r} = \frac{1}{c}.
$$

Choose one such clause $C$.

Claim: $w(C) > \mu(C) \geq \frac{1}{2c}$.

Proof: Pick a minimal size $V'$ s.t. $ST_{V'} \cup \neg \neg = C$. (so $\mu(C)$).

Then $\mu(C) = |V'|/4$ may yield s.t. $\exists ! V' \subseteq (G) \notin E$.

Subclaim: for each such $V'$, $C$ has a literal $x_{ij}$ or $\neg x_{ij}$.

Proof: If not, choose at $i$ be s.t. $(x_{ij}) \in E$.

By minimality, $T = ST_{V'} \cup \neg \neg \cup \overline{E}$, $T \neq ST_i$, $T \notin C$.

In $T$, set $x_{ij}$ true, so $T \notin ST_j$.

+ by assumption, $T \notin C$

+ by inspection, $T \notin ST_{V'} \cup \neg \neg$.

By assumption, we are in $G^{b,1-n}$.

$w(C) \geq w(\neg \neg) \geq \frac{1}{2c}$ for $C \in G^{b,1-n}$ - expand

Q.E.D.
Deg 6: Craig Interpolates + Manytime Craig Interpolate + Resolution

[Mundici '84; Buss-Pitassi-Raz '95; Razborov '95; Krajíček '97; Pudlák '97]

Then [Craig interpolates]

Let $A(\overline{p}, \overline{q})$ and $B(\overline{p}, \overline{r})$ be formulas with $n$ variables (only) as indicated.

Suppose $A(\overline{p}, \overline{q}) \rightarrow B(\overline{p}, \overline{r})$ is $\Sigma^0_1$-takable.

Then $\exists C = C(\overline{p})$ such that $A(\overline{p}, \overline{q}) \rightarrow C(\overline{p})$ and $C(\overline{p}) \rightarrow B(\overline{p}, \overline{r}).$

Proof:

Let $\overline{t_1} \ldots \overline{t_k} \in \{0,1\}^m$ be the $k$-way conjunction.

Let $C(\overline{p}) = \bigvee_{i=1}^{k} \overline{p}(\overline{t_i})$

where $\overline{p}(\overline{t_i}) = p_{t_1} \land p_{t_2} \land \cdots \land p_{t_k}$

and $p_{t_i} = \left( \begin{array}{c} \overline{t_i} \\ \overline{p} \end{array} \right)_{t_i}$

Then clearly $C(\overline{p}) \land A(\overline{p}, \overline{q}) \rightarrow C(\overline{p})$

Note $C(\overline{p})$ is true, let $\overline{t_0}$ be such $A(\overline{p}, \overline{q}).$

The $B(\overline{p}, \overline{r})$ follow for all truth $\overline{t_0} \in \{0,1\}^m$

Note

Equivalent formula: $\exists C(\overline{p}) \land A(\overline{p}, \overline{q}) \lor B(\overline{p}, \overline{r})$, then

$\exists C(\overline{p}) \land \forall \overline{t_1}(\overline{p}) \land \exists \overline{t_2} C(\overline{p}) \land \Theta$, the $B(\overline{p}, \overline{r})$ is true

$\forall \overline{t_0}, \overline{t_1}$ of $C(\overline{p})$, the $A(\overline{p}, \overline{q})$ is false
Thm' [Mundici '89]: If there is a polynomial size upper bound on the size of $C$, then (in terms of the sizes of $A + B$), the $NP \cap coNP \subseteq P/poly$.

cave: $NP/poly \cap coNP/poly \subseteq (P/poly)$, so $NC/poly \subseteq NP/poly$.

Let $\exists \forall A(\bar{p}, \bar{q})$ express an $NP/poly$ property of $\bar{p}$.
+ $\forall \bar{p} B(\bar{p}, \bar{q})$ is the same property of $\bar{p}$ in $coNP/poly$ form.

Then $\exists \forall (A(\bar{p}, \bar{q}) \rightarrow \forall \bar{p} B(\bar{p}, \bar{q}))$ is valid.

Claim: $C(\bar{p}) \equiv \exists \forall A(\bar{p}, \bar{q}) \rightarrow C(\bar{p})$ and $C(\bar{p}) \rightarrow B(\bar{p}, \bar{q})$.

