

On Proof Systems for #QBF

Sravanthi Chede   

The Institute of Mathematical Sciences (A CI of Homi Bhabha National Institute), Chennai, India

Leroy Chew   

Czech Technical University in Prague, Czech Republic

Vaibhav Krishan   

The Institute of Mathematical Sciences (A CI of Homi Bhabha National Institute), Chennai, India

Anil Shukla   

Indian Institute of Technology Ropar, Rupnagar, India

Abstract

For a quantified Boolean formula (QBF), the problem of computing the number of winning strategies is known as the #QBF problem. This problem is considered harder than the analogous #SAT problem [15]. Recently, important proof systems for QBFs [4, 2] and #SAT [5, 9] have been studied. By extending the ideas from both fields, we show that it is possible to design proof systems for #QBF. Such proof systems are important not only for advancing the theory of #QBF but also for certifying and designing better #QBF solvers, an area that is still in its early stages [19, 16].

In this paper, we explore #QBF proof systems to count the number of Skolem functions. In addition to a naive system, we study #QBF systems based on the \forall -expansion rule of QBFs [13]. We observe that these systems have inherent structural weaknesses that lead to lower bounds. As an alternative, we propose a #QBF proof system that we call Q-MICE, which consists of sound inference rules for computing and certifying the #QBF solution, similar to the line-based #SAT proof system MICE [11, 5]. To demonstrate the strength of Q-MICE, we present various upper bounds, such as the quantified version of the propositional XOR-PAIRS formula, which is known to be hard for MICE [5]. Consequently, we also separate Q-MICE from \forall -expansion based #QBF proof systems.

2012 ACM Subject Classification Theory of computation \rightarrow Proof complexity

Keywords and phrases QBF, Model Counting, Proof Systems, #QBF

Funding *Sravanthi Chede*: Supported by the ANRF J C Bose fellowship no. JCB/2023/000006.

Leroy Chew: This project is supported by the European Union under the project ROBOPROX (reg. no. CZ.02.01.01/00/22_008/0004590) and by the Czech Science Foundation project 24-12759S.

Acknowledgements We thank the anonymous SAT 2026 reviewers for their detailed and helpful suggestions.

1 Introduction

#QBF, the problem of counting the number of winning strategies of a QBF, is challenging from several perspectives. Firstly, from a computational complexity point of view, #QBF is known to be #PSPACE-complete [15]. #PSPACE is at least as large as #P, but potentially much larger. Secondly, the number of winning strategies may be doubly exponential, beyond the mere exponential bounds of propositional model counting (#SAT). Several proof systems for the #SAT problem have been studied. Notable systems include KCPS(#SAT) [7] and CPOG [6] that use *knowledge-compilation*. These systems prove a model count by a transformation to a knowledge compilation class where model counting is easy. Recently, the CLIP system [9] worked using a connection between circuits and PSPACE. Another approach is to derive the model count via line-based systems, such as MICE (Model-counting Induction by Claim Extension [11]). Starting at axioms, it computes the model count using inference rules.

In this paper, by extending ideas from QBF and #SAT proof systems, we provide the

first proof systems for the general #QBF problem, and study its proof complexity. Such proof systems are important to advance the theory of #QBF. The existence of proof systems can be useful towards #QBF solving, in both the design and correctness of the solvers.

The main contribution of the paper is extending the MICE proof system for #QBF (Section 3.2), denoted as Q-MICE. Q-MICE is a line based #QBF proof system, in which each line is of the form $(Q.F, A, c)$, where $Q.F$ is a true QBF, A is a partial strategy that consists of Skolem functions for some existential variables, and c is the number of ways to extend A into complete winning strategies for the existential player of $Q.F$. Q-MICE consists of the axiom rule (Definition 7), the composition rule (Definition 9) and the join rule (Definition 12). Each rule can be applied if its corresponding conditions are satisfied, which are required for the rule to be sound.

In addition to proving that Q-MICE is sound and complete (Theorem 16), we provide meaningful families with short proofs (Section 4) and establish an exponential separation between Q-MICE and the #QBF proof system $\forall\text{Exp}+\text{MICE}$ (Theorem 17). The $\forall\text{Exp}+\text{MICE}$ proof system (Section 3.1) semantically expands the \forall variables of the QBF (as in [13]), then finishes the proof with a #SAT proof system, in this case MICE.

Related work: Recently, some #QBF solvers [16, 19, 8, 18] have been introduced for solving the #QBF problem. For example, the d4-QBF [8] solver has been designed for #QBF which uses few techniques from SAT-solving and works on the full assignment tree of the QBF recursively along with a decomposition step ([8, Section 3.3]). The decomposition step identifies two or more non-connected components in the QBF matrix and separately computes the model-count in the components and merges them at the end. Another state-of-the-art #QBF solver for the restricted case, that is, for QBFs with two quantifier alternations, is the qCounter solver [16]. qCounter tries to enumerate winning strategies systematically one by one and then tries to certify that no more winning strategies exists.

2 Preliminaries

For a CNF ϕ and its variables ($\text{vars}(\phi)$), a partial assignment α is a mapping from some variables ($\text{vars}(\alpha) \subseteq \text{vars}(\phi)$) to $\{0, 1\}$. $\phi|_\alpha$ (read as restricting ϕ with α) denotes substituting values of $\text{vars}(\alpha)$ from α into ϕ . If $\phi|_\alpha$ is true, α satisfies ϕ .

Quantified Boolean Formulas (QBFs) are an extension of propositional Boolean formulas where each variable is quantified with one of $\{\exists$ (existential), \forall (universal) $\}$. In this paper, QBFs (represented as $Q.\phi$) are of the form $Q_1 X_1 \dots Q_p X_p . \phi(X_1 \cup \dots \cup X_p)$, where X_i s are disjoint sets of variables; $Q_i \in \{\exists, \forall\}$ and $Q_i \neq Q_{i+1}$, Q is the quantifier prefix with p alternations and the matrix ϕ is a CNF. The outermost (resp. innermost) quantified variables are X_1 (resp. X_p). If $x \in X_i$, for any $y \in X_j$ where $j < i$, we say y occurs to the left of x in Q (i.e. $y \leq_Q x$). $L_Q(x)$ is the set of \forall -variables to the left of an \exists -variable x .

We can understand the semantics of QBFs as a game between a \forall and an \exists player, i.e., in the i^{th} step the player corresponding to Q_i assigns a Boolean value to each variable in X_i . At the end, the \exists (resp. \forall) player wins if substituting this complete assignment of variables in ϕ evaluates to 1 (resp. 0). An \exists **strategy** is a set \mathcal{S} containing a Boolean function S_x for each $x \in \text{vars}_\exists(Q)$, called Skolem functions. The Skolem function for x depends only on the variables in $L_Q(x)$, i.e. S_x only takes $|L_Q(x)|$ -many arguments, corresponding to the values of the universal variables in $L_Q(x)$, that would be played before x .

Formally, for a true QBF $Q.\phi$, existential strategy \mathcal{S} is $\{S_x(L_Q(x)) \mid x \in \text{vars}_\exists(Q)\}$. The **winning strategy** for \exists is a strategy that for every possible assignment of $\text{vars}_\forall(Q)$, the Skolem functions of the strategy respond on $\text{vars}_\exists(Q)$ so that the QBF matrix is satisfied

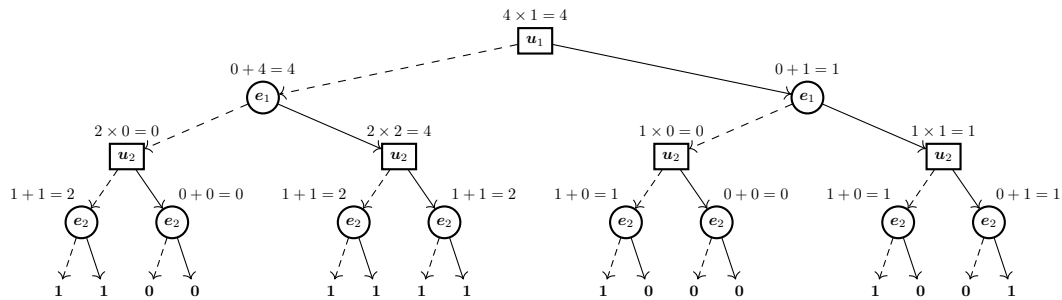
under the joint assignment to \exists and \forall variables. A QBF is true iff there exists a winning strategy for the \exists -player [1]. TQBF is the set of all true QBFs. There is a dual notion of falsity (FQBF) for winning strategies (sets of Herbrand functions) for the \forall -player, defined in a similar manner. Given a QBF, the problem of #QBF is to compute the number of winning strategies for its \exists -player. We can also extend the concept of restriction to functions which respect some total order of variables. E.g., if $A := \{z = f(x, y), y = g(x)\}$, and the ordering of variables is $x \leq y \leq z$, $\phi|_A$ denotes z substituted with $f(x, y)$, then y with $g(x)$.

