On Proof Systems for #QBF

Sravanthi Chede[1] Leroy Chew[2] Vaibhav Krishan[1] **Anil Shukla**[3]

[1]The Institute of Mathematical Sciences, Chennai, India
[2]Czech Technical University in Prague, Czech Republic
[3]Indian Institute of Technology Ropar, India

SAT 2026
Lisbon, Portugal
July 22, 2026

Quantified Boolean Formulas

- $\Phi = Q.F = Q_1X_1Q_2X_2\dots Q_kX_k\ .\ F(X_1, X_2, \dots, X_k)$ is a QBF, where
  - $Q_i \in \{\exists, \forall\}$ and $Q_i \neq Q_{i+1}, i = 1, 2, k-1$.
  - X_i are pairwise disjoint set of variables.
  - $F(X_1, X_2, \dots X_k)$ is a CNF formula.
  - If $Q_i = \exists$ (resp.$Q_i = \forall$), then all variables $x \in X_i$ are called existential (reps. universal) variables.
  - E, U are the sets of all existential and universal variables respectively.
  - For $x \in X_i$ and $y \in X_j$, with $i \leq j$, we say that x occurs to the left of y in Q (denoted $x \leq_Q y$).
  - For a existential variable e, $L_Q(e) = \{u \mid u \in U \text{ and } u \leq_Q e\}$

QBF as two player game

$$Q.F = \forall u_1 \; \exists e_1 \; \forall u_2 \; \exists e_2 \; . \; (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2)$$

- $Q.F$ can be seen as a two player game: $\exists$-player and $\forall$-player.

Existential player: Tries to make CNF True
Universal player: Tries to make CNF False

Existential player has a winning strategy $\Leftrightarrow$ QBF is True

Universal player has a winning strategy $\Leftrightarrow$ QBF is False

Winning Strategies, Witness Assignments, and #QBF Problem

- A Boolean function for e (denoted S_e) is a function from assignments to variables in $L_Q(e)$ to $\{0,1\}$.
- A strategy $\mathcal{S}$ for existential player is a set of such Boolean functions S_e one for every $e \in E$.
- $\mathcal{S}$ is a winning strategy if assigning each $e \in E$ according to it always makes existential player win.

How to prove that two strategies $\mathcal{S}_1 = \{S_{1,x}(L_Q(x)) \mid x \in E\}$, $\mathcal{S}_2 = \{S_{2,x}(L_Q(x)) \mid x \in E\}$ are different?

- Provide a complete assignment α to U, (**witness assignment**)
- such that, for some $x \in E$, $S_{1,x}(\alpha|_{L_Q(x)}) \neq S_{2,x}(\alpha|_{L_Q(x)})$

#QBF Problem

Given a True QBF, how many distinct winning strategies does it have?

Naive proof system for #QBF

For a True QBF $Q.F$,

- Enumerate all k existential strategies
  - Provide a proof that they are all correct winning strategies and
  - provide $\binom{k}{2}$ witness assignments to show that these strategies are all different
- Prove that there are no other winning strategies of $Q.F$
  - can be achieved by providing a refutation of a QBF carefully encoded to capture this (next slide).

Theorem

Any QBF which has exponential many winning strategies has an obvious lower bound in the Naive system.

Absence of models

We use similar encoding in Q-MICE also.

Claim

Given a True QBF $Q.F$ and a set of winning strategies $\mathcal{S}_1, \ldots, \mathcal{S}_k$,
the following QBF is False if and only if there are no other winning strategies for $Q.F$

$$\exists \vec{\alpha}_1, \ldots, \vec{\alpha}_k Q \;.\; F \wedge \bigwedge_{i \in [k]} \left(\bigwedge_{u \in U} (u \leftrightarrow \alpha_{i,u}) \rightarrow \bigvee_{e \in E} \left(e \not\leftrightarrow S_{i,e}(\vec{\alpha}_i) \right) \right)$$

This statement encodes that:

- there is a $k+1^{\text{th}}$ strategy for $Q.F$.
- it is different from the given k strategies as proved by the k witness assignments $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$.
- it is a winning strategy for $Q.F$

Hence, proving that this is a FQBF disproves the existence of any such strategy!

Universal Expansion: $\forall$Exp+MICE

Popular technique in the QBF proof complexity [Janota and Marques-Silva, TCS 2015].

Proposition

A true QBF Φ, when expanded with all complete assignments to universal variables, leads to a CNF formula ϕ such that every model of ϕ leads to a distinct model of Φ and vice versa. In other words, their model-counts are the same.

