Reasons for Hardness in QBF Proof Systems

Olaf Beyersdorff¹, Luke Hinde¹, and Ján Pich²

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 \( \phi \) and proof system \( P \), what is the size of the shortest proof of \( \phi \) 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.
2 Reasons for Hardness in QBF Proof Systems

(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 $C$ we obtain a hierarchy of (QBF) $C$-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 $C$, a lower bound for proof size in QBF $C$-Frege corresponds to either a lower bound for propositional $C$-Frege, or a lower bound for the circuit class $C$. 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 $C$-Frege proofs of QBFs $\psi_n$, one can construct small $C$ circuits witnessing the existential quantifiers in $\psi_n$ in such a way that the resulting ‘witnessed’ propositional formulas have polynomial-size proofs in $C$-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 $\Phi$ and $\Psi$ into their product formula $\Phi \otimes \Psi$ such that each short QU-Res proof must refute $\Psi$ before it refutes $\Phi$. 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, $\Sigma^p_k$-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 $\Sigma^p_k$-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 $\Sigma^p_k$-QU-Resolution to our trichotomy shown in A. In this direction, we prove that $\Sigma^p_k$-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 $\Sigma^p_k$-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 $\Sigma^p_k$-QU-Resolution. We also demonstrate that a variant of the prominent proof systems of Kleine Büning et al. [23] simultaneously has genuine QBF lower bounds as per case (3) in A (Theorem 4) and is hard for $\Sigma^p_k$-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 $\Sigma^p_k$-QU-Res and the analysis of several QBF families in this proof system. In Sec. 6, we extend $\Sigma^p_k$-QU-Res to a stronger system allowing parallel oracle queries.

2 Preliminaries

Quantified Boolean Formulas. A (prenex normal form) quantified Boolean formula (QBF) $\Phi = Q_1x_1 \ldots Q_nx_n.\phi(x_1,\ldots,x_n)$ consists of a propositional formula $\phi$, usually expressed as a CNF, and a quantifier prefix $Q_1x_1 \ldots Q_nx_n$, where each $Q_i \in \{\exists, \forall\}$ 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 $Q_i$ 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 $\phi$ evaluates to 1 (resp. 0).

Given a variable $x_i$, a strategy for the variable $i$ is a function $s_i : \{x_1,\ldots,x_{i-1}\} \to \{0,1\}$. 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 $\Phi$. 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 $\Sigma^p_i$ and $\Pi^p_i$, counting the number of quantifier alternations. By $\Sigma^p_k$ (resp. $\Pi^p_k$) we denote the $i$th level of the polynomial hierarchy, for which deciding truth of $\Sigma^p_k$ (resp. $\Pi^p_k$) 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 $\pi$ is an $f$-proof of $\phi$. 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 $\pi$. 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 $C \lor x$ and $D \lor \neg x$, Resolution can derive the clause $C \lor D$. A Resolution proof that a CNF $\phi$ is unsatisfiable is a derivation of the empty clause $\bot$ using the resolution rule.

$QU$-Resolution (QU-Res) [16] is a natural extension of Resolution to QBFs. Given a QBF $\Phi = Q_1 x_1 \ldots Q_n x_n . \phi$, where $\phi$ is a CNF, a QU-Res refutation of $\Phi$ is a derivation of $\bot$ from the clauses of $\phi$. 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 $C \lor l$ 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 [9].

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 $\land, \lor, \neg$. A Frege proof of $\phi$ is a sequence of formulas, ending with $\phi$, 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 $C$, we define $C$-Frege, as in [22], to be a Frege system which works with lines consisting of circuits in $C$ and a finite set of derivation rules. If $C$ consists of all Boolean circuits, then $C$-Frege is $p$-equivalent to extended Frege (EF). If $C$ is restricted to Boolean formulas, i.e. $C = NC^1$, then $NC^1$-Frege is Frege as defined above.

An elegant method for extending $C$-Frege systems to QBF was shown in [4]. The QBF proof system $C$-Frege+$\forall$-red is a refutational proof system working with circuits from $C$. The inference rules of $C$-Frege+$\forall$-red are those of $C$-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 $\pi$ of a QBF $\psi$ 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 $\phi$ is a propositional formula, there are $|\pi|^{O(1)}$-size circuits $C_i$ witnessing the existential quantifiers in $\psi$, i.e.

