<u>Propositional Proof Systems</u> – Overview/Introduction

Resolution
Frege systems
extended Frege / extended Resolution
Cutting planes (integer linear inequalities on 0/1 variables)
Nullstellensatz / Polynomial calculus (polynomials over finite fields)
Stronger proof systems
Abstract proof systems.

Goal of a proof systems is to prove tautologies

<u>Example.</u>

Language: Variables $x, y, z, \ldots$ $x_1, x_2, x_3, \ldots$
that range over $\{T, F\}$

Fanin-2: $\wedge, \vee, \rightarrow$
Unary negation

Formulas: $x_i \mid \neg\varphi \mid (\varphi \wedge \psi) \mid (\varphi \vee \psi) \mid (\varphi \rightarrow \psi)$

~~$p \rightarrow (q \rightarrow$~~ $((p \rightarrow p) \rightarrow p) \rightarrow p$

$\neg(\neg(\neg p \vee p) \vee p) \vee p$ is a Tautology.

<u>Step depth</u> Truth assignment
$\rho: Vars \rightarrow \{T, F\}$

T	F	F	F
T			
F			

<u>Defn</u> Tautology – True under all truth assignments

<u>Simple fact</u> φ is a tautology $\Leftrightarrow$ $\neg\varphi$ is not satisfiable

Def φ is <u>satisfiable</u> iff φ is true under some truth assignment
iff $\neg\varphi$ is false under ~~all~~ some truth assignment

$\neg\varphi$ is satisfiable iff φ is false under some truth assignment
iff φ is not a tautology

I.e. Showing φ is a tautology is same as showing
$\neg\varphi$ is not satisfiable.

<u>Thus</u> TAUT is coNP complete

How to show φ is a tautology

(a) Try all truth assignments.

(Exponential time! in worst case)

(b) Give a proof.

Defn Frege system (in language $\wedge, \vee, \neg$) $\mathcal{F}$.

Axioms are: Any formula of the form

$$\varphi \to (\varphi \to \varphi)$$
$$(\varphi \to \psi) \to ((\varphi \to (\psi \to \chi)) \to (\varphi \to \chi))$$
$$(\varphi \to \psi) \to (\varphi \to \neg\psi) \to (\neg\varphi)$$
$$\neg\neg\varphi \to \varphi$$

$$\varphi \wedge \psi \to \varphi \qquad \varphi \wedge \psi \to \psi$$
$$\varphi \to (\psi \to (\varphi \wedge \psi))$$
$$\varphi \to \varphi \vee \psi \qquad \psi \to \varphi \vee \psi$$
$$(\varphi \to \chi) \to (\psi \to \chi) \to (\varphi \vee \psi \to \chi)$$

Only rule of inference: Modus Ponens

$$\frac{\varphi \quad \varphi \to \psi}{\psi}.$$

Defn $\mathcal{F} \vdash \varphi$ iff $\exists\, \varphi_1 \ldots \varphi_\ell = \varphi$, etc.

~~Thm So~~

Thm $\mathcal{F}$ is sound

$\mathcal{F}$ is complete

$\boxed{\text{Also implicationally sound \& complete}}$

Thm If φ is a tautology, then φ has an $\mathcal{F}$-proof of size $\leq 2^{|\varphi|}$

Defn $|\varphi| = \#$ of symbols in φ

size of $\mathcal{F}$-proof $= \sum |\varphi_i|$, φ_i a line in $\mathcal{F}$.

Pf omitted.

Key properties of $\mathcal{F}$:

(1) Soundness/completeness.

(2) Polynomial time verifiability.

$\exists$ poly time procedure which given P, φ determine (a) if P is a valid $\mathcal{F}$-pr

(b) output the formula φ that P is a proof of.

<u>Defn</u> An abstract proof system is a polynomial-time function $f: \{0,1\}^* \xrightarrow{\text{onto}} TAUT$.

<u>Discuss</u>: $\mathcal{F}$ is an abstract proof system.

$$f(P) = \begin{cases} \text{last line of } P & \text{if } P \text{ is valid Frege} \\ x_1 \vee \neg x_1 & \text{o/w.} \end{cases}$$

ZFC " " " " "

Resolution is too, – a "refutation system"

E.g. For φ a DNF, express $\neg\varphi$ as a CNF,

i.e. $\neg\varphi$ is $\bigwedge_i C_i$ and C_i a clause.

A resolution refutation of $\neg\varphi$ is a derivation of $\emptyset$ from $\{C_i\}_i$

is a resolution pf of f

This applies only to DNF formulas φ, however.

~~Theorem~~ <u>Defn</u> Let f, g be abstract proof systems

f <u>simulates</u> g iff $\forall P, \varphi$, $g(P) = \varphi$

$\Rightarrow \exists P'$, $|P'| \le p(|P|)$ and $f(P') = \varphi$

for some polynomial $p(\cdot)$

f p-simulates g iff ..

f is ~~simple~~ maximum iff $\forall$ aps g, f simulates g.

f is <u>maximal</u> iff $\neg\exists g$: g simulates f and f does not simulate g

~~Theorem [Cook-Reckhow]~~

~~$\exists$ a p-simulating aps f iff NP = coNP~~

f is <u>polynomially bounded</u> iff $\forall \varphi \in TAUT$ $\exists P$, $|P| < p(|\varphi|)$ $f(P) = \varphi$

for some polynomial p

<u>Theorem</u> [Cook-Reckhow '79]: $\exists$ a polynomially bounded aps f

iff $NP = coNP$.

Pf (Easy). Note TAUT is coNP complete.
(Pf: TAUT $\in$ coNP by defn)
& $\varphi \notin SAT$ iff $\neg\varphi \in TAUT$ shows $\overline{SAT} \leq_m TAUT$.

$\Leftarrow$ If NP = coNP, TAUT $\in$ NP. So from $Q \in P$ time, poly r

$\forall \varphi \quad \varphi \in TAUT$ iff $\exists x \leq r(|\varphi|)\, Q(x, \varphi)$.

Define fcn f by $f(\langle x, \varphi\rangle) = \begin{cases} \varphi & \text{if } Q(x,\varphi) \\ x_1 \vee \neg x_1 & \text{o/w.} \end{cases}$

$\Leftrightarrow$ Given poly bd'd ap'n f

$\forall \varphi \,(\, \varphi \in TAUT$ iff $\exists P \leq p(|\varphi|)\, f(P) = \varphi)$

gives an NP-definition of TAUT

qed.

Corolly: If no poly bd'd ap'n exists, then $P \neq NP$.

Known Res, CP, NS, PC – not poly bd'd
F, eF – ~~not~~ open.

Day 2

Best known lower bound for F:

Let $\top$ abbreviate $\varphi(x_1 \vee \neg x_1)$
$\bot$ " $(x_1 \wedge \neg x_1)$

Let φ_0 be $\top$
φ_{i+1} be $\bot \vee \varphi_i$
So $|\varphi| = \Theta(n)$

For Day 2

Thm If $P \vdash \varphi_n$ then $|P| = \Omega(n^2)$ i.e. $|P| > c \cdot |\varphi|^2$ for some

Pf: Fix $P \vdash \varphi_n$.
For $i \geq n$, define φ_i to be actively used in P (actively used)
iff is a $\varphi \vee \psi$ of one of the axioms

If $|P| \leq cn$ some φ_i is not actively used. Choose one, say the last.
Form P' by replacing every subfmla φ_i in P with F.
P' is still a valid pf, but its last line is not a tautology. #

Discuss proof size symbols vs. lines!

Extended Frege

extension rule $x \leftrightarrow \varphi$ i.e., $(x \to \varphi) \wedge (\varphi \to x)$

Defn Seq $\varphi_0 \ldots \varphi_n$

and φ_i – axiom or inferred by MP

or $x \leftrightarrow \psi$ where x not used in ψ, any φ_j, $j<i$ or ~~any~~ in φ_n.

Thm If P is an EFrege proof of φ of m lines, then $\exists P'$, EF proof of φ of $O(m + |\varphi|^2)$ symbols.

Pf (Sketch):

(a) Enumerate all formulas in P which are active in some inference of P. (Explain) i.e. appear as a line or is a component formula of an axiom or a use of MP.

actively used

$x_1 \ldots x_{m'}$ $\quad m' = O(m)$.

For new variable $y_{x_1}, y_{x_{m'}}$, use extension axioms $y_i \leftrightarrow x_i$. } Idea.

or is a subformula of the last line of P $O(|\varphi_n|^2)$

(b) For each subformula in P of the form $\neg\psi$ or $\psi \vee \psi'$ or $\psi \wedge \psi'$ or $\psi \to \psi'$ (resp.)

with both ψ, ψ' active,

~~add extension~~ use extension rule

Do in correct order

$y_{\neg\psi} \leftrightarrow \neg y_\psi$ or $y_\psi \leftrightarrow y_\psi \vee y_{\psi'}$ etc. (resp.)

Since $O(m)$.

(c) For each line φ_i in P,

prove y_{φ_i} : (c.i) Axiom (Do one example)

(c.ii) MP $\quad \dfrac{\varphi_i \quad \varphi_i \to \varphi_j}{\varphi_j} \qquad \dfrac{y_{\varphi_i} \quad y_{\varphi_i \to \varphi_j}}{y_{\varphi_j}}$

$O(m)$ symbols.

Example #1

(b) $\chi_{\varphi\to(\varphi\vee\psi)} \Longleftrightarrow \chi_\varphi \to \chi_{\varphi\vee\psi}$ extension

(a) $\chi_{\varphi\vee\psi} \Leftrightarrow \chi_\varphi \vee \chi_\psi$ "

(c) $\chi_\varphi \to \chi_\varphi \vee \chi_\psi$ axiom

(a) → (b) → (c) → $\chi_{\varphi\to(\varphi\vee\psi)}$ Tautology of size $O(1)$
Hence has a proof of size $O(1)$
by completeness

$\therefore$ $\chi_{\varphi\to(\varphi\vee\psi)}$ 3 uses of MP.

Ex #2

$$\frac{\varphi \qquad \varphi\to\psi}{\psi}$$

(a) χ_φ ind hyp

(b) $\chi_{\varphi\to\psi}$ ind hyp

(c) $\chi_{\varphi\to\psi} \Leftrightarrow (\chi_\varphi \to \chi_\psi)$ extension

$\chi_{\varphi\to\psi} \to$ (c) $\to \chi_\varphi \to \chi_\psi$ Tautology of size $O(1)$

$\chi_\varphi \to \chi_\psi$ 2 uses of MP

χ_ψ one more use of MP

(d) From ψ_{φ_n} derive φ_n

$O(|\varphi|)$ steps, $O(|\varphi|^2)$ symbols.

