SETH and Resolution

Ilario Bonacina

January 23, 2020

This talk: what are the strongest possible resolution size lower bounds?

2 open problems

1 proof sketch

Resolution (notations)

$$\frac{C \vee x \qquad D \vee \neg x}{C \vee D}$$

- $w(F)$: width needed to refute the CNF formula F in resolution
- $S(F)$, $S_{tree}(F)$, $S_{reg}(F)$: size needed to refute F in general, treelike and regular resolution resp.

F unsatiafiable k-CNF in n variables

$S(F) \geqslant 2^{n^\delta}$ for some $0 < \delta < 1$?

F unsatiafiable k-CNF in n variables

$S(F) \geqslant 2^{n^\delta}$ for some $0 < \delta < 1$?

E.g. for F the pigeonhole principle, reflection principle, mutilated chessboard, coloring principle...

F unsatiafiable k-CNF in n variables

$S(F) \geqslant 2^{n^\delta}$ for some $0 < \delta < 1$?

E.g. for F the pigeonhole principle, reflection principle, mutilated chessboard, coloring principle...

$S(F) \geqslant 2^{n/c}$ for some $c > 1$?

F unsatiafiable k-CNF in n variables

$S(F) \geqslant 2^{n^\delta}$ for some $0 < \delta < 1$?
E.g. for F the pigeonhole principle, reflection principle, mutilated chessboard, coloring principle...

$S(F) \geqslant 2^{n/c}$ for some $c > 1$?
E.g. for F random 3-CNFs, random 3-XOR, Tseitin, graph-pigeonhole principle...

F unsatiafiable k-CNF in n variables

$S(F) \geqslant 2^{n^\delta}$ for some $0 < \delta < 1$?

E.g. for F the pigeonhole principle, reflection principle, mutilated chessboard, coloring principle...

$S(F) \geqslant 2^{n/c}$ for some $c > 1$?

E.g. for F random 3-CNFs, random 3-XOR, Tseitin, graph-pigeonhole principle...

$S(F) = 2^n$?

F unsatiafiable k-CNF in n variables

$S(F) \geqslant 2^{n^\delta}$ for some $0 < \delta < 1$?

E.g. for F the pigeonhole principle, reflection principle, mutilated chessboard, coloring principle...

$S(F) \geqslant 2^{n/c}$ for some $c > 1$?

E.g. for F random 3-CNFs, random 3-XOR, Tseitin, graph-pigeonhole principle...

$S(F) = 2^{n}$?

None!

Thm

For every unsatisfiable k-CNF F_n in n variables

$$S_{tree}(F_n) \leqslant 2^{n(1-\sigma_k)},$$

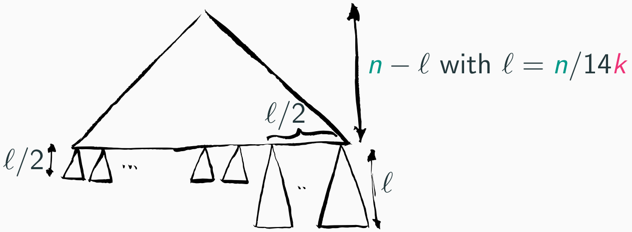
where $\sigma_k = \frac{1}{28k}$.

Thm

For every unsatisfiable k-CNF F_n in n variables

$$S_{tree}(F_n) \leqslant 2^{n(1-\sigma_k)},$$

where $\sigma_k = \frac{1}{28k}$.



Open problem 1

Show there are unsatisfiable k-CNF formulas F_n in n variables s.t.

$$S(F_n) \geqslant 2^{n(1-\sigma_k)},$$

where $\sigma_k \xrightarrow{k \to +\infty} 0$ (maybe $\sigma_k = \mathcal{O}(k^{-1})$?).

Open Problem 1 $\Rightarrow$ no CDCL solver can refute SETH, since resolution refutations $\equiv$ CDCL solvers execution traces

Open problem 1

Show there are unsatisfiable k-CNF formulas F_n in n variables s.t.

$$S(F_n) \geqslant 2^{n(1-\sigma_k)},$$

where $\sigma_k \xrightarrow{k\to+\infty} 0$ (maybe $\sigma_k = \mathcal{O}(k^{-1})$?).