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

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 $\psi$, either there is a propositional formula as in (1) equivalent to $\psi$, 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 $\psi$ 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 $\Sigma^2_p$-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 \( EF + \forall \text{-red} \)\(^1\) have \( R^* \)-formalized strategy extraction. More precisely, we improve the formalised strategy extraction for \( EF + \forall \text{-red} \) from [8] by observing that the witness 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 \( \psi \), 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 \( C_i \).

\[ \textbf{Theorem 1.} \text{ Let } \mathcal{C} \text{ be the circuit class } NC^1 \text{ or } P/poly. \text{ Given a } \mathcal{C}\text{-Frege } + \forall \text{-red} \text{ refutation } \pi \text{ of a QBF } \exists x \forall y_1 \ldots \exists x_n \forall y_n. \phi(x_1, \ldots , x_n, y_1, \ldots , y_n) \text{ where } \phi \in \Sigma^n_0, \text{ we can construct in time } |\pi|^{O(1)} \text{ an } R^* \text{ refutation of} \]

\[ \bigwedge_{i=1}^{n} (y_i \leftrightarrow C_i(x_1, \ldots , x_i, y_1, \ldots , y_i-1)) \land \phi(x_1, \ldots , x_n, y_1, \ldots , y_n) \]  \hspace{1cm} (2)

for some circuits \( C_i \in \mathcal{C} \).

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

\[ \text{Ext} \land \bigwedge_{i=1}^{n} (y_i \leftrightarrow C_i(x_1, \ldots , x_i, y_1, \ldots , y_i-1)) \land \phi(x_1, \ldots , x_n, y_1, \ldots , y_n) \]

where \( \text{Ext} \) 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 \( \text{Ext} \) substituted by 0 and the other with occurrences of \( y_n \) in \( \text{Ext} \) 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 \( EF + \forall \text{-red} \) 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

\[ ^1 \text{ this includes all commonly studied Resolution-based QBF systems} \]

\[ ^2 \text{ The result easily generalises to further ‘natural’ circuit classes } \mathcal{C} \text{ such as } AC^0 \text{ or } TC^0, \text{ but we will focus here on the two most interesting cases } NC^1 \text{ and } P/poly \text{ leading to Frege and EF systems, respectively.} \]
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 $\psi$ as above is hard for a QBF proof system $P$ it is for one of the following reasons:

1. the existential quantifiers in $\psi$ 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. $\psi$ is witnessable as in 1, but the witnessed formula $\bigwedge_{i=1}^n (y_i \leftrightarrow C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \land \neg \phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$ 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 $C$ 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 $\phi_n$, have no polynomial-size proofs in $P$, then one of the following holds:

1. **Circuit lower bound.** The existential variables in $\psi_n$ are not witnessable by $C$ circuits.
2. **Resolution lower bound.** Condition 1. does not hold, but for all $C$ circuits witnessing $\psi_n$, the witnessed formulas require super-polynomial size Resolution refutations.
3. **Genuine QBF hardness.** There are circuits $C_i \in C$ witnessing $\psi_n$, 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 $\psi_n$ are not witnessable by $C$ circuits, we are done. We therefore assume that there are $C$ circuits witnessing the existential variables.

Suppose that there are some circuits $C_i \in C$ 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 $\bigwedge_i (C_i \leftrightarrow y_i) \land \neg \phi_n$. Since the refutation of $\bigwedge_i (C_i \leftrightarrow y_i) \land \neg \phi_n$ 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 $C_i \in C$, 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

\[
\begin{align*}
\neg y_0 & \lor y_0 \lor \neg y_1 \lor \neg y'_1 \\
y_k & \lor \neg x_k \lor \neg y_{k+1} \lor \neg y'_{k+1} & \quad y'_k & \lor x_k \lor \neg y_{k+1} \lor \neg y'_{k+1} \\
y_n & \lor \neg x_n \lor \neg y_{n+1} \lor \cdots \lor \neg y_{n+n} & \quad y'_n & \lor x_n \lor \neg y_{n+1} \lor \cdots \lor \neg y_{n+n} \\
x_t & \lor y_{n+t} & \quad \neg x_t & \lor y_{n+t} \\
\end{align*}
\]

and quantifier prefix $\exists y_0 y_1 y'_1 \cdots \exists y_k y'_k \forall x_k \cdots \forall x_n \exists y_{n+1} \cdots y_{n+n}$.
This family of QBFs is known to require proofs of size $2^{O(n)}$ 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.

