Are Short Proofs Narrow? QBF Resolution is not Simple

Olaf Beyersdorff[1] Leroy Chew[1] Meena Mahajan[2]

Anil Shukla[2]

[1] School of Computing, University of Leeds, UK
[2] Institute of Mathematical Sciences Chennai, India

IRISS-2017: 11th Inter-Research-Institute Student Seminar
Kolkata, India
January 20, 2017

Outline

Outline

Resolution

- Introduced by Blake in 1937.
- Resolution is a proof system for proving that boolean formulas in a CNF form are unsatisfiable.
- The only inference rule in resolution is:

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

- CNF formula $F \in \text{UNSAT} \implies F$ has a **resolution proof** (completeness).
- A CNF formula F has a **resolution proof** $\implies F \in \text{UNSAT}$ (Soundness).

Resolution Proof

Resolution Proof

- Let $F = \{C_1, \ldots, C_k\}$ be an unsatisfiable formula over n variables.

Resolution Proof

- Let $F = \{C_1, \ldots, C_k\}$ be an unsatisfiable formula over n variables.
- A resolution proof of $F \in UNSAT$ is a sequence of clauses $\pi = \{D_1, \ldots, D_t\}$ such that
  - The last clause D_t is the empty clause $\square$.
  - Each clause D_q is either one of the initial clauses or is derived from some clause D_m, D_n with $m, n < q$ using the resolution rule.

Resolution Proof

- Let $F = \{C_1, \ldots, C_k\}$ be an unsatisfiable formula over n variables.
- A resolution proof of $F \in UNSAT$ is a sequence of clauses $\pi = \{D_1, \ldots, D_t\}$ such that
  - The last clause D_t is the empty clause $\Box$.
  - Each clause D_q is either one of the initial clauses or is derived from some clause D_m, D_n with $m, n < q$ using the resolution rule.
- If we store pointers from each D_m, D_n to D_q then we actually get a DAG G_π. We call G_π, proof graph associated with π.
- If G_π is a tree then π is called a tree-like resolution proof of F.

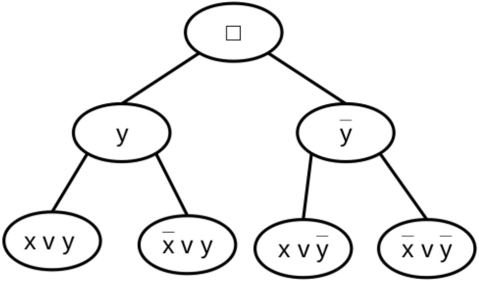
Some Examples

Some Examples

- Consider the following unsatisfiable formula on two variables: $(x \vee y) \wedge (\neg x \vee y) \wedge (x \vee \neg y) \wedge (\neg x \vee \neg y)$.

Some Examples

- Consider the following unsatisfiable formula on two variables: $(x \vee y) \wedge (\neg x \vee y) \wedge (x \vee \neg y) \wedge (\neg x \vee \neg y)$.

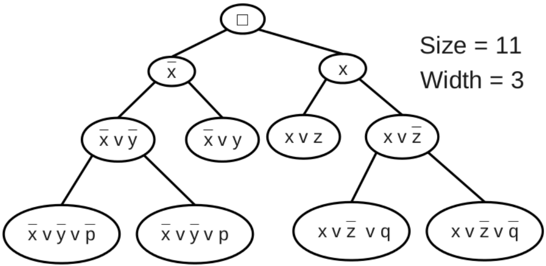


Example 3

Consider the CNF formula on five variables: $F = \{(\neg x \vee \neg y \vee \neg p), (\neg x \vee \neg y \vee p), (\neg x \vee y), (x \vee z), (x \vee \neg z \vee q), (x \vee \neg z \vee \neg q)\}$.

Example 3

Consider the CNF formula on five variables: $F = \{(\neg x \vee \neg y \vee \neg p), (\neg x \vee \neg y \vee p), (\neg x \vee y), (x \vee z), (x \vee \neg z \vee q), (x \vee \neg z \vee \neg q)\}$.



