LAST TIME

Intro to proof complexity
Focus on certifying unsatisfiable formulas in conjunctive normal form (CNF)

DEF 1 Proof system for UNSAT

Deterministic algorithm $P(F, \pi)$

$|\cdot|$ denotes size

- Runs in time polynomial in $|F| + |\pi|$
- $F \in UNSAT \Rightarrow \exists$ proof / refutation π such that $P(F, \pi) = 1$
- $F \notin UNSAT \Rightarrow \forall \pi'$ holds that $P(F, \pi') = 0$

DEF 2 A proof system P is polynomially bounded if $\exists$ polynomial p such that $\forall F \in UNSAT$ $\exists \pi$ such that $|\pi| \leq p(|F|)$ and $P(F, \pi) = 1$

Widely believed that no polynomially bounded proof systems for UNSAT exist, because this would imply $NP = coNP$

THEOREM 3 [Cook & Reckhow '79]
If there are no polynomially bounded proof systems for UNSAT, then $P \neq NP$

"Cook's program" Prove superpolynomial lower bounds for stronger and stronger proof systems

"Actually not proposed by Steve Cook, at least not according to Steve Cook, but this name is well established"

THIS COURSE

Survey most of what is known about Cook's program

Limited success... (But the problems are hard)
Lots of nice (and sometimes mysterious) mathematics

TODAY

Lower bound for resolution proof system
Arguably most well-studied proof system in proof complexity
Basis of state-of-the-art SAT solvers using conflict-driven clause learning (CDCL)

DEF 4 Resolution proof system

Resolution refutation π of unsat CNF formula F — notation $\pi : F \vdash \bot$ — is a sequence of clauses $\pi = (D_1, D_2, \ldots, D_{L-1}, D_L)$ such that each clause D_i is either

(a) axiom clause in F, or

(b) derived from D_j, D_k, $j,k < i$, by

RESOLUTION RULE $\qquad \dfrac{B \lor x \quad C \lor \overline{x}}{B \lor C}$

and D_L is the empty clause containing no literals (denoted $\bot$)

"Resolvent of $B \lor x$ and $C \lor \overline{x}$ over x"

LEMMA 5 F is unsatisfiable if and only if ("iff") $\exists$ resolution refutation of F

Proof sketch

($\Leftarrow$) Suppose $\exists$ satisfying assignment α to F. α satisfies all axiom clauses. By induction over $\pi = (D_1, D_2, \ldots, D_{L-1}, D_L)$ satisfies all resolvents. But empty clause $\perp$ cannot be satisfied. Contradiction

($\Rightarrow$) Not hard, but requires an argument. Left as an exercise (will perhaps be on the first problem set) $\boxed{\text{☒}}$

EXAMPLE 6 $F = (x \vee y) \wedge (x \vee \bar{y} \vee z) \wedge (\bar{x} \vee z) \wedge \bar{z}$

1. $x \vee y$
2. $x \vee \bar{y} \vee z$
3. $\bar{x} \vee z$
4. $\bar{z}$

---

5. $\bar{x}$
6. $x \vee \bar{y}$
7. x
8. $\perp$

Can associate DAG G_π with any refutation π in this way

sources = axioms

sink = $\perp$

Length of refutation π = # clauses
$\boxed{L(\pi)}$ (8 in our example)

Length of refuting F = length of a shortest refutation
$\boxed{L_R(F \vdash \bot)}$

Other complexity measures of interest

MENTIONED LAST TIME

- Clause space: how many clauses needed in memory while carrying out proof
- Width: size of largest clause in refutation

WILL COME UP LATER

PIGEONHOLE PRINCIPLE (PHP)

$n+1$ pigeons don't fit into n pigeonholes if each pigeon needs its own hole

Encode (opposite of) this statement as family of CNF formulas

Variables $x_{i,j}$ $i \in [m]$ pigeons $m > n$
$j \in [n]$ pigeonholes

For rest of today, fix $m = n+1$

$x_{i,j}$ true $\Leftrightarrow$ pigeon i flies into hole j

Clauses:

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

$$H_j^{i,i'} = \overline{x}_{i,j} \vee \overline{x}_{i',j} \qquad i,i' \in [m],\ i<i',\ j \in [n]$$

