Reasons for Hardness in QBF Proof Systems[*]

Olaf Beyersdorff[1], Luke Hinde[2], and Ján Pich[3]

1 School of Computing, University of Leeds, UK
2 School of Computing, University of Leeds, UK
3 Kurt Gödel Research Center, University of Vienna, Austria

Abstract

We aim to understand inherent reasons for lower bounds for QBF proof systems, and revisit and compare two previous approaches in this direction.

The first of these relates size lower bounds for strong QBF Frege systems to circuit lower bounds via *strategy extraction* (Beyersdorff & Pich, LICS'16). Here we show a refined version of strategy extraction and thereby for any QBF proof system obtain a trichotomy for hardness: (1) via circuit lower bounds, (2) via propositional Resolution lower bounds, or (3) 'genuine' QBF lower bounds.

The second approach tries to explain QBF lower bounds through *quantifier alternations* in a system called relaxing QU-Res (Chen, ICALP'16). We prove a strong lower bound for relaxing QU-Res, which also exhibits significant shortcomings of that model. Prompted by this we propose an alternative, improved version, allowing more flexible oracle queries in proofs. We show that lower bounds in our new model correspond to the trichotomy obtained via strategy extraction.

1998 ACM Subject Classification F.2.2 Nonnumerical Algorithms and Problems

Keywords and phrases proof complexity, quantified Boolean formulas, resolution, lower bounds

Digital Object Identifier 10.4230/LIPIcs.FSTTCS.2017.14

1 Introduction

Proof complexity studies the question of how difficult it is to prove theorems in different formal proof systems. The main question is thus: given a theorem ϕ and proof system P, what is the size of the shortest proof of ϕ in P? This research has strong and productive connections to several other areas, most notably to computational complexity, with the aim of separating complexity classes through Cook's programme [14, 11], and to first-order logic (theories of bounded arithmetic [26, 13]). In recent years, progress in practical SAT- and QBF-solving has been a major motivation for proof complexity, as runs of SAT-solvers correspond to proofs of the (un)satisfiability of CNFs. Analysis of the corresponding proof system provides a framework for understanding the power and limitations of the solver [11].

The majority of work in proof complexity has been focused on *propositional proof complexity*, on proof systems for classical propositional logic. In particular, Resolution [32] has received much attention as it models the approach taken by many modern SAT-solvers.

QBF proof complexity is a comparatively young field, studying proof systems for quantified Boolean formulas. Determining the truth of a QBF is PSPACE-complete, and so has wider ranging applications than SAT-solving, extending to fields such as formal verification and planning [3, 31, 15]. Similarly to the propositional case, several Resolution-based QBF

[*] Supported by grant no. 48138 from the John Templeton Foundation and by the Austrian Science Fund (FWF) under project number 28699.

37th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2017).
Editors: Satya Lokam and R. Ramanujam; Article No. 14; pp. 14:1–14:15
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

proof systems have been suggested and analysed [24, 36, 1, 17, 5, 22, 7, 6, 35, 29] to model the approaches taken by QBF solvers. Of particular importance are Q-Resolution [24] and universal Q-Resolution (QU-Res) [17], which as analogues of propositional Resolution form the base systems for conflict-driven clause learning (CDCL) QBF solving [18].

Stronger systems in the form of QBF cutting planes [8] or QBF Frege systems [4] were developed recently by adding to the propositional system a single ∀-reduction rule to handle universal quantifiers. As in the propositional framework, by restricting the lines in Frege to a circuit class $\mathcal{C}$, such as AC^0, NC^1 or $P/poly$, we obtain a hierarchy of (QBF) $\mathcal{C}$-Frege systems, corresponding to the hierarchy of circuit classes.

A conceptually simple but powerful technique for constructing QBF proof size lower bounds from Boolean circuit lower bounds was developed in [6, 4]. This *strategy extraction technique* employs the complexity of Herbrand functions witnessing the universal quantifiers. In [4] the technique was used to show strong lower bounds for QBF Frege systems, including exponential lower bounds for QBF $AC^0[p]$-Frege (in stark contrast to the propositional situation, where lower bounds for $AC^0[p]$-Frege are wide open).

Recent work has tightened the connection to circuit complexity further. In [9] it was shown that for natural circuit classes $\mathcal{C}$, a lower bound for proof size in QBF $\mathcal{C}$-Frege corresponds to either a lower bound for propositional $\mathcal{C}$-Frege, or a lower bound for the circuit class $\mathcal{C}$. This characterisation points to a distinction between QBF lower bounds derived from those on propositional proof systems, and 'genuine' QBF lower bounds.

More widely, *understanding the reasons of hardness* for QBF proof systems and solving constitutes a major challenge, which currently is only insufficiently mastered. Most QBF proof systems use a propositional system such as Resolution or Frege as their core, implying that on existentially quantified formulas the QBF system and the classical core system coincide. This leads to the rather disturbing fact that lower bounds for e.g. Resolution trivially lift to any of the studied QBF Resolution systems.

Motivated by this observation, Chen [12] introduced the new notions of *relaxing QU-Res* and a *proof system ensemble*, with the aim of distinguishing 'genuine' QU-Res lower bounds, arising from the alternation of quantifiers, from those lifted from propositional Resolution. Quantifier alternation has also been empirically observed as a source of hardness [28, 27], making this a very interesting direction for theoretical study.

Our Contributions. The main aim of this paper is to gain a refined understanding of the reasons for QBF hardness, both following the strategy extraction paradigm [9] and the paradigm via quantifier alternation [12]. We revisit both models and relate them in their explanatory power.

A. Refinement of formalised strategy extraction. We describe a decomposition of QBF solving into SAT solving and a search for small circuits witnessing a given QBF. This relies on an improvement of the strategy extraction theorem from [9] which says that, given polynomial-size QBF $\mathcal{C}$-Frege proofs of QBFs ψ_n, one can construct small $\mathcal{C}$ circuits witnessing the existential quantifiers in ψ_n in such a way that the resulting 'witnessed' propositional formulas have polynomial-size proofs in $\mathcal{C}$-Frege. Here, we show that in fact the witnessed formulas have polynomial-size proofs even in tree-like Resolution (Theorem 1).

Applying a similar decomposition, we observe that polynomial-size lower bounds on a sequence of QBFs in any QBF proof system can be categorized as either (1) a circuit lower bound, (2) a Resolution lower bound, or (3) a genuine QBF lower bound (Theorem 2).

B. Lower bounds for relaxing QU-Res. We revisit relaxing QU-Res, introduced in [12] with the aim of distinguishing propositional bounds from QBF bounds arising from quantifier alternation. The exponential lower bound for relaxing QU-Res given in [12] applies only to quantified Boolean circuits with no small CNF representations (Appendix **??**). As this is a somewhat atypical feature in proof complexity, we improve this by presenting QBFs with CNF matrices that require exponential-size relaxing QU-Res proofs (Theorem 9). Our formulas use a new construction that combines two false QBFs Φ and Ψ into a product formula $\Phi \otimes \Psi$ such that any short QU-Res proof must refute Ψ before Φ.

These product formulas have another compelling feature: their hardness for relaxing QU-Res (and QU-Res) rests on the hardness of the pigeonhole principle for propositional Resolution. Our lower bound therefore suggests that relaxing QU-Res does not capture 'genuine' QBF hardness due to quantifier alternation.