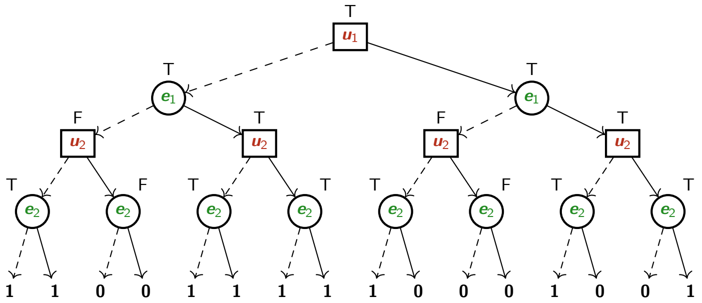
Corollary

Proofs in $\forall$Exp+MICE *are exponential in terms of the number of universal variables in the QBF.*

Full Binary Assignment Tree for QBFs

$\forall u_1 \; \exists e_1 \; \forall u_2 \; \exists e_2 \; . \; (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2)$

Dashed edges for 0, solid edges for 1.



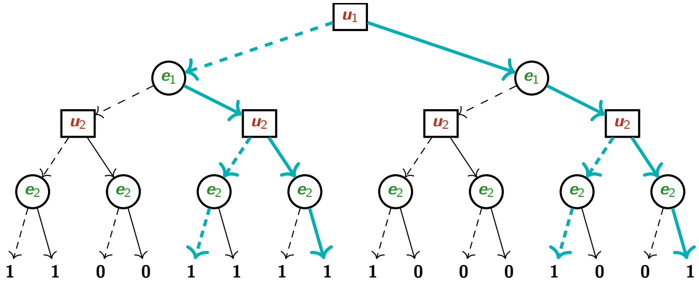
Satisfiability of QBF:

existential node $\rightarrow \vee$

universal node $\rightarrow \wedge$

Full Binary Assignment Tree for QBFs (contd.)

$$\forall u_1 \exists e_1 \forall u_2 \exists e_2 . (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2)$$



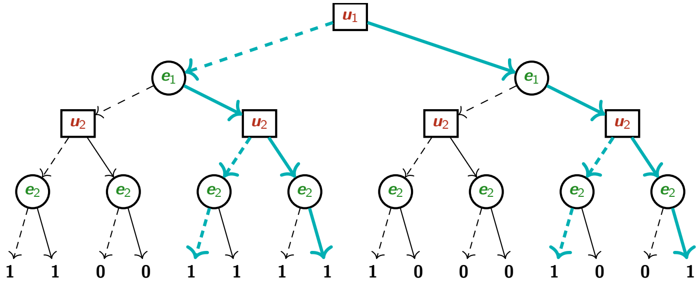
$$\mathcal{S}_1 = \{S_{e_1} = 1, S_{e_2} = u_2\}$$

Model Tree:

- Existential node has 1 outgoing edge
- Universal node has both outgoing edges
- contains the root node
- All leaves are 1

Full Binary Assignment Tree for QBFs (contd.)

$\forall u_1\ \exists e_1\ \forall u_2\ \exists e_2\ .\ (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2)$

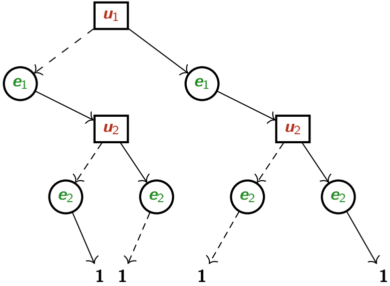


$\mathcal{S}_1 = \{S_{e_1} = 1, S_{e_2} = u_2\}$

$\mathcal{S}_2 = \{S_{e_1} = 1, S_{e_2} = u_1 \leftrightarrow u_2\}$

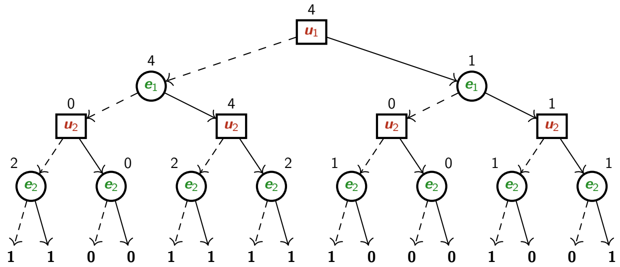
Model Tree:

- Existential node has 1 outgoing edge
- Universal node has both outgoing edges
- contains the root node
- All leaves are 1



Full Binary Assignment Tree for QBFs (contd.)