P^i = "pigeon i gets some hole"

$H_j^{i,i'}$ = "pigeons i and i' don't both fly to hole j"

$$\boxed{PHP_n^m = \bigwedge_{i=1}^{m} P^i \wedge \bigwedge_{j=1}^{n} \bigwedge_{i'=2}^{m} \bigwedge_{i=1}^{i'-1} H_j^{i,i'}} \qquad (*)$$

Probably hands-down <u>the</u> most studied formula family in all of proof complexity

There is even a survey paper [Razborov '02] dedicated exclusively to this family

As discussed last time, PHP formulas come in several different flavours – can add also

functionality axioms $\quad F_{j,j'}^{i} = \overline{x}_{i,j} \vee \overline{x}_{i,j'}$

onto axioms $\quad O_j = \bigvee_{i=1}^{m} x_{i,j}$

Still quite a few things we don't know about PHP formulas

Today, focus on "vanilla version" $(*)$ for $m=n+1$

<u>THEOREM 7</u> [Haken '85]

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

PHP_n^{n+1} has

- $\Theta(n^2)$ variables
- $\Theta(n^3)$ clauses
- size $\Theta(n^3)$

In terms of formula size $N = \Theta(n^3)$
Thm 7 yields lower bound $\exp(\Omega(\sqrt[3]{N}))$

Can show (not hard) that resolution never needs length more than $\exp(O(N))$

Which bound is closer to the truth?
Will see next lecture formulas of size N with truly exponential lower bounds $\exp(\Omega(N))$ — tight up to constant factors in the exponent

---

To prove Thm 7, need to show that $\exists\, \delta > 0$ such that for large enough $N \in \mathbb{N}^+$ it holds if $n \geq N$ that any resolution refutation of PHP_n^{n+1} requires $2^{\delta n}$ steps.

As $n \to \infty$ we get infinitely many possible refutations of PHP_n^{n+1}

Need to show that no such refutation can be shorter than $2^{\delta n}$

How can one prove such a thing?

Not obvious at all – Haken's 1985 paper considered a major breakthrough

We will present a nicer, cleaner (and cuter) proof from [Pudlák '00]

Prove lower bound using a game
Works for any formula – let's focus on PHP

Two players:

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, explicitly contradictory answers

(2) PROSECUTOR OFTEN NEEDS STAND-IN
Might need to leave early to pick up kids at daycare (or stay home with them when they are ill)
Stand-in needs book with super-explicit instructions how to crossexamine defendant

Questions: "Does pigeon i go to hole j?"
Answers: "Yes" / "no"

Prosecutor stand-in (whom we will refer to as prosecutor from now on) keeps list of information (a record)

notes
(i_1, j_1, yes)
(i_2, j_2, no)
(i_3, j_3, yes) etc

Defendant is able to see this info

Explicit contradictions that will convince jury

(a) (i, j, yes) and (i, j, no)

(b) (i_1, j, yes) and (i_2, j, yes) $\quad i_1 \neq i_2$

(c) $(i, 1, \text{no}), (i, 2, \text{no}), \ldots, (i, n, \text{no})$

Instructions to prosecutor

Look up record (one per page)
Has to match exactly (except order irrelevant)
Instruction what to do next is one of
(a) ask about pigeon i^* and hole j^*
(b) forget $(i_?, j_?, \text{yes/no})$ currently on record (one or several)

Why forget? To minimize # pages in instruction book. Not very impressive if prosecutor needs to flip through several times just to figure out which question to ask next...

But... If prosecutor asks a question, forgets the answer, and then asks again, defendant might give different answer.

OK, this is a cute game, but why are we doing this?

LEMMA 8

If $\exists$ resolution refutation $\pi : PHP_n^{n+1} \vdash \bot$ of length $L(\pi) = L$, then $\exists$ prosecutor instruction book with $O(L)$ pages/records.

Proof Suppose $\pi : F \vdash \bot$ is a resolution refutation in length $L(\pi) = L$. Look at the DAG representation G_π of π.

