Journal of Artificial Intelligence Research 77 (2023) 1455-1487 Submitted 03/2023; published 08/2023

Classes of Hard Formulas for QBF Resolution

Agnes Schleitzer AGNES.SCHLEITZER@UNI-JENA.DE
Olaf Beyersdorff OLAF.BEYERSDORFF@UNI-JENA.DE
Friedrich-Schiller-Universität Jena,
Fakultät für Mathematik und Informatik,
Institut für Informatik,
Ernst-Abbe-Platz 1, 07743 Jena, Deutschland

Abstract

To date, we know only a few handcrafted quantified Boolean formulas (QBFs) that are hard for central QBF resolution systems such as Q-Res and QU-Res, and only one specific QBF family to separate Q-Res and QU-Res.

Here we provide a general method to construct hard formulas for Q-Res and QU-Res. The construction uses simple propositional formulas (e.g. minimally unsatisfiable formulas) in combination with easy QBF gadgets (Σ_2^b formulas without constant winning strategies). This leads to a host of new hard formulas, including new classes of hard random QBFs.

We further present generic constructions for formulas separating Q-Res and QU-Res, and for separating Q-Res and LD-Q-Res.

1. Introduction

The main objective in *proof complexity* is to study the size of proofs in different formal proof systems. Proof complexity has its origins in computational complexity (Cook & Reckhow, 1979) with many important connections to other fields, in particular to logic (Krajíček, 2019; Cook & Nguyen, 2010) and solving (Buss & Nordström, 2021). For the latter, proof complexity provides the main theoretical tool to assess the strength of modern solving methods.

The main objective in proof complexity – and often also the most challenging – is to show *lower bounds* to the size of proofs and to obtain *separations* between different calculi. For this, *specific formula families* are needed on which the lower bounds are demonstrated. In propositional proof complexity and in particular for propositional resolution – arguably the best studied system, not least because of its tight connections to SAT solving (Buss & Nordström, 2021; Pipatsrisawat & Darwiche, 2011; Atserias, Fichte, & Thurley, 2011; Beame, Kautz, & Sabharwal, 2004) – there is a vast literature on hard formulas stemming from diverse areas such as combinatorics (e.g., Haken, 1985; Bonet, Esteban, Galesi, & Johannsen, 2000), graph theory (Urquhart, 1987), logic (Krajíček, 1995), random formulas (Beame & Pitassi, 1996), and many more (Krajíček, 2019; Segerlind, 2007).

In comparison, *proof complexity of quantified Boolean formulas* (QBF) is at an earlier stage. As in the propositional domain, QBF resolution systems received key attention, of which Q-Resolution (Q-Res, Kleine Büning, Karpinski, & Flögel, 1995) and QU-Resolution (QU-Res, Van Gelder, 2012) are the most important base systems. They augment the propositional resolution system by a simple universal reduction rule allowing to eliminate certain universal variables from clauses.

As in SAT, QBF resolution systems are intricately connected to QBF solving (cf. Beyersdorff, Janota, Lonsing, & Seidl, 2021a, for a recent overview), with Q-Res and its extension long-distance Q-Resolution (LD-Q-Res, Balabanov & Jiang, 2012) corresponding to quantified conflict-driven clause learning (QCDCL, cf. Beyersdorff et al., 2021a; Zhang & Malik, 2002; Beyersdorff & Böhm, 2021; Lonsing, Egly, & Gelder, 2013).

In contrast to the multitude of hard formulas for propositional resolution, we are somewhat short of interesting QBF families that are amenable to a proof-theoretic study. Only a handful of QBF families (and their modifications) have been used for lower bounds and separations in the QBF literature. The most prominent of these are arguably the KBKF formulas from the very first article that introduced Q-Res (Kleine Büning et al., 1995). The other 'notorious' QBF families are the equality formulas (Beyersdorff, Blinkhorn, & Hinde, 2019), the parity formulas (Beyersdorff, Chew, & Janota, 2019), and the CR formulas (Janota & Marques-Silva, 2015). Together these more or less comprise the formula toolbox of QBF proof complexity and are used for almost all of the known separations.

It would thus be desirable to have more interesting and natural QBFs that can be shown to be hard for Q-Res or QU-Res. More such QBFs would not only be valuable for proof complexity, but also for solving where they can be used as benchmarks to compare different solving techniques.[1]

It is also not so easy to tap into the fund of hard propositional formulas. While the existentially quantified version of each CNF that is hard for propositional resolution is trivially also hard for Q-Res and QU-Res, we are rather interested in 'genuine' QBF hardness that stems from quantifier alternations and not from the propositional base system.[2]

Our Contributions. Our contributions can be summarised as follows.

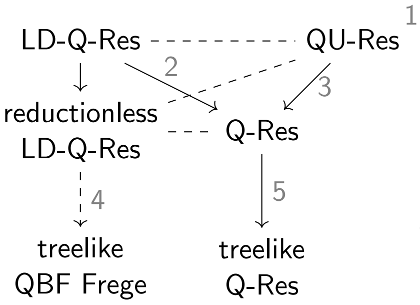
(1) Hard QBFs for Q-Res and QU-Res. We introduce a generic construction to obtain large classes of QBFs that are hard for Q-Res and QU-Res. The construction uses two key ingredients: (i) suitable propositional base formulas and (ii) simple QBF gadgets. The *propositional base formula* needs to have a sufficiently large set of clauses that we identify as 'critical', e.g. all minimally unsatisfiable formulas meet that requirement. Otherwise, the base formulas can be quite simple (and in particular can be easy for propositional resolution). The *QBF gadget* must be a false Σ_2^b formula without a constant winning strategy for the universal player in the evaluation game for QBFs. Otherwise, the gadgets can again be quite simple.

We then combine the propositional base formula with the QBF gadgets in a rather straightforward way to obtain Σ_3^b QBFs that require exponential-size proofs in Q-Res and QU-Res. The lower bound follows by the size-cost lower-bound technique (Beyersdorff et al., 2019) that always yields 'genuine' QBF lower bounds, i.e., our construction yields 'genuinely' hard QBFs in the sense discussed above.

We illustrate our method with a couple of examples. These include the equality formulas (Beyersdorff et al., 2019) (which actually inspired our construction), new circle, equivalence, and XOR formulas, as well as a large class of random QBFs.

[1] A track of crafted formulas was introduced into QBFEval 2020 and a tool to generate the mentioned QBF families was presented by Beyersdorff, Pulina, Seidl, and Shukla (2021b).

[2] A formal framework for 'genuine' QBF hardness was introduced by Beyersdorff, Hinde, and Pich (2020). All the mentioned QBF examples – KBKF, equality, and parity – are genuinely hard in this sense.



Hard Formulas		
1	Section 3:	Theorem 12
Separating Formulas		
2	Section 4:	Corollary 26
3	Section 5.3:	Theorem 43
4	Section 4:	Proposition 29
5	Section 5.1:	Theorem 40

Figure 1: The simulation order of QBF proof systems mentioned in this article and our contributions to formulas for lower bounds and separations.

$A \longrightarrow B$: A simulates B + exponential separation; A - - B : A and B are incomparable; $A \dashrightarrow B$: B does not simulate A.

(2) Separations between Q-Res and LD-Q-Res. We show that our construction above yields QBFs that exponentially separate the systems Q-Res and LD-Q-Res, if the propositional base formulas are easy for propositional resolution and the QBF gadgets are easy for Q-Res. These conditions are met by all our examples above.

This should be welcome news as we previously knew of only very few formulas (essentially KBKF, equality, and parity) that separate Q-Res from LD-Q-Res (Beyersdorff et al., 2019; Egly, Lonsing, & Widl, 2013; Chew, 2017; Beyersdorff et al., 2019).

(3) Separations between Q-Res and QU-Res. To obtain separations between Q-Res and QU-Res, we first modify the Σ_3^b prefix of the QBFs constructed in (1) to an unbounded 'interleaved' prefix. These 'interleaved' QBFs become easy for Q-Res (while still retaining hardness for treelike Q-Res), but a further 'tail' construction (inspired by KBKF) modifies them into QBFs that become hard for Q-Res, yet easy for QU-Res.

In comparison to our quite transparent method in (1) above, the technical details of these constructions are somewhat more involved. Yet again we obtain a large class of QBFs separating Q-Res and QU-Res. Previously, the KBKF formulas were the only known separating example (Kleine Büning et al., 1995; Van Gelder, 2012; Beyersdorff & Blinkhorn, 2021). Interestingly, all formulas we construct in (3) have unbounded quantifier complexity, which we know must be the case for a separation of QU-Res from Q-Res (Clymo, 2021; Beyersdorff, Blinkhorn, & Mahajan, 2020).

The simulation order of the proof systems mentioned in this paper as well as pointers to the relevant results are shown in Figure 1.

Organisation. We start in Section 2 with preliminaries on QBF and the relevant proof systems. Section 3 contains our generic construction of hard QBFs together with a couple of examples. QBFs separating LD-Q-Res from Q-Res and of QU-Res from Q-Res are constructed in Sections 4 and 5, respectively. We conclude in Section 6 with some open questions.

2. Preliminaries

A *CNF (conjunctive normal form)* is a conjunction of disjunctions of literals. The disjunctions are called *clauses.* A *literal* l is a propositional variable x or its negation $\overline{x}$, we write $\mathsf{vars}(l) = x$.

QBFs. A *quantified Boolean formula (QBF)* in *closed prenex form* $\phi = \mathcal{P} \cdot \varphi$ consists of a *quantifier prefix* $\mathcal{P}$ and a propositional formula φ, called the *matrix.* The prefix is a series of quantifiers $Q_i \in \{\forall, \exists\}$, each followed by a set X_i of variables. No variable can be quantified twice, so $X_i \cap X_j = \varnothing$ if $i \neq j$. For a *closed* QBF (which we only consider here), $\mathcal{P}$ quantifies exactly the variables occurring in φ. Thus, for $\mathcal{P} = Q_1 X_1 Q_2 X_2 \dots Q_n X_n$, the matrix φ is a formula in variables $\bigcup_{i \in [n]} X_i$ and we write $\mathsf{vars}(\mathcal{P} \cdot \varphi) = \mathsf{vars}(\varphi) = \bigcup_{i \in [n]} X_i$. As there are no free variables in a closed QBF, it is either *true* or *false.* We write $\mathsf{vars}_{\exists}(\varphi)$ for the set of existential variables in $\mathcal{P} \cdot \varphi$ and $\mathsf{vars}_{\forall}(\varphi)$ for those associated with $\forall$. A *QCNF* is a QBF with a CNF matrix.

An *assignment* assigns truth values to variables. We sometimes represent an assignment as a set of pairs of variables and their associated (boolean) values. We denote by v^{α}, l^{α} the value of a variable v respective a literal l under an assignment α. We write $\langle V \rangle$ for the set of all possible assignments to V, $\langle \chi \rangle = \langle \mathsf{vars}(\chi) \rangle$ for the assignments of a propositional formula χ and $\langle \phi \rangle = \langle \mathcal{P} \cdot \varphi \rangle = \langle \varphi \rangle$ for those of a QBF $\phi = \mathcal{P} \cdot \varphi$.

Closed QBFs can be viewed as a game between an existential and a universal player generating a total assignment (Sipser, 2005). The players assign truth values to all variables in the order of the quantifier prefix (the existential player chooses the values for existential variables, the universal player those for universals). The existential player wins, if the generated assignment satisfies the matrix; otherwise the universal player wins. For a closed QBF, there is always a *winning strategy* for one of the two players. We call this game the *assignment game.*

A countermodel is a winning strategy for the universal player. While countermodels are often considered as a collection of functions (one for each universal variable), we prefer to understand them as a single function, whose output is an assignment to the universal variables (for further explanations see e.g. Beyersdorff et al., 2020). The range of a countermodel is therefore the number of different assignments to the universal variables that can be generated within the framework of the associated strategy. The range of a countermodel on a single universal block is analogously the number of different assignments to the variables of this block. We define *strategy size* in accordance with Beyersdorff and Blinkhorn (2020):

Definition 1 (Strategy Size ρ; Beyersdorff & Blinkhorn, 2020)**.** *Let ϕ be a false QBF. We refer to the smallest cardinality of the range of a countermodel for ϕ as the* strategy size *$\rho(\phi)$ of ϕ.*

Proof systems. *Resolution* (Res) is a refutational proof system for propositional formulas with only two inference rules: For a input formula χ, we can derive any $C \in \chi$ as an axiom and from two Clauses $C_1 \cup \{x\}$, $C_2 \cup \{\overline{x}\}$ we can derive the resolvent $C_1 \cup C_2$ by Resolution over the pivot x.

Q-Res (Kleine Büning et al., 1995) transfers Resolution from propositional logic to QBF. It uses the resolution rule (`Q-Res`) which only allows existential pivots and forbids

`Axiom`	$\dfrac{}{C}$	C is a non-tautologous clause in the matrix φ.
`Q-Res`	$\dfrac{C_1 \cup \{x\} \quad C_2 \cup \{\overline{x}\}}{C_1 \cup C_2}$	$C_1 \cup C_2$ is non-tautologous; $x \in \mathsf{vars}_{\exists}(\phi)$.
`QU-Res`	$\dfrac{C_1 \cup \{x\} \quad C_2 \cup \{\overline{x}\}}{C_1 \cup C_2}$	$C_1 \cup C_2$ is non-tautologous.
`LDQ-Res`	$\dfrac{C_1 \cup \{x\} \quad C_2 \cup \{\overline{x}\}}{C_1^* \cup C_2^* \cup U^*}$	$l^* = l \vee \bar{l}$, $\{l^*\} = \{l, \bar{l}\}$ for any literal l; $C_1^* = C_1 \setminus (C_1 \cap \overline{C_2})$; $C_2^* = C_2 \setminus (\overline{C_1} \cap C_2)$; $U^* = \{u^* \mid u \in \mathsf{vars}(C_1 \cap \overline{C_2})\}$; $x \in \mathsf{vars}_{\exists}(\phi)$; $C_1 \cup C_2$ does not contain any existential tautologies; any $u \in \mathsf{vars}(U^*)$ is quantified right of x in $\mathcal{P}$.
`∀Red`	$\dfrac{C \cup \{u\}}{C}$	$u \in \mathsf{vars}_{\forall}(\phi)$ and quantified right of each existential variable in C regarding $\mathcal{P}$.

Figure 2: Rules of the QBF proof systems Q-Res, QU-Res and LD-Q-Res for a QBF $\phi = \mathcal{P}.\varphi$.

tautologous resolvents. Universal variables are eliminated by universal reduction (∀`Red`). The rules are given in Figure 2.

QU-Res (Van Gelder, 2012) extends the weaker system Q-Res by allowing resolution also over universal pivots in its resolution rule `QU-Res`. Nevertheless Q-Res is refutationally sound and complete.

LD-Q-Res (Balabanov & Jiang, 2012) is an extension of Q-Res which allows long-distance resolution steps under certain conditions (see Figure 2 for the definition of the resolution rule `LDQ-Res`), allowing tautological resolvents. The ∀`Red` rule is modified such that merged universal literals from long distance steps can also be reduced under the same conditions as usual universal variables.

The size of a proof π, denoted $|\pi|$, is the number of clauses in π. A proof system S *p-simulates* a system S', if every S' proof can be transformed in polynomial time into an S proof of the same formula.

3. Construction of Hard Formulas for QU-Res

We start by recalling the lower-bound technique for QU-Res via cost introduced by Beyersdorff et al. (2019).

Definition 2 (Cost)**.** *We consider all countermodels for a false QBF ϕ and determine for each of them the largest range on a single universal block. The minimum over these cardinalities is the* cost *of ϕ.*

For Σ_3^b formulas (i.e., with only one universal block), cost coincides with strategy size (Definition 1). Cost is an absolute lower bound for proof size in QU-Res (and Q-Res):

Theorem 3 (Beyersdorff et al., 2019)**.** *Let ϕ be a false QCNF. Then QU-Res refutations of ϕ have size at least* $\mathrm{cost}(\phi)$*.*

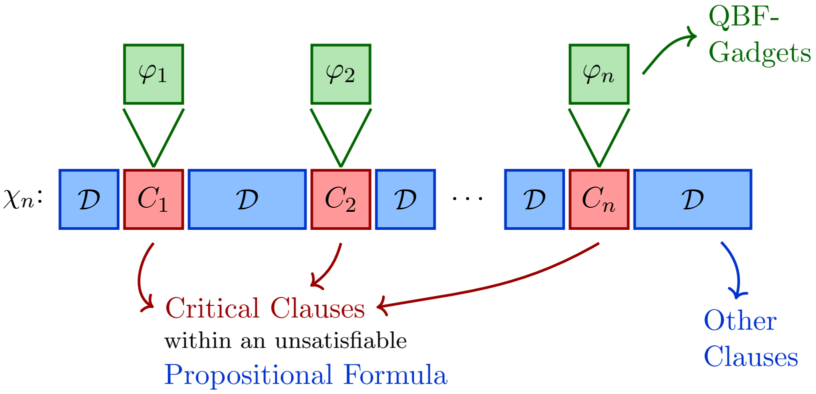


Figure 3: Design idea of the construction principle for hard formulas for QU-Res.

