Resolution Lower Bounds for Refutation Statements

Michal Garlík
Polytechnic University of Catalonia

Banff, Jan 19 - 24, 2020

Outline and results

$\mathrm{REF}^{F}_{\mathrm{Res},v}$ ... propositional formula expressing that a CNF F has a resolution refutation of length v. Unary encoding is used.

Outline and results

$\mathrm{REF}^F_{\mathrm{Res},v}$ ... propositional formula expressing that a CNF F has a resolution refutation of length v. Unary encoding is used.

- An exponential lower bound (2^{v^δ}) on the size of resolution refutations of $\mathrm{REF}^F_{\mathrm{Res},v}$ for any unsatisfiable F (and any v greater than a fixed small polynomial in the size of F).

Outline and results

$\mathrm{REF}^F_{\mathrm{Res},v}$ ... propositional formula expressing that a CNF F has a resolution refutation of length v. Unary encoding is used.

- An exponential lower bound (2^{v^δ}) on the size of resolution refutations of $\mathrm{REF}^F_{\mathrm{Res},v}$ for any unsatisfiable F (and any v greater than a fixed small polynomial in the size of F).
- An exponential lower bound on the size of resolution refutations of $\mathrm{SAT}^{n,r} \wedge \mathrm{REF}^F_{\mathrm{Res},v}$ (negation of the reflection principle for resolution).

Outline and results

$\mathrm{REF}^{F}_{\mathrm{Res},v}$ ... propositional formula expressing that a CNF F has a resolution refutation of length v. Unary encoding is used.

- An exponential lower bound ($2^{v^{\delta}}$) on the size of resolution refutations of $\mathrm{REF}^{F}_{\mathrm{Res},v}$ for any unsatisfiable F (and any v greater than a fixed small polynomial in the size of F).
- An exponential lower bound on the size of resolution refutations of $\mathrm{SAT}^{n,r} \wedge \mathrm{REF}^{F}_{\mathrm{Res},v}$ (negation of the reflection principle for resolution).
- New examples of CNFs exponentially separating Res(2) from resolution.

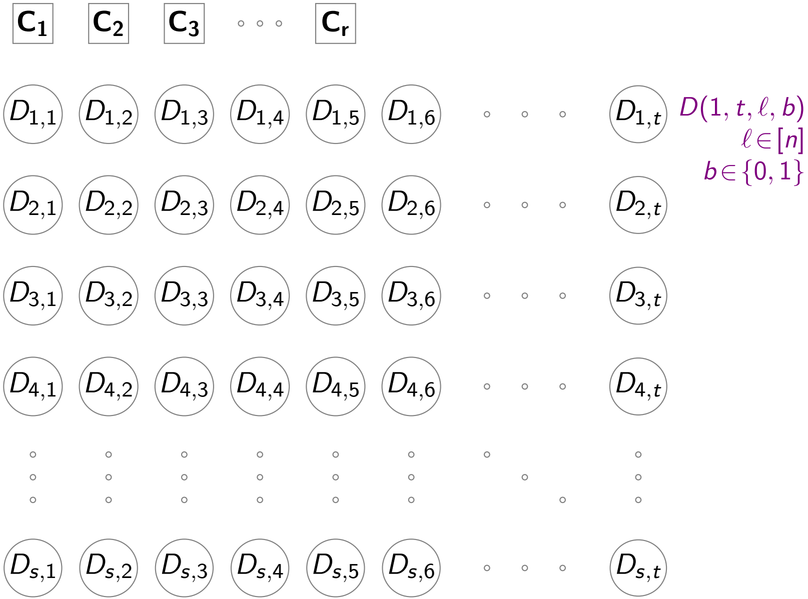
Outline and results

$\mathrm{REF}^F_{\mathrm{Res},v}$ ... propositional formula expressing that a CNF F has a resolution refutation of length v. Unary encoding is used.

