Mathematical Logic 2016

Lecture 7: Resolution proof complexity

Instructor: Ashutosh Gupta

TIFR, India

Compile date: 2016-08-27

Where are we and where are we going?

We have seen

- propositional logic
- proof methods for the logic
- soundness and completeness of the methods

We will see

- proof complexity of resolution

Topics skipped in this course!

We are also skipping

- NP-Hardness of satisfiability(Cook's theorem)
- (*many other things*)

Topic 7.1

Proof complexity

Properties of proof systems

We know finding a proof is hard.

We may wish to know other vital properties of our proof methods.

For example

- what is the length of shortest proof of a given theorem?
- Are there theorems that have large proofs no matter, which proof system we choose?

Here, we will consider only CNF formulas and resolution is the choice for a proof method.

We will study one such property of resolution.

Proof complexity of resolution

Theorem 7.1

For every n, there is a formula F_n whose shortest resolution refutation proof is exponentially large.

Proof sketch.

The proof proceeds in the following two steps

1. wide proofs for narrow formulas are long
2. there are narrow formulas that necessarily have wide proofs

□

Commentary: The presentation is borrowed from The Art of computer programming Section 7.2.2.2 (Beta), Donald Kunuth, p57-60. `http://www-cs-faculty.stanford.edu/~uno/fasc6a.ps.gz`

Resolution derivation

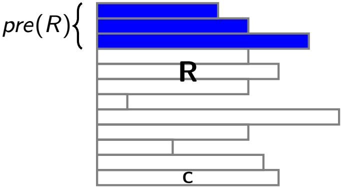
Since we assume that input formulas are in CNF, we only need the resolution rule.

Definition 7.1

A resolution derivation *R that derives clause C form formula F is a sequence of clauses that*

- *are either from F or derived by applying resolution on earlier clauses, and*
- *has C as the last clause.*

Let pre(R) *is the set of clauses in R that are from F.*



Commentary: The drawing may be misleading. The clauses from F are not forced to be at the prefix. They may appear anywhere in R.

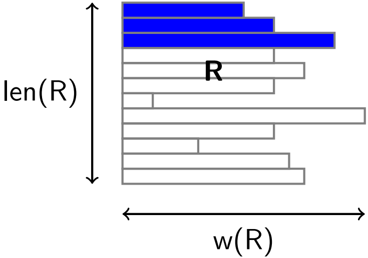
Width and length

Definition 7.2

Let $w(F)$ *denote the size of largest clause in* F*. We say* $w(F)$ *is width of* F*. Similarly for a resolution derivation* R*,* $w(R)$ *is defined.*

Definition 7.3

For a resolution derivation R*, let* $len(R)$ *be the length of the derivation.*



Proofs

Definition 7.4

Let $F \vdash C$ denote that there is a resolution derivation that derives clause C from F.

Definition 7.5 (Narrowest proofs)

Let $w(F \vdash C) \triangleq min(\{w(R) | R \text{ derives } C \text{ from } F\})$.
Let N_F be a derivation that derives $\emptyset$ from F and $w(N_F) = w(F \vdash \emptyset)$.

Definition 7.6 (Shortest proofs)

Let $|F \vdash C| \triangleq min(\{len(R) | R \text{ derives } C \text{ from } F\})$.
Let S_F be a derivation that derives $\emptyset$ from F and $len(S_F) = |F \vdash \emptyset|$.

Commentary: N_F is the narrowest proof and S_F is the shortest proof. N_F and S_F may not be the same.

Conditional proofs

Definition 7.7

For a clause C and literal ℓ, let

$$C|_\ell \triangleq \begin{cases} \top & C \in \ell \\ C - \{\bar{\ell}\} & \textit{otherwise} \end{cases}$$

For a formula F, let $F|_\ell \triangleq \{ C|_\ell \, | C \in F\}$.
Similarly for a derivation $R = C_1, \dots, C_n$, let $R|_\ell \triangleq C_1|_\ell, \dots, C_n|_\ell$.

We further generalize the notation.
For partial model $m = \{p_1 \mapsto b_1, .., p_k \mapsto b_k\}$, $F|m \triangleq F|_{p_1 \mapsto b_1}| \dots |_{p_k \mapsto b_k}$

Exercise 7.1

Let $F = \{(p \vee q), (\neg p \vee \neg q), (q \vee \neg r), r\}$. Give $F|_p$, $F|_{\neg p}$, $F|_q$, and $F|_{\neg q}$.