A QBF $Q.\phi$ can be represented as a full binary **assignment tree** where nodes in every level are labelled with one variable in the order of Q (i.e., the root is the outermost variable). Two outgoing edges from every node are labelled with 0 or 1. The leaves are labelled with 0/1, which is the value that ϕ evaluates to when substituted with the complete assignment according to the edges on the root-to-leaf path. The satisfiability of the QBF is then computed in a bottom-up fashion (in the assignment tree) with the syntactic meaning of the variables. Here, we define subtree of the assignment tree as containing the root and at least one leaf. A **model-tree** (winning strategy) of a true QBF in this representation is a subtree that satisfies the following conditions:

- it contains one outgoing edge for nodes with an \exists -variable and two outgoing edges for nodes with an \forall -variable,
- and all its leaves are labeled 1s.

Given a true QBF, we can count the number of model-trees combinatorially with a bottom-up procedure as follows. First, consider the 0/1 values at the leaves as natural numbers, and proceed to their parents. At a node with an \exists -variable, add the values of the children as we only need one outgoing edge in a model-tree. Otherwise, if the node has a \forall -variable, multiply the values of the children as we need both outgoing edges in a model-tree. Finally at the root, the value equals the #QBF answer. We illustrate this calculation in the following example, which we use as a running example throughout.

► **Example 1.** Let $\Phi := \forall u_1 \exists e_1 \forall u_2 \exists e_2 . (e_1 \vee \bar{u}_2) \wedge (\bar{u}_1 \vee u_2 \vee \bar{e}_2) \wedge (\bar{u}_1 \vee \bar{u}_2 \vee e_2)$. The complete assignment tree of Φ is shown in Figure 1 for convenience. The node labels show how the calculation proceeds as per the bottom-up procedure for calculating the #QBF answer.



■ **Figure 1** Assignment tree of the QBF Φ from Example 1 (solid edge is 1 and dashed edge is 0)

The #QBF(Φ) from Figure 1 is 4, as denoted by the value at the root. Also, for instance, an explicit winning strategy from the same Figure 1 is, $\mathcal{S} = \{S_{e_1} = 1, S_{e_2} = u_2\}$.

Verifying that two strategies are different: Given two strategies $\mathcal{S}_1, \mathcal{S}_2$ of \exists -player for a QBF

$Q.\phi$, they are different if for some complete assignment α to the \forall variables (witness assignment), $\mathcal{S}_1, \mathcal{S}_2$ output different values for at least one of the Skolem functions corresponding to some \exists -variable x . That is, given two winning strategies $\mathcal{S}_1 = \{S_{1,x}(L_Q(x)) \mid x \in \text{vars}_{\exists}(Q)\}$ and $\mathcal{S}_2 = \{S_{2,x}(L_Q(x)) \mid x \in \text{vars}_{\exists}(Q)\}$, they are different if there exists an $x \in \text{vars}_{\exists}(Q)$ and a witness assignment α to $\text{vars}_{\forall}(Q)$ such that $S_{1,x}(\alpha) \neq S_{2,x}(\alpha)$ (here, $S_{1,x}(\alpha)$ ignores the values of the \forall -variables of α which are not in $L_Q(x)$). We opt for complete assignments for witnessing, as in general, the variable x is not known in advance). Given a witness assignment, it is easy to verify that the two strategies are different.

Verifying correctness of a winning strategy: In the QBF matrix, replacing all occurrences of \exists -variables with the Skolem functions of the given strategy leads to a propositional statement with only \forall -variables in it. A proof that this is a tautology certifies it is a winning strategy.

We use the Cook-Reckhow [10] notion of a proof system as a sound and complete polynomial time checking function. For proof systems g_1, g_2 for a language L , g_1 is exponentially separated from g_2 if there is a family of $x \in L$ for which there are small sized g_1 -proofs but require exponential size g_2 -proofs. For FQBFs (set of false QBFs), we can provide refutations by combining propositional inference with a rule for handling universal variables. ‘ \forall red’ allows us to perform a 0 or 1 substitution on a universal variable u , appearing in a conjunct (i.e. any derived line). The condition is that no other variable quantified to the right of u is in that particular conjunct.

Q-Res [14] is a FQBF proof system which allows the \forall red rule and the propositional Resolution rule [17] when the pivot is an existential variable, to construct refutations which eventually derive a \perp from the input QBF. In the FQBF-refutations we provide in this paper we will use Frege+ \forall red [4] system. Frege systems consist of a complete set of axioms schemas that define the Boolean connectives ($\perp, \top, \neg, \rightarrow, \leftrightarrow, \wedge, \vee$), and a Modus ponens rule. Frege is chosen here because it is a powerful proof system. We will omit individual propositional inference steps.

3 Proof Systems for #QBF

Naively, we can define a rudimentary proof system for the #QBF problem. The system enumerates all k winning strategies for the given true QBF $Q.\phi$. Then, to argue the correctness of the count, the system also proves:

- the correctness of each winning strategy, which requires a tautological proof of the propositional statement obtained after replacing \exists -variables with their respective Skolem functions in $Q.\phi$,
- that the strategies are all distinct from each other, with explicit witness assignments for distinguishing each pair of winning strategies,
- that no other winning strategy exists for $Q.\phi$, which we encode succinctly (in the size of k and $Q.\phi$) as a false QBF Ψ as follows.

▷ **Claim 2.** Given a true QBF $Q.\phi$ and a set of winning strategies $\mathcal{S}_1, \dots, \mathcal{S}_k$, the following QBF is false if and only if there are no other winning strategies for $Q.\phi$:

$$\Psi := \exists \vec{\alpha}_1, \dots, \vec{\alpha}_k \ Q . \phi \wedge \bigwedge_{i \in [k]} \left(\bigwedge_{u \in U} (u \leftrightarrow \alpha_{i,u}) \rightarrow \bigvee_{y \in E} (y \not\leftrightarrow S_{i,y}(\vec{\alpha}_i)) \right)$$

where, $U = \text{vars}_{\forall}(Q)$ and $E = \text{vars}_{\exists}(Q)$. Here, we use $\vec{\alpha}_i$ as a witness assignment of the fact that any potential new winning strategy must differ from \mathcal{S}_i . $\alpha_{i,u}$ denotes the Boolean

assignment corresponding to universal variable u in $\vec{\alpha}_i$, that is $\alpha_i = \{\vec{\alpha}_{i,u} \mid u \in U\}$. $S_{i,y}$ is the Skolem function of the existential variable y in the winning strategy \mathcal{S}_i .

Proof. Consider any winning strategy \mathcal{S} for the \exists -player of Ψ , which would contain an assignment for $\vec{\alpha}_1, \dots, \vec{\alpha}_k$. Now, for Ψ to be true, \mathcal{S} must differ from each \mathcal{S}_i with $\vec{\alpha}_i$ as a witness. Moreover, the Skolem functions in \mathcal{S} for each $x \in \text{vars}_{\exists}(Q)$ must also satisfy ϕ on each assignment to $\text{vars}_{\forall}(Q)$. Hence, any winning strategy for Ψ corresponds to a $k + 1^{\text{th}}$ distinct winning strategy for $Q.\phi$, and vice-versa. Therefore, Φ is a false QBF if and only if there are no other winning strategies for $Q.\phi$. \triangleleft

Observe that, as opposed to the qCounter solver [16], our naive system is capable of certifying the correct #QBF number of winning strategies and with no restrictions on the number of alternations on the given QBF. However, any such system has trivial lower bounds whenever the number of distinct winning strategies is (doubly) exponential.

