Hardness Characterisations and Size-Width Lower Bounds for QBF Resolution

Olaf Beyersdorff\textsuperscript{1}, Joshua Blinkhorn\textsuperscript{1}, and Meena Mahajan\textsuperscript{2}

\textsuperscript{1}Institut f"{u}r Informatik, Friedrich-Schiller-Universit"{a}t Jena, Germany
\textsuperscript{2}The Institute of Mathematical Sciences, HBNI, Chennai, India

Abstract. We provide a tight characterisation of proof size in resolution for quantified Boolean formulas (QBF) by circuit complexity. Such a characterisation was previously obtained for a hierarchy of QBF Frege systems \cite{14}, but leaving open the most important case of QBF resolution. Different from the Frege case, our characterisation uses a new version of decision lists as its circuit model, which is stronger than the CNFs the system works with. Our decision list model is well suited to compute countermodels for QBFs. Our characterisation works for both Q-Resolution and QU-Resolution, which we show to be polynomially equivalent for QBFs of bounded quantifier alternation. Using our characterisation we obtain a size-width relation for QBF resolution in the spirit of the celebrated result for propositional resolution \cite{3}. However, our result is not just a replication of the propositional relation – intriguingly ruled out for QBF in previous research \cite{10} – but shows a different dependence between size, width, and quantifier complexity. We demonstrate that our new technique elegantly reproves known QBF hardness results and unifies previous lower-bound techniques in the QBF domain.

1 Introduction

Proof complexity is a field at the intersection of logic and complexity that studies the difficulty of proving formal theorems, where difficulty of proving is associated with the size of proofs in different proof calculi. Obtaining lower bounds to the size of proofs is the central and most challenging goal in proof complexity, and the endeavour bears tight relations to central questions in computational complexity \cite{22,32} and first-order logic \cite{4,21}. In addition to this foundational quest, proof complexity has become the main theoretical tool for the analysis of powerful SAT solvers that routinely solve huge industrial instances of the NP-complete SAT problem \cite{10,38,18}.

Many conceptually different proof systems have been studied, but the resolution system \cite{15,42} – operating on clauses and using just one rule – has received by far the greatest attention. This is because resolution is a foundational system from the theoretical point of view \cite{45}, but also because resolution (and its subsystems) underpin modern SAT solving \cite{38,18}, whereby lower bounds on resolution proof size provide lower bounds on solving time.

In the past two decades, researchers have tried to lift the successes of SAT solving and propositional proof complexity to even more computationally challenging settings, with quantified Boolean formulas (QBF) receiving key attention. As a PSPACE-complete problem, QBF widely generalises SAT and encompasses the polynomial hierarchy, a source of many practical problems \cite{23,37,31} that are efficiently tackled by modern QBF solvers. As in the propositional case, QBF resolution systems play a key role in understanding the efficiency and limits of current solving. Arguably, the simplest QBF resolution system is QU-Res, augmenting propositional resolution by just one universal reduction rule \cite{30,24}.

There is a long-standing belief in the proof complexity community (cf. \cite{2}) that there exist strong connections between the logical problem of determining the size of the shortest proof for a given formula (proof size bounds) and the complexity problem of finding small circuits for explicit functions corresponding to the formula (circuit bounds).
While such a formal connection has so far appeared elusive for central propositional proof systems such as resolution or Frege systems, some connections are known, for example between algebraic proof systems and algebraic circuit complexity [25]. Arguably, the clearest such connection has been shown in the QBF domain, between the hierarchy of QBF Frege systems and the corresponding circuit classes. For QBF Frege (where lines are propositional formulas, i.e. $NC^1$ circuits) the connection manifests as follows: there are QBFs that require superpolynomial-size proofs in QBF Frege if, and only if, there are functions requiring superpolynomial-size $NC^1$ circuits or there are propositional formulas requiring superpolynomial-size propositional Frege proofs [14]. This characterisation unites central problems from circuit complexity ($NC^1$ lower bounds) with central problems from proof complexity (Frege lower bounds). However, such a connection has remained open for resolution systems (either QBF or propositional), which are of prime importance, theoretically and practically.

1.1 Our contributions

A. Characterising QU-Res hardness. We obtain a tight characterisation of QU-Res hardness in terms of circuit lower bounds. More precisely, we show that a sequence of QBFs $Q_n$ of bounded quantifier complexity requires superpolynomial QU-Res proofs if and only if each countermodel for $Q_n$ requires superpolynomial circuit size (in a natural circuit model defined on decision lists as explained below) or if $Q_n$ exhibits propositional resolution hardness (defined in a precise sense, Theorem 26). We thus identify a dichotomy for QU-Res hardness: it either rests on circuit lower bounds or on propositional resolution lower bounds. We note that the second case is inevitable: each propositional resolution lower bound (e.g. for the pigeonhole principle [26]) can be easily turned into a QU-Res lower bound. The surprising insight is that ‘genuine QBF hardness’ (cf. [12,19]) can be completely characterised by circuit hardness.

Our result is best obtained in a model of QBF systems that ‘filters out’ propositional hardness (the second case above). For this we use the model of oracle QBF proof systems defined in [12], which employs an NP oracle to perform arbitrary propositional entailments in one inference step. For example, in the oracle system QU$^{NP}$-Res, propositional resolution derivations of arbitrary size can be performed in just one step. The use of an NP oracle in QU$^{NP}$-Res is akin to the use of SAT solvers as oracles in QBF solving [30].

The hardness characterisation we obtain for QU$^{NP}$-Res is in terms of unified decision lists (UDL). This is a natural adaptation of the classical model of decision lists [41], which computes functions $\{0,1\}^n \rightarrow \{0,1\}$, to multi-output functions $\{0,1\}^n \rightarrow \{0,1\}^m$. Our first main result (Theorem 11) shows that for bounded-alternation QBFs, proof size in QU$^{NP}$-Res is polynomially related to the size of UDLs computing countermodels of the QBF.

Technically, this result is shown via two simulations. The first efficiently extracts UDLs from QU$^{NP}$-Res proofs (Theorem 14). Single-output decision lists have been used before to extract winning strategies for QBFs [13,6]. Here we show that winning strategies can also be extracted via multi-output decision lists, and these can be combined via a direct product construction (Definition 12) into one single UDL that computes the countermodel. We argue that representing the countermodel by just one function (computed by the UDL) is quite natural. However, it differs from the conventional approach, which represents the countermodel as a collection of Herbrand functions, one for each universal variable.

The second simulation turns a UDL into a QU$^{NP}$-Res refutation (Theorem 19). This is conceptually novel, as – to the best of our knowledge – the efficient construction of proofs from countermodels has not been considered before. In the course of the simulation, we obtain a normal form for proofs via the entailment sequence associated with a UDL (Definition 17). Inference steps in this entailment sequence also allow us to pinpoint sources for propositional
hardness that arise when replacing NP oracle calls with actual resolution derivations. This way we obtain the dichotomy for QU-Res explained above (Theorem 26).

B. QU-Resolution and Q-Resolution. While QU-Res is arguably the simplest QBF resolution system from a logical perspective (it just adds the universal reduction rule to propositional resolution), there are other QBF resolution systems that better correspond to ideas in QBF solving. A core system among these is Q-Resolution (Q-Res), which is also historically the first QBF resolution system. Q-Res is a restriction of QU-Res in which resolution pivots must be existential. This corresponds to techniques in QCDCL solving (even though Q-Res does not capture QCDCL precisely).

The system QU-Res is exponentially stronger than Q-Res, the separation provided by the prominent KBKF_n formulas. These formulas use unbounded quantifier alternations, and indeed, we show that every separation must be of this form. We obtain the surprising result that Q-Res and QU-Res are polynomially equivalent on QBFs of bounded quantifier alternation (Theorem 31). This simulation is shown by a direct construction.

As a consequence, our hardness characterisation in terms of UDLs transfers directly to Q-Res (Corollary 33).

C. Size and width for QBF Resolution. Our new connection between QBF resolution and UDLs does not only provide a tight characterisation of QBF resolution hardness, it also paves the way towards a powerful lower-bound method. We show that lower bounds on resolution width – defined as the size of the largest clause in the proof – directly imply lower bounds for proof size. The celebrated result of Ben-Sasson & Wigderson provides such a size-width result for propositional resolution. Indeed, the vast majority of resolution hardness results are nowadays shown via this method.

Here we provide the first size-width result for QBF (Theorem 35). In a nutshell it says that each short QU-Res proof can be transformed into a narrow proof, where a proof is narrow if it does not contain a clause with many existential literals. What is perhaps most surprising is that the authors of have previously ruled out such a size-width result for Q-Res and QU-Res. Not only did they show that the proof method of does not lift to QBF, they also provided concrete QBF counterexamples to their size-width relation.

Here we use our UDL characterisation, together with a size-width transfer for decision lists of Bshouty, to obtain a size-width result for QU-Res (indeed even for the model of QU^{NP}-Res, yielding stronger size lower bounds). Our result, however, is not a mere QBF replication of Ben-Sasson & Wigderson’s result. There are two crucial differences. First, in contrast to our size-width result does not depend on the initial width of the formula. This makes the technique easier to apply and avoids the need for Tseitin transformations, which are often required in the propositional domain. Second, our size bound depends on the number of quantifier alternations of the QBF. Crucially, the counterexamples of use unbounded alternations, thus ruling out the relation of, but not contradicting our Theorem.

D. Unification of previous lower-bound techniques. Our hardness characterisation in terms of UDLs together with the size-width method encompasses and extends previous lower bound methods for QBF resolution. In addition to lifted propositional techniques, there exist two genuine QBF techniques: strategy extraction and the size-cost-capacity technique. These techniques are orthogonal in the sense that each yields hardness results that cannot be shown by the other. Here we demonstrate that UDL hardness captures both.

In the strategy extraction method, lower bounds are shown by extracting strategies in terms of a collection of single-output decision lists, which can be turned into bounded-depth circuits. The authors then construct QBFs with a single universal variable
whose unique Herbrand function is hard to compute by bounded-depth circuits (such as the parity function \textsuperscript{[27]}). Such functions are also hard for UDLs (Section \textsuperscript{[4.3]}). Moreover, we show that width bounds for QBFs based on the parity and majority functions are easy to obtain (Section \textsuperscript{[6.2]}). We thus \textit{elegantly reprove previous hardness results} for parity and majority formulas with our technique, without the need to import substantial circuit complexity results \textsuperscript{[27,10,44]}.

The \textit{size-cost-capacity technique} \textsuperscript{[5]} establishes hardness for QBFs where countermodels might be easy to compute by single-output decision lists, but must have large range. The large range immediately implies large UDLs (Section \textsuperscript{[4.5]}), hence again we can show the hardness results with our new technique. We illustrate this with the equality formulas (Theorem \textsuperscript{39}).

\textbf{Organisation.} The remainder of this article is organised as follows. In Section \textsuperscript{2} we review results with our new technique. We illustrate this with the equality formulas (Theorem \textsuperscript{39}). We thus width bounds for QBFs based on the parity and majority functions are easy to obtain (Section \textsuperscript{6.2}). We thus elegantly reprove previous hardness results \textsuperscript{[27,40,44]}. We thus conclude in Section \textsuperscript{7} with a discussion and open problems.

\section{Preliminaries}

\textbf{Propositional logic.} \( \mathcal{V} \) is a countable set of Boolean \textit{variables}. A \textit{literal} is a variable \( z \) in \( \mathcal{V} \) or its negation \( \overline{z} \), with \( \text{var}(z) = \text{var}(\overline{z}) = z \). The literals \( z \) and \( \overline{z} \) are \textit{complementary}. For any literal \( a \), the complementary literal is denoted \( \overline{a} \).

