Course "Propositional Proof Complexity", JASS'09

Width-based lower bounds for resolution

Mykola Protsenko

9.5.2009

Contents

1 Notation and definitions

In this section we will introduce some notation used in in this paper.

x will denote a **variable** over $\{0, 1\}$, 1 corresponds to True and 0 - to False.

A literal over x is either x (also x^1) or $\overline{x}$ (x^0).

A clause is defined as a disjunction of literals.

A CNF formula is conjunction of clauses.

Example 1 *CNF:* $(\overline{x}_1 \vee x_2) \wedge (\overline{x}_2 \vee x_3 \vee x_4)$

Definition 1 *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 $D_S = A$ and 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***

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

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

The Weakening rule is not essential, as even without it the Resolution proof system is complete.

Example 2 *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 2 *A **resolution refutation** is a resolution derivation of the empty clause 0.*

Example 3 $\mathfrak{F} = \{\ (\overline{x}_1 \vee \overline{x}_3),\ (x_3 \vee \overline{x}_2),\ x_2,\ x_1\ \}$

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

The **Graph** G_π of a derivation π is a DAG with the clauses of the derivation as nodes and derivation steps as edges, from the assumption clauses to the consequence clause. 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.

The size of a derivation π, denoted S_π, is the number of lines (clauses) in it. $S(\mathfrak{F})$ is the minimal size of a refutation of $\mathfrak{F}$, and $S_T(\mathfrak{F})$ is the minimal size of a **tree-like** refutation of $\mathfrak{F}$.

Definition 3 ***The width** of a clause C, denoted $w(C)$, is the number of literals in it. The width of a set of clauses $\mathfrak{F}$ is the maximal width of a clause in the set:*

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

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

***The width of deriving** a clause A from the formula $\mathfrak{F}$, denoted $w(\mathfrak{F} \vdash A)$, is defined as*

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

where the minimum is taken over all derivations π of A from $\mathfrak{F}$. The notation $\mathfrak{F} \vdash_w A$ means also that A can be derived from $\mathfrak{F}$ in width w.

In our scope: width of refutations, namely

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

Definition 4 *For C a clause, x a variable and $a \in \{0,1\}$, **restriction** of x on a is:*

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

Similarly, for $\mathfrak{F}$

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

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

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

2 The Size-Width Relations

Theorem 1 $w(\mathfrak{F} \vdash 0) \leq w(\mathfrak{F}) + \log S_T(\mathfrak{F})$

Proof.

We show this by **induction** on the **size** of the resolution proof.

The claim holds for $S_T(\mathfrak{F}) = 1$. Now assume that for all sets $\mathfrak{F}'$ of clauses with a tree-like resolution refutation of size $S_T(\mathfrak{F}') < S$, there is tree-like resolution refutation π' of $\mathfrak{F}$ with

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

.

Consider a tree-like resolution refutation of $\mathfrak{F}$ with $S_T(\mathfrak{F}) = S$. Let **x** be the last variable resolved on to derive 0. So, we have two subtrees: one that derives **x**, and another one that derives $\overline{x}$. One of the two subtrees has size size at most $S/2$ and the other has size strictly less that S. Assume W.l.o.g that these are left (deriving $\overline{x}$) and right (deriving x) subtree, respectively.

Since we can prove $\overline{x}$ from $\mathfrak{F}$ in size S/2, we can also prove 0 from $\mathfrak{F}\mid_{x=1}$ in size at most S/2. The induction hypotheses implies that we can also derive 0 from $\mathfrak{F}\mid_{x=1}$ with width at most w-1:

$$w(\mathfrak{F}\mid_{x=1} \vdash 0) = \lceil \log_2(S/2) \rceil + w(\mathfrak{F}) = \lceil \log_2(S) \rceil + w(\mathfrak{F}) - 1$$

We add $\overline{x}$ to each of clauses in this proof, so we derive $\overline{x}$ from $\mathfrak{F}$ in width $w = \lceil \log_2(S) \rceil + w(\mathfrak{F})$.

In similar way, starting with another subtree, which has size strictly smaller than S, we can derive 0 from $\mathfrak{F}\mid_{x=0}$ in width at most $w = \lceil \log_2(S) \rceil + w(\mathfrak{F})$.