3.1 An Expansion-based #QBF Proof System: $\forall\text{Exp}+\text{MICE}$

We can avoid an enumerative approach to build more advanced proof systems. The expansion-based approach [13] for QBF solving is a well studied technique which can be applied for #QBF. This can be used to transform the #QBF problem to a #SAT problem while preserving the model count.

To be precise, given a QBF $Q.\phi$, one can expand it over all universal variable assignments so that the resulting formula consists of clauses over only existential variables. To keep track of the existential variable dependency on the universal variables, annotate the existential variable e with an assignment α_e to $L_Q(e)$ and denote it as a new existential variable e^{α_e} , as described in [13].

Formally, the following rule is allowed to download an axiom in expansion-based systems:

$$\overline{\{e^{\alpha_e} \mid e \in C \text{ and } e \in \text{vars}_{\exists}(Q)\} \cup \{\alpha(u) \mid u \in C \text{ and } u \in \text{vars}_{\forall}(Q)\}},$$

where $C \in \phi$, α is an assignment to all $\text{vars}_{\forall}(Q)$. α_e is the partial assignment from α to variables in $L_Q(e)$ when $e \in \text{vars}_{\exists}(Q)$.

For example, consider a QBF $\exists e_1 \forall u_1 \exists e_2 \forall u_2 \exists e_3. (e_1 \vee u_1 \vee e_2 \vee \bar{u}_2 \vee e_3) \wedge (\bar{u}_1 \vee \bar{e}_2)$. Let $\alpha = \{u_1 = 0, u_2 = 1\}$ be the assignment to all universal variables of the QBF, then the corresponding clauses in the expanded CNF are $(e_1 \vee 0 \vee e_2^{u_1/0} \vee 0 \vee e_3^{u_1/0, u_2/1}), (1 \vee \bar{e}_2^{u_1/0})$. After expanding the QBF over all assignments to the universal variables, we obtain a SAT instance, such that its models are in bijective correspondence with the models of the QBF. We state this formally below.

► **Proposition 3.** *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.*

Before proving the bijection of Proposition 3 for general QBFs, we would like to discuss a simple case below for the sake of intuition.

► **Example 4.** Consider a QBF Φ with one universal variable u , existential variables x_1, \dots, x_n , and its CNF matrix ' χ '. Assume that each x_i depends on u . After expansion, the CNF obtained is $\phi = \chi(u = 0, x_1^{u/0}, \dots, x_n^{u/0}) \wedge \chi(u = 1, x_1^{u/1}, \dots, x_n^{u/1})$.

Any model of ϕ assigns a value to each $(x_i^{u/0} = a_{i,0})$ and $(x_i^{u/1} = a_{i,1})$, such that ϕ is satisfied. The corresponding model of the QBF Φ chooses $(x_i = a_{i,b})$ when $u = b$. Given two

different models for ϕ , they must differ at some $(x_i^{u/b})$. Then, the corresponding winning strategies also differ, as the Skolem function for x_i will differ at $u = b$.

Conversely, consider a winning strategy \mathcal{S} for Φ with $\{S_{x_i}(u)\}$ as the individual Skolem functions. The corresponding satisfying assignment for ϕ assigns $x_i^{u/b} = S_{x_i}(b)$. Again, two different winning strategies lead to different satisfying assignments. Hence, we establish the required bijection for Φ .

Proof of Proposition 3. Consider a QBF formula $\Phi = Q.\chi$ with the universal variables u_1, \dots, u_m , existential variables x_1, \dots, x_n , and the CNF matrix $\chi(u_1, \dots, u_m, x_1, \dots, x_n)$. After complete semantic expansion of Φ , the SAT instance we obtain is:

$$\phi := \bigwedge_{\alpha \in \langle u_1, \dots, u_m \rangle} \chi(u_1 \dots u_m = \alpha, \{x_i^{L_Q(x_i)/\alpha[L_Q(x_i)]} \mid \text{for } i \in [n]\})$$

where $\langle U \rangle$ is the set of all complete assignments to variables in U , $L_Q(x)$ is the set of all universal variables occurring to the left of the existential variable x in Q . $\alpha[L_Q(x)]$ is the set of individual 0/1-assignments from α for variables in $L_Q(x)$. For example, if $\alpha = \{u_1 = 0, u_2 = 1, u_3 = 0\}$ then $\alpha[u_2, u_3] = [1, 0]$ and $\{u_2, u_3\}/\alpha[u_2, u_3] = \{u_2 = 1, u_3 = 0\}$.

Now, any assignment to this SAT formula is of the form $x_i^{L_Q(x_i)/\alpha[L_Q(x_i)]} = a_{i,\alpha[L_Q(x_i)]}$, where $a_{i,\alpha[L_Q(x_i)]} \in \{0, 1\}$, $\alpha \in \{0^m, \dots, 1^m\}$ and $i \in [n]$. Below we show that any satisfying assignment $(x_i^{L_Q(x_i)/\alpha[L_Q(x_i)]} = a_{i,\alpha[L_Q(x_i)]})$ corresponds to a winning strategy of the QBF Φ where, the existential player chooses $x_i = a_{i,\alpha[L_Q(x_i)]}$ if the universal chooses $u = \alpha$ and vice-versa.

One direction is easy: when a satisfying assignment for ϕ is known the corresponding winning strategy is simply to choose x_i to be $a_{i,\alpha[L_Q(x_i)]}$. In the other direction: when a winning strategy \mathcal{S} for Φ (i.e. $\{S_{x_i}(L_Q(x_i))\}$) is known the corresponding satisfying assignment would be to set $x_i^{L_Q(x_i)/\alpha[L_Q(x_i)]} = S_{x_i}(\alpha[L_Q(x_i)])$.

This is clearly a bijective correspondence, as any two distinct assignments, would differ in at least one $x_i^{L_Q(x_i)/\alpha[L_Q(x_i)]}$ value and the corresponding strategies would need to be different as $S_{x_i}(\alpha[L_Q(x_i)])$ is just a Boolean value and to represent both 0 and 1 (from both assignments), would require two different S_{x_i} functions and vice-versa. \blacktriangleleft

In $\forall\text{Exp}+\text{MICE}$, one needs to expand the QBF with all possible assignments to universal variables. Otherwise, if one expands on a smaller set of assignments to obtain a CNF $\phi' \subset \phi$, one can only guarantee $\#\text{QBF}(\Phi) \leq \#\text{SAT}(\phi')$. This is because, for any CNF ϕ' obtained after dropping a few clauses from a CNF ϕ , we have $\#\text{SAT}(\phi') \geq \#\text{SAT}(\phi)$.

► Corollary 5. *For any #SAT proof system \mathcal{P} , the proofs in the #QBF proof system $\forall\text{Exp}+\mathcal{P}$ for a QBF Φ need exponential size in terms of $|\text{vars}_\forall(\Phi)|$.*

3.2 A Line-based #QBF Proof System: Q-MICE

In $\forall\text{Exp}+\text{MICE}$, eliminating all universal quantifiers at the beginning of the proof can cause an exponential explosion, even where the model count may otherwise be straightforward. In this section, we introduce a line-based #QBF proof system Q-MICE. The idea is that interleaving quantifier handling and other rules allows better control of the proof size in instances where the model count ought to be easy to determine. Q-MICE is inspired from MICE for #SAT [11]. A claim in MICE is of the form (F, A, c) where F is a CNF formula, A is a partial assignment, and c is the correct number of satisfying assignments to $F|_A$. Below, we define the Q-MICE system for #QBF along similar lines, borrowing notations from [5] for ease.

3.2.1 Inference rules for Q-MICE

In Q-MICE, we use the claims of the following format: $(Q.F, A, c)$, where Q is the quantifier prefix. F is a CNF formula (matrix), c is a non-negative integer written in decimal¹ and A is a partial strategy. In a partial strategy A , some of the \exists -variables x are allotted strategies in the form of a Skolem function $S_x(L_Q(x))$. The set of variables which has allotted strategies in A is represented by $\text{vars}(A)$. One representation for the Skolem functions in A is via Boolean circuits, one for each $x \in \text{vars}(A)$. In this representation, A becomes a collection of circuits.