A \textit{clause} is a disjunction \( c := a_1 \lor \cdots \lor a_k \) of pairwise non-complementary literals, with \( \text{vars}(c) := \{ \text{var}(a_i) : i \in [k] \} \). We often remove the disjunction symbols from a written clause, for example we write \( z_1 \overline{z}_2 z_3 \) for \( z_1 \lor \overline{z}_2 \lor z_3 \). Given a set \( Z \) of Boolean variables, \( c|_Z \) is the disjunction of literals \( a \) appearing in \( c \) with \( \text{var}(a) \in Z \).

A \textit{conjunctive normal form} formula (CNF) is a conjunction \( F := c_1 \land \cdots \land c_k \) of clauses, with \( \text{vars}(F) := \bigcup_{i=1}^k \text{vars}(c_i) \).

A \textit{term} is a finite conjunction \( t := a_1 \land \cdots \land a_k \) of non-complementary literals, with \( \text{vars}(t) := \{ \text{var}(a_i) : i \in [k] \} \). The negation of \( t \) is the clause \( \overline{t} := \overline{a}_1 \lor \cdots \lor \overline{a}_k \). The negation of a clause \( c \) is the unique term \( \overline{c} \) whose negation is \( c \).

An \textit{assignment} \( \tau \) to a set \( Z \) of Boolean variables is a function from \( Z \) into the set of \textit{Boolean constants} \( \{0,1\} \). The set of all assignments to \( Z \) is denoted \( \langle Z \rangle \). A partial assignment to \( Z \) is an assignment to a subset of \( Z \). We often represent assignments as terms, as there is a natural one-one correspondence between the two. The term \( t \) with \( \text{vars}(t) = Z \) represents the assignment \( \tau : Z \to \{0,1\} \) which maps \( z \in Z \) to 0 if, and only if, \( \overline{z} \) is a conjunct in \( t \).

The \textit{restriction} of a literal, clause, CNF or term \( \phi \) by \( \tau \), denoted \( \phi[\tau] \), is the result of substituting each variable \( z \) in \( Z \) by \( \tau(z) \), followed by applying the standard simplifications for Boolean constants, i.e. \( \overline{0} \mapsto 1, \overline{1} \mapsto 0, 0 \lor 0 \mapsto c, c \lor 0 \mapsto c, c \lor 1 \mapsto 1, t \land 1 \mapsto t, \) and \( t \land 0 \mapsto 0 \). We say that \( \tau \) \textit{satisfies} \( \phi \) when \( \phi[\tau] = 1 \), and falsifies \( \phi \) when \( \phi[\tau] = 0 \).

Otherwise, a \textit{formula}, and a \textit{substitution} of formulas for variables, is defined in the standard way for propositional logic (cf. \textsuperscript{[45]}). A formula \( F \) \textit{entails} another formula \( G \) (written \( F \models G \)) when every assignment to \( \text{vars}(F) \cup \text{vars}(G) \) satisfying \( F \) also satisfies \( G \). Formulas \( F \) and \( G \) are \textit{logically equivalent} (written \( F \equiv G \)) when they entail one another.

\textbf{Quantified Boolean formulas.} A \textit{quantified Boolean formula} (QBF) \( Q \) of alternation depth \( d \) is a formula of the form \( P \cdot F \), where \( P := \exists X_1 \forall U_1 \cdots \exists X_d \forall U_d \exists X_{d+1} \) is called the \textit{quantifier prefix} and \( F \) is a CNF called the \textit{matrix}. The \( X_i, U_i \) are pairwise-disjoint sets of Boolean variables called the \textit{blocks} of \( Q \).

The sets \( \text{vars}_q(Q) := \bigcup_{i=1}^{d+1} X_i \) and \( \text{vars}_u(Q) := \bigcup_{i=1}^d U_i \) are referred to as the \textit{existential variables} and \textit{universal variables} of \( Q \), respectively, and their union \( \text{vars}(Q) \) as the \textit{variables}.
of Q. Given two variables z, z’ in \text{vars}(Q), we say that z is left of z’ (written \(z <_P z’\)) when z belongs to a block quantified before that of z’. We deal only with closed QBFs, i.e. those for which \(\text{vars}(F) \subseteq \text{vars}(Q)\). The restriction of Q by an assignment \(\tau\) is \(Q[\tau] := P[\tau] \cdot F[\tau]\), where \(P[\tau]\) is obtained from \(P\) by deleting each variable in \(\text{vars}(\tau)\) and any redundant quantifiers.

A set of QBFs has bounded alternation if each has alternation depth at most \(d\), for some constant \(d\).

**QBF resolution proof systems.** We work with refutational QBF proof systems, i.e. systems proving the falsity of a given QBF. We call a refutational QBF proof system \(P\) sound when there is no \(P\)-refutation of a true QBF, and complete when every false QBF has a \(P\)-refutation. Given two refutational QBF proof systems \(P\) and \(Q\), we say that \(P\) \(p\)-simulates \(Q\) (written \(Q \leq_P P\)) when there exists a polynomial-time computable translation mapping \(Q\)-refutations into \(P\)-refutations, while preserving the refuted QBF [22]. We say that \(P\) and \(Q\) are \(p\)-equivalent (written \(P \equiv_P Q\)) when they \(p\)-simulate one another.

**QU-Resolution (QU-Res)** is the QBF analogue of propositional resolution [1542], defined as follows.

**Definition 1 (QU-Res [2430]).** A QU-Res derivation from a QBF \(P \vdash F\) is a sequence of clauses \(\pi := c_1, \ldots, c_s\) in which each \(c_i\) is derived by one of the following rules:

- Axiom: \(c_i\) is a clause in the matrix \(F\);
- Resolution: \(c_i = a \lor b\), where \(c_j = a \lor z\) and \(c_k = b \lor \neg \pi\) for some \(r, s < i\) and variable \(z\).
- Weakening: \(c_i = c_r \lor b\) for some \(r < i\) and clause \(b\).
- Universal reduction: \(c_i = c_r[\mu]\) for some \(r < i\) and some universal assignment \(\mu\) with \(\text{vars}_3(c_r) <_P \text{vars}(\mu)\).

The size of \(\pi\) is \(|\pi| = s\), and \(\pi\) is a refutation when \(c_s = \bot\).

The axiom, resolution and weakening rules together are propositionally implicationally complete; that is, if \(F \models c\), then there exists a derivation of \(c\) from \(F\). The refutational QBF proof system QU\(^W\)-Res allows any such correct propositional implication to be derived in a single step, eliminating all hardness due to propositional resolution.

**Definition 2 (QU\(^W\)-Res [12]).** QU\(^W\)-Res is defined as for QU-Res, except that the resolution and weakening rules are replaced by the following single rule:

- \(\Sigma_1\)-rule: \(\bigwedge_{j=1}^{i-1} c_j \models c_i\).

3 **Countermodels as decision lists**

A countermodel witnesses the falsity of a QBF. In the literature, countermodels are usually defined in one of two equivalent ways (under various names): either as a collection of functions, one for each universal variable (called here distributed countermodel), or as a single function (unified countermodel). In this section, we recall the definitions of distributed and unified countermodels. We show that distributed countermodels represented by term decision lists are unsuitable for characterising hardness in QU\(^W\)-Res (Subsection 3.1) and propose a model for multi-output term decision lists which serves as a natural representation for unified countermodels (Subsection 3.2).

\(^1\) Some definitions of QU-Res disallow deriving tautological clauses [30]. The definition of universal reduction chosen here eliminates this restriction.

\(^2\) Note that proofs in QU\(^W\)-Res cannot necessarily be checked in polynomial time, hence QU\(^W\)-Res is not a proof system in the sense of [22], but conforms to our definition of proof system above (cf. also [13] for a formal definition of oracle proof systems).

5
3.1 Distributed countermodels

A distributed countermodel defines a set of formulas which, when substituted for the universal variables, leaves the matrix unsatisfiable. In order to respect the variable dependencies imposed by the order of quantification, each function must depend only on the preceding existential variables.

**Definition 3 (distributed countermodel).** Let $Q$ be a QBF with $\text{vars}_v(Q) = u_1, \ldots, u_m$, and let $D_i$ denote the union of the existential blocks preceding $u_i$ in the prefix. A distributed countermodel for $Q$ is a collection of functions $\{f_i\}_{i \in [m]}$ of the form $f_i : \langle D_i \rangle \rightarrow \{0, 1\}$, such that the substitution of formula representations of $f_1, \ldots, f_m$ for the universal variables $u_1, \ldots, u_m$ in $F$ yields an unsatisfiable formula.

We illustrate this concept with the equality formulas, which we will use as a running example.

**Definition 4 (equality [5]).** The $n$th equality formula is

$$Q_{EQ}^n := \exists x_1 \cdots x_n \forall u_1 \cdots u_n \exists z_1 \cdots z_n \cdot (\overline{x_1} \lor \cdots \lor \overline{x_n}) \land \bigwedge_{i=1}^{n} \left( (\overline{x_i} \lor \overline{u_i} \lor z_i) \land (x_i \lor u_i \lor z_i) \right).$$

**Example 5.** The $n$th equality formula has the unique distributed countermodel $\{f_i\}_{i \in [n]}$, where

$$f_i : \langle \{x_1, \ldots, x_n\} \rangle \rightarrow \{0, 1\}$$

$$\tau \mapsto \begin{cases} 0 & \text{if } \tau(x_i) = 0, \\ 1 & \text{if } \tau(x_i) = 1. \end{cases}$$

Here, each function $f_i$ is represented by the atomic formula $x_i$. It is easy to see that substituting each $u_i$ for $x_i$ in the matrix of $Q_{EQ}^n$ yields an unsatisfiable formula. \[\blacksquare\]

Particularly in the context of strategy extraction, whereby one translates QBF refutations into countermodels, it is quite natural to represent a distributed countermodel as a set of term decision lists, one for each individual function [6]. Let us recall the traditional definition of a term decision list.

**Definition 6 (decision list [41]).** Given a set $X$ of variables, a decision list is a sequence of pairs $L := (\varepsilon_1, b_1), \ldots, (\varepsilon_s, b_s)$ where

- the $\varepsilon_i$ are terms with $\text{vars}(\varepsilon_i) \subseteq X$ and $\bigvee_{i=1}^s \varepsilon_i \equiv T$,
- the $b_i$ are Boolean constants, i.e. 0 or 1.

$L$ computes the function from $\langle X \rangle$ into $\{0, 1\}$ mapping $\tau$ to $\mu_i$, where $i$ is the least natural number for which $\tau$ satisfies $\varepsilon_i$.

As far as characterising $\text{QU-Res}$ hardness is concerned, the problem with this computation model – distributed countermodels represented as decision lists – is that it is too strong, even for bounded alternation depth. For example, the distributed countermodel $\{f_i\}_{i \in [n]}$ from Example [4] can be computed by $n$ constant-size decision lists, namely

$$L_i := (x_i, u_i), (\overline{x_i}, \overline{u_i}), \quad i \in [n],$$

but the equality formulas require exponential-size $\text{QU}^\text{np}$-$\text{Res}$ refutations [5].

\[\blacksquare\]
3.2 Unified countermodels

A unified countermodel is a single function which simultaneously represents the individual functions of a distributed countermodel. Formally, there are two differences. First, the output of the function is not a \(\{0, 1\}\) value, but a total assignment to the universal variables, giving a \(\{0, 1\}\) value for each universal variable. Secondly, the prefix dependencies, which are implicit in the function signatures of a distributed countermodel, must be explicitly enforced.

