

DEF2 Propositional proof system

Proof system for $\overline{\text{CNF-SAT}} = \{ F \mid \text{CNF formula } F \text{ is unsatisfiable} \}$

DEF 3 A proof system is polynomially bounded if $\exists \text{ poly } p \text{ s.t. } \forall x \in \Sigma^* \exists \pi \text{ s.t. } |\pi| \leq p(|x|) \text{ and } P(x, \pi) = 1$

THEOREM 4 [Cook & Reckhow '79]

$NP = coNP$ iff there exists a polynomially bounded propositional proof system

Proof NP is exactly the set of languages with polynomially bounded proof systems.

Now use $coNP$ -completeness of $\overline{\text{CNF-SAT}}$ Pm

COR 5 If there is no P -bounded propositional proof system, then $P \neq NP$.

Proof P is closed under complement. Pm

(1ST REASON FOR PROOF CPLX)

Cook's program: Smiley stronger and stronger proof systems; prove super poly lower bounds; ultimately hope to get to $P \neq NP$

Get stuck pretty soon ...

At roughly same place as circuit complexity

For roughly similar reasons

2ND REASON FOR PROOF COMPLEXITY

IV

Connections to SAT solving

Used to think of SAT as hard problem.

But there are amazingly good SAT solvers out there that are used routinely to solve formulas with 100 000s or even 1 000 000s of variables

Used in e.g.

- hardware verification
- software testing
- artificial intelligence
- bioinformatics
- cryptography
- ... and the list goes on...

} Study corresponding proof systems to understand potential and limitations of such SAT solvers

(but this is a theory course)

Best SAT solvers today use technique called conflict-driven clause learning (CDCL)

Can be seen to search for proofs in resolution proof system

Rest of today's lecture:

- o define resolution
- o give exposition of lower bound by [Haken '85] early breakthrough result
(but we will give different, hopefully simpler, proof)

RESOLUTION PROOF SYSTEM

$\Pi : F \vdash I$

$\vdash I$

Resolution refutation of F sequence of clauses ^{Π} ; each clause either
 (a) $C \in F$ (axiom clause), or
 (b) derived from two previous clauses by resolution rule

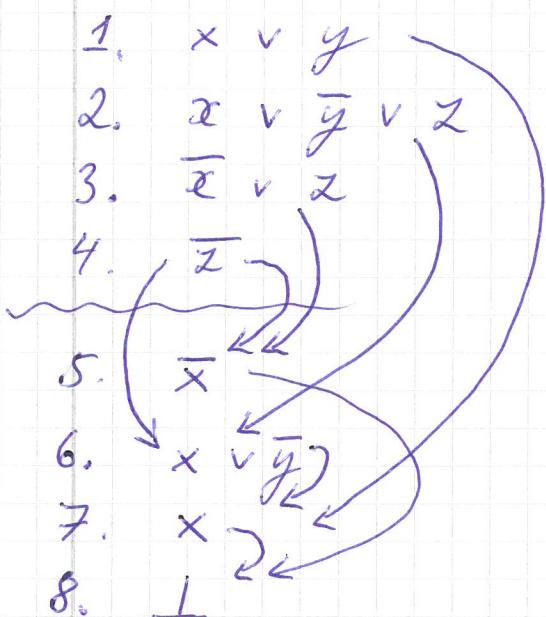
$$\frac{C \vee x \quad D \vee \bar{x}}{C \vee D}$$

Refutation ends with empty clause \perp containing no literals

LEMMA 6 F is unsatisfiable iff \exists resolution refutation of F

Proof sketch (\Leftarrow) Suppose \exists satisfying assignment α . Satisfies all axiom clauses. Then satisfies all resolvents. But empty clause \perp unsatisfiable. Contradiction
 (\Rightarrow) Not hard, but requires an argument. \square

EXAMPLE 7 $F = (x \vee y) \wedge (x \vee \bar{y} \vee z) \wedge (\bar{x} \vee z) \wedge \bar{z}$



Can associate DAG G_Π with any refutation Π
 In this way
 sources = axioms
 sink = \perp

Length of refutation = # clauses (here: 8)
 Length of refuting F = length of a shortest refutation

Also interested in

- o width - size of largest clause in refutation
 - o space - how many clauses need to remember during verification
- } Don't have time to talk about this today

PIGEONHOLE PRINCIPLE

VI

$n+1$ pigeons don't fit into n holes if each pigeon should get a separate hole.