A claim $(Q.F, A, c)$ is said to be a **valid claim** if c is the correct number of ways to extend A to get a winning strategy A' (by assigning strategies to the remaining \exists -variables) for the \exists -player in $Q.F$. The **size** of a claim is the number of symbols needed to represent the claim in some fixed representation. For example, circuits in A can be represented as CNFs using Tseitin transformation [20]. We need the following definitions for Q-MICE.

► **Definition 6** (Restriction of \forall -variables in a QBF). *Let $Q.F$ be a QBF. By a restriction of the \forall -variable $(y = b \in \{0, 1\})$ in a QBF $Q.F$ (denoted as $Q.F|_{\{y=b\}} = Q'.F \wedge (y = b) = Q'.F'$), we mean that the quantification of y is flipped to \exists in the prefix Q' and an additional unit clause forcing the restriction $y = b$ (i.e. if $b = 1$ then (y) else (\bar{y})) is added in the matrix. All other clauses in F remain.*

We start the description of the Q-MICE system by first defining its inference steps and providing examples to illustrate their usage.

► **Definition 7** (Axiom rule). *For a QBF $Q.F$, one can derive: $\overline{(Q.F|_{\rho}, A, c)}$ where*

- (A-1) ρ is a (partial) assignment to $\text{vars}_{\forall}(Q)$ and $Q.F|_{\rho}$ is denoted as $Q'.F'$ (as in Def 6).
- (A-2) $F|_{\{\rho \cup A\}}$ is a tautology and an explicit proof of this is provided.
- (A-3) $\text{vars}(A) \subseteq \text{vars}_{\exists}(Q)$, calculate c as follows:

- Initially, $\ell = 1$. Starting from the innermost quantified variable in Q (say x):
- if $x \in \text{vars}_{\exists}(Q)$ and $x \notin \text{vars}(A)$ then: $\ell \leftarrow 2 \cdot \ell$ (i.e. double the count),
- if $x \in \text{vars}_{\forall}(Q)$ and $x \notin \text{vars}(\rho)$ then: $\ell \leftarrow \ell^2$ (i.e. square the count),
- at the end of the reverse quantification sequence, $c \leftarrow \ell$.

The intuition of Axiom rule is as follows: if ϕ be a tautology, then for any quantification Q to $\text{vars}(\phi)$, $Q.\phi$ will be a true QBF. In fact, all strategies are winning in $Q.\phi$, allowing us to easily count the number of model. For instance, in the QBF from Example 1, we can derive the following axioms: $(\Phi|_{\{u_1=0\}}, \{e_1 = 1\}, 4)$, $(\Phi|_{\{u_2=0\}}, \{e_1 = \bar{u}_1, e_2 = 0\}, 1)$, $(\Phi|_{\{u_1=1, u_2=0\}}, \{e_1 = 1, e_2 = 0\}, 1)$. Tautology proofs here are trivial.

► **Lemma 8.** *Any claim $(Q.F|_{\rho}, A, c)$ derived by using the Axiom rule of Definition 7 is valid i.e., c is the correct number of models for the QBF $Q.F|_{\rho} \wedge \bigwedge_{x \in \text{vars}(A)} (x \leftrightarrow A(x))$.*

Proof. In this rule, we find a subtree $(Q'.F' \cup A)$ of the assignment tree $(Q.F)$ which has all 1-leaves and compute all possible valid models in this subtree. This computation is just combinatorial (described in Section 2). For the correctness of this model-count, we argue inductively on the subtree $(Q'.F' \cup A)$: Base case: the model-count at the leaves is 1. Inductively, model-count at unrestricted existential nodes x i.e. $x \notin \text{vars}(A)$ (or universal nodes x i.e. $x \notin \text{vars}(\rho)$) is the addition (or multiplication) of model-counts at their two children owing to the structure of any model-tree. The remaining two cases of induction are

¹ Future improvements could use succinct integer representations to avoid trivial exponential lower bounds.

restricted existential variables x (i.e. $x \in \text{vars}(A)$) or universal variables x (i.e. $x \in \text{vars}(\rho)$) of Q . The model-count in these cases is retained from the only remaining child as both are now existentially quantified in Q' and need the only remaining outgoing edge in any model-tree. \blacktriangleleft

For a QBF $Q.F$, one can drop some variables and their strategies from the partial strategy part of the claims using one of the following composition rules. Note that all these rules require a proof for the absence of models statement, which is defined at the end.

► **Definition 9** (Composition rules). *Given a QBF $Q.F$,*

1. (Composition-a:)
$$\frac{(Q.F|_{\rho}, A_1, 1), \dots, (Q.F|_{\rho}, A_n, 1)}{(Q.F|_{\rho}, A, n)}, \text{ where}$$
 - (C-a1) for all $i \in [n]$, $\text{vars}(A_i) = \text{vars}_{\exists}(Q)$ and $\text{vars}(\rho) \subseteq \text{vars}_{\forall}(Q)$,
 - (C-a2) for $i \neq j \in [n]$, $A_i \neq A_j$ (providing assignments witnessing that A_i, A_j disagree),
 - (C-a3) $A \subseteq \bigcap_{i \in [n]} A_i$ (a subset of strategies where all A_i s are syntactically equal).
2. (Composition-b:)
$$\frac{(Q.F|_{\rho}, A_1, c_1)}{(Q.F|_{\rho}, A, c_1)}, \text{ where}$$
 - (C-b1) $A \subseteq A_1 \subseteq \text{vars}_{\exists}(Q)$ and $\text{vars}(\rho) \subseteq \text{vars}_{\forall}(Q)$.
3. (Composition-c:)
$$\frac{(Q.F|_{\rho}, A_1, c_1), \dots, (Q.F|_{\rho}, A_n, c_n)}{(Q.F|_{\rho}, A, \Sigma_{i \in [n]} c_i)}, \text{ where}$$
 - (C-c1) $\text{vars}(A_1) = \dots = \text{vars}(A_n) \subseteq \text{vars}_{\exists}(Q)$ and $\text{vars}(\rho) \subseteq \text{vars}_{\forall}(Q)$,
 - (C-c2) for $i \neq j \in [n]$, $A_i \neq A_j$ and $A \subseteq \bigcap_{i \in [n]} A_i$.
 - (C-c3) Let x be the innermost \exists -variable in Q such that $x \in \text{vars}(A_1) \setminus \text{vars}(A)$.
 - For all $y \in \text{vars}_{\exists}(Q)$ and $y \leq_Q x \implies y \in \text{vars}(A_i)$.
 - For all $y \in \text{vars}_{\forall}(Q)$ and $y \leq_Q x \implies y \in \text{vars}(\rho)$.

For ease, we denote $Q.F|_{\rho}$ as $Q'.F'$ in these rules. All these rules additionally need an FQBF-proof of the **absence of models statement**: $\Psi := Q'.F' \cup A \cup \{\overline{A_i} \setminus \overline{A}\}_{i \in [n]}$ where n is the number of hypothesis claims. Ψ encodes as a QBF the negation of the fact that there exists no other winning strategies for the \exists -variables in $\text{vars}(A_i) \setminus \text{vars}(A)$. The exact encoding of this statement is provided in the next claim.

▷ **Claim 10.** Ψ in the composition rules (Definition 9) can be encoded as a short QBF.

Proof. This encoding is a generalization of that defined in Claim 2. For an input QBF $Q.F$, the composition rule in general is of the form where there are n partial strategies A_1, \dots, A_n over the same set of existential variables $X \subseteq \text{vars}_{\exists}(Q)$ in the hypothesis, and a subset of these strategies ($X' \in X$) which appear in all of them are retained as A in the conclusion. The ‘absence of models’ statement encodes that there are no other winning strategies (in $Q'.F'$) for the variables in $X \setminus X'$ when also adhering to strategies from A .

Recall that A_i s are a set consisting of one function $S_{A_i, x}$ for every $x \in \text{vars}(A_i)$. So, in $Q'.F'$, enforcing the strategies in A is simply adding clauses $(x \leftrightarrow S_{A, x})$ for every $x \in X'$.