**Definition 7 (unified countermodel).** Let \(Q := P \cdot F\) be a QBF of alternation depth \(d\). A unified countermodel for \(Q\) is a function \(f : \langle \text{vars}_3(Q) \rangle \rightarrow \langle \text{vars}_0(Q) \rangle\) satisfying two conditions:

(a) for each \(\tau \in \text{dom}(f)\), \(\tau \land f(\tau)\) falsifies \(F\);

(b) for each \(\tau, \rho \in \text{dom}(f)\) and each \(i \in [d]\), if \(\tau, \rho\) agree on the first \(i\) existential blocks, then \(f(\tau), f(\rho)\) agree on the first \(i\) universal blocks.

**Example 8.** The \(n^{th}\) equality formula has the unique unified countermodel

\[f_{EQ} : \langle (x_1, \ldots, x_n) \rangle \rightarrow \langle \{u_1, \ldots, u_n\} \rangle\]

where \(f_{EQ}(\tau) : \{u_1, \ldots, u_n\} \rightarrow \{0, 1\}\) is the assignment mapping each \(u_i\) to \(\tau(x_i)\). It is easy to see that \(f_{EQ}\) is a single-function representation of the distributed countermodel from Example 5 and readily verified that conditions (a) and (b) of Definition 7 are satisfied.

In order to represent a unified countermodel as a decision list, we specify a new format to allow simultaneous output for multiple Boolean variables. This is achieved in the most natural way, specifying a term over the universal variables which represents the desired output assignment.

**Definition 9 (multi-output decision list).** Given sets \(X\) and \(U\) of Boolean variables, a multi-output term decision list is a sequence of pairs \(L := (\varepsilon_1, \mu_1), \ldots, (\varepsilon_s, \mu_s)\) where

- the \(\varepsilon_i\) are terms with \(\text{vars}(\varepsilon_i) \subseteq X\) and \(\bigvee_{i=1}^s \varepsilon_i \equiv \top\);
- the \(\mu_i\) are terms with \(\text{vars}(\mu_i) = U\).

\(L\) computes the function from \(\langle X\rangle\) into \(\langle U\rangle\) mapping \(\tau\) to \(\mu_i\), where \(i\) is the least natural number for which \(\tau\) satisfies \(\varepsilon_i\).

We refer to a multi-output term decision list computing a unified countermodel for a QBF \(Q\) as a unified decision list (UDL) for \(Q\). Without ambiguity, we will use the same symbol (e.g. \(L\)) to represent both the UDL and its computed function.

Note that the insistence on a single function suitably reduces the strength of the computational model, in terms of representation size. For example, UDLs for the equality formulas must have exponential size, matching the exponential-size \(\text{QU}^{NP}_{\text{Res}}\) refutations. This is due to the fact that the range of the unique unified countermodel, which is the complete set of universal assignments, has cardinality \(2^n\). The minimal range cardinality of a unified countermodel is an obvious lower bound to the size of a UDL.

4 Characterising hardness in QU-Res

In this section, we demonstrate that UDLs have exactly the right strength to characterise \(\text{QU}^{NP}_{\text{Res}}\) refutation size on bounded alternation QBFs. For this, we cast UDLs as a refutational QBF proof system.
Let \( \text{Definition 12 (direct product).} \) A UDL-refutation of a QBF \( Q \) is a UDL \( L := (\varepsilon_1, \mu_1), \ldots, (\varepsilon_s, \mu_s) \) for \( Q \). The size of \( L \) is \( |L| := s \).

Our central result is the following.

**Theorem 11.** \( \text{QU}^{\text{NP}} \text{-Res} \equiv_p \text{UDL} \) on bounded-alternation QBFs.

The two individual p-simulations are shown in Subsection 4.1 (Corollary 15) and Subsection 4.2 (Corollary 20). In Subsection 4.3 we demonstrate that the equivalence cannot be extended to unbounded alternation depth.

In Subsection 4.4 we characterise bounded-alternation hardness in QU-Res, insofar as superpolynomial QU-Res lower bounds come either from large UDLs or from an embedded propositional resolution lower bound. Finally, in Subsection 4.5 we discuss how UDL lower bounds encompass both the strategy extraction [7,6] and size-cost techniques for QU-Res [5].

### 4.1 From QU-Res to unified decision lists

In this subsection, we show an efficient transformation from QU-Res refutations into unified decision lists. The transformation is a two-step process.

In the first step, we transform the refutation into a collection of multi-output term decision lists, each of which computes the countermodel for just a single universal block, based on assignments to all previous blocks. This constitutes a modification of the strategy extraction procedure from [11], which works per universal variable, rather than per universal block.

In the second step, we transform the collection into a single unified decision list. This involves taking a kind of ‘direct product’ of multi-output term decision lists. We turn first to the definition of this operation.

**Definition 12 (direct product).** Let \( X_1, U_1, X_2 \) and \( U_2 \) be pairwise-disjoint sets of Boolean variables, and let \( L := (\varepsilon_1, \mu_1), \ldots, (\varepsilon_s, \mu_s) \) and \( M := (\delta_1, \nu_1), \ldots, (\delta_t, \nu_t) \) be multi-output term decision lists with

\[
\begin{align*}
\text{vars}(\varepsilon_i) & \subseteq X_1 \text{ and vars}(\mu_i) = U_1, & \text{for } i \in [s], \\
\text{vars}(\delta_j) & \subseteq X_1 \cup U_1 \cup X_2 \text{ and vars}(\nu_j) = U_2, & \text{for } j \in [t].
\end{align*}
\]

The direct product \( L \times M \) is the decision list

\[
(\varepsilon_1 \land \delta_1 [\mu_1] \land \nu_1), \ldots, (\varepsilon_s \land \delta_t [\mu_s] \land \nu_t). 
\]

The direct product \( L \times M \) computes a function based on \( M \), which first queries \( L \) for the assignment to \( U_1 \). Informally, the \( U_1 \) variables in \( M \) are substituted for the function computed by \( L \), while \( U_1 \) is moved from the domain to the codomain. This is stated formally as follows.

**Proposition 13.** Let \( X_1, U_1, X_2 \) and \( U_2 \) be pairwise-disjoint Boolean variable sets, and let \( L \) and \( M \) be multi-output decision lists computing \( L : \langle X_1 \rangle \to \langle U_1 \rangle \) and \( M : \langle X_1 \cup U_1 \cup X_2 \rangle \to \langle U_2 \rangle \). Then \( L \times M \) computes the function

\[
L \times M : \langle X_1 \cup X_2 \rangle \to \langle U_1 \cup U_2 \rangle \\
\tau \mapsto f(\tau |_{X_1}) \land g(\tau \land f(\tau |_{X_1})).
\]
Proof. Let $L := (\varepsilon_1, \mu_1), \ldots, (\varepsilon_s, \mu_s)$, $M := (\delta_1, \nu_1), \ldots, (\delta_t, \nu_t)$. Let $\tau \in \langle X_1 \cup X_2 \rangle$, and let $a$ and $b$ be the least natural numbers such that $\tau|_{X_1}$ satisfies $\varepsilon_a$ and $\tau$ satisfies $\delta_b[\mu_a]$. By definition of decision list (Definition 9),

$$(L \times M)(\tau) = \mu_a \land \nu_b.$$ 

Clearly, $L(\tau|_{X_1}) = \mu_a$ by definition of decision list, therefore $\tau \land L(\tau|_{X_1}) = \tau \land \mu_a$. Aiming for contradiction, suppose that $M(\tau \land \mu_a) \neq \nu_b$. Since $\tau$ satisfies $\delta_b[\mu_a]$, $\tau \land \mu_a$ satisfies $\delta_b$. Therefore $\tau \land \mu_a$ satisfies some $\delta_{b'}$ with $b' < b$. It follows that $\tau$ satisfies $\delta_{b'}[\mu_a]$, contradicting the minimality of $b$.

We note that the size of a direct product is the product of the sizes of the original decision lists.

Proof of the simulation. The complete transformation is detailed in the proof of the following theorem.

Theorem 14. A $\text{QU}^\text{Res}$ refutation $\pi$ of a QBF $Q$ of alternation depth $d$ can be transformed into a UDL $t(\pi)$ for $Q$, where $|t(\pi)| \leq |\pi|^4$. The transformation $t$ is computable in time $O(|\pi|^4)$.

Proof. Let $Q := P := \exists X_1 \forall U_1 \cdots \exists X_d \forall U_d \exists X_{d+1} \cdot F$ be a QBF, and let $\pi := c_1, \ldots, c_s$ be a $\text{QU}^\text{Res}$ refutation of $Q$. We assume without loss of generality that each universal reduction step in $\pi$ is due to a total assignment to a universal block.

For each $i \in [d]$ and $j \in [s+1]$, we define a collection of multi-output term decision lists as follows: $L^{i+1}_j := \langle (\top, \alpha_i) \rangle$, where $\alpha_i$ is some fixed assignment to $U_i$; for each $j \in [s]$, $L^j_i := \langle (\overline{c_j}, \mu) \rangle$, $L^{j+1}_i$ if $c_j$ was derived by universal reduction due to $\mu \in \langle U_i \rangle$, and $L^j_i := L^{j+1}_i$ otherwise.

By backwards induction on $j \in [s+1]$, we show that the combined direct product of these lists

$$L^j := L^j_1 \times (L^2_2 \times \cdots \times (L^d_{d-1} \times L^j_d) \cdots)$$

is a UDL for $P \cdot F \land \bigwedge_{k=1}^{j-1} c_k$. We therefore prove the theorem, i.e. that $L^1$ is a UDL for $Q$ of size at most $|\pi|^d$, that can clearly be constructed in time $O(|\pi|^4)$.

It is clear by construction that each $L^j_i$ computes a function

$$L^j_i : \langle X_1 \cup \cdots \cup X_i \cup U_1 \cup \cdots \cup U_{i-1} \rangle \rightarrow \langle U_i \rangle.$$ 

Hence, by definition of direct product (Definition 12), $L^j_i$ computes a function

$$L^j_i : \langle \text{vars}_2(Q) \rangle \rightarrow \langle \text{vars}_s(Q) \rangle$$

satisfying condition (b) for a unified countermodel (Definition 7). It remains to show that condition (a) is satisfied; that is, for each $\tau \in \langle \text{vars}_s(Q) \rangle$, we must show that $\tau \land L^j_i(\tau)$ falsifies $F \land \bigwedge_{k=1}^{j-1} c_k$. 

Base case $j = s + 1$. Since $c_s$ is the empty clause, $\tau \land L^{s+1}_j(\tau)$ always falsifies $F \land \bigwedge_{k=1}^{s} c_k$.

Inductive step $j \in [s]$. We consider two cases, based on how $c_j$ was derived.

Suppose that $c_j$ was introduced as an axiom, or derived by the $\Sigma_1$-rule. In either case, $L^j = L^{j+1}_j$ and $F \land \bigwedge_{k=1}^{j-1} c_k \vDash c_j$. By the inductive hypothesis we know that $\tau \land L^{j+1}(\tau)$ falsifies $F \land \bigwedge_{k=1}^{j-1} c_k$. It follows that $\tau \land L^j_i(\tau)$ falsifies $F \land \bigwedge_{k=1}^{j-1} c_k$.