Open Problem 1 $\Rightarrow$ no CDCL solver can refute SETH, since resolution refutations $\equiv$ CDCL solvers execution traces

Open problem 2

Show that for every unsatisfiable k-CNF formula F_n in n variables

$$S(F_n) \geqslant 2^{(w(F_n)-k)^2/n}.$$

I.e. remove the "Ω" from the size-width inequality

S_{tree}(random k-CNF) $\leqslant 2^{n/c}$ for some $c < 1$ [follows from BKPS'98]

(same u.b. for random k-XOR)

S_{tree}(Tseitin formulas) $\leqslant 2^{n/c}$ for some constant $c < 1$ [KRT'19?]

S_{tree}(random k-CNF) $\leqslant 2^{n/c}$ for some $c < 1$ [follows from BKPS'98]

(same u.b. for random k-XOR)

S_{tree}(Tseitin formulas) $\leqslant 2^{n/c}$ for some constant $c < 1$ [KRT'19?]

Size-width Inequality

For every unsatisfiable k-CNF formula F_n in n variables

$$S(F_n) \geqslant 2^{\Omega((w(F_n)-k)^2/n)}$$

Unfortunately the Ω-notation is hiding a constant $c < 1/5$.

S_{tree}(random k-CNF) $\leqslant 2^{n/c}$ for some $c < 1$ [follows from BKPS'98]

(same u.b. for random k-XOR)

S_{tree}(Tseitin formulas) $\leqslant 2^{n/c}$ for some constant $c < 1$ [KRT'19?]

Size-width Inequality

For every unsatisfiable k-CNF formula F_n in n variables

$$S(F_n) \geqslant 2^{\Omega((w(F_n)-k)^2/n)}$$

Unfortunately the Ω-notation is hiding a constant $c < 1/5$.

XOR-ifications

For every unsatisfiable k-CNF F, $S(F[\oplus^2]) \geqslant 2^{\Omega(w(F)-k)}$

F unsatisfiable k-CNF in n vars (a different formula in all the l.b. below...)

$S_{tree}(F) \geqslant 2^{n(1-\sigma_k)}$ with $\sigma_k = \widetilde{\mathcal{O}}(k^{-1/8})$ [PI'00]

$S_{reg}(F) \geqslant 2^{n(1-\sigma_k)}$ with $\sigma_k = \widetilde{\mathcal{O}}(k^{-1/4})$ [BI'13]

$S_{\delta\text{-}reg}(F) \geqslant 2^{n(1-\sigma_k)}$ with σ_k and δ both $\widetilde{\mathcal{O}}(k^{-1/4})$ [**B**T'16]

$S(F) \geqslant 2^{0.585 \cdot n(1-\sigma_k)}$ with $\sigma_k = \widetilde{\mathcal{O}}(k^{-1/3})$ [BI'13,**B**T'16]

A strong width l.b.

Thm (BI'13)

For large n and k there are unsatisfiable k-CNF formulas Ψ_n

$$w(\Psi_n) \geqslant n(1 - \sigma_k)\,,$$

where $\sigma_k = \widetilde{\mathcal{O}}(k^{-1/4})$.
(We can actually get $\sigma_k = \widetilde{\mathcal{O}}(k^{-1/3})$ [**B**T'16])

In particular Open problem 2 $\Rightarrow$ Open problem 1 and

$$S_{tree}(\Psi_n) \geqslant 2^{n(1-\sigma_k)}\,,$$

where $\sigma_k = \widetilde{\mathcal{O}}(k^{-1/3})$.

Ψ_n & the width l.b.

Take p prime

1. there exist a system $\mathscr{E}$ of lin.eq. mod p in m vars s.t.

   - each equation in $\mathscr{E}$ has $\leqslant p^2$ vars
   - every $\mathscr{G} \subseteq \mathscr{E}$ of size $\geqslant 3m/p$ is unsatisfiable
   - ($\sim$ expansion) for every $\mathscr{G} \subseteq \mathscr{E}$ with $|\mathscr{G}| \in [m/p, 3m/p]$, every lin. comb. of the equations in $\mathscr{G}$ has $\geqslant m(1 - c/p)$ variables

2. write each mod p var as a sum of p^2 Boolean variables & encode as a CNF, this is Ψ_n. It is a $\widetilde{\mathcal{O}}(p^4)$-CNF in $n = \widetilde{\mathcal{O}}(mp)$ vars
(A less naive construction gives a $\widetilde{\mathcal{O}}(p^3)$-CNF in $n = \widetilde{\mathcal{O}}(mp)$ vars)

3. a "clause-of-medium-complexity" type of argument implies
$w(\Psi_n) \geqslant n(1 - \widetilde{\mathcal{O}}(p^{-1}))$ $\square$

Thm

There are unsatisfiable k-CNF formulas Θ_n in n variables s.t.

$$S_{reg}(\Theta_n) \geqslant 2^{n(1-\sigma_k)},$$

where $\sigma_k = \widetilde{\mathcal{O}}(k^{-1/4})$.