<u>Method</u>: For each subformula ψ of φ_n, prove

$\gamma_\psi \leftrightarrow \psi$. (working from smallest formula out to largest)

<u>qed</u>

<u>Rk</u> Earlier proof lower bound also applies to eF.
<u>Thm</u> If eF $\vdash^{n \text{ symbols}} \varphi$, then F $\vdash^{n \text{ lines}} \varphi$. <u>Open</u> F simulates eF?

[CR'79] <u>Theorem</u> PHP_n^{n+1} has poly size eF proofs.

<u>Def</u> Let $n \geq 2$ PHP_n^{n+1} is the following formula

$$PHP_n^{n+1}(\vec{x}) := \bigwedge_{i=1}^{n+1} \bigvee_{j=1}^{n} x_{ij} \rightarrow \bigvee_{i=1}^{n} \bigvee_{i'=i+1}^{n+1} \bigvee_{j=1}^{n} x_{ij} \wedge x_{i'j}$$

<u>Pf (Sketch)</u>

Introduce new variables $x^l_{i,j}$ for $1 \leq i \leq l+1$; $1 \leq j \leq l$

So that

x^n_{ij} is just x_{ij},

~~each~~ ~~for~~ ~~So~~

and for each $l < n$,

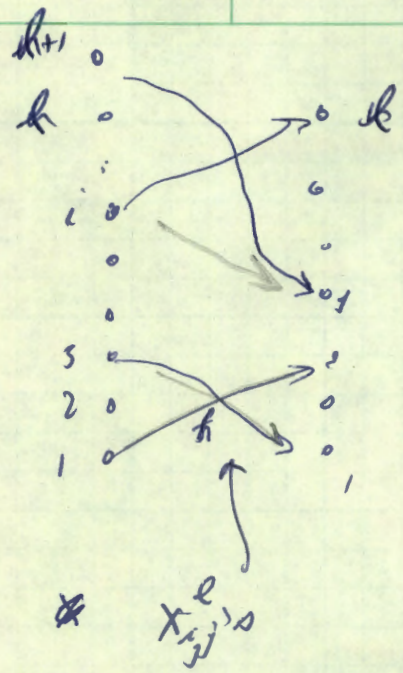
$$\neg PHP_l^{l+1}(\vec{x}^l) \rightarrow \neg PHP_{l-1}^{l}(\vec{x}^{l-1}) \qquad (\star)_l$$

has a ~~F~~ proof of size $l^{O(1)}$

Then from $(\star)_l$'s ~~derive~~ and for $PHP_1^2(\vec{x}^1)$

prove $PHP_1^2(\vec{x}^1) \rightarrow PHP_n^{n+1}(\vec{x}^n)$

and hence $PHP_n^{n+1}(\vec{x}^n)$.



$$\boxed{x^{\ell-1}_{ij} := x^{\ell}_{ij} \vee \left(x^{\ell}_{i,\ell} \wedge x^{\ell}_{\ell+1,j}\right)} \quad \star$$

<u>Get:</u> $\cdot$ $LHS\text{-}PHP^{\ell+1}_{\ell}(\vec{x}^{\ell}) \to LHS\text{-}PHP^{\ell}_{\ell-1}(\vec{x}^{\ell-1})$

$RHS\text{-}PHP^{\ell}_{\ell-1}(\vec{x}^{\ell-1}) \to RHS\text{-}PHP^{\ell+1}_{\ell}(\vec{x}^{\ell})$

<u>Thus</u> $PHP^{\ell}_{\ell-1}(\vec{x}^{\ell}) \to PHP^{\ell+1}_{\ell}(\vec{x}^{\ell+1})$.

<u>qed..</u>

<u>Theorem</u> [Buss 1986] $\mathcal{F} \nvdash^{poly} PHP^{n+1}_{n}(\vec{x})$.

<u>Pf</u> omit – Uses counting.

<u>Theorem</u> [Bun, Jan, 2014] $\mathcal{F} \nvdash^{qpoly} PHP^{n+1}_{n}(\vec{x})$.

<u>Pf</u> We mimic the proof of [Cook-Reckhow '79].

<u>Define:</u> φ^{ℓ}_{ij} by:

Fix $\ell = 0..n$

Let $f : [n+1] \to [n]$ (~~potentially~~ be assumed to violate the PHP^{n+1}_{n}

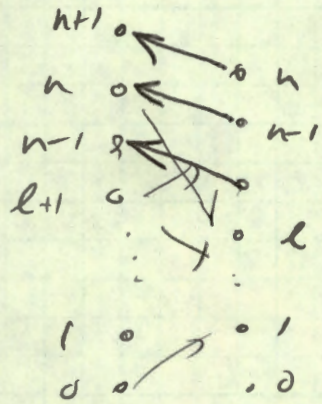
Define a directed graph G^{ℓ} by

G^ℓ : bipartite on $[n+1] \dot\cup [n]$, directed
$= ([n+1]\times\{0\}) \cup ([n]\times\{1\})$

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

and for $j>\ell$, $j\le n$

G has an edge $(j,1)\to(j+1,0)$



$\varphi^\ell_{ij} \iff$ "exist ~~an edge~~ a path in G^ℓ from i to j
(for $i\le \ell+1$, $j\le \ell$)

More generally define
$\mathrm{Reach}^\ell_{\langle i,\alpha\rangle,\langle j,\beta\rangle}$: $\exists$ path in G^ℓ from $\langle i,\alpha\rangle$ to $\langle j,\beta\rangle$.

<u>Claim</u> φ^ℓ_{ij} has a quasipolynomial formula:

$\cancel{\varphi^{\ell,m}_{ij}}$ $\mathrm{Reach}^{\ell,m}_{\langle i,\alpha\rangle,\langle j,\beta\rangle} \iff \exists$ path of length $\le m$

$$\mathrm{Reach}^{\ell,m}_{\langle i,\alpha\rangle,\langle j,\beta\rangle} \iff \bigvee_{\langle k,\gamma\rangle} \left(\mathrm{Reach}^{\ell,\lceil m/2\rceil}_{\langle i,\alpha\rangle,\langle k,\gamma\rangle} \wedge \mathrm{Reach}^{\ell,\lfloor m/2\rfloor}_{\langle k,\gamma\rangle,\langle j,\beta\rangle}\right)$$

for $m\ge 2$.

$\mathrm{Reach}^{\ell,1}_{\langle i,\alpha\rangle,\langle j,\beta\rangle}$ defined in obvious way.

<u>Claim (2)</u> φ^ℓ_{ij}'s satisfy the equations (*) of page 7 and this can be proved w/ qpo by size proof.

(Proof idea from Buss '86]

Using polysize formulas for Vector Addition,

<u>define:</u>

$$\text{Count}_i(x_1 .. x_r) \iff \geq i \text{ of the } x_j\text{'s are true.}$$

<u>Then show:</u>

$$\text{Count}_i\left(\bigvee_j x_{j,1}, \bigvee_j x_{j,2}, .. \bigvee_j x_{j,n}\right) \geq n+1.$$

$$\vdots \quad \vdots \quad \vdots$$

~~and~~ if $f: [n+1] \xrightarrow[\text{onto}]{1-1} [n]$.

~~Hence~~ Whence obtain a contradiction.

<u>Extended resolution</u> substitution SF p simulates e F.

<u>Cutting planes</u>

~~4 Frege sys~~

<u>Theorem</u> V Tree-like (+ log ~~depth~~ height) Frege systems p-simulate dag-like Frege system.

<u>Pf</u> ~~Let $\varphi_0, \varphi_1, \ldots \varphi_k$ be a Frege~~

Let $A_1, A_2, \ldots, A_n$ be a (dag-like) Frege proof of size $m \leq n \cdot \max_i |A_i|$.

Let $B_i := A_1 \wedge A_2 \wedge \ldots \wedge A_i$ (associated left-to-right)

$B_0 = T$ (true)

<u>Claim</u> There is a tree-like, log depth (= depth $O(\log m)$) proof of $B_i \to B_j \wedge A_i$ $\forall i > j$, of size $m^{O(1)}$.

Pf: We have proofs of (i) $(\varphi_1 \wedge \varphi_2) \wedge \varphi_3 \to \varphi_1 \wedge (\varphi_2 \to \varphi_3)$

and (ii) $\varphi_1 \wedge (\varphi_2 \wedge \varphi_3) \to (\varphi_1 \wedge \varphi_2) \wedge \varphi_3$

and (iii) $(\varphi_1 \wedge \varphi_2) \wedge \varphi_3 \to [(\varphi_1 \wedge \varphi_2) \wedge \varphi_3] \wedge \varphi_2$

and (iv) $(\varphi \to \psi) \to (\varphi \wedge \chi) \to (\psi \wedge \chi)$.

Thus we have Frege proofs of

$B^*_{i+1} := A_{i+1} \wedge \ldots A_m$

$B_i \to B_{i-1} \wedge (A_{i-1} \wedge A_i)$ by (i)

$B_{i-1} \wedge A_i \to B_{i-2} \wedge (A_{i-1} \wedge A_i)$ by (i)

$\vdots$

$B_i \wedge B^*_{i+1} \to B_{i-1} \wedge B^*_i$

$B_{j+1} \wedge (A_{j+1} \wedge \ldots A_i) \to B_j \wedge (A_{j+1} \wedge \ldots A_i) \to [B_j \wedge (A_{j+1} \wedge \ldots A_i)] \wedge A_j$ (by)

$\to [B_{j+1} \wedge (A_{j+2} \wedge \ldots A_i)] \wedge A_j$ by (ii) + (iv)

by (ii) + (iv)

$\to B_i \wedge A_j$

Now combine in a tree-like manner $\dfrac{\varphi \to \psi \quad \psi \to \chi}{\varphi \to \chi}$ (infinite ~~par~~ pairs cases hyp's once end)

1st complicated proof!! Use simpler proof!!

<u>Claim</u>: $(B_i \to A_j) \to (B_i \to (A_j \to A_k) \to (B_i \to A_k)$
has a ~~the~~ proof or constant height

<u>Claim</u> $B_j \to B_{j+1}$ has a proof of bounded depth + poly size (in n)

<u>Pf</u> (a) A_{i+1} is an axiom
~~Prove B_j~~ ~~Let A_k~~

<u>Proof</u>: $A_{i+1} \to (B_n \to A_{i+1})$ (axiom!)
Use <u>MP</u>, Get $B_n \to A_{i+1}$

(b) A_{i+1} is inferred by MP $\dfrac{A_j \quad A_{j'}}{A_{i+1}}$ where $j, j' \le i$
$A_{j'}$ is $A_j \to A_k$

~~The~~ Fixed proof of:

$B_n \to A_j \qquad B_n \to A_{j'}, \qquad A_j \to (A_{j'} \to A_k) \to A_k$

Fixed proof of $(\quad) \to (\quad) \to (\quad) \to (B_n \to A_k)$
~~Fixed~~ (instance of fixed tautology)

<u>To prove Theorem</u>: Combine ~~all~~ previous Claims' constructions in a tree like fashion to get

$B_1 \to B_n$.