On the other hand, suppose that $c_j$ was derived by universal reduction from $c_r$ due to the assignment $\mu \in U_i$. In this case, $L^j_k = L^{j+1}_k$ for each $k \neq i$. We consider two cases.
(a) Suppose that \( \tau \land L^{j+1}(\tau) \) falsifies \( c_j \). Consider the direct product of lists up to, but not including \( L^j_i \), namely

\[
M^j := L^j_1 \times (L^j_2 \times \cdots \times (L^j_{i-2} \times L^j_{i-1}) \cdots ),
\]

and let \( D_i \) and \( D_{i-1} \) denote the union of existential blocks preceding \( U_i \) and \( U_{i-1} \) respectively. It is easy to see that

\[
\tau|_{D_i} \land M^j(\tau|_{D_{i-1}}) \text{ satisfies } \overline{\tau_j},
\]

from which it follows that

\[
L^j_i(\tau|_{D_i} \land M^j(\tau|_{D_{i-1}})) = \mu.
\]

As a result, \( L^j(\tau) \) extends \( \mu \). Therefore \( \tau \land L^j(\tau) \) falsifies \( c_j \). Then the addition of \( (\overline{\tau_j}, \mu) \) to \( L^{j+1} \) has no effect on \( L^{j+1} \), so that \( L^j(\tau) = L^{j+1}(\tau) \). Hence \( \tau \land L^j(\tau) \) falsifies \( F \land \bigwedge_{k=1}^{i-1} c_k \) by the inductive hypothesis. \( \square \)

(b) On the other hand, suppose that \( \tau \land L^j(\tau) \) falsifies \( c_j \). Then, \( L^{j+1} \) has no effect on \( L^{j+1} \), so that \( L^j(\tau) = L^{j+1}(\tau) \). Hence \( \tau \land L^j(\tau) \) falsifies \( F \land \bigwedge_{k=1}^{i-1} c_k \) by the inductive hypothesis.

**Corollary 15.** \( \text{QU}^{\text{NP}}_{\text{Res}} \leq_{\mu} \text{UDL} \) on bounded alternation.

### 4.2 From unified decision lists to \( \text{QU}^{\text{NP}}_{\text{Res}} \)

In this subsection, we show an efficient translation from UDLs back into \( \text{QU}^{\text{NP}}_{\text{Res}} \) refutations. The transformation uses a notion of restriction for UDLs.

**Definition 16 (restriction of a UDL).** Given an assignment \( \alpha \) and a multi-output decision list \( L := (\varepsilon_1, \mu_1), \ldots, (\varepsilon_s, \mu_s) \), the restriction of \( L \) by \( \alpha \) is

\[
L[\alpha] := (\varepsilon_1[\alpha], \mu_1[\alpha]), \ldots, (\varepsilon_s[\alpha], \mu_s[\alpha]).
\]

**The entailment sequence.** We summarise our method as follows: we transform a UDL \( L \) into a sequence of clauses \( \mathcal{E}(L) \). Each clause in the sequence is entailed by the QBF and the universal reduction of the previous clauses in the sequence. The final clause is fully universal, yielding a refutation. We refer to the sequence \( \mathcal{E}(L) \) as the entailment sequence for \( L \).

First, some extra notation and nomenclature. Given a clause \( b \) and a sequence of clauses \( \pi := c_1, \ldots, c_s \), we define

\[
b \otimes \pi := b \lor c_1, \ldots, b \lor c_s.
\]

Given a UDL \( L := (\varepsilon_1, \mu_1), \ldots, (\varepsilon_s, \mu_s) \) for a QBF \( Q \) and block \( Z \) of \( Q \), the \( Z \)-component of \( (\varepsilon_1, \mu_i) \) is \( (\varepsilon_1 \land \mu_i)|_Z \).

Also, we note the following: without loss of generality we can assume that rightmost existential variables (on which no universal variable can depend) do not appear in a UDL. That is, given a QBF with prefix

\[
P := \exists X_1 \forall U_1 \cdots \exists X_d \forall U_d \exists X_{d+1},
\]

the \( X_{d+1} \)-components in any UDL for \( Q \) can be deleted while preserving the computed countermodel. This is an easy consequence of condition (b) in the definition of unified countermodel (Definition 7).

**Definition 17 (entailment sequence).** Given a UDL \( L := (\varepsilon_1, \mu_1), \ldots, (\varepsilon_s, \mu_s) \) for a QBF \( Q \), the entailment sequence \( \mathcal{E}(L) \) is defined recursively on the alternation depth \( d \) of \( Q \).
• if \( d = 1 \), \( \mathcal{E}(L) := \overline{x_1} \lor \overline{p_1}, \ldots, \overline{x_{s}} \lor \overline{p_{s}} \),

• if \( d \geq 2 \), for each \( i \in [s] \) define \( L_i \) as the list obtained from \( L \) by replacing the first \( i - 1 \) existential terms by their \( X_1 \) components, and setting all \( U_1 \) components to \( \mu_i |_{U_1} \). We define \( \mathcal{E}(L) \) as the sequence \( \pi_1, \ldots, \pi_s \), where

\[
\pi_i := (\overline{x_i}|_{X_1} \lor \mu_i |_{U_1}) \otimes \mathcal{E}(L [x_i|_{X_1} \land \mu_i |_{U_1}]).
\]

The size of \( \mathcal{E}(L) \), denoted \(|\mathcal{E}(L)|\), is the number of clauses in the sequence.

The intuition behind the construction of the entailment sequence, in particular when the alternation depth exceeds 1, is not obvious. We will elaborate upon this later. For now, the important property is the fulfilment of the following lemma.

**Lemma 18.** Let \( L \) be a unified decision list for a QBF \( Q := P \cdot F \), and let \( \mathcal{E}(L) = c_1, \ldots, c_r \). Then \( c_r \) is fully universal, and, for each \( i \in [r] \),

\[
F \land \bigwedge_{j=1}^{i-1} \text{red}(c_j) \models c_i.
\]

We defer the proof of this lemma to the end of the subsection. The entailment of each clause by the universal reduction of its predecessors (in conjunction with the matrix \( F \)) gives rise to a straightforward \( QU^{np} \text{-Res} \) refutation.

**Theorem 19.** A UDL \( L \) for a QBF \( Q \) of alternation depth \( d \) can be transformed into a \( QU^{np} \text{-Res} \) refutation \( t(L) \) for \( Q \), where \(|t(L)| \leq O(|L|^d)\). The transformation \( t \) is computable in time \( O(|L|^d) \).

**Proof.** Let \( \mathcal{E}(L) = c_1, \ldots, c_r \). By Lemma 18, the sequence \( \pi \), consisting of the clauses of the matrix of \( Q \) followed by

\[
c_1, \text{red}(c_1), \ldots, c_r, \text{red}(c_r),
\]

is a \( QU^{np} \text{-Res} \) refutation of \( Q \). By a simple induction on alternation depth \( d \), one verifies that \( r \leq s^d \), and that \( \pi \) can be constructed in time \( O(r) \). \( \Box \)

**Corollary 20.** UDL \( \leq_p QU^{np} \text{-Res} \) on bounded alternation.

**Intuition and example.** In the simplest case, with alternation depth \( d = 1 \), the entailment sequence is composed merely of the negations of the combined existential and universal terms in the UDL (i.e. \( \overline{x_1} \land \overline{p_i} \)). The universal reduction of each clause is merely \( \overline{x_1} \), the negation of the corresponding existential term. In this case, the fact that each clause is entailed by the universal reductions of its predecessors in conjunction with the matrix (Lemma 18) follows straightforwardly from the definition of UDL.

This forms the base case for a general argument by induction, when the alternation depth exceeds 1. In the entailment sequence definition, the lists \( L_i \) are defined so that \( L_i [x_i|_{X_1} \land \mu_i |_{U_1}] \) is a UDL for the QBF

\[
\left( P \cdot F \land \bigwedge_{k}^{i-1} \overline{x_k}|_{X_1} \right) [x_i|_{X_1} \land \mu_i |_{U_1}].
\]

Note that each of the negated \( X_1 \)-components \( \overline{x_k}|_{X_1} \) is the universal reduction of a clause already appearing in \( \mathcal{E}(L) \) before \( \pi_i \). This is not obvious; it relies on the fact that the final clause of each \( \mathcal{E}(L_k [x_k|_{X_1} \land \mu_k |_{U_1}]) \) is fully universal.
The addition of these negated $X_1$-components to the matrix is the reason why the first $i-1$ existential terms in $L_i$ are replaced by their $X_1$ components. Assignments satisfying the $i^{th}$ term are guaranteed to falsify one of these clauses. One might suspect that the first $i-1$ lines could be removed altogether, somewhat simplifying the definition of $\mathcal{E}(L)$. Unfortunately, it is not clear that such a construction would produce a UDL for the QBF in (1). The assignments satisfying the removed lines are distributed arbitrarily across the remaining ones, so that the computed function may not satisfy the proper dependencies (condition (b) of Definition 7).

Note that the $U_i$-components in $L_i$ are set uniformly to $\mu_i[U_i]$ merely so that restriction by that assignment deletes them all.

Construction of the entailment sequence, along with the corresponding QU$^\text{NP}$-Res refutation, is illustrated by the following example.

**Example 21.** We will construct an entailment sequence for the QBF

$$\exists x_1 \forall u_1 \exists z_1 \exists x_2 \forall u_2 \exists z_2 \cdot \overline{x_1 u_1 z_1} \land x_1 u_1 z_1 \land \overline{x_2 u_2 z_2} \land x_2 u_2 z_2 \land \overline{z_1 z_2}.$$  

This QBF is $Q^\text{int}_2$, the second instance of the interleaved equality family, which we will meet in the following subsection. We write the blocks of $Q^\text{int}_2$ as follows: $X_1 := \{x_1\}$, $U_1 := \{u_1\}$, $X_2 := \{z_1, x_2\}$, $U_2 := \{u_2\}$, and $X_3 := \{z_2\}$. Note that the alternation depth of $Q^\text{int}_2$ is 2.

Similar to the original equality formulas, a unified countermodel for this QBF sets each $u_i$ equal to the corresponding $x_i$, with the values of the $z_i$ essentially ignored. This countermodel is computed by the following UDL $L$:

$$(x_1 \land x_2, u_1 \land u_2), (x_1 \land \overline{x_2}, u_1 \land \overline{u_2}), (x_2, u_1 \land u_2), (\top, \overline{u_1} \land \overline{u_2}).$$

We now construct the entailment sequence $\mathcal{E}(L)$. First we obtain the lists $L_1, L_2, L_3, L_4$ and their appropriate restrictions. These restrictions are easily transformed (they have alternation depth 1), and pieced together to obtain the complete entailment sequence.

$L_1$ is obtained from $L$ by replacing each $U_1$-component by the $U_1$-component of the first line, namely the term $u_1$. So the restriction of $L_1$ by the $X_1$- and $U_1$-components of the first line, namely the assignment $x_1 \land u_1$, is

$$(x_2, u_2), (\overline{x_2}, \overline{u_2}), (x_2, u_2), (\top, \overline{u_2}).$$

Since the final two lines are redundant, this simplifies to $L_1 [x_1 \land u_1] = (x_2, u_2), (\top, \overline{u_2})$. Hence we have

$$\mathcal{E}(L_1 [x_1 \land u_1]) = \overline{x_2 u_2}, u_2,$$

$$\pi_1 = \overline{x_1 u_1} \otimes \mathcal{E}(L_1 [x_1 \land u_1]) = x_1 u_1 x_2 u_2, x_1 u_1 u_2.$$  

$L_2$ is obtained from $L$ by replacing the first existential term by its $X_1$-component $x_1$, then replacing each $U_1$-component by the $U_1$-component of the second line, namely the term $u_1$:

$$(x_1, u_1 \land u_2), (x_1 \land \overline{x_2}, u_1 \land \overline{u_2}), (x_2, u_1 \land u_2), (\top, u_1 \land \overline{u_2}).$$

Restriction of $L_2$ by the $X_1$- and $U_1$-components of the second line, namely $x_1 \land u_1$, yields

$$(\top, u_2), (\overline{x_2}, \overline{u_2}), (x_2, u_2), (\top, \overline{u_2}).$$

Every line except the first is redundant, so this simplifies to $L_2 [x_1 \land u_1] = (\top, u_2)$. In this case we get

$$\mathcal{E}(L_2 [x_1 \land u_1]) = \overline{u_2},$$

$$\pi_2 = \overline{x_1 u_1} \otimes \mathcal{E}(L_2 [x_1 \land u_1]) = x_1 u_1 u_2.$$  

12
Continuing in this way for $L_3$ and $L_4$, one verifies that

$$L_3 \vdash u_1 = L_4 \vdash u_1 = (x_1, u_2), (x_2, u_2), (\top, u_2),$$

$$\pi_3 = \pi_4 = x_1 u_1 u_2, u_1 x_2 u_2, u_1 u_2.$$  

The fact that $\pi_3 = \pi_4$ is coincidental (note that the $X_1$-components of the third and fourth lines are both empty, and both $U_1$-components are $u_1$).

