Electronic Colloquium on Computational Complexity, Report No. 157 (2019)

How QBF Expansion Makes Strategy Extraction Hard

Leroy Chew
University of Leeds, School of Computing, United Kingdom
http://www.leroychew.wordpress.com
scslnc@leeds.ac.uk

Judith Clymo
University of Leeds, School of Computing, United Kingdom
scjc@leeds.ac.uk

Abstract

In this paper we show that the QBF proof checking format QRAT (Quantified Resolution Asymmetric Tautologies) by Heule, Biere and Seidl cannot have polynomial-time strategy extraction unless P=PSPACE. In our proof, the crucial property that makes strategy extraction PSPACE-hard for this proof format is universal expansion, even expansion on a single variable.

While expansion reasoning used in other QBF calculi can admit polynomial time strategy extraction, we find this is conditional on a property studied in proof complexity theory. We show that strategy extraction on expansion based systems can only happen when the underlying propositional calculus has the property of feasible interpolation.

2012 ACM Subject Classification Theory of computation → Proof Complexity

Keywords and phrases QBF, Proof Complexity, QRAT, Strategy Extraction, Quantifier Expansion, Feasible Interpolation

Digital Object Identifier 10.4230/LIPIcs...

1 Introduction

Quantified Boolean logic is an extension of propositional logic in which variables may be existentially or universally quantified. This can allow problems to be represented more succinctly than is possible in propositional logic. Deciding the truth of a quantified Boolean formula (QBF) is PSPACE-complete. Propositional proof systems can be lifted to the QBF situation by the addition of rules to handle the universal quantification.

In addition to deciding whether a given QBF is true or false it is desirable that algorithms for solving QBFs can provide verification by outputting a proof. The QRAT proof system [13] is sufficiently strong to simulate the reasoning steps of all current QBF solvers and preprocessors and is a candidate for a standard format for verification of solvers.

In many settings it is not simply desirable to know that a QBF is true or false but also to find functions that witness to this. For example, QBFs may be used to model safety verification so that if the QBF is false then the modelled system is able to reach an unsafe state. It is important to also know *how* this state may be reached. If a QBF is true (resp. false) then there must exist Skolem (resp. Herbrand) functions for the existentially (resp. universally) quantified variables that certify this. Substituting the certifying Skolem functions in to the original QBF yields a tautology. Equivalently, substituting Herbrand functions results in an unsatisfiable propositional formula. The ability to efficiently extract Skolem or Herbrand functions from the proof output by a QBF solver is called strategy extraction.

There are generally two main paradigms in QBF solving: QCDCL (Conflict Driven Clause Learning) and QBF expansion. Both of these paradigms borrow techniques from propositional satisfiability solving for existential variables, but they differ in how they handle universal variables. The performance and limitations of these solvers can be analysed by

Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

ISSN 1433-8092

studying proof systems that follow the solver steps. QCDCL adds the universal *reduction* rule, such as in the Q-Res proof system. QBF expansion, on the other hand, adds the universal *expansion* rule such as in the proof system ∀Exp+Res. Both Q-Res and ∀Exp+Res are based on the resolution system in propositional logic.

The relationship between the two systems has been studied extensively in both QBF theory and practice. In [15, 4] it was shown that Q-Res and ∀Exp+Res are incomparable. However the picture becomes much more nuanced on certain fragments of QBF. Lonsing and Egly ran experiments on QBFs which were parametrised by the number of quantifier alternations and found better performance in the expansion based solvers on formulas with a low number of alternations [20]. This observation was confirmed in proof complexity in [3] where the expansion calculus ∀Exp+Res was shown to polynomially simulate the QCDCL calculus Q-Res on bounded quantifier alternations.

As well as using the calculi Q-Res and ∀Exp+Res to compare the strengths of the two types of QBF solvers, other properties can be studied for each of these systems. One very important property is the aforementioned strategy extraction. Often the strategies are just as important as whether a QBF is true or false. Many QBF proof systems with the universal reduction rule (from QCDCL) have been studied and shown to have polynomial-time strategy extraction using a technique from [1] and later generalised in [2, 7]. For QBF systems with universal expansion some strategy extraction results are known using a different technique [11, 4].

QRAT is a very different kind of proof system, not only can it simulate both the universal reduction and expansion rules but it draws from a stronger form of propositional reasoning than resolution. With this power it has been shown to simulate a number of different QBF proof systems [16, 17].

Strategy extraction on a universal checking format like QRAT would have certain benefits for the solving community. One could extract a QRAT proof from a solver and then from that proof separately extract the Skolem/Herbrand functions that give the winning strategy. This would avoid having to extract strategies directly from solvers while they are running which may affect performance.

On the other hand the property of strategy extraction can actually provide a source of weakness in QBF proof systems. In fact, a source of weakness in Q-Res is that it can always extract strategies as bounded depth circuits. This means that QBFs with winning strategies that can not be expressed in small bounded depth circuits necessarily have large Q-Res proofs [4]. This is similar to the proof size lower bound technique based on feasible interpolation [19, 21] where if a propositional proof system can extract Craig interpolants in polynomial time then super-polynomial interpolant size lower bounds become super-polynomial proof size lower bounds.

It was shown in [12] that Skolem functions to certify that a QBF is true can be extracted in polynomial time from a QRAT proof. In [8] a partial result was presented showing that Herbrand functions may be extracted from proofs in a restricted version of refutational QRAT. Here, we show that it is not possible in general to efficiently extract Herbrand functions certifying falsity from proofs in QRAT. This is due to QRAT providing short proofs to formulas that have PSPACE-hard strategies. Thus we show the asymmetry between the refutation or false QBF and proof of true QBF in the QRAT system. We demonstrate that this is due to the presence of universal expansion steps which manifest from the powerful reduction rules in the full QRAT proof system. [13, 17].

The universal expansion reasoning technique is present in QBF proof systems other than QRAT, but does not always exhibit the same hardness issues that we demonstrate for QRAT regarding strategy extraction. For example, the proof system $\forall$Exp+Res [15] uses expansion, but allows polynomial time strategy extraction [4]. In this paper we strengthen the important connection, first explored in [5], between strategy extraction and feasible interpolation.

This paper is organised as follows: Section 2 introduces the main concepts used in this paper. We show that strategy extraction in QRAT is PSPACE-hard in Sections 3 and 4. In Section 5 we look at expansion based systems that do have strategy extraction. We show that it is necessary for their underlying proof systems to have feasible interpolation. A sufficient condition with a relationship to feasible interpolation is also shown.

