Course "Propositional Proof Complexity", JASS'09

Width-based lower bounds for resolution

Mykola Protsenko

Fakultät für Informatik
TU München

May 9, 2009

Definition 1

- x - variable over $\{0, 1\}$, 1 - True, 0 - False
- A literal over x: x (also x^1) or $\overline{x}$ (x^0)
- A clause: a disjunction of literals
- A CNF formula: conjunction of clauses

Example 2

CNF: $(\overline{x}_1 \vee x_2) \wedge (\overline{x}_2 \vee x_3 \vee x_4)$

Definition 3

Let $\mathfrak{F} = \{C_1, C_2, ...C_m\}$ be a CNF formula over n variables. A Resolution derivation of a clause A from $\mathfrak{F}$ is a sequence of clauses $\pi = \{D_1, D_2, ...D_S\}$ with

- D_S = A
- Each line D_i is either initial clause $C_j \in \mathfrak{F}$ or derived from previous lines used one of derivation rules
  - **(1) The Resolution Rule**

$$\frac{E \vee x \quad F \vee \overline{x}}{E \vee F}$$

  - **(2) The Weakening Rule**

$$\frac{E}{E \vee F}$$

- **(1) The Resolution Rule**

$$\frac{E \vee x \quad F \vee \overline{x}}{E \vee F}$$

- **(2) The Weakening Rule**

$$\frac{E}{E \vee F}$$

Where $x \in \{x_1, x_2, ..., x_n\}$ and E, F - arbitrary clauses.

Example 4

Application of resolution rule:

$$(\overline{x}_1 \vee x_2) \wedge (\overline{x}_2 \vee x_3 \vee x_4) \quad \Rightarrow \quad (\overline{x}_1 \vee x_3 \vee x_4)$$

Definition 5

A resolution refutation is a resolution derivation of the empty clause 0.

Example 6

$\mathfrak{F} = \{ (\overline{x}_1 \vee \overline{x}_3),\ (x_3 \vee \overline{x}_2),\ x_2,\ x_1 \}$

1) $(\overline{x}_1 \vee \overline{x}_3) \quad (x_3 \vee \overline{x}_2) \Rightarrow (\overline{x}_1 \vee \overline{x}_2)$
2) $(\overline{x}_1 \vee \overline{x}_2) \quad x_2 \Rightarrow \overline{x}_1$
3) $\overline{x}_1 \quad x_1 \Rightarrow 0$

$\pi = \{ (\overline{x}_1 \vee \overline{x}_3),\ (x_3 \vee \overline{x}_2),\ x_2,\ x_1,\ (\overline{x}_1 \vee \overline{x}_2),\ \overline{x}_1,\ 0 \}$

Graph G_π:

- **Nodes** - clauses of derivation
- **Edges** - derivation steps, from assumption clause to consequence clause

- G_π is a **DAG**
- if G_π is a **tree**, derivation π is called **tree-like**
- we may make copies of original clauses in $\mathfrak{F}$ to make π tree-like

Definition 7

S_π, the size of a derivation π is the number of lines (clauses) in it.

- $S(\mathfrak{F})$ is the minimal size of a refutation of $\mathfrak{F}$
- $S_T(\mathfrak{F})$ is the minimal size of a **tree-like** refutation of $\mathfrak{F}$

Definition 8

- w(C) - the width of a clause C: number of literals in it
- The width of a set of clauses $\mathfrak{F}$:

$$w(\mathfrak{F}) = max_{C \in \mathfrak{F}}\{w(C)\}$$

  In most cases input tautologies $\mathfrak{F}$ have $w(\mathfrak{F}) = O(1)$

- $w(\mathfrak{F} \vdash A)$ - the width of deriving a clause A from $\mathfrak{F}$:

$$w(\mathfrak{F} \vdash A) = min_{\pi}\{w(\pi)\}$$

$\mathfrak{F} \vdash_w A$ means that A can be derived from $\mathfrak{F}$ in width w. In our scope:

$$w(\mathfrak{F} \vdash 0)$$

In this section will be shown, that if $\mathfrak{F}$ has a short resolution refutation then it has a refutation with small width.