The equality formulas from Beyersdorff et al. (2019) have exponential cost and are therefore hard for QU-Res:

Definition 4 (Equality formulas; Beyersdorff et al., 2019). *For $n \in \mathbb{N}$ we define the n^{th}equality formula as*

$$\mathrm{EQ}_n = \exists x_1 \dots x_n \forall u_1 \dots u_n \exists t_1 \dots t_n \cdot \left(\bigcup_{i \in [n]} \{\{x_i, u_i, \overline{t_i}\}, \{\overline{x_i}, \overline{u_i}, \overline{t_i}\}\} \right) \cup \{\{t_1, \dots, t_n\}\} \,. \quad (1)$$

We take the equality formulas as a starting point and then subsequently generalize their construction. The underlying principle of the equality formulas is to enforce a unique universal winning strategy of exponential size. In the case of equality, the winning strategy is to assign $u_i = x_i$. The formulas can be understood as being based on a simple propositional formula consisting of the clause $\{t_1, \dots, t_n\}$ and unit clauses $\{\overline{t_1}\}, \dots, \{\overline{t_n}\}$, into which this exponential size winning strategy is injected through adding the x and u variables.

Based on this intuition, we outline a general construction for hard QBFs, comprising the following steps:

- Find a family $(\chi_i)_{i \in \mathbb{N}}$ of propositional formulas whose n^{th}member χ_n has at least n critical clauses (we define that notion in Definition 5).
- Find QBF gadgets (defined in Definition 9) that enforce exponential strategy size.
- Connect the two components such that any winning strategy has exponential range and forces the existential player to lose on the propositional formula.

We illustrate this idea in Figure 3.

3.1 Suitable Propositional Formulas

Let us first formally define the afore mentioned critical clauses:

Definition 5 (critical clauses). *For an unsatisfiable propositional formula χ we call a clause $C \in \chi$* critical, *if $\chi \setminus \{C\}$ is satisfiable. We call a set $\mathcal{C} \subseteq \chi$ critical, if any $C \in \mathcal{C}$ is critical.*

Note that for a minimally unsatisfiable formula, every subset of clauses is critical.

We now have a look at some suitable propositional formula families. We will denote the critical clauses by $\mathcal{C} = \{C_i \mid i \in [n]\}$ and by $\mathcal{D} = \{D_i \mid i \in [|\chi_n| - n]\}$ the remaining clauses. The subset of critical clauses can be chosen in more than one way, but for each example we make a specific choice that we will also use later in the construction of the hard QBFs.

The underlying propositional formulas from the equality formulas are:

Example 6 (Simple Contradiction)**.** $\mathrm{SC}_n = \{D_1\} \cup \bigcup_{i \in [n]} \{C_i\}$ *with* $D_1 = \{t_1, \ldots, t_n\}$ *and* $C_i = \{\overline{t_i}\}$ *for* $i \in [n]$*. Note that* SC_n *is minimally unsatisfiable.*

In addition, we consider two further running examples.

Example 7 (Implication Chain)**.** $\mathrm{IC}_n = \bigcup_{i \in [n]} \{C_i\}$ *for* $n > 1$ *with* $C_i = \{t_{i-1}, \overline{t_i}\}$ *for* $i \in [1, n-2]$ *and* $C_{n-1} = \{\overline{t_0}\}$*,* $C_n = \{t_{n-2}\}$*. In this minimally unsatisfiable formula we set* $\mathcal{D} = \varnothing$*.*

Example 8 (Equivalence Chain)**.** $\mathrm{EC}_n = \left(\bigcup_{i \in [n]} \{C_i, D_i\}\right) \cup \{D_{n+1}, D_{n+2}\}$ *with* $C_i = \{t_{i-1}, \overline{t_i}\}$*,* $D_i = \{\overline{t_{i-1}}, t_i\}$ *for* $i \in [n]$ *and* $D_{n+1} = \{t_0, t_n\}$*,* $D_{n+2} = \{\overline{t_0}, \overline{t_n}\}$*. Note that even though the formula is minimally unsatisfiable, we can choose a large set* $\mathcal{D}$*.*

3.2 QBF Gadgets

We now define the second ingredient of our construction, the QBF gadgets:

Definition 9 (QBF Gadget)**.** *A* QBF gadget *is a false* Σ_2^b *QBF* $\phi = \mathcal{P} \cdot \varphi$ *with only non-constant winning strategies, i.e., there is no strategy to falsify* ϕ *that uses only one fixed assignment to the variables in the universal block.*

In fact, it is not necessary to restrict gadgets to Σ_2^b formulas, but it is sufficient for our purposes and simplifies constructions and proofs.

The equality formulas can be understood to use the equality gadget:

Example 10 (Equality Gadget)**.** *The equality gadget forces the universal player to assign* $u = x$*:* $\mathrm{EQ} = \exists x \forall u \cdot \{\{x, u\}, \{\overline{x}, \overline{u}\}\}$*.*

Note that the gadget is equivalent to $\exists x \forall u \cdot x \not\leftrightarrow u$, so the unique winning strategy for the universal player is $u = x$. Therefore it is a QBF gadget.

To see more clearly, how the equality formulas are composed from the gadget and the propositional base formulas SC_n, we could restate (1) as

$$\exists x_1 \cdots x_n \forall u_1 \cdots u_n \exists t_1 \cdots t_n \cdot \left(\bigwedge_{i=1}^{n} ((x_i \leftrightarrow u_i) \rightarrow \bar{t}_i) \right) \wedge \left(\bigvee_{i=1}^{n} t_i \right). \tag{2}$$

The formulas (1) are then simply a transformation of (2) into CNF. Note that the gadget is not inserted into all clauses, but only into the chosen set of critical clauses of SC_n.

The equality gadget is arguably the simplest QBF gadget and except for $\exists x \forall u \cdot x \leftrightarrow u$ the only one in two variables. Nevertheless, it is easy to construct many further gadgets. As an example, we consider the XOR gadget $\exists x^1 x^2 \forall u \cdot (x^1 \oplus x^2) \not\leftrightarrow u$, which has the unique winning strategy $u = x^1 \oplus x^2$.

Example 11 (XOR Gadget)**.** *The XOR gadget forces the universal player to assign* $u = x_1 \oplus x_2$*:* $\mathrm{XOR} = \exists x^1 x^2 \forall u \cdot$

$$\{\{x^1, x^2, u\}, \{x^1, \overline{x^2}, \overline{u}\}, \{\overline{x^1}, x^2, \overline{u}\}, \{\overline{x^1}, \overline{x^2}, u\}\}.$$

It is also possible to construct gadgets with more than one universal variable, e.g. by using functions with more than one (logical) output variable (e.g. a half adder). We will use this approach to get random gadgets in Section 3.5.

3.3 Hard Formulas for QU-Res

We now want to combine the described propositional formulas with QBF gadgets.

We need a QBF gadget for each clause in a sufficiently large set of critical clauses. As we intend to construct families of hard QBFs, for any $n \in \mathbb{N}$ we first collect a sequence of n QBF gadgets whose variables are pairwise disjoint. The simplest way to obtain such a sequence is to choose n instances of the same gadget for each $n \in \mathbb{N}$. Another possibility would be to insert different gadgets into the critical clauses, e.g. we could choose them from the previously mentioned examples.

We define the product $\varphi \times C$ of a CNF φ and a clause C as $\varphi \times C := \{D \cup C \mid D \in \varphi\}$. Note that for a CNF φ and a Clause C the implication $\overline{\varphi} \to C$ is a CNF again and $\overline{\varphi} \to C \equiv \varphi \times C$. Our first main result follows:

Theorem 12. *Let* $\Phi_n = (\phi_i)_{i\in[n]} = (\exists X_i \forall U_i \cdot \varphi_i)_{i\in[n]}$ *be a sequence of variable disjoint QBF gadgets and* χ_n *a propositional formula with a set* $\mathcal{C} = \{C_1, \dots, C_n\}$ *of critical clauses and a set* $\mathcal{D}$ *of remaining clauses. Set* $T_n = \mathsf{vars}(\chi_n)$ *and let* χ_n *have no common variables with* $\bigcup_{i\in[n]}(X_i \cup U_i)$*. Then*

$$\chi_n^\Phi = \exists X_1 \dots X_n \forall U_1 \dots U_n \exists T_n \cdot \left[\bigcup_{i\in[n]} \{\varphi_i \times C_i\}\right] \cup \mathcal{D}$$

requires QU-Res *refutations of size at least* 2^n*.*

We illustrate the construction in Figure 4.

Let us first show the following:

Lemma 13. *Let* Φ_n*,* χ_n*, and* χ_n^Φ *be as described in Theorem 12. Then any winning strategy for* χ_n^Φ *is a combination of winning strategies of the used gadgets in* Φ_n*.*

Proof. Obviously, χ_n^Φ is false: It is sufficient to combine the winning strategies of the gadgets (these are variable-disjoint and false). The existential player then has to satisfy the formula χ_n by assigning the variables in T_n, but he cannot succeed because χ_n is unsatisfiable.

We now consider an arbitrary winning strategy S for χ_n^Φ. We first argue that S must falsify each gadget: If it would satisfy the matrix φ_i of a gadget ϕ_i, it would also satisfy all clauses of $\varphi_i \times C_i$ in χ_n^Φ stemming from φ_i. This relieves the existential player from the burden of having to satisfy all the clauses in $\mathcal{C}$. By not satisfying C_i (because the concerned clauses are already satisfied), he can find a satisfying assignment for the remaining clauses in χ_n, since C_i is critical. Since all variables from χ_n are quantified in the last block, the existential player can react accordingly. Thus, he succeeds in satisfying the matrix of χ_n^Φ, which means that S is not a winning strategy.

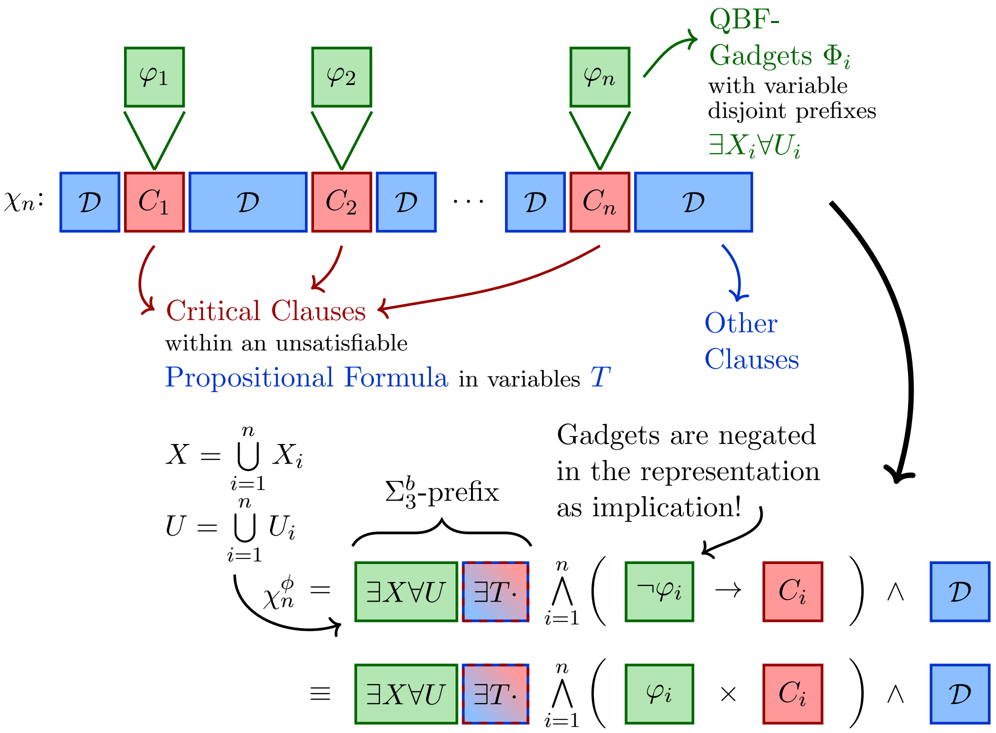

QBF-
Gadgets Φ_i
with variable
disjoint prefixes
$\exists X_i \forall U_i$
φ_1
φ_2
φ_n
χ_n:
$\mathcal{D}$
C_1
$\mathcal{D}$
C_2
$\mathcal{D}$
$\cdots$
$\mathcal{D}$
C_n
$\mathcal{D}$
Critical Clauses
within an unsatisfiable
Propositional Formula in variables T
Other
Clauses
$X = \bigcup_{i=1}^{n} X_i$
$U = \bigcup_{i=1}^{n} U_i$
Σ_3^b-prefix
Gadgets are negated
in the representation
as implication!
$\chi_n^\phi =$ $\exists X \forall U$ $\exists T \cdot$ $\bigwedge_{i=1}^{n}$ ($\neg\varphi_i$ $\rightarrow$ C_i) $\wedge$ $\mathcal{D}$
$\equiv$ $\exists X \forall U$ $\exists T \cdot$ $\bigwedge_{i=1}^{n}$ (φ_i $\times$ C_i) $\wedge$ $\mathcal{D}$

Figure 4: Details of the construction principle for hard formulas for QU-Res.

So let us assume that S falsifies the matrix of each gadget. Then S contains a winning strategy for each gadget contained in χ_n^Φ, which, due to their variable disjointness, implies the claim of the lemma. □

Proof of Theorem 12. We know from Lemma 13 that any winning strategy S for χ_n^Φ is composed of winning strategies for the single gadgets. As the n gadgets in χ_n^Φ do not have constant winning strategies and are variable disjoint, the combination of winning strategies must have range at least 2^n, i.e., χ_n^Φ has cost $\geq 2^n$. By Theorem 3 this implies QU-Res refutations of size at least 2^n. □

In this way, we get a large collection of formulas that are hard for QU-Res (and hence also for Q-Res). The constructed formulas all have a Σ_3^b prefix, which is the result of using Σ_2^b gadgets. The Σ_3^b case is probably also the most natural setting as the size-cost technique from Theorem 3 essentially works for Σ_3^b formulas. However, as mentioned, the restriction to Σ_2^b-gadgets is not necessary (we then only have to give some thought on how to suitably compose the prefix and define the non-constant property). This also allows the construction of formulas with more complex prefixes (incl. unrestricted).

3.4 Examples

Let us look at some example formulas which can be constructed using the propositional base formulas and the equality gadget, all of them exponentially hard for QU-Res.