Encode (opposite of) this statement as CNF

$$x_{ij} \quad \begin{array}{l} 1 \leq i \leq m \\ 1 \leq j \leq n \end{array} \quad \begin{array}{l} \text{pigeons} \\ \text{pigeonholes} \end{array} \quad (m > n) \quad \text{we fix } m = n+1$$

x_{ij} true \Leftrightarrow pigeon i goes to hole j

(clauses)

$$P^i = \bigvee_{j=1}^n x_{ij} \quad i \in [m]$$

$$H_j^{i,i'} = \overline{x_{ij}} \vee \overline{x_{i'j}} \quad i, i' \in [m], i \neq i', j \in [n]$$

P^i = pigeon i gets same hole

$H_j^{i,i'}$ = pigeons i and i' don't both sit in hole j .

$$\text{PHP}_n^m = \bigwedge_{i=1}^m P^i \wedge \bigwedge_{j=1}^n \bigwedge_{1 \leq i < i' \leq m} H_j^{i,i'}$$

Arguably the most studied formula family in all of proof cplx (and still quite a few things we don't know about it)

Fix $m = n+1$

PHP_n^{n+1} has $\leq \Theta(n^2)$ variables
 $\Theta(n^3)$ clauses
size $\Theta(n^3)$

Today we'll prove:

THEOREM 8 [Haken '85]

Resolution refutations of PHP_n^{n+1} require length $\exp(-\Omega(n))$.

In terms of formula size $N = O(n^3)$ [VII]

get lower bound $\exp(-\Omega(\sqrt[3]{N}))$.

Also known^{for other formulas} truly exponential lower bounds
 $\exp(-\Omega(N))$ - right up to constant factors in exponent

Prove lower bound via game. Works for any formula - let's focus on PHP

DEFENDANT: claims can fit $n+1$ pigeons into n holes.

PROSECUTOR: Wants to convict defendant of lying

Should be a clear-cut case, but two problems:

(1) JURY TRIAL

And the jury will only be convinced by obviously contradictory answers.

(2) PROSECUTOR OFTEN NEEDS STAND-IN

Has to take care of small kids at home who have cold/fever and can't go to daycare

Stand-in needs super-explicit book with instructions how to cross examine defendant.

Questions: "Does pigeon i go to hole j ?"

Answers: Yes / no

Prosecutor stand-in keeps list of information

$(i_1, j_1, \text{ yes})$

$(i_2, j_2, \text{ no})$

$(i_3, j_3, \text{ yes})$

etc

Defendant
can see
this info

Explicit contradiction (nothing else will convince jury) VIII

- (a) (i, j, yes) and (i, j, no)
- (b) (i_1, j, yes) and (i_2, j, yes) $i_1 \neq i_2$
- (c) $(i, 1, \text{no}), (i, 2, \text{no}), \dots, (i, n, \text{no})$

Instructions to prosecutor stand-in

Look up record $(i_1, j_1, \text{yes/no}), (i_2, j_2, \text{yes/no}), \dots$
(one per page) $(i_s, j_s, \text{yes/no})$

Instruction one of

- (a) ask about pigeon i^* and pigeonhole j^*
- (b) forget $(i_q, j_q, \text{yes/no})$

Why forget? To minimize # pages in book with instructions. Not very impressive if prosecutor needs to flip through several pages to find out which question to ask...

But if prosecutor asks same question again defendant might answer differently !

If \exists resolution refutation Π : $P\text{rep}_n^{n+1} + L$ of length L ,
then \exists prosecutor rule book with $O(L)$ pages.

Proof Look at DAG G_Π representing Π .

Start at sink node labelled \perp

Derived from $\frac{x_{ij}}{\perp} \quad \overline{x_{ij}}$ for some x_{ij}

Ask: Does pigeon i go to hole j ?

Move to clause falsified by defendant's answer

Invariant Say at clause $C \vee D$ in resolution derived from $\frac{C \vee x_{ij} \quad D \vee \bar{x}_{ij}}{C \vee D}$

Current record: Minimal assignment falsifying current clause $C \vee D$

Ask "does pigeon i go to hole j ?" (for variable x_{ij} resolved over)

Move to clause falsified by answer, say $C \vee x_{ij}$

Forget all records/proofs not talking about $\text{Vars}(C \vee x_{ij})$

Sooner or later, reach source = clause of PHP_n^{n+1} . By invariant, this clause is falsified. This is an explicit contradiction as defined above. Pf

Hence, if we can prove there is no small rule book, then there is no short resolution refutation

LEMMA 10

There is a δ such that any prosecutor stand-in rule book must have $\geq 2^{\delta n}$ pages / rules.

Prove this by exhibiting defendant strategy that forces prosecutor to have many pages. Use randomization.

DEFENDANT STRATEGY

L X

Choose $n/4$ pigeons completely uniformly at random and assign them to $n/4$ partial uniformly random pigeonholes to get matching [assume for simplicity $4/n - \text{no big deal.}$]

Let α be this [matching] partial

Defendant always maintains partial matching

$$\beta \supseteq \alpha$$

Let's say hole j' is prohibited for pigeon i if prosecutor has (i, j', no) on record

How defendant answers question "Does i go to j' ?"

