

Classes of Hard Formulas for QBF Resolution

Agnes Schleitzer ✉

Institut für Informatik, Friedrich-Schiller-Universität Jena, Germany

Olaf Beyersdorff ✉ 

Institut für Informatik, Friedrich-Schiller-Universität Jena, Germany

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.

2012 ACM Subject Classification Theory of computation → Proof complexity

Keywords and phrases QBF, proof complexity, resolution, separations

Funding Agnes Schleitzer: DFG grant BE 4209/3-1

Olaf Beyersdorff: Carl-Zeiss Foundation and DFG grant BE 4209/3-1

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 [27] with many important connections to other fields, in particular to logic [26, 33] and solving [22]. 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 [4, 8, 22, 36] – there is a vast literature on hard formulas stemming from diverse areas such as combinatorics (e.g. [21, 29]), graph theory [39], logic [32], random formulas [7], and many more [33, 37].

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, [31]) and QU-Resolution (QU-Res, [40]) 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. [18] for a recent overview), with Q-Res and its extension long-distance Q-Resolution (LD-Q-Res, [5]) corresponding to quantified conflict-driven clause learning (QCDCL) (cf. [14, 18, 34, 41]).

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 [31] that introduced Q-Res. The other ‘notorious’ QBF families are the

46 equality formulas [11], the parity formulas [15], and the CR formulas [30]. Together these
 47 more or less comprise the formula toolbox of QBF proof complexity and are used for almost
 48 all of the known separations.

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

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

57 **Our Contributions.** Our contributions can be summarised as follows.

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

67 We then combine the propositional base formula with the QBF gadgets in a rather
 68 straightforward way to obtain Σ_3^b QBFs that require exponential-size proofs in Q-Res and
 69 QU-Res. The lower bound follows by the size-cost lower-bound technique [11] that always
 70 yields ‘genuine’ QBF lower bounds, i.e., our construction yields ‘genuinely’ hard QBFs in the
 71 sense discussed above.

72 We illustrate our method with a couple of examples. These include the equality for-
 73 mulas [11] (which actually inspired our construction), new circle, equivalence, and XOR
 74 formulas, as well as a large class of random QBFs.

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

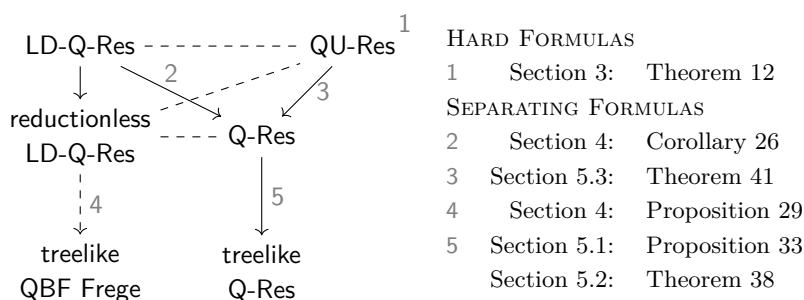
79 This should be welcome news as we previously knew of only very few formulas (essentially
 80 KBKF, equality, and parity) that separate Q-Res from LD-Q-Res [11, 15, 23, 28].

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

86 In comparison to our quite transparent method in (1) above, the technical details of
 87 these constructions are somewhat more involved. Yet again we obtain a large class of

¹ A track of crafted formulas was introduced into QBF Eval 2020 and a tool to generate the mentioned QBF families was presented in [19].

² A formal framework for ‘genuine’ QBF hardness was introduced in [17]. All the mentioned QBF examples – KBKF, equality, and parity – are genuinely hard in this sense.



■ **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; $A \dashv\vdash B$: A and B are incomparable; $A \dashv\rightarrow B$: B does not simulate A .

88 QBFs separating Q-Res and QU-Res. Previously, the KBKF formulas were the only known
 89 separating example [10,31,40]. Interestingly, all formulas we construct in (3) have unbounded
 90 quantifier complexity, which we know must be the case for a separation of QU-Res from
 91 Q-Res [12,25].

