Electronic Colloquium on Computational Complexity, Report No. 44 (2017)

Reasons for Hardness in QBF Proof Systems*

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

1 **School of Computing, University of Leeds**
`{o.beyersdorff,sclpeh}@leeds.ac.uk`
2 **Kurt Gödel Research Center, University of Vienna**
`jan.pich@univie.ac.at`

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 at the same time exhibits significant shortcomings of that model. Prompted by this we propose an alternative, improved version, allowing fewer but more flexible oracle queries in proofs. We show that lower bounds in our new model correspond to the trichotomy obtained via strategy extraction.

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

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: for a given 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 [10, 13], and to first-order logic (theories of bounded arithmetic [12, 25]). 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 (un)satisfiability of CNFs. Analysis of the corresponding proof system provides the framework for understanding the power and the limitations of the solver [10].

The majority of work in proof complexity has been focussed on *propositional proof complexity*, on proof systems for classical propositional logic. In particular, Resolution [30] 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, 14, 29]. Similarly to the propositional case, several Resolution-based QBF proof systems have been suggested and analysed [1, 5–7, 16, 21, 23, 33] to model the approaches taken by QBF solvers. Of particular importance are Q-Resolution [23] and universal Q-Resolution

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

ISSN 1433-8092

(QU-Res) [16], which as analogues of propositional Resolution form the base systems for conflict-driven clause learning (CDCL) QBF solving [17].

Stronger systems in the form of QBF Frege systems were developed recently [4]. As in the propositional framework, by restricting the lines in Frege to a circuit class $\mathcal{C}$ 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 [4, 6]. 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 (which is in stark contrast to the situation in propositional Frege, where lower bounds for $AC^0[p]$-Frege are wide open).

Recent work has tightened the connection to circuit complexity further. In [8] it has been 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 lower bounds derived from lower bounds 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 at current 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 coincides with its classical core system. This leads to the somewhat disturbing fact that lower bounds for e.g. propositional Resolution trivially lift to any of the studied QBF Resolution systems.

Motivated by this observation, Chen [11] introduced a new notion of *proof system ensemble*, in particular for QU-Res called *relaxing QU-Res*, with the aim to distinguish between lower bounds lifted from propositional Resolution and 'genuine' QBF lower bounds arising from quantifier alternation of the QBFs. Quantifier alternation as also been empirically observed as a source of hardness [26, 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 [8] and the paradigm via quantifier alternation [11]. 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 [8] 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 [11] with the aim of distinguishing propositional bounds from QBF bounds arising from quantifier alternation. In particular, Chen [11] gives an exponential lower bound for relaxing QU-Res that applies to quantified Boolean circuits, however with no small CNF representations (Appendix A). 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 their product formula $\Phi \otimes \Psi$ such that each short QU-Res proof must refute Ψ before it refutes 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' hardness of QBFs due to quantifier alternation.

C. New systems for 'genuine' QBF hardness. Noting this situation, we propose new QBF proof systems, Σ_k^p-QU-Resolution (Def. 14). 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 our algorithm is only permitted a constant number of oracle queries, but these may appear at any point in the proof.

It is interesting to relate lower bounds in Σ_1^p-QU-Resolution to our trichotomy shown in A. In this direction, we prove that Σ_1^p-QU-Resolution admits strategy extraction by depth-3 Boolean circuits (Lemma 16). 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-Resolution. 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-Resolution. We also demonstrate that a variant of the prominent formulas of Kleine Büning et al. [23] 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 20).

Organisation. In Sec. 2 we detail necessary background. Section 3 refines formalised strategy extraction and the characterisation of QBF lower bounds from [8]. In Sec. 4 we show the lower bound for relaxing QU-Res. Section 5 contains the definition of Σ_k^p-QU-Res and the analysis of several QBF families in this proof system. In Sec. 6, we extend Σ_1^p-QU-Res to a stronger system allowing parallel oracle queries.

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 the variable 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 $f : \{0,1\}^* \to \mathcal{L}$ [13]. 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.

Here we consider proof systems for propositional tautologies and fully quantified true QBFs. We also consider proof systems for unsatisfiable formulas and false QBFs and use the words *proof* and *refutation* interchangeably.

Resolution [30] is one of the best studied propositional proof systems [32]. 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 $\perp$ using the resolution rule.

QU-Resolution (QU-Res) [16] is a natural extension of Resolution to QBFs. Given a QBF $\Phi = \mathcal{Q}_1 x_1 \dots \mathcal{Q}_n x_n . \phi$, where ϕ is a CNF, a QU-Res refutation of Φ is a derivation of $\perp$ 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 $x_{i+1}, \dots, x_n$.

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 $\perp$, 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 [9].

Frege Systems. Frege systems are common 'textbook' proof systems comprised of a set of axiom schemes and inference rules [13]. 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 [22], 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 L_j with respect to the quantifier prefix, and the circuit B does not contain any variables to the right of u. Restricting the circuit B in the $\forall$-red rule to the constants $0, 1$ results in a p-equivalent system [8].

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 $\forall x_1 \exists y_1 \dots \forall x_n \exists y_n . \phi(x_1, \dots, x_n, y_1, \dots, y_n)$, where ϕ is a propositional formula, there are $|\pi|^{O(1)}$-size circuits C_i witnessing the existential quantifiers in ψ, i.e.

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

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:

$$\exists C_1, \ldots, C_n \forall x_1, \ldots, x_n, y_1, \ldots, y_n. \bigwedge_{i=1}^{n} (y_i \leftrightarrow C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \rightarrow \phi.$$

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 [8] 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 $\phi \in \Sigma_0^q$, we can construct in time $|\pi|^{O(1)}$ an R^* refutation of*

$$\bigwedge_{i=1}^{n} (y_i \leftrightarrow C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \wedge \phi(x_1, \ldots, x_n, y_1, \ldots, y_n) \tag{2}$$

for some circuits $C_i \in \mathcal{C}$.

Proof. By the formalised strategy extraction theorem for $\mathcal{C}$-Frege systems [8], there is a $\mathcal{C}$-Frege proof of the witnessed formula (2). This means there is an R^* refutation of

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

where Ext is a set of extension axioms defining $\mathcal{C}$ formulas built on 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 the 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 [8] 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 QBFs (given in a prenex form with CNF matrices) which contains a resolution rule that allows resolution on both existential and universal variables. We say that a set of clauses C defines

[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.

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.