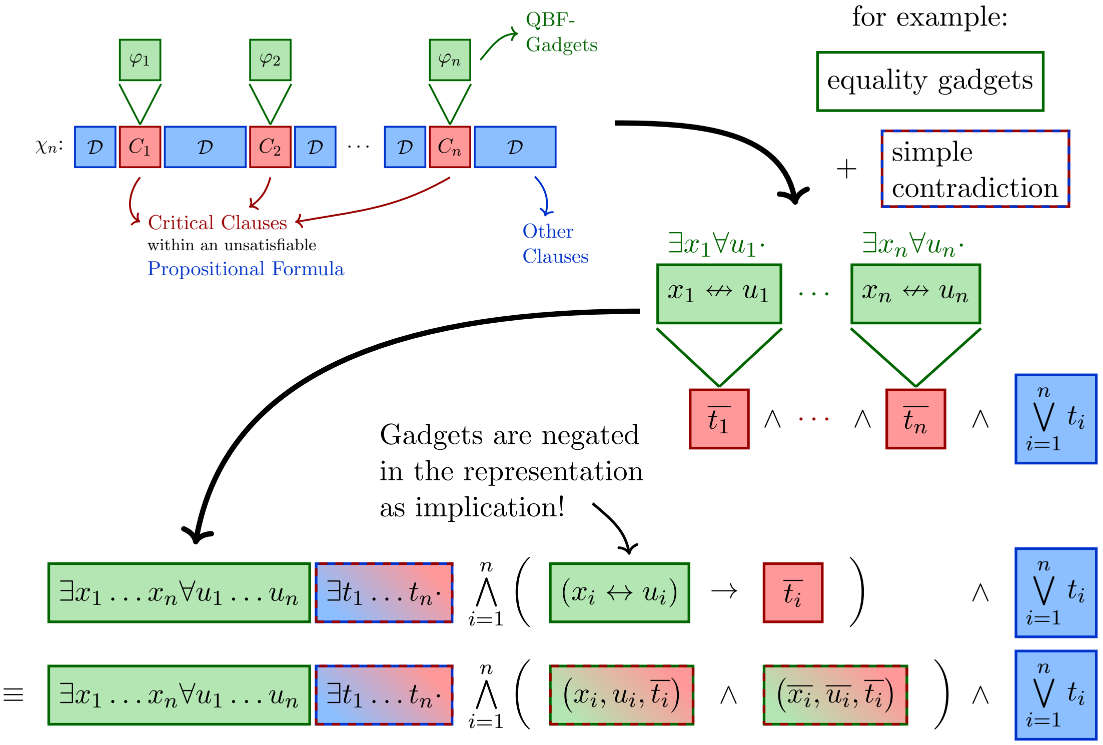

φ_1
φ_2
φ_n
QBF-Gadgets
χ_n:
$\mathcal{D}$
C_1
C_2
C_n
Critical Clauses
within an unsatisfiable
Propositional Formula
Other Clauses
for example:
equality gadgets
+
simple contradiction
$\exists x_1 \forall u_1 \cdot$
$\exists x_n \forall u_n \cdot$
$x_1 \not\leftrightarrow u_1$
$x_n \not\leftrightarrow u_n$
$\overline{t_1} \wedge \cdots \wedge \overline{t_n} \wedge \bigvee_{i=1}^{n} t_i$
Gadgets are negated in the representation as implication!
$\exists x_1 \dots x_n \forall u_1 \dots u_n \; \exists t_1 \dots t_n \cdot \bigwedge_{i=1}^{n} \left((x_i \leftrightarrow u_i) \rightarrow \overline{t_i} \right) \wedge \bigvee_{i=1}^{n} t_i$
$\equiv \exists x_1 \dots x_n \forall u_1 \dots u_n \; \exists t_1 \dots t_n \cdot \bigwedge_{i=1}^{n} \left((x_i, u_i, \overline{t_i}) \wedge (\overline{x_i}, \overline{u_i}, \overline{t_i}) \right) \wedge \bigvee_{i=1}^{n} t_i$

Figure 5: The construction of EQ_n from equality gadgets and simple contradiction.

Example 14 (Equality Formulas; Beyersdorff et al., 2019). *The equality formulas (Definition 4) arise from applying equality gadgets to simple contradiction formulas:* $\mathrm{EQ}_n = \mathrm{SC}_n^{\mathrm{EQ}}$. *The construction is illustrated in Figure 5.*

Example 15 (Circle Formulas). *Consider now the application of equality gadgets to the implication chain formulas. For $n > 1$ we obtain the QBFs*

$$\begin{aligned}\mathrm{IC}_n^{\mathrm{EQ}} =& \exists x_1 \dots x_n \forall u_1 \dots u_n \exists t_0 \dots t_{n-2} \cdot \\ & \left(\bigcup_{i=1}^{n-2} \{ \{u_i, x_i, t_{i-1}, \overline{t_i}\}, \{\overline{u_i}, \overline{x_i}, t_{i-1}, \overline{t_i}\} \} \right) \\ & \cup \{ \{u_{n-1}, x_{n-1}, \overline{t_0}\}, \{\overline{u_{n-1}}, \overline{x_{n-1}}, \overline{t_0}\}, \{u_n, x_n, t_{n-2}\}, \{\overline{u_n}, \overline{x_n}, t_{n-2}\} \} \, .\end{aligned}$$

Example 16 (Equivalence Formulas). *Instead of the implication chain, we can also use the equivalence chain* EC. *Applying equality gadgets on these formulas, we get*

$$\mathrm{EC}_n^{\mathrm{EQ}} = \exists x_1 \dots x_n \forall u_1 \dots u_n \exists t_0 \dots t_n \cdot \left(\bigcup_{i \in [n]} \{C_{i,1}, C_{i,2}, D_i\} \right) \cup \{D_{n+1}, D_{n+2}\}$$

with clauses $C_{i,1} = \{x_i, u_i, t_{i-1}, \overline{t_i}\}$, $C_{i,2} = \{\overline{x_i}, \overline{u_i}, t_{i-1}, \overline{t_i}\}$, $D_i = \{\overline{t_{i-1}}, t_i\}$ *for* $i \in [n]$ *and* $D_{n+1} = \{t_0, t_n\}$, $D_{n+2} = \{\overline{t_0}, \overline{t_n}\}$.

We would argue that the circle and equivalence formulas are almost as canonical and intuitive as the already familiar equality formulas.

Example 17 (XOR Formulas)**.** *We combine the XOR gadgets (Example 11) with* SC*:*

$$\begin{aligned}\mathrm{SC}_n^{\mathrm{XOR}} =& \exists x_1^1 x_1^2 \dots x_n^1 x_n^2 \forall u_1 \dots u_n \exists t_1 \dots t_n \cdot \\ & \left[\bigcup_{i \in [n]} \left\{ \{x_i^1, x_i^2, u_i, \overline{t_i}\}, \{x_i^1, \overline{x_i^2}, \overline{u_i}, \overline{t_i}\}, \{\overline{x_i^1}, x_i^2, \overline{u_i}, \overline{t_i}\}, \{\overline{x_i^1}, \overline{x_i^2}, u_i, \overline{t_i}\} \right\} \right] \\ & \cup \{t_1, \dots, t_n\}.\end{aligned}$$

3.5 Random Formulas

Using our construction, it is also quite straightforward to obtain various random QBFs. For this we construct gadgets from Boolean functions. We need the following notion:

Definition 18 (F-satisfying Assignment)**.** *For* $X = \{x_1, \dots, x_a\}$*,* $U = \{u_1, \dots, u_b\}$ *and a function* $F : \langle X \rangle \to \langle U \rangle$ *we call an assignment* $\alpha \in \langle X \cup U \rangle$ F-satisfying *iff* $F(x_1^\alpha \dots x_a^\alpha) = u_1^\alpha \dots u_b^\alpha$*.*

Definition 19 ($F_{a,b}$-Gadget)**.** *An* $F_{a,b}$*-gadget is built from a non-constant Boolean function* $F : \{0,1\}^a \to \{0,1\}^b$ *as follows: We introduce sets of variables* $X = \{x_1, \dots, x_a\}$ *and* $U = \{u_1, \dots, u_b\}$*. Consider* F *as function from* $\langle X \rangle$ *to* $\langle U \rangle$*. For any* F*-satisfying assignment* α *we add the clause* $\{v \mid v^\alpha = 0\} \cup \{\overline{v} \mid v^\alpha = 1\}$*. We call the following QBF an* $F_{a,b}$*-gadget:*

$$\mathrm{RG}_{a,b}^F = \exists x_1 \dots x_a \forall u_1 \dots u_b \cdot \{\{v \mid v^\alpha = 0\} \cup \{\overline{v} \mid v^\alpha = 1\} \mid \alpha \textit{ is } F\textit{-satisfying}\}.$$

We check that $F_{a,b}$-gadgets satisfy the required properties:

Lemma 20. *Let* $\mathrm{RG}_{a,b}^F$ *be an* $F_{a,b}$*-gadget based on a Boolean function* $F : \{0,1\}^a \to \{0,1\}^b$ *as described in Definition 19. Then* $\mathrm{RG}_{a,b}^F$ *is a QBF gadget.*

Proof. Obviously, any such QBF is a Σ_2^b formula. To argue for its falsity, let us consider the assignment game: First, the existential player assigns the X-variables. Let α be the F-satisfying extension of the chosen assignment to $X \cup U$, i.e., $F(x_1^\alpha \dots x_a^\alpha) = u_1^\alpha \dots u_b^\alpha$. The strategy of the universal player is now to assign U according to α. This will falsify the clause $\{v \mid v^\alpha = 0\} \cup \{\overline{v} \mid v^\alpha = 1\}$ and thus the whole QBF. Thus the strategy following F is apparently a winning strategy. The non-constancy is also clear as the function F is not constant: Suppose, there was a constant winning strategy and $\{l_1^u, \dots, l_b^u\}$ was its negation pattern on $\{u_1, \dots, u_b\}$ (i.e. $l_i^u = \overline{u_i}$ iff u_i is assigned 0 in the strategy and $l_i^u = u_i$ else). A winning strategy always falsifies a clause, so for every possible assignment to the existential variables, there needs to be a clause containing the inverse negation pattern of this assignment and $\{\overline{l_1^u}, \dots, \overline{l_b^u}\}$. Since every clause is based on a F-satisfying assignment (by definition), we see that F is constant, which violates the assumptions. □

There are $(2^b)^{(2^a)} - 2^b$ different non-constant functions with a inputs and b outputs. Each of them leads to an $F_{a,b}$-gadget. Such a gadget uses 2^a clauses, containing $a + b$ literals each.

For the construction of random formulas, we need multiple gadgets. A possible procedure to construct sequences of random gadgets is to set lower and upper bounds for a, b, for each $i \in [n]$ choose parameters a_i, b_i randomly within the bounds and then obtain a F_{a_i,b_i}-gadget from a randomly chosen non-constant function $F : \{0,1\}^{a_i} \to \{0,1\}^{b_i}$ (repeating this process for each index $n \in \mathbb{N}$).

We also want to randomly choose the propositional base formulas. Each clause of a minimally unsatisfiable formula is critical, so we focus on generating minimally unsatisfiable formulas. A full characterization of minimally unsatisfiable 2-CNFs was recently given by Abbasizanjani and Kullmann (2020) (see also Abbasizanjani, 2021; Abbasizanjani & Kullmann, 2018). We can use this characterization to obtain the propositional part of our construction (thereby restricting ourselves to 2-CNFs). This includes the IC_n formulas (the implication chain formulas), but not the SC_n formulas (simple contradiction formulas).

Abbasizanjani (2021) also describes a generation procedure for special minimally unsatisfiable formulas that are 2-CNFs with deficiency one (exactly one clause more than the number of variables). Using the approach described there with a small modification (allowing C_1 and C_2 to contain more than one literal) enables us to generate unsatisfiable deficiency one formulas (which are not necessarily 2-CNFs):

Lemma 21. *Consider the following construction method:*

Start with $F_0 := \{\bot\}$. Repeat the following steps for $i = 1, \ldots, n$:

- *Choose a clause $C \in F_{i-1}$ at random (set $C := \{\}$ if $F_{i-1} = \bot$).*
- *Choose C_1 and C_2 with $C_1 \cup C_2 = C$.*
- *Build $F_i = F_{i-1} \setminus \{C\} \cup \{C_1 \cup \{v\}\} \cup \{C_2 \cup \{\overline{v}\}\}$ for some $v \notin \mathsf{vars}(F_{i-1})$.*

The formulas constructed according to this method are minimally unsatisfiable.

Proof. We show this by induction: Clearly, $F_0 = \{\bot\}$ is minimally unsatisfiable. No we consider F_{i+1}. To get F_{i+1} from F_i we choose a new variable v, a clause $C \in F_i$ (or $C = \{\}$ for F_1) and a decomposition $C_1 \cup C_2 = C$. Now we replace C by $C_1 \cup \{v\}$ and $C_2 \cup \{\overline{v}\}$. At this point it is very easy to modify a proof of resolution for F_i to one for F_{i+1}: We just have to replace any axiom C by the resolution from $C_1 \cup \{v\}$ and $C_2 \cup \{\overline{v}\}$ to C. Thus we already know that F_{i+1} is unsatisfiable.

Now, to show minimality, have a look at the single clauses. We distinguish two cases: Suppose first, we omit a clause $D \in F_i \setminus \{C\}$ from F_{i+1}. We know from induction that F_i is minimally unsatisfiable, thus $F_i \setminus \{D\}$ is satisfiable. A satisfying assignment to $F_i \setminus \{D\}$ satisfies $C = C_1 \vee C_2$, i.e. it satisfies at least one of C_1 and C_2 resp. $C_1 \cup \{v\}$ and $C_2 \cup \{\overline{v}\}$. The second can easily be satisfied by extending the assignment to v (with the appropriate value). The resulting assignment satisfies $F_{i+1} \setminus \{D\}$.

For the second case, suppose we omit w.l.o.g $C_1 \cup \{v\}$ (the case of omitting $C_2 \cup \{\overline{v}\}$ is analogous). We know by induction that there is a satisfying assignment to $F_i \setminus \{C\}$. Extending this assignment by $v = 0$ satisfies $C_2 \cup \{\overline{v}\}$ and thus $F_{i+1} \setminus \{C_1 \cup \{v\}\}$. □

Now SC_n can be obtained in this way.

Combining random QBF gadgets (according to Lemma 20) with random minimally unsatisfiable formulas, we get random QBFs, which are hard for $\mathsf{QU\text{-}Res}$ by Theorem 12:

Proposition 22. *Let $\Phi_n = (\phi_i)_{i\in[n]}$ be a sequence of variable disjoint random (a_i, b_i)-gadgets, χ_n a random minimally unsatisfiable formula with n clauses and $T_n = \mathsf{vars}(\chi_n)$. Then any* QU-Res *refutation of χ_n^{Φ} (constructed as in Theorem 12) has length at least 2^n.*

Let us briefly compare our random QBFs with the hard random formulas presented by Beyersdorff et al. (2019). The formulas shown by Beyersdorff et al. resemble our formulas, but with one major difference: the QBFs from Beyersdorff et al. are only false and hard with high probability. In contrast, we construct QBFs that are always hard and false by design. The random formulas from Beyersdorff et al. can be understood to be based on the SC formulas. To this they add a random construction that is akin to a QBF gadget, but only yields one with high probability. Note that in our construction here, we can choose both the propositional base formulas and the QBF gadgets randomly.

Finally, let us give a specific construction for random QBFs.

Example 23 (Random SC)**.** *To keep the example as simple as possible, we again resort to the* SC *formulas. As we assemble the gadgets, we will set a and b fixed at $a = 2, b = 1$, instead of randomly choosing these parameters. Thus, all gadgets will be random $F_{1,2}$-gadgets. There are $2^4 - 2 = 16$ such gadgets (resp. functions) from which we can choose. We construct $\mathrm{SC}_n^{\mathrm{RG}}$ as follows: Let $(F_i)_{i\in[n]}$ be a sequence of randomly chosen non-constant functions $F_i : \{0,1\}^2 \to \{0,1\}$ for $i \in [n]$ and $\mathrm{RG}_n = (\mathrm{RG}_{2,1}^{F_i})_{i\in[n]}$ the sequence of the associated gadgets in variables x_i^1, x_i^2 and u_i each, i.e. $\mathrm{RG}_{2,1}^{F_i} = \exists x_i^1 x_i^2 \forall u_i \cdot \varphi_i$. We build*

$$\mathrm{SC}_n^{\mathrm{RG}} = \exists x_1^1 x_1^2 \dots x_n^1 x_n^2 \forall u_1 \dots u_n \exists t_1 \dots t_n \cdot \left(\bigcup_{i\in[n]} \{\varphi_i \times \{\overline{t_i}\}\} \right) \cup \{\{t_1, \dots, t_n\}\}\,.$$

These formulas have $4n$ clauses with four literals each (three from the gadget and one from a critical clause in SC_n) and the additional clause with all the positive t literals.

Their hardness follows directly from Proposition 22 and the construction of $\mathrm{SC}_n^{\mathrm{RG}}$:

Corollary 24. *Any* QU-Res *refutation of $\mathrm{SC}_n^{\mathrm{RG}}$ has size at least 2^n.*

4. Formulas Separating Q-Res and LD-Q-Res

We now prove that most of our constructed QBFs, including all the explicit examples and the random formulas, separate Q-Res and LD-Q-Res. This requires just one further natural condition, namely that the propositional base formulas have polynomial-size propositional resolution refutations and the QBF gadgets have polynomial-size Q-Res refutations.