$\forall u_1 \; \exists e_1 \; \forall u_2 \; \exists e_2 \; . \; (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2)$



#QBF = Number of model trees:

existential node $\rightarrow +$

universal node $\rightarrow \times$

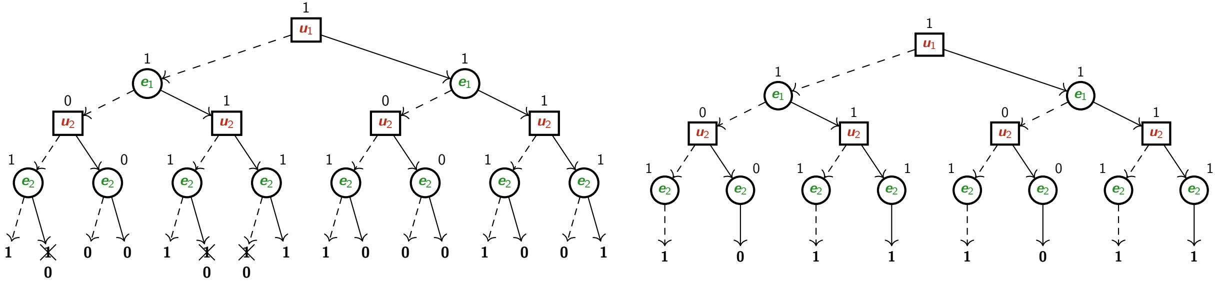
$$\mathcal{S}_1 = \{S_{e_1} = 1, S_{e_2} = u_2\}$$
$$\mathcal{S}_2 = \{S_{e_1} = 1, S_{e_2} = u_1 \leftrightarrow u_2\}$$
$$\mathcal{S}_3 = \{S_{e_1} = 1, S_{e_2} = \overline{u_1} \vee u_2\}$$
$$\mathcal{S}_4 = \{S_{e_1} = 1, S_{e_2} = u_1 \wedge u_2\}$$

Subtrees and QBF restrictions

$$\Phi := \forall u_1 \; \exists e_1 \; \forall u_2 \; \exists e_2 \; . \; (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2)$$

Restricting existential variables:

$$\Phi|_{\{e_2=u_2\}} = \forall u_1 \; \exists e_1 \; \forall u_2 \; \exists e_2 \; . \; (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2) \wedge (e_2 \leftrightarrow u_2)$$



Subtrees and QBF restrictions (contd.)

$\Phi := \forall u_1\ \exists e_1\ \forall u_2\ \exists e_2\ .\ (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2)$

Restricting universal variables:

$\Phi|_{\{u_1=0\}} \neq \forall u_1\ \exists e_1\ \forall u_2\ \exists e_2\ .\ (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2) \wedge (\overline{u_1}) \rightarrow$ False QBF

Subtrees and QBF restrictions (contd.)

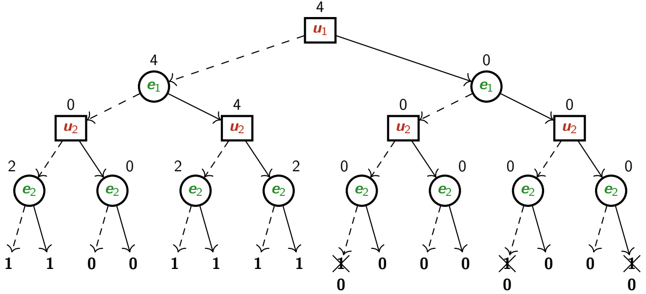
$\Phi := \forall u_1\ \exists e_1\ \forall u_2\ \exists e_2\ .\ (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2)$

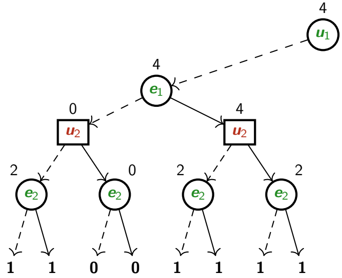
Restricting universal variables:

$\Phi|_{\{u_1=0\}} \neq \forall u_1\ \exists e_1\ \forall u_2\ \exists e_2\ .\ (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2) \wedge (\overline{u_1}) \rightarrow$ False QBF

Making it existential will work:

$\Phi|_{\{u_1=0\}} = \exists u_1\ \exists e_1\ \forall u_2\ \exists e_2\ .\ (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2) \wedge (\overline{u_1})$





Q-MICE (Quantified Model-counting Induction by Claim Extension)

For #SAT, the proof system MICE [Fitche, Hecher, Roland, SAT 2022, Beyersdorff, Hoffmann, Spachmann SAT 2023] has claims of the form (F, α, c) where

- F is a CNF formula,
- α is a partial assignment
- c is the correct number of models for $F|_\alpha$.

Q-MICE (Quantified Model-counting Induction by Claim Extension)

For #SAT, the proof system MICE [Fitche, Hecher, Roland, SAT 2022, Beyersdorff, Hoffmann, Spachmann SAT 2023] has claims of the form (F, α, c) where

- F is a CNF formula,
- α is a partial assignment
- c is the correct number of models for $F|_{\alpha}$.