2 Preliminiaries

2.1 Proof Complexity

Let Γ be an alphabet and $\mathcal{L}$ a language over Γ. A *proof system* [9] for $\mathcal{L}$ is a polynomial-time computable partial function $f : \Gamma^\star \rightharpoondown \Gamma^\star$ with range $\mathcal{L}$. The size $|\pi|$ of a proof π in $\Gamma^\star$ is the number of characters it contains. f maps a proof to the theorem it proves (or refutes, in the case of a refutational proof system). Soundness of f requires that $\mathit{rng}(f) \subseteq \mathcal{L}$ and completeness that $\mathit{rng}(f) \supseteq \mathcal{L}$.

In propositional logic a literal is a Boolean variable x or its negation $\neg x$. A clause is disjunction of literals. A formula in conjunctive normal form (CNF) is a conjunction of clauses. Let l be a literal. If $l = x$ then $\bar{l} = \neg x$, if $l = \neg x$ then $\bar{l} = x$. A PCNF is naturally understood as a set of clauses, and a clause as a set of literals. Where it is convenient to do so we will therefore use set notation $C \in \phi$ and $l \in C$ to state that clause C appears in the matrix of QBF $\Psi = \Pi\phi$ and literal l appears in clause C. It is often convenient to notationally treat clauses as unordered disjunctions and sets simultaneously, so we can use $C \vee l$ to denote the clause that contains all literals of clause C and also the literal l if it is not already included, and $D \cup E$ to denote the disjunction of all literals that appear in either clause D or E. An assignment τ for formula A over n variables is a partial function from the variables of A to $\{0, 1\}^n$. For clause C, $\tau(C)$ is the result of evaluating C under assignment τ. For formula (or circuit) A, we define $A[b/x]$ so that all instances of variable x in A are replaced with $b \in \{0, 1\}$.

2.2 Quantified Boolean Formulas

Quantified Boolean formulas (QBF) extend propositional logic by allowing Boolean variables to be universally or existentially quantified [18]. $\forall x\, \Psi$ is satisfied by the same truth assignments as $\Psi[0/x] \wedge \Psi[1/x]$ and $\exists x\, \Psi$ is satisfied by the same truth assignments as $\Psi[0/x] \vee \Psi[1/x]$. In a closed QBF all variables must be quantified. A QBF is in prenex form if all quantification occurs before any propositional connectives, so a prenex QBF Ψ consists of a prefix Π defining how each variable is quantified and a propositional part ϕ called the matrix. We write $\Psi = \Pi\phi$. The prefix Π has a linear structure. A PCNF is a QBF in prenex form and with the propositional part in conjunctive normal form. We consider only closed PCNFs.

Starting from the left we can assign each variable x a level, denoted $\mathrm{lv}(x)$. The first variable has level 1. The level is incremented by 1 every time the quantifier type changes and otherwise remains the same. It is often convenient to write quantifiers in a prefix only when the level changes. When QBF are written in this way we can think of entire levels quantifying *blocks* of variables.

2.3 Winning Strategies

A closed prenex QBF is analogous to a game between two players where one player is responsible for assigning values to the existentially quantified variables, and the other to the universally quantified variables. The players make assignments according to the quantifier prefix, so each level of the prefix corresponds to one turn in the game. The existential player wins the game if the formula evaluates to true once all assignments have been made, the universal player wins if the formula evaluates to false.

A strategy for the universal player on QBF $\Pi\phi$ is a set of rules for making the assignments to each universal u. The rule for setting u must depend only on variables earlier than u in Π, respecting the idea that when u is being decided the universal player cannot know what choices will be made in future turns. If this strategy ensures the universal player always wins games on $\Pi\phi$ (however the existential player makes assignments), then it is called a winning strategy. A QBF is false if and only if the universal player has a winning strategy. Strategies for the existential player are defined analogously. A refutational proof system is said to admit strategy extraction if and only if it is possible to efficiently (i.e. in polynomial time in the size of the proof) construct a circuit representing a winning strategy for the universal player from a refutation of a QBF.

2.4 Expansion-based proof systems

Since QBF includes and extends all propositional formulas, proving (or refuting) QBFs typically involves adapting existing propositional proof systems to deal with variables that are now quantified.

One such approach is to take the semantic definition of the universal quantifier $\forall u \Psi = \Psi[0/u] \wedge \Psi[1/u]$, this can be used as a rule to eliminate universal quantifiers. If Ψ is a QBF then $\Psi[0/u]$ and $\Psi[1/u]$ each contain their own quantifiers, the variables bound by these quantifiers would have to be renamed to avoid repeating the other's variables. We take a convention of putting a partial assignment in the superscript on the renaming of these variables such that the variables $\vec{x} = \{x_i \mid i \in I\}$ bound in Ψ are renamed $\vec{x}^{0/u} = \{x_i^{0/u} \mid i \in I\}$ in $\Psi[0/u]$ and $\vec{x}^{1/u} = \{x_i^{1/u} \mid i \in I\}$ in $\Psi[1/u]$. Repeated expansions create a larger superscript e.g.

$$\begin{aligned}
&\forall u \exists x \forall v \exists y (\neg u \vee x \vee v \vee \neg y)\\
&= \forall u \exists x y^{0/v} y^{1/v} (\neg u \vee x \vee 0 \vee \neg y^{0/v}) \wedge (\neg u \vee x \vee 1 \vee \neg y^{1/v})\\
&= \forall u \exists x y^{0/v} y^{1/v} (\neg u \vee x \vee \neg y^{0/v})\\
&= \exists x^{0/u} x^{1/u} y^{0/u,0/v} y^{0/u,1/v} y^{1/u,0/v} y^{1/u,1/v} (1 \vee x^{0/u} \vee \neg y^{0/u,0/v}) \wedge (0 \vee x^{1/u} \vee \neg y^{1/u,0/u})\\
&= \exists x^{0/u} x^{1/u} y^{0/u,0/v} y^{0/u,1/v} y^{1/u,0/v} y^{1/u,1/v} (x^{1/u} \vee \neg y^{1/u,0/u})
\end{aligned}$$

Note that because we started here with a prenix formula, we can maintain that throughout the expansions. In the end, once we expand all universal variables we just get a prenex QBF with only existential quantifiers, this is known as a *full expansion*. What we are left with is a satisfiability problem. If we use a refutation system Q we can attempt to refute the expanded formula.

In fact any for any refutational propositional proof system Q we can create a refutational QBF proof system, (that is refutationally complete) by taking the full expansion and showing a contradiction using propositional system Q. Such a system would easily have many exponential lower bounds due to the explosion caused by the full expansion on a linear number of universal variables.

