

Exponential lower bounds for Dag-like Resolution

Nicola Galesi

Dipartimento di Informatica
Università degli Studi di Roma “La Sapienza”

30 Marzo – 3 Aprile
Dipartimento di Informatica “R. Capocelli”

History of Results

The Result.

- Several examples of family of UNSAT formulae requiring exponential size Daglike Resolution (DLR)
- Refinements of the techniques to prove such results.

History of Results

History [Main]

- (1) [Tseitin69] implicitly gave a first example of UNSAT formula requiring subexponential regular Resolution refutations
- (2) [Haken 85] Gave the first exponential lower bounds for DLR. Use PHP.
- (3) [Chvatal Szemeredi 86] usign Haken method, prove the lower bounds for random k-CNF.
- (4) [Urquhart 88] Extended [CS86] to get exponential lower bounds in DLR for Tseitin Tautologies
- (5) [BeamePitassi 96] Simplify the Haken's metod to prove DLR lower bounds for PHP and Random CNF [This chapter]
- (6) [Ben-Sasson Wigderson 99] Synthesis of the [BP] method into a general method based on the **width** [This chapter]
- (7) [Raz 02, Razborov 05] get exponential lower bounds for WeakPHP, introducing **psuedowidth**

Plan of the Day

1. From Resolution to Monotone Resolution. Polynomial equivalence wrt PHP.
2. The Beame-Pitassi method: PHP requires exponential refutations in DLR.
3. Synthesis of BP method: The width method of Ben-Sasson-Wigderson
4. Application of width method - I : Random k-CNF
5. Application of width method - II : Tseitin formulae
6. The “strange case” of Weak PHP: pseudowidth

Notions and Techniques

1. The **Beame-Pitassi method**
2. The **width method** of Ben-Sasson-Wigderson
3. Complexity of **Random systems of linear equations**
4. **Pseudowidth**

Monotone Resolution

Motivations

DLR Complexity of PHP was considered a big problem. Haken's technique was pretty complicated. Many efforts to simplify it

Monotone Resolution: clauses without negations

Polynomial Equivalence with DLR wrt PHP.

[BP96, BP96] noticed that it sufficient to study monotone DLR to prove lower bounds for PHP

Consequences:

- Great simplification of Haken result on PHP
- Slight simplification of [CS 86] results on random k-CNF
- Developing ground for the with method of [BSW99]

Monotone Resolution for PHP

Let us consider PHP[n+1,n]. Only clauses with positive literals

$$\neg p_{i,j} = \bigvee_{\substack{k \in [n+1] \\ k \neq i}} p_{k,j} \quad P_{R,j} = \bigvee_{i \in R} p_{i,j}$$

Monotone Resolution Rule for PHP

$$\frac{A \vee P_{R,j} \vee P_{S,j} \quad B \vee P_{R,j} \vee P_{T,j}}{A \vee P_{R,j}}$$

Where R,S, and T are disjoint set of indices

Idea of the monotone Rule

Since different pigeons can't go to the same hole we delete variables speaking of different holes and keep only those of common pigeons

Polynomial Simulation

Thm[Buss,Pitassi] MR and DLR polynomially simulate each other on the PHP[m,n], $m > n$.

Proof

ML proof \rightarrow DLR proof. See how to simulate the monotone Rule.

$$\frac{A \vee p_{i,j} \vee p_{i_1,j} \quad B \vee p_{i,j} \vee p_{i_2,j}}{A \vee p_{i,j}}$$

Polynomial Simulation

DLR proof \rightarrow MR proof.

Negation Transformation

$$\neg p_{i,j} = \bigvee_{\substack{k \in [n+1] \\ k \neq i}} p_{k,j}$$

Initial clause

$$\bigvee_{j \in [n]} p_{i,j} \text{ unchanged}$$

$$\neg p_{i,k} \vee \neg p_{j,k} \Rightarrow \bigvee_{j \in [n]} p_{i,j}$$

Polynomial Simulation

Clauses Transformation

$$C = A \vee B \Rightarrow C^+ = A \vee B^+$$

where only B contains negated literals

and B^+ is obtained from B applying the transformation

Proof strategy

$$\frac{A \quad B}{C} \Rightarrow \frac{A^+ \quad B^+}{C^+}$$

I case B is an initial clause of the form $\neg P_{i_1, j} \vee \neg P_{i_2, j}$

II case General Case

[Exercise 1] Study the exact simulations and asymptotic

Conclusions

Exponential lower bounds for the size of MR refutations of the PHP will give exponential lower bounds for the size of DLR refutations of the PHP.