So $C(\bar{p})$ expressed $\equiv \exists \forall A(\bar{p}, \bar{q}) \equiv \forall \bar{p} B(\bar{p}, \bar{q})$.

gave a poly size (circuit)/formula for the NP/poly property.

Then Summarize the $\bar{p}$'s occur only positively in $A(\bar{p}, \bar{q})$
+ negatively in $B(\bar{p}, \bar{q})$. The $C(\bar{p})$ and $\exists \forall A(\bar{p}, \bar{q})$
claim is that $\bar{p}$ occur only positively in $C(\bar{p})$.

$\exists \forall A(\bar{p}, \bar{q})$ is a monadic formula of $\bar{p}$,
then it is a monadic propositional formula $C(\bar{p})$.

For negativity, we $C(\bar{p}) \equiv \forall \forall B(\bar{p}, \bar{q}) \equiv \neg \exists \forall B(\bar{p}, \bar{q})$...
Theorem: Let $T = \{A_i(\tilde{p}, \tilde{r}), B_j(\tilde{p}, \tilde{r})\}_i$ be a set of clauses, with a reduced refutation of $\emptyset$ clauses.
Then there is a refutation $C(\tilde{p})$ such that

(i) $\bigwedge_i A_i(\tilde{p}, \tilde{r}) \rightarrow C(\tilde{p})$, i.e., $\neg C(\tilde{p}) \rightarrow \bigvee_i \neg A_i(\tilde{p}, \tilde{r})$

(ii) $C(\tilde{p}) \rightarrow \neg \bigvee_j B_j(\tilde{p}, \tilde{r})$, i.e., $C(\tilde{p}) \rightarrow \bigwedge_j \neg B_j(\tilde{p}, \tilde{r})$.

and $C(\tilde{p})$ has a circuit (dag) size $\leq 3n$.

If the refutation is tree-like, $C(\tilde{p})$ is a formula of size $\leq 3n$.

Pf: For each clause $E$ in the refutation $R$, we form a clause $C_E$ such

A truth assignment $T$ with $T(E) = 1$

$T(C_E) = \text{Falsum}$ \implies \exists i T(A_i(\tilde{p}, \tilde{r})) = \text{Falsum}$

$T(C_E) = \text{Truth}$ \implies \exists j T(B_j(\tilde{p}, \tilde{r})) = \text{Falsum}$

The desired $C$ is $C = C_{\emptyset}$ ($\emptyset$ - looith in $R$)

We construct $C_E$ inductively by:

For $E = A_i$, each and once with clause $C_{A_i} = \top$

For $E = B_j$ \ldots \ldots $C_{B_j} = \neg \top$

Resolution Steps

Resolution $C_E$ \quad $E = F \text{Pe}$ \quad $F, \neg C_{\text{Pe}}$ \quad $G_{\text{Pe}}$

Resolution $G_{\text{Pe}}$ \quad $F, \neg C_{\text{Pe}}$ \quad $G_{\text{Pe}}$ \quad $E = F \text{U} \text{G}$

$C_E = \overline{C_{\text{Pe}}} \lor (F \land \overline{C_{\text{Pe}}})$

$C_E = C_{\text{Pe}} \lor G_{\text{Pe}}$

$C_E = C_{\text{Pe}} \lor G_{\text{Pe}}$, $E = F \text{U} \text{G}$
Resumé of a
\[ \text{F,} \\bar{\text{G,}} \quad \text{E = F, G} \]

\[ \text{CE} \overset{df}{=} \text{C,} \bar{\text{F,}} \bar{\text{G,}} \quad \text{E = F, G} \]

PTI Resolution P1.

Suppose \( T(E) = T(F, G) = \text{False} \).

Then \( T(CE) = T\left( \left( \text{F,} \bar{\text{G,}} \right) \wedge \left( \text{G,} \bar{\text{F,}} \right) \right) \).