Definition 9

For C a clause, x a variable and $a \in \{0, 1\}$, restriction of x on a is:

$$C\mid_{x=a} =^{def} \begin{cases} C, & x \notin C \\ 1, & x^a \in C \\ C \setminus \{x^{1-a}\}, & \text{otherwise} \end{cases}$$

For $\mathfrak{F}$,

$$\mathfrak{F}\mid_{x=a} =^{def} \{C\mid_{x=a} : \ C \in \mathfrak{F}\}$$

For $\pi = \{C_1, \dots C_S\}$ a derivation of C_S from $\mathfrak{F}$ and $a \in \{0,1\}$, let $\pi \mid_{x=a} = \{C'_1, \dots C'_S\}$ be the restriction of π on $x = a$, with:

$$C \mid_{x=a} =^{def} \begin{cases} C_i \mid_{x=a} & C_i \in C \\ C'_{j_1} \vee C'_{j_2} & C_i \text{ was derived from} \\ & C_{j_1} \vee y \text{ and } C_{j_2} \vee \overline{y} \text{ via resolution step,} \\ & \text{for } j_1 < j_2 < i \\ C'_j \vee A \mid_{x=a}, & C_i = C_j \vee A \text{ via the weakening rule,} \\ & \text{for } j < i \end{cases}$$

Theorem 10

$w(\mathfrak{F} \vdash 0) \leq w(\mathfrak{F}) + \log S_T(\mathfrak{F})$

Proof.

Induction on Size of refutation.

- **Base case.** $S_T(\mathfrak{F}) = 1$, clear.
- **Inductive step.** Assume:
  For all $\mathfrak{F}'$ with a tree-like refutation of size $S' < S$ exists a tree-like resolution refutation π' with

$$w(\pi') \leq \lceil \log_2 S' \rceil + w(\mathfrak{F}')$$

Proof.

- Consider tree-like resolution refutation of $\mathfrak{F}$, size S.
- Let **x** be the last variable resolved.
- W.l.o.g.: $\overline{x}$ derived with size at most $S/2$, x - with size strictly smaller than S (the sum of them is S-1).
- Refutation of $\mathfrak{F}\mid_{x=1}$:
  $S(\mathfrak{F} \vdash \overline{x}) \leq S/2 \quad \Rightarrow \quad S(\mathfrak{F}\mid_{x=1} \vdash 0) \leq S/2$
- Applying **induction hypotheses**:
  $w(\mathfrak{F}\mid_{x=1} \vdash 0) = \lceil \log_2(S/2) \rceil + w(\mathfrak{F}) = \lceil \log_2(S) \rceil + w(\mathfrak{F}) - 1$
- Adding $\overline{x}$ to each clause lets us derive $\overline{x}$ with width $\lceil \log_2(S) \rceil + w(\mathfrak{F})$

Proof.

- Another subtree: $w(\mathfrak{F}\mid_{x=0} \vdash 0) = \lceil \log_2(S) \rceil + w(\mathfrak{F})$.
- Use a copy of $\overline{x}$-subtree to eliminate x in a bottom of x-subtree.
- It allows us to refute $\mathfrak{F}$ with width $\lceil \log_2(S) \rceil + w(\mathfrak{F})$

□

Solving the inequality for S_T:

Corollary 11

$S_T(\mathfrak{F}) \geq 2^{w(\mathfrak{F} \vdash 0) - w(\mathfrak{F})}$

Theorem 12

$w(\mathfrak{F} \vdash 0) \leq w(\mathfrak{F}) + O(\sqrt{n \ln S(\mathfrak{F})})$

Idea of proof

- find the **most popular** literals appearing in **large** clauses
- resolving on these literals at the beginning allows to keep the width of whole proof small

Corollary 13

$S(\mathfrak{F}) = \exp(\Omega(w(\mathfrak{F} \vdash 0) - w(\mathfrak{F}))^2 n$

Definition 14

Let

- $\mathfrak{F}$ be a set of unsatisfiable clauses.
- $s(\mathfrak{F})$ the size of the minimum unsatisfiable subset of $\mathfrak{F}$

Define

- the boundary $\delta\mathfrak{F}$ of $\mathfrak{F}$ - the set of variables appearing in **exactly one clause** of $\mathfrak{F}$.
- the sub-critical expansion of $\mathfrak{F}$:

$$e(\mathfrak{F}) = \max_{s \leq s(\mathfrak{F})} \min\{|\ \delta G\ | :\ G \subseteq \mathfrak{F}, s/2 \leq |G| < s\}$$

For clause $C \in \pi$ and collection of clauses $G \subseteq \mathfrak{F}$. Notation $G \Rightarrow_\pi C$ means that all clauses in G are used in π to derive C.

Definition 15

Define complexity $comp_\pi(C)$ to be the size of set $G \subseteq \mathfrak{F}$ with $G \Rightarrow_\pi C$.

- $comp_\pi(0) \geq s(\mathfrak{F})$ (By definition)
- $comp_\pi(C) = 1$ for $C \in \mathfrak{F}$ (By definition)
- $comp_\pi$ is subadditive: $comp_\pi(C) \leq comp_\pi(A) + comp_\pi(B)$ if C is a resolvent of A and B.

Lemma 16

If π is a resolution refutation of $\mathfrak{F}$, then $w(\pi) \geq e(\mathfrak{F})$.

Proof.