Now to see if there is any $n + 1^{\text{th}}$ winning strategy for variables $\in X \setminus X'$, we need it to be different than those already in the hypotheses. As discussed in Section 2, for two strategies to be considered different, there must be some witness assignment (α below) to \forall -variables of Q' (say U') such that the value of the function computed by these strategies is different. Now, if the following QBF encoding is true, it implies that there indeed is a $n + 1^{\text{th}}$ strategy which is missing in the hypothesis and the rule cannot be used.

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

However, if the above encoding is a false QBF, it certifies that there is no such missed strategy and we can proceed to drop the strategy restrictions on variables $\in X \setminus X'$. \triangleleft

The intuition for the composition rules: Composition-a is useful to directly count complete winning strategies. Composition-b is useful when some variables have unique winning Skolem functions in the subtree. Composition-c is useful for combining subtrees which all agree on the restrictions of universal variables and individually are a path graph from the root to the innermost variable where the hypotheses strategies differ.

For instance, in the QBF from Example 1, $\Phi := \forall u_1 \exists e_1 \forall u_2 \exists e_2 . (e_1 \vee \bar{u}_2) \wedge (\bar{u}_1 \vee u_2 \vee \bar{e}_2) \wedge (\bar{u}_1 \vee \bar{u}_2 \vee e_2)$ we can derive the following claims. Using composition-b, we can derive:

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

The absence of models statement Ψ is:

$$\exists \alpha_1 \exists u_1 \exists e_1 \forall u_2 \exists e_2 . (e_1 \vee \bar{u}_2) \vee (\bar{u}_1 \vee u_2 \vee \bar{e}_2) \wedge (\bar{u}_1 \vee \bar{u}_2 \vee e_2) \wedge (u_1) \wedge (e_1) \wedge ((u_2 = \alpha_1) \rightarrow (e_2 \neq \alpha_1))$$

For an FQBF-proof of Ψ in Frege+ \forall red [4], we use propositional inferences to derive $(u_2 \vee \alpha_1)$ and $(\bar{u}_2 \vee \bar{\alpha}_1)$. Using universal reduction to drop variable u_2 , we can derive (α_1) and $(\bar{\alpha}_1)$, which gives the needed contradiction.

Using composition-a (or -c) we can derive the following:

$$\frac{(\Phi|_{u_1=0, u_2=0}, \{e_1 = 0, e_2 = 0\}, 1), (\Phi|_{u_1=0, u_2=0}, \{e_1 = 0, e_2 = 1\}, 1)}{(\Phi|_{u_1=0, u_2=0}, \{e_1 = 0\}, 2)}$$

Here, the corresponding absence of models statement is trivially false.

► **Lemma 11.** *Any claim $(Q'.F', A, c')$ derived by using the composition rules of Definition 9 from valid hypothesis claims is also valid.*

Proof. In composition-a, every hypothesis claim considers a full strategy for the existential player. That is, each hypothesis is a distinct model for the subtree corresponding to $Q'.F' \cup A$ and no other models exist for the same (due to absence of models proof). Therefore, adding them up is the correct number of models for the formula $Q'.F' \cup A$.

In composition-b, there is only one hypothesis strategy for variables in $\text{vars}(A_1) \setminus \text{vars}(A)$ and no other winning strategies are possible due to the absence of models proof. So, there is only one useful branch from these \exists -variables in the subtree of the assignment tree, and these branches need to be in any model tree. Therefore, the count at the root remains the same.

In composition-c, x is the innermost variable from $\text{vars}(A_i) \setminus \text{vars}(A)$ and every variable to the left of x either has some strategy in every A_i or is restricted with 0/1 in the QBF. Hence, the corresponding subtree of the assignment tree for these hypotheses is a line graph from root to x . Let y be the outermost variable from $\text{vars}(A_i) \setminus \text{vars}(A)$. In the subtree corresponding to $Q'.F' \cup A$, it is a line graph up to y and it only branches on every \exists -variable in $\text{vars}(A_i) \setminus \text{vars}(A)$ up to x and at x it has one branch with count c_i and the other with count 0 (due to the absence of models proof). Now the total count at y -node is just combinatorial and equal to $\sum_{i \in n} c_i$. As it is just a line graph until the root, this value propagates as is. \blacktriangleleft

For a QBF $Q.F$, one can drop the \forall -variable restrictions using the following join rule.

► **Definition 12** (Join rule). *For a QBF $Q.F$, one can derive*

$$\frac{(Q.F|_{\rho \cup \{y=0\}}, A, c_1), (Q.F|_{\rho \cup \{y=1\}}, A, c_2)}{(Q.F|_{\rho}, A, c_1 \cdot c_2)}$$

when the following conditions are satisfied:

(J-1) ρ should be a (partial) assignment to $\text{vars}_\forall(Q)$ and $\text{vars}(A) \subseteq \text{vars}_\exists(Q)$.

For ease, the quantifier in both antecedents is Q' and $Q.F|_\rho$ is denoted as $Q''.F_3$.

(J-2) $y \in \text{vars}_\forall(Q)$, $y \in \text{vars}_\exists(Q')$, $y \in \text{vars}_\forall(Q'')$ and unit clauses (y) , (\bar{y}) are dropped.

(J-3) For all $x \in \text{vars}_\exists(Q)$ and $x \leq_Q y \implies x \in \text{vars}(A)$.

(J-4) For all $x \in \text{vars}_\forall(Q)$ and $x \leq_Q y \implies x \in \text{vars}(\rho)$.

The intuition behind the join rule is to combine two subtrees (say G_1, G_2) agreeing everywhere except for one restriction of a \forall -variable (y) and G_1, G_2 are simple path graphs from the root to y . In Example 1, $\Phi := \forall u_1 \exists e_1 \forall u_2 \exists e_2 . (e_1 \vee \bar{u}_2) \wedge (\bar{u}_1 \vee u_2 \vee \bar{e}_2) \wedge (\bar{u}_1 \vee \bar{u}_2 \vee e_2)$, using join we can derive:

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

► **Lemma 13.** Any claim $(Q.F|_\rho, A, c_1 \cdot c_2)$ derived by using the join rule of Definition 12 from valid hypothesis claims is also valid.

Proof. In the hypothesis, y is a \forall -variable of $Q.F$ which is restricted and is now a \exists -variable in Q' . Every variable to the left of y either has some strategy in A or is restricted with 0/1 in ρ (due to J-3, J-4). Hence, the corresponding subtree of the assignment tree for these hypotheses is a path graph from root to y . The counts at root of hypotheses are the same at the y -node. Now, the conclusion subtree $(Q''.F_3 \cup A)$ is similarly a path graph from root up to y and at y branches with 0, 1. Now, any model of this subtree should have both branches in its model-tree, therefore $c_1 \cdot c_2$ is the correct number of models in the subtree. ◀

We now define the #QBF proof system Q-MICE using the inference rules introduced above.

► **Definition 14 (Q-MICE).** A Q-MICE proof of a QBF $Q.F$ with k winning strategies for the existential player is a sequence of lines L_1, \dots, L_s where L_s contains the claim $(Q.F, \emptyset, k)$ and every line L_i for $i \in [s]$ is derived by one of the following rules:

1. Axiom rule from Definition 7 along with the required tautology proof.
2. One of the Composition rules from Definition 9 with hypothesis from L_1, \dots, L_{i-1} , along with witnesses separating the hypothesis (partial) strategies, and absence of models proof
3. Join rule from Definition 12 with hypothesis from L_1, \dots, L_{i-1} .

The ‘length’ of a Q-MICE proof is the number of lines in it, and its ‘size’ is the size of all claims along with additional witnesses, FQBF-proofs and tautology proof sizes.