Similarly in Q-MICE, we define claims to be of the form $(Q.F|_{\rho},\ A,\ c)$ where

- $Q.F$ is the input QBF,
- ρ is a partial assignment to universal variables (ρ can be empty),
- A is a partial strategy for existential variables
  - i.e. $A = \{S_x \mid x \in X \subseteq E\}$
- c is the number of ways to extend A s.t. it is a winning strategy to $Q.F|_{\rho}$.
  - i.e. c is the correct model count for the QBF $Q.F|_{\{\rho \cup A\}}$

Q-MICE Proof System

Q-MICE has the following inference rules:

- Axiom rules
- Composition rules: for manipulating the existential variables.
  It consists of three independent subrules :
  - composition-a,
  - composition-b,
  - composition-c

  All these rules require an absence of models statement and its proof.
- Join rule: designed for manipulating the universal variables.

Q-MICE Proof System

Q-MICE proof

Q-MICE proof of a QBF $Q.F$ with exactly k distinct winning strategies is a sequence of claims

$$L_1, \ldots, L_s,$$

where $L_s = (Q.F, \emptyset, k)$ and every L_i is either an axiom or is derived using the inference rules applied on already derived claims.

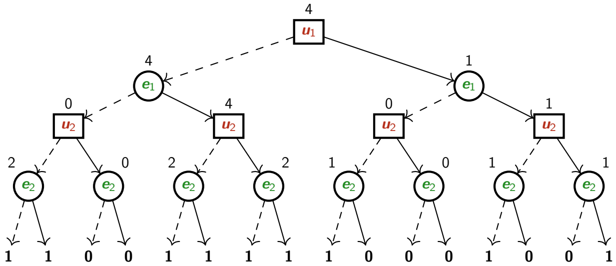
Complexity measures of Q-MICE

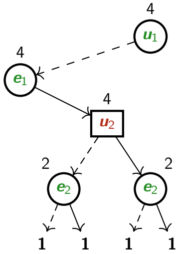
For a Q-MICE proof π of a QBF $Q.F$,

- Length of π is the number of claims in it,
- Size of π is the length of π plus the additional witness, false QBFs proofs, and tautology proofs sizes.

Axiom-Rule: Examples

$\Phi = \forall u_1 \, \exists e_1 \, \forall u_2 \, \exists e_2 \, . \, (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2)$



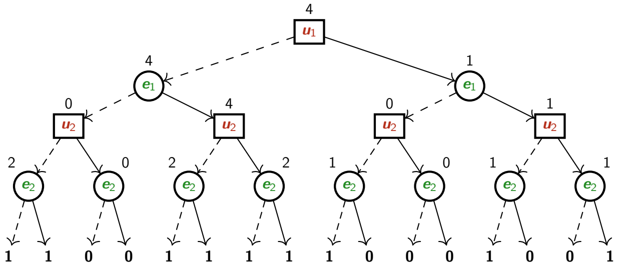


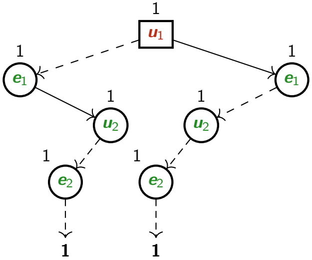
Example 1:
$(\Phi_{u_1=0}, \{e_1 = 1\}, 4)$
$c = 4$ can be computed linear in n.

Model count: existential node $\rightarrow +$
universal node $\rightarrow \times$
single child: copy
Tautology proof explicitly is provided.

Axiom-Rule: Examples

$$\Phi = \forall u_1 \, \exists e_1 \, \forall u_2 \, \exists e_2 \, . \, (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2)$$





Example 2:
$(\Phi_{u_2=0}, \{e_1 = \overline{u}_1, e_2 = 0\}, 1)$
$c = 1$ can be computed linear in n.

Model count: existential node $\rightarrow +$
universal node $\rightarrow \times$
single child: copy
Tautology proof explicitly is provided.