<u>Now</u> B_1 is axiom so finish off w/ B_1 and MP.

QED. Theorem!

<u>Topic 2</u> Substitution Frege systems

Let $\varphi = \varphi(x_1 \ldots x_n)$ be a formula – all occurrences of x_i's indicated.

Let $\psi_1 \ldots \psi_n$ be formulas. The <u>substitution rule</u> allows

$$\frac{\varphi(x_1 \ldots x_n)}{\varphi(\psi_1 \ldots \psi_n)}$$

<u>Rk</u> All x_i's replaced "in parallel" ← Rk: Not really necessary: $n=1$ is good enough (Allow "extra" literals).

<u>Def'n</u> sF = F + substitution rule.

Note sF is sound + complete, but not "implicationally complete"

Eg. $\frac{x}{\neg x}$ but $x \to \neg x$ is not a tautology

Do Deduction Thm here.

Example $\perp_n$ has a linear size sF proof.

$x \to (\perp \vee x)$ $\quad A_i \to \bigvee_i (\perp \vee x)$

$A_0 \to A_1$ $\quad A_i(A_j/x) := A_{i+j}$

$\frac{A_1 \to A_2}{A_0 \to A_1}$ by sub repeat by substitution, sub $\top$ for x

<u>Theorem</u> sF p-simulates eF

<u>Lemma</u> If eF proves $\mathcal{F} \vdash^{m} \varphi$ using extension axioms $y_i \leftrightarrow \psi_i$ (in order)

then $F \vdash^{m^{O(1)}} (y_1 \leftrightarrow \psi_1) \to (y_2 \leftrightarrow \psi_2) \ldots \to (y_k \leftrightarrow \psi_k) \to \varphi$

<u>Pf</u> this is the well-known deduction rule, applied k times.

In detail: Using (w) $(X \wedge A) \to (X \wedge (A \to B) \to (X \wedge B))$

and $A \to (X \to A)$ w/

$X = \bigwedge_i (y_i \leftrightarrow \psi_i)$

and using $X \to (y_i \leftrightarrow \psi_i)$ for fixed i, get

$X \to \varphi$ w/ poly size proof

Now use $((B \wedge C) \to A) \to B \to (C \to A)$ k times to get.

$$(\psi_1 \leftrightarrow \chi_1) \to \cdots \to (\psi_k \leftrightarrow \chi_k) \to \varphi.$$

q.e.d. Lemma.

Discussion on how tantalizing the lemma is.

Now sF-~~pro~~ p-simulates eF by in fact

$$\frac{(\chi_1 \leftrightarrow \psi_1) \to (\chi_2 \leftrightarrow \psi_2) \to \cdots ((\chi_k \to \psi_k) \to \varphi) \cdots)}{(\psi_1 \to \chi_1) \to (\psi_1, \quad , \quad , \quad , \quad , \quad , \quad , \quad , \quad)} \text{ sub}$$

$\psi_1 \to \chi_1$ (tautology)

$(\chi_2 \leftrightarrow \psi_2) \to \cdots (\chi_k \leftrightarrow \psi_k) \to \varphi$

↓ repeat k-1 more times

φ.

QED Theorem

Theorem eF p-simulates sF [Dowd '85 - unpublished. Krajíček & Pudlák '89]

Pf: Let $A_1, A_2, \ldots, A_m$ be an sF-proof of $A = A_m$

Let $x_1 \ldots x_p$ be the ~~fr~~ variables in all of $A_1 \ldots A_m$.

Goal: Given an eF proof of A_m

Suffices (by deduction theorem) to take $\neg A_m$ as an extra axiom (non-schema) and derive a contradiction

For $t = m, \dots, 1$, we ~~the~~ introduce new variables x_i^t i.e. p. ~~Part~~ by extension, and will prove: for $t = m, \dots, 1$

$$C_t := \bigvee_{i=1}^{t} \neg A_i(\vec{x}^t) \quad \left(= \left(\bigvee_{i=1}^{t-1} \neg A_i(\vec{x}^t)\right) \vee \neg A_t(\vec{x}^t) \right).$$

Here ~~this~~ $A_i(\vec{x}^t)$ means A_i with each x_j replaced by x_j^t.

Now C_m follows immediately from $\neg A_m$. (as $x_i^m := x_i$, $\forall i$)

Ind: $\neg C_t$ follows from the fact A_t ~~sin~~ is an axiom (!)

So, it will suffice to give a poly size (Frege) proof of

$$C_{t+1} \wedge (\text{all extension axioms}) \to C_t$$

Extension rule $x_i^m \leftrightarrow x_i$ $(\forall i)$ – base case

Now suppose x_i^{t+1} have been introduced $(\forall i)$ and C_{t+1} holds

~~any~~

Case (1) A_{t+1} is an axiom. (or A_{t+1} is inferred by MP.)

In this case,

$$C_{t+1} \wedge A_{t+1} \to C_t$$

and we take $x_i^t \leftrightarrow x_i^{t+1}$ (even, can be the same variable)

Case (2): C_{t+1} is inferred by substitution for some $j \le t$.

$$\frac{B(x_1 \dots x_p) = C_j}{C_{t+1} = B(\varphi_1 \dots \varphi_p)}$$

Define, by extension rule, (intuition:

$$x_i^t := \begin{cases} x_i^{t+1} & \text{if } \bigvee_{i=1}^{t} \neg A_i(x_i^{t+1}) \\ \varphi_i(\vec{x}^{t+1}) & \text{if } \neg(\underline{\qquad\qquad}) \end{cases} \quad)$$

More formally: $x_i^t \leftrightarrow \left(x_i^{t+1} \wedge \bigvee_{t=1}^{t} \neg A_i(\vec{x}^{t+1})\right) \vee \left(\varphi_i(\vec{x}^{t+1}) \wedge \neg \bigvee_{t=1}^{t} \neg A_i(\vec{x}^{t+1})\right)$

Argue by cases:

Case (1) $\bigvee_{i=1}^{t} \neg A_i(x^{t+1})$

Then $\forall\ A_i(\vec{x}^t) \leftrightarrow A_i(\vec{x}^{t+1})$, ☆'

So C_t holds.

Case (2): $\neg \bigvee_{i=1}^{t} \neg A_i(x^{t+1})$.

Then $\neg A_{t+1}(\vec{x}^{t+1})$ by C_{t+1}.

Claim: From this $\neg A_j(x^t)$ follows ☆'

General proof method for both: Fix ψ_1, ψ_2, fix formula $D(\psi)$

Prove by "brute force" induction on the complexity of subformulas $E(\psi)$ of $D(\psi)$ that

$$(\psi_1 \leftrightarrow \psi_2) \rightarrow (E(\psi_1) \leftrightarrow E(\psi_2))$$

Simple Cases: E is y. then trivial

E is $E_1(y) \wedge E_2(y)$

Already prove $(\psi_1 \leftrightarrow \psi_2) \rightarrow (E_1(\psi_1) \leftrightarrow E_1(\psi_2))$

From there $(\psi_1 \leftrightarrow \psi_2) \rightarrow (E(\psi_1) \leftrightarrow E(\psi_2))$

Eg for ☆' apply with $\psi_1 = \neg A_i(\vec{x}^{t+1})$ $\psi_2 = x_i^t$ $D = A_j(x_i)$

for ☆ " " $\psi_1 = x_i^{t+1}$ $\psi_2 = x_i^t$ $D = A_j$

QED

Def'n Renaming Frege: rF

$$\frac{\varphi(x,\dots)}{\varphi(y,\dots)}$$ where y is any variable.

Claim rF p-simulates eF. [Buss '95] "Sum rules"

Pf Suffices to show rF p-simulates sF.

Suppose $rF \vdash^n A(x_1 \dots x_p)$ $\quad x_1 \dots x_p$ all vars in the proof

~~(a) Let x_1^0 be x_1, x_1^1 be $\overline{x_1}$~~ Find $A_1, A_2, \dots, A_m = A$

(a) $sF \vdash x_1 \wedge \dots \wedge x_p \to A$ has a proof of size $O(|A|^2)$

Pf for each subformula B of A,

prove: $x_1 \dots x_p \to B$ or $x_1 \wedge \dots x_p \to \neg B$

(a') $sF \vdash \neg x_1 \wedge \dots \neg x_p \to A$ has a proof of size $O(|A|^2)$.

Pf By sym argument.

Letting $\mathrm{Distinct}^2(\vec{x})$ be $(\neg x_1 \vee \neg y_2 \vee \dots \vee \neg y_p) \wedge (x_1 \vee y_2 \vee \dots \vee y_p)$

suffices to give a poly size F proof of $\mathrm{Distinct}^2(\vec{x}) \to A$.

By Deduction Rule it suffices to show

F + 2 new (non-schematic) axioms $\neg x_1 \vee \dots \neg x_p$

and $x_1 \vee \dots \vee x_p$

has a poly size proof of A.

We'll show how to derive $A_1, A_2, \dots, A_m$ successively

Suppose $A_1 \dots A_{i-1}$ already proved.

case (i) A_i is an axiom ✓

case (ii) A_i follows by MP from $A_j, A_{j'}$, $j, j' < i$ ✓

Case (iii) A_i is $A_j(\varphi)$ where $A_j = A_j(x)$ is already proved.

Then prove:

~~(b) Find φ_i: $(x_i \wedge \varphi_i)$~~

(b) $A_j(x_\ell)$ for each $\ell = 1 \dots p$ (p. 2 uses of renaming)

(c) For each $l = 1..p$

$$x_l \wedge \varphi \wedge A_j(x_l) \rightarrow A_j(\varphi)$$

Same as A_i

(c') For each $l = 1..p$

$$\neg x_l \wedge \neg\varphi \wedge A_j(x_l) \rightarrow A_j(\varphi)$$

(d) by $x_1 \vee \cdots \vee x_p$ and (c), proves

$$\varphi \rightarrow A_i$$

(d') by $\neg x_1 \vee \cdots \neg x_p$ and (c') proves

$$\neg\varphi \rightarrow A_i$$

(e) By (d), (d'), proves

$$A_i$$

QED.

(HW) Let T/F substitution be $\dfrac{A(x)}{A(T)}$ and $\dfrac{A(x)}{A(\bot)}$

Show T/F-sub Frege p-simulates eF

Lecture on Proof Complexity (Seminar: Math 268)
2/7/14 - Day 4.

<u>Thm</u> sF p-simulates eF.

<u>Pf</u>: Let $A_1, A_2, \ldots, A_m = A$ be an eF proof of A.