Start at sink labelled $\bot$

Derived from $\dfrac{x_{i,j} \qquad \bar{x}_{i,j}}{\bot}$ for some $x_{i,j}$

Ask Does pigeon i go to hole j?

Move to clause/vertex falsified by defendant's answer

Invariant At all times, prosecutor points to vertex/clause D_i in the refutation

Current record is minimal partial assignment falsifying that clause D_i

Instruction: Say prosecutor points to $B \vee C$ derived from

$$\frac{B \vee x_{i,j} \qquad C \vee \bar{x}_{i,j}}{B \vee C}$$

Then ask about $x_{i,j}$ and move to clause falsified by answer. Forget all notes in record not needed to falsify this clause

In this way, can build instruction book by processing all vertices in G_π (with 2 records per clause in π)
However defendant answers, prosecutor will walk backwards through G_π.
Sooner or later, will reach source labelled by axiom of PHP_n^{n+1}.
By the invariant, this clause is falsified.
But this is an explicit contradiction as defined above. $\boxed{\text{Ml}}$

Hence, if we can prove that there cannot exist any small instruction book, then it follows that there is no short resolution refutation. So we are done if we can prove the following.

LEMMA 9
There is a $\delta > 0$ such that for large enough n any instruction book must have at least $2^{\delta n}$ pages / records.

What do we need to do?
Can't just consider single round of play.
Prosecutor can always win by asking at most $n(n+1)$ questions. (How?)
Have to consider several rounds and prove that in order to always win, prosecutor need to be able to deal with exponentially many cases/scenarios/records.

How can we do this? Devise clever defendant strategies.

Intuitively, answering "yes" to a question gives away lots of information, answering "no" not so much

Attempt 1 Defendant answers "no" to question (i,j) as long as there is some other free hole for pigeon i. Answer "yes" when pigeon i has to go into hole j to avoid immediate contradiction.

Doesn't work – prosecutor has strategy with $O(n)$ records. Exercise.

Attempt 2 Use randomization. Choose n out of $n+1$ pigeons randomly. Match pigeons to holes randomly; say matching M. Answer all questions consistently with M (i.e., answer "yes" to (i,j) iff i matched to j in M.

Also doesn't work – again prosecutor has counter-strategy with something like $O(n^2)$ records. Also exercise.

What about mixing the two strategies?

DEFENDANT STRATEGY (Attempt 3; successful)

Choose $n/4$ pigeons uniformly at random
Assign to $n/4$ pigeonholes uniformly at random
to obtain partial matching $\boxed{\mathcal{M}_{init}}$
[assume for simplicity that $4 | n$, and also that all divisions of n that will follow produce integers — not hard to deal with this formally]

Let $Dom(\mathcal{M})$ denote the pigeons matched by a partial matching $\mathcal{M}$. Then $\mathcal{M}$ corresponds to truth value assignment $\alpha_{\mathcal{M}}$ in the natural way:

$$\alpha_{\mathcal{M}}(x_{i,j}) = 1 \quad \text{if } (i,j) \in \mathcal{M}$$
$$\alpha_{\mathcal{M}}(x_{i,j}) = 0 \quad \text{if } (i,j') \in \mathcal{M} \text{ for } j' \neq j$$
$$\alpha_{\mathcal{M}}(x_{ij}) = * \text{ (unassigned) if } i \notin Dom(\mathcal{M})$$

Throughout play, defendant will maintain partial matching $\mathcal{M}$ such that
(a) $\mathcal{M} \supseteq \mathcal{M}_{init}$
(b) $\alpha_{\mathcal{M}}$ consistent with current prosecutor record R

Say that record R prohibits hole j for pigeon i if R contains (i, j, no)

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

1. If $i \in Dom(\mathcal{M})$ answer "yes" if $\alpha_{\mathcal{M}}(x_{ij}) = 1$, else "no"

2. If $i \notin Dom(\mathcal{M})$, always answer "no"

Defendant's update of $\mathcal{M}$ if $i \notin Dom(\mathcal{M})$

Look at # prohibited holes for i in current record. If $\geq n/2$, choose smallest hole j^* not prohibited for i and consistent with $\mathcal{M}$ and set

$$\mathcal{M} = \mathcal{M} \cup \{(i, j^*)\}$$

If such update not possible, defendant gives up

Defendant's update of $\mathcal{M}$ if prosecutor forgets

Look at every pigeon $i \in Dom(\mathcal{M}) \setminus Dom(\mathcal{M}_{init})$ such that some note $(i, j, yes/no)$ forgotten

If (a) i does not have assigned hole on record, and
(b) # prohibited holes $< n/2$,
then remove i from matching $\mathcal{M}$.