In fact, instead of LD-Q-Res we can even use a weaker system, so-called reductionless LD-Q-Res (Bjørner, Janota, & Klieber, 2015; Peitl, Slivovsky, & Szeider, 2019; Beyersdorff, Blinkhorn, & Mahajan, 2021), which is a strict fragment of LD-Q-Res (Beyersdorff et al., 2021). This system allows merging as in LD-Q-Res but no universal reduction, i.e., any refutation ends with a purely universal clause. In other words, it includes LD-Q-Res refutations in which all universal reductions occur at the end of the derivation.

Theorem 25. *For $n \in \mathbb{N}$ let Φ_n be sequences of variable disjoint QBF gadgets with polynomial-size* Q-Res *refutations and χ_n propositional formulas with polynomial-size resolution refutations. Let $\Phi_n = (\phi_i)_{i\in[n]} = (\exists X_i \forall U_i \cdot \varphi_i)_{i\in[n]}$ and $\chi_n = \mathcal{C} \cup \mathcal{D}$ with critical clauses*

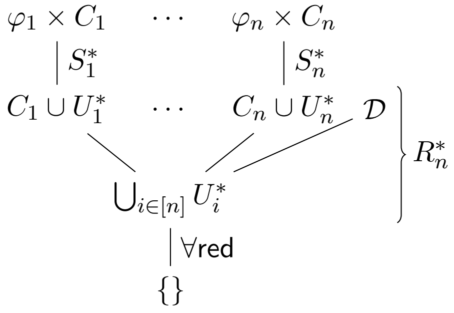


Figure 6: Polynomial-size $\mathsf{LD\text{-}Q\text{-}Res}$ refutations for χ_n^Φ.

$\mathcal{C} = \{C_1, \dots, C_n\}$, additional clauses $\mathcal{D}$, $T_n = \mathsf{vars}(\chi_n)$ and $\mathsf{vars}(\chi_n) \cap \left(\bigcup_{i\in[n]}\{X_i \cup U_i\}\right) = \varnothing$. Then χ_n^Φ (as in Theorem 12) has polynomial-size refutations in reductionless LD-Q-Res.

Proof. We consider the formula χ_n^Φ. Let R_n be polynomial-size resolution refutations of χ_n and $S_1, \dots, S_n$ polynomial-size $\mathsf{LD\text{-}Q\text{-}Res}$ refutations[3] of the gadgets $\phi_1, \dots, \phi_n$. Let S_i' be as S_i, but without the final universal reduction steps. Let U_i^* be the set of (possibly merged) universal variables in the last clause of the resulting derivation. We can enlarge every clause in S_i' by C_i and get a derivation S_i^* of $C_i \cup U_i^*$ from $\exists X_i \forall U_i \exists T_n \cdot \varphi_i \times C_i$. Now we can enlarge every C_i in R_n by U_i^*. This extension runs through the entire proof[4] and we obtain a reductionless $\mathsf{LD\text{-}Q\text{-}Res}$ derivation R_n^* of $\bigcup_{i\in[n]} U_i^*$, which we can complete to a refutation by universal reduction. The composition of the proof is shown in Figure 6. □

By Theorem 12 (the formulas are hard for $\mathsf{QU\text{-}Res}$) and Theorem 25 (which provides short $\mathsf{LD\text{-}Q\text{-}Res}$ refutations) the following holds:

Corollary 26. *The formulas χ_n^Φ from Theorem 25 separate QU-Res from (reductionless) LD-Q-Res.*

Note that all examples from Section 3.4 satisfy the required conditions and are therefore separating formulas. Furthermore the random formulas from Section 3.5 are based on either propositional 2-CNFs, which are known to have short resolution refutations, or a deficiency one formula constructed with the procedure described there, which at the same time provides a polynomial-size resolution refutation (viewed backwards, each step of the algorithm can be transformed into a resolution step with the newly introduced variable as a pivot). Thus all the random formulas separate $\mathsf{QU\text{-}Res}$ from reductionless $\mathsf{LD\text{-}Q\text{-}Res}$.

For the next insight we need a result shown by Beyersdorff and Hinde (2019):

Theorem 27 (Beyersdorff & Hinde, 2019)**.** *For any QBF ϕ, if π is a treelike P+$\forall\mathsf{red}$ proof of ϕ (where P is a propositional proof system), then $|\pi| \geq \rho(\phi)$ (where $\rho(\phi)$ is the strategy size from Definition 1).*

[3] Note that for Σ_2^b-formulas the systems $\mathsf{Q\text{-}Res}$ and $\mathsf{LD\text{-}Q\text{-}Res}$ are equivalent. A $\mathsf{Q\text{-}Res}$ refutation of such a formula is just a resolution refutation of the restriction of the formula to its existential variables with some reductions, which can be moved towards the beginning of the proof (since the universal block is rightmost). Allowing merging, we can move the reductions to the end without any problems.

[4] There can not be any conflicts in form of tautologous resolvents, since the U_i^* are pairwise variable disjoint.

This implies that all the formulas we have constructed so far, including the random QBFs, are hard for all tree-like P+∀red systems.

Corollary 28. *If χ_n^Φ is a QBF as described in Theorem 12, then any refutation of χ_n^Φ in treelike P+∀red systems has length at least 2^n.*

This leads to an interesting fact:

Proposition 29. *Treelike reductionless LD-Q-Res is not simulated by treelike QBF extended Frege systems (EF+∀red).*

Proof. The polynomial-size reductionless LD-Q-Res refutations shown in the proof of Theorem 25 are treelike, as long as the resolution refutation of the propositional formula and the reductionless LD-Q-Res refutation of the gadgets are (it is easy to find examples for both). Since EF+∀red is the extension of propositional extended Frege by universal reduction and all the formulas we constructed have exponential strategy size, the results immediately follow from Theorems 25 and 27. □

This is surprising because reductionless LD-Q-Res itself is not a very strong proof system; certainly the treelike variant is not either. Reductionless LD-Q-Res does not even simulate Q-Res (the two systems are in fact incomparable, see Peitl et al., 2019). This is interesting to contrast with the recent simulation of LD-Q-Res (and even stronger systems) by extended QBF Frege (Chew & Slivovsky, 2022). The simulation there is quite non-trivial and highly dag-like. Proposition 29 above means that it cannot be strengthened to a tree-preserving simulation.

5. Construction of Separating Formulas between Q-Res and QU-Res

We now want to construct QBFs that separate Q-Res and QU-Res. As an intermediate step, we will build QBFs that are easy for Q-Res but have exponential strategy size. In Section 5.1 we will use the examples from Section 3.4 to explain the construction, which, in fact, only changes the prefix in these examples. In Section 5.2 we formalize the general construction, adding some conditions on the underlying propositional formulas. In Section 5.3 we will then use such false QBFs with exponential strategy size and short Q-Res refutations to construct a large class of formulas separating Q-Res from QU-Res.

5.1 Some Formulas with Exponential Strategy Size and Short Q-Res Refutations

First we will look at Examples 14, 16 and 17 from Section 3.4 and show how to obtain formulas from them that are easy for Q-Res but still have exponential strategy size. The key point here is the prefix – while we leave the matrix unchanged, we re-sort the Σ_3^b prefix into an unrestricted prefix. Roughly speaking, we do this by arranging the 'crucial' variables of each critical clause into a separate existential block to the right of the variables of the associated gadget, and the remaining propositional variables into the leftmost existential block. In most of the examples already given, it is intuitively easy to identify the 'crucial' variables of a clause; in the general case, this is somewhat more involved[5], as is to determine

[5] They are in fact the pivots of certain resolution steps in special resolution refutations of the propositional formula.

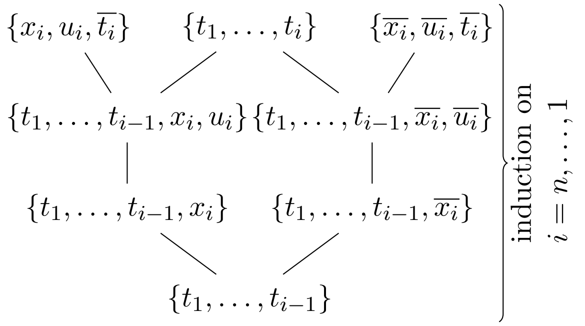

$\{x_i, u_i, \overline{t_i}\}$
$\{t_1, \dots, t_i\}$
$\{\overline{x_i}, \overline{u_i}, \overline{t_i}\}$
$\{t_1, \dots, t_{i-1}, x_i, u_i\}$
$\{t_1, \dots, t_{i-1}, \overline{x_i}, \overline{u_i}\}$
$\{t_1, \dots, t_{i-1}, x_i\}$
$\{t_1, \dots, t_{i-1}, \overline{x_i}\}$
$\{t_1, \dots, t_{i-1}\}$
induction on
$i = n, \dots, 1$

Figure 7: Polynomial-size Q-Res refutation of ${}^{\mathrm{il}}\mathrm{SC}_n^{\mathrm{EQ}}$.

the appropriate order of the critical clauses (i.e., of their variables in the prefix), which is not arbitrary. We therefore initially only verify the desired properties for Examples 14, 16 and 17 from Section 3.4, the general construction in all details follows in Section 5.2.

We start with the equality formulas. These were already modified in the desired way to the *interleaved equality formulas* (Beyersdorff et al., 2019), which have the same matrix as the equality formulas, but with an interleaved prefix (this also inspired our general construction). We adopt the name 'interleaved' also for our other examples and denote the interleaved variant of a Σ_3^b-QBF χ_n^Φ by ${}^{\mathrm{il}}\chi_n^\Phi$. We will give short Q-Res refutations for each example.

Example 30 (Interleaved Equality; Beyersdorff et al., 2019)**.** *We build* ${}^{\mathrm{il}}\mathrm{SC}_n^{\mathrm{EQ}}$ *from* $\mathrm{SC}_n^{\mathrm{EQ}}$ *by reordering the prefix in a natural way according to the indices:*

$$\begin{aligned}
\mathrm{SC}_n^{\mathrm{EQ}} &= \exists x_1 \dots x_n \forall u_1 \dots u_n \exists t_1 \dots t_n \cdot \psi \\
{}^{\mathrm{il}}\mathrm{SC}_n^{\mathrm{EQ}} &= (\exists x_1 \forall u_1 \exists t_1) \dots (\exists x_n \forall u_n \exists t_n) \cdot \psi \\
\psi &= \bigcup_{i \in [n]} \{\{\overline{t_i}, x_i, u_i\}, \{\overline{t_i}, \overline{x_i}, \overline{u_i}\}\} \cup \{t_1, \dots, t_n\}.
\end{aligned}$$

The Q-Res refutation shown in Figure 7 follows closely the resolution proof of SC_n*.*

Example 31 (Interleaved Equivalence)**.** *The prefix of* ${}^{\mathrm{il}}\mathrm{EC}_n^{\mathrm{EQ}}$ *equals the one of interleaved equality, additionally quantifying* t_0 *existentially in the leftmost block,*

$$\begin{aligned}
\mathrm{EC}_n^{\mathrm{EQ}} &= \exists x_1 \dots x_n \forall u_1 \dots u_n \exists t_0 \dots t_n \cdot \psi \\
{}^{\mathrm{il}}\mathrm{EC}_n^{\mathrm{EQ}} &= \exists t_0 (\exists x_1 \forall u_1 \exists t_1) \dots (\exists x_n \forall u_n \exists t_n) \cdot \psi \\
\psi &= \left(\bigcup_{i \in [n]} \{C_{i,1}, C_{i,2}, D_i\} \right) \cup \{D_{n+1}, D_{n+2}\}
\end{aligned}$$

with clauses

$$\begin{aligned}
C_{i,1} &= \{x_i, u_i, t_{i-1}, \overline{t_i}\} & D_i &= \{\overline{t_{i-1}}, t_i\} \quad i \in [n] \\
C_{i,2} &= \{\overline{x_i}, \overline{u_i}, t_{i-1}, \overline{t_i}\} & & \\
D_{n+1} &= \{t_0, t_n\} & D_{n+2} &= \{\overline{t_0}, \overline{t_n}\}.
\end{aligned}$$

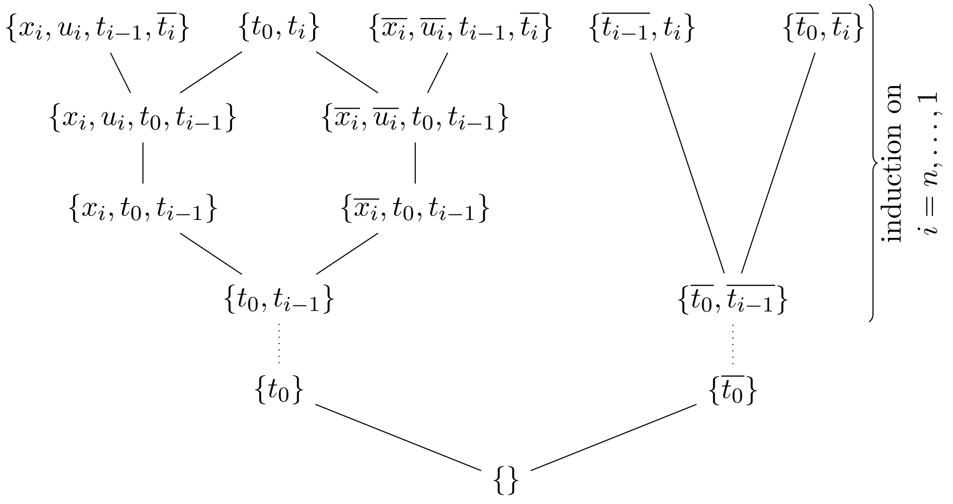

$\{x_i, u_i, t_{i-1}, \overline{t_i}\}$
$\{t_0, t_i\}$
$\{\overline{x_i}, \overline{u_i}, t_{i-1}, \overline{t_i}\}$
$\{\overline{t_{i-1}}, t_i\}$
$\{\overline{t_0}, \overline{t_i}\}$
$\{x_i, u_i, t_0, t_{i-1}\}$
$\{\overline{x_i}, \overline{u_i}, t_0, t_{i-1}\}$
$\{x_i, t_0, t_{i-1}\}$
$\{\overline{x_i}, t_0, t_{i-1}\}$
$\{t_0, t_{i-1}\}$
$\{\overline{t_0}, \overline{t_{i-1}}\}$
$\{t_0\}$
$\{\overline{t_0}\}$
$\{\}$
induction on
$i = n, \ldots, 1$

Figure 8: Polynomial-size Q-Res refutation of ${}^{\mathrm{il}}\mathrm{EC}_n^{\mathrm{EQ}}$.

Again, the Q-Res refutation (see Figure 8) is structurally similar to the resolution proof for EC_n*, although it can be seen quite clearly that only one side of the proof increases by the refutations of the gadgets, due to the choice of the critical clauses.*

We now consider using XOR gadgets:

Example 32 (Interleaved XOR)**.** *For* ${}^{\mathrm{il}}\mathrm{SC}_n^{\mathrm{XOR}}$*, the existential blocks in the prefix each comprise two existential variables, as specified by the XOR gadget. The matrix remains the same as for* $\mathrm{SC}_n^{\mathrm{XOR}}$*:*

$$\begin{aligned}
\mathrm{SC}_n^{\mathrm{XOR}} &= \exists x_1^1 x_1^2 \ldots x_n^1 x_n^2 \forall u_1 \ldots u_n \exists t_1 \ldots t_n \cdot \psi \\
{}^{\mathrm{il}}\mathrm{SC}_n^{\mathrm{XOR}} &= (\exists x_1^1 x_1^2 \forall u_1 \exists t_1) \ldots (\exists x_n^1 x_n^2 \forall u_n \exists t_n) \cdot \psi \\
\psi &= \left[\bigcup_{i \in [n]} \left\{ \{x_i^1, x_i^2, u_i, \overline{t_i}\}, \{x_i^1, \overline{x_i^2}, \overline{u_i}, \overline{t_i}\}, \{\overline{x_i^1}, x_i^2, \overline{u_i}, \overline{t_i}\}, \{\overline{x_i^1}, \overline{x_i^2}, u_i, \overline{t_i}\} \right\} \right] \\
&\quad \cup \{t_1, \ldots, t_n\}.
\end{aligned}$$

The Q-Res refutations are made slightly more complex by the gadgets, but even here the structure of the resolution proof of SC *shines through, as can be seen in Figure 9.*

Note, that all the universal reductions in the Q-Res refutations shown in Figures 7 to 9 comply with the rules thanks to the variable order in the prefixes.