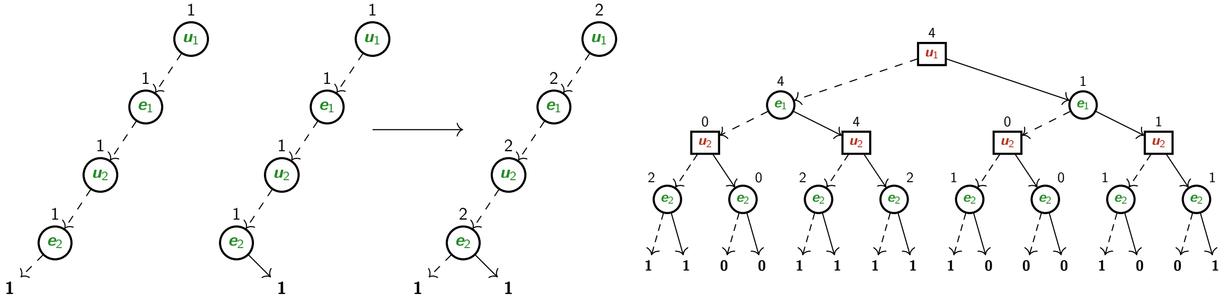
Axiom-Rule

For a QBF $Q.F$, one can derive $\overline{(Q.F|_{\rho},\ A,\ c)}$, when

- $F|_{\{\rho \cup A\}}$ is a Tautology and an explicit proof of the same is provided.
- c is calculated efficiently as follows:
  - Initially $count$=1, start from the innermost quantified variable (say x) in Q.
  - if x is existential and $\notin A$ then $count = 2 \cdot count$
  - if x is universal and $\notin \rho$ then $count = count^2$
  - At the end of the reverse quantification sequence, $c = count$

Composition-a Rule

$$Q.F := \forall u_1\ \exists e_1\ \forall u_2\ \exists e_2\ .\ (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2)$$



Example: $$\frac{(\Phi|_{u_1=0,u_2=0},\ \{e_1{=}0,e_2{=}0\},\ 1)\ ,\ (\Phi|_{u_1=0,u_2=0},\ \{e_1{=}0,e_2{=}1\},\ 1)}{(\Phi|_{u_1=0,u_2=0},\ \{e_1{=}0\},\ 1{+}1)}$$

Absence of models: $Q'.F \wedge (\overline{e_1}) \wedge (e_2 \neq 0) \wedge (e_2 \neq 1)$

Composition-a Rule (contd.)

For a QBF $Q.F$, one can derive $\dfrac{(Q.F|_\rho,\ A_1,\ 1),\dots,(Q.F|_\rho,\ A_n,\ 1)}{(Q.F|_\rho,\ A,\ n)}$, when

- All $A_1, \dots, A_n$ are complete strategies and $A \subseteq \cap_{i\in[n]} A_i$
- All $A_1, \dots, A_n$ are pair-wise distinct i.e. $\binom{n}{2}$ witness assignments needed
- Absence of models proof for existential variables in $A_1 \setminus A$

$$\exists \vec{\alpha}_1, \dots, \vec{\alpha}_n Q' \ . \ F \wedge \bigwedge_{x \in vars(A)} (x \leftrightarrow S_{A,x}) \wedge \bigwedge_{i\in[n]} \left(\bigwedge_{u \in U \setminus vars(\rho)} (u \leftrightarrow \alpha_{i,u}) \rightarrow \bigvee_{e \in vars(A_1 \setminus A)} \left(e \not\leftrightarrow S_{A_i,e}(\vec{\alpha}_i) \right) \right)$$

Composition-a Rule (contd.)

For a QBF $Q.F$, one can derive $\dfrac{(Q.F|_{\rho},\ A_1,\ 1),\ldots,(Q.F|_{\rho},\ A_n,\ 1)}{(Q.F|_{\rho},\ A,\ n)}$, when

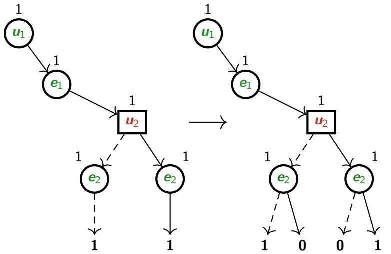
- All $A_1, \ldots, A_n$ are complete strategies and $A \subseteq \cap_{i \in [n]} A_i$
- All $A_1, \ldots, A_n$ are pair-wise distinct i.e. $\binom{n}{2}$ witness assignments needed
- Absence of models proof for existential variables in $A_1 \setminus A$

$$\exists \vec{\alpha}_1, \ldots, \vec{\alpha}_n Q' \ . \ F \wedge \bigwedge_{x \in vars(A)} (x \leftrightarrow S_{A,x}) \wedge \bigwedge_{i \in [n]} \left(\bigwedge_{u \in U \setminus vars(\rho)} (u \leftrightarrow \alpha_{i,u}) \rightarrow \bigvee_{e \in vars(A_1 \setminus A)} \left(e \not\leftrightarrow S_{A_i,e}(\vec{\alpha}_i) \right) \right)$$

Theorem

Axiom rule (with $\rho = \emptyset$) and Composition-a rule are sufficient for completeness of Q-MICE.