- ① If $i \in \text{Dom}(\beta)$, answer yes if $\alpha(i) = j'$, else no.
- ② If $i \notin \text{Dom}(\beta)$, always answer "no".

Then look at # prohibited holes for i

If # prohibited holes $\geq n/2$,

choose smallest hole j'^* that is not prohibited and consistent with matching β and extend β with $(i \mapsto j'^*)$

If Prosecutor forgets

$$i \in \text{Dom}(\beta) \setminus \text{Dom}(\alpha)$$

If a pigeon i does not have assigned hole on record and has less than $n/2$ prohibited holes, then remove i from matching β

If defendant cannot do update in ② \Rightarrow gives up

Let's say pigeon i is thoroughly examined on prosecutor record R if R contains

- (a) (i, j, yes) for some j , or
- (b) (i, j', no) for $\geq n/2$ j' 's

LEMMA 11

Before the prosecutor gets the defendant convicted, she must create record R with $\geq n/4$ thoroughly examined pigeons.

Proof As long as defendant follows strategy he is consistent. Hence, before conviction, an update of β in ② must have failed. How can this happen? Here's how:

Some pigeon i^* radius $n/2$ prohibited holes, but there is no available hole j^* .

$$\text{Means } |\text{Dom}(\beta)| \geq n/2$$

$$\Rightarrow |\text{Dom}(\beta) \setminus \text{Dom}(\alpha)| \geq n/4$$

But $i^* \in \text{Dom}(\beta) \setminus \text{Dom}(\alpha)$ only if

(a) or (b) above holds - QED

◻

Let's call such a record R informative

Want to prove that prosecutor strategy (i.e., rule book) must contain $\geq 2^{5n}$ distinct informative records.

We know that with prob 1 for any choice α of Defendant must reach some informative record R . XII

Prove that for arbitrary fixed record R ,

$$\Pr[\alpha \text{ and } R \text{ consistent}] \leq 2^{-\delta n}$$

Since

\nwarrow Possible to reach R when defendant plays acc to α

$$1 = \Pr[\exists R \text{ consistent with } \alpha]$$

$$\leq \sum_{\substack{\text{informative} \\ R}} \Pr[\alpha \text{ and } R \text{ consistent}]$$

$$\leq 2^{-\delta n} \cdot (\# \text{ informative } R)$$

we get $2^{\delta n}$ distinct informative records

Let $I_R = \{\text{thoroughly investigated pigeons in } R\}$

$$|I_R| \geq n/4.$$

Expected size of intersection $I_R \cap \text{Dom}(\alpha)$ is

$$|I_R \cap \text{Dom}(\alpha)| \geq n/16$$

(by linearity of expectation).

By concentration of measure, except with exponentially small probability we have

$$|I_R \cap \text{Dom}(\alpha)| \geq n/32$$

Suppose $|I_R| = n/4$. Then

$$\Pr_{\alpha} \left[|I_R \cap \text{Dom}(\alpha)| \leq n/32 \right] = \frac{\sum_{i=0}^{n/32} \binom{n/4}{i} \binom{n+1 - n/4}{n/4 - i}}{\binom{n+1}{n/4}}$$

$$\leq \dots \text{calculations} \dots \leq 2^{-\delta' n}$$

for some $\delta' > 0$

Another way of seeing this:

You (sort of) obtain $|I_R \cap \text{Dom}(\alpha)|$

by picking pigeons in α one by one. Every time
choice of picking pigeon in I_R is

$\approx 1/4$ and you do this $n/4$ times.

Actual outcome will be sharply concentrated
around $n/16$ "coin flips" are not independent

(but this is not a formal argument. The
actual calculations are just too boring,
though...)

So suppose $|I_R \cap \text{Dom}(\alpha)| \geq n/32$ XIV

For every $i \in I_R$, it holds that I_R either

- (a) specifies one hole j^*
- (b) rules out $n/2$ holes.

To be consistent, α must comply with these restrictions. Choose pigeons in α one by one.

For $(i+1)$ st pigeon

(a) prob $\leq \frac{1}{n-i}$ to hit exactly right hole

(b) prob $\leq \frac{n/2}{n-i}$ to avoid prohibited hole

$i \leq n/32 \Rightarrow$ Probabilities in (a) & (b) $\ll 2/3$

Probability of getting all pigeons consistent $\ll \left(\frac{2}{3}\right)^n < 2^{-\delta'n}$

$\Pr[\alpha \text{ and } R \text{ consistent}] \leq$

$\Pr[|I_R \cap \text{Dom}(\alpha)| \text{ small}] +$

$\Pr[|I_R \cap \text{Dom}(\alpha)| \text{ large but } \alpha \text{ consistent with } R]$

$\leq 2^{-\delta'n} + 2^{-\delta'n} \leq 2^{-\delta'n}$ for

some $\delta > 0$, QED

R

This concludes our proof of the lower bound on occupation length for resolution)

PfEP_n^{n+1} .