Piecing together the $\pi_i$, the entailment sequence for $L$ is

$$E(L) = \pi_1, \pi_2, \pi_3, \pi_4 = x_1 u_1 x_2 u_2, x_1 u_1 u_2, x_1 u_1 u_2, u_1 x_2 u_2, u_1 u_2, u_1 u_2.$$  

We can now illustrate how the entailment sequence gives rise to a $Q_n^{\text{Res}}$ refutation. In fact, several clauses in this particular entailment sequence are superfluous and can be ignored, so we work with the subsequence

$$x_1 u_1 x_2 u_2, x_1 u_1 u_2, u_1 x_2 u_2, u_1 u_2.$$  

The essential point is that each each clause in the sequence is entailed by the matrix of $Q_n^{\text{Res}}$ in conjunction with the universal reduction of the preceding clauses. For example, the first clause is entailed by the matrix of $Q_2^{\text{Res}}$ alone; in fact

$$x_1 u_1 z_1 \land x_2 u_2 z_2 \land \pi_1 z_2 \models x_1 u_1 x_2 u_2.$$  

An easy way to verify this is to construct a resolution derivation:

$$\frac{x_1 u_1 z_1 \land x_2 u_2 z_2 \land \pi_1 z_2}{x_1 u_1 x_2 u_2}$$

The second clause in the sequence is entailed by the matrix of $Q_2^{\text{Res}}$ and the universal reduction of the first clause ($x_1 u_1 x_2$):

$$x_1 u_1 z_1 \land x_2 u_2 z_2 \land \pi_1 z_2 \land x_1 u_1 x_2 \models x_1 u_1 u_2.$$  

Again, we can verify this with a resolution derivation:

$$\frac{x_2 u_2 z_2 \land x_1 u_1 x_2}{x_1 u_1 u_2 z_2} \frac{x_1 u_1 x_2}{x_1 u_1 u_2}$$

Similarly the third clause is entailed by the matrix and the universal reductions of the first two clauses (strictly, only the reduction of the second ($\pi_1$) is required)

$$x_1 u_1 z_1 \land x_2 u_2 z_2 \land \pi_1 z_2 \land \pi_1 \models u_1 x_2 u_2,$$

and the pattern continues for the final clause:

$$x_1 u_1 z_1 \land x_2 u_2 z_2 \land \pi_1 z_2 \land u_1 x_2 u_2 \models u_1 u_2.$$  

Resolution derivations verifying these steps can be found easily.

Each individual entailment can be derived immediately using the $\Sigma_1$-rule. As the final clause $u_1 u_2$ is fully universal, its universal reduction is the empty clause, yielding a refutation of $Q_n^{\text{Res}}$. \[\square\]
For each \( k \) which is a QBF of alternation depth \( \varepsilon \), we define a countermodel. Since \( \tau \) and claim that \( \exists \) \( \exists \). Otherwise, since \( \exists \) \( \exists \) assignment falsifying \( \exists \) \( \exists \) \( \exists \).

Proof (of Lemma 18). Let \( L := (\varepsilon, \mu_1), \ldots, (\varepsilon, \mu_s) \), and let \( P := \exists X_1 \forall U_1 \ldots \exists X_d \forall U_d \exists X_{d+1} \).

Without loss of generality, we can assume that the \( X_{d+1} \)-components of \( L \) are all empty, and that the final existential term is \( \top \). We proceed by induction on the alternation depth \( d \) of \( Q \).

Base case \( d = 1 \). In this case \( r = s \), \( c_i = \pi_i \lor \pi_i \), and \( \text{red}(c_i) = \pi \). Let \( \tau \) be a total assignment falsifying \( \pi_i \lor \pi_i \). If the existential part \( \exists \pi \) satisfies \( \bigvee_{k=1}^{i-1} \pi_k \), then it falsifies

\[
\bigwedge_{k=1}^{i-1} \pi_k = \bigwedge_{k=1}^{i-1} \text{red}(c_k).
\]

Otherwise, since \( \exists \pi \) satisfies \( \varepsilon_i \), and the universal part \( \forall \pi \) is equal to \( \mu_i \), \( \tau \) falsifies \( F \) by definition of countermodel. Since \( \varepsilon_s = \top \), \( c_s = \bot \land \pi_s \) is fully universal.

Inductive step \( d \geq 2 \). For each \( j \in [s] \), we put

\[
\alpha_j := \varepsilon_j \bigwedge X_1 \land \mu_j \bigwedge U_1,
\]

and claim that \( L_j [\alpha_j] \) is a unified decision list for

\[
Q_j := P [\alpha_j] \cdot \left( F \land \bigwedge_{k=1}^{j-1} \pi_k \bigwedge X_1 \right) [\alpha_j],
\]

which is a QBF of alternation depth \( d - 1 \). We prove the claim later.

Let \( p \) and \( q \) be natural numbers such that

\[
c_i = \pi_p \bigwedge X_1 \lor \pi_p \bigwedge U_1 \lor b_q
\]

where \( \mathcal{E}(L_p [\alpha_p]) = b_1, \ldots, b_p \). By the inductive hypothesis,

\[
\left( F \land \bigwedge_{k=1}^{p-1} \pi_k \bigwedge X_1 \right) [\alpha_p] \land \bigwedge_{k=1}^{q-1} \text{red}(b_k) \models b_q,
\]

from which it follows that

\[
F \land \bigwedge_{k=1}^{p-1} \pi_k \bigwedge X_1 \land \bigwedge_{k=1}^{q-1} \text{red}(\pi_p \bigwedge X_1 \lor \pi_p \bigwedge U_1 \lor b_k)
\]

(2)

entails \( \pi_p \bigwedge X_1 \lor \pi_p \bigwedge U_1 \lor b_q = c_i \).

We show that each conjunct in (2) besides \( F \) is \( \text{red}(c) \) for some \( c \) appearing in \( \mathcal{E}(L) \) before \( c_i \). For each \( k \in [q-1] \), the clause \( \pi_p \bigwedge X_1 \lor \pi_p \bigwedge U_1 \lor b_k \) appears in \( \mathcal{E}(L) \) before \( c_i \) by definition. For each \( k \in [p-1] \),

\[
\pi_k \bigwedge X_1 = \text{red}(\pi_k \bigwedge X_1 \lor \pi_k \bigwedge U_1 \lor f_k)
\]

14
where $f_k$ is the final clause of $\mathcal{E}(L_k[\alpha_k])$, which is fully universal by the inductive hypothesis, and the clause $\overline{e_k} |_{X_1} \lor \overline{e_k} |_{U_1} \lor f_k$ appears in $L$ before $c_i$.

Since $\varepsilon_s = \top$, $c_r = \bot \lor \overline{r_s} |_{U_1} \lor f_s$ is fully universal. This completes the inductive step.

**Proof of claim.** Fixing $j \in [s]$, we show that $L_j[\alpha_j]$ computes a unified countermodel for $Q_j$ by checking both conditions in Definition 7.

(a) Let $\tau \in \langle \text{vars}(Q_j) \rangle$, and let

$$\sigma := \varepsilon_j \land \tau |_{\text{vars}(\tau) \setminus \text{vars}(\varepsilon_j)}.$$

If $\tau$ falsifies $\bigwedge_{k=1}^{j-1} \overline{e_k} |_{X_1}[\alpha_j]$, then $\tau \land L_j[\alpha_j](\tau)$ already falsifies the matrix of $Q_j$, so we assume otherwise. Then $L(\sigma) = \mu_j$, and since $\varepsilon_j |_{X_1} \land \tau$ agrees with $\sigma$ on $X_1$, $L(\varepsilon_j |_{X_1} \land \tau)$ agrees with $\mu_j$ on $U_1$. It follows that

$$L(\varepsilon_j |_{X_1} \land \tau) = \mu_j |_{U_1} \land L_j[\alpha_j](\tau),$$

whereby $\alpha_j \land \tau \land L_j[\alpha_j](\tau)$ falsifies $F$, by definition of countermodel. Hence $\tau \land L_j[\alpha_j](\tau)$ falsifies $F[\alpha_j]$, and therefore falsifies the matrix of $Q_j$.

(b) Let $\tau, \rho \in \langle \text{vars}(Q_j) \rangle$, and suppose that $\tau$ and $\rho$ agree on the first $r$ existential blocks of $Q_j$ for some $r \in [d-1]$. Since $\tau$ and $\rho$ agree on $X_1$ in particular, if either of them satisfies $\bigwedge_{k=1}^{r-1} \overline{e_k} |_{X_1}[\alpha_j]$, then we have $L_j[\alpha_j](\tau) = L_j[\alpha_j](\rho)$ satisfying the condition trivially, so we assume otherwise. Notice that $L_j[\alpha_j](\tau)$ is $L(\varepsilon_j |_{X_1} \land \tau)$ with the $U_1$-component removed, and likewise for $\rho$. Since $\varepsilon_j |_{X_1} \land \tau$ and $\varepsilon_j |_{X_1} \land \rho$ agree on the first $r + 1$ existential blocks of $Q$, $L(\varepsilon_j |_{X_1} \land \tau)$ and $L(\varepsilon_j |_{X_1} \land \rho)$ agree on the first $r + 1$ universal blocks of $Q$, thus $L_j[\alpha_j](\tau)$ and $L_j[\alpha_j](\rho)$ agree on the first $r$ universal blocks of $Q_j$. \qed

### 4.3 Unbounded alternation

Theorem 11 does not extend to QBFs in general; UDLs prove to be too weak for QBFs of unbounded alternation depth. To show this, we consider a version of the equality formulas with an unbounded, ‘interleaved’ prefix.

**Definition 22 (interleaved equality).** The $n^\text{th}$ interleaved equality formula $Q^{\text{int}}_n$ is obtained from $Q^n_0$ by replacing the prefix with $\exists x_1 \forall u_1 \exists z_1 \cdots \exists x_n \forall u_n \exists z_n$.

Recall that the countermodel range for the original equality formulas is the complete set of universal assignments. In fact, this remains true under the interleaved prefix.

**Proposition 23.** If $f$ is a unified countermodel for $Q^{\text{int}}_n$, then $\text{rng}(f) = \langle \{u_1, \ldots, u_n\} \rangle$.

**Proof.** For each $i \in [n]$, let $D_i$ denote the existential variables appearing before $u_i$ in the prefix of $Q^{\text{int}}_n$. We show that the range of any countermodel for $Q^{\text{int}}_n$ is $\langle \{u_1, \ldots, u_n\} \rangle$, and the proposition follows.

