What is a proof? Claim: 25957 product of two primes

1) Proof by intimidation: Obvious – left to the reader.

2) Proof by exhaustion:
$$
\begin{aligned}
25957 &\equiv 1 \pmod 2\\
&\equiv 1 \pmod 3\\
&\ \vdots\\
&\equiv 19 \pmod{99}\\
&\equiv 0 \pmod{101}\\
&\equiv 1 \pmod{103}\\
&\ \vdots\\
&\equiv 0 \pmod{257}\\
&\ \vdots
\end{aligned}
$$

OK, but maybe a bit of overkill

3) $25957 = 101 \cdot 257$, left to the reader to check primality.

A proof should be EFFICIENTLY VERIFIABLE

Formally Proof system for language L

Deterministic algorithm $P(x, \pi)$
Polynomial in $|x| + |\pi|$

$x \in L \Rightarrow \exists\, \pi \quad P(x, \pi) = 1$

$x \notin L \quad \forall\, \pi \quad P(x, \pi) = 0$

PROPOSITIONAL PROOFSYSTEM

Proof system for tautologies in propositional logic (formulas true under all truth value assignments)

Denote this language TAUT

Why care?

Reason R1) P vs NP
Reason R2) Understand limits of mathematical reasoning
Reason R3) SAT-solvers / Automated theorem proving

Complexity of P: smallest $g : \mathbb{N}^+ \to \mathbb{N}^+$ s.t.
Every $x \in L$ has proof π of size $|\pi| \leq g(|x|)$

$g = poly(n)$: POLYNOMIALLY BOUNDED proof system

THM (Cook & Reckhow 1979)
$NP = co\text{-}NP$ iff there exists a polynomially bounded propositional proof system

COR
No polynomially bounded pps $\Rightarrow$ $P \neq NP$

Distant goal... Instead study stronger and stronger concrete systems and prove lower bounds.

Prove tautologies $\Leftrightarrow$ refute unsatisfiable CNF formulas

Follows from NP-completeness of SAT

More direct reduction with linear blow-up

a) Introduce one variable for every subformula

b) Add constraints showing values propagate correctly

Ex $\quad F = G \rightarrow H \qquad (\overline{x}_F \vee \overline{x}_G \vee x_H)$
$$\wedge (x_F \vee x_G)$$
$$\wedge (x_F \vee \overline{x}_H)$$

c) Add clause $\overline{x}_F$ for entire formula F

$\Rightarrow$ CNF formula unsatisfiable iff original formula tautology

FROM now on F unsatisfiable CNF formula. | proof = refutation

Ex 1 $\boxed{\text{Truth tables}}$ List all 2^n truth value assignments and verify that F is false for each assignment

Ex 2 $\boxed{\text{Resolution}}$ Start with clauses in formula

Derive new clauses by resolution rule $\dfrac{C \vee x \quad D \vee \overline{x}}{C \vee D}$

Keep applying resolution rule to old and new clause until we get empty clause $\bot$ without literals.

Ex 3 $\boxed{\text{Cutting planes}}$ Translate clauses to linear inequalities

$$x \vee y \vee \bar{z} \implies x + y + (1-z) \geq 1$$
$$\Updownarrow$$
$$x + y - z \geq 0$$

Add inequalities $\boxed{\begin{array}{c} x \geq 0 \\ -x \geq -1 \end{array}}$ for all variables.

Derivation rules

Addition
$$\frac{\sum_i a_i x_i \geq A \qquad \sum_i b_i x_i \geq B}{\sum (a_i + b_i) x_i \geq A + B}$$

Multiplication
$$\frac{\sum_i a_i x_i \geq A \qquad c \geq 0}{\sum_i c a_i x_i \geq cA}$$

Division
$$\frac{\sum_i a_i x_i \geq A \qquad c \mid a_i \ \forall a_i}{\sum_i (a_i / c) x_i \geq \lceil A/c \rceil}$$

Rounding is crucial

Ex 4 Frege system

$$\boxed{\frac{A \vee C \qquad B \vee \neg C}{A \vee B}}$$ [CUT RULE]

A, B, C arbitrary formulas.

Plus possibly additional rules for purely syntactic massage

All of these systems are

SOUND cannot refute satisfiable formulas

COMPLETE refutes every unsatisfiable formula

(Needs proving, of course)

How to measure strength?