Composition-b Rule



For simplifying the existential strategy in a hypothesis claim

$Q.F := \forall u_1 \, \exists e_1 \, \forall u_2 \, \exists e_2 \,.\, (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2)$

Example: $\dfrac{(\Phi|_{u_1=1},\ \{e_1=1, e_2=u_2\},\ 1)}{(\Phi|_{u_1=1},\ \{e_1=1\},\ 1)}$

Absence of models:

$$\exists \alpha_1 \exists u_1 \exists e_1 \forall u_2 \exists e_2 \,.\, (e_1 \vee \overline{u_2}) \vee (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2) \wedge (u_1) \wedge (e_1) \wedge ((u_2 = \alpha_1) \rightarrow (e_2 \neq \alpha_1))$$

$$\dfrac{\dfrac{\dfrac{(u_2 \vee \overline{e_2}) \qquad (u_2 \vee \alpha_2 \vee e_2)}{(u_2 \vee \alpha_2)}\,(\text{Res})}{(\alpha_2)}\,(\forall\text{red}) \qquad \dfrac{\dfrac{(\overline{u_2} \vee e_2) \qquad (\overline{u_2} \vee \overline{\alpha_2} \vee \overline{e_2})}{(\overline{u_2} \vee \overline{\alpha_2})}\,(\text{Res})}{(\overline{\alpha_2})}\,(\forall\text{red})}{\bot}\,(\text{Res})$$

Composition-b Rule (contd.)

For a QBF $Q.F$, one can derive $\dfrac{(Q.F|_{\rho},\ A_1,\ c_1)}{(Q.F|_{\rho},\ A,\ c_1)}$, when

- $A \subseteq A_1$
- Absence of models proof for existential variables in $A_1 \setminus A$

Composition-c Rule

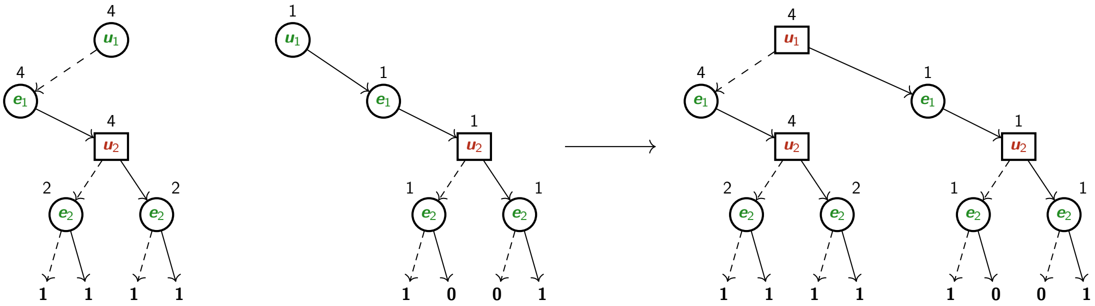
For a QBF $Q.F$, one can derive $\dfrac{(Q.F|_\rho,\ A_1,\ c_1),\ldots,(Q.F|_\rho,\ A_n,\ c_n)}{(Q.F|_\rho,\ A,\ \sum\limits_{i\in[n]} c_i)}$, when

- All $A_1, \ldots, A_n$ are (partial) strategies for the same existential variables and $A \subseteq \cap_{i\in[n]} A_i$
- All $A_1, \ldots, A_n$ are pair-wise distinct i.e. $\binom{n}{2}$ witness assignments needed
- Absence of models proof for existential variables in $A_1 \setminus A$
- Let x be the innermost $\exists$-variable in Q that $\in A_1 \setminus A$.
  - All existential variables of Q s.t. $y \leq_Q x \implies y \in vars(A_i)$.
  - All universal variables of Q s.t. $y \leq_Q x \implies y \in vars(\rho)$.

Join Rule

To drop universal variable restrictions from claims

$Q.F := \forall u_1\ \exists e_1\ \forall u_2\ \exists e_2\ .\ (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2)$



Example: $$\frac{(\Phi|_{u_1=0},\ \{e_1{=}1\},\ 4)\ \ ,\ (\Phi|_{u_1=1},\ \{e_1{=}1\},\ 1)}{(\Phi,\ \{e_1{=}1\},\ 4{\cdot}1)}$$

Join Rule (contd.)

For a QBF $Q.F$, one can derive $\dfrac{(Q.F|_{\rho\cup\{y=0\}},\ A,\ c_1),(Q.F|_{\rho\cup\{y=1\}},\ A,\ c_2)}{(Q.F|_{\rho},\ A,\ c_1{\cdot}c_2)}$, when

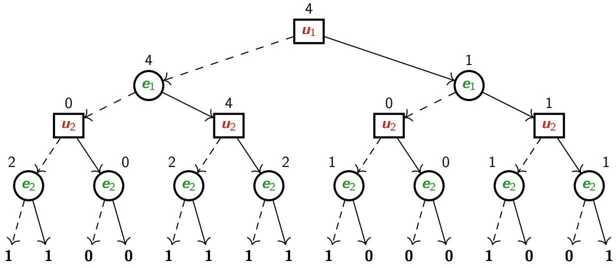
- All existential variables x s.t. $x \leq_Q y \implies x \in vars(A)$.
- All universal variables x s.t. $x \leq_Q y \implies x \in vars(\rho)$.