In the next section we study lower bounds for the PHP in MR

Lower bounds for PHP In daglike Resolution

Main theorem

Th[BP96]. Any monotone Resolution refutation of PHP[$n+1, n$] requires $2^{n/20}$ many clauses

Critical Truth Assignments

Assignments to $p_{i,j}$'s defining 1-1 mapping from pigeons to holes.

- every pigeon is sent to at most one hole
- no two pigeons are sent to the same hole

Critical Truth Assignments

Consider the PHP[5,4] a 5-cta

		pigeons				
		1	2	3	4	5
holes	1	0	1	0	0	0
	2	1	0	0	0	0
	3	0	0	1	0	0
	4	0	0	0	1	0

Property: Exactly one initial clause of PHP is falsified

$$p_{5,1} \vee p_{5,2} \vee p_{5,3} \vee p_{5,4}$$

Notation: *i*-cta if column *i* in the matrix is all 0's or falsifies

$$\text{initial clause } p_{i,1} \vee p_{i,2} \vee \dots \vee p_{i,n}$$

Proof Idea

1. Assume to have a short MR refutation P of $\text{PHP}[n, n-1]$.
2. Identifies **LARGE CLAUSES** in P as those having approx n^2 variables
3. **Killing Process:** Hit the proof P with a simplification process (assigning a partial cta α) that at each step delete many wide clauses from the proof, but leave $P[\alpha]$ yet a proof of a simplified $\text{PHP}[n', n'-1]$ with $n' < n$.
4. **Forcing Prop.** Prove that any proof of the $\text{PHP}[n, n-1]$ contains a **moderately LARGE clause**
5. Argue that If P is short, it contains few LARGE clauses, and hence the simplifications process deletes too fast LARGE clauses contradicting (4).

Killing Large clauses - I

Defn

LARGE clauses are those with $n^2/10$ literals

Let P be a MR refutation of $\text{PHP}[n, n-1]$ with less than S LARGE clauses

Claim. There is a variable that appears in at least $S/10$ LARGE Clauses

Proof.

$$\frac{\#(\text{large clauses}) * \text{size}(\text{large clause})}{\#(\text{variables})} = \frac{S * n^2 / 10}{n(n-1)} \geq \frac{S}{10}$$

Killing Large clauses - II

Defn Assignment

Pick $p_{i,j}$ appearing in at least $S/10$ large clause.

$$\alpha = \begin{cases} p_{i,j} = 1 \\ p_{i,k} = 0 & k \neq j \\ p_{l,j} = 0 & l \neq i \end{cases}$$

		pigeons				
		1	...	i	...	n
holes	1			0		
	...			0		
	j	0	0	1	0	0
	...			0		
	n-1			0		

Claim [Exercise 3]

$P[\alpha]$ is a proof of $\text{PHP}[n-1, n-2]$ with at most $9S/10$ Large Clauses

Killing Large clauses - III

Saturating the Process

Apply previous simplification process x times, up to delete all large clauses and be left with a MR refutation of $\text{PHP}[n-x, n-x-1]$.

Computing x

$$S(1 - \frac{1}{10})^x < 1 \Rightarrow x = \log_{\frac{10}{9}} S$$

Forcing Lemma & Contradiction

Forcing Lemma

Any MR refutation of $\text{PHP}[n, n-1]$ contains a clause with $n^2/9$ variables.

Getting the Contradiction

$S < 2^{n/10}$. By Forcing Lemma applied on $\text{PHP}[n-x, n-x-1]$ for $x = \log_{\frac{10}{9}} S$ we get

$$2(n - \log_{\frac{10}{9}} S)^2 \stackrel{S < 2^{n/10}}{>} 2(0.5n^2)/9 \geq n^2/10$$

This contradicts the fact that after $x = \log_{\frac{10}{9}} S$ steps we have eliminated all the large clauses.

Proof of Forcing Lemma

Idea

- We introduce a complexity measure μ on clauses.
- We prove that there exists a clause K with high measure
- We prove that K contains the required number of variables

Definition of μ

Notation $R \subseteq [n]$, $\wedge R$ clauses of PHP with pigeons in R
 C a clause in the proof

$R \xRightarrow{cta} C$ If every cta that satisfies $\wedge R$ also satisfies C

Defn $\mu(C)$

C a clause in the proof.