P_1 POLYNOMIALLY SIMULATES P_2 if there is a poly-time function f mapping P_2-proofs to P_1-proofs. $P_2 \leq_p P_1$

$\forall F \in$ TAUT/UNSAT $\quad P_2(F, \pi) = 1$ iff $P_1(F, f(\pi)) = 1$

(since we decided to switch to unsatisfiable formulas)

P_1 and P_2 are POLYNOMIALLY EQUIVALENT if $P_1 \leq_p P_2$ and $P_2 \leq_p P_1$

If $P_2 \leq_p P_1$ but there are formulas hard for P_2 but easy for P_1, then P_1 is STRICTLY STRONGER than P_2

Study concrete families of CNF formulas

1) Separate proof systems
2) Quantify how hard/deep various forms of mathematical reasoning is

(formula families often encodings of combinatorial principles or such like)

Connected to reason R2

Three examples:

GRAPH TAUTOLOGY FORMULAS

"A transitive DAG without 2-cycles must have a source"

$x_{i,j}$ true if directed edge (i,j) $\quad i,j \in [n]$

$$GT_n = \bigwedge_{\substack{i,j,k \\ \text{distinct}}} (\overline{x}_{ij} \vee \overline{x}_{jk} \vee x_{ik}) \qquad \text{[transitivity]}$$

$$\wedge \bigwedge_{i \neq j} (\overline{x}_{ij} \vee \overline{x}_{ji}) \qquad \text{[no 2-cycles]}$$

$$\wedge \bigwedge_{j} \bigvee_{i \neq j} x_{ij} \qquad \text{["vertex } j \text{ is not source"]}$$

PIGEONHOLE PRINCIPLE

one word

"m pigeons do not fit into n holes (if $m > n$)"

x_{ij} true if pigeon i sits in hole j

$$\bigwedge_{i \in [m]} \bigvee_{j \in [n]} x_{ij} \qquad \text{["every pigeon sits in some hole"]}$$

$$\wedge \bigwedge_{j \in [n]} \bigwedge_{i_1 \neq i_2 \in [m]} (\overline{x}_{i_1 j} \vee \overline{x}_{i_2 j}) \qquad \text{[no two pigeons in one hole]}$$

RANDOM k-CNF formula

$\mathcal{F}_k^{m,n}$ $\quad$ m clauses over n variables chosen uniformly from set of all $2^k \binom{n}{k}$ k-clauses

$F \sim \mathcal{F}_k^{m,n}$ $\quad$ sample formula from this distribution

(For today) fix $m = c \cdot n$ for some $c \geq 5$, say

Then ~~[illegible]~~ almost surely F unsatisfiable

	p-bounded	Automatizable	Simulation	GT_n	PHP^{n+1}_n	Random k-CNF
TRUTH TABLES	No (trivially)	Yes (trivially)		Hard	Hard	Hard
RESOLUTION	No	Probably not	$TT \leq_p Res$	Easy	Hard	Hard
CUTTING PLANES	No	Open	$Res \leq_p CP$	Easy	Easy	? Open
FREGE SYSTEM	? Open	Probably not*)	$CP \leq_p Frege$	Easy	Easy	? Open

*) Under complexity-theoretic assumptions

What about reason R3 — SAT solving?

Not enough that small proofs exist. We want to find them

Proof search algorithm A_P

input: CNF formula F

output: P-refutation of F if F unsatisfiable

P is AUTOMATIZABLE if there is a proof search algo A_P that finds a proof for any F in time polynomial in the smallest proof for F

(also add poly time in formula size to avoid annoying problems)

Truth tables trivially automatizable (and sometimes this is the best we can do)

Resolution
Frege
} not automatizable under plausible assumptions.

Cutting planes — open but probably not

There are non-trivial automatizable proof systems, but informally, the stronger the system is, the less likely it seems to be automatizable

However, there are really good applied algorithms based on resolution (winners in SAT 08 competition)

THIS CONCLUDES OVERVIEW

From now on focus on one particular proof system
- resolution
one particular formula family
- pigeon hole principle

Prove exponential lower bound

NOTATION / TERMINOLOGY

Literal x or $\overline{x}$ (not x)

clause $x \vee y \vee z$ (set of literals)
size $\leq k$ $\Rightarrow$ k-clause

CNF formula conjunction of clauses (set of clauses)
k-CNF formula

$Vars(F)$ = variables

$F \vDash D$ all truth value assignments that satisfy F must also satisfy D

$[n] = \{1, 2, \ldots, n\}$

TRUTH — 1 FALSITY — 0

Resolution derivation of clause D from formula F

$$\pi : F \vdash D$$

$$\pi = \{ D_1, D_2, \ldots, D_L \}$$

Each D_i either

a) clause of F AXIOM

b) derived by resolution rule $\dfrac{C \vee x \quad D \vee \bar{x}}{C \vee D}$

from D_j, D_k, $j,k < i$

Resolution refutation: Derivation of empty clause 0 (clause with no literals)