Let $f$ be a countermodel for $Q^{\text{int}}_n$, and let $\mu$ be an arbitrary total assignment to the universal variables. We prove that $\mu = f(\varepsilon)$, where

$$
\varepsilon(x_i) := \begin{cases} 0 & \text{if } \mu(u_i) = 0, \\
1 & \text{if } \mu(u_i) = 1, \end{cases} \quad \text{for } i \in [n],$$

$$\varepsilon(z_i) := 1, \quad \text{for } i \in [n].$$
Aiming for contradiction, let \( j \) be the least natural number for which \( f(\varepsilon)\{\{u_j\}\} \neq \mu\{\{u_j\}\} \).

The matrix of \( Q_n^{\text{INT}}[\varepsilon|_{D_j}] \) is

\[
a z_j \land z_j' \land z_{j+1} \land \cdots \land z_n
\]

where \( a \) is the literal represented by the assignment \( f(\varepsilon)|_{\{u_j\}} \). This matrix is satisfied by the assignment 

\[
f(\varepsilon)|_{\{u_j\}} \land z_j \land z_{j+1} \land \cdots \land z_n.
\]

Now, let \( \delta \) be any total existential assignment that extends 

\[
\varepsilon|_{D_j} \land z_j \land z_{j+1} \land \cdots \land z_n.
\]

Since \( \varepsilon \) and \( \delta \) agree on \( D_j \), the assignments \( f(\varepsilon)|_{\{u_j\}} \) and \( f(\delta)|_{\{u_j\}} \) are identical. It follows that the assignment \( \delta \cup f(\delta) \) satisfies the matrix of \( Q_n^{\text{INT}} \), contradicting the fact that \( f \) is a countermodel for \( Q_n^{\text{INT}} \).

As a consequence, the interleaved equality family requires UDLs of exponential size. However, they also admit short QU-Res refutations. As shown in Figure 1, \( Q_n^{\text{INT}} \) can be reduced to \( Q_n^{\text{INT}-1} \) in a constant-size derivation.

**Proposition 24.** The interleaved equality formulas admit linear-size QU-Res refutations.

Thus distributed decision lists are unsuitable for characterising QU-\( \text{NP} \)-Res refutation size when the alternation depth is unbounded.

**Corollary 25.** \( \text{QU-\text{NP} Res} \not\preccurlyeq \p \text{UDL} \) on unbounded alternation.

### 4.4 Characterisation of hardness for QU-Res

If we consider only families of bounded alternation QBFs, given the equivalence between UDLs and the oracle system QU-\( \text{NP} \)-Res (Theorem 11), there can be only two reasons for hardness in the classical system QU-Res: either

(a) the family requires large UDLs, or

(b) the family harbours propositional resolution hardness.

The main question here is regarding case (b), and what it really means for a QBF family to ‘harbour’ propositional hardness. In fact, we can give a precise answer: for every family of small UDLs, some steps in the entailment sequences are hard for resolution. This gives rise to a hard sequence of unsatisfiable CNFs for each small family of UDLs.

The result, stated in the following theorem, is a complete characterisation of QU-Res hardness (on bounded alternation), analogous to the hardness characterisations for Frege+\( \forall \text{red} \) and EF+\( \forall \text{red} \) from [14].
Theorem 26. Given a bounded-alternation QBF family \( \{ P_n \cdot F_n \}_{n \in \mathbb{N}} \) requiring superpolynomial-size QU-Res refutations, either

(a) \( \{ P \cdot F \}_{n \in \mathbb{N}} \) requires superpolynomial-size UDLs, or

(b) for each family of polynomial-size UDLs \( \{ L_n \}_{n \in \mathbb{N}} \) for \( P_n \cdot F_n \) with entailment sequences

\[ \mathcal{E}(L_n) = c^n_1, \ldots, c^n_{r_n}, \]

there exist natural numbers \( i_n \in [r_n] \) such that the CNF family

\[ \left\{ \left( F_n \land \bigwedge_{k=1}^{i_n-1} \text{red}(c^n_k) \right) [c^n_{i_n}] \right\}_{n \in \mathbb{N}} \]

requires superpolynomial-size resolution refutations.

Proof. For \( n \in \mathbb{N} \) and \( i_n \in [r_n] \), we put

\[ \phi_{i_n} := \left( F_n \land \bigwedge_{k=1}^{i_n-1} \text{red}(c^n_k) \right) [c^n_{i_n}] . \]

Note that \( \phi_{i_n} \) is unsatisfiable by Lemma 18.

Suppose now that neither condition (a) nor condition (b) holds. Then there exists some polynomial-size family of UDLs \( \{ L_n \}_{n \in \mathbb{N}} \) with \( \mathcal{E}(L_n) = c^n_1, \ldots, c^n_{r_n} \), such that for all \( i_n \in [r_n] \) the CNFs \( \phi_{i_n} \) have polynomial-size resolution refutations. Let \( p(n) \) be a polynomial bound for the size of \( L_n \), let \( q(n) \) be a polynomial bound for the size of the refutations of \( \phi_{i_n} \), and let \( i_n \in [r_n] \).

By assumption, the alternation depth of each \( P_n \cdot F_n \) is bounded above by a constant \( d \). A simple induction shows that \( |\mathcal{E}(L_n)| \leq p(n)^d \). Given an arbitrary CNF \( G \) and clause \( b \), it is easy to see that a resolution refutation \( \pi \) of \( G \) \( [b] \) can be transformed into a resolution derivation of \( b \) from \( G \) of size \( |\pi| + 1 \) (it may be necessary to add a weakening step). Hence, there exist derivations of \( c^n_{i_n} \) from \( F_n \land \bigwedge_{k=1}^{i_n-1} \text{red}(c^n_k) \) of size \( q' = q(n) + 1 \).

Now, beginning with the axiom clauses \( F_n \), and successively deriving and reducing the clauses in \( \mathcal{E}(L_n) \), we obtain QU-Res refutations of \( P_n \cdot F_n \) of size \( O(|P_n \cdot F_n| + p(n)^d \cdot q'(n)) \). Hence \( P_n \cdot F_n \) has polynomial-size QU-Res refutations. \( \square \)

4.5 Unification of lower-bound techniques

The two main existing lower-bound techniques for resolution-based QBF proof systems are strategy extraction [7,6] and size-cost-capacity [5]. As far as proof-size lower bounds for bounded-alternation QBFs are concerned, our hardness characterisation (Theorem 26) encompasses both.

Indeed, the exact lower bounds for all known bounded-alternation hardness results (all of which have alternation depth 1) can be shown as the result of a UDL lower bound. For QBFs with a single universal block, we have the following immediate corollary to Theorems 14 and 19.

Corollary 27. Let \( \{ Q_n \}_{n \in \mathbb{N}} \) be a QBF family of alternation depth 1. Then the following are equivalent statements:

- \( \{ Q_n \}_{n \in \mathbb{N}} \) admits UDLs of size \( O(s(n)) \);
- \( \{ Q_n \}_{n \in \mathbb{N}} \) admits QU-Res refutations of size \( O(s(n)) \).

Lower bounds by strategy extraction. In [6,7], a general method was exhibited for forming a QBF \( Q_f \) whose unique countermodel is a given Boolean function \( f \). Proof-size lower bounds
were shown via strategy extraction, instantiating the function \( f \) by \textsc{Parity} \cite[Thm. 14]{7}, \textsc{Majority} \cite[Cor. 5.7]{6} and \textsc{Sipser} \cite[Cor. 5.12]{6}, and importing known hardness results for these functions from circuit complexity \cite{27,40,44}. In all three cases, the resulting QBF family has a single universal variable, and the imported circuit lower bound holds also for UDLs. As such, all three lower bounds for \( \text{QU}^\text{NP}_{-\text{Res}} \) follow from Corollary 27.

**Lower bounds by size-cost-capacity.** A largely orthogonal technique was proposed in \cite{5}. Here it was shown that the so-called \textit{cost} of a QBF is an absolute lower bound on its \( \text{QU}^\text{NP}_{-\text{Res}} \) refutation size.

In fact, for alternation depth 1, the cost of a QBF is equal to the minimal cardinality of countermodel range, which in turn is a trivial lower bound on UDL size. As such, the lower bounds for equality \cite[Thm. 3.5]{5} and random QBFs \cite[Thm. 7.9]{5}, both of which have alternation depth 1, follow from Corollary 27 once the exponential countermodel-range lower bound is established.

### 5 Equivalence of \textsc{QU-Res} and \textsc{Q-Res} on bounded alternation

The natural follow-up question, prompted by our work in Section 4, is whether our results also hold for \textsc{Q-Resolution} (\textsc{QU-Res} without universal pivots). In particular, does the UDL characterisation (Theorem 11) continue to hold? In this section, we show that the answer is yes. An immediate corollary is that \( \text{Q}^\text{NP}_{-\text{Res}} \) and \( \text{QU}^\text{NP}_{-\text{Res}} \) are p-equivalent on bounded-alternation QBFs.

Perhaps the most obvious approach would be to show that our transformations between \( \text{QU}^\text{NP}_{-\text{Res}} \) and UDL go through without resolution on universal pivots. However, we choose another approach. We show directly that \( \text{Q}^\text{NP}_{-\text{Res}} \) is equivalent to \( \text{QU}^\text{NP}_{-\text{Res}} \), and therefore to UDL. This approach throws up a further interesting result, namely that the classical systems \textsc{Q-Res} and \textsc{QU-Res} are also p-equivalent on bounded alternation.

**Definitions of \textsc{Q-Res} and \textsc{Q}^\text{NP}_{-\text{Res}}.** \textsc{Q-Res} is identical to \textsc{QU-Res}, except that resolution pivots must be existential variables.

**Definition 28 (\textsc{Q-Res} \cite{30}).** A \textsc{Q-Res} derivation from a QBF \( P \cdot F \) is a sequence of clauses \( \pi := c_1, \ldots, c_s \) in which each \( c_i \) is derived by one of the following rules:

- **Axiom:** \( c_i \) is a clause in the matrix \( F \);
- **\exists\text{-Resolution:**} \( c_i = a \lor b \), where \( c_r = a \lor x \) and \( c_s = b \lor \overline{x} \) for some \( r, s < i \) and some existential variable \( x \).
- **Weakening:** \( c_i = c_r \lor b \) for some \( r < i \) and clause \( b \).
- **Universal reduction:** \( c_i = c_r[\mu] \) for some \( r < i \) and some universal assignment \( \mu \) with \( \text{vars}_2(c_r) <_P \text{vars}(\mu) \).

The size of \( \pi \) is \( |\pi| = s \), and \( \pi \) is a refutation when \( c_s = \bot \).

For the oracle version of \textsc{Q-Res}, we want to specify a rule which allows a propositional derivation to be collapsed into a single inference. This is complicated by the fact that \textsc{Q-Res} is not propositionally implicationally complete; that is, from \( F \models c \) it does not follow that \( c \) can be derived from \( F \) using the axiom, \( \exists\text{-resolution} \) and weakening rules. As such we do not reuse the \( \Sigma_1 \)-rule from \textsc{QU}^\text{NP}_{-\text{Res}}, but rather define a new version capturing the insistence on existential pivots.

---

4 This is actually shown in the proof of Theorem 14. The cost of \( Q \) is equal to the maximum, over the individual lists \( L_i \), of the minimal list size (cf. \cite{5}).
Definition 29 (Q⁻Res). Q⁻Res is defined as Q-Res, except that the resolution and weakening rules are replaced by the following rule:

- \( \Sigma^2 \)-rule: For some \( G \subseteq \{ c_1, \ldots, c_{i-1} \} \),
  (a) \( \bigwedge_{b \in G} b^2 \vdash c^3 \), and
  (b) for each \( b \in G \), \( b^2 \) is a subclause of \( c_i^2 \),

where \( c^3 \) and \( c_i^2 \) denote the existential and universal subclauses of any clause \( c \).