C. New systems for 'genuine' QBF hardness. Noting this situation, we propose new QBF proof systems, Σ_k^p-QU-Res (Def. 15). The systems bear similarities to relaxing QU-Res, particularly in the use of relaxations of quantifiers and a proof checking algorithm with access to a Σ_k^p-oracle. The major difference is that oracle queries in our algorithm may appear at any point in the proof.

It is interesting to relate lower bounds in Σ_1^p-QU-Res to our trichotomy shown in A. In this direction, we prove that Σ_1^p-QU-Res admits strategy extraction by depth-3 Boolean circuits (Lemma 18). Hence QU-Res lower bounds stemming from circuit lower bounds (case (1) in the trichotomy in A) translate to lower bounds in Σ_1^p-QU-Res. Further, if a QBF is hard for QU-Res due to a Resolution lower bound (case (2) in A), it has short proofs in Σ_1^p-QU-Res. We also demonstrate that a variant of the prominent formulas of Kleine Büning et al. [24] simultaneously has genuine QBF lower bounds as per case (3) in A (Theorem 4) and is hard for Σ_k^p-QU-Res proofs for any constant k (Theorem 22).

Organisation. In Sec. 2 we detail necessary background. Section 3 refines formalised strategy extraction and the characterisation of QBF lower bounds from [9]. In Sec. 4 we show the lower bound for relaxing QU-Res. Section 5 contains the definition of Σ_k^p-QU-Res and a comparison of lower bounds in these systems with the characterisation in Sec. 3. In Sec. 6, we analyse the hardness of several QBF families in these proof systems.

2 Preliminaries

Quantified Boolean Formulas. A (prenex normal form) *quantified Boolean formula* (QBF) $\Phi = \mathcal{Q}_1 x_1 \dots \mathcal{Q}_n x_n . \phi(x_1, \dots, x_n)$ consists of a propositional formula ϕ, usually expressed as a CNF, and a quantifier prefix $\mathcal{Q}_1 x_1 \dots \mathcal{Q}_n x_n$, where each $\mathcal{Q}_i \in \{\exists, \forall\}$ ranges over $\{0, 1\}$.

The semantics of such a QBF can be considered as a game between players $\exists$ and $\forall$. On the ith turn, the player corresponding to $\mathcal{Q}_i$ assigns a 0/1 value to x_i. After all the variables have been assigned, the $\exists$ player (resp. $\forall$ player) wins the game if ϕ evaluates to 1 (resp. 0).

Given a variable x_i, a *strategy* for x_i is a function $\sigma_i : \{x_1, \dots, x_{i-1}\} \to \{0, 1\}$. A *winning strategy* for the $\exists$ (resp. $\forall$) player, consists of a strategy for each existential (resp. universal) variable which wins all possible games on Φ. A QBF is false (resp. true) if and only if there is a winning strategy for the $\forall$ player (resp. $\exists$ player).

The quantifier complexity of a QBF is described by inductively defined classes Σ_i^b and Π_i^b, counting the number of quantifier alternations. By Σ_i^p (resp. Π_i^p) we denote the i^{th} level of the polynomial hierarchy, for which deciding truth of Σ_i^b (resp. Π_i^b) formulas is complete.

Proof Complexity. A *proof system* for a language $\mathcal{L}$ is a polynomial-time computable surjective function $f : \{0,1\}^* \to \mathcal{L}$ [14]. If $f(\pi) = \phi$, we say π is an f-proof of ϕ. Given proof systems P and Q for $\mathcal{L}$, P *p-simulates* Q if there is a polynomial-time function t with $P(t(\pi)) = Q(\pi)$ for any π. Two proof systems are *p-equivalent* if they p-simulate each other.

We use proof systems for propositional tautologies and fully quantified true QBFs (and for unsatisfiable formulas and false QBFs; we use the words *proof* and *refutation* interchangeably).

Resolution [32] is one of the best studied propositional proof systems [34]. Given two clauses $C \vee x$ and $D \vee \neg x$, Resolution can derive the clause $C \vee D$. A Resolution proof that a CNF ϕ is unsatisfiable is a derivation of the empty clause $\bot$ using the resolution rule.

QU-Resolution (QU-Res) [17] is a natural extension of Resolution to QBFs. Given a QBF $\Phi = \mathcal{Q}_1 x_1 \ldots \mathcal{Q}_n x_n . \phi$, where ϕ is a CNF, a QU-Res refutation of Φ is a derivation of $\bot$ from the clauses of ϕ. It uses the Resolution rule (with the extra condition that deriving tautological clauses is not allowed) and the $\forall$*-reduction rule*, which from a clause $C \vee l$ with literal l on universal variable x_i (i.e., $l = x_i$ or $l = \neg x_i$) can derive the clause C provided C contains no literals on $x_{i+1}, \ldots, x_n$.

A proof in Resolution (and QU-Res, and other proof systems) can be represented as a directed acyclic graph (dag) with a root labelled by $\bot$, and input vertices labelled with clauses from the CNF. If we restrict the dag to be a tree, we define *tree-like Resolution*, which we denote by R^*. Tree-like Resolution is known to be weaker than Resolution [10].

Frege Systems. Frege systems are common 'textbook' proof systems comprised of a set of axiom schemes and inference rules [14]. Lines of a Frege proof are formulas in propositional variables and Boolean connectives $\wedge, \vee, \neg$. A Frege proof of ϕ is a sequence of formulas, ending with ϕ, in which each formula is either a substitution instance of an axiom, or is inferred from previous formulas by a valid inference rule. We also consider refutational Frege systems, in which we start with the formula $\neg\phi$ and derive a contradiction.

For a given circuit class $\mathcal{C}$, we define $\mathcal{C}$-Frege, as in [23], to be a Frege system which works with lines consisting of circuits in $\mathcal{C}$ and a finite set of derivation rules. If $\mathcal{C}$ consists of all Boolean circuits, then $\mathcal{C}$-Frege is p-equivalent to extended Frege (EF). If $\mathcal{C}$ is restricted to Boolean formulas, i.e. $\mathcal{C} = NC^1$, then NC^1-Frege is Frege as defined above.

An elegant method for extending $\mathcal{C}$-Frege systems to QBF was shown in [4]. The QBF proof system $\mathcal{C}$-Frege+$\forall$-red is a refutational proof system working with circuits from $\mathcal{C}$. The inference rules of $\mathcal{C}$-Frege+$\forall$-red are those of $\mathcal{C}$-Frege, along with the $\forall$-red rule $\frac{L_j(u)}{L_j(u/B)}$, where u is quantified innermost among the variables of the proof line L_j with respect to the quantifier prefix, and the circuit B does not contain any variables right of u. Restricting the circuit B in the $\forall$-red rule to the constants $0, 1$ results in a p-equivalent system [9].

3 Strategy extraction and reasons for hardness

A QBF proof system P has the *strategy extraction property* if for any P-proof π of a QBF ψ of the general form $\forall x_1 \exists y_1 \ldots \forall x_n \exists y_n . \phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$, where ϕ is a propositional formula, there are $|\pi|^{O(1)}$-size circuits C_i witnessing the existential quantifiers in ψ, i.e.

$$\bigwedge_{i=1}^{n} (y_i \leftrightarrow C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \to \phi(x_1, \ldots, x_n, y_1, \ldots, y_n). \quad (1)$$

The strategy extraction is *Q-formalised* if, in addition, the propositional formulas (1) have $|\pi|^{O(1)}$-size proofs in a propositional proof system Q.

For any QBF ψ, either there is a propositional formula as in (1) equivalent to ψ, or there are no (small) circuits C_i witnessing the existential variables, and so no QBF proof system with the strategy extraction property can prove ψ feasibly.