Exercise 7.2

Prove if R derives C from F then $R|_\ell$ derives $C|_\ell$ from $F|_\ell$.
(we may need to add weakening rule in the proof system)

Width increment

Theorem 7.2

If $k \geq w(F)$, $w(F|_{\ell} \vdash \emptyset) \leq k-1$, and $w(F|_{\overline{\ell}} \vdash \emptyset) \leq k$ then $w(F \vdash \emptyset) \leq k$.

Proof.

$R_1 :=$ derivation that derives $\emptyset$ from $F|_{\ell}$ and $w(R_1) \leq k-1$.
$R_2 :=$ derivation that derives $\emptyset$ from $F|_{\overline{\ell}}$ and $w(R_2) \leq k$.

Construct derivation R_1' by expanding each clause appropriately in R_1 with literal $\overline{\ell}$ such that R_1' is a derivation of $\overline{\ell}$ from F (how?). Note $w(R_1') \leq k$.

Construct a resolution sequence R_3 that is obtained by applying resolution between clauses of F and $\{\overline{\ell}\}$ and produces $pre(R_2)$. Note $w(R_3) \leq w(F)$.

$R_1' R_3 R_2$ is a derivation that derives $\emptyset$ from F(why?).

$$w(R_1' R_3 R_2) \leq max(w(R_1'), w(R_3), w(R_2)) \leq max(k, w(F), k) \leq k$$

Therefore, $w(F \vdash \emptyset) \leq k$. $\square$

Long proofs theorem

Theorem 7.3

Let $n = \mathbf{Vars}(F)$ *and* $\emptyset \notin F$.

if

$$\underbrace{w(F)^2 \leq n}_{\textit{narrow clauses}}$$

then

$$exp(\underbrace{w(F \vdash \emptyset)}_{\textit{wide proofs}}{}^2/(8n)) - 2 \leq \underbrace{|F \vdash \emptyset|}_{\textit{long proofs}}$$

Long proofs theorem

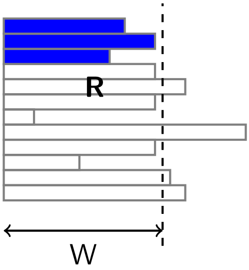
Theorem 7.4

Let $n = \mathbf{Vars}(F)$ *and* $\emptyset \notin F$.
if $w(F)^2 \leq n$ *then* $exp(w(F \vdash \emptyset)^2/(8n)) - 2 \leq |F \vdash \emptyset|$

Proof.

Let $W \geq w(F)$ be a fixed constant and its value will be chosen later.
We will call a clause C fat if $w(C) \geq W$.
Let $fat(R)$ be the number of fat clauses in R.

...



$W(R) = 4$

Long proofs theorem(contd.) II

Proof(contd.)

Observation:

Fat clauses contain at least $fat(R)W$ occurrences of literals.

There is a literal ℓ that occurs in at least $fat(R)W/(2n)$ fat clauses.

Therefore, ℓ does not occur in at most $fat(R)(1 - W/(2n))$ fat clauses.

Let $\rho = (1 - W/(2n))$. ...

Exercise 7.3

Show $1 > \rho \geq 1/2$ *is the only* interesting *range*

Long proofs theorem(contd.) III

Recall :
Let $\rho = (1 - W/(2n))$.

Proof(contd.)

claim: We will prove by induction

$$\text{if } \underbrace{\rho^{-(b-1)} \leq}_{\text{only for } b \geq 1} fat(S_F|_m) < \rho^{-b} \text{ then } w(F|_m \vdash \emptyset) \leq W + b.$$

on $fat(S_F|_m)$ and length of $S_F|_m$.

base case:

$fat(S_F|_m) = 0 < \rho^{-0}$. Since $W \geq w(F)$, $w(F|_m \vdash \emptyset) \leq W$.

induction step:

Consider $\rho^{-(b-1)} \leq fat(S_F|_m) < \rho^{-(b)}$.

Choose ℓ that occurs in at least $fat(S_F|_m)W/(2n)$ clauses. ...

Long proofs theorem(contd.) IV

Proof(contd.)

Therefore, $fat(S_F|_m|_\ell) < fat(S_F|_m)(1 - W/(2n)) < fat(S_F|_m)\rho < \rho^{-(b-1)}$.
Due to ind. hyp., $w(F|_m|_\ell \vdash \emptyset) \leq W + b - 1$.