Ex

1. $(\bar{x} \vee y) \wedge$ axiom
2. $(x \vee z) \wedge$ axiom
3. $(\bar{z} \vee w) \wedge$ axiom
4. $(x \vee \bar{w}) \wedge$ axiom
5. $(\bar{x} \vee \bar{y})$ axiom
6. $x \vee w$ Res(2,3)
7. x Res(4,6)
8. $\bar{x}$ Res(1,5)
9. 0 Res(7,8)

Length

$L(\pi) = 9$

In resolution we measure length rather than size (difference at most linear factor)

$\boxed{L(F \vdash 0)}$ min length of any refutation

Also add WEAKENING rule $\boxed{\dfrac{C}{C \vee D}}$ for tech purposes (doesn't matter)

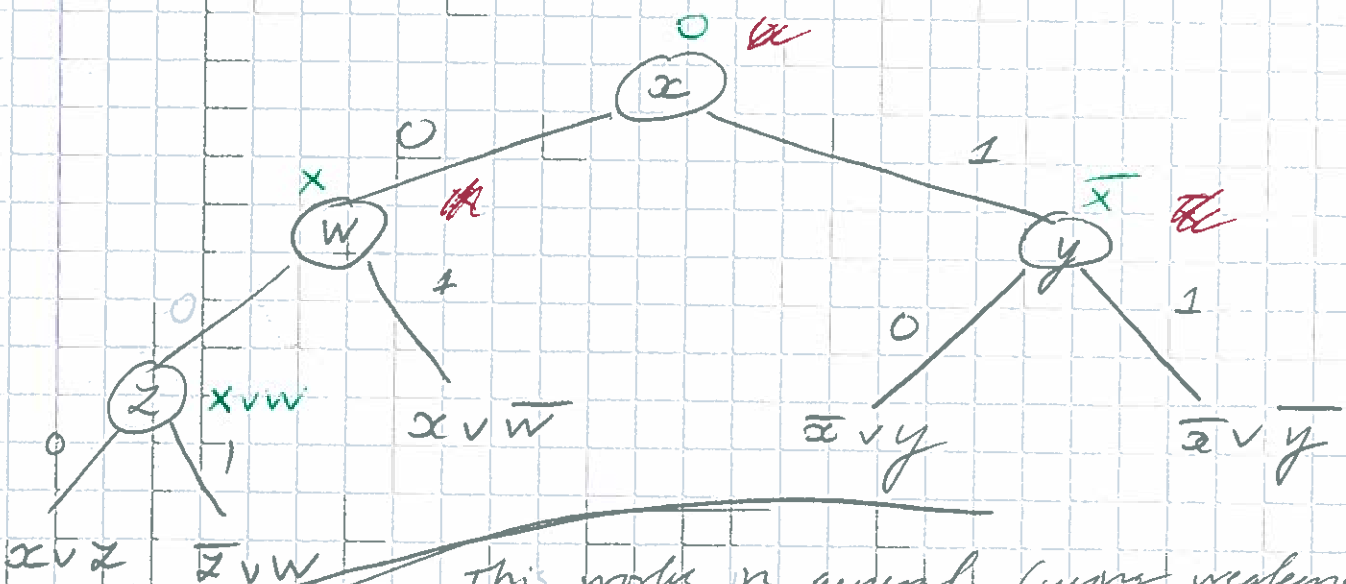
Soundness: Obvious

Completeness: Proof by example

Build search tree
Every vertex queries a variable
0-edge down left
1-edge down right

Each path defines (partial) truth value assignment

As soon as some clause falsified $\Rightarrow$
add leaf labelled by that clause



This works in general (using weakening)
clause at each vertex = minimal clause falsified by partial assignment

Tree height $\leq$ # variables n

$\Rightarrow$ Any formula F can be refuted in length

$$\boxed{L(F \vdash 0) \leq 2^{n+1} - 1 = \exp(O(n))}$$

Tree-like refutation - draw refutation as tree graph

Formally As soon as non-axiom used, mark by $*$.
Starred clauses can never be used again (but can be rederived). Tree like length $\boxed{L_T(F \vdash 0)}$

RESTRICTION = Partial truth value assignment

Identify ρ with literals $\{a, b, c \ldots\}$ set true by ρ.

$$C\restriction_\rho = \begin{cases} 1 & \text{if } \rho \cap C \neq \emptyset \\ C \setminus \{\bar{a} \mid a \in \rho\} & \text{otherwise} \end{cases}$$

$$F\restriction_\rho = \bigwedge_{C \in F} C\restriction_\rho \qquad \pi\restriction_\rho \text{ analogously}$$