The task of *QBF solving based on proof systems admitting strategy extraction is thus reducible to the task of finding the witnessing circuits C_i, and then SAT solving of the witnessed formula.* Alternatively, we can speak about a reduction of QBF solving to Σ_2^q-formulas with existentially quantified witnessing circuits: $\exists C_1, \ldots, C_n \forall x_1, \ldots, x_n, y_1, \ldots, y_n.\ \bigwedge_{i=1}^n (y_i \leftrightarrow C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \rightarrow \phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$.

We will show that all QBF proof systems P p-simulated by EF+$\forall$-red[1] have R^*-formalized strategy extraction. More precisely, we improve the formalised strategy extraction for EF+$\forall$-red from [9] by observing that the witnessing circuits can encode extension variables, which allows us to replace the EF proof of the witnessed formula with an R^* proof.

Consequently, instead of determining whether there is a short P-proof of ψ, one can solve the equivalent problem of whether there are small circuits C_i and a short R^*-proof of (1). As R^* is quasi-automatisable (i.e., R^* refutations for a given CNF can be constructed in quasi-polynomial time in the size of the smallest R^* proof [2]), the problem is essentially reduced to the search for the right witnessing circuits C_i.

▶ **Theorem 1.** *Let $\mathcal{C}$ be the circuit class NC^1 or $P/poly$.*[2] *Given a $\mathcal{C}$-Frege+$\forall$-red refutation π of a QBF $\exists x_1 \forall y_1 \ldots \exists x_n \forall y_n.\ \phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$ where $\phi \in \Sigma_0^b$, we can construct in time $|\pi|^{O(1)}$ an R^* refutation of the witnessed formula $\bigwedge_{i=1}^n (y_i \leftrightarrow C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \wedge \phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$ for some circuits $C_i \in \mathcal{C}$.*

Proof. By the formalised strategy extraction theorem for $\mathcal{C}$-Frege systems [9], there is a $\mathcal{C}$-Frege proof of the witnessed formula (1). This means there is an R^* refutation of $Ext \wedge \bigwedge_{i=1}^n (y_i \leftrightarrow C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \wedge \phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$ where Ext is a set of extension axioms defining $\mathcal{C}$ formulas on the variables $x_1, \ldots, x_n, y_1, \ldots, y_n$. With the exception of those depending on y_n, these axioms can be encoded into circuits C_i with each extension variable represented by a possibly redundant gate of a circuit C_i. In order to remove the extension variables depending on y_n, we construct two independent R^* refutations, one with all occurrences of y_n in clauses of Ext substituted by 0 and the other with occurrences of y_n in Ext substituted by 1. This results in two R^* derivations, both at most as large as the original, one concluding with $\{y_n\}$ and the other with $\{\neg y_n\}$. Resolving on these two clauses we obtain the needed R^* derivation without extension variables depending on y_n. ◀

The reduction of QBF solving to SAT solving presented above is also of use for proving QBF proof complexity lower bounds. In [9] it was shown that any super-polynomial lower bound on EF+$\forall$-red is either a super-polynomial circuit lower bound or a super-polynomial lower bound on EF. Here we generalise this phenomenon to other QBF proof systems.

Let P be a refutational QBF proof system operating on clauses of matrices of (prenex normal form) QBFs which contains a resolution rule that allows resolution on both existential and universal variables. We say that a set of clauses C defines a formula $C_i(\vec{x}) = z$ for a circuit C_i with input variables $\vec{x}$ and output variable z if z appears in a literal of some clause in C and for any assignment of the input variables there is exactly one assignment of the remaining variables satisfying all clauses in C.

[1] This includes all commonly studied Resolution-based QBF systems.

[2] The result easily generalises to further 'natural' circuit classes $\mathcal{C}$ such as AC^0 or TC^0, but we will focus here on the two most interesting cases NC^1 and $P/poly$ leading to Frege and EF systems, respectively.

Whenever a QBF ψ as above is hard for a QBF proof system P it is for one of the following reasons:

1. the existential quantifiers in ψ cannot be witnessed by circuits C_i such that formulas $\bigwedge_i C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1}) = y_i$ have $|\phi|^{O(1)}$-size P-derivations from $\neg\phi$.
2. the existential quantifiers in ψ are witnessable as in 1. but the witnessed formula $\bigwedge_{i=1}^{n} (y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})) \wedge \neg\phi(x_1, \dots, x_n, y_1, \dots, y_n)$ is hard for Resolution.

This characterisation can be specified further.

▶ **Theorem 2.** *Let P be a refutational QBF proof system as above admitting strategy extraction by $\mathcal{C}$ circuits. If $\psi_n = \forall x_1 \exists y_1 \dots \forall x_n \exists y_n .\, \phi_n(x_1, \dots, x_n, y_1, \dots, y_n)$ are QBFs with propositional CNF ϕ_n, which do not have polynomial-size proofs in P, then one of the following holds:*

1. ***Circuit lower bound.*** *The existential variables in ψ_n are not witnessable by $\mathcal{C}$ circuits.*
2. ***Resolution lower bound.*** *Condition 1. does not hold, but for all $\mathcal{C}$ circuits witnessing ψ_n, the witnessed formulas require super-polynomial size Resolution refutations.*
3. ***Genuine QBF hardness.*** *There are circuits $C_i \in \mathcal{C}$ witnessing ψ_n so that the witnessed formulas have polynomial-size Resolution refutations, but for all such circuits C_i it is hard to derive $\bigwedge_i C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1}) = y_i$ from $\neg\phi_n$ in P.*

This means that any QBF lower bound on P is either a circuit lower bound, a propositional proof complexity lower bound, or a 'genuine' QBF proof complexity lower bound in the sense that P cannot derive efficiently some circuits witnessing the existential quantifiers in the original formula and whenever it can do that for some other witnessing circuits, the witnessed formula is hard for Resolution.

The last possibility does not happen in the case of strong systems like EF+∀-red [9]. The situation is, however, more delicate with weaker systems, where we can encounter 'genuine' QBF lower bounds. We give an example.

▶ **Definition 3** (Kleine Büning et al. [24]). The QBFs KBKF_n are defined as $\exists y_0 y_1 y_1' \forall x_1 \dots \exists y_k y_k' \forall x_k \dots \forall x_n \exists y_{n+1} \dots y_{n+n} .\, \bigwedge_{i=1}^{2n} C_i \wedge C_i'$, where

$$\begin{aligned} C_0 &= \{\neg y_0\} & C_0' &= \{y_0, \neg y_1, \neg y_1'\} \\ C_k &= \{y_k, \neg x_k, \neg y_{k+1} \neg y_{k+1}'\} & C_k' &= \{y_k', x_k, \neg y_{k+1}, \neg y_{k+1}'\} \\ C_n &= \{y_n, \neg x_n, \neg y_{n+1}, \dots, \neg y_{n+n}\} & C_n' &= \{y_n', x_n, \neg y_{n+1}, \dots, y_{n+n}\} \\ C_{n+t} &= \{x_t, y_{n+t}\} & C_{n+t}' &= \{\neg x_t, y_{n+t}\} \end{aligned}$$

These QBFs are known to require proofs of size $2^{\Omega(n)}$ in Q-Resolution [24, 6]. This bound can be extended to QU-Res using the formulas KBKF_n', obtained by adding new universal variables z_k, quantified at the same level as x_k, and adding the literal z_k or $\neg z_k$ to each clause containing x_k or $\neg x_k$, respectively [1].