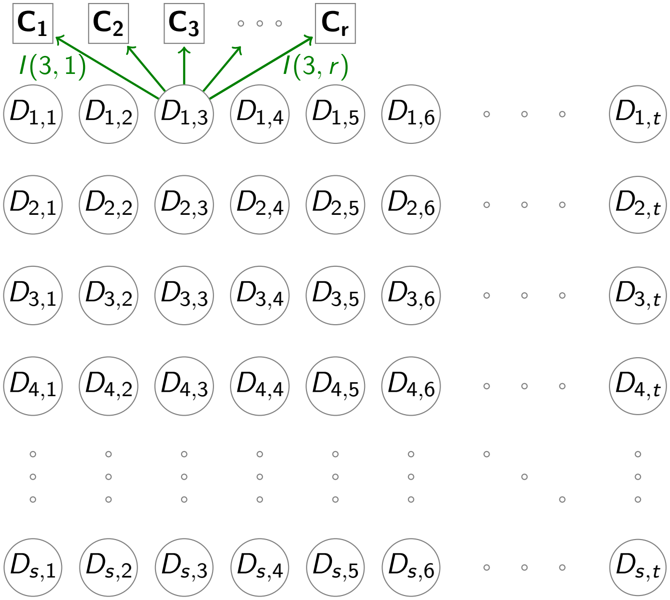
- An exponential lower bound (2^{v^δ}) on the size of resolution refutations of $\mathrm{REF}^F_{\mathrm{Res},v}$ for any unsatisfiable F (and any v greater than a fixed small polynomial in the size of F).
- An exponential lower bound on the size of resolution refutations of $\mathrm{SAT}^{n,r} \wedge \mathrm{REF}^F_{\mathrm{Res},v}$ (negation of the reflection principle for resolution).
- New examples of CNFs exponentially separating Res(2) from resolution.

We first assign some variables in $\mathrm{REF}^F_{\mathrm{Res},v}$ to obtain its layered version $\mathrm{REF}^F_{s,t}$ with s levels of t clauses.

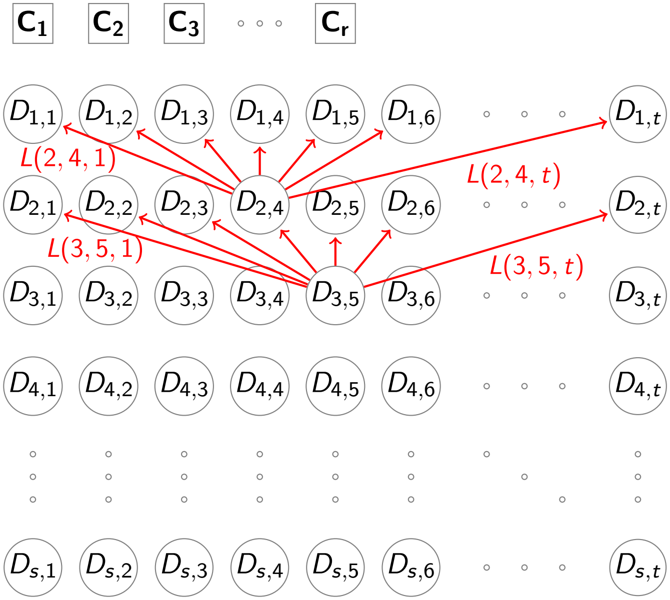
$\boxed{\mathbf{C_1}}$ $\boxed{\mathbf{C_2}}$ $\boxed{\mathbf{C_3}}$ ∘ ∘ ∘ $\boxed{\mathbf{C_r}}$ (clauses of F)



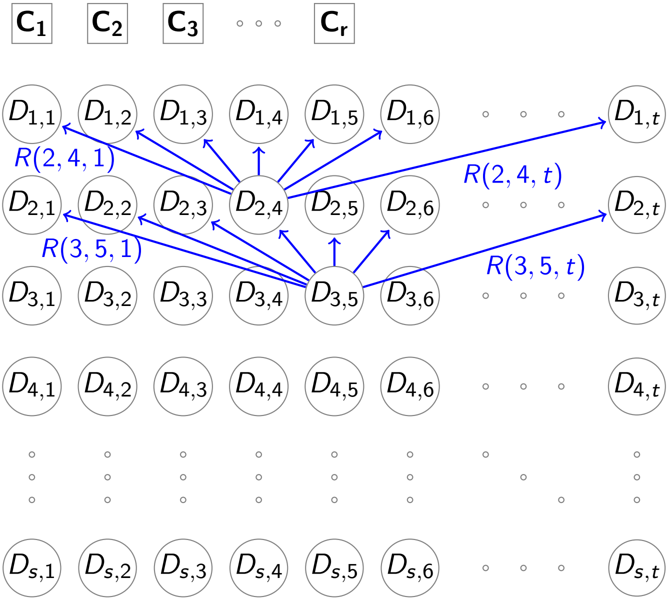
C1 C2 C3 Cr
D1,1 D1,2 D1,3 D1,4 D1,5 D1,6 D1,t
D(1, t, ℓ, b)
ℓ ∈ [n]
b ∈ {0, 1}
D2,1 D2,2 D2,3 D2,4 D2,5 D2,6 D2,t
D3,1 D3,2 D3,3 D3,4 D3,5 D3,6 D3,t
D4,1 D4,2 D4,3 D4,4 D4,5 D4,6 D4,t
Ds,1 Ds,2 Ds,3 Ds,4 Ds,5 Ds,6 Ds,t