Suppose \( T(CE) = \text{False} \).

\[ \text{Then } T(F) = \text{False} \]

\[ T(F) = \text{False} \]

\[ \text{WTS } T(F, G) = \text{False} \]

If \( T(\text{G,} \bar{\text{F,}}) = \text{True} \), then \( T(\text{F,} \bar{\text{G,}}) = \text{False} \).

\[ \text{Then } T(G, \bar{F}) = \text{False} \]

\[ \text{Suppose } T(CE) = \text{False} \]

\[ \text{Then } T(G, \bar{F}) = \text{False} \]

\[ T(G, \bar{F}) = \text{False} \]

\[ \text{WTS } T(F, G) = \text{False} \]

If \( T(\text{G,} \bar{\text{F,}}) = \text{False} \), then \( T(F, \bar{\text{G,}}) = \text{False} \).

\[ \text{Then } T(F) = \text{False} \]

\[ T(F) = \text{False} \]

\[ \text{WTS } T(F, G) = \text{False} \]

II Resolution P2:

\[ \text{F, } \bar{\text{G,}} \quad \text{E = F, G} \]

Suppose \( T(E) = \text{False} \).

\[ \text{Then both } T(F) = \text{False} \] and \( T(G) = \text{False} \).

\[ \text{Then, either } T(F, G) = \text{False} \text{ or } T(G, F) = \text{False} \text{ depending on } T(F, G) = \text{False} . \]
Recall $C_E = C_{F_{1E}} \lor C_{F_{2E}}$.

* If $\tau(C_E) = \text{False}$, then $\tau(C_{F_{1E}}) = \text{False} \lor \tau(C_{F_{2E}}) = \text{False}$.

   Apply the $\textsc{hy}$ to one of them to get
   \[ \exists i \cdot \tau(A_i) = \text{False}. \]

* If $\tau(C_E) = \text{True}$,

   then at least one of $T(C_{F_{1E}})$
   
   \[ T(C_{F_{1E}}) = \text{True} \implies \tau(C_{F_{2E}}) = \text{True}. \]

   By symmetry, we have $T(C_{F_{2E}}) = \text{True}$.

   If $T(C_{F_{2E}}) = \text{False}$, use the $\textsc{mod}$ hyp to get
   \[ \exists j \cdot \tau(B_j) = \text{False}. \]

   Let $T = T'$ except $T'(F_{2E}) = \text{False}$ (Sup $F_{2E}$ val).

   Then $T'(C_E) = \text{False}$ (since $C_E$ does not involve $F_{2E}$!)

   \[ + \quad T'(C_{F_{1E}}) = \text{False}, \]

   hence $T'(B_j) = \text{False}$ (since $F_{2E}$ not in $B_j$).

   Can of resolve on $X_2$ is dual.

\textsc{A.E.D.}!!
The result above, but also assume that 

\[ \text{appears only positively in } A_i \text{'s or only negatively in } B_j \text{'s.} \]

The abbreviation for some monotone \( C(p) \).

**Proof:** Similary, but all some major changes:

For each \( E \) in \( \mathcal{E} \), define

\[ E^A = \text{E with all } r \text{-Herds removed} \]

\[ E^B = \ldots \text{g-Herds removed}. \]

We define \( C_E \) as before, except

Replace \( \text{in } P_e \)

\[ \frac{E, P_e \quad G, P_e}{F, P_e} \]

\[ E = F, G \]

\[ C_E = C_{F, P_e} \lor (P_e \land C_{G, P_e}) \quad \# \text{p's negation in } B_j! \]

\[ C_E = (C_{F, P_e} \lor P_e) \land C_{G, P_e} \quad \text{p's negation in } A_i \text{'s} \]

We then prove by induction on \( E \) in \( \mathcal{E} \):

(a) If \( T(E^A) = T \) and \( T(G) = f \) then \( \exists i \ T(A_i) = F \).

(b) If \( T(E^B) = T \) and \( T(G) = T \), then \( \exists i \ T(B_j) = F \).

We'll just do the \( \sim p \)'s negation \( \sim \) by case.

Assume \( T(E^A) = F \), \( T(G) = f \).

Then \( T(G, P_e) = F \) \lor \( T(P_e \land G, P_e) = F \).

If \( T(P_e) = F \), \( T(F, P_e) = F \).

If \( T(P_e) = T \), \( T(G, P_e) = F \) \lor \( T(G, P_e)^A = T((G, P_e)^A) = F \).

So \( \exists i \ T(A_i) = F \) by \( \sim p \).

If \( T(P_e) = F \), then \( T(F, P_e)^A = F \) \lor \( T((F, P_e)^A) = F \).

So \( \exists i \ T(A_i) = F \) by \( \sim p \).
Assume \( T(E^B) = \text{False} + T(C_E) = \text{True} \)

\[ \text{Now } (E_{Fe})_B \text{ is } F^B \text{ (since positive discharge only in } B) \]

So \( T(F^B) = \text{False} \), since \( T(E^B) = \text{False} \).