Thm

There are unsatisfiable k-CNF formulas Θ_n in n variables s.t.

$$S_{reg}(\Theta_n) \geqslant 2^{n(1-\sigma_k)},$$

where $\sigma_k = \widetilde{\mathcal{O}}(k^{-1/4})$.

A resolution refutation π of a CNF formula in n vars is δ-regular if on every path in π a set of $\leqslant \delta n$ is resolved more than once.

Thm

There are unsatisfiable k-CNF formulas Θ_n in n variables s.t.

$$S_{\delta\text{-}reg}(\Theta_n) \geqslant 2^{n(1-\sigma_k)},$$

where both σ_k and δ are $\widetilde{\mathcal{O}}(k^{-1/4})$

Lemma

F k-CNF in n vars, if $w(F) \geqslant w$ then

$$S_{reg}(F[\oplus^{\ell}]) \geqslant 2^{w\ell(1-\varepsilon)}\,,$$

where $\varepsilon = \frac{c}{\ell}\log(\frac{\ell n}{w})$.

Lemma

F k-CNF in n vars, if $w(F) \geqslant w$ then

$$S_{reg}(F[\oplus^{\ell}]) \geqslant 2^{w\ell(1-\varepsilon)} ,$$

where $\varepsilon = \frac{c}{\ell} \log(\frac{\ell n}{w})$.

0. Assume $w(F) \geqslant w$ and let π be regular refutation of $F[\oplus^{\ell}]$
1. for every $\beta \in \{0,1\}^{n\ell}$ exists $C_\beta \in \pi$ mentioning $\geqslant w$ full blocks of vars and $\neg C_\beta$ disagrees with β on most w vars (this uses regularity)
2. a counting argument shows a l.b. on $|\pi|$. $\sim$QED

Lemma

F k-CNF in n vars, if $w(F) \geqslant w$ then

$$S_{reg}(F[\oplus^{\ell}]) \geqslant 2^{w\ell(1-\varepsilon)} ,$$

where $\varepsilon = \frac{c}{\ell} \log(\frac{\ell n}{w})$.

0. Assume $w(F) \geqslant w$ and let π be regular refutation of $F[\oplus^{\ell}]$
1. for every $\beta \in \{0,1\}^{n\ell}$ exists $C_\beta \in \pi$ mentioning $\geqslant w$ full blocks of vars and $\neg C_\beta$ disagrees with β on most w vars (this uses regularity)
2. a counting argument shows a l.b. on $|\pi|$. $\sim$QED

Θ_n is $\Psi_n[\oplus^{\ell}]$ where $\ell = \widetilde{\mathcal{O}}(k^{1/4})$.

Thanks!

References

[BI'13] *Strong ETH Holds for Regular Resolution*
[**B**T'17] *Strong ETH and Resolution via Games and the Multiplicity of Strategies*
[**B**T'16] *Improving resolution width lower bounds for k-CNFs with applications to the Strong Exponential Time Hypothesis*

A game for size and width

F unsat CNF, R set of partial assignments — the "records"

Game(F, R)

Prover: find assignment in R falsifying F

Delayer: delay as much as possible

At step i, **Prover** has an assignment $r_i \in R$ and ask for the Boolean value of a variable $x \notin \mathrm{dom}(r_i)$;

Delayer chooses $b \in \{0, 1\}$;

Prover sets $r_{i+1} \subseteq r_i \cup \{x = b\}$.

$Game_{reg}(F, R)$ if **Prover** cannot ask the same variable twice.

- if whenever **Prover** wins $Game_{(reg)}(F, R)$, $|R| \geqslant s$ then $S_{(reg)}(F) \geqslant s$.
- $w(F) \geqslant w$ iff **Prover** does not win $Game(F, R)$ with R set of all partial assignments of $\leqslant w$ vars