It is readily verified that the interleaved formulas inherit exponential strategy size from their Σ_3^b origins. While the winning strategies of the universal player are no longer unique for the interleaved formulas, the existential player can nevertheless continue to force a game that corresponds to the winning strategy of the associated Σ_3^b formulas, i.e., $u_i = x_i$ for all $i \in [n]$ in the case of equality gadgets and $u_i = x_i^1 \oplus x_i^1$ for all $i \in [n]$ in the case of XOR gadgets. Thus, the interleaved formulas retain exponential strategy size.

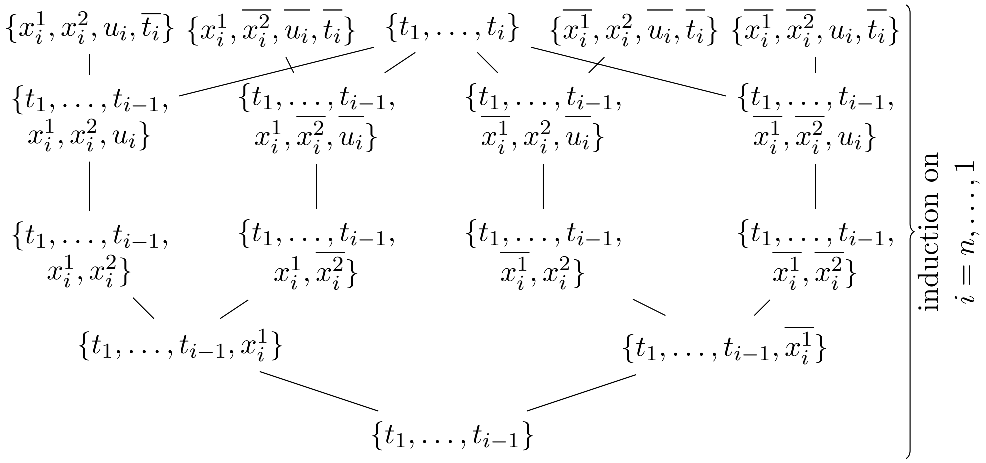

$\{x_i^1, x_i^2, u_i, \overline{t_i}\}$
$\{x_i^1, \overline{x_i^2}, \overline{u_i}, \overline{t_i}\}$
$\{t_1, \dots, t_i\}$
$\{\overline{x_i^1}, x_i^2, \overline{u_i}, \overline{t_i}\}$
$\{\overline{x_i^1}, \overline{x_i^2}, u_i, \overline{t_i}\}$
$\{t_1, \dots, t_{i-1}, x_i^1, x_i^2, u_i\}$
$\{t_1, \dots, t_{i-1}, x_i^1, \overline{x_i^2}, \overline{u_i}\}$
$\{t_1, \dots, t_{i-1}, \overline{x_i^1}, x_i^2, \overline{u_i}\}$
$\{t_1, \dots, t_{i-1}, \overline{x_i^1}, \overline{x_i^2}, u_i\}$
$\{t_1, \dots, t_{i-1}, x_i^1, x_i^2\}$
$\{t_1, \dots, t_{i-1}, x_i^1, \overline{x_i^2}\}$
$\{t_1, \dots, t_{i-1}, \overline{x_i^1}, x_i^2\}$
$\{t_1, \dots, t_{i-1}, \overline{x_i^1}, \overline{x_i^2}\}$
$\{t_1, \dots, t_{i-1}, x_i^1\}$
$\{t_1, \dots, t_{i-1}, \overline{x_i^1}\}$
$\{t_1, \dots, t_{i-1}\}$
induction on
$i = n, \dots, 1$

Figure 9: Polynomial-size Q-Res refutation of ${}^{\mathrm{il}}\mathrm{SC}_n^{\mathrm{XOR}}$.

Note that the circle formulas $\mathrm{IC}_n^{\mathrm{EQ}}$ from Example 15 cannot be modified this way – there are not even enough propositional t variables to build the prefix accordingly[6].

5.2 General Construction of Formulas as in Section 5.1

While we show in Section 5.1 that certain variants of the previously introduced examples satisfy the required conditions, in the following we will give a general construction for such formulas that are easy for Q-Res but have exponential strategy size. We will use the same ingredients as in Section 3. In fact, we only have to change the prefix and some requirements to the underlying propositional formulas and QBF gadgets. This approach is consistent with the relationship between the examples in Section 3.4 and those in Section 5.1 (e.g. the original equality formulas from Beyersdorff et al., 2019, and interleaved equality).

Building on this construction we will later carry out the full construction in Section 5.3 and thus find further separating formulas between Q-Res and QU-Res.

We recall the exponential strategy size from Section 3, and we will reuse the procedure described there, refining our requirements to the propositional base formula as well as to the QBF gadgets and reordering the prefix. To get short Q-Res refutations of the constructed formulas, in addition to gadgets with short proofs, of course we need to use propositional base formulas with short resolution refutations. In fact, the condition is more complex. In the following we denote by $C\restriction_\alpha$ the clause C, where any literal $l \in C$ is replaced by the value l^α of l under α (literals of variables not assigned by α remain unaffected). We call $C\restriction_\alpha$ the restriction of C by α. We further define the restriction of a CNF χ by α as $\chi\restriction_\alpha := \{C\restriction_\alpha \mid C \in \chi\}$ and the restriction of an assignment α by a variable set V as $\alpha\restriction_V := \{(v, b) | v \in V \wedge (v, b) \in \alpha\}$. We denote by $R = (\{C, D\}, p)$ a resolution step with parent clauses C and D over the pivot variable p.

[6] The modification becomes straightforward if we choose $\mathcal{D} = \{\{\overline{t_0}\}, \{t_n\}\}$ and $C_i = \{t_{i-1}, \overline{t_i}\}$ as clauses of IC'_n for $i \in [n]$ instead of the definition from Example 7 (note that the formula family remains the same, only the indices of the formulas shift and the partition in $\mathcal{C}$- and $\mathcal{D}$-clauses changes).

We will use the EC_n-formulas already presented (see Example 8) as an example to illustrate the following definitions.

Definition 33 (suitable refutations)**.** *Let χ be a propositional formula with a set $\mathcal{C}$ of critical clauses and a refutation π of χ. We call a resolution step in π involving a clause from $\mathcal{C}$ a $\mathcal{C}$-step and we call π $\mathcal{C}$-*suitable*, if it satisfies the following properties:*

(i) For any $C \in \mathcal{C}$ there is exactly one $\mathcal{C}$-step in π using C as axiom.

(ii) Every $\mathcal{C}$-step resolves a clause from $\mathcal{C}$ with a clause from $\mathcal{D} = \chi \setminus \mathcal{C}$ or a derived clause.

(iii) The pivots of the $\mathcal{C}$-steps are pairwise different.

(iv) Any resolvent of a $\mathcal{C}$-step contains no pivot which is used in an earlier $\mathcal{C}$-step.

We define some terminology regarding π: Let $R_1, \dots, R_n$ be the sequence of $\mathcal{C}$-steps in π ***in reverse order*** *and $C_1, \dots, C_n$ resp. $t_1, \dots, t_n$ the according sequences of parent clauses from $\mathcal{C}$ respective pivot variables. Let further $T = \mathsf{vars}(\chi)$ and $T_i = T \setminus \{t_{i+1}, \dots, t_n\}$, i.e. $T_0 = T \setminus \{t_1, \dots, t_n\}$ and $T_i = T_{i-1} \cup \{t_i\}$ for $i \in [n]$.*

Example 34 (a suitable refutation for EC_n)**.** *Recall the formulas EC_n from Example 8: $\mathrm{EC}_n = \left(\bigcup_{i\in[n]}\{C_i, D_i\}\right) \cup \{D_{n+1}, D_{n+2}\}$ with $C_i = \{t_{i-1}, \overline{t_i}\}$, $D_i = \{\overline{t_{i-1}}, t_i\}$ for $i \in [n]$ and $D_{n+1} = \{t_0, t_n\}$, $D_{n+2} = \{\overline{t_0}, \overline{t_n}\}$. Figure 10 shows a suitable refutation π for EC_n. $R_1, \dots, R_n$ is the sequence of $\mathcal{C}$-steps (in reverse order), $C_1, \dots, C_n$ and $t_1, \dots, t_n$ are the corresponding sequences of $\mathcal{C}$-parent clauses and pivot variables, respectively. Accordingly, $T = \{t_0, \dots, t_n\}$, $T_0 = \{t_0\}$ and $T_i = \{t_0, \dots, t_i\}$ for $i \in [n]$. Let us briefly review the individual elements of the definition:*

(i) Since the derivation contains exactly one outgoing edge per axiom and there is no resolution step with two parent clauses from $\mathcal{C}$, this condition is obviously satisfied.

(ii) The first $\mathcal{C}$-step resolves $C_n \in \mathcal{C}$ with $D_{n+1} \in \mathcal{D}$, any other $\mathcal{C}$-step resolves a clause from $\mathcal{C}$ with a derived clause.

(iii) The pivot of step R_i is t_i.

(iv) The resolvent of step R_i is $\{t_0, t_{i-1}\}$, so it obviously does not contain any t_j with $j > i$ (which are the pivots of earlier $\mathcal{C}$-steps).

Definition 35 (suitable assignments)**.** *Now let χ be a propositional formula, $\mathcal{C}$ a set of critical clauses and π a $\mathcal{C}$-suitable resolution refutation with T, T_i as described above.*

*Let $\alpha \in \langle T\rangle$ be an assignment to T and $\alpha_i := \alpha\restriction_{T_i}$ for $i \in [0, n]$. We call α π-*suitable*, if $C_i\restriction_{\alpha_{i-1}}$ is critical in $\chi\restriction_{\alpha_{i-1}}$ for any $i \in [n]$.*

Example 36 (a suitable assignment for EC_n)**.** *We build on the suitable refutation for EC_n shown in Example 34 and adopt the terminology used there. Consider as α the assignment that assigns 0 to any t_i, $i \in [0, n]$ and let α_i, $i \in [0, n]$ be as described in Definition 35. We*

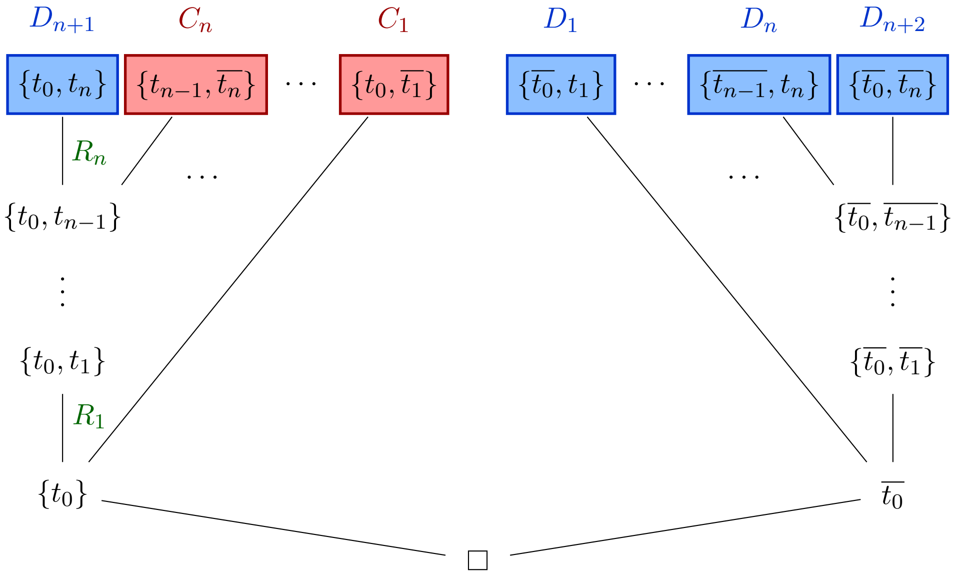

D_{n+1}
C_n
C_1
D_1
D_n
D_{n+2}
$\{t_0, t_n\}$
$\{t_{n-1}, \overline{t_n}\}$
$\{t_0, \overline{t_1}\}$
$\{\overline{t_0}, t_1\}$
$\{\overline{t_{n-1}}, t_n\}$
$\{\overline{t_0}, \overline{t_n}\}$
R_n
$\{t_0, t_{n-1}\}$
$\{\overline{t_0}, \overline{t_{n-1}}\}$
$\{t_0, t_1\}$
$\{\overline{t_0}, \overline{t_1}\}$
R_1
$\{t_0\}$
$\overline{t_0}$
$\square$

Figure 10: Suitable resolution refutation π for EC_n with critical clauses $\mathcal{C} = \{C_1, \dots, C_n\}$, additional clauses $\mathcal{D} = \{D\}$ and $\mathcal{C}$-steps $R_1, \dots, R_n$.

will show that α is π-suitable (for π from Example 34). Let us look at the corresponding restrictions of the formula:

$$\mathrm{EC}_n\restriction_{\alpha_{i-1}} = \{\{\overline{t_i}\}, \{t_n\}\} \cup \{\{t_{j-1}, \overline{t_j}\} \mid j \in [i+1, n]\} \cup \{\{\overline{t_{j-1}}, t_j\} \mid j \in [i+1, n]\}$$

for $i \in [n]$, where $C_i\restriction_{\alpha_{i-1}} = \{\overline{t_i}\}$ should be critical. To verify the property of criticality, it is sufficient to check the satisfiability of $\mathrm{EC}_n\restriction_{\alpha_{i-1}} \setminus \{C_i\restriction_{\alpha_{i-1}}\}$:

$$\begin{aligned}\mathrm{EC}_n\restriction_{\alpha_{i-1}} \setminus \{C_i\restriction_{\alpha_{i-1}}\} &= \mathrm{EC}_n\restriction_{\alpha_{i-1}} \setminus \{\{\overline{t_i}\}\} \\ &= \{\{t_n\}\} \cup \{\{t_{j-1}, \overline{t_j}\} \mid j \in [i+1, n]\} \cup \{\{\overline{t_{j-1}}, t_j\} \mid j \in [i+1, n].\}\end{aligned}$$

It is easy to see that assigning 1 to all t_j, $j \in [i, n]$ leads to a satisfying assignment for this formula, since all clauses contain a positive literal. Thus, $C_i\restriction_{\alpha_{i-1}}$ is critical in $\mathrm{EC}_n\restriction_{\alpha_{i-1}}$ and α is a π-suitable assignment as desired.