\textbf{Theorem 4.} The formulas KBKF’$_n$ are hard for QU-Resolution due to genuine QBF hardness (case 3 in Theorem 2).

\textbf{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 $\bigwedge_{i=1}^n ((x_i \leftrightarrow y'_i) \land z_i \leftrightarrow y'_i)) \land \phi$, 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 $y'_i \lor y_{n+i}$ and $\neg y'_i \lor y_{n+i}$. Resolving on each $y_{n+i}$ gives $y'_n$, $y_n \lor \neg y'_n$ 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.

\section{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 $\Sigma^b_k$ 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.

\textbf{Definition 5} (Relaxing QU-Res [11]). Let $\Pi = Q_1 x_1 \ldots Q_n x_n$ be a quantifier prefix, and let $\Pi' = Q_{\pi(1)} x_{\pi(1)} \ldots Q_{\pi(n)} x_{\pi(n)}$ be obtained from $\Pi$ by a permutation $\pi : [n] \rightarrow [n]$. If $\pi$ has the property that $\pi(i) < \pi(j)$ for any $1 \leq i < j \leq n$ with $Q_i = \forall$ and $Q_j = \exists$, then we call $\Pi'$ a relaxation of $\Pi$. That is, a relaxation is obtained by ‘moving’ $\forall$ quantifiers to the left. We say that $\Pi'$ is a $\Sigma^b_k$-relaxation if $\Pi'$ is a $\Sigma^b_k$ quantifier prefix.

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

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 $H(\Phi, \Pi^b_k)$.

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.
8 Reasons for Hardness in QBF Proof Systems

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 $\Phi = \Lambda(\vec{x}) \cdot \Lambda_{i=1}^{n} C_{i}(\vec{x})$ and $\Psi = \Pi(\vec{z}) \cdot \Pi_{j=1}^{m} D_{j}(\vec{z})$ be QBFs consisting of quantifier prefixes $\Lambda$ and $\Pi$ over the variables $\vec{x}$ and $\vec{z}$ respectively, and of clauses $C_{i}$ and $D_{j}$ over the corresponding variables. Then define

$$\Phi \otimes \Psi := \Lambda(\vec{x})\Pi(\vec{z}) \cdot \Pi(\vec{z}) \cdot \bigwedge_{i=1}^{n} \bigwedge_{j=1}^{m} (C_{i}(\vec{x}) \lor D_{j}(\vec{z}))$$

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

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

**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 $\Phi$ (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 $\Phi$ or the copies of $\Psi$ appropriately, the lines in the proof can be restricted to a refutation of $\Phi$ or $\Psi$, 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 $\bigwedge_{j=1}^{m} (C_{i}(\vec{x}) \lor D_{j}(\vec{z}))$, 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 $\Psi(\vec{z})$ 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\(^m\)_n, is the CNF \(\bigwedge_{i=1}^{m} (x_{i,1} \lor \cdots \lor x_{i,n}) \land \bigwedge_{j=1}^{m} \bigwedge_{1 \leq i_1 < i_2 \leq n} (\neg x_{i_1,j} \lor \neg x_{i_2,j})\).

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 \(\Phi_n := PHP^{n+1}_n \otimes KBKF_n\) 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\(^{n+1}\)_n requires proofs of size \(2^{\Omega(n)}\) in Resolution [18], we know that PHP\(^{n+1}\)_n 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 \(\Phi_n\) given by Lemma 7, this QU-Res lower bound for \(\Phi_n\) is unambiguously due to the lower bound for PHP\(^{n+1}\)_n 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 \(\Pi_t^t\) prefix results in a true QBF, for any \(t < n\).

Proof. To produce a \(\Pi_t^t\)-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 \(y_n\) and \(y'_n\). 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 \(y_{n+1} = 1\) for each \(i\) then satisfies every clause apart from \(y_{k-1} \lor \neg x_k \lor y_{k+1} \lor \neg y'_{k+1}\), which can be satisfied by playing \(x_k = 0\).