We can use a copy of the left-sub tree (that derives $\overline{x}$) to resolve with each leaf clause of the right subtree that contains x. This allows us to eliminate x right at the bottom of the right subtree, and we are effectively left with $\mathfrak{F}\mid_{x=0}$. So, we can derive 0 from this in width $\lceil \log_2(S) \rceil + w(\mathfrak{F})$.

□

Solving the inequality for S_T:

Corollary 1 $S_T(\mathfrak{F}) \geq 2^{w(\mathfrak{F} \vdash 0) - w(\mathfrak{F})}$

Theorem 2 $w(\mathfrak{F} \vdash 0) \leq w(\mathfrak{F}) + O(\sqrt{n \ln S(\mathfrak{F})})$

Proof.

The key idea behind this proof is to repeatedly find the popular literals appearing in large clauses in the given resolution proof. Resolving on these literals at the very beginning allows us to keep the width of whole proof small.

We call a clause **large** if it has width at least $W = \sqrt{2n \ln S}$. Since there are at most 2n literals and at least W of them appear in any large clause, an average literal must occur in at least $W/2n$ fraction of large clauses. Let k be such that $(1 - W/2n)^k S \leq 1$. It holds if $k \leq \sqrt{2n \ln S}$. We show by induction on n and k that any $\mathfrak{F}$ with at most S large clauses has a proof of width $\leq k + w(\mathfrak{F})$.

The base case is trivial. Assume now that the theorem holds for all smaller values of n and k.

Choose the literal x that occurs most frequently in large clauses and set it to 1. This, by what we already observed, will satisfy at least a $W/2n$ fraction of large clauses . What we get as a result is a refutation of $\mathfrak{F}\mid_{x=1}$ with at most $S(1 - W/2n)$ large clauses. By our induction hypothesis, $\mathfrak{F}\mid_{x=1}$ has a refutation of width at most $k - 1 + w(\mathfrak{F})$. Hence there is a derivation of $\overline{x}$ from $\mathfrak{F}$ of width at most $k + w(\mathfrak{F})$.

Now consider $\mathfrak{F}\mid_{x=0}$. If we restrict the proof of $\mathfrak{F}$ which has at most S large clauses, we get a proof of $\mathfrak{F}\mid_{x=0}$ with at most S large clauses and involving one less variable. The induction hypothesis implies that there is a refutation of $\mathfrak{F}\mid_{x=0}$ with width at most $k + w(\mathfrak{F})$.

As in the proof of tree-like resolution case, we can use the derivation of $\overline{x}$ from $\mathfrak{F}$ in width at most $k + w(\mathfrak{F})$ at each leaf of the proof and resolve $\overline{x}$ with each clause of $\mathfrak{F}$ containing x to get $\mathfrak{F}\mid_{x=0}$. We now use the refutation of the latter set in width $k + w(\mathfrak{F})$.

□

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

3 Expansion

Let $\mathfrak{F}$ be a set of unsatisfiable clauses and $s(\mathfrak{F})$ - the size of the minimum unsatisfiable subset of $\mathfrak{F}$. We define **boundary** $\delta\mathfrak{F}$ of $\mathfrak{F}$ to be the set of variable appearing in exactly one clause of $\mathfrak{F}$. Let the **sub-critical expansion** of $\mathfrak{F}$ be

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

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 5 *Define* ***complexity*** $comp_\pi(C)$ *to be the size of set* $G \subseteq \mathfrak{F}$ *with* $G \Rightarrow_\pi C$. *By definition* $comp_\pi(0) \geq s(\mathfrak{F})$ *and* $comp_\pi(C) = 1$ *for* $C \in \mathfrak{F}$. $comp_\pi$ *is subadditive:*

$$comp_\pi(C) \leq comp_\pi(A) + comp_\pi(B)$$

if C *is a resolvent of* A *and* B.

The main tool, used in proving lower bounds on width, is the relationship between width and expansion.

Theorem 3 *If* π *is a resolution refutation of* $\mathfrak{F}$, *then* $w(\pi) \geq e(\mathfrak{F})$.

Proof.

If $G \Rightarrow_\pi C$ then every variable in δG appears in C and so $w(C) \geq | \delta G |$. For any $s \leq s(\mathfrak{F})$ the last clause C in π with $comp_\pi < s$ satisfies $w(C) \geq | \delta G |$ for some $G \subseteq \mathfrak{F}$ with $s/2 \leq | G | < s$. Maximizing over all choices of $s \leq s((F))$ we get $w(\pi) \geq e(\mathfrak{F})$.