Since $S_F|_m|_{\overline{\ell}}$ derives $\emptyset$ from $F|_m|_{\overline{\ell}}$, $len(S_F|_m|_{\overline{\ell}}) < len(S_F|_m)$.(why?)
Due to ind. hyp., $w(F|_m|_{\overline{\ell}} \vdash \emptyset) \leq W + b$.

Due to the width increment theorem, $w(F|_m \vdash \emptyset) \leq W + b$. ...

Exercise 7.4

Give the proof of the above why.

Long proofs theorem(contd.) V

Proof(contd.)

For empty m, we have proven

$$\text{if } \rho^{-(b-1)} \leq fat(S_F) < \rho^{-b} \text{ then } w(F \vdash \emptyset) \leq W + b.$$

Let us choose

$$W = \sqrt{2n \ln |F \vdash \emptyset|}.$$

Since we assumed $n > w(F)^2$ and $|F \vdash \emptyset| \geq 2$(why?), (narrow formula)

$$W = \sqrt{2n \ln |F \vdash \emptyset|} \geq w(F). \text{ (why?)}$$

...

Commentary: The choice of W is clever! No automated theorem prover can guess the W.

Long proofs theorem(contd.) VI

Proof(contd.)

Consider the mathematical identity,

$$e^{cx^2} < \underbrace{(1 - cx)^{-x}}_{increasing} = e^{1+cx^2+c^2x^3/2+..}.$$

Let $c = 1/2n$ and $x = W = \sqrt{2n \ln |F \vdash \emptyset|}$. We obtain

$$|F \vdash \emptyset| < (1 - \sqrt{2n \ln |F \vdash \emptyset|}/(2n))^{-\lceil \sqrt{2n \ln |F \vdash \emptyset|} \rceil}.$$

Therefore, $|F \vdash \emptyset| < \rho^{-\lceil W \rceil}$.Therefore, $fat(S_F) < \rho^{-\lceil W \rceil}$.
Therefore, $w(F \vdash \emptyset) \leq W + \lceil W \rceil \leq 2W + 1$
Therefore, $w(F \vdash \emptyset) \leq \sqrt{8n \ln |F \vdash \emptyset|}$ (if wide then long) $\square$

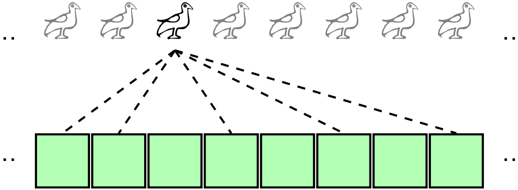
5 min break!

Narrow formulas with wide proofs

Now we present narrow unsat formulas that has only wide proofs.

Restricted pigeon hole principle

Consider $n+1$ pigeons and n holes. Each pigeon i is assigned at most 5 holes $R_i = \{h_{i1}, .., h_{i5}\}$ where it can sit.



And, R_is satisfy the following property.

For each $P \subseteq 0..n$ with $|P| \leq n/3000 \quad |\{k | \text{unique } i \in P \text{ s.t. } k \in R_i\}| \geq |P|$.

The principle: if pigeons are sitting in the respective assigned holes then there is a hole with at least 2 pigeons.

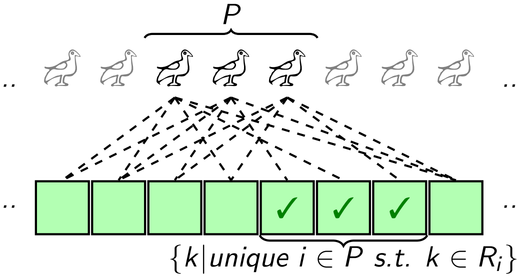
Understanding the restriction

Recall:

For each $P \subseteq 0..n$ with $|P| \leq n/3000 \quad |\{k|\text{unique } i \in P \text{ s.t. } k \in R_i\}| \geq |P|$.

Example 7.1

Let $n \geq 9000$. If $|P| = 3$, P must have the above property.



Exercise 7.5

a. Is it possible to have $|\{k|unique\ i \in 1..n\ s.t.\ k \in R_i\}| = n$?

b. Show any subset of pigeons that are less than $n/3000$ can sit without offending each other.

SAT encoding for restricted pigeon hole principle

Variables: p_{ij} for $i \in 0..n$ and $j \in \{h_{i1}, \ldots, h_{i5}\}$.

Clauses: Let F consists of the following clauses.