If some \(x_k\) is universally quantified to the left of \(y_k\) and \(y'_k\), 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 \(\Phi_n\) can be written as \(X \lor Z_1 \lor \cdots \lor Z_m\) where \(X\) is a clause in the variables of \(\bar{x}\), and \(Z_i\) is a clause in the variables of \(\bar{z}_i\). We use the terms \(Z\)-variables and \(X\)-variables to refer to any variables in \(z_1, \ldots , z_n\) and \(\bar{x}\) 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\(^{n+1}\)_n 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\(^{n+1}\)_n 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 \( A = A^X \lor A^Z \) is derived as an axiom of \( \Phi_n \) by relaxing QU-Res. Let \( Z_1, \ldots, Z_n \) be such that all the existential variables in \( A^Z \) are in some \( Z_i \). Then the clause \( A^X \) is a semantic consequence of the pigeonhole principle axioms \( C_1, \ldots, C_n \), i.e. \( C_1 \land \cdots \land C_n \models A^X \).

Proof. Suppose that \( C_1 \land \cdots \land C_n \nmid A^X \). Let \( \alpha \) be an assignment to the \( X \)-variables which falsifies \( A^X \) but satisfies each \( C_i \). We can extend \( \alpha \) to the minimal assignment \( \alpha' \) which falsifies \( A \). We show that for any \( \Pi^b_t \)-relaxation of \( \Phi_n \), for \( t < n \), we can extend \( \alpha' \) to a winning strategy for the existential player.

Given a \( \Pi^b_t \)-relaxation of \( \Phi_n \), with quantifier prefix \( \vec{P} \), we show by induction that for each \( k \), we can construct a strategy \( \sigma_k \) on the existential variables of \( X \) and \( Z_1, \ldots, Z_k \) which extends \( \alpha' \) and is a winning strategy for

\[
\vec{P} \cdot \bigwedge_{i=1}^{k} \bigwedge_{j=1}^{m} (C_i(\vec{x}) \lor D_j(\vec{z}))
\]

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

- Suppose \( k = i_j \) for some \( 1 \leq j \leq l \). Then \( \alpha' \), and hence \( \sigma_{k-1} \), already satisfies \( C_k(\vec{x}) \).

- Therefore \( \sigma_{k-1} \) satisfies each clause \( C_k(\vec{x}) \lor D_j(\vec{z}) \) for any \( D \), and we can define \( \sigma_k = \sigma_{k-1} \) on the variables of \( X \) and \( Z_1, \ldots, Z_{k-1} \), 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 \( \alpha' \), and hence \( \sigma_{k-1} \), are not defined on any existential variables in \( Z_k \). Any \( \Pi^b_t \)-relaxation of \( \text{KBKF}_n \) is true, by Lemma 10. Let \( \tau_k \) be a strategy for the existential variables of \( Z_k \) which is a winning strategy for \( \vec{P}' \cdot \bigwedge_{j=1}^{m} D_j(\vec{z}) \), and so also for \( \vec{P}' \cdot \bigwedge_{j=1}^{m} C_k \lor D_j(\vec{z}) \).

As \( \sigma_{k-1} \) is not defined on any existential variables from \( Z_k \), \( \tau_k \) and \( \sigma_{k-1} \) are strategies for disjoint sets of variables. We extend our strategy \( \sigma_{k-1} \) with \( \tau_k \) to give \( \sigma_k \), a winning strategy for \( \vec{P}' \cdot \bigwedge_{i=1}^{k} \bigwedge_{j=1}^{m} (C_i(\vec{x}) \lor D_j(\vec{z})) \).

The final strategy \( \sigma_n \) is therefore a winning strategy for the existential variables of the \( \Pi^b_t \)-relaxation of \( \Phi_n \), and \( \sigma_n \) extends the assignment \( \alpha' \). This suffices to show that the relaxation of \( \Phi_n[\alpha'] \) is true. Since \( \alpha' \) extends \( \beta \), the minimal assignment falsifying \( A \), with assignments to existential variables only, the strategy detailed here will also be a winning existential strategy for any \( \Pi^b_t \)-relaxation of \( \Phi[\beta] \), and so any \( \Pi^b_t \)-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 \( \text{PHP}^n_{l+1} \) 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 \( \text{PHP}^n_{l+1} \). 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 \( \text{PHP}^n_{l+1} \), and there exist axioms \( C_1, \ldots, C_t \) from \( \text{PHP}^n_{l+1} \) such that \( C_1 \land \cdots \land C_t \models C \). Then there is a Resolution proof of \( C \) of size at most \( 18^l \).
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 \( \Phi_n \) by relaxing QU-Res. Let \( S(A^X) \) be the size of the smallest Resolution derivation of \( A^X \) from \( \text{PHP}_n^{n+1} \). 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 \( \text{PHP}_n^{n+1} \). This upper bound is far from tight, but is sufficient for the proof of Theorem 9.