Consider example π and $\rho = \{\overline{w}\}$

1 $\quad \bar{x} \vee y$

2 $\quad x \vee z$

3 $\quad \bar{z} \vee \boxed{\cancel{w}} = \bar{z}$

4 $\quad \cancel{x \vee \overline{w}} = 1$

5 $\quad \bar{x} \vee \bar{y}$

6 $\quad x \vee \boxed{\cancel{w}}$ Res (2, 3)

7 $\quad x$ Res (4, 6)

8 $\quad \bar{x}$ Res (1, 5)

9 $\quad 0$ Res (7, 8)

RESTRICTIONS PRESERVE REFUTATIONS

IN GENERAL: If $\pi : F \vdash 0$ then $\pi\restriction_\rho : F\restriction_\rho \vdash 0$

Proof by induction (using weakening)

Want to prove lower bounds on length

Hard... ~~Haken's 85' result took 2025 years to get~~...

Ben-Sasson & Wigderson '99

Look at width = # literals in largest clause

$W(\pi)$ width of refutation

$W(F \vdash 0)$ min width of any refutation

gå till tavlan till exempel direkt.

Easy If a refutation is narrow, then it is short.

Width $w \Rightarrow$ max $\boxed{(2 \cdot |Vars(F)|)^w}$ distinct clauses.

New insight "Short proofs are narrow"

If there is a short ~~pr~~refutation, then there must also exist a narrow one

Road map

1) ~~Prove~~ $W(F \vdash 0)$ large $\Rightarrow L(F \vdash 0)$ large
Actually: Sketch

2) Prove $W(PHP_n^{n+1} \vdash 0)$ large

3) Fill in details in 1 (maybe)

NB! STATE THMS ON PAGES 15-16 BEFORE PROVING LEMMAS

TECHE LEMMA 1 | $\boxed{\begin{array}{l}\text{If } W(F\restriction_x \vdash D) \le w \text{ then} \\ W(F \vdash D \vee \bar{x}) \le \max\{W(F), w+1\}\end{array}}$

Proof Suppose $\pi : \{D_1, D_2, \ldots, \underset{=D}{D_L}\}$ derives D from $F\restriction_x$

Create $\pi' : F \vdash D \vee \bar{x}$ by

First listing all $C \in F$

then listing $D_1 \vee \bar{x}, D_2 \vee \bar{x}, \ldots, D_L \vee \bar{x}$

Claim This is a legal derivation.

If so we're done. $W(\pi') \le w+1$
Final clause $D \vee \bar{x}$

Proof of claim by induction

a) $D_i \vee \bar{x} \in F$ obviously OK

b) $D_i \in F \Rightarrow D_i \vee \bar{x}$ by weakening from previous clause

c) otherwise D_i derived from D_j, D_k by resolution

if so $$\frac{D_j \vee \bar{x} \qquad D_k \vee \bar{x}}{D_i \vee \bar{x}}$$ $\leftarrow$ available by ind hyp

TECH LEMMA 2

If $W(F\restriction_x \vdash 0) \leq w-1$ and $W(F\restriction_{\bar{x}} \vdash 0) \leq W$

then $W(F \vdash 0) \leq \max\{w, W(F)\}$

Proof 1) By Tech Lem 1

Derive $\bar{x}$ in width W

2) Resolve $\bar{x}$ with every clause C in F containing x. This is exactly the same as restricting by $\bar{x}$, so now we have $F\restriction_{\bar{x}}$

the width of this part is $\leq W(F)$

3) By assumption, refute $F\restriction_{\bar{x}}$ in width $\leq W$

$\boxed{}$

Tech Lemma 2 is the key argument in BW's proof

THM 1 (TREE-LIKE RESOLUTION BW '99)

$$\boxed{W(F \vdash 0) \leq W(F) + \log_2 L_T(F \vdash 0)}$$

COR

$$\boxed{L_T(F \vdash 0) \geq 2^{W(F\vdash 0) - W(F)}}$$

Will be proven shortly

MAIN THM 2 (GENERAL RESOLUTION)

$$\boxed{W(F \vdash 0) \leq W(F) + \sqrt{8n \ln L(F \vdash 0)}}$$

where n = # variables in F

Note $\ln$ (worst possible) $= \Theta(n)$

So bound is sort of geometric mean

$$\sqrt{(\text{worst-case upper bound}) \cdot (\text{actual upper bound})}$$

MAIN COR

$$\boxed{L(F \vdash 0) \geq \exp\left(\frac{(W(F \vdash 0) - W(F))^2}{8n}\right)}$$

To get anything ~~interesting~~ need

1) $W(F)$ small

2) $W(F \vdash 0) - W(F) = \omega\left(\sqrt{n \ln n}\right)$

Bonet Galesi '99 proved that the theorem is essentially tight.
using (variant of) GT_n formulas

Proof not hard but more complicated.