A complete Q-MICE proof of Φ from Example 1 is as follows:

► **Example 15.** The QBF from Example 1, $\Phi := \forall u_1 \exists e_1 \forall u_2 \exists e_2 . (e_1 \vee \bar{u}_2) \wedge (\bar{u}_1 \vee u_2 \vee \bar{e}_2) \wedge (\bar{u}_1 \vee \bar{u}_2 \vee e_2)$, has a Q-MICE proof as follows:

$L_1 := (\Phi|_{\{u_1=0\}}, \{e_1 = 1\}, 4)$ (Axiom, tautology proof is easy)

$L_2 := (\Phi|_{\{u_1=1\}}, \{e_1 = 1, e_2 = u_2\}, 1)$ (Axiom, tautology proof is easy)

$L_3 := (\Phi|_{\{u_1=1\}}, \{e_1 = 1\}, 1)$ (Composition-b on L_2)

■ The absence of models statement is: $\Psi_1 := \exists \alpha_2 \exists u_1 \exists e_1 \forall u_2 \exists e_2 . (e_1 \vee \bar{u}_2) \vee (\bar{u}_1 \vee u_2 \vee \bar{e}_2) \wedge (\bar{u}_1 \vee \bar{u}_2 \vee e_2) \wedge (u_1) \wedge (e_1) \wedge ((u_2 = \alpha_2) \rightarrow (e_2 \neq \alpha_2))$.

■ FQBF-proof of Ψ_1 in Q-Res [14] is as follows after unit propagation steps:

$$\frac{\begin{array}{c} \text{(Res)} \frac{(u_2 \vee \bar{e}_2) \quad (u_2 \vee \alpha_2 \vee e_2)}{(\forall\text{red}) \frac{(u_2 \vee \alpha_2)}{(\alpha_2)}} \quad \frac{(\bar{u}_2 \vee e_2) \quad (\bar{u}_2 \vee \bar{\alpha}_2 \vee \bar{e}_2)}{(\forall\text{red}) \frac{(\bar{u}_2 \vee \bar{\alpha}_2)}{(\bar{\alpha}_2)}} \quad \text{(Res)} \\ \hline \perp \end{array}}{\text{(Res)}}$$

$L_4 := (\Phi, \{e_1 = 1\}, 4)$ (Join on L_1, L_3)

$L_5 := (\Phi, \emptyset, 4)$ (Composition-b on L_4)

■ The absence of models statement is: $\Psi_2 := \exists \alpha_1 \forall u_1 \exists e_1 \forall u_2 \exists e_2 . (e_1 \vee \bar{u}_2) \wedge (\bar{u}_1 \vee u_2 \vee \bar{e}_2) \wedge (\bar{u}_1 \vee \bar{u}_2 \vee e_2) \wedge ((u_1 \neq \alpha_1) \rightarrow (e_1 \neq 1))$

■ FQBF-proof of Ψ_2 in Q-Res [14] is as follows:

$$\begin{array}{c} \text{(Res)} \frac{\frac{(u_1 \vee \alpha_1 \vee \bar{e}_1)}{(u_1 \vee \alpha_1)} \quad \frac{(e_1 \vee \bar{u}_2)}{(e_1)} \quad (\forall\text{red}) \quad \frac{(e_1 \vee \bar{u}_2)}{(e_1)} \quad \frac{(\bar{u}_1 \vee \bar{\alpha}_1 \vee \bar{e}_1)}{(\bar{u}_1 \vee \bar{\alpha}_1)} \quad (\text{Res})}{(\alpha_1)} \quad (\forall\text{red}) \quad \frac{(\bar{u}_1 \vee \bar{\alpha}_1)}{(\bar{\alpha}_1)} \quad (\forall\text{red})}{} \\ \perp \end{array}$$

► **Theorem 16.** Q-MICE is a polynomial-time verifiable sound and complete #QBF system.

Proof. Since all the inference rules are sound (Lemmas 8,9,13), the Q-MICE proof system is sound. For completeness: Use the Axiom rule for every winning strategy of $Q.F$ with $c = 1$. Using Composition-a rule with $A = \emptyset$, add these axiom claims to derive the correct #QBF answer: If you consider all winning strategies in the absence of models statement, it is indeed a false QBF and any complete FQBF-proof system suffices. Also every rule of Q-MICE is easily verifiable, hence any Q-MICE-proof is verifiable in time polynomial in the proof-size. ◀

Note that if the input QBF is false, one can use any one of the composition rules with no hypothesis strategies to derive the answer that #QBF answer is 0. However, this is equivalent to directly using a FQBF proof system to prove that the input QBF is false.

4 Upper bounds

In this section, we show the strength of Q-MICE by proving upper bounds for two example QBF families that have roots in theory [5] and practice [12], respectively.

4.1 A QBF family based on XOR-PAIRS

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

$\mathcal{Q}.\oplus_n$ has n^2 variables out of which n are universal variables, hence it requires super-polynomial ($\Omega(2^n)$) sized proofs in the $\forall\text{Exp}+\text{MICE}$ system (Corollary 5).

Below, we show that $\mathcal{Q}.\oplus_n$ has a constant length and polynomial size Q-MICE proof $\pi = \{L_1, L_2\}$, where L_1 is derived using the Axiom rule consisting of the entire QBF $\mathcal{Q}.\oplus_n$, a complete winning strategy $A = \{S_{x_{i,j}} = u_i \oplus u_j \mid i \neq j \in [n]\}$ and the count 1, accompanied by a tautology proof of $\oplus_n \mid_A$. Line L_2 is derived by applying the Composition-b rule on L_1 by dropping the strategy restrictions in A accompanied by a FQBF proof of the absence of models statement. This maintains the previous count, hence $\#\text{QBF}(\mathcal{Q}.\oplus_n) = 1$. Precisely:

(Axiom rule) $L_1 := (\mathcal{Q}.\oplus_n, A := \{S_{x_{i,j}} = u_i \oplus u_j \mid i \neq j \in [n]\}, 1)$; the tautology proof of $\oplus_n \mid_A$ is a straightforward case of any introduction rule of \leftrightarrow in any Frege system.

(Composition-b rule) $L_2 := (\mathcal{Q}.\oplus_n, \emptyset, 1)$; the absence of models statement as per Claim 10 is:

$$\begin{array}{l} \Psi := \exists \bar{\alpha}_1 \forall u_1, \dots, u_n \exists_{i \neq j \in [n]} x_{i,j} . \bigwedge_{i \neq j \in [n]} (x_{i,j} \leftrightarrow u_i \oplus u_j) \\ \quad \wedge ((u_1 = \alpha_{1,u_1} \wedge \dots \wedge u_n = \alpha_{1,u_n}) \rightarrow (\bigvee_{i \neq j \in [n]} x_{i,j} \neq \alpha_{1,u_i} \oplus \alpha_{1,u_j})) \end{array}$$

FQBF proof of Ψ using Frege+ $\forall\text{red}$: (for simplicity, we denote α_{1,u_i} as α_i)

$$\begin{array}{c}
x_{i,j} \leftrightarrow u_i \oplus u_j \quad (u_1 = \alpha_1 \wedge \dots \wedge u_n = \alpha_n) \rightarrow \left(\bigvee_{i \neq j \in [n]} x_{i,j} \neq \alpha_i \oplus \alpha_j \right) \\
\hline
(u_1 = \alpha_1 \wedge \dots \wedge u_n = \alpha_n) \rightarrow \left(\bigvee_{i \neq j \in [n]} u_i \oplus u_j \neq \alpha_i \oplus \alpha_j \right) \quad (\text{Prop. Frege inference}) \\
\hline
(\alpha_1 = \alpha_1 \wedge \dots \wedge \alpha_n = \alpha_n) \rightarrow \left(\bigvee_{i \neq j \in [n]} \alpha_i \oplus \alpha_j \neq \alpha_i \oplus \alpha_j \right) \quad (\forall\text{red with } u_i = \alpha_i \text{ for } i \in [n]) \\
\hline
\perp \quad (\text{Prop. Frege inference})
\end{array}$$

4.2 An Indexed Affine QBF Family

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

The QBF Γ can be thought of as a simple encryption process, where the function for x w.r.t. the index ‘ u ’ is the encryption scheme, which is applied to the plain-text ‘ v ’ to obtain ‘ y ’ as the cipher-text. As the index u for y_u and v_u is denoted by its binary expansion represented by $u_1, \dots, u_{\log(n)}$, it’s not immediately clear how to encode the matrix as a CNF. However, u has only $\log n$ bits so one way to represent y_u, v_u is to go through each assignment $u \in \{0, 1\}^{\log n}$ in some order.