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 $\bigwedge_i C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1}) = y_i$ have $|\phi|^{O(1)}$-size P-derivations from $\neg\phi$.
2. ψ is witnessable as in 1. but the witnessed formula $\bigwedge_{i=1}^{n} (y_i \leftrightarrow C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \wedge \neg\phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$ 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 QBFs $\psi_n = \forall x_1 \exists y_1 \ldots \forall x_n \exists y_n . \phi_n(x_1, \ldots, x_n, y_1, \ldots, y_n)$, with propositional ϕ_n, have no 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 $\bigwedge_i C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1}) = y_i$ from $\neg\phi_n$ in P.* ◀

Proof. If the existential variables in ψ_n are not witnessable by $\mathcal{C}$ circuits, we are done. We therefore assume that there are $\mathcal{C}$ circuits witnessing the existential variables.

Suppose that there are some circuits $C_i \in \mathcal{C}$ such that the witnessed formula (2) has a polynomial-size Resolution refutation. If this is not the case, we are done as we are in case 2.

We can construct a refutation of $\neg\psi_n$ in P by first deriving $\bigwedge_i C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1}) = y_i$ from $\neg\phi_n$, and then refuting $\bigwedge_i (C_i \leftrightarrow y_i) \wedge \neg\phi_n$. Since the refutation of $\bigwedge_i (C_i \leftrightarrow y_i) \wedge \neg\phi$ is assumed to have a polynomial-size refutation, but any refutation of $\neg\psi_n$ requires super-polynomial-size, it must be the case that for the circuits $C_i \in \mathcal{C}$, the derivation of $\bigwedge_i (C_i \leftrightarrow y_i)$ from $\neg\phi_n$ requires super-polynomial size (case 3). ◀

This means that any QBF lower bound on P is either a circuit lower bound, a propositional proof complexity lower bound, or it is 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+$\forall$-red. The situation is, however, more delicate with weaker systems, where we can indeed encounter 'genuine' QBF lower bounds. We give an example.

▶ **Definition 3** ([23]). The QBFs KBKF_n have clauses

$$
\begin{array}{rll}
\neg y_0 & y_0 \vee \neg y_1 \vee \neg y'_1 & \\
y_k \vee \neg x_k \vee \neg y_{k+1} \vee \neg y'_{k+1} & y'_k \vee x_k \vee \neg y_{k+1} \vee \neg y'_{k+1} & \text{for } k \in [n-1] \\
y_n \vee \neg x_n \vee \neg y_{n+1} \vee \cdots \vee \neg y_{n+n} & y'_n \vee x_n \vee \neg y_{n+1} \vee \cdots \vee \neg y_{n+n} & \\
x_t \vee y_{n+t} & \neg x_t \vee y_{n+t} & \text{for } t \in [n]
\end{array}
$$

and quantifier prefix $\exists y_0 y_1 y'_1 \forall x_1 \ldots \exists y_k y'_k \forall x_k \ldots \forall x_n \exists y_{n+1} \ldots y_{n+n}$.

This family of QBFs is known to require proofs of size $2^{\Omega(n)}$ in Q-Resolution [6, 23], and this bound can be extended to QU-Resolution 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]. This lower bound is a 'genuine' QBF proof complexity lower bound.

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

Proof. It is clear that playing the variables x_k and z_k identical to y'_k is a winning strategy for the universal player, and so there are circuits C_i as described in Theorem 2 which are of constant size.

Looking now at the witnessed formula $\bigwedge_{i=1}^{n}((x_i \leftrightarrow y'_i) \wedge z_i \leftrightarrow y'_i)) \wedge \phi$, we show this can be refuted by a linear-size proof. By resolving on each x_i and z_i to replace these with the relevant literal on y'_i, we obtain the clauses $y'_i \vee y_{n+i}$ and $\neg y'_i \vee y_{n+i}$. Resolving on each y_{n+i} gives y'_n, $y_n \vee \neg y'_n$ and consequently y_n. For each i, we use y_i and y'_i to deduce y_{i-1} and y'_{i-1} and finally y_0, completing the refutation.

Since KBKF'_n is known to require exponential size proofs in QU-Res [1], by Theorem 2, it must satisfy one of the three conditions given. We have established that there are small witnessing circuits, and that the witnessed formula is easy to refute, and so it must be the case that it is hard to derive the witnessing circuits. ◀

4 Hardness due to quantifier alternation

The characterisation of QBF proof system lower bounds given above is a very natural one. We now show that other suggested reasons for hardness correspond with it.

An alternative characterisation of QBF lower bounds that has previously been suggested is based on the alternation of quantifiers in the quantifier prefix. Most studied QBF proof systems build on a propositional proof system (e.g. Resolution) and on Σ_1^b formulas just coincide with the propositional base system. Therefore we can obtain QBF lower bounds directly from the propositional lower bounds. Characterising lower bounds by quantifier alternation aims to distinguish between such propositional lower bounds and 'genuine' QBF lower bounds arising from the alternation of quantifiers. Relaxing QU-Res has been put forward as a proof system to determine hardness due to quantifier alternation.

▶ **Definition 5** (Relaxing QU-Res [11])**.** Let $\Pi = \mathcal{Q}_1 x_1 \dots \mathcal{Q}_n x_n$ be a quantifier prefix, and let $\Pi' = \mathcal{Q}_{\pi(1)} x_{\pi(1)} \dots \mathcal{Q}_{\pi(n)} x_{\pi(n)}$ be obtained from Π by a permutation $\pi : [n] \to [n]$. If π has the property that $\pi(i) < \pi(j)$ for any $1 \leq i < j \leq n$ with $\mathcal{Q}_i = \forall$ and $\mathcal{Q}_j = \exists$, then we call Π' a *relaxation* of Π. That is, a relaxation is obtained by 'moving $\forall$ quantifiers to the left'. We say that Π' is a Σ_k^b-relaxation if Π' is a Σ_k^b quantifier prefix.

Let $\Phi = \Pi.\phi$ be a QBF. Let A be a clause in the variables x_i, and define α as the unique minimal assignment that falsifies A. We obtain the quantifier prefix $\Pi[\alpha]$ by removing all variables assigned in α, and replacing any universal quantifiers left of a variable in the domain of α with an existential quantifier. If there is some Π_k^b-relaxation $\Pi'[\alpha]$ of $\Pi[\alpha]$ such that $\Pi'[\alpha].\phi[\alpha]$ is false, then $A \in H(\Phi, \Pi_k^b)$.

Relaxing QU-Res contains the same derivation rules as QU-Res. However, for a fixed constant k, relaxing QU-Res can introduce any axiom from $H(\Phi, \Pi_k^b)$.