Say pigeon i is thoroughly examined in record R if R contains
(a) (i, j, yes) for some j, or
(b) (i, j', no) for $\geq n/2$ different j's

LEMMA 10
Before prosecutor gets defendant convicted, must create record R with $\geq n/4$ thoroughly examined pigeons.

Proof As long as defendant follows strategy the answers are consistent. Hence, before conviction an update of $\mathcal{M}$ for some $i^* \notin \mathrm{Dom}(\mathcal{M})$ must have failed. How did this happen? Pigeon i^* has $n/2$ prohibited holes in current record R, but there is no available free hole

Means $|\mathrm{Dom}(\mathcal{M})| \geq n/2$

$\Rightarrow |\mathrm{Dom}(\mathcal{M}) \setminus \mathrm{Dom}(\mathcal{M}_{init})| \geq n/4$

But $i' \in \mathrm{Dom}(\mathcal{M}) \setminus \mathrm{Dom}(\mathcal{M}_{init})$ only if

(a) some (i', j', yes) is on record R, or

(b) $\geq n/2$ prohibited holes for i',

i.e., only if pigeon i' thoroughly examined $\boxed{}$

Say that record R with $\geq n/4$ thoroughly examined pigeons is informative

Want to prove that any complete instruction book (i.e., can win against any defendant) must contain $\geq 2^{\delta n}$ distinct informative records (clearly implies Lem 9)

By Lem 10, for any choice of $\mathcal{M}_{init}$ round of play passes through informative record R.

CLAIM 11

For any arbitrary fixed informative record R

$\Pr[R \text{ and } \mathcal{M}_{init} \text{ consistent}] \leq 2^{-\delta n}$

where probability over random choice of $\mathcal{M}_{init}$.

If we can prove Claim 11, then we're done. Why?

- For any $\mathcal{M}_{init}$, round of play passes through informative record R
- defendant always consistent with $\mathcal{M}_{init}$
- Hence, the record R cannot contradict $\mathcal{M}_{init}$

Since

$$1 = \Pr[\text{Exists } R \text{ informative such that game passes through } R]$$

$$\leq \sum_{\substack{\text{informative} \\ R}} \Pr[\text{game passes through } R]$$

$$\leq \sum_{\substack{\text{informative} \\ R}} \Pr[R \text{ consistent with } \mathcal{M}_{init}]$$

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

we get that the instruction book must contain at least $2^{\delta n}$ informative records

So all that remains now is to establish Claim 11.

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

Know $|I_R| \geq n/4$

Expected size of intersection $|I_R \cap Dom(\mathcal{M}_{init})|$ is

$$E[|I_R \cap Dom(\mathcal{M}_{init})|] \geq n/16$$

by linearity of expectation.

By concentration of measure, except with exponentially small probability it holds that

$$\left| I_R \cap \mathrm{Dom}(\mathcal{M}_{init}) \right| \geq n/32$$

Formally, one way to prove this is to simply estimate the probability

$$\Pr_{\mathcal{M}_{init}}\left[\left| I_R \cap \mathrm{Dom}(\mathcal{M}_{init}) \right| \leq n/32 \right] \leq$$

$$\leq \frac{\sum_{i=0}^{n/32-1} \binom{n/4}{i} \binom{n+1-n/4}{n/4-i}}{\binom{n+1}{n/4}} \quad (\dagger)$$

$(\dagger) \leq$ (Numerator maximized for large i)

$$\leq \frac{n/32 \binom{n/4}{n/32} \binom{3n/4+1}{7n/32}}{\binom{n+1}{n/4}} \leq$$