- Each pigeon sits in at least one of its assigned holes

$$\text{for each } i \in 0..n \qquad C_i = (p_{i h_{i1}} \vee \cdots \vee p_{i h_{i5}})$$

- There is at most one pigeon in each hole.
  for each $0 \leq i < j \leq n, k \in R_i \cap R_j$

$$(\neg p_{ik} \vee \neg p_{jk})$$

  Let H denote all the hole clauses.

We need to show that $F = H \wedge \bigwedge_{i=0}^{n} C_i$ is unsat.

Narrow formulas : $\mathbf{Vars}(F) = 5n + 5$, $w(F) = 5$, and $|F \vdash \emptyset| > 2_{\text{(why?)}}$.

Existence of the restriction

Theorem 7.5

There exists R_is for sufficiently large n such that

for each $P \subseteq 0..n$ with $|P| \leq n/3000 \quad |\{k|\text{unique } i \in P \text{ s.t. } k \in R_i\}| \geq |P|$.

Proof.

We overestimate the probability p_t of existence of P of size t such that $|\{k|\text{unique } i \in P \text{ s.t. } k \in R_i\}| < t$.

$$p_t < \underbrace{\binom{n+1}{t}}_{1}\underbrace{\binom{5t}{2t}}_{2}\underbrace{(\frac{3t}{n})}_{3}^{2t}$$

1. Choose a P of size t.
2. Choose $2t$ places that repeat the values that are in the other $3t$ places
3. ratio of available choices for the chosen places

...

Existence of the restriction

Proof.

Simplifying

$$p_t < \binom{n+1}{t}\binom{5t}{2t}(\frac{3t}{n})^{2t} < 2\binom{n}{t}\binom{5t}{2t}(\frac{3t}{n})^{2t}.$$

Since $\binom{n}{k} \leq (ne/k)^k$,

$$p_t < 2\binom{n}{t}\binom{5t}{2t}(\frac{3t}{n})^{2t} \leq 2(\frac{ne}{t})^{t}(\frac{5te}{2t})^{2t}(\frac{3t}{n})^{2t} = 2(\frac{225e^3}{4}\frac{t}{m})^{t}.$$

Since $t \leq m/3000$,

$$p_t < 2(\frac{225e^3}{12000})^{t}.$$

$$\sum_{t=2}^{t \leq m/3000} p_t < \sum_{t=2}^{\infty}(\frac{225e^3}{12000})^{t} \approx .455$$

Therefore, the restricted pigeon hole principle exists. □

Wide proofs

Theorem 7.6

$w(F \vdash \emptyset) \geq n/6000$

Proof.

Let $\alpha(P) = \{C_i | i \in P\} \cup H$.
Let $\mu(C) = min\{|P| \,|P \subseteq 0..n \text{ and } \alpha(P) \vdash C\}$.

$$\text{If } \frac{C' \quad C''}{C}\text{Resolution}, \quad \mu(C) \leq \mu(C') + \mu(C'').$$

Due to the restriction def., $\mu(\emptyset) \geq n/3000$.(why?)
For each i, $\mu(C_i) = 1$ and for each $D \in H$, $\mu(D) = 0$.

Therefore, there is a C such that

$$n/6000 \leq \mu(C) \leq n/3000.\text{(why?)}$$

...

Exercise 7.6

Give a proof of the last why.

Wide proofs

Proof.

Let P be s.t. $\alpha(P) \vdash C$ and $|P| = \mu(C)$.

Choose hole k s.t. there is unique pigeon $i \in P$ s.t. $k \in R_i$.

claim: For some j, p_{jk} or $\neg p_{jk}$ occurs in C.

Now assume for any $j \in 0..n$, p_{jk} and $\neg p_{jk}$ do not occur in C.

By def, $\alpha(P - \{i\}) \nvdash C$

Choose m s.t. $m \models \alpha(P - \{i\})$, $m \not\models C_i$, and $m \not\models C$.

For all $j \in 0..n$ if $k \in R_j$, we apply $m := m[p_{jk} \mapsto 0]$.(remove pigeons from kth hole,if any)

And still, $m \models \alpha(P - \{i\})$, $m \not\models C_i$ and $m \not\models C$.(why?)

Now set $m := m[p_{ik} \mapsto 1]$. (placing ith pigeon in kth hole, no challenge to the assignment)

Now, $m \models \alpha(P - \{i\})$, $m \models C_i$ and $m \not\models C$.(why?)Contradiction.

Therefore $|C| \geq n/6000$. □

End of Lecture 7

Commentary: Note that $\alpha(P - \{i\})$ and C do not care who is sitting at kth whole according to m.