I_C be the **minimal subset** of $[n]$ s.t. $I_C \xRightarrow{cta} C$

$\mu(C) = |I_C|$

Properties of μ

Properties of $\mu(C)$ [Exercise 4]

1. $\mu(C)=1$ if $C \in \text{PHP}$
2. $\mu([\])=n$
3. $\frac{A \quad B}{C}$ then $\mu(C) \leq \mu(A) + \mu(B)$
4. (1)+(2)+(3) $\Rightarrow \exists K$ s.t. $n/3 \leq \mu(K) \leq 2n/3$

K is a large clause

Claim K contains $n^2/9$ variables

Proof. By Prop it follows $n/3 \leq |I_K| \leq 2n/3$

Let $L_K = [n] - I_K$. Then $n/3 \leq |L_K| \leq 2n/3$

Let $i \in I_K$ and let α be a i -cta. Let $j \in L_K$

Swap α in β

α i -cta

	1	...	i	...	j	...	n
1			0		0		
...			0		0		
i	0	0	0	0	1	0	0
...			0		0		
$n-1$			0		0		

β j -cta

	1	...	i	...	j	...	n
1			0		0		
...			0		0		
i	0	0	1	0	0	0	0
...			0		0		
$n-1$			0		0		

Since $j \notin I_K$ then β satisfies K. hence $p_{i,i} \in K$

Claim follows since $|I_K| * |L_K| \geq n^2/9$

The Width Method: Short proofs are narrow

Width definitions

Restrictions [Exercise 5] understand what rules add to Resolution in such a way to keep the system consistent with application of restrictions to proofs

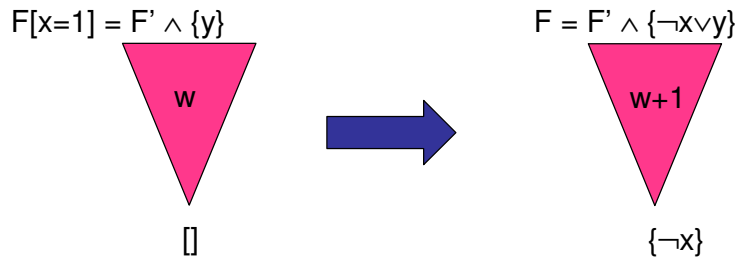
Notation

$F \xrightarrow{w} C$ means there is Resolution refutation of C from F of width w

Width properties

Prop 1 If $F[x=1] \xrightarrow{w} []$ then $F \xrightarrow{w+1} \neg x$

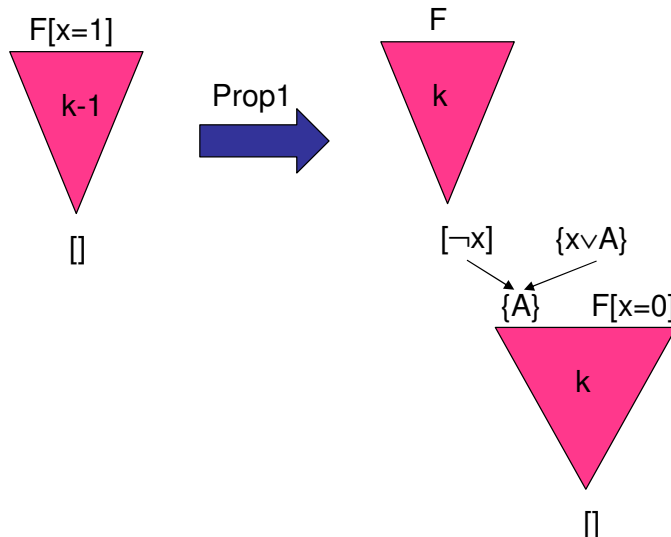
Proof. $F = F' \wedge \{\neg x \vee y\}$ and F' not contain x or $\neg x$



Width properties

Prop2 If $F[x=1] \xrightarrow{k-1} []$ and $F[x=0] \xrightarrow{k} []$, then $w_R(F) \leq \max(k, w(F^x))$
 where F^x is the set of clauses of F containing x

Proof. Assume f.i. that $F^x = \{x \vee A\}$



Short proofs are narrow: TLR

Thm $w_R(F) \leq w(F) + \log S_{TLR}(F)$

Proof. Prove that $S_{TLR}(F) \leq 2^b \Rightarrow w_R(F) \leq w(F) + b$

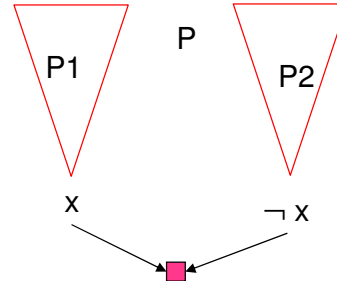
By induction on b and n . $b=0$ OK! Assume wlog $|P1| \leq |P|/2$.