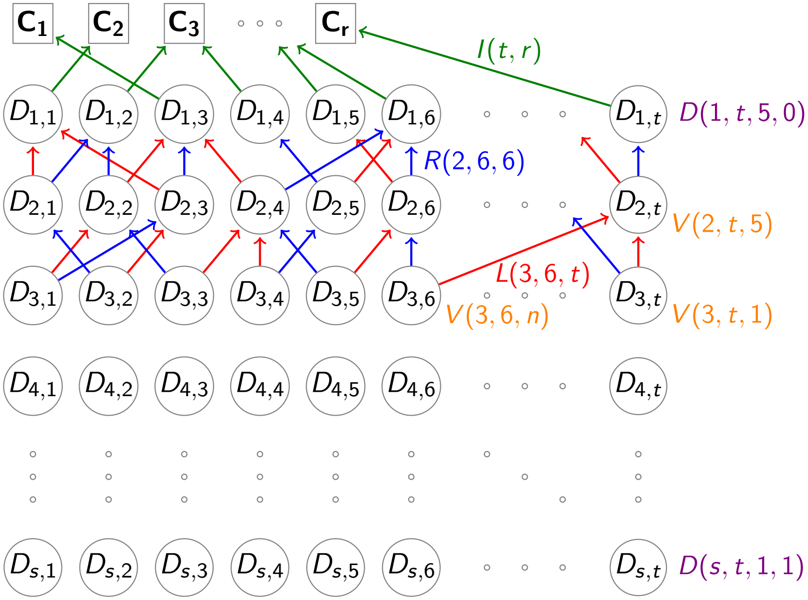
C1
C2
C3
Cr
I(3, 1)
I(3, r)
D1,1 D1,2 D1,3 D1,4 D1,5 D1,6 D1,t
D2,1 D2,2 D2,3 D2,4 D2,5 D2,6 D2,t
D3,1 D3,2 D3,3 D3,4 D3,5 D3,6 D3,t
D4,1 D4,2 D4,3 D4,4 D4,5 D4,6 D4,t
Ds,1 Ds,2 Ds,3 Ds,4 Ds,5 Ds,6 Ds,t



C_1
C_2
C_3
C_r
$D_{1,1}$ $D_{1,2}$ $D_{1,3}$ $D_{1,4}$ $D_{1,5}$ $D_{1,6}$ $D_{1,t}$
$L(2,4,1)$
$L(2,4,t)$
$D_{2,1}$ $D_{2,2}$ $D_{2,3}$ $D_{2,4}$ $D_{2,5}$ $D_{2,6}$ $D_{2,t}$
$L(3,5,1)$
$L(3,5,t)$
$D_{3,1}$ $D_{3,2}$ $D_{3,3}$ $D_{3,4}$ $D_{3,5}$ $D_{3,6}$ $D_{3,t}$
$D_{4,1}$ $D_{4,2}$ $D_{4,3}$ $D_{4,4}$ $D_{4,5}$ $D_{4,6}$ $D_{4,t}$
$D_{s,1}$ $D_{s,2}$ $D_{s,3}$ $D_{s,4}$ $D_{s,5}$ $D_{s,6}$ $D_{s,t}$


C1
C2
C3
Cr
D1,1 D1,2 D1,3 D1,4 D1,5 D1,6 D1,t
D2,1 D2,2 D2,3 D2,4 D2,5 D2,6 D2,t
D3,1 D3,2 D3,3 D3,4 D3,5 D3,6 D3,t
D4,1 D4,2 D4,3 D4,4 D4,5 D4,6 D4,t
Ds,1 Ds,2 Ds,3 Ds,4 Ds,5 Ds,6 Ds,t
R(2, 4, 1)
R(2, 4, t)
R(3, 5, 1)
R(3, 5, t)