- If $G \Rightarrow_\pi C$ then $w(C) \geq \mid \delta G \mid$.
- For any $s \leq s(\mathfrak{F})$ the last clause C in π with $comp_\pi < s$ satisfies $w(C) \geq \mid \delta G \mid$ for some $G \subseteq \mathfrak{F}$ with $s/2 \leq \mid G \mid < s$.
- Maximizing over all choices of $s \leq s((F))$ we become $w(\pi) \geq e(\mathfrak{F})$

Reminder:

$$e(\mathfrak{F}) = \max_{s \leq s(\mathfrak{F})} \min\{\mid \delta G \mid : \; G \subseteq \mathfrak{F}, s/2 \leq |G| < s\}$$

□

A **Tseitin contradiction** is an unsatisfiable CNF based on combinatorial principle that for every graph, the sum of degrees of all vertices is even.

Definition 17

- Fix G a finite connected graph, with $|V(G)| = n$.
- Fix $f : V(G) \to \{0, 1\}$ a function with **odd-weight**, i.e. $\sum_{v \in V(G)} f(v) = 1 \ (mod\ 2)$
- $d_G(v)$ - **degree** of v in G
- Assign distinct variable x_e to each $e \in E(G)$.
- For $v \in V(G)$ define $PARITY_v =^{def} (\bigoplus_{v \in e} x_e \equiv f(v) \ (mod\ 2))$

The Tseitin Contradiction of G and f is:

$$\tau(G, f) = \bigwedge_{v \in V(G)} PARITY_v$$

If the maximal degree of G is constant, then initial size and width of $\tau(G, f)$ is also small:

Lemma 18

If d is the maximal degree of G, then $\tau(G, f)$ is a d-CNF with at most $n \cdot 2^{d-1}$ clauses, and nd/2 variables.

Definition 19

For G a finite graph, the Expansion of G is:

$$e(G) =^{def} min\{|E(V', V \setminus V')| : V' \subseteq V, |V|/3 \leq |V'| \leq 2|V|/3\}$$

The width of refuting $\tau(G, f)$ is a bounded from below by the expansion of the graph G.

Theorem 20

For G a connected graph and f an odd-weight function on V(G),

$$w(\tau(G, f) \vdash 0) \geq e(G)$$

The width of refuting $\tau(G, f)$ is a bounded from below by the expansion of the graph G.

Theorem 20

For G a connected graph and f an odd-weight function on V(G),

$$w(\tau(G, f) \vdash 0) \geq e(G)$$

Corollary 21

For G a 3-regular connected Expander (i.e. $e(G) = \Omega(|V|)$) and f an odd-weight function on $V(G)$,

$$S(\tau(G, f)) = 2^{\Omega(|V|)}$$

The Pigeonhole Principle:

- **m** pigeons
- **n** pigeonholes
- m $\geq$ n $\Rightarrow$ there is no 1-1 map from m to n

Can be stated as formula on $n \cdot m$ variables x_{ij}, $1 \leq i \leq m$, $1 \leq j \leq n$, where $x_{ij} = 1$ means that i is mapped to j.

Definition 22

PHP_n^m is the conjunction of the set of clauses:

$$P_i =^{def} \bigvee_{1 \leq j \leq n} x_{ij}$$

for $1 \leq i \leq m$

$$H_{i,i'}^{j} =^{def} \overline{x}_{ij} \vee \overline{x}_{i'j}$$

for $1 \leq i < i' \leq m$, $1 \leq j \leq n$.

PHP_n^m is a CNF:

- unsatisfiable for $m > n$
- $m \cdot n \geq n^2$ variables
- $O(m^2)$ clauses
- initial width n

Example 23

PHP^3_2: m = 3 pigeons, n = 2 holes

$$P_1 = (x_{11} \vee x_{12}) \quad P_2 = (x_{21} \vee x_{22}) \quad P_3 = (x_{31} \vee x_{32})$$

$$H^1_{12} = (\overline{x}_{11} \vee \overline{x}_{21}) \quad H^1_{13} = (\overline{x}_{11} \vee \overline{x}_{31}) \quad H^1_{23} = (\overline{x}_{21} \vee \overline{x}_{31})$$

$$H^2_{12} = (\overline{x}_{11} \vee \overline{x}_{21}) \quad H^2_{13} = (\overline{x}_{11} \vee \overline{x}_{31}) \quad H^2_{23} = (\overline{x}_{21} \vee \overline{x}_{31})$$