Let $B_1, \ldots B_k$ be the uses of extension rule in ? <u>in order</u>

B_i is: $y_i \leftrightarrow C_i$ $\quad C_i = C_i(y_1 \ldots y_{i-1})$

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

Let D_j be $((B_1 \wedge B_2) \wedge \ldots) \wedge B_j$ — associated left-to-right

(1) Create an F-proof of $D_k \to A$ of polynomial size

<u>Pf</u> Usual construction

(2) Create an F proof of

$$B_k \to (B_{k-1} \to \cdots \to B_2 \to B_1 \to A).$$

<u>Constructive</u> Show: $(D_j \to A) \to [B_j \to B_{j-1} \to \ldots B_1 \to A]$

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

Nowly D_{j+1} is $D_j \wedge B_{j+1}$

and $(D_j \wedge B_{j+1}) \to A \to B_{j+1} \to (D_j \to A)$ is a tautology

and $B_j((D_j \to A) \to [B_j \to \cdots A])$ is

So $[(D_j \wedge B_{j+1}) \to A] \to [(D_j \to A) \to [B_j \to \ldots \to B_1 \to A]] \to (B_{j+1} \to [B_j \to \ldots \to B_1 \to A])$

is a tautology (in D_j, B_{j+1}, A, and $[B_j \to \ldots \to B_1 \to A]$)

(3) Use substitution of C_k for y_k + the MP with $C_k \leftrightarrow C_k$.

Repeat k times.

Discussion on appearance of variables!

<u>Thm</u> eF p-simulates sF.

<u>Pf</u> Let $A_1, A_2, \ldots A_m$ be an sF proof of $A = A_m$.

Let variables in P be $x_1 \ldots x_p$

We'll introduce (by extension) variable $x_1^k \ldots x_k^k$ for $k = m, m-1, \ldots, 1$.

And will give an (eF) proof, for each k, $\neg A_m \to B_k$, where.

$$B_k := \bigvee_{j=1}^{k} \neg A_j(\vec{x}^k)$$ — associate right-to-left (any)

where $A_j(\vec{x}^k)$ means A_j w/ variable x_i replaced by x_i^k.

<u>Base case</u> $k = m$. Identify x_i^k with x_i (or $x_i^k \leftrightarrow x_i$ by extension).

Then $\neg A_m \to \neg B_m$ is easy to prove.

<u>Inductive Step</u> Let $x_1^{k+1} \ldots x_p^{k+1}$ already be introduced and $\neg A_m \to B_{k+1}$ proved.

<u>Case (1)</u> A_k is an axiom.

Set $x_1^k \leftrightarrow x_1^{k+1}$ (i.e. one same variable, w/ unextension)

So then $A_k(\vec{x}^k)$ is an axiom

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

<u>Case (2)</u> A_k introduced by MP. A_k is inferred from A_i and $A_i \to A_k = A_j$ for some $i, j < k$. Use $\vec{x}_1^k \leftrightarrow x_1^{k+1}$ again

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

And from the $B_{k+1} \to B_k$ from the straightforwardly

<u>Case (3)</u> Substitution:

$$A_k \text{ is } A_j(\vec{\varphi}) \quad \text{where } j < k$$

and $A_j(\vec{\varphi})$ is A_j with each x_i replaced by φ_i ~~φ_i free for~~

~~Set~~

Want to define x_i^k by

$$x_i^k := \begin{cases} x_i^{k+1} & \text{if } B_k \text{, i.e. if } \bigvee_{j=1}^{k} \neg A_k \\ \varphi_i(\vec{x}_i^{k+1}) & \text{o/w.} \end{cases}$$

By extension, we have:

$$x_i^k \leftrightarrow \left(B_k \wedge x_i^{k+1} \right) \vee \left(\neg B_k \wedge \varphi_i(\vec{x}^{k+1}) \right)$$

Now w/ a Frege proof argue

If $\neg B_k$, then $x_i^k \leftrightarrow \varphi_i(\vec{x}^{k+1})$ for all i.

For each subformula C of A_j,

$$\neg B_k \rightarrow \left(C(\vec{x}^{k+1}) \rightarrow C(\vec{\varphi}) \right)$$

Argue by ind on complexity of C (as usual)

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

[More generally $(\psi \leftrightarrow \chi) \rightarrow (D(\psi) \leftrightarrow D(\chi))$ has poly size proof. for $D = D(z)$ any formula].

Then $\neg B_k \wedge \neg A_m \rightarrow \neg A_j(\vec{x}^k)$

and $\neg A_j(\vec{x}^k) \rightarrow \neg B_k$, i.e. a contradiction

QED.

<u>Theorem</u> renaming Frege primitives $\mathcal{F}$.

<u>Pf.</u>

Resolution – intro to proof complexity

1/ Define literal $x, y, z;\ \bar{x}, \bar{y}, \bar{z}, \ldots$

Clause C – finite set of literals s.t. no $x, \bar{x} \in C$

Meaning – disjunction

Set of clauses T – meaning: conjunction

~~Unsatisfied~~

A set T of clauses is <u>unsatisfiable</u>

iff the $\bigvee_{C \in T} \bigwedge_{x \in C} \bar{x}$ is a tautology.

The empty clause is unsatisfiable

2/ <u>Resolution rule:</u> $\dfrac{C \cup \{x\} \quad \{\bar{x}\} \cup D}{C \cup D}$

provided $C \cup D$ is a clause.

Resolution refutation of $\emptyset$. (empty clause)

<u>Notation</u> $T \vdash \varphi$, $T \vdash C$

<u>Soundness Thm</u> $T \vdash \emptyset \Rightarrow T$ is unsatisfiable

$T \vdash C \Rightarrow T \models C$

i.e. $\forall$ t.a.'s τ, $\tau \models T \Rightarrow \tau \models C$.

<u>Pf</u> easy from $\tau \models C \cup \{x\}$, $\tau \models D \cup \{\bar{x}\} \Rightarrow \tau \models C \cup D$.

3/ <u>Completeness Thm</u>

(a) If T is unsatisfiable, then $T \vdash \varphi$

(b) If $T \models C$, then $\exists C' \subseteq C$ s.t. $T \vdash C'$

<u>Pf</u>: By Davis-Putnam procedure [DP'60] (orig. for first order logic!)

Loop Let $T_0 = T$ (or $T_0 = \{D \in T$ s.t. D does not "clash" with $C\}$

Choose some x in T_i that does not appear in C.

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

where $x \in D$, $\forall D \in T_x$

$\bar{x} \in D$, $\forall D \in T_{\bar{x}}$

$x, \bar{x} \notin D$, $\forall D \in T_\emptyset$

For each $D \in T_x$, $\bar{x}, E \in T_{\bar{x}}$

form D, E of a clause

Let $T_{i+1} = \{$ the D, E's $\} \cup T_\emptyset$.

Claim $T_{i+1} \models C$.

Pf If not $\exists \tau \models T_{i+1}$ $\tau \not\models C$. Suppose $\tau(x) = T$ (say)

Since $T_i \models C$ (ind hyp), $\tau \not\models T_i$, Hence

$\exists E, \bar{x} \in T_{\bar{x}}$ s.t. $\tau \not\models E$

Now flip value of $\tau(x)$ so $\tau'(x) = T$, τ' o/w like τ

Then $\exists D, x \in T_x$ s.t. $\tau' \not\models D$

~~Hence~~ so all $\tau \models D$ (since $x \in D$)

Now D, E do not have a clashing variable s.t. τ, τ'

agree on all literals in D, E, but $\tau \models E$, $\tau \not\models D'$

Then $D, E \in T_{i+1}$. Now $\tau \models D, E$ #

Repeat Loop

until all vars are removed (except those in C)

$T_m \neq \emptyset$ ~~so~~, since $T_m \models C$.

So clause $D \in T_m$, $D \subseteq C$ since D has only

literals that occur in C.

q.e.d.

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

Def'n: Regular

Upper bound → Remark: this proof is exponentially large in worst case

Theorem: If T is unsatisfiable + has n variables, then $T \vdash \emptyset$ by pf of size $\leq 2^n$

Theorem: Any ~~resolution~~ tree-like resolution refutation of PHP_n^{n+1} clauses due size $\geq 2^n$.

Def'n PHP_n^{n+1} clauses are

(i) Variables are x_{ij} $i=0,\dots,n$; $j=0,\dots,n-1$

(ii) $\bigvee_j x_{ij}$, for $i=0,\dots,n$ (Total)

Big each

(iii) $\{\bar{x}_{i_1 j}, \bar{x}_{i_2 j}\}$ $\forall i_1 \neq i_2$ $\forall j$ Injection

optional

(iv) [Optional]: $\bigvee_i x_{ij}$ Surjection

(iv) [Optional]: $\{\bar{x}_{ij_1}, \bar{x}_{ij_2}\}$ $j_2 \neq j_1$ ~~Functional~~ (Single-valued)

Pf: We use the paradigm that a tree-like resolution proof is an implicit decision tree.
At each internal node, query a literal x.
Go left or right to the clause that contains the negated form of x.
→ (If re-query a literal, get the same answer.)
So always at a clause C where all literals in C are set false by the earlier query answers

~~Claim: If sequence is go~~

At end, decision tree yields a falsified clause

I.e. Input: an unknown truth assignment
Steps: Query truth values one at a time
Output: A falsified ~~truth~~ clause.

Defn size = # of clauses in refutation.

Thm A tree-like resolution proof of ~~depth~~ height h and size S gives rise to a decision tree in the above paradigm of height h + size S.

Pf As discussed above.

Defn ~~Subs~~ ~~C~~ C subsumes D iff $C \subseteq D$

Subsumption Rule $\frac{C}{D}$ if $C \subseteq D$.

Thm A If $\Gamma \vdash \phi$ by a tree like ~~regular~~ proof of size S then $\Gamma \vdash \phi$ by a tree like regular proof of size $\leq S$

Thm B If $\Gamma \vdash \phi$ by a (tree-like) ~~tree~~ proof w/ resolution + subsumption of size S then $\Gamma \vdash \phi$ by a (tree-like) resolution proof of size $\leq S$.

Pf of A. Find ~~the~~ a "non regularity" in the tree proof.

$$\frac{Dx \quad D'\bar{x}}{DD'} \ (\neq)$$

$$\frac{Ey \quad E'\bar{y}}{EE'}$$

$$\frac{Ax \quad A'\bar{x}}{AA'}$$

Add x to every line between Ax and Dx.
Remove the inference $\neq$

Claim Result is a tree-like resolution + subsumption ~~flow~~ refutation

Pf $\frac{Dx}{DD'x}$ is subsumption

$\frac{Ey \quad E'yx}{EE'x}$ is a valid resolution refutation (with a unit $x + E''$ or E.

Thm B Proof: Let the ~~pr~~ refutation be $C_1 C_2 \dots C_k = \phi$

~~Proof: By induction~~ a We form a new

~~def~~ derivation $C_1', C_2' \dots \quad C_k' = \phi$

where each $C_i' \subseteq C_i$

and each C_i is ~~ref~~ either inferred by resolution or is a repeat of a previous clause C_j' $j<i$.

Plus construct respects tree-like ~~form~~

By induction on i:

If $C_i \in T$. ~~No~~ No change $C_i' = C_i$

If ~~C_i~~ $\dfrac{C_j}{C_i}$ $C_j' \subseteq C_i$, ~~set~~ set $C_i' = C_j'$.