By \( E(C_E) = \text{True} \), either \( \text{False} \) or \( T(C_{Fe}) = \text{True} \).

Either \( T(R^2) = \text{True} + T(C_{Fe}) = \text{True} \).

In former case, \( \neg E_i \), \( T(B_i) = \text{False} \), by mod. hyp.

In latter case, \( T(C_{Fe}) = \text{False} \), so \( \neg E_i \) \( T(B_i) = \text{False} \) by mod. hyp.

Resolution on \( g_i \):

\[
\begin{array}{ccc}
F_{g_i} & C_{g_i} & \text{E} = F_g. \\
\end{array}
\]

Suppose \( \neg T(A^B) = \text{False} \), \( T(C_E) = \text{False} \).

Then \( T(C_{Fe}) = \text{False} + T(C_{Fe}) = \text{True} \).

Either \( T(A^B) = \text{False} \) or \( T(C_{Fe}) = \text{False} \).

In either case, \( \neg E_i \), \( T(B^B) = \text{False} \), by mod. hyp.

Resolution on \( v_i \):

\[
\begin{array}{ccc}
F_{v_i} & C_{v_i} & \text{E} = F_g. \\
\end{array}
\]

Suppose \( T(E^A) = \text{False} + T(C_E) = \text{False} \).

Then \( T(F_{v_i}^A) = T(F^A) = \text{False} + \text{True} \).

Either \( T(C_{Fe}) = \text{False} \) or \( T(C_{Fe}) = \text{False} \).

In either case, \( \neg E_i \), \( T(A^B) = \text{False} \), by mod. hyp.
Sym $\varepsilon T(E^8) = \text{False}$. So $T(E_{12}^8) = T(C_{12}^8) = \text{True}$.

And for either $T(E_{12}^8) = \text{False}$ or $T(E_{12}^{10}) = \text{False}$.

In all cases, and by p gives $\exists \theta T(\varepsilon \theta)$ = True.

Red.

Define a clique-colony structure with

Let $G$ be a graph on \([n] = \{1, \ldots, n\}\)

$P_{ij}$ = edge between $i$ and $j$,

A $k$-clique $c$ coded by $\beta_{3i}$

\[
\begin{align*}
\{ & \beta_{3i}, \beta_{5i}, \beta_{7i}, \beta_{9i}, \\
& \beta_{11i}, \beta_{13i}, \beta_{15i}, \beta_{17i} : P_{ij} \}
\end{align*}
\]

$5_{\varepsilon i}$ define a 1-1 map from \([k] : [k] + 1\)

And \(\varepsilon i\) a $k$-clique.

An $l$-colony, coded by $\nu_{ij}$

\[
\begin{align*}
\{ & \nu_{ij} : i \in [k] \\
& \nu_{iu}, \nu_{jv} : u, v \}
\end{align*}
\]

$\{ \nu_{iu}, \nu_{jv}, P_{ij} \}$ No nodes of same color are adjacent

And $-\text{Clique}_{k_{1,\varepsilon}}(\beta_{3i}) \cup \text{Colony}_{k_{1,\varepsilon}}(\nu_{ij})$

Any resolution of spines of size \(\leq 5\) will give a monotone interpolant of size \(\leq 35\).
Thm [Rackoff84, Alon-Boppana87]

Any $k$-clique cover of a graph on $n$ vertices contains a $k$-clique in every graph of $k$ colors for size $2^{O(k^2)}$.

Conley, Sem-Turkoglu apply to eliminate reflexive $k$-clique colorings.

Of course, this is weaker than what is known via PHP.

However, this gives a proof (reflection) size lower bound on term of circuits, and so gives a method of likely proof complexity to circuit complexity.
AlgebraicProof Systems

Work over a field (sometimes a ring) usually \( \mathbb{F}_p \) or \( \mathbb{F}_q \).

Notation: \( \mathbb{F} \) for fields

Boole formulas connect to algebraic formulas \( \mathbb{F}_q \):

\[
\begin{align*}
\forall y & \in \mathbb{F} (y = 0 \text{ is implied}) \\
xy & = x \cdot y \\
x+y & = 1 - (1-x,y) \cdot (1, -y) \\
x & = 1 - x.
\end{align*}
\]

But other ad-box encodings are used as well.