Given \( t \) clauses from \( \text{PHP}_n^{n+1} \), 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 \( C_1, \ldots, C_t \). There are then at most \( t \) blocks \( Y_i \) of pure positive or pure negative literals, at most one corresponding to each \( C_i \). Any clause derived by Resolution from \( C_1, \ldots, C_t \) 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 \( C_1, \ldots, C_t \) is at most \( 3^{2t} \cdot 2^t = 18^t \). Any Resolution derivation of \( C \) from \( C_1, \ldots, C_t \) therefore has size at most \( 18^t \).

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

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

Consider \( \pi|_{\alpha} \), the result of restricting \( \pi \) to those clauses which agree with \( \alpha \). 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 \( \alpha \).
- Suppose a clause \( C \) is derived by a \( \forall \)-red step on a \( Z \)-variable \( u \). Then clearly \( C \lor u \) agrees with \( \alpha \) if \( C \) agrees with \( \alpha \), since \( \alpha \) does not assign \( u \). Also \( C^X = (C \lor u)^X \), so this is a valid step in a Resolution proof on the \( X \)-clauses.
- Suppose \( C \) agrees with \( \alpha \) and \( C \) is derived from \( C_1 \) and \( C_2 \) by resolving on an \( X \)-variable \( x \). Then \( C_1^Z \subseteq C_2 \), and so both \( C_1 \) and \( C_2 \) agree with \( \alpha \) 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 \( \alpha \) 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 \( \alpha \), depending on the value of \( \alpha(z) \). As \( C_1^X \subseteq C_2^X \), we can derive \( C^X \) by a weakening step from whichever agrees with the \( Z \)-assignment, or both if \( \alpha \) is universally quantified.

This completes our induction, and proves that the \( X \)-clauses of the clauses in \( \pi \) which agree with \( \alpha \) are a valid Resolution proof. As we know that any Resolution refutation of \( \text{PHP}_n^{n+1} \) 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 \( \pi \) 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 \( \alpha \), for some constant \( c \).
For every assignment $\alpha$ to the existential $Z$-variables, we can find such an axiom containing at least $g(n)$ existential $Z$-variables and agreeing with $\alpha$. As each of these axioms can agree with at most $a^{2^{-g(n)}}$ proportion of the possible assignments $\alpha$, $\pi$ 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 PHP$_n^{n+1} \otimes$ 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, PHP$_n^{n+1} \otimes$ KBKF$_n$ has linear-size proofs.

> **Definition 14.** A $\Sigma^p_k$-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:

$$(\Sigma^p_k\text{-derivation}) \quad C_1 \quad \ldots \quad C_l \quad D_1 \quad \ldots \quad D_m$$

where there is some $\Sigma^p_k$-relaxation $\Pi'$ of the quantifier prefix $\Pi$ 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 $\Sigma^p_k$-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 $\Sigma^p_k$-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 $\Sigma^p_k$-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 $\Sigma^p_k$-QU-Resolution, parameterised by the number of queries to the $\Sigma^p_k$ 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 $\Sigma^p_k$-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 $\Sigma^b_k$-alternation** if it has short proofs in $\Sigma^p_k$-QU-Resolution, but requires long proofs in any lower class. The proof complexity of formulas in $\Sigma^p_k$-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 $\Sigma^p_k$ 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 $\Sigma^p_k$-P for most QBF proof systems which work with proof lines, such as C-Frege+∀-red systems. Clearly, using a different
We extend this result to we can construct short proofs of these QBFs in which is polynomial in the number of QU-Resolution is known to have strategy extraction by depth-3 Boolean circuits [4].

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

Since there is an $O(n)$-length refutation of $\text{KBKF}_n$ in QU-Res, we know that QU-Res can derive $C_i(\bar{x})$ from $\bigwedge_j C_i(\bar{x}) \vee D_j(\bar{z})$ in $O(n)$ lines. There are $O(n^2)$ clauses $C_i$ in $\text{PHP}_n^{n+1}$, 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 $\text{PHP}_n^{n+1}$ is false, thus from $\bigwedge_j C_i(\bar{x})$, $\Sigma_1^p$-QU-Res derives the empty clause in a single $\Sigma_1^p$-derivation step.

In order to compare this characterisation of QBF proof lower bounds with that in Section 3, we first show that $\Sigma_1^p$-QU-Resolution has strategy extraction. While we only show strategy extraction for $\Sigma_1^p$-QU-Resolution, the result generalises easily to other $\Sigma_1^p$-C-Frege systems.