Equivalences on bounded alternation depth. Both of the p-equivalences that we want to show can be proved constructively, and the essential observation is the following: all of the universal resolutions from a single block can be removed from a QU-Res refutation in quadratic time.

It is also important that the number of universal reduction steps grows only quadratically during the transformation. We denote the number of universal reduction steps in a refutation \( \pi \) by \( |\pi|_U \).

Lemma 30. Let \( \pi \) be a QU-Res refutation of a QBF \( Q \) of alternation depth \( d \). For each \( i \in [d] \), \( \pi \) can be transformed into a refutation \( t(\pi) \) of \( Q \) with \( |t(\pi)| = O(|\pi|^2) \) and \( |t(\pi)|_U = O(|\pi|^2) \) in which there are no resolutions on the \( i \)th universal block. The transformation is computable in time \( O(|\pi|^2) \).

Proof. Let \( c_1, \ldots, c_d \) be a QU-Res refutation of a QBF \( \exists X_1 \forall U_1 \cdots \exists X_d \forall U_d \exists X_{d+1} \cdot F \), and let \( i \in [d] \). We describe the transformation \( t \) recursively on the number \( r \) of \( U_i \) reductions in \( \pi \).

If \( r = 0 \), we obtain \( t(\pi) \) from \( \pi \) by removing all \( U_i \) resolutions in the following way: we delete all clauses containing a positive \( U_i \) literal, and add the empty clause at the end of the refutation. The negative \( U_i \) literals, which are no longer resolved away, accumulate through the refutation, and are removed at the conclusion by the addition of a single universal reduction step (hence the addition of the empty clause).

If \( r \geq 1 \), we find the first \( U_i \) reduction step \( c_j \) appearing in \( \pi \), and consider its subderivation \( \pi_j \). Suppose that the antecedent of \( c_j \) is \( c_j \lor R \). Now we remove all \( U_i \) resolutions from \( \pi_j \), obtaining a new sequence \( \pi'_j \), as follows: for each \( U_i \) literal in \( R \), we remove all clauses containing the complementary literal; for each variable in \( U_i \) not appearing in \( R \), we remove all clauses containing the positive literal. Once again, all \( U_i \) literals that are no longer resolved away accumulate through the derivation, and are universally reduced at the conclusion. Then we define \( t(\pi) := \pi'_j, t(\pi') \), where \( \pi' \) is identical to \( \pi \), except that \( c_j \) is introduced as an axiom, rather than derived by universal reduction.

It is clear that \( |t(\pi)| = O(|\pi|^2) \) and \( |t(\pi)|_U = O(|\pi|^2) \), and that \( t \) can be computed in time \( O(|\pi|^2) \). It remains to prove that \( t(\pi) \) is a valid QU-Res refutation of \( Q \) with no \( U_i \) resolutions. We do this by induction on \( r \).

The base case \( r = 0 \) is clear. For the inductive step \( r \geq 1 \), it is clear that \( \pi'_j \) is a valid QU-Res derivation of \( c_j \) with no \( U_i \) resolutions. Since \( \pi'_j \) is a QU-Res refutation of \( P \cdot F \land c_j \) with \( r-1 \) \( U_i \) reductions, \( t(\pi') \) is a valid QU-Res refutation of \( P \cdot F \land c_j \) with no \( U_i \) resolutions, by the inductive hypothesis. The inductive step follows, as \( c_j \) is the conclusion of \( \pi'_j \). \( \square \)

Now we show the p-equivalence of the classical systems, which is an easy consequence of Lemma 30.

Theorem 31. Q-Res \( \equiv_p \) QU-Res on bounded alternation.

Proof. Since QU-Res trivially p-simulates Q-Res, we need only show the reverse simulation. By repeated application of Lemma 30 QU-Res refutations \( \pi \) of QBFs of alternation depth \( d \) can be transformed into Q-Res refutations of size \( O(|\pi'|^2) \) in time \( O(|\pi|^2) \). Hence Q-Res p-simulates QU-Res when \( d \) is bounded above by a constant. \( \square \)
Next, we show the p-equivalence of the oracle systems.

**Theorem 32.** $Q^{NP}_{Res} \equiv_p QU^{NP}_{Res}$ on bounded alternation.

*Proof.* $QU^{NP}_{Res}$ trivially p-simulates $Q^{NP}_{Res}$, so we need only show the reverse simulation. Let $\pi$ be a $QU^{NP}_{Res}$ refutation of a QBF $Q$ of alternation depth $d$. We transform $\pi$ into a $Q^{NP}_{Res}$ refutation $t(\pi)$ of size $O(|\pi|^{2^d})$.

Since resolution is implicationally complete, whenever the $\Sigma_1$-rule is applied, the consequent can be derived by resolution from the antecedents. Hence we can obtain a $QU_{Res}$ refutation $\pi_0$ from $\pi$ by replacing each entailment step with a resolution derivation. Moreover, $|\pi_0|_\forall = |\pi|_\forall$.

Next we remove the universal resolution steps from $\pi_0$ by applying Lemma 30 for each $i \in [d]$. We obtain a $Q_{Res}$ refutation $\pi_1$ with $|\pi_1|_\forall = O(|\pi|^{2^d})$.

Finally, we transform $\pi_1$ into a $Q^{NP}_{Res}$ refutation $t(\pi)$ as follows. Call a clause in $\pi_1$ *surplus* if it is neither an axiom, nor the conclusion, nor the antecedent of a reduction step. We obtain $t(\pi)$ from $\pi_1$ by deleting all surplus clauses.

To see that $t(\pi)$ is indeed a $QU^{NP}_{Res}$ refutation, observe that the removal of surplus clauses from the antecedents preserves $\exists$-entailment steps (realised by the $\Sigma^3_1$-rule), since surplus clauses are already $\exists$-entailed by the preceding clauses. As $t(\pi)$ contains only axioms, reduction steps, and antecedents of reduction steps, its size is at most

$$|Q| + 2(|\pi_1|_\forall) = |Q| + O(|\pi|^{2^d}).$$

Assuming without loss of generality that $|Q| \leq |\pi|$, we have $|t(\pi)| = O(|\pi|^{2^d})$. \hfill $\square$

As a corollary of Theorems 11 and 32, UDLs characterise $Q^{NP}_{Res}$ refutation size on bounded QBFs.

**Corollary 33.** $Q^{NP}_{Res} \equiv_p UDL$ on bounded alternation.

**Unbounded alternation depth.** The equivalences in Theorems 31 and 32 cannot be extended to QBFs in general. The former case is ruled out by the fact that $Q_{Res}$ does not simulate $QU_{Res}$ [24], the separation being shown by the QBFs $\{KBKF_n\}_{n \in \mathbb{N}}$ introduced by Kleine Büning, Karpinski and Flögel [30], which have unbounded alternation depth. Indeed, Theorem 31 shows that any such constructive separation must be due to a QBF family with unbounded alternation.

The latter case is ruled out by the same QBFs. It is clear that the exponential $Q_{Res}$ lower bound for KBKF$_n$ [30] is due to exponentially many universal reduction steps (see the proof by size-cost in [5]), giving rise to an exponential lower bound for $Q^{NP}_{Res}$. The existence of short (i.e. polynomial-size) $QU^{NP}_{Res}$ refutations follows from the existence of short $QU_{Res}$ refutations. So $Q^{NP}_{Res}$ does not simulate $QU^{NP}_{Res}$ on unbounded alternation.

6 Size-width for QBF resolution

The seminal paper of Ben-Sasson and Wigderson [3] introduced the celebrated size-width relations, equations which show that short resolution refutations must also be narrow. This powerful technique allows resolution size lower bounds to be obtained via width lower bounds, the point being that width lower bounds are often much easier to show.
Let us first recall the size-width relation for (general) resolution. The width of a clause is the number of literals it contains, and the width of a resolution refutation is the maximal width of a clause in the sequence. The initial width of a CNF is the maximal width amongst its clauses.

**Theorem 34 (3).** Let $F$ be a CNF with $n$ variables, let $w(F)$ denote the initial width of $F$, and let $s(F \vdash \bot)$ and $w(F \vdash \bot)$ denote the minimal size and minimal width of a resolution refutation of $F$. Then

$$s(F \vdash \bot) = \exp \left( \Omega \left( \frac{(w(F \vdash \bot) - w(F))^2}{n} \right) \right).$$

Size-width is arguably the main lower-bound technique for resolution, and its applicability to QBFs has already been investigated [10,20]. Unfortunately, only negative results were obtained, ruling out the exact relations of Ben-Sasson and Wigderson for various width measures.

In this section, we use the connection to UDLs to show the first positive results, and we apply our new size-width relation to reprove some superpolynomial lower bounds.

### 6.1 A size-width relation for $\text{QU}^{\text{NP}}\text{-Res}$

Previous work [10] considered two natural width measures for QBF refutations:

(a) the standard notion of width, i.e. the maximal number of literals appearing in a single clause;

(b) existential width, i.e. the maximal number of existential literals appearing in a single clause.

We argue that the correct measure of width for a $\text{QU}^{\text{NP}}\text{-Res}$ refutation is existential width with the axiom clauses not considered. Thus, we define the existential width of a $\text{QU}^{\text{NP}}\text{-Res}$ refutation as the maximal number of existential literals appearing in a non-axiom clause.

With this definition of existential width, the following size-width relation holds.

**Theorem 35.** Let $Q$ be a QBF of alternation depth $d$ with $n$ existential variables, and let $s(F \vdash \bot)$ and $w_\exists(F \vdash \bot)$ denote the minimal size and minimal existential width of a $\text{QU}^{\text{NP}}\text{-Res}$ refutation of $Q$. Then

$$s(F \vdash \bot) = \exp \left( \Omega \left( \frac{(w_\exists(Q \vdash \bot))^2}{d^3 n \log n} \right) \right).$$

Before we proceed to prove Theorem 35, a couple of remarks are in order, by way of comparison with the original relation of Ben-Sasson and Wigderson [3].

The first notable difference is the absence of an initial width term. This is essentially a by-product of ignoring the width of axiom clauses. Moreover, it actually turns out to be quite convenient, as we avoid the need for Tseitin transformations (cf. [3,10]).

The second obvious difference is in the denominator of the exponent. Here we inherit an extra $\log n$ factor (from the transformation of Bshouty [17] which we come to shortly) and a factor of $d^3$, related to alternation depth. Hence our relation works best when the alternation depth is bounded.

---

5 There is a separate relation for tree-like resolution [3].

6 With this definition, the width of an axiom clause $c$ implicitly enters the calculation of the width of a proof in case there is a universal reduction step performed on $c$. 

21
Proof of the QBF size-width relation. We prove Theorem 35 via a transformation from QU^NP-Res to UDL and back. A central step in the transformation is based on the following Lemma of Bshouty [17]. It states a size-width relation for (single-output) term decision list. Here, the width of a decision list is the maximal width of a term in the list.

Lemma 36 ([17]). Let \( f : \langle Z \rangle \rightarrow \{0, 1\} \) be a function, where \( Z \) is a set of \( n \) Boolean variables. If \( f \) is computed by a decision list of size \( s \), then it is also computed by a decision list of width \( O(\sqrt{n \log n \log s}) \).

However, UDLs are multi-output term decision lists, so we need to generalise this result for multiple outputs. This is actually quite straightforward. The proof in [17] is based on manipulating the terms in the list, using a hybrid of decision trees and decision lists, and a result of Blum [16]. However, the argument does not depend anywhere on the codomain of the computed function, and therefore goes through even for multi-output term decision lists.

Thus, we obtain a corresponding result for UDLs. We define the existential width of a UDL as the maximal width of an existential term in the list.