So we prove Thm 1 but use Thm 2... :-)

Proof tree-like case

Prove by induction over b and #vars n

$$L_T(F \vdash 0) \le 2^b \Rightarrow W(F \vdash 0) \le W(F) + b$$

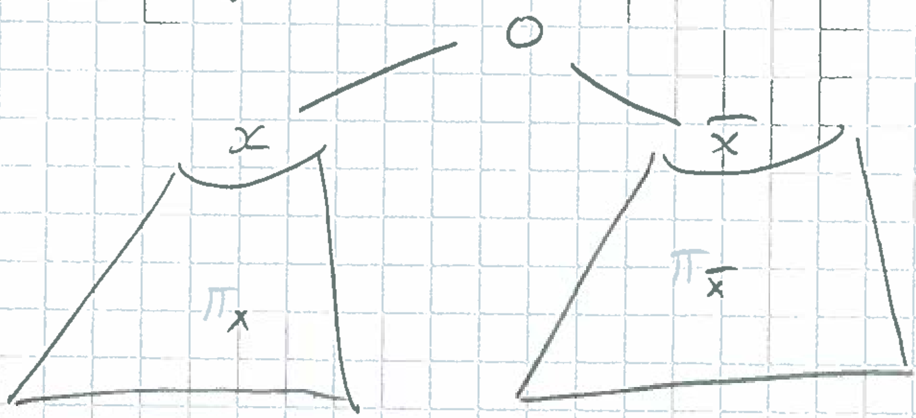
Base cases:

a) $n \le W(F)$ any proof will have width $\le n \le W(F)$

b) $b = 0$ $\Rightarrow$ refutation of length 1

$\Rightarrow$ empty clause $0 \in F$

Induction step $L_T(F \vdash 0) \le 2^b$



$\boxed{L(\pi) = L(\pi_x) + L(\pi_{\bar{x}}) + 1}$ so at least one subderivation has length $\le 2^{b-1}$, say $\pi_{\bar{x}}$

1) Apply induction on $\pi_{\bar{x}}\restriction_x$ and $F\restriction_x$:

$$W(F\restriction_x \vdash 0) \le \overbrace{W(F\restriction_x)}^{\le W(F)} + b - 1$$

2) π_x has length $\le 2^b$ and $F\restriction_{\bar{x}}$ has one less variable

Ind hyp $W(F\restriction_{\bar{x}} \vdash 0) \le W(F\restriction_{\bar{x}}) + b$

3) TECH LEM 2 $\Rightarrow$ $W(F \vdash 0) \le W(F) + b$

Note that this construction leads to exponential blow-up in length!

(so short proofs are not narrow after all?)

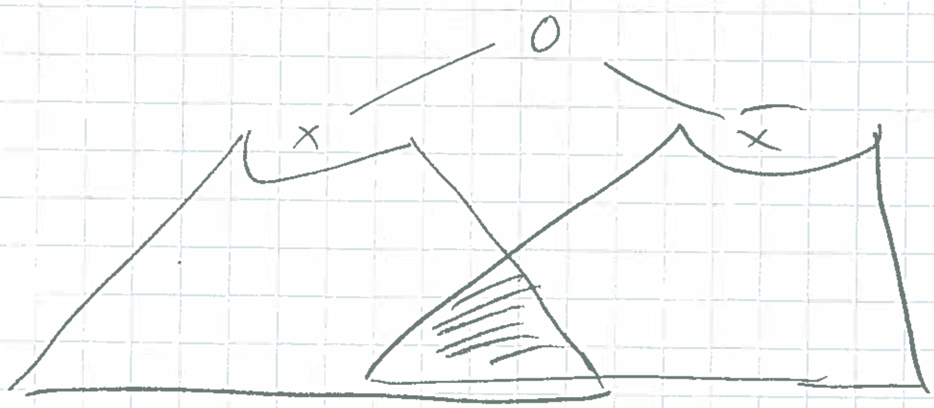
Same thing happens in general thm.

OPEN QUESTION: Is this blow-up necessary?

I.e. is there a trade-off between length and width?

Where does general case fail?

In tree-like case, easy to find restriction that kills $\geq 1/2$ of refutation



Subderivations may (and will) share clauses.

Eliminate many wide clauses by setting commonly occurring literal to true.