Definition 37 ($^{\mathrm{il}}\chi^{\Phi}$)**.** *Let χ be a propositional formula with a set $\mathcal{C}$ of n critical clauses, $\mathcal{D} = \chi \setminus \mathcal{C}$ and a $\mathcal{C}$-suitable refutation π. Let $t_1, \dots, t_n$ and $C_1, \dots, C_n$ be the sequences of pivot variables and $\mathcal{C}$-parent clauses of $\mathcal{C}$-steps in π (in reverse order) and $T_0 = \mathsf{vars}(\chi) \setminus \{t_1, \dots, t_n\}$ as described in Definition 33. Let further $\Phi_n = (\phi_i)_{i \in [n]} = (\mathcal{P}_i \cdot \varphi_i)_{i \in [n]}$ be a sequence of variable disjoint QBF gadgets. We define*

$$\begin{aligned}^{\mathrm{il}}\chi^{\Phi} = &\exists T_0 (\mathcal{P}_1 \exists t_1) \dots (\mathcal{P}_n \exists t_n) \cdot \\ &\bigcup_{i \in [n]} [\varphi_i \times C_i] \cup \mathcal{D}.\end{aligned}$$

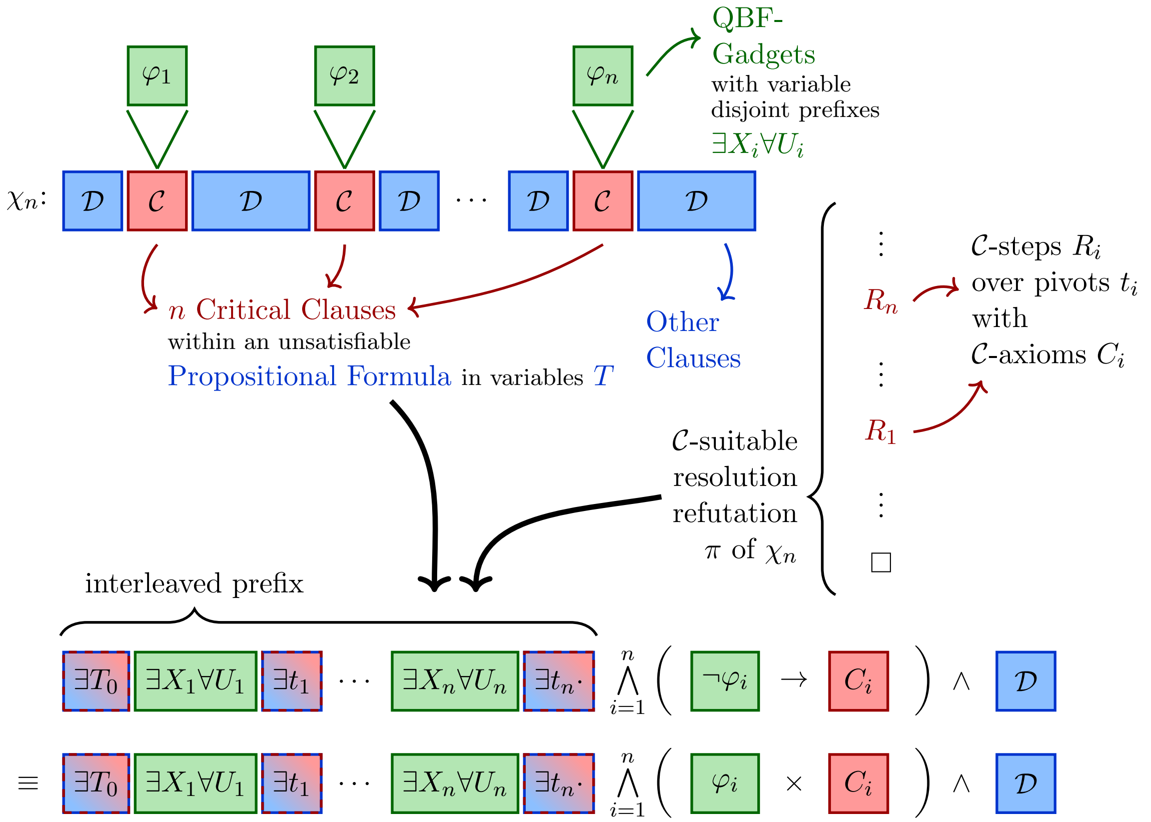

φ_1
φ_2
φ_n
QBF-Gadgets
with variable disjoint prefixes
$\exists X_i \forall U_i$
χ_n:
$\mathcal{D}$
$\mathcal{C}$
$\mathcal{D}$
$\mathcal{C}$
$\mathcal{D}$
$\cdots$
$\mathcal{D}$
$\mathcal{C}$
$\mathcal{D}$
n Critical Clauses
within an unsatisfiable
Propositional Formula in variables T
Other Clauses
$\vdots$
R_n
$\vdots$
R_1
$\vdots$
$\Box$
$\mathcal{C}$-steps R_i
over pivots t_i
with
$\mathcal{C}$-axioms C_i
$\mathcal{C}$-suitable resolution refutation π of χ_n
interleaved prefix
$\exists T_0$ $\exists X_1 \forall U_1$ $\exists t_1$ $\cdots$ $\exists X_n \forall U_n$ $\exists t_n \cdot$ $\bigwedge_{i=1}^{n} \left(\neg\varphi_i \rightarrow C_i \right) \wedge \mathcal{D}$
$\equiv$ $\exists T_0$ $\exists X_1 \forall U_1$ $\exists t_1$ $\cdots$ $\exists X_n \forall U_n$ $\exists t_n \cdot$ $\bigwedge_{i=1}^{n} \left(\varphi_i \times C_i \right) \wedge \mathcal{D}$

Figure 11: Construction principle of interleaved formulas from unsatisfiable propositional formulas with critical clauses $\mathcal{C}$ and a $\mathcal{C}$-suitable refutation π.

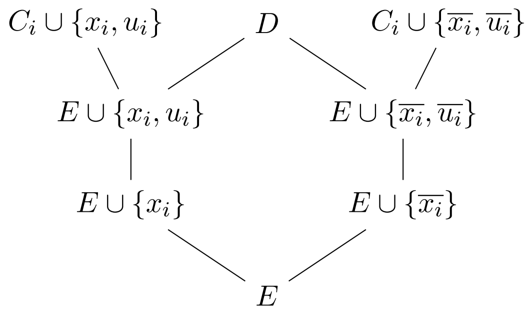

$C_i \cup \{x_i, u_i\}$
D
$C_i \cup \{\overline{x_i}, \overline{u_i}\}$
$E \cup \{x_i, u_i\}$
$E \cup \{\overline{x_i}, \overline{u_i}\}$
$E \cup \{x_i\}$
$E \cup \{\overline{x_i}\}$
E

Figure 12: Q-Res derivation of the resolvent E from EQ $\times$ C_i.

The construction principle of these interleaved formulas is illustrated in Figure 11.

Lemma 38. *For $n \in \mathbb{N}$ let Φ_n be a sequence of n variable disjoint QBF gadgets with polynomial-size Q-Res refutations and χ_n a propositional formula with polynomial-size resolution refutations. Let $\mathcal{C}$ with $|\mathcal{C}| = n$ be a set of critical clauses for χ_n and π a short $\mathcal{C}$-suitable resolution refutation of χ_n. Then ${}^{\text{il}}\chi_n^{\Phi}$, $n \in \mathbb{N}$ has polynomial-size Q-Res refutations.*

Proof. Let $\Phi_n = (\phi_i)_{i \in [n]} = (\mathcal{P}_i \cdot \varphi_i)_{i \in [n]}$ be a sequence of variable disjoint QBF gadgets with polynomial-size Q-Res refutations, χ_n a propositional formula with polynomial-size resolution refutations where $\mathsf{vars}(\chi_n) \cup \mathsf{vars}(\Phi_n) = \varnothing$ and $\mathcal{C}$, $\mathcal{D}$, π as described above. Let $C_1, \ldots, C_n$ and $t_1, \ldots, t_n$ be the sequences of axioms and pivots as described in Definition 33. We consider the $\mathcal{C}$-steps performed in π and show, that the resolvents can be derived in only a few more steps using axioms from ${}^{\text{il}}\chi_n^{\Phi}$ and Q-Res.

Let C_i be an axiom from $\mathcal{C}$ and D an axiom from $\mathcal{D}$ or a derived clause, where C_i and D are resolved with each other in π to the resolvent E. t_i is the pivot element to this resolution step. ${}^{\text{il}}\chi_n^{\Phi}$ contains $\varphi_i \times C_i$ instead of C_i. By first resolving all clauses of $\varphi_i \times C_i$ with D, we obtain $\varphi_i \times E$, thereby eliminating the pivot t_i. Since ϕ_i and χ_n are variable disjoint and all the T-variables are existential, this is easily possible. Since π is $\mathcal{C}$-suitable, E does not contain any variable t_j with $j > i$ (thanks to point (iv) of Definition 33). Now we can use the short refutation of φ_i by extending each clause in it by E. Since $\varphi_i \times E$ only contains variables from $\mathcal{P}_i$ and T, reduction steps within the derivation could – corresponding to the prefix – only be blocked by variables t_j, $j \geq i$. However, these are not contained in $\varphi_i \times E$. So at the end of the derivation we get the clause E instead of the empty clause – as desired.

Figure 12 illustrates the procedure using an equality gadget EQ $= \mathcal{P}_i.\varphi_i = \exists x_i \forall u_i \cdot \{\{x_i, u_i\}, \{\overline{x_i}, \overline{u_i}\}\}$.

In this way we can replace all resolution steps that use an axiom from $\mathcal{C}$. We get the same resolvents with only a few more steps (since the φ_i have short Q-Res refutations) and can connect the rest of π. Overall, we get a Q-Res refutation for ${}^{\text{il}}\chi_n^{\Phi}$ of the same order of magnitude (as π). This method can be found in the Q-Res refutations of all examples from Section 5.1. □

Lemma 39. *For $n \in \mathbb{N}$ let Φ_n be a sequence of n variable disjoint QBF gadgets and χ_n a propositional formula. Let $\mathcal{C}$ with $|\mathcal{C}| = n$ be a set of critical clauses for χ_n, π a short*

$\mathcal{C}$-suitable resolution refutation of χ_n and α a π-suitable assignment to the variables in $T = \mathsf{vars}(\chi_n)$. Then ${}^{\mathrm{il}}\chi_n^{\Phi}$, $n \in \mathbb{N}$ has exponential strategy size.

Proof. We can use a similar argumentation as in Theorem 12 to show that any winning strategy for ${}^{\mathrm{il}}\chi_n^{\Phi}$ is based on a combination of winning strategies for the ϕ_i formulas (but we have to take into account that the prefix does not collect the T-variables at the end and therefore need the π-suitability of α).

Let $\Phi_n = (\phi_i)_{i\in[n]} = (\mathcal{P}_i \cdot \varphi_i)_{i\in[n]}$ be a sequence of variable disjoint QBF gadgets, χ_n a propositional formula and $\mathcal{C}$, $\mathcal{D}$, π, α as described above. Let further T, T_i for $i \in [0, n]$ be the variable sets and α_i for $i \in [0, n]$ the restrictions of α as introduced in Definitions 33 and 35. It is obvious, that assigning u_i according to a winning strategy for ϕ_i for each $i \in [n]$ is a universal winning strategy on ${}^{\mathrm{il}}\chi_n^{\Phi}$ with exponential size (since the gadgets are non-constant). We assume (for contradiction), there is a winning strategy S assigning u_i different from any winning strategy for ϕ_i for some $i \in [n]$ (we consider the smallest i with this property). Then all clauses from $\varphi_i \times C_i$ are satisfied (since φ_i is satisfied). We assume that the existential player has followed α_{i-1} on T_0 and $t_1, \ldots, t_{i-1}$. But since α is π-suitable, we know $C_i\restriction_{\alpha_{i-1}}$ is critical in $\chi_n\restriction_{\alpha_{i-1}}$. That means $\chi_n\restriction_{\alpha_{i-1}} \setminus \{C_i\restriction_{\alpha_{i-1}}\}$ is satisfiable with some assignment α' to the remaining variables $t_i, \ldots, t_n$. Since the clauses $\varphi_i \times C_i$ are already satisfied by the universal assignment, the existential player wins the assignment game with α' and an arbitrary assignment to the remaining existential variables. Thus S is not a winning strategy. □

The formulas for simple contradiction and equivalence chain from Section 3 satisfy the required properties, where the naming of the clauses identifies $\mathcal{C}$ and $\mathcal{D}$ and the related π and α should be obvious[7]. While interleaved equality formulas (Beyersdorff et al., 2019) are an instantiation of ${}^{\mathrm{il}}\chi_n^{\Phi}$-formulas already known from literature, we present some new examples in Section 5.1.

Although we need the interleaved formulas mainly as a basis for separating Q-Res and QU-Res, they also have some noteworthy property, which follows from Theorem 27 together with the fact that all these formulas have exponential strategy size:

Theorem 40. *For $n \in \mathbb{N}$ let Φ_n be a sequence of n variable disjoint QBF gadgets with polynomial-size Q-Res refutations and χ_n a propositional formula with polynomial-size resolution refutations. Let $\mathcal{C}$ with $|\mathcal{C}| = n$ be a set of critical clauses for χ_n and π a short $\mathcal{C}$-suitable resolution refutation of χ_n. Let additionally a π-suitable assignment to the variables in $T = \mathsf{vars}(\chi_n)$ exist. Then ${}^{\mathrm{il}}\chi_n^{\Phi}$, $n \in \mathbb{N}$ separate tree-like from dag-like Q-Res.*

Proof. This follows immediately from Lemmas 38 and 39 and Theorem 27. □

The formulas from Examples 30 to 32 shown in Section 5.1 satisfy the conditions of Theorem 40, thus they separate treelike from dag-like Q-Res.

[7] Note that the formulas for implication chain (IC_n) can't be used within this pattern. As already mentioned in Section 5.1 this is due to the indexing policy - by simply shifting the index by two and renaming the clauses of index n to $\mathcal{D} = \{\{\overline{t_0}\}, \{t_n\}\}$ and $C_i = \{t_{i-1}, \overline{t_i}\}$ for $i \in [n]$ they get usable.

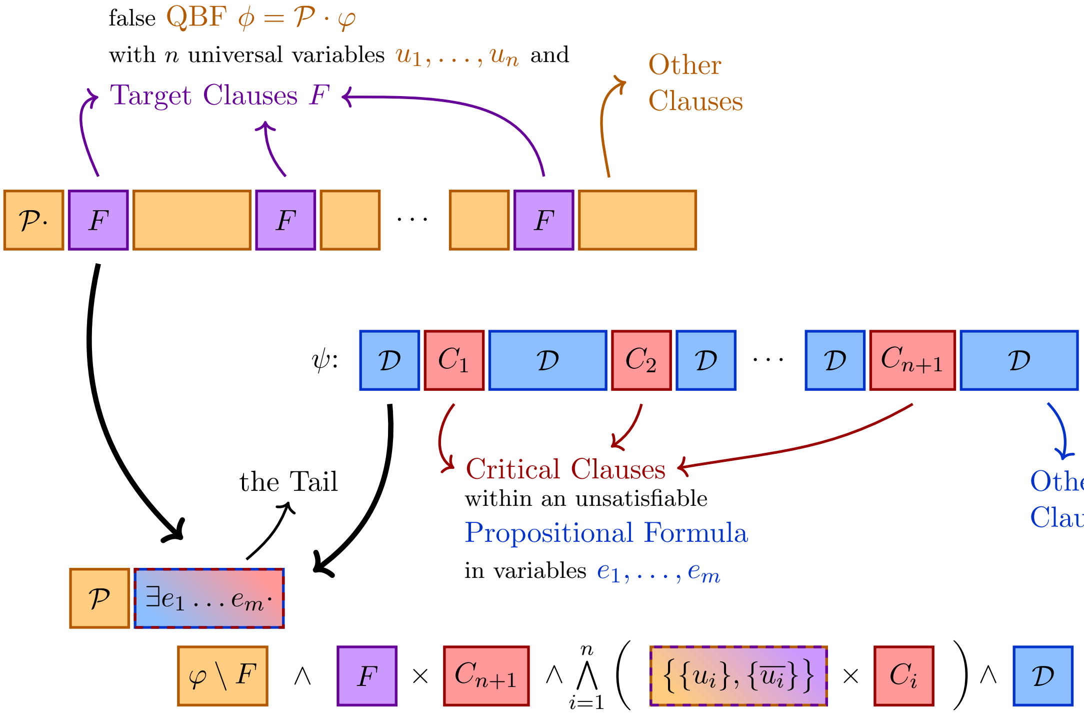

false QBF $\phi = \mathcal{P} \cdot \varphi$
with n universal variables $u_1, \ldots, u_n$ and
Target Clauses F
Other Clauses
$\mathcal{P}\cdot$
F
F
$\cdots$
F
ψ:
$\mathcal{D}$
C_1
$\mathcal{D}$
C_2
$\mathcal{D}$
$\cdots$
$\mathcal{D}$
C_{n+1}
$\mathcal{D}$
Critical Clauses
within an unsatisfiable
Propositional Formula
in variables $e_1, \ldots, e_m$
Other Clauses
the Tail
$\mathcal{P}$
$\exists e_1 \ldots e_m \cdot$
$\varphi \setminus F \quad \wedge \quad F \times C_{n+1} \wedge \bigwedge_{i=1}^{n} \left(\{\{u_i\}, \{\overline{u_i}\}\} \times C_i \right) \wedge \mathcal{D}$

Figure 13: Design idea of the Tail Construction.

5.3 Separating Formulas

In a second step we will use the QBFs with short Q-Res refutations and exponential strategy size to construct separating formulas between Q-Res and QU-Res. Our method is inspired by the structure of the KBKF formulas (Kleine Büning et al., 1995). We first define the concept of target clauses.

Definition 41 (Target Clauses). *For a false QBF $\phi = \mathcal{P} \cdot \varphi$ let F be a set of clauses such that the existential player has a strategy to never lose on clauses from $\phi \setminus F$ in any assignment game (regardless of the strategy chosen by the universal player), i.e., the existential player will always lose on clauses in F. We call F a set of* target clauses.