$\leq$ ... calculations using Stirlings Formula

$$\sqrt{2\pi m}\left(\frac{m}{e}\right)^m e^{\frac{1}{12m+1}} < m! < \sqrt{2\pi m}\left(\frac{m}{e}\right)^m e^{\frac{1}{12m}}$$

in appropriate ways ... $\leq$

$\leq 2^{\delta' n}$ for some $\delta' > 0$ $(\dagger)$

Another way of seeing this intuitively:

We (sort of) obtain pigeons in $I_R \cap Dom(\mathcal{M}_{init})$ by picking pigeons in $\mathcal{M}_{init}$ one by one. Every time, chance of hitting I_R is $\approx 1/4$ and we do this $n/4$ times. If things were independent, then it is well-known that actual outcome of repeated coin flips is sharply concentrated around expectation $n/16$.

(But this is not a formal argument since we don't have independence. The actual calculations in $(\dagger)$ would just take us too long, however

OK, so suppose $|I_R \cap Dom(\mathcal{M}_{init})| \geq n/32$

For every $i \in I_R$ it holds that R
(a) either specifies hole j
(b) or rules out $n/2$ holes $j_1, j_2, \ldots, j_{n/2}$

In order for R and $\mathcal{M}_{init}$ to be consistent, the random matching $\mathcal{M}_{init}$ must comply with restrictions (a) & (b)

Consider pigeons in $\mathcal{M}_{init}$ chosen one by one

Cheating argument:

For pigeon of type (a) have to hit exactly right hole, so probability of being consistent is $\approx \frac{1}{n} < \frac{1}{2}$

For pigeon of type (b) have to avoid half of the holes, so probability of being consistent is $\leq \frac{1}{2}$

All in all, get probability $\leq \left(\frac{1}{2}\right)^{n/32}$ which is exponentially small — done!

But we actually don't have independence

Calculating more carefully, we get for $(i+1)$st pigeon (But still fairly sloppily, just for simplicity)

(a) $\Pr[\text{consistent}] \leq \frac{1}{n-i}$ to hit right hole

(b) $\Pr[\text{consistent}] \leq \frac{n/2}{n-i}$ to avoid prohibited hole

Since $i \leq n/2$, both probabilities in (a) and (b) are $< 2/3$ regardless of what happened for previous pigeons

So $\Pr[\text{all pigeons in } M_{hit} \text{ consistent with } R]$

$$\leq \prod_{i=1}^{n/\cancel{4}} \Pr\left[i\text{th pigeon matched consistently} \,\middle|\, \begin{array}{l}\text{previous pigeons}\\ \text{matched consi}\end{array} \right]$$

$$\leq \prod_{i=1}^{n/2} \Pr[i\text{th pigeon consistent regardless of conditioning}] \leq \left(\frac{2}{3}\right)^{n/32} \quad (**)$$

$$\leq 2^{-\delta'' n} \text{ for some } \delta'' > 0$$

Now we are ready to wrap things up

$$\Pr[\mathcal{M}_{init} \text{ and } R \text{ consistent}] \le$$

$$\underbrace{\Pr[\text{consistent} \mid \text{intersection } |I_R \cap \mathcal{M}_{init}| < n/32]}_{\le 1} \cdot \Pr[|I_R \cap \mathcal{M}_{init}| \le \tfrac{n}{32}]$$

$$+ \Pr[\text{consistent} \mid |I_R \cap \mathcal{M}_{init}| \ge n/32] \cdot \underbrace{\Pr[|I_R \cap \mathcal{M}_{init}| \ge n/32]}_{\le 1}$$

$$\le \Pr[|I_R \cap \mathcal{M}_{init}| \le n/32]$$

$$+ \Pr[\mathcal{M}_{init} \text{ and } R \text{ consistent} \mid |I_R \cap \mathcal{M}_{init}| \ge n/32]$$

$$\le 2^{-\delta' n} + 2^{-\delta'' n} \quad [\text{by } (\dagger) \text{ and } (**)]$$

$$\le 2^{-\delta n}$$ for some appropriately chosen $\delta > 0$.

Claim 11 follows, and so does Lem 9 $\boxed{}$

This concludes the proof of the exponential lower bound on resolution refutations of PHP formulas.