For some families of QBFs, such as the pigeonhole principle, other propositional formulas or indeed any QBF with a prefix with constant alternation, relaxing QU-Res has polynomial-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 [11]. The lower bound for dag-like relaxing QU-Res in [11] is rather unconventional as the proof system works with clauses, whereas the lower bound applies to circuits without polynomial-size CNF representations (cf. Appendix A). Here 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 lower bounds on Resolution proofs of the pigeonhole principle, rather than alternation of quantifiers, or any other 'genuine' QBF reasons. It follows that this is the case for relaxing QU-Res as well. This demonstrates 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 variables $\vec{x}$ and $\vec{z}$ respectively, and of clauses C_i and D_j over the corresponding variables. Then define

$$\Phi \otimes \Psi := \Lambda(\vec{x})\Pi(\vec{z_1})\dots\Pi(\vec{z_n}) \cdot \bigwedge_{i=1}^{n}\bigwedge_{j=1}^{m}(C_i(\vec{x}) \vee D_j(\vec{z_i}))$$

where each $\vec{z_i}$ is a fresh copy of the variables $\vec{z}$ for each $i = 1, \dots, n$.

The new formula $\Phi \otimes \Psi$ is false if and only if Φ and Ψ are both false. We can combine a winning strategy for the universal variables of Φ with a winning strategy for the universal variables of Ψ to construct a strategy which must falsify some $C_i(\vec{x})$ and, for each i, will falsify some $D_j(\vec{z_i})$. It is therefore the case that the strategy will falsify some $C_i(\vec{x}) \vee D_j(\vec{z_i})$. Similarly, a winning strategy for the existential player for either Φ or Ψ will give a winning strategy for $\Phi \otimes \Psi$.

The proof size for $\Phi \otimes \Psi$ is bounded by the size of proofs required by Φ and Ψ.

▶ **Lemma 7.** *Let $\Phi = \vec{P}.\bigwedge_{i=1}^{n} C_i$ and $\Psi = \vec{S}.\bigwedge_{j=1}^{m} D_j$ be minimally unsatisfiable QBFs. Let $s_P(\Phi)$ be the size of the smallest P-proof for Φ (and similarly for other formulas). 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 $s_P(\Phi) + n \cdot s_P(\Psi)$.

As noted, by restricting the variables we can construct a refutation of $\Phi(\vec{x})$ and each $\Psi(\vec{z_i})$ assigning variables. In QU-Res, each resolution step or $\forall$-reduction step can only be performed on one variable, and so will only remain in one of these proofs, 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 $s_P(\Phi) + n \cdot s_P(\Psi)$. Equality comes from the upper bound above. ◀

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, so the hardness of the product is clearly derived 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. [23] as defined in Definition 3 above.

▶ **Definition 8.** The *pigeonhole principle* for m pigeons and n holes, denoted PHP_n^m, 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 has been shown that $2^{\Omega(n)}$ clauses are required to refute it in Resolution, and indeed in any constant-depth Frege system [18, 24, 28].

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

Since QU-Res when restricted to a propositional formula is equivalent to Resolution, and PHP_n^{n+1} requires proofs of size $2^{\Omega(n)}$ in Resolution [18], we know that PHP_n^{n+1} requires QU-Res proofs of size at least $2^{\Omega(n)}$. In QU-Res, it is known that the formulas KBKF_n have linear-size proofs [16]. Given the proof size bounds on Φ_n given 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 show that any relaxation of the quantifier prefix 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. To produce a Π_t^b-relaxation of the quantifier prefix, for $t < n$, there must be some k such that either x_k is quantified existentially, or x_k is quantified to the left of y_k and y'_k. In either case, we can construct a winning strategy for the existential player.

If some x_k is now quantified existentially, then a winning strategy for the existential player is to play $y_i = 0$, $y'_i = 1$ for each $i \leq k$, and to play $y_j = y'_j = 1$ for each $j > k$. Finally, playing $y_{n+i} = 1$ for each i then satisfies every clause apart from $y_{k-1} \vee \neg x_k \vee \neg y_{k+1} \vee \neg y'_{k+1}$, which can be satisfied by playing $x_k = 0$.

If some x_k is universally quantified to the left of y_k, y'_k, then the strategy for the existential variables is as above, except on the variables y_k and y'_k. When assigning these variables, the existential strategy looks at the value of x_k. If $x_k = 0$, then play $y_k = 0$, $y'_k = 1$. If $x_k = 1$, then play $y_k = 1$, $y'_k = 0$. This strategy will then satisfy all clauses. ◀

Proof of Theorem 9. 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 restrictions by C^X and C^Z.

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^{n+1} to prove, then it must also contain at least c existentially quantified Z-variables.

We then establish an upper bound on the size of a proof of an X-clause derived from c axioms of PHP_n^{n+1} which depends only on c. 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.

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. 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 the clause A^X is a semantic consequence of the pigeonhole principle axioms $C_{i_1}, \dots, C_{i_l}$, i.e. $C_{i_1} \wedge \dots \wedge C_{i_l} \models A^X$.*

Proof. Suppose that $C_{i_1} \wedge \dots \wedge C_{i_l} \not\models A^X$. Let α be an assignment to the X-variables which falsifies A^X but satisfies each C_{i_j}. We can extend α to the minimal assignment α' which falsifies A. We show that for any Π_t^b-relaxation of Φ_n, for $t << n$, we can extend α' to a winning strategy for the existential player.

Given a Π_t^b-relaxation of Φ_n, with quantifier prefix $\vec{P}'$, we show by induction that for each k, we can construct a strategy σ_k on the existential variables of X and $Z_1, \dots, Z_k$ which extends α' and is a winning strategy for

$$\vec{P}' \cdot \bigwedge_{i=1}^{k} \bigwedge_{j=1}^{m} (C_i(\vec{x}) \vee D_j(\vec{z_i}))$$

Let $\sigma_0 := \alpha'$. This clearly satisfies the empty conjunction. For each k, we extend the strategy σ_{k-1} which satisfies $\bigwedge_{i=1}^{k-1} \bigwedge_{j=1}^{m} (C_i(\vec{x}) \vee D_j(\vec{z_i}))$. It therefore suffices to find a strategy for the unassigned Z_k variables which satisfies $\bigwedge_{j=1}^{m} (C_k(\vec{x}) \vee D_j(\vec{z_k}))$. We divide into two possible cases:

- Suppose $k = i_j$ for some $1 \leq j \leq l$. Then α', and hence σ_{k-1}, already satisfies $C_k(\vec{x})$. Therefore σ_{k-1} satisfies each clause $C_k(\vec{x}) \vee D(\vec{z_i})$ for any D, and we can define $\sigma_k = \sigma_{k-1}$ on the variables of X and $Z_1, \dots, Z_{k-1}$, and arbitrarily on Z_k.
- Suppose $k \neq i_j$ for any $1 \leq j \leq l$. Then A^Z does not contain any existential variables in Z_k so α', and hence σ_{k-1}, are not defined on any existential variables in Z_k. Any Π_t^b-relaxation of KBKF_n is true, by Lemma 10. Let τ_k be a strategy for the existential variables of Z_k which is a winning strategy for $\vec{P}' \cdot \bigwedge_{j=1}^{m} D_j(\vec{z_k})$, and so also for $\vec{P}' \cdot \bigwedge_{j=1}^{m} C_k \vee D_j(\vec{z_k})$. As σ_{k-1} is not defined on any existential variables from Z_k, τ_k and σ_{k-1} are strategies for disjoint sets of variables. We extend our strategy σ_{k-1} with τ_k to give σ_k, a winning strategy for $\vec{P}' \cdot \bigwedge_{i=1}^{k} \bigwedge_{j=1}^{m} (C_i(\vec{x}) \vee D_j(\vec{z_i}))$.