□

4 Lover bounds for Tseitin and PHP

All lower bounds on width follow the same strategy:

(1) Define a complexity measure $\mu : clauses \rightarrow N$ such that $\mu(Axiom) \leq 1$

(2) Prove $\mu(0)$ is large

(3) Infer that in any refutation there is some clause C with medium size $\mu(C)$

(4) Prove that if $\mu(C)$ is medium, then w(C) is large.

First we need to define a measure that will satisfy conditions (1)-(3).

For f a Boolean function, let Vars(f) denote the set of variables appearing in f. Let $\alpha \in \{0, 1\}^{Vars(f)}$ be an assignment to f. We say that α satisfies f, if $f(\alpha) = 1$. For C a clause and Γ a set of Boolean functions, let $V = Vars(\Gamma) \bigcup Vars(C)$. We say that Γ implies C, denoted $\Gamma \models C$, if every assignment satisfying every function $\gamma \in \Gamma$ satisfies C as well.

Definition 6 *Let $\mathcal{A}$ be an unsatisfiable set of Boolean functions, that is, $\mathcal{A} \models 0$, and let C be a clause.*

$$\mu_{\mathcal{A}}(C) =^{def} min\{\mid \mathcal{A}' \mid : \mathcal{A}' \subseteq \mathcal{A}, \mathcal{A} \models C\}$$

$\mu_{\mathcal{A}}$ is a subadditive complexity measure with respect to resolution steps:

Lemma 1 *Suppose D was inferred from B, C by a single resolution step. Then for any set of boolean functions $\mathcal{A}$:*

$$\mu_{\mathcal{A}}(D) \leq \mu_{\mathcal{A}}(B) + \mu_{\mathcal{A}}(C)$$

To assure Condition (1), we want $\mu(Axiom)$ to be small:

Definition 7 *For $\mathfrak{F}$ a nonsatisfiable CNF we say that $\mathcal{A}$ is **compatible** with $\mathfrak{F}$ if $\mathcal{A} \models 0$ and $\forall C \in \mathfrak{F}$ $\mu(C) \leq 1$.*

The condition (2) is intuitively for "hard" tautologies.
The condition (3) can be deduced from the definitions:

Lemma 2 *If $\mathcal{A}$ is compatible with $\mathfrak{F}$, then in every refutation of $\mathfrak{F}$ there must be a clause C with*

$$\frac{\mu(0)}{3} \leq \mu(C) \leq \frac{2\mu(0)}{3}$$

Definition 8 *A Boolean function f is called **Sensitive** if any two distinct falsifying assignments $\alpha, \quad \beta \in f^{-1}(0)$, have Hamming distance greater than 1.*

Examples of Sensitive functions are PARITY (see below) and OR.

Definition 9 *For $\mathcal{A}$ a set of Boolean functions, and $f \in \mathcal{A}$, a **Critical Assignment** for f is an assignment $\alpha \in \{0,1\}^{Vars\mathcal{A}}$ such that*

$$g(\alpha) = \begin{cases} 0 & g = f \\ 1 & g \neq f, g \in \mathcal{A} \end{cases}$$

For $\alpha, \beta \in \{0,1\}^{Vars(\mathcal{A})}$, we say that β is the result of **flipping** α on the variable x, if

$$g(\alpha) = \begin{cases} 1 - \alpha(y) & y = x \\ \alpha(y) & otherwise \end{cases}$$

Definition 10 *For f a Boolean function and x a variable, we say that f is dependent on x, if there is some assignment α such that $f(\alpha) = 0$, but flipping α on x satisfies f.*

*For $\mathcal{A}$ a set of Boolean functions, the **Boundary** of $\mathcal{A}$, denoted $\delta\mathcal{A}$, is the set of variables x such that there is a unique function $f \in \mathcal{A}$ that is dependent on x.*

Note: for $\mathfrak{F}$ a set of **clauses**, we have defined a Boundary of $\mathfrak{F}$ as set of variables appearing in **exactly one clause**. These definitions are essentially equivalent.