▶ **Theorem 4.** *The formulas KBKF_n' are hard for QU-Res due to genuine QBF hardness (case 3 in Theorem 2).*

Proof Sketch. The strategy $x_k = z_k = y_k'$ is a short winning strategy for the ∀-variables, and has a linear-size refutation by first deriving each y_{n+t}, then y_n' and y_n, and each y_i' and y_i in turn, concluding by resolving y_0 and $\neg y_0$. ◀

4 Hardness due to quantifier alternation

The characterisation of QBF proof system lower bounds given above is a very natural one. We now seek to show that it corresponds with hardness due to alternation, another often suggested reason for hardness.

Most studied QBF proof systems build on a propositional proof system (e.g. Resolution), and coincide with this base system on Σ_1^b-formulas. Any propositional lower bound is therefore also a QBF lower bound. An alternative characterisation of QBF lower bounds based on the alternation of quantifiers in the quantifier prefix has been suggested, with the aim of distinguishing between such propositional lower bounds and 'genuine' QBF lower bounds arising from the alternation of quantifiers. Relaxing QU-Res has previously been put forward as a proof system to determine hardness due to quantifier alternation [12].

▶ **Definition 5** (Chen [12]). For a quantifier prefix $\Pi = \mathcal{Q}_1 x_1 \dots \mathcal{Q}_n x_n$, if π is a permutation such that $\pi(i) < \pi(j)$ whenever $i < j$ and $\mathcal{Q}_i = \forall$ and $\mathcal{Q}_j = \exists$, then the prefix $\Pi' = \mathcal{Q}_{\pi(1)} x_{\pi(1)} \dots \mathcal{Q}_{\pi(n)} x_{\pi(n)}$ is a *relaxation.* Intuitively, a relaxation involves 'moving $\forall$-variables to the left'. If Π' is a Σ_k^b-prefix, we call Π' a Σ_k^b*-relaxation.*

Let $\Phi = \Pi.\phi$ be a QBF. For a clause A, let α be the assignment falsifying each literal in A. Construct $\Pi[\alpha]$ by removing all variables in α, and replacing any $\forall$-quantifers left of a variable in α by $\exists$. If there is some Π_k^b-relaxation $\Pi'[\alpha]$ of $\Pi[\alpha]$ such that $\Pi'[\alpha].\phi[\alpha]$ is false, then $A \in H(\Phi, \Pi_k^b)$.

A *Relaxing QU-Res* proof of a QBF Φ uses the same deduction rules as QU-Res, but can introduce any axiom from the set $H(\Phi, \Pi_k^b)$ for some constant k.

For any propositional CNF, or indeed any QBF with a prefix with bounded alternation, relaxing QU-Res has constant-size proofs, whereas QU-Res may require exponential-size proofs. However, lower bounds for both tree-like and dag-like relaxing QU-Res were also shown in [12]. The lower bound for dag-like relaxing QU-Res in [12] is rather unconventional as the proof system works with clauses, whereas the lower bound applies to circuits without polynomial-size CNF representations. We present formulas with polynomially many clauses that require exponential-size proofs in relaxing QU-Res.

Furthermore, the lower bounds we show on the size of QU-Res proofs of these formulas are clearly due to a lower bound on Resolution proofs, rather than alternation of quantifiers, or any other 'genuine' QBF reasons. It follows that this is the case for relaxing QU-Res as well, demonstrating that relaxing QU-Res is not an adequate formalism to distinguish propositional lower bounds from genuine QBF lower bounds.

To begin, we present a method of combining two false QBFs to produce another false QBF. This method might also be of independent interest for the creation of hard QBFs.

▶ **Definition 6.** Let $\Phi = \Lambda(\vec{x}) \cdot \bigwedge_{i=1}^{n} C_i(\vec{x})$ and $\Psi = \Pi(\vec{z}) \cdot \bigwedge_{j=1}^{m} D_j(\vec{z})$ be QBFs consisting of quantifier prefixes Λ and Π over the disjoint sets of variables $\vec{x}$ and $\vec{z}$ respectively, and of clauses C_i and D_j over the corresponding variables. Then, with $\vec{x}$ and each $\vec{z}_i$ distinct variables, define

$$\Phi \otimes \Psi := \Lambda(\vec{x})\Pi(\vec{z}_1) \dots \Pi(\vec{z}_n) \cdot \bigwedge_{i=1}^{n} \bigwedge_{j=1}^{m} (C_i(\vec{x}) \vee D_j(\vec{z}_i)) \,.$$

The QBF $\Phi \otimes \Psi$ is false if and only if Φ and Ψ are false. Combining winning strategies for the universal variables of Φ and Ψ constructs a strategy which falsifies some $C_i(\vec{x})$ and, for each i, falsifies some $D_j(\vec{z}_i)$. This strategy therefore falsifies some $C_i(\vec{x}) \vee D_j(\vec{z}_i)$. The following lemma establishes that the proof size for $\Phi \otimes \Psi$ is bounded by the size of proofs required by Φ and Ψ, and indeed is precisely determined by it in the case of QU-Res.

▶ **Lemma 7.** *Let $\Phi = \vec{\mathcal{Q}}. \bigwedge_{i=1}^{n} C_i$ and $\Psi = \vec{\mathcal{S}}. \bigwedge_{j=1}^{m} D_j$ be minimally unsatisfiable QBFs. Let $S_P(\Lambda)$ be the size of the smallest P-proof of a QBF Λ. Then $\max(S_P(\Phi), S_P(\Psi)) \leq S_P(\Phi \otimes \Psi) \leq S_P(\Phi) + n \cdot S_P(\Psi)$. Moreover, if P is QU-Res, then $S_P(\Phi \otimes \Psi) = S_P(\Phi) + n \cdot S_P(\Psi)$.*

Proof. All clauses of $\Phi \otimes \Psi$ are necessary for a refutation. By assigning variables from Φ or the copies of Ψ appropriately, the lines in the proof can be restricted to a refutation of Φ or Ψ, and so $max(S_P(\Phi), S_P(\Psi)) \leq S_P(\Phi \otimes \Psi)$. Since $\Phi \otimes \Psi$ can be refuted by first deriving each clause C_i from $\bigwedge_{j=1}^{m}(C_i(\vec{x}) \vee D_j(\vec{z_i}))$, which can be done in $S_P(\Psi)$, and then refuting $\bigwedge_{i=1}^{n} C_i(\vec{x})$ with size $S_P(\Phi)$, we can find a refutation of $\Phi \otimes \Psi$ of size $S_P(\Phi) + n \cdot S_P(\Psi)$.

In QU-Res, each resolution step or ∀-reduction step is performed on only one variable, and so will only remain in one of the proofs of Φ or $\Psi(\vec{z_i})$, being replaced by a weakening or trivial step in all others. Any QU-Res proof of $\Phi \otimes \Psi$ must therefore have size at least $S_P(\Phi) + n \cdot S_P(\Psi)$. By the upper bound shown above, there is equality. ◀

We use this method to construct a family of false QBFs that require exponential-size proofs in QU-Res. These QBFs are the product of propositional formulas hard for Resolution and of QBFs easy for QU-Res. By Lemma 7, it is clear that the hardness of this product is derived only from the propositional lower bound. Yet, these product formulas are also hard for relaxing QU-Res. The QBF is obtained by taking the product of the pigeonhole principle, defined below, and the formulas by Kleine Büning et al. [24] (Definition 3).