More complicated inductive argument.

PHP LOWER BOUND

PHP^m_n consists of clauses

P^i $\quad \bigvee_{j=1}^{n} x_{ij}$ "pigeon i in some hole"

$H^{i,i'}_j$ $\quad \overline{x}_{ij} \vee \overline{x}_{i'j}$ "hole j does not hold both pigeons i and i'"

$m > n \Rightarrow$ unsatisfiable

Today focus on hardest case $m = n+1$ (intuitively easier for larger m)

$$\boxed{\begin{array}{l}\text{THM (Haken '85)} \\ L(PHP^{n+1}_n \vdash 0) = \exp(\Omega(n))\end{array}}$$

Son of Wolfgang Haken 4CT

Want to use BW-machinery. Two problems

1) $\exists$ refutations in width $O(n) = O(\sqrt{\#\text{variables}})$

2) Also, width of formula is n.

Make formula "sparser"

Assume throughout $|U| = m$ $|V| = n$

$G = (U \cup V, E)$ bipartite graph, $N(u)$ neighbours

$$PHP(G) = \boxed{\bigwedge_{u \in U} \bigvee_{v \in N(u)} x_{uv} \wedge \bigwedge_{v \in V} \bigwedge_{u \neq u' \in N(v)} (\overline{x}_{uv} \vee \overline{x}_{u'v})}$$

OBS If $G' = (U \cup V, E')$ has $E' \supseteq E$ then

$$L(PHP(G) \vdash 0) \leq L(PHP(G') \vdash 0)$$

Proof Consider ρ setting $x_{uv} = 0$ for all edges $(u,v) \in E' \setminus E$.

In particular, this holds for $G' = K_n^m$

with $PHP(K_n^m) = PHP_n^m$.

Suppose G has constant left degree $d (\geq 2)$

Then $PHP(G)$ d-CNF formula

with dm variables. $= O(n)$

POTENTIALLY BACK IN BUSINESS!

If we can find G with $W(PHP(G) \vdash 0) = \Omega(n)$

we're done (by the Main Corollary) since

$$L(PHP(G) \vdash 0) = \exp\left(\Omega\left(\frac{(n-d)^2}{d(n+1)}\right)\right) = \exp(\Omega(n)).$$

Why is PHP_n^m hard?

Every set of $s \leq n$ pigeons fit perfectly into holes.

No "local argument" can derive contradiction

What if $\forall U' \subseteq U$, $|U'| \leq O(n)$ have $|N(U')|$ large

Want $\boxed{\begin{array}{ll}(a) & \text{sparse graph with} \\ (b) & \text{good connectivity}\end{array}}$

EXPANDER (BIPARTITE VERTEX EXPANDER GRAPH)

$G = (U \cup V, E)$ is a (d, s, e)-expander if

a) left degree d [sparse]

b) $\forall U' \subseteq U$ $|U'| \leq s$ have $|N(U')| \geq e|U'|$ [connectivity]

In fact need sth slightly stronger

UNIQUE NEIGHBOUR EXPANDER

G is (d,s,e)-unique neighbour expander (or sometimes boundary expander) if

a) left degree d

b) $\forall U' \subseteq U$ $|U'| \leq s$ we have $|\partial U'| \geq e|U'|$

where $v \in \boxed{\partial U'}$ if $|N(v) \cap U'| = 1$

PROPOSITION Any (d,s,κ)-expander is a $(d,s,2\kappa-d)$-unique neighbour expander.

LEMMA A For a (d,s,e)-unique expander, $e \geq 1$, it holds that $W(PHP(G) \vdash 0) \geq s \cdot e/2$

LEMMA B There is a $c > 1$ s.t. $\forall n$ large enough there are $G = (U \cup V, E)$, $|U| = n+1$, $|V| = n$, that are $(5, n/c, 1)$-unique expanders

Proof of B (sketch)

Can be done constructively (~~[illegible]~~) but we won't go there

Prove existence of $(5, n/c, 3)$-expanders

For all $u \in U$ pick 5 neighbours in V uniformly among all $\binom{n}{5}$ subsets. For the right c, this is an expander (with overwhelming probability).