The final strategy σ_n is therefore a winning strategy for the existential variables of the Π_t^b-relaxation of Φ_n, and σ_n extends the assignment α'. This suffices to show that the relaxation of $\Phi_n[\alpha']$ is true. Since α' extends β, the minimal assignment falsifying A, with assignments to existential variables only, the strategy detailed here will also be a winning existential strategy for any Π_t^b-relaxation of $\Phi[\beta]$, and so any Π_t^b-relaxation of $\Phi[\beta]$ is true. This does not satisfy the axiom derivation rules of relaxing QU-Res, and so A cannot be derived as an axiom in this system. ◀

This is enough to show that if we use relaxing QU-Res to derive an axiom A, and A^X requires at least l axioms from PHP_n^{n+1} in any proof, then A must contain existential variables from at least l different Z_i. In particular, A contains at least l distinct Z-variables.

The following lemma gives an upper bound for the size of Resolution proofs from a fixed number of axioms from PHP_n^{n+1}. This upper bound also applies to the length of a Resolution proof of the X-clause of an axiom containing a small number of Z-variables.

▶ **Lemma 12.** *Suppose C is a clause derived by Resolution from PHP_n^{n+1}, and there exist axioms $C_1, \dots, C_t$ from PHP_n^{n+1} such that $C_1 \wedge \dots \wedge C_t \models C$. Then there is a Resolution proof of C of size at most 18^t.*

Combining this with Lemma 11 shows that any relaxing QU-Res axiom A for which A^X requires a large QU-Res derivation from the axioms of the pigeonhole principle must also contain a large number of Z-variables.

▶ **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^{n+1}. Then A must contain at least $\frac{1}{\log 18} \log S(A^X)$ existential Z-variables.*

Proof of Lemma 12. We show that without weakening, which can be done in one step at the end if needed, there are at most 18^t clauses that can be derived by Resolution from t axioms of PHP_n^{n+1}. This upper bound is far from tight, but is sufficient for the proof of Theorem 9.

Given t clauses from PHP_n^{n+1}, all negative literals are in clauses of size 2. Thus there are at most $2t$ variables x_i which appear in both positive and negative literals in the clauses $C_1, \dots, C_t$. There are then at most t blocks Y_j of pure positive or pure negative literals, at most one corresponding to each C_i. Any clause derived by Resolution from $C_1, \dots, C_t$ must contain each variable x_i as a positive literal, a negative literal or not at all, and must contain some subset of the blocks of pure literals. Thus the total number of clauses derivable in Resolution from $C_1, \dots, C_t$ is at most $3^{2t} \cdot 2^t = 18^t$. Any Resolution derivation of C from $C_1, \dots, C_t$ therefore has size at most 18^t. ◀

To conclude the proof of Theorem 9 we show that for any relaxing QU-Res proof π of Φ_n and for any assignment to the existential Z-variables, we can find an axiom in π which agrees with the Z-assignment and contains linear number of Z-variables.

Suppose that Φ_n has relaxing QU-Res proofs of size $f(n)$. Given a proof π with $|\pi| \leq f(n)$, and an assignment α to the existentially quantified Z-variables, we will show that by restricting π to the clauses which agree with α, and restricting these clauses to their respective X-clauses, we can construct a sound Resolution refutation of PHP_n^{n+1} from the X-axioms.

Consider $\pi|_\alpha$, the result of restricting π to those clauses which agree with α. We show by induction that ${\pi|_\alpha}^X$ is a Resolution refutation from the X-axioms, of size at most $f(n)$.

- The empty clause is the root of the Resolution proof on the X-variables, and clearly agrees with α.
- Suppose a clause C is derived by a $\forall$-red step on a Z-variable u. Then clearly $C \vee u$ agrees with α if C agrees with α, since α does not assign u. Also $C^X = (C \vee u)^X$, so this is a valid step in a Resolution proof on the X-clauses.
- Suppose C agrees with α and C is derived from C_1 and C_2 by resolving on an X-variable x. Then $C_1^Z, C_2^Z \subseteq C^Z$, and so both C_1 and C_2 agree with α since C does so. Observe also that C^X is derived from C_1^X and C_2^X by a single Resolution step on x.
- Suppose C agrees with α and C is derived from C_1 and C_2 by resolving on a Z-variable z. Then at least one of C_1 and C_2 must agree with α, depending on the value of $\alpha(z)$. As $C_1^X, C_2^X \subseteq C^X$, we can derive C^X by a weakening step from whichever agrees with the Z-assignment, or both if z is universally quantified.

This completes our induction, and proves that the X-clauses of the clauses in π which agree with α are a valid Resolution proof. As we know that any Resolution refutation of PHP_n^{n+1} requires proofs of size at least 2^{kn}, for some constant k, we know that there is some X-axiom B in this proof which requires Resolution derivation of size at least $\frac{2^{kn}-f(n)}{f(n)} = \frac{1}{f(n)} 2^{kn} - 1$.

From the construction above, there is some axiom A in π such that $A^X = B$, and by Corollary 13, A must contain at least $c(kn - \log f(n)) =: g(n)$ existentially quantified Z-variables, which agree with α, for some constant c.

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 a. 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 $f(n) = 2^{\Omega(n)}$. ◀

We have shown that $\mathrm{PHP}_n^{n+1} \otimes \mathrm{KBKF}_n$ requires proofs of size $2^{\Omega(n)}$ in relaxing QU-Res, despite consisting of a propositional formula which is hard for Resolution combined with a QBF which is easy for QU-Res.

5 An alternative definition of hardness from alternation

In this section, we propose a new set of proof systems which better characterise whether a QBF lower bound is due to alternating quantifiers or due to a propositional lower bound. In this proof system, $\mathrm{PHP}_n^{n+1} \otimes \mathrm{KBKF}_n$ has linear-size proofs.