▶ **Definition 8.** The *pigeonhole principle* PHP_n^m, for m pigeons and n holes, is the CNF $\bigwedge_{i=1}^{m} (x_{i,1} \vee \cdots \vee x_{i,n}) \wedge \bigwedge_{j=1}^{m} \bigwedge_{1 \leq i_1 < i_2 \leq n} (\neg x_{i_1,j} \vee \neg x_{i_2,j})$.

For $m > n$, this is unsatisfiable, and for $m = n + 1$ it is known that $2^{\Omega(n)}$ clauses are required to refute it in Resolution, and indeed in any constant-depth Frege system [19, 30, 25].

▶ **Theorem 9.** *Any relaxing QU-Res proof of $\Phi_n := \mathrm{PHP}_n^{n+1} \otimes \mathrm{KBKF}_n$ has size $2^{\Omega(n)}$.*

When restricted to a propositional formula, QU-Res is equivalent to Resolution, and PHP_n^{n+1} requires proofs of size $2^{\Omega(n)}$ in Resolution [19], so PHP_n^{n+1} requires QU-Res proofs of size at least $2^{\Omega(n)}$. In QU-Res, the formulas KBKF_n have linear-size proofs [17]. Given the precise determination of the size of QU-Res proofs of Φ_n by Lemma 7, this QU-Res lower bound for Φ_n is unambiguously due to the lower bound for PHP_n^{n+1} in Resolution.

We first note that any relaxation of KBKF_n is true.

▶ **Lemma 10.** *Any relaxation of the quantifier prefix of KBKF_n to a Π_t^b prefix results in a true QBF, for any $t < n$.*

Proof Sketch. Any relaxation must quantify some x_i left of y_i, y_i'. The winning strategy for each x_i depends on y_i, y_i' and so there is a winning strategy for the existential player by playing y_i, y_i' according to x_i. ◀

Any clause in the variables of Φ_n can be written as $X \vee Z_1 \vee \cdots \vee Z_m$ where X is a clause in the variables of $\vec{x}$, and Z_i is a clause in the variables of $\vec{z_i}$. We use the terms Z-variables and X-variables to refer to any variables in $\vec{z}_1, \ldots, \vec{z}_m$ and $\vec{x}$ respectively. Similarly, given a clause C, we use X-clause and Z-clause to refer to the restriction of C to the X-variables and Z-variables, and denote these by C^X and C^Z.

To prove Theorem 9, we show that if the oracle deriving axioms 'proves' a large part of the pigeonhole principle when deriving an axiom, it can only do so under a large restriction on the existential variables of the copies of KBKF_n. Thus a relaxing QU-Res proof of Φ_n must contain a large proof of the pigeonhole principle, or a large number of different restrictions on the copies of KBKF_n.

To this end, we first show that, for any clause A derived as an axiom by relaxing QU-Res, if A^X requires at least c clauses from PHP^{n+1}_n to prove, then it also contains at least c existentially quantified Z-variables (Lemma 11). We then establish an upper bound on the size of a proof of an X-clause derived from c axioms of PHP^{n+1}_n which depends only on c (Lemma 12). Using this, we conclude that any relaxing QU-Res axiom where the corresponding X-clause requires proofs of size 2^k must contain $\Omega(k)$ Z-variables (Corollary 13).

Lastly, we show that given any relaxing QU-Res proof, for each assignment to the Z-variables, we can find an axiom containing $\Omega(n)$ Z-variables which agrees with the given Z-assignment (Lemma 14). From this, we conclude that the proof must contain $2^{\Omega(n)}$ axioms.

▶ **Lemma 11.** *Suppose that the clause $A = A^X \vee A^Z$ is derived as an axiom of Φ_n by relaxing QU-Res. Let $Z_{i_1}, \dots, Z_{i_l}$ be such that all the existential variables in A^Z are in some Z_{i_j}. Then $C_{i_1} \wedge \cdots \wedge C_{i_l} \models A^X$ for the corresponding pigeonhole principle axioms $C_{i_1}, \dots, C_{i_l}$.*

Proof Sketch. If not, there is some smallest assignment α satisfying $C_{i_1} \wedge \cdots \wedge C_{i_l} \wedge \neg A$. For any Π^b_k-relaxation Φ', we extend this to a winning strategy for the existential player. On variables in Z_{i_j} for some $1 \leq j \leq l$, the strategy is arbitrary as α already satisfies C_{i_j}. On variables in Z_k where $k \neq i_j$ for any $1 \leq j \leq l$, no variables from Z_k are defined in α so we use a winning strategy for the relevant relaxation of KBKF_n in the variables of Z_k.

As no Π^b_k-relaxation of $\Phi[\alpha]$ is true, A is not an axiom in relaxing QU-Res. ◀

By Lemma 11, if relaxing QU-Res derives an axiom A, and any proof of A^X requires l axioms from PHP^{n+1}_n, then A contains existential variables from l different Z_i. In particular, A contains at least l distinct Z-variables.

Lemma 12 gives an upper bound for the size of Resolution proofs from a fixed number of axioms from PHP^{n+1}_n. From this and Lemma 11 follows the key observation for the proof of Theorem 9, that for any relaxing QU-Res axiom A, if A^X requires a large Resolution derivation from the pigeonhole principle then A contains a large number of Z-variables.

▶ **Lemma 12.** *Suppose C is a clause such that $C_1 \wedge \cdots \wedge C_t \models C$ for some axioms $C_1, \dots, C_t$ from PHP^{n+1}_n. Then there is a Resolution proof of C from PHP^{n+1}_n of size at most 18^t.*

Proof Sketch. As all negative literals are in axioms of width two, the axioms contain positive and negative literals on at most $2t$ variables. Each axiom may also contain a set of pure literals, so there are at most $3^{2t}2^t$ derivable clauses. ◀

▶ **Corollary 13.** *Let A be an axiom derived from Φ_n by relaxing QU-Res. Let $S(A^X)$ be the size of the smallest Resolution derivation of A^X from PHP^{n+1}_n. Then A contains at least $\frac{1}{\log 18} \log S(A^X)$ existential Z-variables.*

▶ **Lemma 14.** *Given a relaxing QU-Res proof π and an assignment α to the existential Z-variables of Φ_n, $\pi|^X_\alpha$ contains a sound Resolution refutation of the X-axioms corresponding to axioms agreeing with α.*

Proof of Theorem 9. Suppose that π is a relaxing QU-Res proof of Φ_n with $|\pi| = f(n)$. Given an assignment α to the existential Z-variables, $\pi|^X_\alpha$ is a sound Resolution refutation of the X-axioms (Lemma 14), and has at most $f(n)$ axioms. Since any Resolution refutation of PHP^{n+1}_n requires proofs of size at least 2^{kn} for some constant k, some X-axiom B in $\pi|^X_\alpha$ requires a Resolution derivation of size at least $\frac{2^{kn}-f(n)}{f(n)} = \frac{2^{kn}}{f(n)} - 1$. By Corollary 13, there is an axiom A in π such that $A^X = B$, and so A contains at least $c(kn - \log f(n)) =: g(n)$ existential Z-variables, which agree with α.