In practice we can often do better than this. The full expansion gives a large conjunction and we may only need to use *some* of the conjuncts in order to prove a contradiction. This can be tightened up further when the original QBF is a prenexed conjunction (like a PCNF), checking whether a conjunct is in the full expansion can be decided in polynomial time. We define this formally below.

2.4.1 $\mathsf{Q}+\forall\mathsf{Exp}_{0,1}$

We start with a propositional proof system Q and prenex QBF $\Pi\phi$, where Π is the quantifier prefix and ϕ is a propositional matrix in variables of Π, we treat ϕ as a conjunction of formulas.

Let τ be a full assignment to all universal variables and let l be an existential literal. We define $\mathsf{restrict}_l(\tau)$ to be the partial assignment of τ for all universal variables left of the variable of l in the prefix. Now let us use that to define C^τ, where C is a propositional formula in both existential and universal variables.

C^τ is the same as C except we replace every existential variable l with the annotated variable $l^{\mathsf{restrict}_l(\tau)}$ and every universal variable l with its value $\tau(l)$.

▶ **Definition 1.** *The refutational QBF proof system* $\mathsf{Q}+\forall\mathsf{Exp}_{0,1}$ *[2] allows the instantiation of* ***axiom*** C^τ*, whenever* C *is a conjunct from the matrix and* τ *is an assignment to all universal variables. A* Q *refutation of the conjunction of the axioms is provided, treating differently annotated variables as different.*

A $\mathsf{Q}+\forall\mathsf{Exp}_{0,1}$ proof π of QBF Φ therefore consists of a propositional Q proof of a sub-conjunction of the full expansion, we denote this conjunction as $\mathsf{subexp}_\pi(\Phi)$.

A well-known example of $\mathsf{Q}+\forall\mathsf{Exp}_{0,1}$ is when Q is propositional resolution (known as $\forall\mathsf{Exp}+\mathsf{Res}$ in the literature [15]). This is the proof system that underlies the reasoning in the competitive QBF solver RAReQS [14]. Resolution is chosen because of its use in SAT solving.

2.5 QRAT

The QRAT proof system [13] was introduced as a universal proof checking format for QBF. It is able to express many QBF preprocessing techniques and proof systems. QRAT works on a PCNF QBF $\Pi\phi$ which is modified throughout the proof by satisfiability preserving rules. Clauses may be added, altered or deleted depending on the current status of $\Pi\phi$.

QRAT may be used either to prove that a QBF is true or to refute it. The refutational version of QRAT uses the following rules: Asymmetric Tautology Addition (ATA), Quantified Resolution Asymmetric Tautology Addition (QRATA), Quantified Resolution Asymmetric Tautology Universal (QRATU), Extended Universal Reduction (EUR), and Clause Deletion. We define only the rules that are relevant for this paper, for a full definition of the QRAT system please refer to [13].

If C is a clause, then $\bar{C}$ is the conjunction of the negation of the literals in C. *Unit propagation* is a procedure on a formula ϕ in CNF that builds a partial assignment τ. τ is applied to ϕ and then for any literal l that appears in a singleton (unit) clause in the resulting formula the assignment satisfying l is added to τ. This is repeated until reaching fix-point, which must happen in polynomial time in the number of clauses in ϕ. Unit propagation is used extensively in QRAT for deciding whether a derivation rule may be applied. We denote that empty clause $\bot$ is derived by unit propagation applied to $\Pi\phi$ by $\Pi\phi \vdash_1 \bot$.

▶ **Definition 2** (Asymmetric Tautology Addition (ATA)). *Let $\Pi\phi$ be a closed PCNF with prefix Π and CNF matrix ϕ. Let C be a clause not in ϕ. Let Π' be a prefix including the variables of C and ϕ, Π is a sub-prefix of Π' containing the variables of ϕ only.*

Suppose $\Pi'\phi \wedge \bar{C} \vdash_1 \bot$. Then we can make the following inference

$$\frac{\Pi\phi}{\Pi'\phi \wedge C}\ (ATA)$$

▶ **Definition 3** (Outer Clause). *Let $\Pi\phi$ be a PCNF with closed prefix Π and CNF matrix ϕ. Let C be a clause not in ϕ. Let Π' be a prefix including the variables of C and ϕ, Π is a sub-prefix of Π' containing the variables of ϕ only.*

Suppose C contains a literal l. Consider all clauses D in ϕ with $\bar{l} \in D$. The outer clause *O_D of D is $\{k \in D \mid \mathrm{lv}(k) \leq_\Pi \mathrm{lv}(l), k \neq \bar{l}\}$.*

▶ **Definition 4** (Quantified Resolution Asymmetric Tautology Addition (QRATA)). *Let $\Pi\phi$ be a PCNF with closed prefix Π and CNF matrix ϕ. Let C be a clause not in ϕ. Let Π' be a prefix including the variables of C and ϕ, Π is a sub-prefix of Π' containing the variables of ϕ only.*

If C contains an existential literal l such that for every $D \in \phi$ with $\bar{l} \in D$, $\Pi\phi \wedge \bar{C} \wedge \bar{O}_D \vdash_1 \bot$ then we can derive

$$\frac{\Pi\phi}{\Pi'\phi \wedge C}\ (QRATA\ w.r.t.\ l)$$

▶ **Definition 5** (Extended Universal Reduction (EUR)). *Given a clause $C \vee u$ with universal literal u, consider extending C by*

$C := C \cup \{k \in D \mid \mathrm{lv}(k) >_\Pi \mathrm{lv}(u)$ *or* $k = \bar{u}\}$,
where $D \in \phi$ is any clause with some $p : \mathrm{lv}(p) >_\Pi \mathrm{lv}(u)$, $p \in C$ and $\bar{p} \in D$,
until we reach a fix-point denoted ε. If $\bar{u} \notin \varepsilon$ then we can perform the following rule.

$$\frac{\Pi\phi \wedge (C \vee u)}{\Pi'\phi \wedge C}\ (EUR)$$

We can also define a weaker version of QRAT, QRAT(UR), which uses universal reduction instead of EUR.

▶ **Definition 6** (Universal Reduction (UR)). *Given a clause $C \vee u$ with universal literal u such that $\mathrm{lv}(u) > \mathrm{lv}(x)$ for all existentially quantified variables x in C we can apply the following rule.*

$$\frac{\Pi\phi \wedge (C \vee u)}{\Pi'\phi \wedge C}\ (UR)$$

3 Cheating a QBF game

It is rumoured that the famous chess players Alekhine and Bogoljubov were once both separately challenged to a game of correspondence chess by an anonymous opportunist. The third player had deviously remembered the moves of each opponent to play Alekhine's and Bogoljubov's moves against each other, effectively removing themselves from the game. The player was guaranteed to win or draw in at least one game, and with the money odds against them, they stood to make a profit.