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

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

98 2 Preliminaries

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

101 **QBFs.** A *quantified Boolean formula (QBF)* in *closed prenex form* $\phi = \mathcal{P} \cdot \varphi$ consists
 102 of a *quantifier prefix* \mathcal{P} and a propositional formula φ , called the *matrix*. The prefix is
 103 a series of quantifiers $Q \in \{\forall, \exists\}$, each followed by a set of variables. For a *closed* QBF
 104 (which we only consider here), \mathcal{P} quantifies exactly the variables occurring in φ . Thus, for
 105 $\mathcal{P} = Q_1 X_1 Q_2 X_2 \dots Q_n X_n$, the matrix φ is a formula in variables $\bigcup_{i \in [n]} X_i$ and we write
 106 $\text{vars}(\mathcal{P} \cdot \varphi) = \text{vars}(\varphi) = \bigcup_{i \in [n]} X_i$. As there are no free variables in a closed QBF, it is either
 107 *true* or *false*. We write $\text{vars}_{\exists}(\varphi)$ for the set of existential variables in $\mathcal{P} \cdot \varphi$ and $\text{vars}_{\forall}(\varphi)$ for
 108 those associated with \forall . A QCNF is a QBF with a CNF matrix.

109 An *assignment* assigns truth values to variables. We denote by v^α the value of a variable
 110 v under an assignment α . We write $\langle V \rangle$ for the set of all possible assignments to V ,
 111 $\langle \chi \rangle = \langle \text{vars}(\chi) \rangle$ for the assignments of a propositional formula χ and $\langle \phi \rangle = \langle \mathcal{P} \cdot \varphi \rangle = \langle \varphi \rangle$ for
 112 those of a QBF $\phi = \mathcal{P} \cdot \varphi$. A clause C or a (propositional) formula χ can be restricted by an
 113 assignment α : $C \upharpoonright_\alpha := \{v \in C \mid v^\alpha = 0\} \cup \{\bar{v} \in C \mid v^\alpha = 1\}$ and $\chi \upharpoonright_\alpha := \{C \upharpoonright_\alpha \mid C \in \chi\}$.

114 Closed QBFs can be viewed as a game between an existential and a universal player
 115 generating a total assignment [38]. The players assign truth values to all variables in the order
 116 of the quantifier prefix (the existential player chooses the values for existential variables, the
 117 universal player those for universals). The existential player wins, if the generated assignment

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

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

118 satisfies the matrix; otherwise the universal player wins. For a closed QBF, there is always a
 119 *winning strategy* for one of the two players. We call this game the *assignment game*.

120 A countermodel is a winning strategy for the universal player. We define *strategy size* in
 121 accordance with [9]:

122 ► **Definition 1** (Strategy Size ρ [9]). *Let ϕ be a false QBF. We refer to the smallest cardinality*
 123 *of the range of a countermodel for ϕ as the strategy size $\rho(\phi)$ of ϕ .*

124 **Proof systems.** *Resolution (Res)* is a refutational proof system for propositional formulas
 125 with only two inference rules: For an input formula χ , we can derive any $C \in \chi$ as an axiom
 126 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
 127 over the pivot x .

128 *Q-Res* [31] transfers Resolution from propositional logic to QBF. It uses the resolution rule
 129 (Q-Res) which only allows existential pivots and forbids tautologous resolvents. Universal
 130 variables are eliminated by universal reduction (\forall Red). The rules are given in Figure 2.

131 *QU-Res* [40] extends the weaker system Q-Res by allowing resolution also over universal
 132 pivots in its resolution rule QU-Res. Nevertheless Q-Res is refutationally sound and complete.

133 *LD-Q-Res* [5] is an extension of Q-Res which allows long-distance resolution steps under
 134 certain conditions (see Figure 2 for the definition of the resolution rule LDQ-Res), allowing
 135 tautological resolvents. The \forall Red rule is modified such that merged universal literals from
 136 long distance steps can also be reduced under the same conditions as usual universal variables.