▶ **Definition 14.** A Σ_k^p-QU-Resolution proof is a derivation of the empty clause by the rules of QU-Resolution, and a constant number of instances of the following rule:

$$(\Sigma_k^p\text{-derivation}) \quad \frac{C_1 \quad \dots \quad C_l}{D_1 \quad \dots \quad D_m}$$

where there is some Σ_k^b-relaxation Π' of the quantifier prefix Π such that $\Pi' \cdot \bigwedge_{i=1}^{l} C_i \models \Pi' \cdot \bigwedge_{j=1}^{m} D_j$. In the context of this proof system, we define a Σ_k^b-relaxation of a quantifier prefix as in Definition 5, but we also allow the replacing of any $\forall$ quantifier by $\exists$.

This proof system is clearly complete as QU-Res is complete. The soundness of this system can be seen by noting that QU-Res (with weakening) is sound and implicationally complete. Furthermore, any QU-Res step consistent with the relaxed prefix is also consistent with the original prefix, and so if a Σ_k^p-QU-Resolution refutation exists, then we can construct a QU-Res refutation. Allowing a relaxation to replace universal quantifiers with existential quantifiers is not necessary, but as we shall see later, it reduces the number of levels of the polynomial hierarchy we need to consider.

This definition differs from the definition of relaxing QU-Res as it allows the proof checker to make queries to a Σ_k^p-oracle at any point in the proof. However, the number of queries it can make is bounded by a constant, rather than the unbounded number permitted in relaxing QU-Res. Note that Σ_k^p-QU-Resolution, parameterised by the number of queries to the Σ_k^p oracle, forms a proof system ensemble as defined in [11].

We can now define a QBF to be *hard due to (quantifier) alternation* if it is hard for Σ_1^p-QU-Resolution, i.e. if efficiently solving a SAT problem does not significantly shorten the proof. We can extend this to a hierarchy of QBFs, saying a QBF is *hard due to Σ_k^b-alternation* if it has short proofs in Σ_k^p-QU-Resolution, but requires long proofs in any lower class. The proof complexity of formulas in Σ_1^p-QU-Resolution is of particular interest, as recent success in SAT solving has resulted in some QBF solvers embedding a SAT solver as a black box [20,31]. The oracle access to Σ_1^p models this technique, and may provide some insight as to the power and limitations of such QBF solvers.

It is straightforward to extend this definition to construct Σ_k^p-P for most QBF proof systems which work with proof lines, such as $\mathcal{C}$-Frege+$\forall$-red systems. Clearly, using a different proof system may change proof sizes, and so the definition of hardness due to alternation is dependent upon the proof system used.

As noted in Section 4, the formulas $\mathrm{PHP}_n^{n+1} \otimes \mathrm{KBKF}_n$ require QU-Res proofs of size $2^{\Omega(n)}$ due to the lower bound on Resolution. Here we show that these formulas have polynomial-size proofs in Σ_1^p-QU-Resolution, and so are not hard for QU-Res due to quantifier alternation. This is in sharp contrast with the lower bound shown in Theorem 9 for relaxing QU-Res, despite this proof system also making use of oracles for Σ_k^p.

▶ **Theorem 15.** $\mathrm{PHP}_n^{n+1} \otimes \mathrm{KBKF}_n$ *have* Σ_1^p*-QU-Resolution proofs of length* $O(n^3)$*.*

Proof. Define the clauses C_i and D_j such that $\mathrm{PHP}_n^{n+1} = \bigwedge_i C_i$ and $\mathrm{KBKF}_n = \Pi \cdot \bigwedge_j D_j$, and so the clauses of $\mathrm{PHP}_n^{n+1} \otimes \mathrm{KBKF}_n$ are $C_i(\bar{x}) \vee D_j(\bar{z}_i)$ for all i, j.

Since there is an $O(n)$-length refutation of KBKF_n in QU-Res, we know that QU-Res can derive $C_i(\bar{x})$ from $\bigwedge_j C_i(\bar{x}) \vee D_j(\bar{z}_i)$ in $O(n)$ lines. There are $O(n^2)$ clauses C_i in PHP_n^{n+1}, so there is a QU-Res derivation of $\bigwedge_i C_i(\bar{x})$ in $O(n^3)$ lines. All the variables in $\bar{x}$ are existentially quantified, and PHP_n^{n+1} is false, thus from $\bigwedge_i C_i(\bar{x})$, Σ_1^p-QU-Res derives the empty clause in a single Σ_1^p-derivation step. ◀

In order to compare this characterisation of QBF proof lower bounds with that in Section 3, we first show that Σ_1^p-QU-Resolution has strategy extraction. While we only show strategy extraction for Σ_1^p-QU-Resolution, the result generalises easily to other Σ_1^p-$\mathcal{C}$-Frege systems.

▶ **Lemma 16.** Σ_1^p*-QU-Resolution has strategy extraction by depth-3 Boolean circuits.*

Proof. QU-Resolution is known to have strategy extraction by depth-3 Boolean circuits [4]. We extend this result to Σ_1^p-QU-Resolution by showing that Σ_1^p-derivations do not contain any information on the strategy for the universal player.

From any Σ_k^p-QU-Resolution proof we can construct a QU-Resolution proof by replacing the Σ_k^p-derivation steps with a QU-Resolution derivation of the clauses. By the implicational completeness of QU-Resolution, this is possible, and each Σ_k^p-derivation can be replaced by a QU-Resolution derivation consistent with the Σ_k^b-relaxation.

In the case of Σ_1^b, the relaxation of the prefix treats all variables as existential. A QU-Resolution proof constructed in this way, while potentially much larger than the Σ_1^p-QU-Resolution proof, does not contain any additional ∀-reduction steps that were not in the Σ_1^p-QU-Resolution proof. Strategy extraction for QU-Resolution constructs a strategy which is polynomial in the number of ∀-reduction steps of the proof, as noted in [4]. Given any Σ_1^p-QU-Resolution proof, it is therefore possible to extract a strategy for the universal variables as a depth-3 Boolean circuit with size polynomial in the length of the proof. ◀

QBFs hard for QU-Res by item 1 of Theorem 2 (hardness due to strategy extraction) are therefore still hard for Σ_1^p-QU-Res. Intuitively, lower bounds due to strategy extraction can also be considered lower bounds due to quantifier alternation, as strategy extraction is a technique that inherently relies on universally quantified variables.

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 super-polynomial size proofs in Resolution. Using the normal form for proofs described in [8], we can construct short proofs of these QBFs in Σ_1^p-QU-Res, deriving the witnessed formula, and then using a Σ_1^p-derivation to derive $\perp$. This demonstrates that QBFs in the second category are not hard due to alternation of quantifiers.