Resolution of PHP^m_n:

$$w(PHP^m_n \vdash 0) \leq n$$

Example 24

- Take $(x_{11} \vee x_{12} \vee x_{13} \vee ... \vee x_{1n})$ (*)
  and $(\overline{x}_{11} \vee \overline{x}_{21})$, $(\overline{x}_{12} \vee \overline{x}_{22})$, ... $(\overline{x}_{1n} \vee \overline{x}_{2n})$.
- Apply **resolution rue** consecutively, to achieve $(\overline{x}_{11} \vee \overline{x}_{12} \vee \overline{x}_{13} \vee ... \vee \overline{x}_{1n})$
- Then apply the **resolution rule** with (*) to become **0**.

$$w(PHP_n^m \vdash 0) \leq n$$

$\Rightarrow$ we **cannot** achieve lower bound on size via **size-width relation:**

$$S_T(\mathfrak{F}) \geq 2^{w(\mathfrak{F} \vdash 0) - w(\mathfrak{F})}$$

$$S_T(PHP_n^m) \geq 2^{w(PHP_n^m \vdash 0) - w(PHP_n^m)}$$

$$S_T(PHP_n^m) \geq 2^{w(PHP_n^m \vdash 0) - n}$$

$$S_T(PHP_n^m) \geq 1$$

Definition 25

A Nondeterministic Extension of a Boolean function $f(\overrightarrow{x})$ is a function $g(\overrightarrow{x}, \overrightarrow{y})$ with:

$$f(\overrightarrow{x}) = 1 \quad \textit{iff} \quad \exists \overrightarrow{y}\ g(\overrightarrow{x}, \overrightarrow{y}) = 1$$

- $\overrightarrow{x}$ - **Original** variables
- $\overrightarrow{y}$ - **Extension** variables

Definition 26

$EPHP^m_n$, a Row-Extension of PHP^m_n:
derived by replacing every P_i with some **nondeterministic extension** CNF formula EP_i, using **distinct** extension variables $\overrightarrow{y}_i$ for distinct rows.

One standard extension:

Example 27

Replace each P_i with:

$$\overline{y}_{i0} \wedge \bigwedge_{j=1}^{n} (y_{ij-1} \vee x_{ij} \vee \overline{y}_{ij}) \wedge y_{in}$$

- 3-CNF over n+2 clauses and 2n+1 variables

Theorem 28

For $m > n$, $w(EPHP_n^m \vdash 0) \geq n/3$

Theorem 28

For $m > n$, $w(EPHP^m_n \vdash 0) \geq n/3$

Corollary 29

For all $m > n$ and any Row Extension of PHP^m_n,
$S_T(EPHP^m_n) = 2^{\Omega(n)}$

Definition 30

Generalized PHP:

- $G = ((V \uplus U), E)$ - bipartite graph
- $|V| = m, \quad |U| = n$
- x_e - distinct variable assigned to each edge

G - PHP is the conjunction of

- $P_v =^{def} \bigvee_{v \in e} x_e \quad for \quad v \in V$
- $H^u_{v,v'} =^{def} \overline{x}_e \vee \overline{x}_{e'} \quad for \quad e = (v, u),\ e' = (v', u), \qquad v, v' \in V,\ v \neq v',\ u \in U$

Note: $PHP^m_n = K_{m,n} - PHP$

Lemma 31

For any two bipartite graphs G, G' mit V(G) = V(G'):

$$E(G') \subseteq E(G), \quad \Rightarrow \quad S(G' - PHP) \leq S(G - PHP)$$

It means:

$$S(PHP_n^m) \geq S(G - PHP)$$

Definition 32

Bipartite Expansion. For a vertex $u \in U$, let $N(u)$ be its set of neighbors. For a subset $V' \subset V$ let its **boundary** be

$$\delta V' =^{def} \{u \in U : |N(u) \bigcap V'| = 1\}$$

A bipartite graph G is a (m,n,d,r,e)-Expander if:

- $|V| = m$, $|U| = n$
- $d_G(v) \leq d$ for $\forall v \in V$
- $\forall\ V' \subset V, |V'| \leq r \quad |\delta V'| \geq e|V'|$

Theorem 33

For every bipartite graph **G** *that is an* **(m,n,d,r,e)-expander**

$$w(G - PHP \vdash 0) \geq (r \cdot e)/2$$

For m = n + 1 there exist $(m, n, 5, n/c, 1)$-expanders for some constant $c \geq 1$

Corollary 34

$S(PHP_n^{n+1}) = 2^{\Omega(n)}$

For $m \gg n$ there exist $(m, n, \log m, \Omega(n/\log m), \frac{3}{4}\log m)$-expanders

Corollary 35

$S(PHP_n^m) = 2^{\Omega(n^2/m\log m)}$

For τ a contradiction over n variables:

- if exists tree-like refutation of size S_T, then there is a refutation of maximal width $\log_2 S_T$.
- if it has a general refutation of size S, then it has a refutation of maximal width $O(\sqrt{n \log S})$

This relations can be useful to

- prove size lover bounds by proving width lover bounds
- develop automatic provers