C_1 C_2 C_3 … C_r
$D_{1,1}$ $D_{1,2}$ $D_{1,3}$ $D_{1,4}$ $D_{1,5}$ $D_{1,6}$ … $D_{1,t}$
$D_{2,1}$ $D_{2,2}$ $D_{2,3}$ $D_{2,4}$ $D_{2,5}$ $D_{2,6}$ … $D_{2,t}$
$V(2, t, \ell)$
$\ell \in [n]$
$D_{3,1}$ $D_{3,2}$ $D_{3,3}$ $D_{3,4}$ $D_{3,5}$ $D_{3,6}$ … $D_{3,t}$
$V(3, 6, \ell')$
$\ell' \in [n]$
$D_{4,1}$ $D_{4,2}$ $D_{4,3}$ $D_{4,4}$ $D_{4,5}$ $D_{4,6}$ … $D_{4,t}$
$D_{s,1}$ $D_{s,2}$ $D_{s,3}$ $D_{s,4}$ $D_{s,5}$ $D_{s,6}$ … $D_{s,t}$



C1
C2
C3
Cr
I(t, r)
D(1, t, 5, 0)
R(2, 6, 6)
V(2, t, 5)
L(3, 6, t)
V(3, 6, n)
V(3, t, 1)
D(s, t, 1, 1)

Writing down the propositional formula $\mathrm{REF}^F_{s,t}$

$$\neg D(s,t,\ell,b) \qquad \ell \in [n], b \in \{0,1\}$$

Clause $D_{s,t}$ is empty.

Writing down the propositional formula $\mathrm{REF}^F_{s,t}$

$$\neg D(s,t,\ell,b) \qquad \ell\in[n], b\in\{0,1\}$$

Clause $D_{s,t}$ is empty.

$$\neg L(i,j,j') \lor \neg V(i,j,\ell) \lor D(i-1,j',\ell,1)$$
$$i\in[s]\setminus\{1\}, j,j'\in[t], \ell\in[n]$$

Clause $D_{i-1,j'}$ used as the premise given by $L(i,j,j')$ to derive $D_{i,j}$ by resolving on x_ℓ must contain the literal x_ℓ.

And so on...

The main result

- An exponential lower bound on the size of resolution refutations of $\mathrm{REF}^F_{s,t}$ for any unsatisfiable F.

Theorem

For each $\epsilon > 0$ there is $\delta > 0$ and an integer t_0 such that if n, r, s, t are integers satisfying $t \geq s \geq n+1$, $r \geq n \geq 2$, $t \geq r^{3+\epsilon}$, $t \geq t_0$, and F is an unsatisfiable CNF consisting of r clauses $C_1, \ldots, C_r$ in n variables $x_1, \ldots, x_n$, then any resolution refutation of $\mathrm{REF}^F_{s,t}$ has length greater than 2^{t^δ}.

High-level proof sketch

- Proof by contradiction: Assume there is $\epsilon > 0$ s.t. for all δ and t_0 there are n, r, s, t, F satisfying the conditions of the Theorem and there is a refutation Π of $\mathrm{REF}^F_{s,t}$ with $|\Pi| < 2^{t^\delta}$.
- Find suitable δ and t_0, and prove a contradiction in two steps:

1. Apply a random restriction ρ to obtain $\Pi \restriction \rho$ with small "width": ρ satisfies all "wide" clauses of Π w.h.p.
2. Use an adversary argument to show that small "width" refutations of $\mathrm{REF}^F_{s,t} \restriction \rho$ don't exist.

Proof ingredients: important pairs

- Usual notions of width (or block-width or index-width) don't work: the restriction ρ has to respect *functionality* (e.g. $L(i,j,1) \vee \ldots \vee L(i,j,t)$ together with $\neg L(i,j,j') \vee \neg L(i,j,j''), j' \neq j''$), and so setting $L(i,j,\cdot)$ at random satisfies a single positive literal with too small probability $(1/t)$.