For sufficiently strong proof systems, such as Frege+∀-red, these are the only two possible reasons for hardness [8]. As Lemma 16 extends naturally to Σ_1^p-Frege+∀-red, the characterisation of hardness for QBF Frege systems in [8] (circuit lower bounds vs propositional Frege lower bounds) therefore coincides with our characterisation via quantifier alternation.

In the following, we determine the *precise alternation hardness* for two formulas known to be hard for QU-Resolution, one from each of the two interesting categories 1 and 3 from Theorem 2. Formulas in category 2 such as the existentially quantified PHP_n^{n+1} formulas (or, less trivially, the formulas from Theorem 15) are all easy for Σ_1^p-QU-Res.

We first show a simulation result for certain levels of the polynomial hierarchy, which has the effect of restricting the interesting quantifier relaxations to the classes Σ_{2k-1}^b.

▶ **Lemma 17.** *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.*

In particular, given a family of QBFs Φ_n, if the alternation hardness of Φ_n is precisely $\mathcal{C}$, then $\mathcal{C} = \Sigma_{2k+1}^b$ for some integer k.

Proof. We begin by demonstrating that from a Π_m^p-QU-Resolution refutation of Φ_n of size $s(n)$, we can construct a Σ_{m-1}^p-QU-Resolution refutation of size $O(s(n))$.

Consider the outermost block of universal variables in a Π_m^b-relaxation. A Σ_{m-1}^b-relaxation can be obtained by quantifying the variables in this block existentially. If a Π_m^p-derivation does not derive the empty clause, then all possible clauses derived by the Π_m^p-derivation contain at least one variable quantified existentially in the Π_m^b-relaxation. Thus we can still derive the same clauses using the Σ_{m-1}^b relaxation, as at no point would any QU-Resolution proof consistent with the Π_m^b-relaxation contain a $\forall$-reduction step on these universal variables. If the Π_m^p-derivation does derive the empty clause, then it is possible in the Σ_{m-1}^b-relaxation to derive a clause containing only variables which were universally quantified in the first block in the Π_m^b-relaxation. As these variables must be universally quantified in the original QBF, there is a proof using a Σ_{m-1}^b-relaxation of size $\leq p(n) + n$, which replaces the Π_m^p-deduction with a Σ_{m-1}^p-deduction and at most n $\forall$-reduction steps.

Given a Σ_{2k}^b-relaxation of the quantifier prefix, the innermost block of variable is universally quantified. By the definition of relaxation, these variables must also have been innermost in the original quantifier prefix. The first step in a Σ_{2k-1}^p-QU-Resolution proof is to $\forall$-reduce these variables in each axiom. The Σ_{2k}^p-QU-Res proof is then followed, with the innermost variables removed from the clauses. At each Σ_{2k}^p-derivation, the innermost variables are not present in any of the clauses, and so the Σ_{2k}^b-relaxation can be replaced by a Σ_{2k-1}^b-relaxation with these variables also existentially quantified. ◀

The proof of Lemma 17 relies on the fact that we allow relaxations to replace universal quantifiers with existential quantifiers. If the definition of relaxation were restricted to that of relaxing QU-Res, then the simulation of Π_m^p-QU-Resolution by Σ_{m-1}^p-QU-Resolution would not hold. With the exception of Σ_2^p-QU-Resolution, it would still be possible to reduce a Σ_{2k}^p-QU-Resolution proof to a Σ_{2k-1}^p-QU-Resolution proof by moving the innermost universal variables outwards to another block of universal quantifiers.

Lemmas 16 and 17 immediately allow us to extend a strategy extraction lower bound to obtain a lower bound on Σ_1^p-QU-Resolution. We illustrate this on the QParity formulas from [4, 6], for which we establish the precise alternation hardness.

▶ **Definition 18** ([6]). The formulas $\mathrm{QParity}_n$ have 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 are false, and the only winning strategy for the $\forall$ player is to play $z \equiv \bigoplus_{i=1}^n x_i$. However, the parity function is hard to compute for depth-3 circuits [15, 19], and so any QU-Resolution proof requires length $\Omega(2^n)$.

▶ **Corollary 19.** *The formulas* $\mathrm{QParity}_n$ *have* Σ_3^b*-alternation hardness. In particular, they are hard for QU-Resolution due to the alternation of quantifiers.*

Proof. It is clear that $\mathrm{QParity}_n$ has short proofs in Σ_3^p-QU-Resolution, as their quantifier prefix is Σ_3^b. By Lemma 17, we need only show that $\mathrm{QParity}_n$ does not have polynomial size proofs in Σ_1^p-QU-Resolution. By Lemma 16, Σ_1^p-QU-Resolution has strategy extraction by depth-3 circuits. Since any depth-3 circuit for the parity function requires exponential size [15, 19], any Σ_1^p-QU-Resolution refutation of $\mathrm{QParity}_n$ requires exponential size. ◀

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

▶ **Theorem 20.** *For any constant k, the formulas* KBKF'_n *require proofs of length* $2^{\Omega(n)}$ *in* Σ_k^p*-QU-Resolution.*

Proof. Throughout this proof, we will refer only to universal variables x_i. Since the variables x_i and z_i appear with the same polarity in all clauses, we only need to consider whichever is quantified first in any relaxation, which w.l.o.g. we assume is x_i.

The first step in our proof is to observe that the winning strategy for the universal player in KBKF'_n is to play the variable x_i according only to the values of the variables y_i and y'_i. Thus any Σ_k^b relaxation in which x_i is quantified existentially, or is quantified before y_i and y'_i cannot contribute to the strategy derived for x_i.

Moreover, as noted in [23], whenever a variable x_i is reduced, the clause must contain literals on each x_j variable for $1 \leq j < i$. Since the strategy for x_i depends only on y_i, y'_i and not on the x_j, define a $\forall$-reduction on x_i to be 'useful' if there is a literal on y_i or y'_i in the clause. In QU-Res, there must be a useful $\forall$-reduction on x_i for each of the 2^{i-1} different combinations of literals on $x_1, \ldots, x_{i-1}$.

Given a Σ_k^b-relaxation of the quantifier prefix of KBKF'_n, there are at most $\frac{k}{2}$ blocks of universal variables. If such a block contains x_i, then for each $j > i$, the variables y_j, y'_j must be quantified to the right of the block. Hence each block contains at most one universal variable x_i, namely the x_j in the block with the smallest index j, which is right of the corresponding variables y_i, y'_i.