Notice that F is in general not unique. It is always possible to choose $F = \varphi$. Based on this, the construction is remarkably simple (it is illustrated in Figure 13):

Definition 42 (Tail Construction). *Let $\phi = \mathcal{P} \cdot \varphi$ be a false QBF with universal variables $\mathsf{vars}_\forall(\phi) = \{u_1, \ldots, u_n\}$ and ψ an unsatisfiable propositional formula with $n + 1$ critical clauses $\mathcal{C} = \{C_1, \ldots, C_{n+1}\}$, $\mathcal{D} = \psi \setminus \mathcal{C}$ and variables $\mathsf{vars}(\psi) = \{e_1, \ldots, e_m\}$ where $\mathsf{vars}(\phi) \cap \mathsf{vars}(\psi) = \varnothing$. Let further F be a set of target clauses for ϕ. Then we call*

$$\begin{aligned}\phi_\psi^{\mathsf{tail}} =& \mathcal{P}_\psi^{\mathsf{tail}} \cdot \varphi_\psi^{\mathsf{tail}} \\ =& \mathcal{P} \exists e_1 \ldots e_m \cdot (\varphi \setminus F) \cup (F \times C_{n+1}) \cup \left(\bigcup_{i \in [n]} \{\{u_i\}, \{\overline{u_i}\}\} \times C_i \right) \cup \mathcal{D}\end{aligned}$$

the ψ-tailed version $\phi_{\psi}^{\mathrm{tail}}$ *of* ϕ.

Although the choice of $F = \varphi$ will not significantly increase the size of the resulting formula, i.e., we always have $|\phi_{\psi}^{\mathrm{tail}}| \in \mathcal{O}(|\phi|)$, it makes sense to choose F as small as possible. These tailed formulas have exactly the properties we aim for (if we choose a suitable ϕ):

Theorem 43. *For $n \in \mathbb{N}$ let $\phi_{\psi,n}^{\mathrm{tail}}$ be tailed versions of formulas ϕ_n as described in Definition 42, where ϕ_n requires super-polynomial strategy size, but has polynomial-size* Q-Res *refutations and ψ_n has polynomial-size resolution refutations. Then $\phi_{\psi,n}^{\mathrm{tail}}$ separates* Q-Res *from* QU-Res*, i.e., $\phi_{\psi,n}^{\mathrm{tail}}$ requires super-polynomial size* Q-Res *refutations, but has polynomial-size* QU-Res *refutations.*

We will split the proof of Theorem 43 into two parts, first showing hardness for Q-Res of the constructed formulas and afterwards constructing short QU-Res proofs.

To show hardness of $\phi_{\psi,n}^{\mathrm{tail}}$ for Q-Res, we modify $\phi_{\psi}^{\mathrm{tail}}$ once more, similarly as described by Balabanov, Widl, and Jiang (2014) for the KBKF formulas. That is, we use new variables $v_1, \ldots, v_n$ and put them into the formula as copies of the universal variables $u_1, \ldots, u_n$. While Balabanov et al. (2014) create $\forall u_i v_i$ from each $\forall u_i$ in the prefix, we group the universal copies in a (possibly additional) universal quantification block to the right of $\mathcal{P}$ (and to the left of the existential tail variables), similarly as in shown by Beyersdorff et al. (2019), i.e., $\mathcal{P}_{\psi}^{\mathrm{tail}} = \mathcal{P}\exists e_1 \ldots e_m$ becomes $\mathcal{P}_{\psi}^{\mathrm{double}} = \mathcal{P}\forall v_1 \ldots v_n \exists e_1 \ldots e_m$. In addition, the occurrences of u_i in the matrix are effectively doubled, i.e., $\varphi_{\psi}^{\mathrm{double}}$ contains for each clause $C \in \varphi_{\psi}^{\mathrm{tail}}$ the extended clause $\mathrm{dupl}\,(C) := C \cup \{v_i : u_i \in C\} \cup \{\overline{v_i} : \overline{u_i} \in C\}$. We extend the $\mathrm{dupl}\,()$ function to clause sets S via $\mathrm{dupl}\,(S) := \{\mathrm{dupl}\,(C) \mid C \in S\}$.

Definition 44 ($\phi_{\psi}^{\mathrm{double}}$)**.** *For any QBF $\phi_{\psi}^{\mathrm{tail}} = \mathcal{P}_{\psi}^{\mathrm{tail}} \cdot \varphi_{\psi}^{\mathrm{tail}}$ constructed from a QBF $\phi = \mathcal{P} \cdot \varphi$ following Definition 42 we define*

$$\begin{aligned}\phi_{\psi}^{\mathrm{double}} = \mathcal{P}_{\psi}^{\mathrm{double}} \cdot \varphi_{\psi}^{\mathrm{double}} &= \mathcal{P}\forall v_1 \ldots v_n \exists e_1 \ldots e_m \cdot \mathrm{dupl}\left(\varphi_{\psi}^{\mathrm{tail}}\right)\\ &= \mathcal{P}\forall v_1 \ldots v_n \exists e_1 \ldots e_m \cdot \mathrm{dupl}\,(\varphi \setminus F) \cup \mathrm{dupl}\,(F \times C_{n+1})\\ &\qquad \cup \left(\bigcup_{i \in [n]} \{\{u_i, v_i\}, \{\overline{u_i}, \overline{v_i}\}\} \times C_i\right) \cup \mathcal{D}.\end{aligned}$$

Moving the universal variable copies to the right into a common universal block can only shorten QU-Res refutations, since it might enable additional universal reductions, but can never block a reduction previously possible. We then use Theorem 3 to show that $\phi_{\psi}^{\mathrm{double}}$ requires long QU-Res proofs. To do so, we first show:

Lemma 45. *Let $\phi_{\psi}^{\mathrm{tail}}$ be a QBF constructed from ϕ and ψ following Definition 42 and let $\phi_{\psi}^{\mathrm{double}}$ be as described in Definition 44. Then in the assignment game for $\phi_{\psi}^{\mathrm{double}}$ the existential player can force the universal player to*

(i) follow a winning strategy for ϕ on $u_1, \ldots, u_n$ and

(ii) assign $v_i = u_i$ for every $i \in [n]$.

Proof. We first show (i). Consider the assignment game on $\mathcal{P}$. If the universal player does not use a winning strategy on ϕ, he will lose on ϕ. Thus the assignment α constructed on $\mathcal{P}$ will satisfy φ and thus all the clauses in $\operatorname{dupl}(\varphi \setminus F)$ and $\operatorname{dupl}(F \times C_{n+1})$, because these are just weakenings of clauses from φ. The remaining clauses are $\bigcup_{i\in[n]} \{\{u_i, v_i\}, \{\overline{u_i}, \overline{v_i}\}\} \times C_i$ and $\mathcal{D}$. Since $C_1, \ldots, C_{n+1}$ are critical clauses in ψ, $\psi \setminus \{C_{n+1}\} = \{C_i \mid i \in [n]\} \cup \mathcal{D}$ is satisfiable. All variables occurring in this clause set are quantified existentially in the last (i.e. right most) block. Therefore, the existential player can choose an assignment to this variables, which satisfies $\psi \setminus \{C_{n+1}\}$ and thus as well $\left(\bigcup_{i\in[n]} \{\{u_i, v_i\}, \{\overline{u_i}, \overline{v_i}\}\} \times C_i\right) \cup \mathcal{D}$. This immediately makes the existential player the winner.

For (ii) again we consider the game on $\mathcal{P}$. Now we assume that the existential player plays according to his strategy on ϕ to only lose on clauses in F. Since F is a target set, we know that such a strategy exists. Let α be the assignment constructed on $\mathcal{P}$ (by both the existential and the universal player). By definition of target clauses α does not falsify any clause $C \in \varphi \setminus \{F\}$; these are also part of $\varphi_\psi^{\text{tail}}$. α also satisfies the corresponding clauses $\operatorname{dupl}(\varphi \setminus F)$ in $\phi_\psi^{\text{double}}$. Thus, the remaining clauses are $\operatorname{dupl}(F \times C_{n+1})$, the additional clauses $\bigcup_{i\in[n]} \{\{u_i, v_i\}, \{\overline{u_i}, \overline{v_i}\}\} \times C_i$ and $\mathcal{D}$. Now assume towards a contradiction that the universal player assigns $v_j \neq u_j$ for some $j \in [n]$. Since $C_1, \ldots, C_{n-1}$ are critical clauses of ψ, there is an assignment to $\{e_1, \ldots, e_m\}$ that satisfies $\psi \setminus \{C_j\}$. Let the existential player choose this assignment. Then C_j is falsified, but since $u_j \neq v_j$ each of the clauses $C_j \cup \{u_j, v_j\}$, $C_j \cup \{\overline{u_j}, \overline{v_j}\}$ is still satisfied, as is any other clause mentioned above. □

Lemma 46. *Let ϕ, ψ, ϕ_ψ^{tail}, and $\phi_\psi^{\text{double}}$ be as in Lemma 45. Then* QU-Res *proof size of $\phi_\psi^{\text{double}}$ is at least $\rho(\phi)$.*

Proof. According to Lemma 45 the universal player has to assign $u_1, \ldots, u_n$ according to a ϕ-strategy and $v_i = u_i$ for $i \in [n]$. Thus the cost of $\phi_\psi^{\text{double}}$ is at least $\rho(\phi)$, because the whole strategy is pooled in the last universal block. Now we can use the cost/size argument (Theorem 3) and obtain that proof size of $\phi_\psi^{\text{double}}$ in QU-Res is at least $\rho(\phi)$. □

We can now prove the lower bound for ϕ_ψ^{tail}, following an approach described by Beyersdorff et al. (2019).

Lemma 47. *Let $\phi_\psi^{\text{tail}} = \mathcal{P}_\psi^{\text{tail}} \cdot \varphi_\psi^{\text{tail}}$ be a QBF constructed from $\phi = \mathcal{P} \cdot \varphi$ and ψ according to Definition 42. Then proof size of ϕ_ψ^{tail} in* Q-Res *is at least $\frac{1}{2}\rho(\phi)$.*

Proof. Suppose that proof size of ϕ_ψ^{tail} in Q-Res was smaller than $\frac{1}{2}\rho(\phi)$ and let π be such a short Q-Res refutation. To obtain the empty clause all universal variables must be reduced by universal reduction in π (there is no other option, which is the decisive difference to QU-Res). But then we can construct a Q-Res proof π' for $\phi_\psi^{\text{double}}$ by just doubling all reduction steps in π in the sense of introducing an additional reduction step for v_i as soon as u_i is reduced. That is always possible, because v_i is never quantified left from u_i. The remainder of the proof can be left unchanged, since the variable copies $(v_i, \overline{v_i})$ cannot cause any tautologies that would not also be caused by the originals $(u_i, \overline{u_i})$. The proof constructed in this way remains in the same order of magnitude as the original one, more precisely $|\pi'| \leq 2|\pi| < \rho(\phi)$ in contradiction to the above observation of Lemma 46. Thus any Q-Res refutation for ϕ_ψ^{tail} has size at least $\frac{1}{2}\rho(\phi)$. □

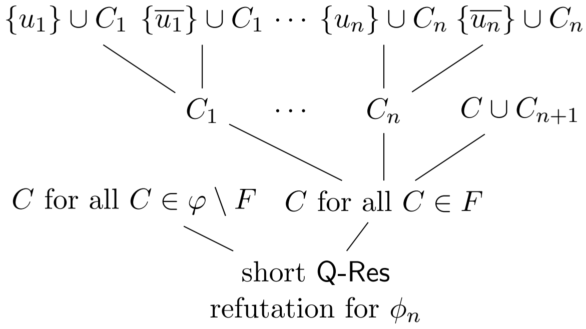


Figure 14: Polynomial-size QU-Res refutations for $\phi^{\text{tail}}_{\psi,n}$.

Lemma 47 in combination with the conditions from Theorem 43 (i.e., exponential strategy size of ϕ_n) implies Q-Res-hardness of $\phi^{\text{tail}}_{\psi}$:

Corollary 48 ($\phi^{\text{tail}}_{\psi,n}$ is Hard for Q-Res)**.** *For $n \in \mathbb{N}$ let $\phi^{\text{tail}}_{\psi,n}$ be tailed versions constructed from ϕ_n and ψ_n following the rules and conditions from Theorem 43. Then $\phi^{\text{tail}}_{\psi,n}$ requires exponential-size Q-Res refutations.*

Let us now prove the upper bound stated in Theorem 43:

Lemma 49 ($\phi^{\text{tail}}_{\psi,n}$ has Short QU-Res Refutations)**.** *If for $n \in \mathbb{N}$ $\phi^{\text{tail}}_{\psi,n}$ are QBFs constructed from ϕ_n and ψ_n following the rules and conditions from Theorem 43, then $\phi^{\text{tail}}_{\psi,n}$ has polynomial-size QU-Res refutations.*

Proof. $\phi_n = \mathcal{P} \cdot \varphi_n$ has by assumption short Q-Res proofs. $\phi^{\text{tail}}_{\psi,n}$ additionally contains the clauses $\{u_i\} \cup C_i$ and $\{\overline{u_i}\} \cup C_i$ for all $i \in [n]$, from which we can get all the clauses $C_i, i \in [n]$ in only n universal resolution steps (available in QU-Res). We then remove all the additional literals from the clauses $F \times C_{n+1}$ originated from F, which needs $|F|$ times as many resolution steps as the short refutation of ψ_n. Together with the unchanged clauses from $\varphi_n \setminus F$ we now derived all clauses from φ_n and can proceed with the short Q-Res refutation of ϕ_n. Overall the proof of ϕ_n is extended by polynomially many steps. Therefore we get a polynomial-size QU-Res refutation of $\phi^{\text{tail}}_{\psi,n}$. The composition of the proof is shown in Figure 14.

□

Proof of Theorem 43. The theorem follows from Corollary 48 and Lemma 49. □

5.4 Examples

We illustrate our construction on the interleaved equality formulas from Beyersdorff et al. (2019), which we already discussed in Section 5.1:

Example 50 (SC-Tailed Equality)**.** *We first need suitable formulas, on which we can use the tail construction:*

$$\phi_n = (\exists x_1 \forall u_1 \exists t_1) \dots (\exists x_n \forall u_n \exists t_n) \cdot \left(\bigcup_{i \in [n]} \{\{x_i, u_i, \overline{t_i}\}, \{\overline{x_i}, \overline{u_i}, \overline{t_i}\}\} \right) \cup \{\{t_1, \dots, t_n\}\}\,.$$

As mentioned in Section 5.1, these are exactly the ${}^{\mathrm{il}}\mathrm{SC}_n^{\mathrm{EQ}}$*-formulas, i.e., they have exponential strategy size and short* Q-Res *refutations. Thus, they meet the requirements for constructing separating formulas according to the above method. The existential player has a strategy to satisfy all clauses except for* $\{x_n, u_n, \overline{t_n}\}$, $\{\overline{x_n}, \overline{u_n}, \overline{t_n}\}$ *and* $\{t_1, \dots, t_n\}$ *in any game (by just setting* $t_i = 0$ *for* $i < n$*). With* $u_n = x_n$ *we get the following possible assignments:*

- $x_n = u_n = 1, t_n = 1$ *falsifies* $\{\overline{x_n}, \overline{u_n}, \overline{t_n}\}$,
- $x_n = u_n = 0, t_n = 1$ *falsifies* $\{x_n, u_n, \overline{t_n}\}$ *and*
- $x_n = u_n, t_n = 0$ *falsifies* $\{t_1, \dots, t_n\}$.