Lemma 16. $\Sigma_1^p$-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 $\Sigma_1^p$-QU-Resolution by showing that $\Sigma_1^p$-derivations do not contain any information on the strategy for the universal player.

From any $\Sigma_1^p$-QU-Resolution proof we can construct a QU-Resolution proof by replacing the $\Sigma_1^p$-derivation steps with a QU-Resolution derivation of the clauses. By the implicational completeness of QU-Resolution, this is possible, and each $\Sigma_1^p$-derivation can be replaced by a QU-Resolution derivation consistent with the $\Sigma_1^p$-relaxation.

In the case of $\Sigma_1^p$, the relaxation of the prefix treats all variables as existential. A QU-Resolution proof constructed in this way, while potentially much larger than the $\Sigma_1^p$-QU-Resolution proof, does not contain any additional $\forall$-reduction steps that were not in the $\Sigma_1^p$-QU-Resolution proof. Strategy extraction for QU-Resolution constructs a strategy which is polynomial in the number of $\forall$-reduction steps of the proof, as noted in [4]. Given any $\Sigma_1^p$-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 $\Sigma_1^p$-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 $\Sigma_1^p$-QU-Res, deriving the witnessed formula, and then using a $\Sigma_1^p$-derivation to derive $\bot$. This demonstrates that QBFs in the second category are not hard due to alternation of quantifiers.

For sufficiently strong proof systems, such as Frege+$\forall$-red, these are the only two possible reasons for hardness [8]. As Lemma 16 extends naturally to $\Sigma_1^p$-Frege+$\forall$-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 \( \Phi^{n+1} \) formulas (or, less trivially, the formulas from Theorem 15) are all easy for \( \Sigma^p_1 \)-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 \( \Sigma^p_{2k-1} \).

**Lemma 17.** If a family of QBFs has proofs of size \( s(n) \) in \( \Pi^p_m \)-QU-Res or \( \Sigma^p_{2k} \)-QU-Res, then it has proofs of size \( n \cdot s(n) \) in \( \Sigma^p_{m-1} \)-QU-Res or \( \Sigma^p_{2k-1} \)-QU-Res respectively.

In particular, given a family of QBFs \( \Phi_n \), if the alternation hardness of \( \Phi_n \) is precisely \( C \), then \( C = \Sigma^p_{2k+1} \) for some integer \( k \).

**Proof.** We begin by demonstrating that from a \( \Pi^p_m \)-QU-Resolution refutation of \( \Phi_n \) of size \( s(n) \), we can construct a \( \Sigma^p_{m-1} \)-QU-Resolution refutation of size \( O(s(n)) \).

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

Given a \( \Sigma^p_{2k} \)-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 \( \Sigma^p_{2k-1} \)-QU-Resolution proof is to \( \forall \)-reduce these variables in each axiom. The \( \Sigma^p_{2k} \)-QU-Res proof is then followed, with the innermost variables removed from the clauses. At each \( \Sigma^p_{2k} \)-derivation, the innermost variables are not present in any of the clauses, and so the \( \Sigma^p_{2k} \)-relaxation can be replaced by a \( \Sigma^p_{2k-1} \)-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 \( \Pi^p_m \)-QU-Resolution by \( \Sigma^p_{m-1} \)-QU-Resolution would not hold. With the exception of \( \Sigma^p_{2} \)-QU-Resolution, it would still be possible to reduce a \( \Sigma^p_{2k} \)-QU-Resolution proof to a \( \Sigma^p_{2k-1} \)-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 \( \Sigma^p_{2} \)-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 QParity, \( \forall x_1 \ldots x_n \exists z \forall z \exists t_2 \ldots t_n \) 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 QParity$_n$ have $\Sigma_3^b$-alternation hardness. In particular, they are hard for QU-Resolution due to the alternation of quantifiers.

Proof. It is clear that QParity$_n$ has short proofs in $\Sigma_3^p$-QU-Resolution, as their quantifier prefix is $\Sigma_3^b$. By Lemma 17, we need only show that QParity$_n$ does not have polynomial size proofs in $\Sigma_3^p$-QU-Resolution. By Lemma 16, $\Sigma_3^p$-QU-Resolution has strategy extraction by depth-3 circuits. Since any depth-3 circuit for the parity function requires exponential size [15, 19], any $\Sigma_3^p$-QU-Resolution refutation of 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 $\Sigma_k^p$-QU-Resolution for all $k$.