Definition: Let \( \mathbb{F} \) be a field, and \( Q_1, \ldots, Q_m \) be \( \mathbb{F} \)-polynomials in variables \( x_1, \ldots, x_n \).

A nullstellensatz refutation of \( Q_1, \ldots, Q_m \) is a set of polynomials \( F_1, \ldots, F_m, R_1, \ldots, R_n \) such that

\[
F_1 Q_1 + \ldots + F_m Q_m + R_1 (x_1^2 - x_1) + \ldots + R_n (x_n^2 - x_n) = 0
\]

for some \( d \neq 0, d \in \mathbb{F} \).

Then \( \text{[Nullstellensatz]} \) is the set \( Q_1 = 0, \ldots, Q_m = 0 \) does not have a \( 0/1 \) solution if and only if there is a nullstellensatz refutation of \( Q_1, \ldots, Q_m \).

If \( \mathbb{F} \) (namely finite or \( \mathbb{F} \) algebraically closed) consider the radical of the ideal, but since using \( 0/1 \) solutions, these assumptions are not needed here.

For omitted - use induction on \( n \). (?)
Let \( Q = \{ Q_1, Q_{-1} \} \). 

**Proof**: By induction, 

\[ Q(x, x_{n-1}) \text{ and } \overline{Q(x, x_{n-1})} \text{ have} \]

\[ NS \text{ refutations} \]

\[ \sum_{j=1}^{n} F^{(i)}_j Q_j(x, j) + \sum_{j=1}^{n} R^{(i)}_j (x_j^2 - x_j) = 1, \quad j \neq 0, 1. \]

From \( \overline{F}^{(1)}_n \)

Note \( Q_j(x, x_n) = \bigoplus_{i} p_i(x) x_i + q_i(x) \)

So \( x_n Q_j(x, x_n) = p_i(x) x_n^2 + q_i(x) x_n \)

Thus, \( x_n \overline{F}^{(1)}_n \)

\[ \sum_{j=1}^{n} F^{(i)}_j Q_j(x, j) + \sum_{j=1}^{n} R^{(i)}_j (x_j^2 - x_j) + \left( \sum_{i} p_i(x) (x_n - x_j) \right) = x_n \]

A similar argument gives a linear constraint equal to \( 1 - x_n \).

Adding give a NS refutation of \( \overline{Q} \).

**Refutation Calculus** (aka "Grobner basis system")

Refutation system:

- Work over a field \( F \) (arithmetic)

Initial polynomial \( Q_0, Q_{-1}, x_i^2 - x_i, n \in F \)

Inference rules:

\[ \frac{p}{q} \rightarrow \overline{p, q} \]

\[ \frac{p_1, p_2}{p_1 + p_2} \]

Last line: \( x_n \) and \( \#0, \#0 \) for \( F \) (for field \( d = 1 \))
PC: Soundness - immediate
Completeness - immediate for completion of NS

Def: Degree of a PC refutation - max degree poly in the ref.

Next step: Allow arbitrary terms, not just polynomials, but this is just equivalent to Frege (for finite $E$ at least)

Then [CFI 96]: Given $Q_1, ..., Q_m$ in variables $x_1, ..., x_n$
there is an $O(n^3)$ algorithm for deciding if there is a
degree $d$ refutation of $Q_1, ..., Q_m$ (if $m < n^d$)

**Proof Idea:** Gröbner basis algorithm:

Let $\mathcal{S} = \{Q_1, Q_2, ..., Q_m\}$ - stack of pols to process

Let $B = \emptyset$ - a set of polynomials of distinct
leading terms (by degree $d$)

Algorithm Choose $Q \in \mathcal{S}$, remove $Q$ from $\mathcal{S}$

Reduce $Q$ by:

- If $\deg(Q) = \deg(P)$ for some $P \in B$
  - set $Q = Q - \deg(P) \cdot P$ and continue
- repeat: If $Q \in B$, continue to next $Q \in \mathcal{S}$
- Else: Add $Q$ to $B$

If $\deg(Q) < d$, add $x_i \cdot Q \to S$ for all $x_i$

Repeat until:

$\deg(B) < d$, $d \notin S$ (Construct) - terminates
or $S$ is empty (No refutation)
So we usually treat algebraic part size by degree
   Constant degree \Rightarrow \text{Polynomial size}
   Polylogarithmic degree \Rightarrow \text{Quasipoly size}
   Linear or \textit{f} degree \Rightarrow \text{Exponential size}.