Proof graph of F

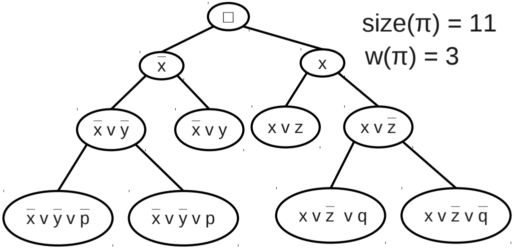
Outline

Complexity measures: Size and Width

$$S(\vdash F) = \min \{\text{size}(\pi) : \pi \text{ resolution proof of } F\}$$

$$w(\vdash F) = \min \{w(\pi) : \pi \text{ resolution proof of } F\}$$

$$S_T(\vdash F) = \min \{\text{size}(\pi) : \pi \text{ tree-like res proof of } F\}$$



$\text{size}(\pi) = 11$

$w(\pi) = 3$

Outline

Short Proofs are Narrow — Resolution Made Simple

Theorem (Ben-Sasson and Wigderson, J. ACM 2001)

For all unsatisfiable CNFs F in n variables the following holds:

- $S_T(\vdash F) \geq 2^{w(\vdash F) - w(F)}$.
- $S(\vdash F) = \exp\left(\Omega\left(\frac{(w(\vdash F) - w(F))^2}{n}\right)\right)$.

- Thus for CNF F with n variables and constant initial width, proving $w(\vdash F) = \Omega(n)$ proves tree-like size lower bounds.

Complexity Measure: Clause Space

- The concept of resolution clause space was first introduced by Esteban and Torán 2001.
- Intuitively, resolution clause space of an unsatisfiable CNF formula is the minimum number of clauses that have to be kept simultaneously in memory in order to refute the formula.
- Let $CSpace(\vdash F)$ = Minimum clause space requirements to refute F.

Theorem (Atserias and Dalmau 2008)

For all unsatisfiable CNFs F the following relation holds:
$w(\vdash F) \leq CSpace(\vdash F) + w(F) - 1$

Outline

Introduction

- QBFs are propositional formulas with Boolean quantifiers ranging over $0, 1$.

Introduction

- QBFs are propositional formulas with Boolean quantifiers ranging over $0, 1$.
- Consider a false QBF formula

$$\mathcal{Q}_1 x_1 \dots \mathcal{Q}_i x_i \dots \mathcal{Q}_j x_j \dots \mathcal{Q}_n x_n.\ F,$$

where F is a quantifier free CNF formula over variables $x_1, \dots, x_n$, each $\mathcal{Q} \in \{\exists, \forall\}$.

Introduction

- QBFs are propositional formulas with Boolean quantifiers ranging over $0, 1$.
- Consider a false QBF formula

$$\mathcal{Q}_1 x_1 \ldots \mathcal{Q}_i x_i \ldots \mathcal{Q}_j x_j \ldots \mathcal{Q}_n x_n.\ F,$$

  where F is a quantifier free CNF formula over variables $x_1, \ldots, x_n$, each $\mathcal{Q} \in \{\exists, \forall\}$.
- We say x_i is on left of x_j or x_i is before x_j.
- Proof systems based on resolution for QBF formulas are called QBF resolution.
- We now define an important QBF resolution (**Q-resolution**) and show that size-width, and space-width relation fails for it.

Q-resolution: Definition

- Q-Res = resolution + ∀-reduction [Kleine Büning, Karpinski, and Flögel; Information and Computation, 1995].
- Q-Res proof system proofs the falseness of QBF formulas.
- Q-Res has two inference rules:
  - **Resolution rule**: $\frac{C \vee x \quad D \vee \neg x}{C \vee D}$, where x is existential literal and $C \vee D$ is not a tautology.
  - ∀-**reduction**: $\frac{C \vee x}{C}$, where x is universal variable, and all existential variable in C are before x in the prenex of the given QBF formula.

Q-Res Proof

- Let $\mathcal{F} = \mathcal{Q}_1 x_1 \dots \mathcal{Q}_n x_n . F$ be a false QBF formula.
- A Q-Res proof for $\mathcal{F}$ is a sequence of clause $\pi = C_1, C_2, \dots, C_m$ such that:
  - C_m is the empty clause.
  - Each C_i is either from F *or* is derived from previous clauses using one of the above inference rules.
- Once again we have proof graph G_π.
- If G_π is a tree, then π is called a tree-like Q-Res proof for $\mathcal{F}$.

Examples 1

- Consider the false formula

$$\mathcal{F} = \exists e \forall u.(e \vee u) \wedge (\neg e \vee \neg u)$$

- The Q-Res proofs first derive the clause (e) and $(\neg e)$ by $\forall$-reduction and then apply resolution rule to derive the empty clause.