We see that this devious idea can also be used in the conjunction of QBF two-player games. We will show have these conjunctions have short QRAT proofs. We take a QBF and conjunct it with its negation in new variables. We interleave the prefixes so that the existential player plays first and the universal player is able to copy the moves at the right time. The universal player has to win on only one of the conjuncts and an easy winning strategy is to copy the opponent's move for the other side. The easy winning strategy is essential for the short proofs, but despite the guaranteed win, it is PSPACE-hard to find out which game the universal player wins prior to playing it. In the next section we add an extra universal variable that requires the calculation of who wins in order to make the game hard. However we see that expansion allows us to quickly return to the original easy problem.

In this chapter we will define these formulas that conjunct a QBF and its negation and show how a short QRAT proof can be uniformly obtained.

3.1 Duality Formulas

Let $\Pi\phi(X)$ be a QBF where Π is a prefix binding all variables in $X = \{x_1 \dots x_{2n}\}$. Let $\Pi = \forall x_1 \exists x_2 \forall x_3 \dots \exists x_{2n}$ and let $\phi(X)$ be a CNF in the variables X. We also define a second set of 2n variables $X' = \{x'_1 \dots x'_{2n}\}$ and an alternative prefix $\Pi' = \exists x'_1 \forall x'_2 \exists x'_3 \dots \forall x'_{2n}$. The QBF $\Pi\phi(X) \wedge \Pi'\neg\phi(X')$ is necessarily false. However this QBF is not in PCNF, which many proof systems require.

Firstly we will transform $\neg\phi(X')$ into a CNF $\bar{\phi}(X', T)$ via the use of Tseitin variables $T = \{t_K \mid K \in \phi(X)\}$. We overload the $'$ notation:

- For literal l if $l = x_i$ then $l' = x'_i$ and if $l = \neg x_i$ then $l' = \neg x'_i$.
- For each clause K in $\phi(X)$ we denote the corresponding clause in $\phi(X')$ as K' so that $K' = \bigvee_{l \in K} l'$.

We require that $\bar{\phi}(X', T)$ is true precisely when $\phi(X')$ is false. We will introduce clauses stating that variable t_K is true if and only if clause K' is satisfied. Then $\phi(X')$ is false if and only if at least one t_K is false, so we will also add a clause specifying that this must hold.

$\bar{\phi}(X', T)$ contains the following clauses:

- $(\neg t_K \vee K')$ for each clause K in $\phi(X)$
- $(\neg l' \vee t_K)$ for each literal l in K
- $\left(\bigvee_{K \in \phi(X)} \neg t_K\right)$

The next part is the most important- the prenexing of the QBF. We place every universal variable to the right of its existential version. The auxiliary T variables must be placed at the end of the prefix. Thus, from any PCNF $\Psi = \Pi\phi$ we generate a formula $\mathsf{Duality}(\Pi\phi)$ encoding in PCNF the claim that both Ψ and its negation are true:

$$\mathsf{Duality}(\Pi\phi) = \exists x'_1 \forall x_1 \exists x_2 \forall x'_2 \dots \exists x'_{2n-1} \forall x_{2n-1} \exists x_{2n} \forall x'_{2n} \exists T \ \phi(X) \wedge \bar{\phi}(X', T)$$

3.2 Short proofs of Duality Formulas

In [6], Beyersdorff et. al showed short $\mathsf{Frege} + \forall\mathsf{red}$ proofs of a family of QBFs that take an input of a graph and state that there is a k-clique (Clique) and dually that there is no k-clique (Co-Clique). The short proofs exploited the fact that the Co-Clique part of the formula was structured in a similar way to the Clique part.

We generalise this approach here for short proofs of the $\mathsf{Duality}$ formulas. First we will give a sketch proof of how this can be done using $\mathsf{Frege} + \forall\mathsf{red}$ rules before we show those short proofs formally in QRAT. $\mathsf{Frege} + \forall\mathsf{red}$ is simply a propositional Frege system augmented with the $\forall\mathsf{red}$ rule for removing universally quantified variables. $\forall\mathsf{red}$ allows to substitute a Boolean value for universally quantified u in a previously derived line, provided that $\mathrm{lv}(u) > \mathrm{lv}(x)$ for all existentially quantified x in the proof line.

The clauses in $\mathsf{Duality}(\Pi\Phi)$ state $\bigwedge_K (t_K \leftrightarrow K')$, $\bigvee_K \neg t_K$ and $\bigwedge K$.

Recall that clause K is identical to clause K' with all instances of x'_i replaced with x_i (for all i). From assumption $\bigwedge_{i=1}^{2n} (x_i \leftrightarrow x'_i)$ we would find a contradiction in polynomially many Frege steps. The outline of the derivation is given below:

$$\dfrac{\bigvee_K \neg t_K \qquad \dfrac{\bigwedge K \qquad \dfrac{\bigwedge_K (t_K \leftrightarrow K') \qquad \bigwedge_{i=1}^{2n} (x_i \leftrightarrow x'_i)}{\bigwedge_K (t_K \leftrightarrow K)}}{\bigwedge_K t_K}}{\bot}$$

We therefore conclude that $\bigvee_{i=1}^{2n} \neg(x_i \leftrightarrow x'_i)$.

Now, starting from the variables quantified innermost in the prefix, we perform $\forall\mathsf{red}$ on all universally quantified x'_{2j} and x_{2j+1}:

$$\neg(x_{2n} \leftrightarrow 0) \vee \bigvee_{i=1}^{2n-1} \neg(x_i \leftrightarrow x'_i) \qquad = x_{2n} \vee \bigvee_{i=1}^{2n-1} \neg(x_i \leftrightarrow x'_i)$$

Reduction can also be done with $x'_{2j} = 1$

$$\neg(x_{2n} \leftrightarrow 1) \vee \bigvee_{i=1}^{2n-1} \neg(x_i \leftrightarrow x'_i) \qquad = \neg x_{2n} \vee \bigvee_{i=1}^{2n-1} \neg(x_i \leftrightarrow x'_i)$$

We can resolve these two disjunctions together and conclude $\bigvee_{i=1}^{2n-1} \neg(x_i \leftrightarrow x'_i)$

Now x_{2n-1} is the innermost universally quantified variable. The same sequence of steps is applied for each universal variable leading to a contradiction which completes the proof.