If $\dfrac{x C_j \quad C_k}{C_i}$; consider $\dfrac{C_j' \quad C_k'}{C_i'}$

C_j, C_k are $x C_j \quad \bar{x} C_k$

If $x \in C_j'$, set $C_i' = C_j'$

If $\bar{x} \notin C_k'$ set $C_i' = C_k'$

o/w $C_j' = x D_j' \quad C_k' = \bar{x} D_k'$ set $C_i' = D_j' D_k'$.

qed.

Corollary: A decision tree for the problem, of height h and size S yield a tree like resolution proof of height h + size S.

From decision tree T, label each node
w/ the clause containing the negation of the
literals known to be true so far.
At the leaves, the clause is subsumed by an input clause
Add subsumptions.
Apply previous construction
good.
[CEI'96, Beame Pitassi '96; Ben-Sasson + Wigderson '01]

Define width of a clause
width of a refutation of "$T \vdash_\omega A$"

Then if $T \vdash_\omega \phi$, then $T \vdash^{n^{O(\omega)}} \phi$, or $n^{\omega + O(1)}$

Pf There are $\binom{n}{\omega} \cdot 2^\omega = n^{\omega + O(1)}$ many clauses,

$n^\omega \cdot 2^\omega = (2n)^\omega$
$2^\omega = n^{\omega/\log n} = n^{O(1)}$

Lets Consider tree-like proofs + their size + relationship to width.

Thm [CEI'96; also Beame Pitassi '96]
There is a deterministic algorithm which given input T, S
s.t. $T \vdash^S \phi$ with a tree-like refutation of size S
determines that T is unsatisfiable in time $n^{O(\log S)}$.

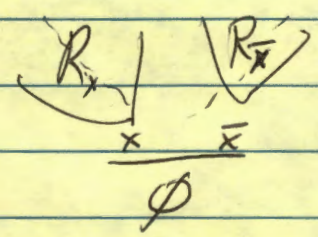
Pf: Let $F(S, n)$ = running time of algorithm (TBD)
on inputs of width n variables

<u>Algorithm</u> For each of the $2n$ literals x ~~check~~
Recursively check if $T \restriction x=F$ is unsatisfiable
If none, answer "~~Fail~~" "Unknown"
~~If~~ ~~For~~ the first one found,
set $x=T$ and call recursively

<u>Runtime:</u> $F(S,n) \le 2n\, F(S/2, n) + F(S, n-1)$
We claim $F(S,n) \le n^{3\log S}$.
To prove this, note $F(S,0) = \emptyset$ (
And
$$n^{3\log S} \ge \sum_{i=1}^{n} 2i\, F(S/2, i) \le \sum_{i=1}^{n} 2i \cdot i^{3\log S} \le n \cdot 2n\, n^{3\log S}$$
as $n \cdot 2n \cdot n^{3\log(S/2)} < n^{3\log S}$.

<u>Thm</u> [BS-W'91] If $\mathrm{width}(T) = w_0$ and $T \vdash^{S} \emptyset$ with tree-like refutation
then T ~~has~~ has a refutation (dag-like)
of ~~size~~ width $\le w_0 + \log S$.

<u>Pf:</u> ~~The~~ Consider the refutation of T (tree-like)



w/o loss of generality R is regular

Suppose $|R_x| < S/2$
Form $R_x|_{\bar{x}}$: i.e. ① each clause with $\bar{x}$ is removed (there are none!)
② x ~~occ~~ is removed from clauses where it appears.
③ Resolution on x ~~doesn't~~ (doesn't occur, by regularity)
~~④~~

It is a refutation of $T \restriction \bar{x}$ of size $S/2$. ~~Hence there~~

Hence $T_{\restriction \bar{x}}$ has a refutation R'_x of width $\leq (\omega_0 + \log S) - 1$
by the ind hyp.

In R'_x - initial clauses are (a) clauses of T
or (b) clauses C s.t. $Cx \in T$.
Put the x's back in and percolate down,
get a derivation R''_x of x of width $\leq (\omega_0 + \log S)$.

By ind hyp, from $T_{\restriction x}$, there is a derivation $R'_{\bar{x}}$
of $\emptyset$ of width $\leq (\omega_0 + \log S)$

Its leaves are (a) clauses of T
and (b) clauses C s.t. $C\bar{x} \in T$.

~~For~~
New derivation S from $R'_{\bar{x}}$ by
(a) Replacing each C in $R'_{\bar{x}}$ with

$$\frac{C\bar{x} \quad x \; R''_x}{C}$$

(b) Erasing all occurrences of $\bar{x}$ in other clauses.

Width is $\leq (\omega_0 + \log S)$ ✓

Next: ~~depth~~ width $\leq \omega_0 + O(\sqrt{n \log S})$ for daglike

Runtime: ~~$2^{O(\sqrt{n})}$~~ $n^{O(\sqrt{n \log S})}$ for daglike.

Day 5

[CEI '96; Beame-Pitassi '96; Ben Sasson-Wigderson '01]

Def'n Width of ~~of~~ a clause = # of literals $\boxed{w(C)}$

Width of a refutation = $\max_{C \in R} w(C)$ $\quad w(R)$

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

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

~~$T \vdash_w \phi$~~

Thm If $w(T \vdash \phi) = w$, then $T \vdash^{n^{O(w)}} \phi$ ($n^{O(w)}$ = # of clauses in the refutation)

Pf There are only $\leq \binom{2n}{w} = n^{w(\log(1))}$ many clauses of width $\leq w$.

Since $(2n)^w = n^w \cdot 2^w = n^w \cdot n^{w/\lg n} = n^{w + w/\log n}$

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

Thm [CEI; BP] There is a deterministic algorithm, which on input T, S s.t. $T \vdash^S \phi$ with a tree-like proof of size S determines T ~~produces a refut~~ ~~is unsatisfiable~~ is unsatisfiable in time $n^{O(\log S)}$, and for all T never falsely says T is unsatisfiable

Pf Let $F(S, n)$ = running time of the algorithm

$F(S, n) = n^{3 \log S}$.

Algorithm For each of x ~~$\bar{x}$~~ (literals, $2n$)

In time $F(S/2, n)$ check if $T|_{x=F} \vdash \phi$ recursively.

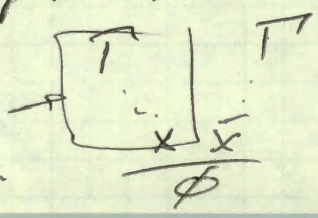
If so, check, in time $F(S, n)$, if $T|_{x=T} \vdash \phi$ recursively

~~Cor~~ **Def'n** $T|_{x=F}$ is: Each clause with $\bar{x}$ is removed

Each occurrence of x in any clause is removed

Correctness if $T \vdash^S \phi$ tree-like then

Hitting w/ $x = F$, + using subsumption — more proofs shrink. size $< S/2$.



regular

wlog is regular!!

Suffices to have

~~Need~~ $F(S,n) \geq 2n\, F(S/2, n) + F(S, n-1)$

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

$$F(S,n) \geq 2n^2 F(S/2, n)$$

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

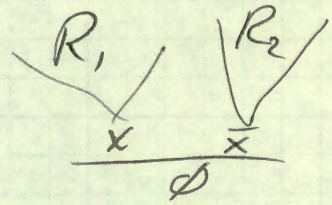
$$n^{3\log S} \geq 2n^2 \cdot n^{3(\log S)-3}. \quad \boxtimes$$

qed.

<u>Theorem</u> [CEI; BS-W]: If $T \vdash^S \emptyset$ tree like, then

$w(T \vdash \emptyset) \leq w_0 + \log S$ where $w_0 = \max\{w(C) : C \in T\}$.

<u>Pf</u>: Consider the refutation of T tree-like + regular:



Wlog $|R_1| < S/2$.

Form $R_1|_{x=F}$. a refutation for $T|_{x=F}$.

By ind hyp, $w(T|_{x=F} \vdash \emptyset) \leq w_0 + \log(S/2) = (w_0 + \log S) - 1 =: k-1$.

<u>Lemma</u> If $w(T|_{x=F} \vdash \emptyset) \leq k-1$ & $w(T|_{x=T} \vdash \emptyset) \leq k$,

then $w(T \vdash \emptyset) \leq k$.

<u>Pf</u>: From R_1' ($= R_1|_{x=F}$) ~~add~~ each initial clause is either

(a) $C \in T$

or (b) C s.t. $Cx \in T$.

Add x's back in, percolate down, get $T \vdash x$ with width k

or ($T \vdash \emptyset$ w/ with width $k-1$),

Do same for R_2' ($R_2|_{x=T}$). Gives at first a proof of width $k+1$.

For each $C \in R_2'$ s.t. $C\bar{x} \in T$, resolve w/ x to obtain C.

This makes a valid proof of width k.

qed.

Remark on dag-like form of the proof...

<u>Thm</u> [CEI; BS-W] If $\Gamma \vdash^{S} \phi$ then $w(\Gamma \vdash \phi) \le w_0 + O(\sqrt{n \log S})$

$\boxed{w_0 + O(\sqrt{n \log S})}$

~~Pf.~~

<u>Corollary</u> [CEI, BP]: There is an correct algorithm, of deterministic time $n^{O(\sqrt{n \log S})}$, which when $\Gamma \vdash^{S} \phi$, (correctly) determines Γ is unsatisfiable

<u>Pf</u>: ~~Let~~ R be a size S refutation of Γ. $S \ge 2$ wlog.

Let $d = \sqrt{2n \log S}$ Call a clause <u>fat</u> if $w(C) > d$.

$$a = \frac{1}{1 - \frac{d}{2n}} = (1 - d/2n)^{-1}$$

<u>Idea</u>: Some literal occurs in fraction $> \frac{d}{2n}$ of the fat clauses.

<u>Pf</u> Each fat clause has $> d$ literals + there are $2n$ literals.

<u>Claim</u>: If ~~R~~ R has $< a^b$ fat clauses, and is a ~~refutation~~ of Δ, then $w(\Delta \vdash \phi) \le w_0 + d + b$. where $w_0 \ge \max\{w(C) : C \in \Delta\}$

<u>Pf</u> By induction on b, $b=0$ is trivially true

<u>Ind Step</u> Choose some literal x in the idea.

Form $R_{|x=T}$. $R_{|x=T}$ has $< a^{b-1}$ many fat clauses

So $R_{|x=T}$ is a refutation of Δ $= w_0 + d + b - 1$ by ind hy.

And $R_{|x=F}$ is a refutation of width $\le w_0 + d + b$

Hence, by lemma, $w(\Delta \vdash \phi) \le w_0 + d + b$.

~~qed~~. <u>qed</u> Claim.