The remaining two clauses are satisfied in each case. Thus there are three possibilities for a minimal set F *of target clauses, containing one of these three clauses. The most intuitive choice for* F *is* $F = \{\{t_1, \dots, t_n\}\}$*. As a template for the tail, we use the simple contradiction formulas from Section 3.1 (note that we slightly change the naming of the clauses:* $C_i = \{\overline{e_i}\}$ *for* $i \in [n]$ *and* $C_{n+1} = \{e_1, \dots, e_n\}$*). The tail construction then leads to the following formulas, separating* Q-Res *and* QU-Res*:*

$$\phi^{\mathrm{tail}}_{\mathrm{SC},n} = \left({}^{\mathrm{il}}\mathrm{SC}^{\mathrm{EQ}}\right)^{\mathrm{tail}}_{\mathrm{SC},n} = (\exists x_1 \forall u_1 \exists t_1) \dots (\exists x_n \forall u_n \exists t_n) \exists e_1 \dots e_n \cdot \left(\bigcup_{i \in [n]} \{\{x_i, u_i, \overline{t_i}\}, \{\overline{x_i}, \overline{u_i}, \overline{t_i}\}, \{u_i, \overline{e_i}\}, \{\overline{u_i}, \overline{e_i}\}\} \right) \cup \{\{t_1, \dots, t_n, e_1, \dots, e_n\}\}.$$

Example 51 (IC-Tailed Equality)**.** *We could also use another propositional template to tail the* ${}^{\mathrm{il}}\mathrm{SC}_n^{\mathrm{EQ}}$*-formulas, e.g. implication chain formulas from Section 3.1. With* $F = \{\{t_1, \dots, t_n\}\}$ *again and* $\psi = \mathrm{IC}_{n+1} = \bigcup_{i \in [n+1]} \{C_i\}$ *with* $C_i = \{e_{i-1}, \overline{e_i}\}$ *for* $i \in [1, n-1]$ *and* $C_n = \{\overline{e_0}\}$, $C_{n+1} = \{e_{n-1}\}$ *we get the following formulas, separating* Q-Res *and* QU-Res*:*

$$\phi^{\mathrm{tail}}_{\mathrm{IC},n} = \left({}^{\mathrm{il}}\mathrm{SC}^{\mathrm{EQ}}\right)^{\mathrm{tail}}_{\mathrm{IC},n} = (\exists x_1 \forall u_1 \exists t_1) \dots (\exists x_n \forall u_n \exists t_n) \exists e_0 \dots e_n \cdot \left(\bigcup_{i \in [1,n]} \{\{x_i, u_i, \overline{t_i}\}, \{\overline{x_i}, \overline{u_i}, \overline{t_i}\}\} \right) \cup \left(\bigcup_{i \in [1,n-1]} \{\{u_i, e_{i-1}, \overline{e_i}\}, \{\overline{u_i}, e_{i-1}, \overline{e_i}\}\} \right) \cup \{\{u_n, \overline{e_0}\}, \{\overline{u_n}, \overline{e_0}\}\} \cup \{\{t_1, \dots, t_n, e_{n-1}\}\}.$$

Interestingly, the KBKF formulas (Kleine Büning et al., 1995) correspond to the tail construction with simple contradiction formulas, where we just flip positive and negative literals (SC′ formulas). They actually inspired our construction:

Example 52 (KBKF). *The KBKF formulas presented by Kleine Büning et al. (1995) are defined as*

$$\phi^{\text{tail}}_{\text{SC}',n} = \text{KBKF}_n = \exists y_0 (\exists y_1 y_1' \forall u_1) \dots (\exists y_n y_n' \forall u_n) \exists y_{n+1} \dots y_{n+n} \cdot \bigcup_{i \in [0,2n]} \{C_i, C_i'\}$$

where the matrix clauses are defined as follows:

$$\begin{aligned} C_0 &= \{\overline{y_0}\} & C_0' &= \{y_0, \overline{y_1}, \overline{y_1'}\} \\ C_k &= \{y_k, \overline{u_k}, \overline{y_{k+1}}, \overline{y_{k+1}'}\} & C_k' &= \{y_k', u_k, \overline{y_{k+1}}, \overline{y_{k+1}'}\} \\ C_n &= \{y_n, \overline{u_n}, \overline{y_{n+1}}, \dots, \overline{y_{n+n}}\} & C_n' &= \{y_n', u_n, \overline{y_{n+1}}, \dots, \overline{y_{n+n}}\} \\ C_{n+t} &= \{\overline{u_t}, y_{n+t}\} & C_{n+t}' &= \{u_t, y_{n+t}\} \end{aligned}$$

with $1 \leq k < n$ and $1 \leq t \leq n$. We now immediately see, that some parts of the formula equal those constructed in Section 5. Especially the variables $y_{n+1}, \dots, y_{n+n}$ correspond to those called $e_1, \dots, e_m$ in Section 5, which make up the tail. We examine the basic formula, whose modification according to the tail construction leads to the KBKF formulas:

$$\phi_n = \exists y_0 (\exists y_1 y_1' \forall u_1) \dots (\exists y_n y_n' \forall u_n) \cdot \bigcup_{i \in [0 \dots n]} \{D_i, D_i'\}$$

with

$$\begin{aligned} D_0 &= C_0 {=} \{\overline{y_0}\} & D_0' &= C_0' {=} \{y_0, \overline{y_1}, \overline{y_1'}\} \\ D_k &= C_k {=} \{y_k, \overline{u_k}, \overline{y_{k+1}}, \overline{y_{k+1}'}\} & D_k' &= C_k' {=} \{y_k', u_k, \overline{y_{k+1}}, \overline{y_{k+1}'}\} \\ D_n & {=} \{y_n, \overline{u_n}\} & D_n' & {=} \{y_n', u_n\} \end{aligned}$$

for $1 \leq k < n$.

ϕ_n is also a false QBF and the existential player can force the universal player to follow the same strategy as in KBKF: setting $u_k = y_k'$ for each $k \in [n]$. (Note that this is not a unique winning strategy, since the existential player could leave the universal player a wide range of freedom in assigning the universal variables.) To force the universal player assigning variables according to the KBKF-strategy, the existential player will assign $y_0 = 0$ and $y_k' \neq y_k$ in every round $k \in [n]$. The last remaining clauses are $D_n = \{y_n, \overline{u_n}\}$ and $D_n' = \{y_n', u_n\}$, and every so constructed assignment falsifies exactly one of them: $y_n = 0$, $y_n' = 1 = u_n$ falsifies D_n and $y_n = 1$, $y_n' = 0 = u_n$ falsifies D_n'; in each case the other clause is satisfied. Thus it is sufficient for the set F of target clauses to contain one of the two clauses. For KBKF $F = \{D_n, D_n'\}$ was chosen (which is not minimal), which makes the tail construction with SC' as propositional tail pattern formula generating just the KBKF formulas. Polynomial-size Q-Res refutations of ϕ_n are shown in Figure 15.

Hence ϕ_n, $n \in \mathbb{N}$ has exponential strategy size and short Q-Res refutations, thus satisfying the conditions of the tail construction. It follows immediately, that the KBKF formulas separate Q-Res from QU-Res.

As an aside we see that F can be minimized, i.e., the negative literals $\overline{y_{n+1}}, \dots, \overline{y_{n+n}}$ can be removed from one of the clauses C_n or C_n' without affecting the separation property.

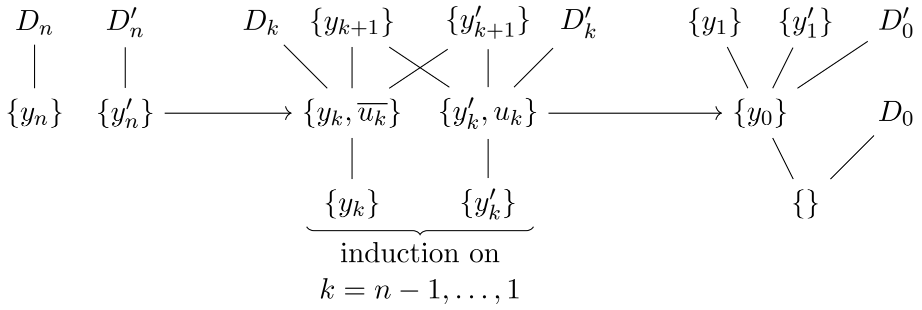


Figure 15: Polynomial-size Q-Res refutation of the base formulas ϕ_n of KBKF_n.

6. Conclusion and Open Problems

While our construction of hard formulas in Section 3 yields a large class of hard QBFs, it does not allow to generate all hard QBFs. One apparent limitation is that we only produce Σ_3^b formulas. While this is arguably the most interesting case, it would be worthwhile to explore systematically how to construct hard QBFs with higher quantifier complexity. While it is easy to derive such formulas from Σ_3^b QBFs by just adding further dummy quantifiers, 'more natural' constructions appear of interest.

A related question is which exact class of formulas can be generated by our construction. As we always import hardness via the size-cost method, one might aim for a construction that yields all such formulas. We do not achieve this yet, as one can even find Σ_3^b-formulas with high costs that do not stem from our method. Of course there are also further sources of hardness. E.g. the parity formulas (Beyersdorff et al., 2019) are hard for QU-Res, but have small cost. Finding general constructions for other QBF families, where hardness does not originate from cost, also appears interesting for future work.

7. Acknowledgments

This research was supported by the Carl-Zeiss Foundation and DFG grant BE 4209/3-1. We would like to express our appreciation to the anonymous reviewers for their helpful comments and constructive feedback, which contributed to the improvement of Section 5.2 and hopefully increased its comprehensibility. An extended abstract of this paper has been published in the proceedings of SAT (Schleitzer & Beyersdorff, 2022).

References

Abbasizanjani, H. (2021). *The combinatorics of minimal unsatisfiability: connecting to graph theory.* dissertation, Department of Computer Science, Swansea University.

Abbasizanjani, H., & Kullmann, O. (2018). Minimal unsatisfiability and minimal strongly connected digraphs. In Beyersdorff, O., & Wintersteiger, C. M. (Eds.), *Theory and Applications of Satisfiability Testing (SAT)*, Vol. 10929 of *Lecture Notes in Computer Science*, pp. 329–345. Springer.

Abbasizanjani, H., & Kullmann, O. (2020). Classification of minimally unsatisfiable 2-cnfs. *CoRR*, *abs/2003.03639*.

Atserias, A., Fichte, J. K., & Thurley, M. (2011). Clause-learning algorithms with many restarts and bounded-width resolution. *J. Artif. Intell. Res.*, *40*, 353–373.

Balabanov, V., & Jiang, J.-H. R. (2012). Unified QBF certification and its applications. *Formal Methods in System Design*, *41*(1), 45–65.

Balabanov, V., Widl, M., & Jiang, J.-H. R. (2014). QBF resolution systems and their proof complexities. In *Proc. Theory and Applications of Satisfiability Testing (SAT)*, pp. 154–169.

Beame, P., & Pitassi, T. (1996). Simplified and improved resolution lower bounds. In *Proc. 37th IEEE Symposium on the Foundations of Computer Science*, pp. 274–281. IEEE Computer Society Press.

Beame, P., Kautz, H. A., & Sabharwal, A. (2004). Towards understanding and harnessing the potential of clause learning. *J. Artif. Intell. Res. (JAIR)*, *22*, 319–351.

Beyersdorff, O., & Blinkhorn, J. (2020). Lower bound techniques for QBF expansion. *Theory Comput. Syst.*, *64*(3), 400–421.

Beyersdorff, O., & Blinkhorn, J. (2021). A simple proof of QBF hardness. *Information Processing Letters*, *168*.

Beyersdorff, O., Blinkhorn, J., & Hinde, L. (2019). Size, cost, and capacity: A semantic technique for hard random QBFs. *Logical Methods in Computer Science*, *15*(1).

Beyersdorff, O., Blinkhorn, J., & Mahajan, M. (2020). Hardness characterisations and size-width lower bounds for QBF resolution. In *Proc. ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pp. 209–223. ACM.

Beyersdorff, O., Blinkhorn, J., & Mahajan, M. (2021). Building strategies into QBF proofs. *J. Autom. Reasoning*, *65*(1), 125–154.

Beyersdorff, O., & Böhm, B. (2021). Understanding the Relative Strength of QBF CDCL Solvers and QBF Resolution. In *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, Vol. 185 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pp. 12:1–12:20.

Beyersdorff, O., Chew, L., & Janota, M. (2019). New resolution-based QBF calculi and their proof complexity. *ACM Transactions on Computation Theory*, *11*(4), 26:1–26:42.

Beyersdorff, O., & Hinde, L. (2019). Characterising tree-like Frege proofs for QBF. *Inf. Comput.*, *268*.

Beyersdorff, O., Hinde, L., & Pich, J. (2020). Reasons for hardness in QBF proof systems. *ACM Transactions on Computation Theory*, *12*(2).

Beyersdorff, O., Janota, M., Lonsing, F., & Seidl, M. (2021a). Quantified boolean formulas. In Biere, A., Heule, M., van Maaren, H., & Walsh, T. (Eds.), *Handbook of Satisfiability*, Frontiers in Artificial Intelligence and Applications, pp. 1177–1221. IOS Press.

Beyersdorff, O., Pulina, L., Seidl, M., & Shukla, A. (2021b). Qbffam: A tool for generating QBF families from proof complexity. In Li, C., & Manyà, F. (Eds.), *Theory and*

Applications of Satisfiability Testing (SAT), Vol. 12831 of *Lecture Notes in Computer Science*, pp. 21–29. Springer.

Bjørner, N., Janota, M., & Klieber, W. (2015). On conflicts and strategies in QBF. In Fehnker, A., McIver, A., Sutcliffe, G., & Voronkov, A. (Eds.), *20th International Conferences on Logic for Programming, Artificial Intelligence and Reasoning LPAR 2015*, Vol. 35 of *EPiC Series in Computing*, pp. 28–41. EasyChair.

Bonet, M. L., Esteban, J. L., Galesi, N., & Johannsen, J. (2000). On the relative complexity of resolution refinements and cutting planes proof systems. *SIAM J. Comput.*, *30*(5), 1462–1484.

Buss, S., & Nordström, J. (2021). Proof complexity and SAT solving. In Biere, A., Heule, M., van Maaren, H., & Walsh, T. (Eds.), *Handbook of Satisfiability*, Frontiers in Artificial Intelligence and Applications, pp. 233–350. IOS Press.

Chew, L. (2017). *QBF proof complexity.* Ph.D. thesis, University of Leeds, Leeds.

Chew, L., & Slivovsky, F. (2022). Towards uniform certification in QBF. In *39th International Symposium on Theoretical Aspects of Computer Science (STACS 2022).* Schloss Dagstuhl-Leibniz-Zentrum für Informatik.

Clymo, J. (2021). *Proof Complexity for Quantified Boolean Formulas.* Ph.D. thesis, School of Computing, University of Leeds.

Cook, S. A., & Nguyen, P. (2010). *Logical Foundations of Proof Complexity.* Cambridge University Press.

Cook, S. A., & Reckhow, R. A. (1979). The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, *44*(1), 36–50.

Egly, U., Lonsing, F., & Widl, M. (2013). Long-distance resolution: Proof generation and strategy extraction in search-based QBF solving. In *Proc. Logic for Programming, Artificial Intelligence, and Reasoning (LPAR)*, pp. 291–308.

Haken, A. (1985). The intractability of resolution. *Theoretical Computer Science*, *39*, 297–308.

Janota, M., & Marques-Silva, J. (2015). Expansion-based QBF solving versus Q-resolution. *Theor. Comput. Sci.*, *577*, 25–42.

Kleine Büning, H., Karpinski, M., & Flögel, A. (1995). Resolution for quantified Boolean formulas. *Inf. Comput.*, *117*(1), 12–18.

Krajíček, J. (1995). *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, Vol. 60 of *Encyclopedia of Mathematics and Its Applications.* Cambridge University Press, Cambridge.

Krajíček, J. (2019). *Proof complexity*, Vol. 170 of *Encyclopedia of Mathematics and Its Applications.* Cambridge University Press.

Lonsing, F., Egly, U., & Gelder, A. V. (2013). Efficient clause learning for quantified Boolean formulas via QBF pseudo unit propagation. In *Proc. International Conference on Theory and Applications of Satisfiability Testing (SAT)*, pp. 100–115.

Peitl, T., Slivovsky, F., & Szeider, S. (2019). Proof complexity of fragments of long-distance Q-resolution. In Janota, M., & Lynce, I. (Eds.), *Theory and Applications of Satisfiability Testing - SAT 2019 - 22nd International Conference, SAT, Proceedings*, Vol. 11628 of *Lecture Notes in Computer Science*, pp. 319–335. Springer.

Pipatsrisawat, K., & Darwiche, A. (2011). On the power of clause-learning SAT solvers as resolution engines. *Artif. Intell.*, *175*(2), 512–525.

Schleitzer, A., & Beyersdorff, O. (2022). Classes of hard formulas for QBF resolution. In Meel, K. S., & Strichman, O. (Eds.), *25th International Conference on Theory and Applications of Satisfiability Testing, SAT 2022, August 2-5, 2022, Haifa, Israel*, Vol. 236 of *LIPIcs*, pp. 5:1–5:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik.

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

Sipser, M. (2005). *Introduction to the Theory of Computation* (2nd edition). Course Technology.

Urquhart, A. (1987). Hard examples for resolution. *J. ACM*, *34*(1), 209–219.

Van Gelder, A. (2012). Contributions to the theory of practical quantified Boolean formula solving. In *Proc. Principles and Practice of Constraint Programming (CP)*, pp. 647–663.

Zhang, L., & Malik, S. (2002). Conflict driven learning in a quantified Boolean satisfiability solver. In *Proc. IEEE/ACM International Conference on Computer-aided Design (ICCAD)*, pp. 442–449.