After '84:
   \text{BKVPR}'84: \text{Raz '87}
\text{Arora-Timoftezzio}
\text{Krajicek, Pillers-Pudlak}
\text{Free proofs of Counting Fan}
\text{Cantor when } \gcd(m, m') = 1

\text{BKVPR}
\text{Buss-Krajicek-Englhauser}
\text{Pudlak-Razborov-Sgall}
\text{Exponential lower bounds}
Defin

Mod m counting principle: \( \text{Count}_m^N \) \( m \geq 1, N > 0. \)

Let \( N \neq 0 \mod m \)

Variable \( p \) for each \( e \in \{0, 1, 2, \ldots, N - 1\} \)

\[ \text{Count}_m^N = \forall (p \in \mathbb{P}) \quad \forall (e \in \{0, 1, 2, \ldots, N - 1\}) \]

\[ \text{if } p \mid N \]

\[ \text{else } e \in \{0, 1, 2, \ldots, N - 1\} \]

i.e. \( N \) cannot be partitioned into sets of size \( m \)

where \( \text{if } e \in \mathbb{P} \quad \text{then } 0 < |e| < m. \)

[BFK89]

Fact: If \( p_1, \ldots, p_r \) are the prime factors of \( m \),

the \( \text{Count}_m^N \)

can be parsed by a poly-size constant-depth

Frege proof for instances of \( \text{Count}_m^N \). \( \text{Count}_m^N \)

Conversely:

\( \text{Count}_m^N \) follows by poly-size constant-depth

Frege proof for \( \text{Count}_m^N \) instances of \( \text{Count}_m^N \).

Defins

\( (N, \Phi) \) polynomial system: \( N \equiv 0 \mod q \)

\( \forall \sigma \quad \sum_{e \in \{0, 1, \ldots, N - 1\}} x_e = 1 \) \quad \{ \forall e \quad \text{one part in each} \}

\( \forall e, f \quad x_e \cdot x_f = 0 \) \quad \{ \forall e, f \quad \text{exclude same part} \}

Thus [BFK89]

Let \( q \) be prime, \( m \equiv \Phi \mod m' > 1 \)

\( \text{Let } d \) \( \text{degree of } NS \) \( \text{refined} \) \( \{ \forall e \text{ (depth) over } Z \} \)

\( \text{Then } \forall e \text{ Frege proof of } \text{Count}_m^N \) \( \text{for instance of } \text{Count}_m^N \) \( \text{recently } \text{incorporate} \)

\( \exists N \in \text{Count}_m^N \) \( \forall \text{ for size } 6 > 0 \) \( \text{decide with proof} \)
\[ \sum Q_v = \sum \left( \sum x_e - 1 \right) \]

\[ = \sum \sum x_e - N \]

\[ = -N \pmod{q} \]

Thus a NS refutation.
Then \([BIPRS]\) Any \(\mathbb{R}\) reflection of the \(\mathbb{Q}\) reflection for \(\mathbb{Q}\) odd \(p\) over \(\mathbb{Z}\), \(n\) given

has degree

\[ \Omega \left( \frac{N^{1/2} \log p}{p} \right) \ll \frac{1}{p}. \]

Corollary: all Frattini groups of \(\mathbb{Z}/p\) contain instance of \(\mathbb{Z}/n\) for \(n\) a prime

\[ N \ll \log \frac{d}{\delta} \]

Thus \([BGJP]\): Bus Gyarfas Imrepezzio Polczi

Any polynomial calculus reflection of \(\mathbb{Z}/p\) for instance of \(\mathbb{Z}/n\) requires degree \(\gg \log p\) for \(\mathbb{Z}/n\) with \(n\) a prime

\[ \Omega \]

\[ \Phi \text{ works for composite } p \text{ as well} \]

\[ \Phi \text{ idea via first step: } \text{first step:} \]

and 

\[ \text{diameter two of first } \]

Use a low degree subgraph of a low degree graph of high expansion.
Thin [Razborov '98]

Over any field polynomial calculus sets of PPM
require degree ≥ N/2.

see also IPS '99 [Impagliazzo-Pudlak-Spiegel]