Following this idea, given an assignment to $a \in \{0, 1\}^{\log(n)}$, we create four clauses to represent the condition $(u_1 = a_1, \dots, u_{\log(n)} = a_{\log(n)}) \rightarrow (v_a = y_a \oplus \bar{x})$. For example, if $a_1 = \dots = a_{\log(n)} = 0$, the four clauses are:

$$\begin{array}{ll}
u_1 \vee \dots \vee u_{\log(n)} \vee v_0 \vee y_0 \vee x & u_1 \vee \dots \vee u_{\log(n)} \vee v_0 \vee \bar{y}_0 \vee \bar{x} \\
u_1 \vee \dots \vee u_{\log(n)} \vee \bar{v}_0 \vee y_0 \vee \bar{x} & u_1 \vee \dots \vee u_{\log(n)} \vee \bar{v}_0 \vee \bar{y}_0 \vee x
\end{array}$$

Similarly, for each $a' \neq a$, we create four clauses to represent the condition $(u_1, \dots, u_{\log(n)}) = (a_1, \dots, a_{\log(n)}) \rightarrow v_{a'} = y_{a'} \oplus x$. In total, we have $O(n)$ clauses for each assignment $a \in \{0, 1\}^{\log(n)}$, hence, the resulting CNF has $O(n^2)$ clauses.

Based on the values of $u = \langle u_1, \dots, u_{\log n} \rangle$, x and all v_i for $i \in [n]$, there is a single way to pick the value of all y_i s for $i \in [n]$ to make Γ true and the number of possible Skolem functions for x (i.e. $S_x(u_1, \dots, u_{\log(n)})$) is 2^n . Since Γ has $n + \log n$ \forall -variables and 2^n winning strategies, it requires exponential-size proofs in both the naive system and $\forall\text{Exp}+\text{MICE}$ (Corollary 5).

A linear length and polynomial size Q-MICE proof for Γ is as follows (for ease, we represent $\langle u_1 \dots u_{\log n} \rangle$ as \vec{u}): For each $\beta \in [n]$, derive the following (below $i \in [n] \setminus \beta$):

$$\begin{array}{c}
\frac{}{(\Gamma|_{\vec{u}=\beta}, \{x=0, y_\beta = \bar{v}_\beta, y_i = v_i\}, 1)} \quad (\text{Axiom}) \quad \frac{}{(\Gamma|_{\vec{u}=\beta}, \{x=1, y_\beta = v_\beta, y_i = \bar{v}_i\}, 1)} \\
\frac{}{(\Gamma|_{\vec{u}=\beta}, \{x=0\}, 1)} \quad (\text{Comp-b}) \quad \frac{}{(\Gamma|_{\vec{u}=\beta}, \{x=1\}, 1)} \\
(\text{Comp-c}) \quad \frac{}{L_\beta := (\Gamma|_{\vec{u}=\beta}, \emptyset, 2)}
\end{array}$$

We used composition-b and composition-c rules in the above derivation. These rules require an FQBF proof of the corresponding absence of models statements. We next describe the absence of model statement for the composition-b rules. For ease, we represent $\langle v_1 \dots v_n \rangle$ as \vec{v} below. For each $\beta \in [n]$ and $q \in \{0, 1\}$, we give the absence of models statement $\Psi_{\beta, x=q}$ for the Composition-b rule below (for ease, we only show useful clauses in the matrix):

$$\Psi_{\beta, x=q} := \exists \vec{\alpha}_1 \exists \vec{u} \exists x \forall \vec{v} \exists y_1, \dots, y_n \cdot (\vec{u} = \beta \rightarrow (v_\beta = y_\beta \oplus \bar{x}) \wedge \bigwedge_{i \in [n] \setminus \beta} (v_i = y_i \oplus x)) \\
\wedge (x = q) \wedge (\vec{u} = \beta) \wedge \left((\vec{v} = \vec{\alpha}_1) \rightarrow (y_\beta \neq \alpha_{1, v_\beta} \oplus \bar{x}) \vee \bigvee_{i \in [n] \setminus \beta} (y_i \neq \alpha_{1, v_i} \oplus x) \right)$$

FQBF proof of $\Psi_{\beta, x=q}$ in Frege+ \forall red proof system (after propagating $x = q$ and $\vec{u} = \beta$) is given below. For simplicity we denote α_{1, v_i} as α_i and the soundness of inference-lines A, B, C are explained after the derivation:

$$\begin{array}{c}
\frac{(v_\beta = y_\beta \oplus \bar{q}) \wedge \bigwedge_{i \in [n] \setminus \beta} (v_i = y_i \oplus q) \left((\vec{v} = \vec{\alpha}_1) \rightarrow (y_\beta \neq \alpha_\beta \oplus \bar{q}) \vee \bigvee_{i \in [n] \setminus \beta} (y_i \neq \alpha_i \oplus q) \right)}{\left((\vec{v} = \vec{\alpha}_1) \rightarrow (v_\beta \oplus \bar{q} \neq \alpha_\beta \oplus \bar{q}) \vee \bigvee_{i \in [n] \setminus \beta} (v_i \oplus q \neq \alpha_i \oplus q) \right)} \quad (A) \\
\frac{\left((\vec{v} = \vec{\alpha}_1) \rightarrow (v_\beta \oplus \bar{q} \neq \alpha_\beta \oplus \bar{q}) \vee \bigvee_{i \in [n] \setminus \beta} (v_i \oplus q \neq \alpha_i \oplus q) \right)}{\left((\vec{\alpha}_1 = \vec{\alpha}_1) \rightarrow (\alpha_\beta \oplus \bar{q} \neq \alpha_\beta \oplus \bar{q}) \vee \bigvee_{i \in [n] \setminus \beta} (\alpha_i \oplus q \neq \alpha_i \oplus q) \right)} \quad (B) \\
\frac{\left((\vec{\alpha}_1 = \vec{\alpha}_1) \rightarrow (\alpha_\beta \oplus \bar{q} \neq \alpha_\beta \oplus \bar{q}) \vee \bigvee_{i \in [n] \setminus \beta} (\alpha_i \oplus q \neq \alpha_i \oplus q) \right)}{\perp} \quad (C)
\end{array}$$

In this FQBF proof, we are only left with the soundness of inference lines A,B and C. For (A), the hypothesis is the input QBF and the conclusion is derived by propositional Frege inferences which substitute y_i, y_β variables with the functions $v_i \oplus q, v_\beta \oplus \bar{q}$ respectively. To derive (B), since \vec{v} are the rightmost variables in the hypothesis clause, the conclusion is derived by a \forall red rule which substitutes $\vec{v} = \vec{\alpha}_1$. Finally, the hypothesis in (C) is a contradiction as it's equivalent to $\text{true} \rightarrow \text{false}$, allowing us to derive \perp .

For each $\beta \in [n]$, the absence of models statement for the Composition-c rule is :

$\Psi_\beta := \exists \vec{\alpha}_1, \vec{\alpha}_2 \exists \vec{u} \exists x \forall \vec{v} \exists y_1, \dots, y_n \cdot \chi_n \wedge (\vec{u} = \beta) \wedge ((\vec{v} = \vec{\alpha}_1) \rightarrow (x \neq 0)) \wedge ((\vec{v} = \vec{\alpha}_2) \rightarrow (x \neq 1))$. Since $\vec{v} \geq_{\Psi_\beta} x$, the Frege+ \forall red proof of Ψ_β is easy: use \forall red rule to substitute $\vec{v} = \vec{\alpha}_1$ and $\vec{v} = \vec{\alpha}_2$ in the two axiom clauses to derive $(x \neq 0)$ and $(x \neq 1)$, a contradiction. So far in Q-MICE proof, we have derived lines L'_β for every $\beta \in [n]$. Now we can apply the join rule $n - 1$ times and remove the restriction of universal variables $u_{\log n}$ to u_1 (in this order). This results in the last claim being $(\Gamma, \emptyset, 2^n)$.

The two upper bounds describe above, put together, allow us to prove the following separation between the proof systems we have considered.