Lemma 37. Let \( f \) be a unified countermodel for a QBF \( Q \) with \( n \) existential variables. If \( f \) is computed by a UDL of size \( s \), then it is also computed by a UDL of existential width \( O(\sqrt{n \log n \log s}) \).

We may now prove Theorem 35.

Proof. Let \( Q \) be a QBF of alternation depth \( d \) with \( n \) existential variables, and let \( \pi \) be a shortest QU^NP-Res refutation of \( Q \), i.e. \( s(Q \vdash \bot) = |\pi| \). By Theorem 14, \( \pi \) can be transformed into a UDL \( L \) of size at most \( |\pi|^d \). By Lemma 37, \( L \) can be transformed into a UDL \( M \) of existential width

\[
w_\exists(M) = O\left(\sqrt{n \log n \log (|\pi|^d)}\right) = O\left(\sqrt{dn \log n \log |\pi|}\right).
\]

Now, for any UDL, it is clear by construction that the existential width of each clause in the entailment sequence is at most the existential width of the UDL, multiplied by the alternation depth. It follows that the QU^NP-Res refutation \( \rho \) of \( Q \) based on \( E(M) \) (i.e. \( t(M) \)) as described in the proof of Theorem 19 has existential width at most \( d \cdot w_\exists(M) \).

Therefore

\[
w_\exists(Q \vdash \bot) = O\left(d \cdot \sqrt{dn \log n \log |\pi|}\right),
\]

and solving for \( |\pi| \) yields the theorem statement.

\( \Box \)

6.2 QU^NP-Res lower bounds by size-width

We illustrate the application of the QBF size-width relation by reproving three superpolynomial QU-Res lower bounds from the literature.[7]

A useful feature of our translation via UDLs is that UDL width lower bounds imply QU^NP-Res width lower bounds. Indeed, it is readily verified that the translation in Theorem 19 (from UDL to QU^NP-Res) preserves existential width when the alternation depth is 1.

Proposition 38. A UDL for a QBF \( Q \) of alternation depth 1 can be transformed into a QU^NP-Res refutation of \( Q \) with no increase in existential width.

[7] Note that we do not obtain the optimal lower bounds.
In the forthcoming examples, linear lower bounds on the existential width of UDLs can be shown with relative ease, whereby application of Proposition 38 and Theorem 35 yields a size lower bound of \( \exp(O(n/\log n)) \). This is in contrast to the application of size-width relations for propositional resolution, where showing width lower bounds still entails quite some work (cf. [3]).

**The equality family.** We first show that UDLs for the equality formulas require linear existential width.

**Theorem 39.** Any UDL for \( Q_{n}^{\text{EQ}} \) has existential width \( n \).

**Proof.** Let \( L := (\varepsilon_1, \mu_1), \ldots, (\varepsilon_n, \mu_n) \) be a UDL for \( Q_{n}^{\text{EQ}} \), and note that \( L \) computes the unique countermodel

\[
f_{\text{EQ}} : \langle(x_1, \ldots, x_n) \rangle \rightarrow \langle \{u_1, \ldots, u_n\} \rangle
\]

\[
\tau \mapsto f(\tau),
\]

where \( f_{\text{EQ}}(\tau)(u_i) = \tau(x_i) \) for each \( i \in [n] \). Note that the countermodel \( f \) amounts to setting each \( u_i = x_i \).

Aiming for contradiction, suppose that \( L \) has existential width \( w < n \). In particular, \( \varepsilon_1 \) is a term of width less than \( n \), so there exists some variable \( x_i \) that does not appear in \( \varepsilon_1 \). It follows that there exist two assignments \( \tau, \rho \in \langle \{x_1, \ldots, x_n\} \rangle \), both of which satisfy \( \varepsilon_1 \), with \( \tau(x_i) \neq \rho(x_i) \). We deduce that \( f_{\text{EQ}}(\tau) = f_{\text{EQ}}(\rho) \), but also that \( \tau(x_i) \neq \rho(x_i) \), in contradiction with the definition of \( f_{\text{EQ}} \). \( \square \)

**The parity family.** Arguing along the same lines, we obtain a linear lower bound on the existential width of UDLs for the parity formulas.

**Definition 40 (parity [7]).** The \( n^{\text{th}} \) parity formula is

\[
Q_{n}^{\text{PAR}} := \exists x_1 \cdots x_n \forall u \exists z_1 \cdots z_n \cdot (x_1 \lor \neg z_1) \land (\ldots \land (x_n \lor \neg z_n) \land \bigwedge_{i=1}^{n-1} \oplus(x_{i+1}, z_i, z_{i+1})
\]

where \( \oplus(x_{i+1}, z_i, z_{i+1}) \) consists of the four clauses

\[
(x_{i+1} \lor z_i \lor \neg z_{i+1}) \land (\neg x_{i+1} \lor \neg z_i \lor \neg z_{i+1}) \land
\]

\[
(x_{i+1} \lor \neg z_i \lor z_{i+1}) \land (\neg x_{i+1} \lor z_i \lor \neg z_{i+1})
\]

**Theorem 41.** Any UDL for \( Q_{n}^{\text{PAR}} \) has existential width \( n \).

**Proof.** Let \( L := (\varepsilon_1, \mu_1), \ldots, (\varepsilon_n, \mu_n) \) be a UDL for \( Q_{n}^{\text{PAR}} \), and note that \( L \) computes the unique countermodel

\[
f_{\text{PAR}} : \langle(x_1, \ldots, x_n) \rangle \rightarrow \langle \{u\} \rangle
\]

\[
\tau \mapsto \langle u \mapsto (\Sigma_{i=1}^{n} \tau(x_i)) \mod 2 \rangle,
\]

which amounts to \( u = \oplus(x_1, \ldots, x_n) \).

Similarly as for equality, if the width of \( \varepsilon_1 \) is strictly less than \( n \), then there exist two assignments \( \tau, \rho \in \langle \{x_1, \ldots, x_n\} \rangle \), both of which satisfy \( \varepsilon_1 \), and which disagree only at some variable \( x_i \). It follows that \( f_{\text{PAR}}(\tau) = f_{\text{PAR}}(\rho) \), and also that

\[
(\Sigma_{i=1}^{n} \tau(x_i)) \mod 2 = (\Sigma_{i=1}^{n} \rho(x_i)) \mod 2,
\]

contradicting the definition of the function \( f_{\text{PAR}} \). \( \square \)
The majority family. The majority function $\text{MAJ}$ is defined as

\[
\text{MAJ}(x_1, \ldots, x_n) = \left\lceil \frac{1}{2} + \frac{\sum_{i=1}^{n} x_i}{n} \right\rceil.
\]

For each $n \in \mathbb{N}$, let $Q_n^{\text{MAJ}} := \exists x_1 \cdots x_n \forall \exists z_1 \cdots z_m \cdot F_n$ denote a polynomial-size QBF whose unique countermodel $f_{\text{MAJ}}$ amounts to $u = \text{MAJ}(x_1, \ldots, x_n)$; that is,

\[
f_{\text{MAJ}} : \langle (x_1, \ldots, x_n) \rangle \rightarrow \langle \{u\} \rangle
\]

\[
\tau \mapsto (u \mapsto \text{MAJ}(\tau(x_1), \ldots, \tau(x_n))).
\]

(For the explicit construction of such formulas, see [6].) We can show straightforwardly that UDLs for $\{Q_n^{\text{MAJ}}\}_{n \in \mathbb{N}}$ also require linear existential width.

**Theorem 42.** A UDL for $Q_n^{\text{MAJ}}$ has existential width $\Omega(n)$.

**Proof.** Let $L := (\varepsilon_1, \mu_1), \ldots, (\varepsilon_n, \mu_n)$ be a UDL for $Q_n^{\text{MAJ}}$. If the width of $\varepsilon_1$ is strictly less than $n/2$, then there exist two assignments $\tau, \rho \in \{\langle x_1, \ldots, x_n \rangle\}$, both of which satisfy $\varepsilon_1$, such that

\[
\text{MAJ}(\tau(x_1), \ldots, \tau(x_n)) \neq \text{MAJ}(\rho(x_1), \ldots, \rho(x_n)).
\]

We reach a contradiction, since $L(\tau) = L(\rho)$, implying that $L$ does not compute the unique countermodel $f_{\text{MAJ}}$. \qed

**Application.** Application of Proposition 38 and Theorem 35 gives the following refutation size lower bounds.

**Corollary 43.** $\{Q_n^{\exists \text{Q}}\}_{n \in \mathbb{N}}, \{Q_n^{\text{Par}}\}_{n \in \mathbb{N}},$ and $\{Q_n^{\text{MAJ}}\}_{n \in \mathbb{N}}$ require $\text{QU}^{-\text{Res}}$ refutations of size $\exp(\Omega(n / \log n))$.

We note that, in contrast to the original hardness proofs for the parity and majority families [8,6], we obtained Corollary 43 without importing any lower bounds from circuit complexity.

### 6.3 Relation to previous work

As it was shown in [10,20] that the propositional size-width relations (Theorem 34) do not lift to $\text{Q-Res}$ or $\text{QU-Res}$, it is worthwhile taking a moment to see how those results are consistent with our size-width relation (Theorem 35).

The authors of [10,20] showed that the ‘existential-width analogue’ of the propositional size-width relation, namely

\[
s(Q \vdash \bot) = \exp \left( \Omega \left( \frac{(w_\exists(Q \vdash \bot) - w_\exists(Q))^2}{n} \right) \right),
\]

does not hold in $\text{Q-Res}$ or $\text{QU-Res}$. In particular, there exist QBFs $\{\phi_n\}_{n \in \mathbb{N}}$ (based on formulas from [29]) that

- have a linear number of variables: $|\text{vars}(\phi_n)| = O(n)$;
- have constant initial existential width: $w_\exists(\phi_n) = O(1)$;
- require $\text{QU-Res}$ refutations of linear existential width: $w_\exists(\phi_n \vdash \bot) = \Omega(n)$;
- admit $\text{QU-Res}$ refutations of polynomial size: $s(\phi_n \vdash \bot) = n^{O(1)}$.

The QBFs $\{\phi_n\}_{n \in \mathbb{N}}$ clearly violate (3). However, no contradiction follows from Theorem 35. Since $\{\phi_n\}_{n \in \mathbb{N}}$ are unbounded alternation QBFs, the $n^{\text{th}}$ instance having alternation depth $n$, Theorem 35 yields only a constant lower bound.
7 Conclusions

It is interesting to compare our characterisation of QBF resolution hardness with the characterisation of QBF Frege systems [13]. There the authors show a direct correspondence between C-Frege (where lines in the system are C-circuits) and the circuit class C, e.g. hardness in QBF NC$^1$-Frege is characterised by NC$^1$ hardness. This is not the case in our results here. Resolution works with CNFs, i.e. formulas of depth 2. By a result of Krause [33], the complexity of decision lists (and hence of UDLs) is strictly intermediate between depth-2 and depth-3 circuits. Hence in QBF resolution, our circuit model is strictly stronger than the model we use to represent the formulas. This partly explains why ideas from [6,14] do not suffice to characterise QBF resolution [12]. In addition to finding the right circuit model of UDLs, new technical ideas (such as the entailment sequence) are needed.

It is also clear from our results that UDLs do not characterise QU-Res hardness for QBFs of unbounded quantifier complexity. While QBFs of bounded quantification succinctly represent all problems from the polynomial hierarchy, which covers most applications of modern QBF solving and is prominently represented in QBF evaluation benchmarks [34,39], we leave open the question of finding the right computational model to characterise QBF resolution for unbounded quantifier complexity.

Acknowledgments

Research was supported by grants from the John Templeton Foundation (grant no. 60842) and the Carl Zeiss Foundation.

References