As in the proof of Lemma 16, we see that for a Σ_k^p-QU-Resolution proof, we can construct a QU-Resolution proof by replacing the Σ_k^p-derivations with QU-Resolution derivations consistent with a Σ_k^b-relaxation. By the above, the QU-Resolution derivations that replace the Σ_k^p-derivations can only contain useful $\forall$-reduction steps on k universal variables.

Given a Σ_k^p-QU-Resolution proof which contains at most m Σ_k^p-derivations, we can conclude that there are at most mk universal variables which appear to the right of their corresponding y_i, y'_i variables in at least one Σ_k^b-relaxation. Since at least one of $x_{n-mk}, \ldots, x_n$ does not have this property, the Σ_k^p-QU-Resolution proof must contain all useful $\forall$-reduction steps on one of these variables, and so must contain at least 2^{n-mk} clauses in total. ◀

6 Allowing parallel queries: stronger QBF proof systems

In Σ_k^p-QU-Resolution, the algorithm for verifying the proof is allowed to make a constant number of queries to a Σ_k^p-oracle. Here we will propose a stronger system, motivated by the observation that a Σ_k^p-oracle query can be used to check multiple parallel Σ_k^p-derivations at once. Thus as long as no path in the proof dag contains more than m Σ_k^p-derivation steps, there is a polynomial-time proof checking algorithm which requires at most m Σ_k^p-oracle queries.

▶ **Definition 21.** A *parallel Σ_k^p-QU-Resolution* proof of a QBF ϕ is a derivation of the empty clause by the same rules as Σ_k^p-QU-Resolution. The proof may contain an arbitrary number of Σ_k^p-derivation steps, but there is a constant m such that any path through the proof dag contains no more than m such steps.

It is clear that parallel Σ_k^p-QU-Resolution p-simulates Σ_k^p-QU-Resolution. However the converse does not hold: there is an exponential separation between the two systems for $k \geq 3$.

▶ **Theorem 22.** *For $k \geq 3$, there is a family of QBFs Φ_n such that Φ_n has polynomial size proofs in parallel Σ_k^p-QU-Resolution, but requires proofs of size $2^{\Omega(n)}$ in Σ_k^p-QU-Resolution.*

Proof. Let Φ_n be the QBF $\mathrm{PHP}_n^{n+1} \otimes \mathrm{QParity}_n$. Note in particular that the definition of $\otimes$ quantifies the variables from each copy of $\mathrm{QParity}_n$ sequentially, and so Φ_n has a Σ_{2N+1}^b quantifier prefix, where N is the number of clauses in PHP_n^{n+1}.

It is easy to see that Φ_n has short proofs in parallel Σ_k^p-QU-Resolution. Each clause of PHP_n^{n+1} can be derived by a Σ_k^p-derivation, each of which is independent of the others. We then require a single Σ_k^p-derivation to derive $\perp$ from the clauses of PHP_n^{n+1}. Each path through this proof contains at most two Σ_k^p-derivations.

Since the strategy for each universal variable in Φ_n requires size $2^{\Omega(n)}$ as a depth-3 Boolean circuit, we see that any polynomial size Σ_k^p-QU-Resolution proof of Φ_n must contain for each universal variable, at least one Σ_k^p-derivation in which the relaxation quantifies the universal variable to the right of the corresponding existential variables from that copy of $\mathrm{QParity}_n$. If this were not the case, it would be possible to extract a strategy for this variable from the proof, which cannot be done in polynomial size.

As a Σ_k^b-relaxation can only contain $\frac{k}{2}$ blocks of universal variables, a Σ_k^p-QU-Resolution proof containing m Σ_k^p-derivations can only contain suitable relaxations for $\frac{1}{2}mk$ universal variables. Thus for any Σ_k^p-QU-Resolution proof, there is some universal variable for which we can extract a strategy from the $\forall$-reduction steps of the proof. The proof must therefore have size $2^{\Omega(n)}$. ◀

Note that this separation only holds for $k > 1$. When $k = 1$, the two systems are in fact p-equivalent, since there is only one possible Σ_1^b-relaxation. Parallel Σ_1^p-derivations can therefore be combined into a single such step. The two proof systems therefore give equivalent definitions for hardness due to (Σ_1^b-)alternation.

It is relatively straightforward to see that the strategy extraction from Lemma 17 can be extended to parallel Σ_k^p-QU-Resolution. Defining a hierarchy of alternation hardness as before, we conclude that $\mathrm{QParity}_n$ still has Σ_3^b-alternation hardness for parallel Σ_k^p-QU-Resolution.

The example in Theorem 22 demonstrates that the alternation hardness of a family of QBFs need not be the same in parallel Σ_k^p-QU-Resolution as it is in Σ_k^p-QU-Resolution. We conclude by showing that there exist QBFs which do not have short proofs in any parallel Σ_k^p-QU-Resolution. The formulas we use for this are the same KBKF'_n formulas for which the analogous result for Σ_k^p-QU-Resolution was shown above.

▶ **Theorem 23.** *The formulas KBKF'_n require super-polynomial size proofs in parallel Σ_k^p-QU-Resolution for any constant k.*

Proof. The proof uses much the same technique as the proof of Theorem 20. As in that proof, we refer only to universal variables x_i. We first observe that in a QU-Res proof, any

$\forall$-reduction on a universal variable x_i must be in a clause containing a literal on each x_j for $j < i$. Furthermore, each $\forall$-reduction on x_i must be preceded by a $\forall$-reduction on x_l for each $i < l \leq n$. Clearly, these $\forall$-reductions must also contain the same literals on $x_1, \ldots, x_i$ as in the $\forall$-reduction on x_i.

We now fix constant k and m. Assume that KBKF'_n has a polynomial size proof in parallel Σ^p_k-QU-Resolution with at most m Σ^p_k-derivations on any path. This proof can be expanded to a QU-Res proof by replacing the Σ^p_k-derivations with QU-Res derivations. This QU-Res proof requires 2^i $\forall$-reductions on x_i, but there is some polynomial $p(n)$ such that for each i, at most $p(n)$ $\forall$-reductions on x_i are not contained in the expansion of a Σ^p_k-derivation, as the parallel Σ^p_k-QU-Resolution proof has polynomial size.

The number of $\forall$-reductions on variables $x_{n-mk}, \ldots, x_n$ that are not in the expansion of some Σ^p_k-derivation is at most $(mk+1)p(n) < 2^{n-mk-1}$ for large enough n. We can therefore find an assignment to the variables $x_1, \ldots, x_{n-mk-1}$ for which all $\forall$-reductions on $x_{n-mk}, \ldots, x_n$ agreeing with this assignment are in an expansion of a Σ^p_k-derivation.