Theorem 20. For any constant $k$, the formulas KBKF$_n$ require proofs of length $2^{\Omega(n)}$ in $\Sigma_k^p$-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 $\Sigma_k^b$ 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 $\Sigma_k^b$-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 $y_j, y'_j$.

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

Given a $\Sigma_k^p$-QU-Resolution proof which contains at most $m \Sigma_k^p$-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 $\Sigma_k^b$-relaxation. Since at least one of $x_n-mk, \ldots, x_n$ does not have this property, the $\Sigma_k^p$-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 $\Sigma_k^p$-QU-Resolution, the algorithm for verifying the proof is allowed to make a constant number of queries to a $\Sigma_k^p$-oracle. Here we will propose a stronger system, motivated by the observation that a $\Sigma_k^p$-oracle query can be used to check multiple parallel $\Sigma_k^p$-derivations at once. Thus as long as no path in the proof dag contains more than $m \Sigma_k^p$-derivation steps,
there is a polynomial-time proof checking algorithm which requires at most $m$ $\Sigma^p_k$-oracle queries.

► **Definition 21.** A parallel $\Sigma^p_k$-QU-Resolution proof of a QBF $\phi$ is a derivation of the empty clause by the same rules as $\Sigma^p_k$-QU-Resolution. The proof may contain an arbitrary number of $\Sigma^p_k$-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 $\Sigma^p_k$-QU-Resolution p-simulates $\Sigma^p_k$-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 $\Phi_n$ such that $\Phi_n$ has polynomial size proofs in parallel $\Sigma^p_k$-QU-Resolution, but requires proofs of size $2^{O(n)}$ in $\Sigma^p_k$-QU-Resolution.

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

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

Since the strategy for each universal variable in $\Phi_n$ requires size $2^{O(n)}$ as a depth-3 Boolean circuit, we see that any polynomial size $\Sigma^p_k$-QU-Resolution proof of $\Phi_n$ must contain for each universal variable, at least one $\Sigma^p_k$-derivation in which the relaxation quantifies the universal variable to the right of the corresponding existential variables from that copy of 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 $\Sigma^p_k$-relaxation can only contain $\frac{1}{2}$ blocks of universal variables, a $\Sigma^p_k$-QU-Resolution proof containing $m$ $\Sigma^p_k$-derivations can only contain suitable relaxations for $\frac{1}{2}mk$ universal variables. Thus for any $\Sigma^p_k$-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 $2^{O(n)}$. ▶

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 $\Sigma^p_1$-relaxation. Parallel $\Sigma^p_1$-derivations can therefore be combined into a single such step. The two proof systems therefore give equivalent definitions for hardness due to $(\Sigma^p_1)$-alternation.

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

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

► **Theorem 23.** The formulas KBKF$_n^k$ require super-polynomial size proofs in parallel $\Sigma^p_k$-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
∀-reduction on a universal variable $x_i$ must be in a clause containing a literal on each $x_j$ for $j < i$. Furthermore, each ∀-reduction on $x_i$ must be preceded by a ∀-reduction on $x_l$ for each $i < l \leq n$. Clearly, these ∀-reductions must also contain the same literals on $x_1, \ldots, x_i$ as in the ∀-reduction on $x_i$.

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

The number of ∀-reductions on variables $x_{n-mk}, \ldots, x_n$ that are not in the expansion of some $\Sigma^p_k$-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 $x_1, \ldots, x_{n-mk}$ for which all ∀-reductions on $x_{n-mk}, \ldots, x_n$ agreeing with this assignment are in an expansion of a $\Sigma^p_k$-derivation.

As mentioned previously, the $x_i$ variables depend only on the $y_i, y'_i$ variables and an expansion of a $\Sigma^p_k$-derivation can only contain a ∀-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 $x_1, \ldots, x_{n-mk}$ is preceded by $mk + 1$ successive ∀-reductions, all of which are obtained by expanding a $\Sigma^p_k$-derivation. Consequently, the path through these ∀-reductions must contain at least $m+1$ $\Sigma^p_k$-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$^\prime_n$. We also leave open the question of finding formulas which have alternation hardness precisely $\Sigma^b_k$ for odd $k > 3$.

References


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 $\psi_n$ defined such that

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

The quantified Boolean circuits $\Psi_n$ then provide a lower bound for relaxing QU-Res.

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

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

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