By induction on b

$$w_R(F[x=0]) \leq w(F) + b - 1$$

By induction on n

$$w_R(F[x=1]) \leq w(F) + b$$



$|P| = |P1| + |P2| + 1$. The claim follows from Prop 2

Cor. $S_{TLR}(F) \geq 2^{(w_R(F) - w(F))}$

Short proofs are narrow: DLR

Thm $w_R(F) \leq w(F) + O(\sqrt{n \ln S_{DLR}(F)})$

Proof. Let P be a minimal size DLR refutations for F of size S .

Set “clause largeness” $d = \lfloor \sqrt{2n \ln S_{DLR}(F)} \rfloor$

$$a = \left(1 - \frac{d}{2n}\right)^{-1}$$

Let $P^L \subseteq P$ the set of “large clauses”. Prove induction on b and n that

$$|P^L| \leq a^b \Rightarrow w_R(F) \leq d + w(F) + b$$

Short proofs are narrow: DLR

Argue [Exercise 7]

$$F[x = 1] \xrightarrow{d+w(F)+b-1} [\]$$

$$F[x = 0] \xrightarrow{d+w(F)+b} [\]$$

Claim follows from Prop2

Cor. $S_{DLR}(F) \geq \exp\left(\frac{(w_R(F) - w(F))^2}{n}\right)$

Limitations and optimality

Thm [BG00] The sizewidth tradeoffs for DLR is optimal

Proof. Use a formula F over $O(n^2)$ variables and with bounded initial width and prove that

1. $S_{DLR} \leq nO(1)$
2. $w_R(F) \geq n$
3. $w(F) \leq O(1)$

Width proof search

An algorithm to produce a DLR refutation of a UNSAT formula A in CNF

$\text{Res}_k(A) = \{C : w(C) \leq k \text{ and } C \text{ is resolvent of two clauses in } S\}$

1. $k=1$
2. Repeat
3. $S = \text{Res}_k(S)$
4. $k = k+1$
5. While ($\square \notin S$)
6. Output($\square \in S$)

Running Time. On UNSAT F over n variables
The algorithm runs in time $n^{O(w_R(F))}$

Width Lower bounds: general framework

Given an UNSAT F , define a complexity measure on clauses μ_F s.t.

1. $\mu_F(\text{Axioms}) \leq 1$
2. $\mu_F(\square) \geq \text{“large”}$
3. μ_F is subadditive, i.e. $\frac{A \quad B}{C} \quad \mu_F(C) \leq \mu_F(A) + \mu_F(B)$
4. (1)+(2)+(3) \Rightarrow there is a clause K of “medium” measure $\mu_F(K)$
5. Argue that “medium” complexity implies “large” width

Lower bounds for Tseitin Tautologies

Tseitin Tautologies

Let $G=(V,E)$ be a connected graph. Let $m:V\rightarrow\{0,1\}$ a labelling of the nodes of V s.t. $\sum_{v\in V} m(v) \equiv 1(\text{mod } 2)$

Assign a variable x_e to each edge e in G .

For a node v in V $PARITY(v) = \bigoplus_{v\in e} x_e \equiv m(v)(\text{mod } 2)$

$$T(G,m) =_{def} \bigwedge_{v\in V} PARITY(v)$$

[Exercise 6] Take a small graph and build Tseitin formula on it

Expander Graphs

We will apply the $T(G,m)$ formulas on a graph G which is a good expander and we will show that the width of refuting $T(G,m)$ is lower bounded by the expansion of G

Expansion

G a connected graph the

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

Thm There are 3-regular graphs $G=(V,E)$ with expansion

$$e(G) = \Omega(|V|)$$

Define the measure

$$A_v = \bigwedge_{v \in V} \text{PARITY}(v)$$
$$V' \subseteq V, \partial V' = \{x_e : e \in E(V', V-V')\}$$

A v -cta for $T(G,m)$ is an assignment which falsifies only $\text{PARITY}(v)$ and satisfies all the other $\text{PARITY}(v')$
[Exercise 8: prove it exists]

For C clause let $V_C = \min V' \subseteq V$ s.t. $A_{V'} \Rightarrow C$ under ctas

$$\mu(C) = |V_C|$$

Verifying the measure

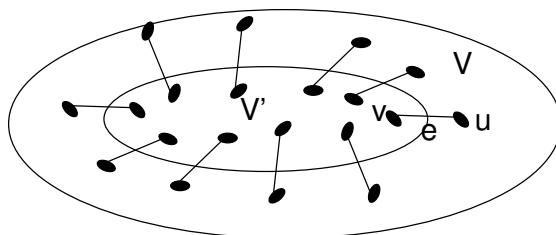
1. C an Axiom, $\mu(C)=1$ easy: C is in $\text{PARITY}(v)$ for some v
2. $\mu([\])=|V|$. [Exercise 9: Prove that for any $|V'| < |V|$, $A_{V'}$ is SAT)
3. Take the complex clause K having

$$|V|/3 \leq \mu(K) = 2|V|/3.$$
 Let V_K be the subset of V witnessing K
4. [Forcing] We prove that each variable in ∂V_K belongs to C
5. The result follows since $|\partial V_K| \geq e(G)$ (by def of $e(G)$)

Forcing

V_K is the minimal set implying K under ctas.