As mentioned previously, the x_i variables depend only on the y_i, y'_i variables and an expansion of a Σ^p_k-derivation can only contain a $\forall$-reduction on k variables x_i with a corresponding y_i or y'_i variable in the same clause. The clause corresponding to the assignment to $x_1, \ldots, x_{n-mk-1}$ is preceded by $mk+1$ successive $\forall$-reductions, all of which are obtained by expanding a Σ^p_k-derivation. Consequently, the path through these $\forall$-reductions must contain at least $m+1$ Σ^p_k-derivations, contradicting our assumption that the proof contained at most m on any path. ◀

7 Conclusion

We have undertaken an analysis of 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), these two criteria are equivalent, and proposed a system for which all lower bounds are such proper QBF lower bounds.

A natural question is whether for weaker Resolution-based systems, QBFs from the third category of Theorem 2 are always hard due to alternation. Here we have only shown this for the special case of KBKF'_n. 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 *Theory and Applications of Satisfiability Testing - SAT 2014*, pages 154–169, 2014.

2 Paul Beame and Toniann Pitassi. Simplified and improved resolution lower bounds. In *Symposium on Foundations of Computer Science (FOCS)*, pages 274–282, 1996.

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 *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science*, pages 249–260, 2016.

5 Olaf Beyersdorff, Leroy Chew, and Mikoláš Janota. On unification of QBF resolution-based calculi. In *MFCS, II*, pages 81–93, 2014.

6 Olaf Beyersdorff, Leroy Chew, and Mikoláš Janota. Proof complexity of resolution-based QBF calculi. In *Proc. Symposium on Theoretical Aspects of Computer Science (STACS'15)*, pages 76–89. LIPIcs, 2015.

7 Olaf Beyersdorff, Leroy Chew, Meena Mahajan, and Anil Shukla. Feasible interpolation for QBF resolution calculi. In *Proc. International Colloquium on Automata, Languages, and Programming (ICALP'15)*, pages 180–192. Springer, 2015.

8 Olaf Beyersdorff and Ján Pich. Understanding Gentzen and Frege systems for QBF. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science, LICS*, pages 146–155, 2016.

9 Maria Luisa Bonet, Juan Luis Esteban, Nicola Galesi, and Jan Johannsen. On the relative complexity of resolution refinements and cutting planes proof systems. *SIAM Journal on Computing*, 30(5):1462–1484, 2000.

10 Samuel R. Buss. Towards NP-P via proof complexity and search. *Ann. Pure Appl. Logic*, 163(7):906–917, 2012.

11 Hubie Chen. Proof complexity modulo the polynomial hierarchy: Understanding alternation as a source of hardness. In *43rd International Colloquium on Automata, Languages, and Programming, ICALP*, pages 94:1–94:14, 2016.

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

13 Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *J. Symb. Log.*, 44(1):36–50, 1979.

14 Uwe Egly, Martin Kronegger, Florian Lonsing, and Andreas Pfandler. Conformant planning as a case study of incremental QBF solving. In *Artificial Intelligence and Symbolic Computation (AISC'14)*, pages 120–131, 2014.

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

16 Allen Van Gelder. Contributions to the theory of practical quantified Boolean formula solving. In *Principles and Practice of Constraint Programming - 18th International Conference, CP*, pages 647–663, 2012.

17 Enrico Giunchiglia, Paolo Marin, and Massimo Narizzano. Reasoning with quantified boolean formulas. In *Handbook of Satisfiability*, pages 761–780. IOS Press, 2009.

18 Armin Haken. The intractability of resolution. *Theor. Comput. Sci.*, 39:297–308, 1985.

19 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.

20 Mikolás Janota, William Klieber, Joao Marques-Silva, and Edmund M. Clarke. Solving QBF with counterexample guided refinement. *Journal of Artificial Intelligence*, 234:1–25, 2016.

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

22 Emil Jerábek. Dual weak pigeonhole principle, Boolean complexity, and derandomization. *Ann. Pure Appl. Logic*, 129(1-3):1–37, 2004.

23 Hans Kleine Büning, Marek Karpinski, and Andreas Flögel. Resolution for quantified Boolean formulas. *Inf. Comput.*, 117(1):12–18, 1995.

24 Jan Krajícek, Pavel Pudlák, and Alan R. Woods. An exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle. *Random Struct. Algorithms*, 7(1):15–40, 1995.

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

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

27 Florian Lonsing, Uwe Egly, and Martina Seidl. Q-resolution with generalized axioms. In *Theory and Applications of Satisfiability Testing (SAT'16)*, pages 435–452, 2016.

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

29 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.

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

31 Horst Samulowitz and Fahiem Bacchus. Using SAT in QBF. In *Principles and Practice of Constraint Programming, CP*, pages 578–592, 2005.

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

33 Lintao Zhang and Sharad Malik. Conflict driven learning in a quantified Boolean satisfiability solver. In *Proceedings of the 2002 IEEE/ACM International Conference on Computer-aided Design, ICCAD*, pages 442–449, 2002.

A Chen's lower bound for relaxing QU-Res

Define $\Psi_n = \vec{P}_n \cdot \psi_n$ to be the quantified Boolean circuit consisting of the quantifier prefix $\vec{P}_n := \exists x_1 \forall y_1 \ldots \exists x_i \forall y_i \ldots \exists x_n \forall y_n$ and a (polynomial-sized) Boolean circuit ψ_n defined such that

$$\psi_n \leftrightarrow \sum_{i=1}^{n} (x_i + y_i) \not\equiv 0 \mod 3.$$

The quantified Boolean circuits Ψ_n then provide a lower bound for relaxing QU-Res.

▶ **Theorem 24** (Chen [11]). *Relaxing QU-Res requires proofs of size $\Omega(2^n)$ on Ψ_n.*

Lines in the relaxing QU-Res proof system are clauses, however there is no polynomial-size CNF equivalent to ψ_n.

▶ **Lemma 25.** *Any CNF $\phi_n(\vec{x}, \vec{y})$ equivalent to $\psi_n(\vec{x}, \vec{y})$ must contain $\Omega(2^n)$ clauses.*

Proof. The circuit ψ_n has $2n$ input variables. For any assignment to $2n - 1$ of these, the corresponding restriction of the circuit is not equivalent to 0. Any clause in an equivalent CNF must therefore contain literals on all $2n$ variables.

For each clause C in ϕ_n, there is therefore a unique assignment to $\vec{x}, \vec{y}$ which falsifies C. As each of the $\Omega(2^n)$ assignments on which ψ_n evaluates to 0 must falsify a clause, ϕ_n must contain $\Omega(2^n)$ clauses. ◀

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il