Sketch of calculations: (d, s, e)

G fails to be expander if $\exists\, U'$ $|U'| \le s$

and $V' \subseteq V$, $|V'| \le 3s$ s.t. $N(U') \subseteq V'$.

$$\Pr[N(U') \subseteq V'] = \frac{\binom{3s}{5}^s}{\binom{n}{5}^s}$$

By the union bound, the probability that there is ~~some~~ such pair (U', V') is at most

$$\sum_{t=1}^{s} \underbrace{\binom{m}{t}}_{U'} \underbrace{\binom{n}{3t}}_{V'} \frac{\binom{3t}{5}^t}{\binom{n}{5}^t} < 1 \quad \text{if we pick}$$

$s = n/c$ for c large enough

So expanders exist

And there are even explicit constructions:

Capalbo-Reingold-Vadhan-Wigderson STOC '02

(But note that we don't need this — we just use the expander inside the proof, so non-explicitness is perfectly OK)

USEFUL FACTS FOR CALCULATIONS

(i) if $m > n$ then $\dfrac{\binom{n}{k}}{\binom{m}{k}} < \left(\dfrac{n}{m}\right)^k$

(ii) $\binom{n}{k} \le \left(\dfrac{ne}{k}\right)^k$ [here $e = \exp(1)$]

PROOF OF LEMMA A. Proof strategy: Given

$\Pi = \{D_1, D_2, \ldots, D_L\}$, define measure

$\mu : \{\text{clauses}\} \to \mathbb{N}$ of "progress" s.t.

(i) $\mu(\text{axioms}) \leq 1$

(ii) $\mu(\text{final empty clause } 0) \geq$ large

(iii) μ only increases gradually, so there is some D_i with medium-sized measure $\mu(D_i)$

(iv) Such a D_i must contain many literals (because of expansion)

Let $\mathcal{H}$ denote all "hole axioms" on form $\overline{x}_{u,v} \vee \overline{x}_{u',v}$

Let $P^u = \bigvee_{v \in N(u)} x_{u,v}$

$$\boxed{\mu(D)} := \min\{|U'| : \bigwedge_{u \in U'} P^u \wedge \mathcal{H} \vDash D\}$$

(i) $C \in \mathcal{H} \Rightarrow \mu(C) = 0$

$C = P^u \Rightarrow \mu(C) = 1$

(ii) $\mu(0) > s$

Any set U' of s pigeons fit into $|\partial U'| \geq |U'|$ distinct holes

Because of expansion
Use Hall's theorem
or argue directly
by induction
over $|U'|$

Hence $\bigwedge_{u \in U'} P^u \wedge \mathcal{H} \nvDash 0$.

(iii) If
$$\frac{D \vee x \qquad D' \vee \overline{x}}{D \vee D'}$$

SUBADDITIVITY WRT RESOLUTION RULE

then $\mu(D \vee D') \leq \mu(D \vee x) + \mu(D' \vee \overline{x})$

If $\mathcal{U}_1$ satisfies $\bigwedge_{u\in\mathcal{U}_1} P^u \wedge \mathcal{H} \models D \vee x$

$\mathcal{U}_2$ $\bigwedge_{u\in\mathcal{U}_2} P^u \wedge \mathcal{H} \models D' \vee \bar{x}$

then $\bigwedge_{u\in\mathcal{U}_1\vee\mathcal{U}_2} P^u \wedge \mathcal{H} \models D \vee D'$

Hence there is some $D \in \pi$ with

$$\boxed{s/2 \leq \mu(D) < s}$$

Fix $\mathcal{U}'$ of size $\mu(D)$ s.t.

$$\bigwedge_{u\in\mathcal{U}'} P^u \wedge \mathcal{H} \models D$$

CLAIM $\boxed{\forall v \in \partial\mathcal{U}' \ \exists \text{ variable } x_{u_v,v} \text{ in } D}$

But $|\partial\mathcal{U}'| \geq e|\mathcal{U}'| \geq s\cdot e/2$ since G is an expander. Hence $\boxed{W(D) \geq se/2}$ and LEM A follows.

Proof of claim: By contradiction. Fix such $v^* \in \partial\mathcal{U}'$

Assume: No variable X_{u',v^*} in D

Let $u^* \in \mathcal{U}'$ be the unique neighbour.

$$\bigwedge_{u\in\mathcal{U}'\setminus\{u^*\}} P^u \wedge \mathcal{H} \not\models D \quad \text{by definition}$$

($\mathcal{U}'$ minimal size)

Fix α satisfying LHS and falsifying D.

Wlog $\alpha(x_{u,v^*}) = 0 \ \forall u \in N(v^*)$ This cannot falsify $\mathcal{H}$

Cannot falsify any P^u since u^* is the unique neighbour of v in $\mathcal{U}'$

Cannot satisfy D since there are no variables x_{u,v^*} in D.