Examples 2

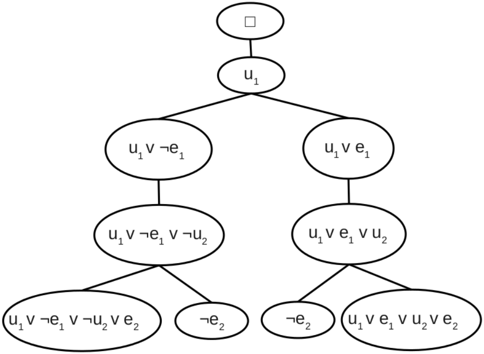
- Consider the false formula

$$\mathcal{F} = \forall u_1 \exists e_1 \forall u_2 \exists e_2 .$$
$$(u_1 \vee e_1 \vee u_2 \vee e_2) \wedge (u_1 \vee \neg e_1 \vee \neg u_2 \vee e_2) \wedge (\neg e_2)$$

Examples 2

- Consider the false formula

$$\mathcal{F} = \forall u_1 \exists e_1 \forall u_2 \exists e_2.$$
$$(u_1 \vee e_1 \vee u_2 \vee e_2) \wedge (u_1 \vee \neg e_1 \vee \neg u_2 \vee e_2) \wedge (\neg e_2)$$



Complexity Measures for Q-Res

- Keep the definition of size, width and space same as that of resolution proof system.
- That is, $w(\mathcal{F}) = \max\{w(C) : C \in F\}$,
- Let $S(\vdash_{\text{Q-Res}} \mathcal{F}) = \min\{size(\pi) : \pi \vdash_{\text{Q-Res}} \mathcal{F}\}$.
- $w(\vdash_{\text{Q-Res}} \mathcal{F}) = \min\{w(\pi) : \pi \vdash_{\text{Q-Res}} \mathcal{F}\}$.

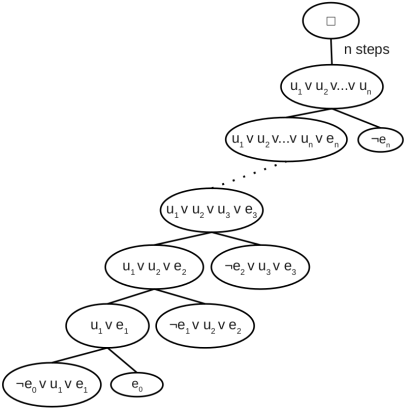
Outline

Size-width Relation Fails

- Consider the following false QBF formula:
$\mathcal{F}_n = \forall u_1 \ldots u_n \exists e_0 \exists e_1 \ldots e_n . (e_0) \wedge \bigwedge_{i \in [n]} (\neg e_{i-1} \vee u_i \vee e_i) \wedge (\neg e_n)$

Size-width Relation Fails

- Consider the following false QBF formula:
  $\mathcal{F}_n = \forall u_1 \ldots u_n \exists e_0 \exists e_1 \ldots e_n . (e_0) \wedge \bigwedge_{i \in [n]} (\neg e_{i-1} \vee u_i \vee e_i) \wedge (\neg e_n)$



Size-width Relation Fails (Cont.)

- Above examples illustrates that it is easy to accumulate universal variables in one clause which makes the width large but has a short proofs.
- Natural question: just count existential variables and then ask about size-width relation.
- $w_\exists(C) =$ number of existential literals in C.
- $w_\exists(\vdash_{\text{Q-Res}} \mathcal{F}) = \min\{w_\exists(\pi) : \pi \vdash_{\text{Q-Res}} \mathcal{F}\}$.

Negative Results: Size-existential-width and Space-existential-width Relation Fails in tree-like Q-Res

Theorem

There exists a false QBF formula $\mathcal{F}_n$ over $O(n^2)$ variables such that:

- $S_T(\vdash_{\text{Q-Res}} \mathcal{F}_n) = n^{O(1)}$,
- $w_\exists(\mathcal{F}_n) = 3$,
- $w_\exists(\vdash_{\text{Q-Res}} \mathcal{F}_n) = \Omega(n)$.
- $CSpace(\vdash_{\text{Q-Res}} \mathcal{F}_n) = O(1)$.

- Note that $\mathcal{F}_n$ has $O(n^2)$ variables, they do not rule out size-existential-width relation in general Q-Res proof system.

Negative Results: Size-existential-width Relation Fails in Q-Res

Theorem

There exists a false QBF formula ϕ_n over $O(n)$ variables such that:

- $S(\vdash_{\text{Q-Res}} \phi_n) = n^{O(1)}$,
- $w_\exists(\phi_n) = 3$,
- $w_\exists(\vdash_{\text{Q-Res}} \phi_n) = \Omega(n)$.

- ϕ_n is known to be hard for tree-like Q-Res, so it can not be used to disprove size-existential-width relation in tree-like Q-Res.

Thank you.