For every assignment α to the existential Z-variables, we can find such an axiom containing at least $g(n)$ existential Z-variables and agreeing with α. As each of these axioms can agree with at most a $2^{-g(n)}$ proportion of the possible assignments α, π must contain at least $2^{g(n)}$ axioms. As a proof cannot contain more axioms than its length, we conclude that $2^{g(n)} \leq f(n)$, i.e. $2^{ckn} \leq f(n)2^{c \log f(n)} = f(n)^{c+1}$ and so $f(n) = 2^{\Omega(n)}$. Thus any relaxing QU-Res proof of Φ_n has size $2^{\Omega(n)}$. ◀

We have shown that $\mathrm{PHP}_n^{n+1} \otimes \mathrm{KBKF}_n$ requires relaxing QU-Res proofs of size $2^{\Omega(n)}$, despite consisting of a hard propositional formula for Resolution combined with a QBF which is easy for QU-Res. This strengthens previous lower bounds for relaxing QU-Res, as well as demonstrating a QBF which is hard due to Resolution but also hard for relaxing QU-Res.

5 An alternative definition of hardness from alternation

We now define a family of proof systems which do characterise whether a QBF lower bound is due to quantifier alternation, or due to a propositional lower bound. As expected, $\mathrm{PHP}_n^{n+1} \otimes \mathrm{KBKF}_n$ have short proofs in these proof systems.

▶ **Definition 15.** A Σ_k^p-QU-Res proof of a QBF $\Phi = \Pi.\phi$ is a derivation of the empty clause by any of the rules of QU-Res, or the Σ_k^p*-derivation* rule $\frac{C_1 \ \dots \ C_l}{D}$ for any l, where there is some Σ_k^b-relaxation Π' of the quantifier prefix Π such that $\Pi'. \bigwedge_{i=1}^{l} C_i \models \Pi'.D \wedge \bigwedge_{i=1}^{l} C_i$.

In the context of these proof systems, we define a Σ_k^b-relaxation of a quantifier prefix as in Definition 5, i.e. any movement of $\forall$-variables to the left, but also allow replacing any $\forall$ quantifier by $\exists$. Allowing this replacement is not necessary, but, as shown in Lemma 19, it allows us to restrict our attention to Σ_{2k+1}^p-QU-Res, eliminating the need for a similarly defined Π_m^p-QU-Res.

It is straightforward to define Σ_k^p-P similarly for any line-based QBF proof system P, and several of the following results for QU-Res have analogues in these systems.

Any QU-Res proof is also a Σ_k^p-QU-Res proof, so Σ_k^p-QU-Res is complete. For soundness, note that QU-Res (with weakening) is both sound and inferentially complete [17]. Thus we can replace any Σ_k^p-derivation with a QU-Res derivation consistent with the Σ_k^b-relaxation. This QU-Res derivation will also be consistent with the original quantifier prefix, and so from any Σ_k^p-QU-Res refutation, we can construct such a QU-Res refutation. Since QU-Res is sound, Σ_k^p-QU-Res is therefore also sound.

We can now give our definition of hardness due to quantifier alternation.

▶ **Definition 16.** A family of QBFs is *hard due to quantifier alternation* if it requires superpolynomial-size Σ_1^p-QU-Res refutations.

A QBF family has *alternation hardness* Σ_k^p if it has polynomial-size proofs in Σ_k^p-QU-Res, but requires superpolynomial-size proofs in Σ_{k-1}^p-QU-Res.

The proof complexity of QBFs in Σ_1^p-QU-Res is of particular interest, as recent success in SAT solving has led to some QBF solvers embedding a SAT solver as a black box [33, 21]. The Σ_1^p-oracle access models this technique, and may provide insights into the power and limitations of such QBF solvers. As discussed below, proofs in Σ_1^p-QU-Res also characterise whether a QBF is hard due to a propositional lower bound, or whether the lower bound is, at least in part, derived from the use of universal quantifiers.

In Section 4, the formulas $\mathrm{PHP}_n^{n+1} \otimes \mathrm{KBKF}_n$ were shown to require QU-Res proofs of size $2^{\Omega(n)}$ due to a lower bound on Resolution. However, there are short Σ_1^p-QU-Res proofs of these formulas, even with only a single Σ_1^p-derivation, demonstrating that they are not hard for QU-Res due to quantifier alternation. This is in sharp contrast with the lower bound shown in Theorem 9, despite relaxing QU-Res also using Σ_k^p-oracles.

▶ **Theorem 17.** $\mathrm{PHP}_n^{n+1} \otimes \mathrm{KBKF}_n$ *have* Σ_1^p*-QU-Res proofs of length* $O(n^3)$*.*

Proof Sketch. The refutation first derives each of the $O(n^2)$ axioms of PHP_n^{n+1} in $O(n)$ lines in QU-Res, then derives the empty clause with a Σ_1^p-derivation. ◀

Any clause derived as an axiom of Φ using a Σ_k^p-oracle by relaxing QU-Res can also be derived from the clauses of Φ by a single Σ_k^p-derivation in Σ_k^p-QU-Res. It is easy to see from this that the instance of relaxing QU-Res using Σ_k^p-oracles is p-simulated by Σ_k^p-QU-Res. Theorems 9 and 17 show an exponential separation between even Σ_1^p-QU-Res and relaxing QU-Res for any k.

In order to compare the characterisation of lower bounds by quantifier alternation with the characterisation given in Section 3, we first show that Σ_1^p-QU-Res still has the same strategy extraction property as QU-Res. Analogous strategy extraction results apply for all $\mathcal{C}$-Frege+∀-Red systems.

▶ **Lemma 18.** Σ_1^p*-QU-Res admits strategy extraction by depth-3 Boolean circuits.*

Proof Sketch. The Σ_1^p-derivations can be replaced by Resolution derivations. Strategy extraction in QU-Res is done with circuits polynomial in the number of ∀-reduction steps [4], and so polynomial in the size of the Σ_1^p-QU-Res proof. ◀

As a consequence of Lemma 18, QBFs hard for QU-Res by item 1 of Theorem 2 (strategy extraction) are therefore hard for Σ_1^p-QU-Res. Intuitively, we expect strategy extraction lower bounds to also be lower bounds due to alternation, as the strategy extraction technique inherently relies on universally quantified variables and the order of quantification.

Consider now QBFs hard for QU-Res by item 2 in Theorem 2. There are polynomial-size strategies for the universal variables, but for all of these, the witnessed formulas require superpolynomial-size proofs in Resolution. Using the normal form for proofs described in [9], we can construct short proofs of these QBFs in Σ_1^p-QU-Res, deriving the witnessed formula, then using a Σ_1^p-derivation to derive $\bot$. This demonstrates that QBFs hard by item 2 are not hard due to quantifier alternation.

For sufficiently strong proof systems, such as Frege+∀-red, these are the only two reasons for hardness [9]. As Lemma 18 extends naturally to Σ_1^p-Frege+∀-red, the characterisation of hardness for QBF Frege systems in [9] (circuit lower bounds vs propositional Frege lower bounds) therefore coincides with our characterisation via quantifier alternation.

6 Alternation Hardness of Specific Formulas

Finally, we determine the precise alternation hardness of specific families of QBFs from each of the categories defined in Theorem 2. Not all formulas from the same category necessarily have the same alternation hardness, but the bounds shown here reinforce the distinctions from Theorem 2.

The first step in establishing the alternation hardness of QBFs is to understand which levels we need to consider. The definition of relaxation allows replacing universal quantifiers with existential quantifiers, so we need only consider proof size in Σ_k^p-QU-Res for odd k.