Let α^* be as α except $\alpha^*(x_{u^*,v^*}) = 1$

$\alpha(\bigwedge_{u\in\mathcal{U}'} P^u \wedge \mathcal{H}) = 1$ for all x_{u',v^*} $\alpha(x_{u',v^*}) = 0$ so $\mathcal{H}$ satisfied $\alpha(D) = 0$ Contradiction ☐

MISSING DETAILS IN [BW 99]

Recall TECH LEMMA 2

If $W(F\restriction_x \vdash 0) \le w-1$ and $W(F\restriction_{\bar{x}} \vdash 0) \le w$
then $W(F \vdash 0) \le \max\{W(F), w\}$.

Let F k-CNF formula over n variables.
Suppose $L(F \vdash 0) = L$. Want to prove

$$W(F \vdash 0) \le k + \sqrt{8n \ln L}$$

Fix min-length refutation $\pi : F \vdash 0$ of length L

Set
$$d := \sqrt{2n \ln L}$$
$$a := \left(1 - \frac{d}{2n}\right)^{-1}$$

Note $a > 1$ since $d < 2n$ $(L \ll e^{2n})$

Call a clause D FAT if $W(D) \ge d$

$\boxed{fat(\pi)}$ = # fat clauses in π

CLAIM Let G be any k-CNF over $m \le n$ variables and suppose $\exists \pi' \; G \vdash 0$ s.t. $fat(\pi') < a^b$, $b \in \mathbb{N}$
Then
$$W(G \vdash 0) \le k + d + b - 1 \quad (*)$$

From this we get

$$W(F \vdash 0) \le k + \sqrt{8n \ln L}$$

$d = \sqrt{2n \ln L}$

$\boxed{\log_a x = \frac{\ln x}{\ln a}}$

$fat(\pi) < L \leq a^{\lfloor \log_a L \rfloor + 1}$

så $\quad b \leq \log_a L + 1 = 1 + \frac{\ln L}{\ln a}$

$\ln a = \ln\left(\left(1 - \frac{d}{2n}\right)^{-1}\right)$

$\ln(1+x) \leq x \quad x > -1$

$= -\ln\left(1 - \frac{d}{2n}\right)$

$\left[-\ln(1-x) \geq x \text{ if } |x| < 1 \right.$ and $d < 2n$ $\left. \right]$

$\geq d/2n$

$= \sqrt{\ln L / 2n}$

so $\quad b \leq 1 + \frac{\ln L}{\ln a} \leq 1 + \sqrt{2n \ln L}$

$k + d + b - 1 = k + 2\sqrt{2n \ln L}$ $\blacksquare$

$W(F \vdash 0) \leq$

Remains to prove claim. Nested induction over b and m.

[i.e. $\exists$ subformula $x \wedge \bar{x}$]

Base cases:

(1) $m=1$ or $k=1$ or $L \leq 3$: Don't care — theorem obviously true.

(2) $m \leq k$ (for $m, k \geq 2$): $L > 3 \Rightarrow d > 1$

Refutation width is at most $m \leq k \leq k + \overbrace{d + b - 1}^{\geq 0}$

(3) $b = 0 \Rightarrow$ no fat clauses $\Rightarrow$ refutation width at most

$d \leq d + \overbrace{k + b - 1}^{\geq 0}$

Inductive step Suppose $(*)$ holds for

a) all k-CNFs over $< m$ variables

b) all k-CNFs over $= m$ variables with $fat(\pi') < a^{b-1}$

Consider $\pi : G \vdash 0$ with $fat(\pi) < a^b$

$\leq 2m$ literals all in all

$d \cdot fat(\pi)$ literals in fat clauses.

Pigeonhole principle $\Rightarrow$ some literal in at least

$$\frac{d}{2m} fat(\pi) \geq \frac{d}{2n} fat(\pi) \quad \text{clauses.}$$

$\leq$ Suppose wlog literal x

Consider $\pi\restriction_x : G\restriction_x \vdash 0$ — all these clauses disappear

$\pi\restriction_x$ has

$$< \left(1 - \frac{d}{2n}\right) a^b \leq a^{b-1} \text{ fat clauses}$$

So by the induction hyp

$$W(G\restriction_x \vdash 0) \leq k + d + b - 2$$

Now consider $\pi\restriction_{\bar{x}} : G\restriction_{\bar{x}} \vdash 0$.

$\pi\restriction_{\bar{x}}$ has less than a^b fat clauses and

$G\restriction_{\bar{x}}$ has $< m$ variables. By ind. hyp

$$W(G\restriction_{\bar{x}} \vdash 0) \leq k + d + b - 1$$

Use Tech Lemma 2 $\Rightarrow$

$$W(G \vdash 0) \leq \max\{k, k+d+b-1\}$$
$$= k + d + b - 1 \quad \text{QED}$$