Proof ingredients: important pairs

- Usual notions of width (or block-width or index-width) don't work: the restriction ρ has to respect *functionality* (e.g. $L(i,j,1) \vee \ldots \vee L(i,j,t)$ together with $\neg L(i,j,j') \vee \neg L(i,j,j''), j' \neq j''$), and so setting $L(i,j,\cdot)$ at random satisfies a single positive literal with too small probability $(1/t)$.
- However, the probability of satisfying a single negative literal is very good $((t-1)/t)$. This motivates:

Definition

We say that (i,j) is *L-important* in a clause E of Π if E contains a negative literal of a variable in $L(i,j,\cdot)$ or if E contains at least $t/2$ positive literals of variables in $L(i,j,\cdot)$.

Proof ingredients: random restrictions

Set $p = t^{-a}$ with $a = \min\{\frac{2+\epsilon/2}{3+\epsilon/2}, \frac{3}{4}\}$, and define a random restriction ρ by the following experiment:

1. For each pair $(i, j) \in [s] \times [t]$, with indep. prob. p include (i, j) in a set A_D. Then for each $(i, j) \in A_D$, independently, sample a complete clause $D_{i,j}$
2. For each $j \in [t]$, with independent probability p include the pair $(1, j)$ in a set A_I. Then for each $(1, j) \in A_I \setminus A_D$, independently, choose at random $m \in [r]$ and set $I(j, \cdot)$ to m.
3. For each pair $(i, j) \in \{2, \ldots, s\} \times [t]$, with independent probability p include (i, j) in a set A_V. Then for each $(i, j) \in A_V$, independently, choose at random $\ell \in [n]$ and set $V(i, j, \cdot)$ to ℓ.
4. For each pair $(i, j) \in \{2, \ldots, s\} \times [t]$, with independent probability p include the pair (i, j) in a set A_{RL}. Then, for each $i \in \{2, \ldots, s\}$, sample a random 1:2 injection to level $i - 1$. Set $L(i, j, \cdot)$ and $R(i, j, \cdot)$ accordingly.

Proof ingredients: properties of ρ

Lemma

Each of A_{RL}, A_D, A_I, A_V contains $< 2pt$ index pairs on each level w.h.p.

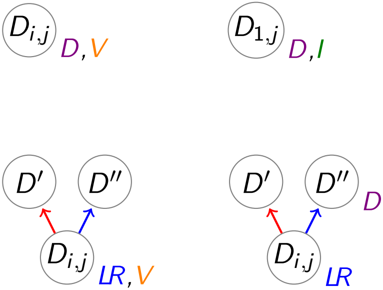
Proof ingredients: properties of ρ

Lemma

Each of A_{RL}, A_D, A_I, A_V contains $< 2pt$ index pairs on each level w.h.p.

Lemma

W.h.p., ρ does not create "worse" connected components then the following:



ρ simplifies clauses of Π

Lemma

W.h.p. for every clause E in $\Pi \restriction \rho$ and every $Z \in \{D, V, I, L, R\}$, the number of Z-important pairs in E is $< w := t^{4/5}$.

Adversary argument

- We run the adversary argument with "admissible" extensions of ρ, which are partial assignments satisfying certain closure properties.
- We start the adversary argument at the empty clause of $\Pi \restriction \rho$ with the minimal "admissible" extension $\sigma_\emptyset$ of ρ, and we inductively build a path going from a clause to one of its premises, following certain rules and modifying our admissible assignment.
- We show that for each clause E we visit in $\Pi \restriction \rho$, the current admissible assignment σ_E satisfies the following:
  1. σ_E assigns all variables in E with important indices,
  2. whenever σ_E evaluates a variable with a literal in E, it falsifies that literal.

Adversary argument

- We show that because the "width" of clauses E in $\Pi \restriction \rho$ is small, every new σ_E can be found such that it never falsifies an axiom of $\mathrm{REF}^F_{s,t}$.
- Consider the case when the resolved variable is $L(i,j,j')$ and it is not set by σ_E. At each level, σ_E touches few index-pairs: ρ touches $O(pt)$ pairs and $\sigma_E \setminus \rho$ touches $O(w)$ (due to the small "width" of E).
- Also, we must avoid satisfying any of the variables $L(i,j,j'')$ which may be present in E. But there is at most at most $t/2$ of them in E, since (i,j) is not L-important (otherwise $L(i,j,j')$ would be already set)
- We still have $O(pt+w)+t/2<t$ untouched possibilities where to map $L(i,j,\cdot)$, which makes it easy not to falsify any axiom of $\mathrm{REF}^F_{s,t}$.

Thank you!