<u>Thus</u>: $w(\Gamma \vdash \phi) \le w_0 + d + \log_a S = w_0 + d + \frac{\log S}{-\log(1 - d/2n)} = w_0 + d + \log(2n) + \log S - \log d$

$$= w_0 + d + \frac{\log S}{-\log\left(1 - \sqrt{\frac{\log S}{2n}}\right)} < w_0 + d + \frac{\log S}{\sqrt{\frac{\log S}{2n}}} = w_0 + d + \sqrt{2n \log S}.$$

$$= w_0 + O(\sqrt{2n \log S}).$$

$\log(1-x) \le -x$

<u>QED</u>

Lower bounds for PHP

PHP_n^{n+1} - clauses of width n (unfortunately!)

(1) $\bigvee_{j \in U} x_{ij}$ $\quad i \in V$ $\qquad V \to U$, $V = \{1..n+1\}$, $U = \{1..n\}$

(2) $\bigvee_{\{i_1, i_2\}} \overline{x_{i_1 j}} \vee \overline{x_{i_2 j}}$ $\quad i_1 = x_2$.

Sparse PHP: G bipartite graph on $V \cup U$; E = set of edges

(1) $\bigvee_{(i,j) = e \in E} x_{ij}$ $\quad i \in V$ $\qquad ST_1$ axiom (sparse totality)

$G\text{-}PHP_n^{n+1}$

(2) $\bigvee_{\substack{i_1, i_2 \\ (i_1,j), (i_2,j) \in E}} \overline{x_{i_1 j}} \vee \overline{x_{i_2 j}}$. $\qquad$ (Injectivity axiom)

We'll choose G to be a "bipartite expander" of a special kind: a $(n+1, n, d, r, e)$ $\quad (d=5, e=1)$

s.t. $\forall V' \subseteq V$, $|V'| \le r$, then

$$\partial V' = \{ j \in U : \exists! i \in V', (i,j) \in E \}$$

satisfies $|\partial V'| \ge e \cdot |V'|$

~~Fact~~ For some constant c_3:

Thm: A random bipartite graph of degree 5 is a $(n+1, n, 5, n/c, 1)$ expander.

Pf: Omitted (the usual counting argument)

Theorem: $\exists$ constant k s.t. $w(G\text{-}PHP_n^{n+1} \vdash \phi) \ge kn$.

Corollary: $G\text{-}PHP_n^{n+1} \vdash^S \phi$ requires $S \ge 2^{\Omega(n)}$.

$PHP_n^{n+1} \vdash^S \phi$ " ...

Pf: $w(G\text{-}PHP_n^{n+1} \vdash \phi) \le O(\sqrt{n \log S} + 5)$ so $n^2 \le O(n \log S)$

so $\log S \ge \Omega(n)$ $\quad S \ge 2^{\Omega(n)}$.

<u>Proof of Theorem</u>

$ST_{V'} = \{ST_i : i \in V'\} \cup \{\bar{x}_{i_1 j_1} \cdot \bar{x}_{i_2 j_2} : i_1, i_2 \in V'\}$

~~the~~ For C a clause, define

$$\mu(C) = \min\{|V'| : \{ST_i : i \in V'\} \cup \{\text{Injectivity for } i_1, i_2 \in V'\} \models C\}$$

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

For $C = \emptyset$, $\mu(C) \geq n/c = r$

<u>Pf</u> Any $V' \subseteq V$ has $\geq |N'|$ many neighbors in U, for $\underline{|N'| \le r}$
So by Hall's Thm, $\exists$ a matching ~~for the~~ involving
any $V' \subseteq V$, $|V'| \le r$, hence $ST_{V'} \cup \text{Inj}$ consistent

For $\dfrac{D \quad E}{C}$, $\mu(C) \le \mu(D) + \mu(E)$ – subadditivity

Therefore, if $R : GPHP_n^{n+1} \vdash \emptyset$, $\exists C \in R$ "complex clause"
s.t. ~~not~~

$$\frac{1}{2} r = \frac{n}{2c} \le \mu(C) \le r = \frac{n}{c}.$$

Choose one such clause C.

<u>Claim</u>: $w(C) \geq \mu(C) \geq n/2c$.

<u>Pf</u>: Pick a minimal size V' s.t. $\{ST_{V'} \cup \text{Inj}\} \models C$. (size $\mu(C)$).
There are $\mu(C) = |N'|$ many $j \in U$ s.t. $\exists! i \in V'$ $(i,j) \in E$.
<u>Subclaim</u>: for each such j, C has a literal x_{ij} or $\bar{x}_{ij}$ for some i.
<u>Pf</u>: If not, ~~choose~~ let i be s.t. $(i,j) \in E$.
By minimality $\exists \tau$: $\tau \models ST_{V' \setminus \{i\}} \cup \text{Inj}$, $\tau \not\models ST_j$, $\tau \not\models C$.

In τ, set x_{ij} true, so $\tau \models ST_j$,
+ by assumption, $\tau \not\models C$
+ by inspection, $\tau \models ST_{V'} \cup \text{Inj}_{V'}$ (Injectivity can't break by choice of j.)

q.e.d. Sub Claim + Claim

~~QED~~ Hence $w(GPHP_n^{n+1} \vdash \emptyset) > \frac{n}{2c}$ for G a $(\text{hol}, n, 5, 1/2, 1)$-expander

<u>QED.</u>

Day 6 Craig Interpolation + Monotone Craig Interpolation + Resolution

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

Thm [Craig interpolation]
Let $A(\vec{p},\vec{q})$ and $B(\vec{p},\vec{r})$ be propositional formulas w/ variables (only) as indicated.
Suppose $A(\vec{p},\vec{q}) \to B(\vec{p},\vec{r})$ is a tautology
Then $\exists\, C = C(\vec{p})$ s.t. $\models A(\vec{p},\vec{q}) \to C(\vec{p})$ and $\models C(\vec{p}) \to B(\vec{p},\vec{r})$.

~~and $C(\vec{p}) \to B(\vec{p},\vec{r})$~~

Pf: Let $\vec{p}_1 \cdots \vec{p}_k \in \{0,1\}^{|\vec{p}|}$ be the k-many assignments for which $\exists \vec{q}\, A(\vec{p},\vec{q})$ is true.
Set $C(\vec{p}) = \bigvee_{i=1}^{k} \vec{p}^{(\tau_i)}$
where $\vec{p}^{(\tau_i)} = p_1^{\tau_i} \wedge p_2^{\tau_i} \cdots \wedge p_{|\vec{p}|}^{\tau_i}$
with $p_j^{\tau_i} := \begin{cases} p_j & \text{if } \tau_i(p_j) = T \\ \overline{p_j} & \text{o/w.} \end{cases}$

Alternate proof based on $\exists \vec{q}\, A(\vec{p},\vec{q})$ would be better: $\models C(\vec{p}) \to \forall \vec{r}\, B(\vec{p},\vec{r})$

Then clearly ~~$C(\vec{p}) \models A(\vec{p},\vec{q})$~~ $A(\vec{p},\vec{q}) \models C(\vec{p})$
~~Also~~ Suppose $C(\vec{p})$ is true. Let $\vec{q}_0$ be s.t. $A(\vec{p},\vec{q}_0)$.
Then $B(\vec{p},\vec{r}_0)$ follows for all fixed $\vec{r}_0 \in \{0,1\}^{|\vec{r}|}$.

qed

Equivalent reformulation: If $\models \overline{A(\vec{p},\vec{q})} \vee \overline{B(\vec{p},\vec{r})}$, then
$\exists\, C(\vec{p})$ s.t. $\forall \vec{p}_0 \in \{0,1\}^{|\vec{p}|}$, $\forall \vec{q}_0, \vec{r}_0$ $\begin{cases} \text{if } C(\vec{p}_0) \text{ is true, then } B(\vec{p}_0,\vec{r}_0) \text{ is false} \\ \text{if } C(\vec{p}_0) \text{ is false, then } A(\vec{p}_0,\vec{q}_0) \text{ is false} \end{cases}$

Pf From $\models \overline{A(\vec{p},\vec{q})} \vee \overline{B(\vec{p},\vec{r})}$, get $\models A(\vec{p},\vec{q}) \to B(\vec{p},\vec{r})$.

Then $C(\vec{p})$ s.t. $\models A(\vec{p},\vec{q}) \to C(\vec{p})$ & $\models C(\vec{p}) \to B(\vec{p},\vec{r})$.

Thm' [Mundici '84] If there is a polynomial ~~size~~ upper bound on the (circuit) size of C, ~~then~~ (in terms of the sizes of A + B), then $NP \cap coNP \subseteq P/poly$,

and $NP/poly \cap coNP/poly \subseteq (P/poly)$ ~~In fact~~ or in $NC^1/poly$

Pf Let $\exists \vec{q}\, A(\vec{p},\vec{q})$ express an $NP/poly$ property of $\vec{p}$

+ $\forall \vec{r}\, B(\vec{p},\vec{r})$ is the same property of $\vec{p}$ in $coNP/poly$ form.

Then $\exists \vec{q}(A(\vec{p},\vec{q}) \to \forall \vec{r}\, B(\vec{p},\vec{r})$ is valid

Then $A(\vec{p},\vec{q}) \to B(\vec{p},\vec{r})$ is valid.

Then $C(\vec{p})$ s.t. $A(\vec{p},\vec{q}) \to C(\vec{p})$ and $C(\vec{p}) \to B(\vec{p},\vec{r})$.

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

gives a poly size (circuit)/(formula) for the $NP/poly \cap coNP/poly$ property.

qed.

Thm Suppose the $\vec{p}$'s occur ~~only~~ only positively in $A(\vec{p},\vec{q})$ or negatively in $\overline{B}$. $B(\vec{p},\vec{r})$. Then $C(\vec{p})$ can be chosen so that $\vec{p}$'s occur only positively in $C(\vec{p})$.

This equiv to ~~Thm above~~ "equivalent formulation" above

Pf $\exists \vec{q}\, A(\vec{p},\vec{q})$ is a monotone function of $\vec{p}$.

Hence it has a monotone propositional formula $C(\vec{p})$

qed.

For negatively, use $C(\vec{p}) \equiv \exists \vec{r}\, \overline{B(\vec{p},\vec{r})} \equiv \neg \forall \vec{r}\, B(\vec{p},\vec{r})$

<u>Theorem</u>: Let $\Gamma = \{A_i(\vec{p},\vec{q})\}_i \cup \{B_j(\vec{p},\vec{r})\}_j$ be a set of clauses, with a resolution refutation of n clauses. Then there is a interpolant $C(\vec{p})$ so that

(i) $\bigwedge_i A_i(\vec{p},\vec{q}) \to C(\vec{p})$, i.e., $\neg C(\vec{p}) \to \bigvee_i \neg A_i(\vec{p},\vec{q})$

& (ii) $C(\vec{p}) \to \neg \bigwedge_j B_j(\vec{p},\vec{r})$, i.e. $C(\vec{p}) \to \bigvee_j \neg B_j(\vec{p},\vec{q})$.

and $C(\vec{p})$ has circuit (deg) size $\leq 3n$.