This proof idea works for showing short proofs in QRAT. In fact these proofs have a uniform structure.

▶ **Theorem 7.** *Given a formula* $\mathsf{Duality}(\Pi\Phi)$ *we can in polynomial-time construct a quadratic size QRAT(UR) refutation of* $\mathsf{Duality}(\Pi\Phi)$.

Proof. Let $|K|$ be the number of literals in clause $K \in \Phi$, then $|\mathsf{Duality}(\Pi\Phi)| \geq |\Phi| \geq \Sigma_{K\in\Phi}|K|$. Recall $\Pi\Phi$ has $2n$ variables.

Extension Variables

The refutation begins by using QRATA to introduce extension variable eq_{x_i} for each $x_i \in X$. eq_{x_i} is existentially quantified and is introduced to the prefix so that $\mathrm{lv}(\mathrm{eq}_{x_i}) > \mathrm{lv}(x_i), \mathrm{lv}(x'_i)$ and $\mathrm{lv}(\mathrm{eq}_{x_i}) < \mathrm{lv}(x_j), \mathrm{lv}(x'_j)$ for all $j > i$ (which is possible since $\mathrm{lv}(x_i), \mathrm{lv}(x'_i) < \mathrm{lv}(x_j), \mathrm{lv}(x'_j)$ in $\mathsf{Duality}(\Pi\Phi)$ whenever $j > i$). For each $x_i \in X$ we use QRATA to add four clauses:

- $(\neg x_i \vee x'_i \vee \neg \mathrm{eq}_{x_i})$
- $(x_i \vee \neg x'_i \vee \neg \mathrm{eq}_{x_i})$
- $(\neg x_i \vee \neg x'_i \vee \mathrm{eq}_{x_i})$
- $(x_i \vee x'_i \vee \mathrm{eq}_{x_i})$

Recall that adding a clause by QRATA requires that we have an existential literal l in the new clause C such that $\Phi \wedge \bar{C} \wedge \bar{O}_D \vdash_1 \bot$ for all D with $\bar{l} \in D$. For the first two clauses this is vacuously satisfied with $l = \neg\mathrm{eq}_{x_i}$ since eq_{x_i} does not appear positively anywhere in the formula.

To add the latter clauses we have $l = \mathrm{eq}_{x_i}$ and must consider the two outer clauses $(\neg x_i \vee x'_i)$ and $(x_i \vee \neg x'_i)$. The QRATA condition is satisfied for $(\neg x_i \vee \neg x'_i \vee \mathrm{eq}_{x_i})$ because $x_i \wedge x'_i \wedge x_i \wedge \neg x'_i \vdash_1 \bot$ and $x_i \wedge x'_i \wedge \neg x_i \wedge x'_i \vdash_1 \bot$, and similarly for the final clause.

For each of the original $2n$ variables in $\Pi\Phi$ we have added four clauses of constant size. Following $O(n)$ steps the formula has increased in length by $O(n)$ characters.

Non Equivalence of X and X'

The next three steps are equivalent to those in the derivation of $\bigvee_{i=1}^{2n} \neg(x_i \leftrightarrow x'_i)$ in the sketch proof above. By ATA we derive:

- $(\bigvee_{i=1}^{2n} \neg\mathrm{eq}_{x_i} \vee t_K \vee \bar{l})$ for every $K \in \Phi(X)$ and every $l \in K$
- $(\bigvee_{i=1}^{2n} \neg\mathrm{eq}_{x_i} \vee t_K)$ for every $K \in \Phi(X)$
- $(\bigvee_{i=1}^{2n} \neg\mathrm{eq}_{x_i})$

Each clause has $O(n)$ literals and there are at most $|\Phi|$ clauses of each type. In $O(|\Phi|)$ proof steps the formula has increased in length by $O(n|\Phi|)$.

Removing the Universal Variables

Finally, we want to derive $(\bigvee_{i=1}^{j-1} \neg\mathrm{eq}_{x_i})$ for $j = 2n \dots 1$ (thus $j = 1$ means that we have derived the empty clause). Assuming that we already have $(\bigvee_{i=1}^{j} \neg\mathrm{eq}_{x_i})$ we can use ATA to add:

- $(\bigvee_{i=1}^{j-1} \neg\mathrm{eq}_{x_i} \vee x_j \vee x'_j)$
- $(\bigvee_{i=1}^{j-1} \neg\mathrm{eq}_{x_i} \vee \neg x_j \vee \neg x'_j)$

In clauses $(\bigvee_{i=1}^{j-1} \neg\mathrm{eq}_{x_i} \vee x_j \vee x'_j)$ and $(\bigvee_{i=1}^{j-1} \neg\mathrm{eq}_{x_i} \vee \neg x_j \vee \neg x'_j)$, whichever of x_j and x'_j is universally quantified is innermost by the construction of $\mathsf{Duality}(\Pi\Phi)$ and the decision of where to introduce the variables eq_{x_i} in the prefix. Without loss of generality, assume x'_j is universally quantified so we can use UR to derive clauses $\bigvee_{i=1}^{j-1} \neg\mathrm{eq}_{x_i} \vee x_j$ and $\bigvee_{i=1}^{j-1} \neg\mathrm{eq}_{x_i} \vee \neg x_j$, then ATA allows to add the resolvent $\bigvee_{i=1}^{j-1} \neg\mathrm{eq}_{x_i}$.

For each of the $2n$ variables from Φ there are five proof steps in this final part of the refutation, each introducing a new clause of size $O(n)$, and in total the formula has increased in length by $O(n^2)$. The whole refutation therefore has size $O(|\mathsf{Duality}(\Pi\Phi)|^2)$. ◀

4 Making strategies hard

The formulas $\mathsf{Duality}(\Pi\Phi)$ have short winning strategies for the universal player, namely to always play so that $x_i = x'_i$. By construction one or other of $\Phi(X)$ or $\bar{\Phi}(X', T)$ will be falsified, but which subformula is falsified depends on the existential assignments. We know also that one of $\Pi\Phi(X)$ or $\Pi'\bar{\Phi}(X', T)$ is false and so has a winning strategy for the universal player. Deciding which subformula is false is PSPACE-hard and the winning strategy for the false formula could be much more complicated than the strategy for $\mathsf{Duality}(\Pi\Phi)$. We introduce formulas exploiting this hardness:

$$\mathsf{Select}(\Pi\Phi) = \forall u \ \mathcal{Q} \ \exists T \ (\Phi_u(X)) \wedge (\bar{\Phi}_{\neg u}(X', T))$$

$$\text{where } \Phi_u(X) = \bigwedge_{K \in \Phi(X)} (K \vee u)$$

$$\text{and } \mathcal{Q} = \exists x'_1 \forall x_1 \exists x_2 \forall x'_2 \dots \exists x'_{2n-1} \forall x_{2n-1} \exists x_{2n} \forall x'_{2n}$$

4.1 Short proofs of Select Formulas in QRAT

It was shown in [12] that satisfaction QRAT has strategy extraction, and in [8] that refutational QRAT(UR) has strategy extraction. In this section we use the formulas $\mathsf{Select}(\Pi\Phi)$ to show that refutational QRAT does not have strategy extraction under a strong complexity assumption.