Q-MICE proof example

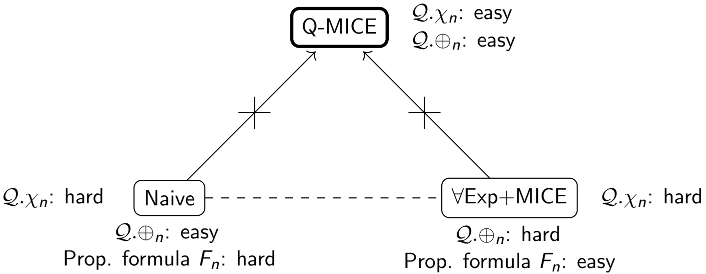
$\Phi := \forall u_1\ \exists e_1\ \forall u_2\ \exists e_2\ .\ (e_1 \vee \overline{u_2}) \wedge (\overline{u_1} \vee u_2 \vee \overline{e_2}) \wedge (\overline{u_1} \vee \overline{u_2} \vee e_2)$

$L_1 = (\Phi|_{\{u_1=0\}}, \{e_1 = 1\}, 4)$ (Axiom)
$L_2 = (\Phi|_{\{u_1=1\}}, \{e_1 = 1, e_2 = u_2\}, 1)$ (Axiom)
$L_3 = (\Phi|_{u_1=1}, \{e_1 = 1\}, 1)$ (Composition-b on L_2)
<absence of models: shown in example>
$L_4 = (\Phi, \{e_1 = 1\}, 4)$ (Join on L_1, L_3)
$L_5 = (\Phi, \emptyset, 4)$ (Composition-b on L_4)

- The absence of models statement is required.



#QBF Landscape



Quantified XOR-Pairs:

$$\mathcal{Q}.\oplus_n := \forall u_1, \ldots, u_n \underset{i \neq j \in [n]}{\exists} x_{i,j} \, . \, \bigwedge_{i \neq j \in [n]} (x_{i,j} \leftrightarrow u_i \oplus u_j)$$

Indexed Affine QBFs:

$$\mathcal{Q}.\chi_n := \forall u_1 \ldots u_{\log n} \, \exists x \, \forall v_1 \ldots v_n \, \exists y_1 \ldots y_n \, . \, \bigwedge_{i \neq (u)} (y_i = v_i \oplus x) \wedge (y_u = v_u \oplus \overline{x})$$

Discussions

- Exponential lower bounds for Q-MICE?
  - A possible candidate: propositional XOR-PAIRS.
- MICE proof system [Fitche, Hecher, Roland, SAT 2022,] is shown to be very useful for proof logging.
- We hope that Q-MICE plays a similar role in QBF model counting.

Thank you.

Separating Formulas

Indexed Affine QBFs:

$\mathcal{Q}.\chi_n := \forall u_1 \ldots u_{\log n}\ \exists x\ \forall v_1 \ldots v_n\ \exists y_1 \ldots y_n\ .\ \bigwedge_{i \neq (u)} (y_i = v_i \oplus x) \wedge (y_u = v_u \oplus \overline{x})$

These have linear number of universal variables and exponential many winning strategies.

Theorem

$\mathcal{Q}.\chi_n$ *formulas require exponential size proofs in both the Naive and the* $\forall$Exp+MICE *proof systems.*

$\mathcal{Q}.\chi_n$ *formulas have a polynomial size* Q-MICE *proof.*

Corollary

Q-MICE *is exponentially separated from the Naive and* $\forall$Exp+MICE *proof systems.*

Quantified XOR-Pairs:

$\mathcal{Q}.\oplus_n := \forall u_1, \ldots, u_n \underset{i \neq j \in [n]}{\exists} x_{i,j}\ .\ \bigwedge_{i \neq j \in [n]} (x_{i,j} \leftrightarrow u_i \oplus u_j)$

n universal variables $\implies$ exponential lower bound for $\forall$Exp+MICE.

$\#\mathrm{QBF}(\mathcal{Q}.\oplus_n) = 1 \implies$ Easy for Naive system using a sufficiently powerful FQBF proof system

XOR-PAIRS

$$\mathcal{Q}.\oplus_n := \forall u_1, \ldots, u_n \underset{i \neq j \in [n]}{\exists} x_{i,j} \, . \bigwedge_{i \neq j \in [n]} (x_{i,j} \leftrightarrow u_i \oplus u_j)$$

n universal variables $\implies$ exponential lower bound for $\forall$Exp+MICE.