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

<u>Pf</u>: For each clause E in the refutation R, we form a clause C_E st.

$\forall$ truth assignments τ with $\tau(E) = \bot$

$\tau(C_E) = \text{False} \Rightarrow \exists i, \tau(A_i(p,\vec{q})) = \text{False}$

$\tau(C_E) = \text{True} \Rightarrow \exists j \ \tau(B_j) = \text{False}$

The desired C is $C = C_\emptyset$ ($\emptyset$ - last line in R)

We construct C_E inductively by:

For $E = A_i$ ~~each~~ an initial clause $C_{A_i} = \bot$

For $E = B_j$ " " " $C_{B_j} = \top$

<u>Resolution steps</u>

<u>Resolution p_ℓ</u>

$$\frac{F, p_\ell \quad G, \bar{p}_\ell}{F, G} \qquad E = F \cup G$$

$$C_E \stackrel{df}{=} (\bar{p}_\ell \wedge C_{F,p_\ell}) \vee (p_\ell \wedge C_{G,\bar{p}_\ell})$$

<u>Resolution of q_i</u>

$$\frac{F, q_\ell \quad G, \bar{q}_\ell}{F, G} \qquad E = F \cup G$$

$$C_E = C_{F,q_\ell} \vee C_{G,\bar{q}_\ell}.$$

Resolution of r_ℓ

$$\frac{F, r_\ell \quad G, \bar{r}_\ell}{F, G} \qquad E = F \cup G$$

$$C_E \overset{df}{=} C_{F, r_\ell} \wedge C_{G, \bar{r}_\ell}.$$

Pf I Resolve on p_ℓ.

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

~~If $T(p_\ell) = \text{False}$, then $T(F, p_\ell) = \text{False}$.~~

Then $T(C_E) = T((\bar{p}_\ell \vee C_{F,p_\ell}) \wedge (p_\ell \wedge C_{G,\bar{p}_\ell}))$

~~$\Leftrightarrow = T((\bar{p}_\ell \wedge C_{F,p_\ell}) \vee (\bar{p}_\ell \wedge C_{G,\bar{p}_\ell}) \vee (C_{F,p_\ell} \wedge C_{G,\bar{p}_\ell}))$~~

~~IF~~

Suppose $T(C_E) = \text{False}$. ~~(WTS $T(F) = \text{False}$~~

WTS $T(F, p_\ell) = \text{False}$ or $T(G, \bar{p}_\ell) = \text{False}$.

If $T(p_\ell) = \text{True}$, $T(G, \bar{p}_\ell) = \text{False}$

then $T(C_{G, \bar{p}_\ell}) = \text{False}$, so $\exists A_i$ s.t. $T(A_i) = \text{False}$ by ind hyp

If $T(p_\ell) = \text{False}$, $T(F, p_\ell) = \text{False}$

then $T(C_{F, p_\ell}) = \text{False}$ so " again

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

~~Since~~ then similar argument gives $\exists_j B_j(\vec{p}, \vec{q})$ s.t.

$\exists_j T(B_j) = \text{False}$.

by $T(C_{F,p_\ell})$ or $T(C_{G,\bar{p}_\ell}) = \text{False}$

II Resolve on q_ℓ:

$$\frac{F, q_\ell \quad G, \bar{q}_\ell}{F, G} \qquad E = F, G$$

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

~~The case of $T(F \vee q_\ell)$ or $T(G \vee \bar{q}_\ell) = \text{False}$.~~

Then both $T(F) = \text{False}$ + $T(G) = \text{False}$.

Also, either $T(F, p_\ell) = \text{False}$ or $T(G, \bar{p}_\ell) = \text{False}$ depending on if $T(p_\ell) = F$ or T.

Recall $C_E = C_{F,q_\ell} \vee C_{G,\overline{q_\ell}}$.

* If $\tau(C_E) = \text{False}$, then both $\tau(C_{F,q_\ell}) = \text{False}$ + $\tau(C_{G,\overline{q_\ell}}) = \text{False}$

Apply ind hyp to one of them to get
$\exists i \; \tau(A_i) = \text{False}$.

* If $\tau(C_E) = \text{True}$,
then at least one of ~~$\tau(C_{F,q_\ell})$~~
$\tau(C_{F,q_\ell}) = \text{True}$ or $\tau(C_{G,\overline{q_\ell}}) = \text{True}$.

By symmetry, assume $\tau(C_{F,q_\ell}) = \text{True}$.

If $\tau(F \vee q_\ell) = \text{False}$, use the ind hyp to get
$\exists j \; \tau(B_j) = \text{False}$. ← ie. $\tau(p_\ell) = \text{False}$

O/W, Form $\tau' = \tau$ except $\tau(q_\ell) = \text{False}$ (swap q_ℓ value)

Then $\tau'(C_E) = \cancel{\text{False}}$ True (since C_E does not involve q_ℓ!

+ $\tau'(F \vee q_\ell) = \text{False}$,

so by ind hyp $\exists j$ s.t. $\tau'(B_j) = \text{False}$

Hence $\tau(B_j) = \text{False}$ (since q_ℓ not in B_j).

* Can of resolve on r_ℓ is dual.

QED. !!

<u>Thm</u> Assume as above, but also assume $\vec{p}$ appears only positively in A_i's <u>or</u> only negatively in B_j's. Then above hold for some <u>monotone</u> $C(\vec{p})$.

<u>Pf</u> Similar, but w/ some major changes:

For each E in refutation, define

E^A = E with all r-literals removed

E^B = " " " q-literals and positive p-literals removed.

We define C_E ~~in a manner~~ as before, except

Resolve on p_e
$$\frac{F, p_e \qquad G, \bar{p}_e}{F, G} \qquad E = F, G$$

$$C_E = C_{F,p_e} \vee (p_e \wedge C_{G,p_e}) \qquad \text{if } \vec{p}\text{'s negative in } B_j\text{'s}$$

or

$$C_E = (C_{F,p_e} \vee p_e) \wedge C_{G,p_e} \qquad \vec{p}\text{'s positive in } A_i\text{'s}$$

We then prove by induction on E in R:

(a) If $\tau(E^A) = \bot$ and $\tau(C_E) = \bot$ then $\exists i$ $\tau(A_i) = \text{False}$

(ii) If $\tau(E^B) = \bot$ and $\tau(C_E) = \top$, then $\exists i$ $\tau(B_j) = \text{False}$.

We'll just do the $\vec{p}$'s negative in B_j case.

<u>Assume</u> $\tau(E^A) = \text{False}$, $\tau(C_E) = \bot$.

Then $\tau(C_{F,p_e}) = \text{False}$ + $\tau(p_e \wedge C_{G,p_e}) = \text{False}$

If $\tau(p_e) = \text{False}$, $\tau((F,p_e)^A) = \text{False}$, so $\exists i$ $\tau(A_i) = \text{False}$ by ind hyp

If $\tau(p_e) = \text{True}$, $\tau(C_{G,p_e}) = \text{False}$ + $\tau((G,p_e)^A) = \text{False}$

So $\exists i$, $\tau(A_i) = \text{False}$ by ind hyp

If $\tau(p_e) = \text{False}$, then $\tau((F,p_e)^A) = \text{False}$ & so $\exists i$ $\tau(A_i) = \text{False}$ by ind hyp

Assume $\tau(E^B) = \text{False}$ + $\tau(C_E) = \text{True}$

Now $(F_{,p_\ell})^B$ is F^B (since positive p_ℓ's are removed by B).

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

By $\tau(C_E) = \text{True}$, either ~~τE~~ (a) $\tau(C_{F,p_\ell}) = \text{True}$ or

(b) $\tau(p_\ell) = \text{True}$ + $\tau(C_{G,\bar{p}_\ell}) = \text{True}$.

In former case, $\exists i$, $\tau(B_i) = \text{False}$, by ind hyp

In latter case, $\tau(G_{G,\bar{p}_\ell}^B) = \text{False}$, so $\exists j$ $\tau(B_j) = \text{False}$, by ind hyp

<u>Resolve on q_ℓ</u>

$$\frac{F, q_\ell \quad G, \bar{q}_\ell}{F, G} \qquad E = F, G. \qquad C_E \text{ is } C_{F,p_\ell} \vee C_{G,\bar{p}_\ell}$$

<u>Suppose</u> $\tau(E^A) = \text{False}$, $\tau(C_E) = \text{False}$

So $\tau(C_{F,p_\ell}) = \text{False}$ + $\tau(C_{G,p_\ell}) = \text{False}$.

Either $\tau((F,p_\ell)^A) = \text{False}$ or $\tau((G,\bar{p}_\ell)^A) = \text{False}$

In either case, ind hyp gives $\exists i$, $\tau(A_i) = \text{False}$

Suppose $\tau(E^B) = \text{False}$ + $\tau(C_E) = \text{True}$.

$(F,q_\ell)^B = F$ & $(G,q_\ell)^B = G$, so

$\tau((F,q_\ell)^B) = \text{False}$ + $\tau((G,\bar{q}_\ell)^B) = \text{False}$

~~In either case, we~~

Either $\tau(C_{F,p_\ell}) = \text{False}$ or $\tau(C_{G,\bar{p}_\ell}) = \text{False}$

+ in either case, $\exists j$ $\tau(B_j) = \text{False}$, by ind hyp

<u>Resolve on r_ℓ</u>

$$\frac{F, r_\ell \quad G, \bar{r}_\ell}{F, G} \qquad E = F, G. \qquad C_E \text{ is } C_{F,r_\ell} \vee C_{G,\bar{r}_\ell}$$

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

Then $\tau((F,r_\ell)^A) = \tau(F^A) = \text{False}$ + likewise $\tau((G,\bar{r}_\ell)^A) = \text{False}$

Either $\tau(C_{F,r_\ell}) = \text{False}$ or $\tau(C_{G,\bar{r}_\ell}) = \text{False}$

+ in either case $\exists i$ $\tau(A_i) = \text{False}$ by ind hyp.

Suppose $T(\underline{E}^B) = \text{False}$ & $T(C_E) = \text{True}$.

So $T(C_{E,r_e}) = T(C_{G,\bar{r}_e}) = \text{True}$.

And ~~E_{r_e}~~ either $T((E,r_e)^B) = \text{False}$ or $T((E,\bar{r}_e)^B) = \text{False}$.

In either case, ind hyp gives $\exists j\ T(\xi_j) = \text{True}$.

<u>qed.</u>

<u>Defn</u> Clique-Colorg tautology with

Let G be a graph on $[n] = \{0..n-1\}$

p_{ij} = edge from i to j, $(i<j)$

A k-clique is coded by $q_{s,i}$ $\quad s=0..k-1;\ i=0..n-1$.