4.1 Tseitin Formulas

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 11 *Fix G a finite connected graph, with $|V(G)| = n$. Fix $f : V(G) \rightarrow \{0, 1\}$ a function which is* ***odd-weight****, i.e. $\sum_{v \in V(G)} f(v) = 1$ (mod 2). Denote by $d_G(v)$ the* ***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 3 *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.*

One very important lemma:

Lemma 4 *If G is connected, then $\tau(G, f)$ is contradictory iff f is an odd weight function.*

Definition 12 *For G a finite graph, the* ***Expansion*** *of G is:*

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

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

Theorem 4 *For G a connected graph and f an odd-weight function on V(G),*

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

Proof.

Set $\mathcal{A}_V = \{PARITY_v : v \in V(G)\}$ and denote $\mu(C) = \mu_{\mathcal{A}_V}(C)$. Every axiom C is one of the defining axioms of $PARITY_v$. Clearly for this v $PARITY_v \models C$. So, for any axiom C, $\mu(C) = 1$. We have shown, that $\mathcal{A}_V$ is compatible for $\tau(G, f)$.

Now we claim that $\mu(0) =\mid V(G) \mid$, because for any $\mid V' \mid < \mid V(G() \mid$ $\mathcal{A}_V$ is satisfiable. This can be explained as follows: let v be some vertex in V
V'. The formula $\tau(G, f')$ for

$$f'(u) = \begin{cases} 1 - f(uy) & u = v \\ f(u) & otherwise \end{cases}$$

So by Lemma 5, $\tau(G, f')$ is satisfiable. $\mathcal{A}_V$ is a subformula of $\tau(G, f')$, and hence satisfiable as well. $\mathcal{A}_{V(G)}$ is a collection of PARITY functions, which are sensitive. Finally, for $V' \subseteq V, \delta\mathcal{A}_{V'} = \{x_e : e \in E(V', V$
$V')\}$. This is true because, if e=(v,u), $v \in V'$, $u \in V$
V', then $PARITY_v$ is the only function of $\mathcal{A}_{V'}$ dependent on x_e. Hence, $e(\mathcal{A}_V) \geq e(G)$ and we can apply Theorem 3 to complete the proof.

4.2 The Pigeonhole Principle

The Pigeonhole Principle with **m** pigeons and **n** pigeonholes states that for $m > n$ there is no 1-1 map from m to n.

This 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 13 *PHP_n^m is the conjunction of the sets 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 $1 \leq i < i' \leq m$, $1 \leq j \leq n$.

For $m > n$, PHP_n^m is unsatisfiable CNF with $m \cdot n \geq n^2$ variables, $O(m^2)$ clauses and initial width n.

Example 4 *PHP_2^3: m = 3 pigeons, n = 2 holes*

$P_1 = (x_{11} \vee x_{12})$ $P_2 = (x_{21} \vee x_{22})$ $P_3 = (x_{31} \vee x_{32})$ $H_{12}^1 = (\overline{x}_{11} \vee \overline{x}_{21})$ $H_{13}^1 = (\overline{x}_{11} \vee \overline{x}_{31})$ $H_{23}^1 = (\overline{x}_{21} \vee \overline{x}_{31})$ $H_{12}^2 = (\overline{x}_{11} \vee \overline{x}_{21})$ $H_{13}^2 = (\overline{x}_{11} \vee \overline{x}_{31})$ $H_{23}^2 = (\overline{x}_{21} \vee \overline{x}_{31})$

Resolution of PHP_n^m:

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

Example 5 • *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**.*

$w(PHP_n^m \vdash 0) \leq n$, therefore we **cannot** achieve lower bound on size via **size-width relation:**

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

$$S_T(PHP_n^m) \geq 2^{w(PHP_n^m \vdash 0) - w(PHP_n^m)}$$
$$S_T(PHP_n^m) \geq 2^{w(PHP_n^m \vdash 0) - n}$$
$$S_T(PHP_n^m) \geq 1$$

There are 2 different ways to generalize the pigeonhole tautologies to reduce the initial width.

Definition 14 ***A Nondeterministic Extension*** *of a Boolean function* $f(\overrightarrow{x})$ *is a function* $g(\overrightarrow{x}, \overrightarrow{y})$ *with:*

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

The $\overrightarrow{x}$ *variables are called **Original** variables, and the* $\overrightarrow{y}$ *- **Extension** variables.*

Definition 15 $EPHP_n^m$, *a **Row-Extension** of* PHP_n^m *is derived by replacing every row axiom* P_i *with some **nondeterministic extension** CNF formula* EP_i, *using **distinct** extension variables* $\overrightarrow{y}_i$ *for distinct rows.*

One standard extension:

Example 6 *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 5 *For* $m > n$, $w(EPHP_n^m \vdash 0) \geq n/3$

Proof.