XOR-PAIRS

$$\mathcal{Q}.\oplus_n := \forall u_1, \ldots, u_n \underset{i \neq j \in [n]}{\exists} x_{i,j} \ . \ \bigwedge_{i \neq j \in [n]} (x_{i,j} \leftrightarrow u_i \oplus u_j)$$

n universal variables $\implies$ exponential lower bound for $\forall$Exp+MICE.

Theorem

XOR-PAIRS has linear sized Q-MICE *proofs.*

(Axiom rule) $L_1 := \left(\mathcal{Q}.\oplus_n,\ A := \{S_{x_{i,j}} = u_i \oplus u_j | i \neq j \in [n]\},\ 1\right)$
(Composition-b rule) $L_2 := \left(\mathcal{Q}.\oplus_n,\ \emptyset,\ 1\right)$. The absence of models statement is:

$$\exists \vec{\alpha}\ \forall u_1, \ldots, u_n \underset{i \neq j \in [n]}{\exists} x_{i,j}. \bigwedge_{i \neq j \in [n]} (x_{i,j} \leftrightarrow u_i \oplus u_j) \wedge ((u_1 = \alpha_1 \wedge \ldots \wedge u_n = \alpha_n) \rightarrow (\bigvee_{i \neq j \in [n]} x_{i,j} \neq \alpha_i \oplus \alpha_j))$$

XOR-PAIRS

$$\mathcal{Q}.\oplus_n := \forall u_1, \ldots, u_n \underset{i \neq j \in [n]}{\exists} x_{i,j} \,.\, \bigwedge_{i \neq j \in [n]} (x_{i,j} \leftrightarrow u_i \oplus u_j)$$

n universal variables $\implies$ exponential lower bound for $\forall$Exp+MICE.

Theorem

XOR-PAIRS has linear sized Q-MICE *proofs.*

(Axiom rule) $L_1 := \left(\mathcal{Q}.\oplus_n,\ A := \{S_{x_{i,j}} = u_i \oplus u_j | i \neq j \in [n]\},\ 1\right)$
(Composition-b rule) $L_2 := \left(\mathcal{Q}.\oplus_n,\ \emptyset,\ 1\right)$. The absence of models statement is:

$$\exists \vec{\alpha}\ \forall u_1, \ldots, u_n \underset{i \neq j \in [n]}{\exists} x_{i,j} . \bigwedge_{i \neq j \in [n]} (x_{i,j} \leftrightarrow u_i \oplus u_j) \wedge ((u_1 = \alpha_1 \wedge \ldots \wedge u_n = \alpha_n) \rightarrow (\bigvee_{i \neq j \in [n]} x_{i,j} \neq \alpha_i \oplus \alpha_j))$$

$$\cfrac{\cfrac{\cfrac{x_{i,j} \leftrightarrow u_i \oplus u_j \qquad (u_1 = \alpha_1 \wedge \ldots \wedge u_n = \alpha_n) \rightarrow (\bigvee_{i \neq j \in [n]} x_{i,j} \neq \alpha_i \oplus \alpha_j)}{(u_1 = \alpha_1 \wedge \ldots \wedge u_n = \alpha_n) \rightarrow (\bigvee_{i \neq j \in [n]} u_i \oplus u_j \neq \alpha_i \oplus \alpha_j)}\text{(Prop. Frege inference)}}{(\alpha_1 = \alpha_1 \wedge \ldots \wedge \alpha_n = \alpha_n) \rightarrow (\bigvee_{i \neq j \in [n]} \alpha_i \oplus \alpha_j \neq \alpha_i \oplus \alpha_j)}(\forall\text{red with } u_i = \alpha_i \text{ for } i \in [n])}{\perp}\text{(Prop. Frege inference)}$$

Separations

We introduce a new family of QBFs called the 'Indexed Affine QBFs'.
$\mathcal{Q}.\chi_n := \forall u_1 \ldots u_{\log n} \, \exists x \, \forall v_1 \ldots v_n \, \exists y_1 \ldots y_n \, . \, \bigwedge_{i \neq (u)} (y_i = v_i \oplus x) \wedge (y_u = v_u \oplus \overline{x})$
These have linear number of universal variables and exponential many winning strategies.

Theorem

$\mathcal{Q}.\chi_n$ formulas require exponential size proofs in both the Naive and the $\forall$Exp+MICE *proof systems.*

Theorem

$\mathcal{Q}.\chi_n$ formulas have a polynomial size Q-MICE *proof.*

Corollary

Q-MICE *is exponentially separated from the Naive and* $\forall$Exp+MICE *proof systems.*