► **Theorem 17.** *The #QBF proof system Q-MICE is exponentially separated from the naive #QBF system and the $\forall\text{Exp}+\text{MICE}$ proof system.*

5 Discussion and Future Work

The paper proposes a #QBF proof system Q-MICE based on the #SAT proof system MICE [11] and proves that it is exponentially stronger than the naive (Section 3) and $\forall\text{Exp}+\text{MICE}$ proof systems (Section 3.1). For this, we introduced two new families of true QBFs: the quantified XOR-PAIRS and the indexed affine QBFs. We give easy Q-MICE proofs for both the formulas, and show that they are hard for the naive and $\forall\text{Exp}+\text{MICE}$ proof systems.

Recently, a #QBF solver d4-QBF [8] has been introduced. One open problem is to compare the strength of Q-MICE and the d4-QBF solver. It is easy to observe that Q-MICE is capable of certifying all the rules of d4-QBF except the decomposition rule. However, Q-MICE is modular, in the sense that, based on the requirements, one can always add more sound #QBF inference rules like the decomposition rule from [8]. One way to incorporate the decomposable rule is to add it at the beginning of a Q-MICE proof whenever possible. To be precise, suppose $Q.\phi$ is the input QBF. Run the ‘connected-component’ function of d4-QBF, and let it returns, $Q_1.\phi_1, Q_2.\phi_2, Q_3.\phi_3$ with disjoint variables. Since Q-MICE is complete, running it on $Q_1.\phi_1$ will eventually derive the claim $(Q_1.\phi_1, c_1)$ and similarly, the claims with c_2, c_3 . Finally, the model-count of $Q.\phi$ would be $c_1 \cdot c_2 \cdot c_3$ owing to the correctness of the decomposition step.

The challenge of doubly exponential solutions may be mitigated in Q-MICE by representing integers by arithmetic circuits. An immediate open problem is to establish a genuine lower bound [3] for Q-MICE. We conjecture that the propositional XOR-PAIRS (which are hard for MICE [5]) would be hard for Q-MICE but it is not a genuine lower bound. Another open

problem is to extend other #SAT proof systems CPOG [6], CLIP [9], KCPS(#SAT) [7] for #QBF.

References

- 1 Sanjeev Arora and Boaz Barak. *Computational Complexity - A Modern Approach*. Cambridge University Press, 2009.
- 2 Olaf Beyersdorff. *Proof Complexity of Quantified Boolean Logic — A Survey*, chapter Chapter 15, pages 397–440. 2023. doi:10.1142/9789811245220_0015.
- 3 Olaf Beyersdorff and Joshua Blinkhorn. Genuine lower bounds for QBF expansion. In Rolf Niedermeier and Brigitte Vallée, editors, *35th Symposium on Theoretical Aspects of Computer Science, STACS 2018, Caen, France, February 28 - March 3, 2018*, LIPIcs, pages 12:1–12:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018. doi:10.4230/LIPICs.STACS.2018.12.
- 4 Olaf Beyersdorff, Ilario Bonacina, Leroy Chew, and Ján Pich. Frege systems for Quantified Boolean Logic. *J. ACM*, 67(2):9:1–9:36, 2020. doi:10.1145/3381881.
- 5 Olaf Beyersdorff, Tim Hoffmann, and Luc Nicolas Spachmann. Proof complexity of propositional model counting. *J. Satisf. Boolean Model. Comput.*, 15(1):27–59, 2024. doi:10.3233/SAT-231507.
- 6 Randal E. Bryant, Wojciech Nawrocki, Jeremy Avigad, and Marijn J. H. Heule. Certified knowledge compilation with application to formally verified model counting. *J. Artif. Intell. Res.*, 82, 2025. doi:10.1613/jair.1.15958.
- 7 Florent Capelli. Knowledge compilation languages as proof systems. In Mikolás Janota and Inês Lynce, editors, *Theory and Applications of Satisfiability Testing - SAT 2019 - 22nd International Conference, SAT 2019, Lisbon, Portugal, July 9-12, 2019, Proceedings*, Lecture Notes in Computer Science, pages 90–99. Springer, 2019. doi:10.1007/978-3-030-24258-9_6.
- 8 Florent Capelli, Jean-Marie Lagniez, Andreas Plank, and Martina Seidl. A top-down tree model counter for quantified boolean formulas. In *Proceedings of the Thirty-Third International Joint Conference on Artificial Intelligence, IJCAI 2024, Jeju, South Korea, August 3-9, 2024*, pages 1853–1861. ijcai.org, 2024. URL: <https://www.ijcai.org/proceedings/2024/205>.
- 9 Sravanthi Chede, Leroy Chew, and Anil Shukla. Circuits, proofs and propositional model counting. In Siddharth Barman and Slawomir Lasota, editors, *44th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2024, Gandhinagar, Gujarat, India, December 16-18, 2024*, LIPIcs, pages 18:1–18:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024. doi:10.4230/LIPICs.FSTTCS.2024.18.
- 10 Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *J. Symb. Log.*, 44(1):36–50, 1979. doi:10.2307/2273702.
- 11 Johannes Klaus Fichte, Markus Hecher, and Valentin Roland. Proofs for propositional model counting. In Kuldeep S. Meel and Ofer Strichman, editors, *25th International Conference on Theory and Applications of Satisfiability Testing, SAT 2022, Haifa, Israel, August 2-5, 2022*, LIPIcs, pages 30:1–30:24. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. doi:10.4230/LIPICs.SAT.2022.30.
- 12 Aysegül Ihsan and Nurettin Dogan. Improved affine encryption algorithm for color images using LFSR and XOR encryption. *Multim. Tools Appl.*, 82(5):7621–7637, 2023. doi:10.1007/S11042-022-13727-W.
- 13 Mikolás Janota and João Marques-Silva. Expansion-based QBF solving versus Q-resolution. *Theor. Comput. Sci.*, 577:25–42, 2015. doi:10.1016/j.tcs.2015.01.048.
- 14 Hans Kleine Büning, Marek Karpinski, and Andreas Flögel. Resolution for quantified Boolean formulas. *Information and Computation*, 117(1):12–18, 1995. doi:10.1006/INCO.1995.1025.
- 15 Richard E. Ladner. Polynomial space counting problems. *SIAM J. Comput.*, 18(6):1087–1097, 1989. doi:10.1137/0218073.

- 16 Andreas Plank, Sibylle Möhle, and Martina Seidl. Counting QBF solutions at level two. *Constraints An Int. J.*, 29(1-2):22–39, 2024. doi:10.1007/S10601-024-09369-4.
- 17 John Alan Robinson. Theorem-proving on the computer. *Journal of the ACM*, 10(2):163–174, 1963. doi:10.1145/321160.321166.
- 18 Arijit Shaw, Brendan Juba, and Kuldeep S. Meel. An approximate skolem function counter. In Michael J. Wooldridge, Jennifer G. Dy, and Sriraam Natarajan, editors, *Thirty-Eighth AAAI Conference on Artificial Intelligence, AAAI 2024, Thirty-Sixth Conference on Innovative Applications of Artificial Intelligence, IAAI 2024, Fourteenth Symposium on Educational Advances in Artificial Intelligence, EAAI 2024, February 20-27, 2024, Vancouver, Canada*, pages 8108–8116. AAAI Press, 2024. doi:10.1609/AAAI.V38I8.28650.
- 19 Ankit Shukla, Sibylle Möhle, Manuel Kauers, and Martina Seidl. Outercount: A first-level solution-counter for quantified boolean formulas. In Kevin Buzzard and Temur Kutsia, editors, *Intelligent Computer Mathematics - 15th International Conference, CICM 2022, Tbilisi, Georgia, September 19-23, 2022, Proceedings*, Lecture Notes in Computer Science, pages 272–284. Springer, 2022. doi:10.1007/978-3-031-16681-5_19.
- 20 G. S. Tseitin. On the complexity of derivations in propositional calculus. In A. O. Slisenko, editor, *Studies in Mathematics and Mathematical Logic, Part II*, pages 115–125. 1970. Translated from Russian: Zapiski Nauchnykh Seminarov LOMI 8 (1968), pp. 234–259.