▶ **Lemma 19.** *If a family of QBFs has proofs of size $s(n)$ in Π_m^p-QU-Res or Σ_{2k}^p-QU-Res, then it has proofs of size $n \cdot s(n)$ in Σ_{m-1}^p-QU-Res or Σ_{2k-1}^p-QU-Res respectively. Given a family of QBFs Φ_n, if the alternation hardness of Φ_n is $\mathcal{C}$, then $\mathcal{C} = \Sigma_{2k+1}^b$ for some k.*

Proof Sketch. A Σ_{2k}^p-derivation can be replaced by $\forall$-reduction on the rightmost variables, then a Σ_{2k-1}^p-derivation which quantifies the previously rightmost $\forall$-variables existentially. A Π_k^p-derivation can be replaced by a Σ_{k-1}^p-derivation, with the leftmost $\forall$-variables quantifed existentially, followed by a $\forall$-reduction if necessary. ◀

If the definition of relaxation were restricted to that given in the definition of relaxing QU-Res, by not allowing additional existential quantifiers, then the simulation of Π_m^p-QU-Res by Σ_{m-1}^p-QU-Res would not hold. With the exception of Σ_2^p-QU-Res, it would still be possible to reduce a Σ_{2k}^p-QU-Res proof to a Σ_{2k-1}^p-QU-Res proof by moving the rightmost universal variables leftwards to another block of universal quantifiers.

Lemmas 18 and 19 allow us to determine the precise alternation hardness of QParity_n, which were introduced in [6] as examples of formulas which are hard due to strategy extraction (item 1 in Theorem 2).

▶ **Definition 20** ([6]). The formulas QParity_n consist of the quantifier prefix $\exists x_1 \dots x_n \forall z \exists t_2 \dots t_n$ and clauses expressing that $t_2 \equiv x_1 \oplus x_2$, $t_k \equiv t_{k-1} \oplus x_k$ for each $3 \leq k \leq n$, and $z \equiv \neg t_n$.

The QBFs QParity_n are false, and the only winning strategy for the $\forall$-player is to play $z \equiv \bigoplus_{i=1}^n x_i$. As the parity function is hard to compute for depth-3 circuits [16, 20], any QU-Res proof has size $2^{\Omega(n)}$. The formulas QParity_n are therefore hard due to strategy extraction as defined in Theorem 2.

▶ **Corollary 21.** *The formulas* QParity_n *have Σ_3^b-alternation hardness.*

That the formulas QParity_n have Σ_3^b-alternation hardness shows that they are hard for QU-Res due to the alternation of quantifiers.

It is clear that all formulas which fall under item 2 of Theorem 2, of being hard only due to a lower bound on Resolution, such as PHP_n^{n+1}, have polynomial-size proofs in Σ_1-QU-Res, and so have Σ_1^p-alternation hardness.

The last family of QBFs we consider is KBKF'_n. By Theorem 4, the formulas KBKF'_n are hard for QU-Res due to a genuine QBF lower bound. As their hardness does not originate from a Resolution lower bound, we expect them to be hard due to alternation. In fact, we can go further and show that KBKF'_n are hard for Σ_k^p-QU-Res for all k.

▶ **Theorem 22.** *The formulas* KBKF'_n *require proofs of size $2^{\Omega(n)}$ in Σ_k^p-QU-Res for any constant k.*

▶ **Lemma 23.** *If a clause derived from* KBKF'_n *contains a literal on x_i, and the derivation does not contain a $\forall$-reduction step on x_i, then it contains y_j or y'_j for some $i \leq j \leq 2n$.*

Proof Sketch of Theorem 22. In the expansion to a QU-Res proof, no resolution steps are possible on universal pivots before these variables could be $\forall$-reduced.

For all assignments α to the universal variables, there is a $\forall$-reduction on each x_i containing literals agreeing with α on all universal variables left of x_i. By Lemma 23, these $\forall$-reductions can be chosen to contain a literal on y_i or y'_i. Thus at most k consecutive such $\forall$-reductions can be contained in one Σ_k^p-derivation, and so each of the 2^{n-k} assignments to $x_1, \dots, x_{n-k}$ must appear in full in a clause in the Σ_k^p-QU-Res proof. ◀

7 Conclusion

We have analysed both strategies and alternation as underlying reasons for the size of proofs in QBF proof systems. In the search for 'genuine' QBF lower bounds, these are the two characterisations which have received the most attention. We have shown that, for sufficiently strong proof systems (Frege and above), the two criteria are equivalent, and provided a natural proof system for which all lower bounds are such proper QBF lower bounds.

A natural question is whether for weaker Resolution-based systems, QBFs hard due to item 3 of Theorem 2 are always hard due to alternation. We have shown this only for the case of KBKF'_n in QU-Res. We also leave open the question of finding formulas which have alternation hardness precisely Σ^b_k for odd $k > 3$.

References

1 Valeriy Balabanov, Magdalena Widl, and Jie-Hong R. Jiang. QBF resolution systems and their proof complexities. In Carsten Sinz and Uwe Egly, editors, *Theory and Applications of Satisfiability Testing - SAT 2014 - 17th International Conference, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 14-17, 2014. Proceedings*, volume 8561 of *Lecture Notes in Computer Science*, pages 154–169. Springer, 2014. doi:10.1007/978-3-319-09284-3_12.

2 Paul Beame and Toniann Pitassi. Simplified and improved resolution lower bounds. In *37th Annual Symposium on Foundations of Computer Science, FOCS '96, Burlington, Vermont, USA, 14-16 October, 1996*, pages 274–282. IEEE Computer Society, 1996. doi:10.1109/SFCS.1996.548486.

3 Marco Benedetti and Hratch Mangassarian. QBF-based formal verification: Experience and perspectives. *JSAT*, 5(1-4):133–191, 2008.

4 Olaf Beyersdorff, Ilario Bonacina, and Leroy Chew. Lower bounds: From circuits to QBF proof systems. In Madhu Sudan, editor, *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science, Cambridge, MA, USA, January 14-16, 2016*, pages 249–260. ACM, 2016. doi:10.1145/2840728.2840740.

5 Olaf Beyersdorff, Leroy Chew, and Mikolas Janota. On unification of QBF resolution-based calculi. In Erzsébet Csuhaj-Varjú, Martin Dietzfelbinger, and Zoltán Ésik, editors, *Mathematical Foundations of Computer Science 2014 - 39th International Symposium, MFCS 2014, Budapest, Hungary, August 25-29, 2014. Proceedings, Part II*, volume 8635 of *Lecture Notes in Computer Science*, pages 81–93. Springer, 2014. doi:10.1007/978-3-662-44465-8_8.

6 Olaf Beyersdorff, Leroy Chew, and Mikolás Janota. Proof complexity of resolution-based QBF calculi. In Ernst W. Mayr and Nicolas Ollinger, editors, *32nd International Symposium on Theoretical Aspects of Computer Science, STACS 2015, March 4-7, 2015, Garching, Germany*, volume 30 of *LIPIcs*, pages 76–89. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2015. doi:10.4230/LIPIcs.STACS.2015.76.

7 Olaf Beyersdorff, Leroy Chew, Meena Mahajan, and Anil Shukla. Feasible interpolation for QBF resolution calculi. In Magnús M. Halldórsson, Kazuo Iwama, Naoki Kobayashi, and Bettina Speckmann, editors, *Automata, Languages, and Programming - 42nd International Colloquium, ICALP 2015, Kyoto, Japan, July 6-10, 2015, Proceedings, Part I*, volume 9134 of *Lecture Notes in Computer Science*, pages 180–192. Springer, 2015. doi:10.1007/978-3-662-47672-7_15.