Assume that there is $x_e \in \partial V_K$ s.t $x_e \notin C$



Let α s.t. $A_{V_K}[\alpha]=1$ and $C[\alpha]=1$.

Form β from α setting $x_e=0$ and keeping that β is a cta

$A_{V_K - \{v\}}[\beta]=1$ and $C[\beta]=1$.

Contradictions with minimality of V_K

Lower bounds for Random k-CNF

Preliminary Definitions

Dfn. A literal l is **pure in a set of clauses** F if l appears in F but no clause of F contains $\neg l$

Dfn. A set of clauses F over n variables is **1-sparse** if $|F| \leq n$

Properties. For $s \geq 1$ and $0 < \epsilon < 1$.

- $A(s)$ iff every set of $r \leq s$ clauses is 1-sparse
- $B_\epsilon(s)$ iff every set of r clauses, $s/2 < r \leq s$, has at least ϵr pure literals

Preliminary Definitions

Dfn. A literal l is **pure in a set of clauses** F if l appears in F but no clause of F contains $\neg l$

Dfn. A set of clauses F over n variables is **1-sparse** if $|F| \leq n$

Properties. For $s \geq 1$ and $0 < \varepsilon < 1$.

- $A(s)$ iff every set of $r \leq s$ clauses is 1-sparse
- $B_\varepsilon(s)$ iff every set of r clauses, $s/2 < r \leq s$, has at least εr pure literals

Properties for Random Formulas

Thm [CS,BSW,BKPS]

Let F be a random k -CNF over n variables and Δn clauses, $\varepsilon > 0$. If $s = O\left(\frac{n}{\Delta^{2/(k-2-\varepsilon)}}\right)$, then w.h.p property $A(s)$ and $B_\varepsilon(s)$ both hold.

Proof

Relatively elementary probability and counting. See [BKPS]

Assumption

From now on we assume to have for F both $A(s)$ and $B_\varepsilon(s)$.

Define the measure

Let P be DLR refutations of a random k -CNF F .

$$\mu(C) = \min I \subseteq F. \text{ s.t. } I \rightarrow C$$

Prop1 μ is sub-additive

Prop2 $C \in F \rightarrow \mu(C) \leq 1$

Prop3 $\mu(\{\}) > s$.

If a subset of F is 1-sparse then is satisfiable

[Exercise: hint Hall theorem]. Then property $A(s)$ implies $\mu(\{\}) > s$.

Prop4. There exists a clause K such that $s/2 < \mu(C) \leq s$.

Choose the first clause in P with $\mu(C) > s/2$. By sub-additivity get $\mu(C) \leq s$.

High complexity implies high width

Lemma. $w(K) \geq \epsilon s/2$

Proof.

$\mu(K) \geq s/2$, hence the minimal subset of F implying K has size at least $s/2$.

Claim

If S minimally implies K and I is pure in S , then $I \in C$.

[Exercise]

Lemma follows from property $B_\epsilon(s)$.

Weak PHP: pseudowidth

Weak PHP

The width method does not work for PHP[m,n] when $m \geq n^2 / \log n$

It was a big problem to understand the exact complexity of such a PHP

[Raz 02] Proved that it is hard for Resolution

[Razborov,03-05] Introduced a measure that generalize the width, called pseudowidth and prove Raz Result and extend it to weaker form of Weak PHP

Weak PHP

Pseudowidth.

Let $i \in [m]$ and let C a clause

$$J_C(i) = \{j \in [n] : p_{i,j} \in C\}$$

Consider a vector of pigeons threshold $\mathbf{d} = (d_1, \dots, d_m)$

$$pw_{\mathbf{d}}(C) = \{i \in [m] : |J_C(i)| \geq d_i\}$$

Thm Short proofs of PHP $[m, n]$ have small pseudowidth

Thm PHP $[m, n]$ requires high pseudowidth

Open Problems

Apply and define pseudowidth to other examples of formulas.

For instance

- Exact complexity of Ramsey formulas is not known in Resolution.
- Try to get stronger DLR lower bounds for random formulas (f.i. for a great density)