▶ **Theorem 8.** *QRAT has short uniform proofs of* $\mathsf{Select}(\Pi\Phi)$ *for any QBF* $\Pi\Phi$*.*

Proof. The first step in the proof is to use Extended Universal Reduction (EUR) to remove u from all clauses in $\Phi_u(X)$ and $\neg u$ from all clauses in $\bar{\Phi}_{\neg u}(X', T)$. Using EUR to reduce l in C requires that $\bar{l}$ does not appear in ϵ the fix-point of the inner expansion as given in Definition 5, in other words, there is no inner resolution path between any clauses containing the removed literal and its negation. We can only add literals to the inner expansion from clauses that share variables in common with the current inner expansion. However u and $\neg u$ appear in sections of the formula that have no other variables in common. Hence we can always reduce u (and $\neg u$) in $\mathsf{Select}(\Pi\Phi)$.

Having performed these (polynomially many) EUR steps the formula is identical to $\mathsf{Duality}(\Pi\Phi)$, which is uniformly refuted as in Theorem 7. ◀

▶ **Corollary 9.** *Refutational QRAT does not have strategy extraction unless P = PSPACE.*

Proof. If QRAT has strategy extraction we can decide the truth of closed QBF in polynomial time - a PSPACE-complete problem.

Given a QBF $\Pi\Phi$, with Π a prefix and Φ a propositional formula in the variables of Π, we create the formula $\mathsf{Select}(\Pi\Phi)$ and then in polynomial time we can output the proofs as in Theorem 8. Then from the proof of $\mathsf{Select}(\Pi\Phi)$ we can extract the strategy for u. u is outermost in the prefix, so this strategy must be constant. If the strategy sets $u = 0$ then all clauses in $\bar{\Phi}_{\neg u}(X', T)$ are immediately satisfied so we know that the rest of the extracted strategy is a strategy for $\Pi\Phi$, showing that $\Pi\Phi$ is false. Similarly, if the strategy sets $u = 1$ then it must be the case that $\bar{\Phi}_{\neg u}(X', T)$ is false and so, by construction, $\Pi\Phi$ is true. Therefore we have a polynomial time decision procedure for an arbitrary QBF. ◀

In fact, the full power of EUR is not required. QRAT(UR) is capable of refuting the formulas $\mathsf{Duality}(\Pi\Phi)$, and the initial EUR step can be replaced by universal expansion of u, producing a formula equivalent to $\mathsf{Duality}(\Pi\Phi)$ with renamed variables. Even QBF solvers whose underlying proof system uses universal reduction to handle universally quantified variables often employ a preprocessing stage that includes universal expansion. Our $\mathsf{Select}(\Pi\Phi)$ formulas show that a single initial expansion step may be sufficient to prevent strategy extraction.

5 Relation to feasible interpolation

The results of the previous section indicate that expansion can be used to make strategy extraction implausible. However we have seen many proof systems and solvers that admit strategy extraction despite using universal expansion. It is clear that the other rules of the calculus play an important role on whether or not strategy extraction is admissible.

If we wish to guarantee strategy extraction in our proof systems and solvers, it may be important for future work to explore *sufficient* conditions for strategy extraction when using expansion. In this section we instead explore a *necessary* condition for strategy extraction when using expansion and see that it is related to feasible interpolation in propositional proof systems.

Given a true propositional implication $A(\vec{p},\vec{q}) \rightarrow B(\vec{p},\vec{r})$ (or, equivalently, a false conjunction $A(\vec{p},\vec{q}) \wedge \neg B(\vec{p},\vec{r})$) Craig's interpolation theorem [10], states that there is an interpolant $C(\vec{p})$ in only the joint variables $\vec{p}$. Feasible interpolation is a property of proof systems. A proof system has feasible interpolation [19, 21] if and only if there is a polynomial-time procedure that takes a proof of $A(\vec{p},\vec{q}) \rightarrow B(\vec{p},\vec{r})$ as an input and extracts an interpolating circuit $C(\vec{p})$.

In [5] Beyersdorff et al. lifted a version of the feasible interpolation lower bound technique from propositional logic to QBF. In Section 5 of [5] feasible interpolation was linked to strategy extraction by adding an extra universal variable with similarities to Section 4 and how the Select formulas are created from the Duality formulas.

▶ **Theorem 10.** *Given a propositional refutation system Q if the refutational QBF proof system $\mathsf{Q}+\forall\mathsf{Exp}_{0,1}$ has strategy extraction then Q must have feasible interpolation (provided refutations of Q work independently of the variable names).*

Proof. Suppose $\mathsf{Q}+\forall\mathsf{Exp}_{0,1}$ has strategy extraction and we have a Q-refutation π of $A(\vec{p},\vec{q}) \wedge B(\vec{p},\vec{r})$ with $\vec{p},\vec{q},\vec{r}$ disjoint sets of variables. We will show we can find an interpolant in polynomial time.

We consider the following QBF

$$\exists \vec{p} \forall u \exists \vec{q} \exists \vec{r} (A(\vec{p},\vec{q}) \vee u) \wedge (B(\vec{p},\vec{r}) \vee \bar{u})$$

We can refute this formula in $\mathsf{Q}+\forall\mathsf{Exp}_{0,1}$ using π. Expansion gives us

$$(A(\vec{p},\vec{q}^{0/u}) \vee 0) \wedge (B(\vec{p},\vec{r}^{0/u}) \vee 1) \wedge (A(\vec{p},\vec{q}^{1/u}) \vee 1) \wedge (B(\vec{p},\vec{r}^{1/u}) \vee 0)$$

but this immediately simplifies to

$$A(\vec{p},\vec{q}^{0/u}) \wedge B(\vec{p},\vec{r}^{1/u})$$

We can now refute this using π using $\vec{q}^{0/u}$ variables instead of $\vec{q}$, and using $\vec{r}^{1/u}$ variables instead of $\vec{r}$. The provision here is important for this as one could make Q a pathological proof system that disallowed steps using variables named as in $\vec{q}^{0/u}$, but allowed them named as in $\vec{q}$.