8 Olaf Beyersdorff, Leroy Chew, Meena Mahajan, and Anil Shukla. Understanding cutting planes for qbfs. In Akash Lal, S. Akshay, Saket Saurabh, and Sandeep Sen, editors, *36th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2016, December 13-15, 2016, Chennai, India*, volume 65

of *LIPIcs*, pages 40:1–40:15. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016. doi:10.4230/LIPIcs.FSTTCS.2016.40.

9 Olaf Beyersdorff and Ján Pich. Understanding gentzen and frege systems for QBF. In Martin Grohe, Eric Koskinen, and Natarajan Shankar, editors, *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science, LICS '16, New York, NY, USA, July 5-8, 2016*, pages 146–155. ACM, 2016. doi:10.1145/2933575.2933597.

10 Maria Luisa Bonet, Juan Luis Esteban, Nicola Galesi, and Jan Johannsen. On the relative complexity of resolution refinements and cutting planes proof systems. *SIAM J. Comput.*, 30(5):1462–1484, 2000. doi:10.1137/S0097539799352474.

11 Samuel R. Buss. Towards NP-P via proof complexity and search. *Ann. Pure Appl. Logic*, 163(7):906–917, 2012. doi:10.1016/j.apal.2011.09.009.

12 Hubie Chen. Proof complexity modulo the polynomial hierarchy: Understanding alternation as a source of hardness. In Ioannis Chatzigiannakis, Michael Mitzenmacher, Yuval Rabani, and Davide Sangiorgi, editors, *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy*, volume 55 of *LIPIcs*, pages 94:1–94:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016. doi:10.4230/LIPIcs.ICALP.2016.94.

13 Stephen A. Cook and Phuong Nguyen. *Logical Foundations of Proof Complexity.* Cambridge University Press, 2010.

14 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.

15 Uwe Egly, Martin Kronegger, Florian Lonsing, and Andreas Pfandler. Conformant planning as a case study of incremental QBF solving. In Gonzalo A. Aranda-Corral, Jacques Calmet, and Francisco J. Martín-Mateos, editors, *Artificial Intelligence and Symbolic Computation - 12th International Conference, AISC 2014, Seville, Spain, December 11-13, 2014. Proceedings*, volume 8884 of *Lecture Notes in Computer Science*, pages 120–131. Springer, 2014. doi:10.1007/978-3-319-13770-4_11.

16 Merrick L. Furst, James B. Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. *Mathematical Systems Theory*, 17(1):13–27, 1984. doi:10.1007/BF01744431.

17 Allen Van Gelder. Contributions to the theory of practical quantified boolean formula solving. In Michela Milano, editor, *Principles and Practice of Constraint Programming - 18th International Conference, CP 2012, Québec City, QC, Canada, October 8-12, 2012. Proceedings*, volume 7514 of *Lecture Notes in Computer Science*, pages 647–663. Springer, 2012. doi:10.1007/978-3-642-33558-7_47.

18 Enrico Giunchiglia, Paolo Marin, and Massimo Narizzano. Reasoning with 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 761–780. IOS Press, 2009. doi:10.3233/978-1-58603-929-5-761.

19 Armin Haken. The intractability of resolution. *Theor. Comput. Sci.*, 39:297–308, 1985. doi:10.1016/0304-3975(85)90144-6.

20 Johan Håstad. Almost optimal lower bounds for small depth circuits. In S. Micali, editor, *Randomness and Computation, Advances in Computing Reasearch, Vol 5*, pages 143–170. JAI Press, 1989.

21 Mikolás Janota, William Klieber, Joao Marques-Silva, and Edmund M. Clarke. Solving QBF with counterexample guided refinement. *Artif. Intell.*, 234:1–25, 2016. doi:10.1016/j.artint.2016.01.004.

22 Mikolás Janota and Joao Marques-Silva. Expansion-based QBF solving versus q-resolution. *Theor. Comput. Sci.*, 577:25–42, 2015. doi:10.1016/j.tcs.2015.01.048.

23 Emil Jerábek. Dual weak pigeonhole principle, boolean complexity, and derandomization. *Ann. Pure Appl. Logic*, 129(1-3):1–37, 2004. doi:10.1016/j.apal.2003.12.003.

24 Hans Kleine B"uning, Marek Karpinski, and Andreas Flögel. Resolution for quantified boolean formulas. *Inf. Comput.*, 117(1):12–18, 1995. doi:10.1006/inco.1995.1025.

25 Jan Krajícek, Pavel Pudlák, and Alan R. Woods. An exponenetioal lower bound to the size of bounded depth frege proofs of the pigeonhole principle. *Random Struct. Algorithms*, 7(1):15–40, 1995. doi:10.1002/rsa.3240070103.

26 Jan Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, volume 60 of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, Cambridge, 1995.

27 Florian Lonsing and Uwe Egly. Evaluating QBF solvers: Quantifier alternations matter. *CoRR*, abs/1701.06612, 2017.

28 Florian Lonsing, Uwe Egly, and Martina Seidl. Q-resolution with generalized axioms. In Nadia Creignou and Daniel Le Berre, editors, *Theory and Applications of Satisfiability Testing - SAT 2016 - 19th International Conference, Bordeaux, France, July 5-8, 2016, Proceedings*, volume 9710 of *Lecture Notes in Computer Science*, pages 435–452. Springer, 2016. doi:10.1007/978-3-319-40970-2_27.

29 Tomás Peitl, Friedrich Slivovsky, and Stefan Szeider. Long distance q-resolution with dependency schemes. In Nadia Creignou and Daniel Le Berre, editors, *Theory and Applications of Satisfiability Testing - SAT 2016 - 19th International Conference, Bordeaux, France, July 5-8, 2016, Proceedings*, volume 9710 of *Lecture Notes in Computer Science*, pages 500–518. Springer, 2016. doi:10.1007/978-3-319-40970-2_31.

30 Toniann Pitassi, Paul Beame, and Russell Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Computational Complexity*, 3:97–140, 1993. doi:10.1007/BF01200117.

31 Jussi Rintanen. Asymptotically optimal encodings of conformant planning in QBF. In *Proceedings of the Twenty-Second AAAI Conference on Artificial Intelligence*, pages 1045–1050, 2007.

32 John Alan Robinson. A machine-oriented logic based on the resolution principle. *J. ACM*, 12(1):23–41, 1965.

33 Horst Samulowitz and Fahiem Bacchus. Using SAT in QBF. In Peter van Beek, editor, *Principles and Practice of Constraint Programming - CP 2005, 11th International Conference, CP 2005, Sitges, Spain, October 1-5, 2005, Proceedings*, volume 3709 of *Lecture Notes in Computer Science*, pages 578–592. Springer, 2005. doi:10.1007/11564751_43.

34 Nathan Segerlind. The complexity of propositional proofs. *Bulletin of Symbolic Logic*, 13(4):417–481, 2007.

35 Friedrich Slivovsky and Stefan Szeider. Soundness of q-resolution with dependency schemes. *Theor. Comput. Sci.*, 612:83–101, 2016. doi:10.1016/j.tcs.2015.10.020.

36 Lintao Zhang and Sharad Malik. Conflict driven learning in a quantified boolean satisfiability solver. In Lawrence T. Pileggi and Andreas Kuehlmann, editors, *Proceedings of the 2002 IEEE/ACM International Conference on Computer-aided Design, ICCAD 2002, San Jose, California, USA, November 10-14, 2002*, pages 442–449. ACM / IEEE Computer Society, 2002. doi:10.1145/774572.774637.