Define $\mathcal{A} = \{A_i : 1 \leq i \leq m\}$ where A_i is the conjunction of EP_i and all hole axioms $H_j^{i,i'}$. We denote $A_I = \bigwedge_{i \in I} A_i$. Set $\mu(C) = \mu_{\mathcal{A}}(C)$.

Clearly, $\mu(Axiom) \leq 1$, $\mu(0) = n+1$, and μ is subadditive. Hence, in every refutation π there must be a clause C with $n/3 \leq \mu(C) < 2n/3$. Fix such a C and fix a minimal $I \subset [m]$ such that $A_I \models C$. Let R(C) be the set of rows who have a literal in C.

If $\mid C \mid \geq n/3$, we are done. Otherwise, there must be some $i \in I \backslash R(C)$. Take any assignment α such that $A_{I\backslash i}(\alpha) = 1$, $A_i(\alpha) = C(\alpha) = 0$, which must exist by the minimality of I. Without loss of generality, α sets all variables outside $R(C) \bigcup I \backslash i$ to 0. By the definition of the A_k's the 1's of original variables in α must be a partial matching. But as $\mid C \mid < n/3$ and $\mid I \mid \leq 2n/3$, there must be a column j in which no original variable is set to 1. Flip the assignment α to set x_{ij} to 1, and extend the nondeterministic variables y_i in any way to set EP_i to 1. Call this new assignment β. It is easy to verify, that $A_I(\beta) = 1$, $C(\beta) = 0$. This is a contradiction.

□

Corollary 3 *For all $m > n$ and any Row Extension of PHP_n^m, $S_T(EPHP_n^m) = 2^{\Omega(n)}$*

Definition 16 ***Generalized PHP:*** *Let $G = ((V \biguplus U), E)$ be a bipartite graph, $|V| = m$, $|U| = n$. We assign a distinct variable x_e to each edge.* ***G - PHP*** *is the conjunction of following clauses:*

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

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

Lemma 5 *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 17 ***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 6 *For every bipartite graph* ***G*** *that is an* ***(m,n,d,r,e)-expander***

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

Proof.

We define $\mathcal{A} = \{A_v : v \in V\}$ with A_v as the conjunction of P_v and all hole axioms $H_u^{v,v'}$. Let us denote $A_{V'} = \bigwedge_{v \in V'} A_v$. Set $\mu(C) = \mu_{\mathcal{A}}(C)$.

$\mu(Axiom) \leq 1$, $\mu(0) \geq r$ (because every V' of size $\mid V' \mid \leq r$ has a matching into U), and μ is subadditive. Hence, in every refutation π there must be a clause C with $r/2 \leq \mu(C) < r$. Fix such a C and fix a minimal $V' \subset V$ such that $A_{V'} \models C$.

We claim that for each $u \in \delta V'$, there must appear in C some variable $x_{(\hat{v},u)}$, for some $\hat{v} \in V$ (but not necessarily in V'). Indeed, for such a boundary u, let v be its only neighbor in V'. Assume for the sake of contradiction that C has no variable $x_{(\hat{v},u)}$. Let α be the assignment satisfying $A_{V' \setminus \{v\}}$ and falsifying A_v and C. Clearly α assigns zero to $x_{v,u}$. We assume without loss of generality that α sets to zero all variables $x_{(\hat{v},u)}$, because this cannot falsify any axiom P_v, for $v' \in V'$ (recall that $x_{(v,u)}$ is a boundary variable). Thus, we may flip α on $x_{(v,u)}$, and get an assignment satisfying $A_{V'}$, without changing the value of C (zero), so we get a contradiction. This means, that the width of C is at least the size of its boundary, and the theorem is proven.

□

5 Conclusion

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

References

- Eli Ben-Sasson and Avi Wigderson "Short Proofs Are Narrow - Resolution Made Simple"
- Paul Beame, "Proof Comlexity" (Lecture Notes)
- Samuel R. Buss "An Introduction to Proof Theory"