We can then extract a strategy for u as a circuit in the variables $\vec{p}$. However this circuit is also an interpolant for $A(\vec{p},\vec{q}) \wedge B(\vec{p},\vec{r})$.

◀

In regards to making *sufficient* conditions for strategy extraction using feasible interpolation we can look at the results that have come before. We see that $\forall\mathsf{Exp}+\mathsf{Res}$ has strategy extraction. This is done by a "round-based" strategy extraction, the technique, that gives a winning response for the universal player works by taking the outermost block of existential and applying a restriction to the $\forall\mathsf{Exp}+\mathsf{Res}$ proof on that block in correspondence to the existential player's moves. The universal player can then "read off", from the restricted proof, which universal assignment to the next block of variables actually is useful in the proof. The proof can be restricted by the universal assignment and we repeat until we end up with a complete set of universal responses and a falsified formula.

The "reading off" of which clauses actually contribute to the proof is a weak form of feasible interpolation. and so we can say we have strategy extraction for $\mathsf{Q}+\forall\mathsf{Exp}_{0,1}$ whenever refutational proof system Q satisfies two conditions:

▶ **Theorem 11.** Q+$\forall$Exp$_{0,1}$ *has strategy extraction whenever:*

1. *Q is closed under restriction, meaning that from a refutation π of ϕ one can extract in polynomial time a Q refutation π_ϵ of $\phi|_\epsilon$ for any assignment ϵ with $|\pi_\epsilon| \leq |\pi|$*
2. *From any refutation π in Q of $A(\vec{q}) \wedge B(\vec{r})$ where $\vec{q}, \vec{r}$ share no common variables another refutation π_{int} of either $A(\vec{q})$ or $B(\vec{r})$ can be extracted in polynomial time with $|\pi_{\mathsf{int}}| \leq |\pi|$.*

Proof. Suppose we have a closed prenix QBF $\exists X \forall Y \Pi \phi$ where Π is a prefix in variables Z and ϕ is a propositional matrix with variables in X,Y and Z. Now suppose we have a Q+$\forall$Exp$_{0,1}$ refutation π of $\Pi\phi$. This gives a Q proof π' of $\mathsf{subexp}_\pi(\exists X \forall Y \Pi \phi)$, a subset of the full expansion of $\Pi\phi$ using π.

We will show that under conditions 1 and 2 we have a polynomial time procedure that takes any assignment ϵ to X and outputs a response μ in Y and a $\Pi\Phi|_{\epsilon,\mu}$ refutation in Q+$\forall$Exp$_{0,1}$.

From π', we can extract π'_ϵ in polynomial time, using condition 1, which provides a Q refutation of $\mathsf{subexp}_\pi(\exists X \forall Y \Pi\phi)|_\epsilon$. Every conjunct $D^\tau|_\epsilon$ of $\mathsf{subexp}_\pi(\exists X \forall Y \Pi\phi)|_\epsilon$ is also an axiom C^τ of $\forall Y \Pi \phi|_\epsilon$, because $D \in \phi$ means $C = D|_\epsilon$ can be found in $\phi|_\epsilon$. Therefore π'_ϵ becomes a Q+$\forall$Exp$_{0,1}$ refutation π_ϵ of $\forall Y \Pi \phi|_\epsilon$.

Now we find the universal response in universal variables Y. We separate $Y = \{y_1 \dots y_m\}$ and we can start with a response c to y_1 and then find a Q+$\forall$Exp$_{0,1}$ refutation of $\forall y_2 \dots y_m \Pi\phi|_{\epsilon, c/y_1}$. We make sure the proofs do not increase in size. Then we can repeat this for each variable in Y in turn.

Suppose we have a Q+$\forall$Exp$_{0,1}$ refutation π_i of the QBF formula $\forall y_i \dots y_m \Pi\phi|_{\epsilon,\mu_i}$ where μ_i $1 \leq i \leq m$ is a Boolean assignment to variables $\{y_1 \dots y_{i-1}\}$. The variables of $\mathsf{subexp}_{\pi_i}(\forall y_i \dots y_m \Pi\phi|_{\epsilon,\mu_i})$ can be partitioned into $Z_{0/y_i} = \{z^\alpha \mid z \in Z, \alpha(y_i) = 0\}$ and $Z_{1/y_i} = \{z^\alpha \mid z \in Z, \alpha(y_i) = 1\}$. This completely partitions the variables because y_i is leftmost in the prefix.

Conjunct $C \in \mathsf{subexp}_{\pi_i}(\Pi\phi)|_{\epsilon,\mu_i}$ cannot mix variables Z_{0/y_i} and Z_{1/y_i} since the axiom rule in Definition 1 substitutes one or the other everywhere in the conjunct. Therefore $\mathsf{subexp}_{\pi_i}(\forall y_i \dots y_m \Pi\Phi|_{\epsilon,\mu_i})$ can be written as $A(Z_{0/y_i}) \wedge B(Z_{1/y_i})$ with Q refutation π'_i (based on the Q+$\forall$Exp$_{0,1}$ refutation π_i).

We define a new partial assignment μ_{i+1}, which is defined as $\mu_{i+1}(y_j) = \mu_i(y_j)$ for $1 \leq j < i$ Now we can use condition 2 to extract from π'_i a Q refutation π'_{i+1} of either $A(Z_{0/y_i})$ or $B(Z_{1/y_i})$ in polynomial time. If it is $A(Z_{0/y_i})$ then we let $\mu_{i+1}(y_i) = 0$ and if it is $B(Z_{1/y_i})$ then we let $\mu_{i+1}(y_i) = 1$. π'_{i+1} can be used as part of a Q+$\forall$Exp$_{0,1}$ refutation π_{i+1} of $\forall y_{i+1} \dots y_m \Pi\phi|_{\epsilon,\mu_{i+1}}$ as $\mathsf{subexp}_{\pi_{i+1}}(\forall y_{i+1} \dots y_m \Pi\phi|_{\epsilon,\mu_{i+1}})$ is equal to $A(Z_{0/y_i})$ or $B(Z_{1/y_i})$. Condition 2 guarantees $|\pi'_{i+1}| \leq |\pi'_i|$ so $|\pi_{i+1}| \leq |\pi_i|$ as well.

Once we get to μ_m we have a complete assignment to Y and a guarantee that the remaining QBF game on $\Pi\Phi|_{\epsilon,\mu_m}$ is false by the Q+$\forall$Exp$_{0,1}$ refutation π_m, with $|\pi_m| < |\pi|$.