$\mathrm{Clique}_{k,n}(\vec{p},\vec{q})$

$$\left.\begin{array}{ll} \bigvee_i q_{s,i} & s=0..k-1 \\ \neg q_{s,i},\ \neg q_{s',i} & \\ \neg q_{s,i},\ \neg q_{s',j};\ p_{ij} & \end{array}\right\}$$

$q_{s,i}$ $s \mapsto i$ defines a 1-1 map from $[k]$ to $[n]$ + image is a k-clique.

An k-coloring, coded by $r_{i,u}$ "node i has color u"

$\mathrm{Color}_{k,n}(\vec{p},\vec{r})$

$\bigvee_u r_{iu}$ $\quad i \in [k]$

$\neg r_{iu};\ \neg r_{iv}$ $\quad u \neq v$

$\neg r_{iu},\ \neg r_{ju},\ \neg p_{ij}$ $\quad$ No nodes of same color are adjacent

And $\models \neg\mathrm{Clique}_{k+1}(\vec{p},\vec{q}) \vee \neg\mathrm{Color}_k(\vec{p},\vec{r})$

Any resolution refutation of size S will give a <u>monotone</u> interpolant of size $\leq 3S$.

<u>Thm</u> [Razborov '85, Alon-Boppana '87]

Any monotone circuit separating graphs from k-cliques from graphs of k colors has size $2^{\Omega(\sqrt{k})}$ if $k < \sqrt[4]{n}$.

<u>Corollary</u> Same bound ~~apply~~ applies to resolution refutations of clique coloring.

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

However, this gives a proof (refutation) size lower bound in terms of circuits, and so gives a method of linking proof complexity to circuit complexity.

Algebraic Proof Systems

Work over a field (sometimes a ring) usually F_p or F_{p^k}.

$\Rightarrow$ Use 0 for true

~~Nullst~~ 1 for false

Boolean formulas convert to algebraic formulas by:

$x \mapsto x$ ($=0$ is implicit)

$x \vee y \mapsto x \cdot y$

$x \wedge y \mapsto 1-(1-x)\cdot(1-y)$

$\neg x \mapsto 1-x$.

But other ad-hoc encodings are used as well.

<u>Def'n</u> Let F be a field, and $Q_1, \ldots, Q_m$ ~~pa~~ F-polynomials in variables $x_1 \ldots x_n$.

A <u>nullstellensatz refutation</u> of $Q_1 \ldots Q_m$ is a set of polynomials $F_1, \ldots, F_m, R_1, \ldots, R_n$ s.t.

$$F_1 Q_1 + \cdots + F_m Q_m + R_1 \cdot (x_1^2 - x_1) + \cdots + R_n \cdot (x_n^2 - x_n) = d$$

for some $d \neq 0$, $d \in F$.

<u>Thm</u> [Nullstellensatz] (over a field) The set $Q_1 = 0 \ldots Q_m = 0$ does not ~~Q_1, Q_m can~~ have an 0/1 solution iff there is a nullstellensatz refutation of $Q_1, \ldots, Q_m$.

<u>Pf</u> (Normally have to have F algebraically closed + consider the radical of the ideal, but since using 0/1 solutions, these assumptions are not needed here.)

<u>Pf</u>: Omitted – Use induction on n. (!)

Let $\overline{Q} = \{Q_1 \ldots Q_m\}$

<u>Pf</u> By induction,

$\overline{Q}(x_1 \ldots x_{n-1}, 1)$ and $\overline{Q}(x_1 \ldots x_{n-1}, 0)$ have NS refutations

$R^{(j)}$ $$\sum_{i=1}^{m} F_i^{(j)} Q_i(\vec{x}, j) + \sum_{j=1}^{n-1} R_j^{(j)}(x_j^2 - x_j) = 1. \qquad j = 0, 1.$$

For $j = 1$

Form $R^{(1)}$.

Note $Q_i(\vec{x}, x_n) = p_i(\vec{x}) x_n + q_i(\vec{x})$

So $x_n Q_i(\vec{x}, x_n) = p_i(\vec{x}) x_n^2 + q_i(\vec{x}) x_n$

$= p_i(\vec{x}) x_n + q_i(\vec{x}) x_n + (-p_i(\vec{x})(x_n^2 - x_n))$.

$= Q_i^{(1)} \cdot x_n$

Thus, $$\sum_{i=1}^{m} x_n F_i^{(1)} Q_i(\vec{x}, x_n) + \sum_{j=1}^{n-1} R_j^{(1)}(x_j^2 - x_j) + \left(\sum_i -p_i(\vec{x})\right)(x_n^2 - x_n) = x_n$$

A similar argument gives a linear combination equal to $1 - x_n$.

Adding gives a NS refutation of $\overline{Q}$.

<u>qed.</u>

<u>Grö Polynomial Calculus</u> (aka "Groebner basis system")

Refutation system.

Work over a field F (or ring)

Initial polynomial $Q_1 \ldots Q_m$, $x_i^2 - x_i$ $i = 1 \ldots n$

Inference rules

$$\frac{p}{q \cdot p} \quad \forall \text{ polys } p, q$$

$$\frac{p_1 \quad p_2}{p_1 + p_2}$$

Last line: and $d \neq 0$, $d \in F$ (for field $d = 1$)

PC: Soundness – immediate
Completeness – immediate from completeness of NS.

Def'n Degree of a PC refutation = max degree of poly in the refutation

Next step Allow ~~other~~ arbitrary terms, not just polynomials, but this is just equivalent to Frege (for finite $\mathbb{F}$ at least).

Thm [CEI '96]. Given $Q_1, \ldots Q_m$ in variables $x_1 \ldots x_n$, ~~then~~, and given a degree bound d, there is an $O(n^{3d})$ algorithm for determining if there is a degree d refutation of $Q_1 \ldots Q_m$ (if $m < n^d$)

Pf Idea: Groebner basis algorithm:
Let $S = \{Q_1 \ldots Q_m\}$ = stack of polys to process
Let $B = \emptyset$ – a set of polynomials w/ distinct leading terms (of degree $\leq d$).

Def'n Leading Term = Monomial of highest degree + β^{st} in some ordering

Algorithm Choose $Q \in S$, remove Q from S.
Reduce Q by:
If $LT(Q) = LT(P)$ for some $P \in B$,
set $Q = Q - d \cdot P$ to cancel leading term
+ repeat. If $Q \in B$, continue to next $Q \in S$.
Else: Add Q to B.
If $\deg(Q) < d$, add $x_i Q$ to S for all x_i
Repeat until either:
$\exists d \in B$ $d \in \mathbb{F}$, $d \neq 0$ (Contradiction) – Gives refutation
or S is empty (No refutation).

So we usually ~~bound~~ measure algebraic proof size by degree

Constant degree $\overset{\sim}{\Longrightarrow}$ Polynomial size

(Poly)logarithmic degree $\overset{\sim}{\Longrightarrow}$ Quasipoly size

Linear, or n^{ε}, degree $\overset{\sim}{\Longrightarrow}$ Exponential size.

Ajtai '84; BIKPP '84; Riis '87 } Superpolynomial (barely) lower bounds on size of ~~Cnt~~ constant depth

Beame-Impagliazzo, Krajicek, Pitassi-Pudlak — Frege proofs of Count_m from $\mathrm{Count}_{m'}$ when $\gcd(m,m') = 1$

BIKPRS, Buss-Krajicek-Impagliazzo, Pudlak-Razborov-Sgall } Exponential lower bounds

Def'n Mod m counting principle, Count_m^N $\quad m \geq 1,\ N > 0.$

Let $N \not\equiv 0 \bmod m$.

Variables p_e for each $e \in [N]^m = \{ f \subseteq [N] : |f| = m \}$

$[N] = \{0, 1, 2, \ldots, N-1\}$.

$$\mathrm{Count}_m^N \overset{df}{:=} \bigvee_{e \perp f} (p_e \wedge p_f) \vee \bigvee_{v \in [N]} \bigwedge_{v \in e} \neg p_e \qquad e, f \in [N]^m$$

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

where $e \perp f \overset{df}{\iff} 0 < |e \cap f| < m$.

[BIKPR 84] **Fact:** If $p_1, \ldots, p_k$ are the prime factors of m, then

Count_m^N can be proved by a polysize constant-depth Frege proof from instances of $\mathrm{Count}_{p_1} \ldots \mathrm{Count}_{p_k}$

Conversely:

$\mathrm{Count}_{p_1} \ldots \mathrm{Count}_{p_k}$ follow by polysize constant depth Frege proofs from ~~Count~~ instances of Count_m.

Def'ns: (N, q) polynomial system: $N \equiv 0 \bmod q$

$$Q_v: \quad \sum_{e : v \in e} x_e - 1 \qquad \text{(each } v \text{ in some partition each) for all } v \in [N]$$

$$Q_{e,f}: \quad x_e \cdot x_f \qquad \text{for all } e \perp f,\ e, f \in [N]^q$$

Thm [BIKPR 84] Let q be prime, $q \nmid m$, $m > 1$,

Let $d(N)$ be lower bound on degree of NS refutations of $\{Q_v\}_v \cup \{Q_{e,f}\}_{e,f}$ over $\mathbb{Z}_q$

Then all Frege proofs of Count_q^N from instances of Count_m require size $\geq N^{\varepsilon d(N^\varepsilon)}$ for some $\varepsilon > 0$ (ε depends on the depth)

$$\sum_{v} Q_v = \sum_{v \in [N]} \left(\sum_{e : v \in e} x_e - 1 \right)$$

$$= \sum_{e} \sum_{v \in e} x_e - N$$

$$\equiv -N \mod q$$

$\boxed{\text{Thus a NS refutation.}}$

'96/97

<u>Thm</u> [BIKPR5] Any NS refutation of the $\{Q_i\}_{i=1}$, $\{Q_{e,d}\}_{e,d}$ for $N \neq 0$ mod q over $\mathbb{Z}_m$, $q \nmid m$ has degree

$$\Omega\left(N^{1/\log_2(m+q)}\right) = \Omega\left(N^{\delta}\right)$$

<u>Corollary</u>: all Frege proofs of Count_q from ~~Count~~ instances of Count_m require size

~~N^{γ} for some $\gamma > 0$~~

$N^{N^{\gamma}}$ for some $\gamma > 0$ — γ depends on the depth of the Frege proof

'99

<u>Thm</u> [BGIP; Buss-Grigoriev-Impagliazzo-Pudlák]
Any polynomial calculus refutation of Count_q^N from instances of Count_p requires degree αN for some constant $\alpha = \alpha(p,q)$

Pf: Works for composite p as well.

<u>Pf</u> <u>Idea</u> via Tseitin tautologies and binomials ~~from a field~~
- Use a ~~low degree~~ subgraph of a low degree graph w/ high expansion

Thm [Razborov '98]

Over any field Polynomial Calculus proofs of PHP_n^m require degree $\geq n/2$.

See also IPS '99 [Impagliazzo-Pudlak-Sgall]

8604558 | 4320