We can repeat this procedure for every universal block and we end up with the false proposition $\bot$ and since our proof are decreasing in size in each step we guarantee this can be done in a polynomial time procedure.

◀

Note that because of Theorem 10 feasible interpolation is implied by these two conditions (although this can be shown without Theorem 10). This extraction technique is heavily inspired by the one used in [11], instead here we use it for expansion systems.

Conclusion

We have answered the open question of [8] in showing that refutational QRAT does not have strategy extraction, and have introduced a family of QBFs witnessing this fact. In showing the connection between strategy extraction and feasible interpolation we have also formalised one condition for strategy extraction to be present in QBF proof systems using universal expansion. This adds to an existing awareness of the trade-off between strength of QBF proof systems and the ability to offer explanation via winning strategies [4].

References

1 Valeriy Balabanov and Jie-Hong R. Jiang. Resolution proofs and Skolem functions in QBF evaluation and applications. In Ganesh Gopalakrishnan and Shaz Qadeer, editors, *CAV*, volume 6806, pages 149–164. Springer, 2011.

2 Olaf Beyersdorff, Ilario Bonacina, and Leroy Chew. Lower bounds: From circuits to QBF proof systems. In *Proc. ACM Conference on Innovations in Theoretical Computer Science (ITCS'16)*, pages 249–260. ACM, 2016.

3 Olaf Beyersdorff, Leroy Chew, Judith Clymo, and Meena Mahajan. Short proofs in QBF expansion. In Mikoláš Janota and Inês Lynce, editors, *Theory and Applications of Satisfiability Testing – SAT 2019*, pages 19–35, Cham, 2019. Springer International Publishing.

4 Olaf Beyersdorff, Leroy Chew, and Mikoláš Janota. Proof complexity of resolution-based QBF calculi. In *Proc. Symposium on Theoretical Aspects of Computer Science*, pages 76–89. LIPIcs series, 2015.

5 Olaf Beyersdorff, Leroy Chew, Meena Mahajan, and Anil Shukla. Feasible Interpolation for QBF Resolution Calculi. *Logical Methods in Computer Science*, Volume 13, Issue 2, June 2017. URL: `https://lmcs.episciences.org/3702`, `doi:10.23638/LMCS-13(2:7)2017`.

6 Olaf Beyersdorff, Leroy Chew, Meena Mahajan, and Anil Shukla. Understanding cutting planes for qbfs. *Information and Computation*, 262:141 – 161, 2018. URL: `http://www.sciencedirect.com/science/article/pii/S0890540118301184`, `doi:https://doi.org/10.1016/j.ic.2018.08.002`.

7 Olaf Beyersdorff, Luke Hinde, and Ján Pich. Reasons for hardness in QBF proof systems. *Electronic Colloquium on Computational Complexity (ECCC)*, 24:44, 2017. URL: `https://eccc.weizmann.ac.il/report/2017/044`.

8 Leroy Chew and Judith Clymo. The equivalences of refutational QRAT. In *Theory and Applications of Satisfiability Testing - SAT 2019 - 22nd International Conference, SAT 2019, Lisbon, Portugal, July 9-12, 2019, Proceedings*, pages 100–116, 2019. URL: `https://doi.org/10.1007/978-3-030-24258-9_7`, `doi:10.1007/978-3-030-24258-9\_7`.

9 Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44(1):36–50, 1979.

10 William Craig. Three uses of the Herbrand-Gentzen theorem in relating model theory and proof theory. *The Journal of Symbolic Logic*, 22(3):269–285, 1957.

11 Alexandra Goultiaeva, Allen Van Gelder, and Fahiem Bacchus. A uniform approach for generating proofs and strategies for both true and false QBF formulas. In Toby Walsh, editor, *International Joint Conference on Artificial Intelligence IJCAI*, pages 546–553. IJCAI/AAAI, 2011.

12 Marijn Heule, Martina Seidl, and Armin Biere. Efficient extraction of skolem functions from QRAT proofs. In *Formal Methods in Computer-Aided Design, FMCAD 2014, Lausanne, Switzerland, October 21-24, 2014*, pages 107–114, 2014. URL: `https://doi.org/10.1109/FMCAD.2014.6987602`, `doi:10.1109/FMCAD.2014.6987602`.

13 Marijn Heule, Martina Seidl, and Armin Biere. A unified proof system for QBF preprocessing. In *Automated Reasoning - 7th International Joint Conference, IJCAR 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 19-22, 2014. Proceedings*, volume

8562, pages 91–106. Springer, 2014. URL: `https://doi.org/10.1007/978-3-319-08587-6_7`, `doi:10.1007/978-3-319-08587-6\_7`.

14 Mikoláš Janota, William Klieber, João Marques-Silva, and Edmund M. Clarke. Solving QBF with counterexample guided refinement. In Alessandro Cimatti and Roberto Sebastiani, editors, *Proc. 15th International Conference on Theory and Applications of Satisfiability Testing*, volume 7317, pages 114–128. Springer, 2012.

15 Mikoláš Janota and Joao Marques-Silva. Expansion-based QBF solving versus Q-resolution. *Theor. Comput. Sci.*, 577:25–42, 2015.

16 Benjamin Kiesl, Marijn J. H. Heule, and Martina Seidl. A little blocked literal goes a long way. In Serge Gaspers and Toby Walsh, editors, *Theory and Applications of Satisfiability Testing – SAT 2017*, pages 281–297, Cham, 2017. Springer International Publishing.

17 Benjamin Kiesl and Martina Seidl. QRAT polynomially simulates ∀Exp+Res. In Mikoláš Janota and Inês Lynce, editors, *Theory and Applications of Satisfiability Testing – SAT 2019*, pages 193–202, Cham, 2019. Springer International Publishing.

18 Hans Kleine Büning and Uwe Bubeck. Theory of quantified Boolean formulas. In Armin Biere, Marijn Heule, Hans van Maaren, and Toby Walsh, editors, *Handbook of Satisfiability*, volume 185 of *Frontiers in Artificial Intelligence and Applications*, pages 735–760. IOS Press, 2009.

19 Jan Krajíček. Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997.

20 Florian Lonsing and Uwe Egly. QRAT+: generalizing QRAT by a more powerful QBF redundancy property. *CoRR*, abs/1804.02908, 2018. URL: `http://arxiv.org/abs/1804.02908`, `arXiv:1804.02908`.

21 Pavel Pudlák. Lower bounds for resolution and cutting planes proofs and monotone computations. *The Journal of Symbolic Logic*, 62(3):981–998, 1997.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il