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

140 3 Construction of Hard Formulas for QU-Res

141 We start by recalling the lower-bound technique for QU-Res via cost from [11].

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

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

147 ► **Theorem 3** ([11]). *Let ϕ be a false QCNF. Then QU-Res refutations of ϕ have size at*
 148 *least $\text{cost}(\phi)$.*

149 The equality formulas from [11] have exponential cost and are therefore hard for QU-Res:

150 ► **Definition 4** (Equality formulas [11]). *For $n \in \mathbb{N}$ we define the n^{th} equality formula as*

$$151 \quad \text{EQ}_n = \exists x_1 \dots x_n \forall u_1 \dots u_n \exists t_1 \dots t_n \cdot \left(\bigcup_{i \in [n]} \{ \{x_i, u_i, \bar{t}_i\}, \{\bar{x}_i, \bar{u}_i, \bar{t}_i\} \} \right) \cup \{ \{t_1, \dots, t_n\} \}. \quad (1)$$

152 We take the equality formulas as a starting point and then subsequently generalize
 153 their construction. The underlying principle of the equality formulas is to enforce a unique
 154 universal winning strategy of exponential size. In the case of equality, the winning strategy is
 155 to assign $u_i = x_i$. The formulas can be understood as being based on a simple propositional
 156 formula consisting of the clause $\{t_1, \dots, t_n\}$ and unit clauses $\{\bar{t}_1\}, \dots, \{\bar{t}_n\}$, into which this
 157 exponential size winning strategy is injected through adding the x and u variables.

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

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

165 3.1 Suitable Propositional Formulas

166 Let us first formally define the afore mentioned critical clauses:

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

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

170 We now have a look at some suitable propositional formula families. We will denote the
 171 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.
 172 The subset of critical clauses can be chosen in more than one way, but for each example we
 173 make a specific choice that we will also use later in the construction of the hard QBFs.

174 The underlying propositional formulas from the equality formulas are:

175 ► **Example 6** (Simple Contradiction). $\text{SC}_n = \{D_1\} \cup \bigcup_{i \in [n]} \{C_i\}$ with $D_1 = \{t_1, \dots, t_n\}$ and
 176 $C_i = \{\bar{t}_i\}$ for $i \in [n]$. Note that SC_n is minimally unsatisfiable.

177 In addition, we consider two further running examples.

178 ► **Example 7** (Implication Chain). $\text{IC}_n = \bigcup_{i \in [n]} \{C_i\}$ with $C_i = \{t_{i-1}, \bar{t}_i\}$ for $i \in [1, n-2]$
 179 and $C_{n-1} = \{\bar{t}_0\}$, $C_n = \{t_{n-2}\}$. In this minimally unsatisfiable formula we set $\mathcal{D} = \emptyset$.

180 ► **Example 8** (Equivalence Chain). $\text{EC}_n = \left(\bigcup_{i \in [n]} \{C_i, D_i\} \right) \cup \{D_{n+1}, D_{n+2}\}$ with $C_i =$
 181 $\{t_{i-1}, \bar{t}_i\}$, $D_i = \{\bar{t}_{i-1}, t_i\}$ for $i \in [n]$ and $D_{n+1} = \{t_0, t_n\}$, $D_{n+2} = \{\bar{t}_0, \bar{t}_n\}$. Note that even
 182 though the formula is minimally unsatisfiable, we can choose a large set \mathcal{D} .

183 3.2 QBF Gadgets

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

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

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

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

191 ► **Example 10** (Equality Gadget). $\text{EQ} = \exists x \forall u \cdot \{\{x, u\}, \{\bar{x}, \bar{u}\}\}$.

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

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

$$196 \quad \exists x_1 \cdots x_n \forall u_1 \cdots u_n \exists t_1 \cdots t_n \cdot \left(\bigwedge_{i=1}^n ((x_i \leftrightarrow u_i) \rightarrow \bar{t}_i) \right) \wedge \left(\bigvee_{i=1}^n t_i \right). \quad (2)$$

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

199 The equality gadget is arguably the simplest QBF gadget and except for $\exists x \forall u \cdot x \leftrightarrow u$
 200 the only one in two variables. Nevertheless, it is easy to construct many further gadgets. As
 201 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
 202 winning strategy $u = x^1 \oplus x^2$.

203 ► **Example 11** (XOR Gadget). $\text{XOR} = \exists x^1 x^2 \forall u \cdot$
 204 $\{\{x^1, x^2, u\}, \{x^1, \bar{x}^2, \bar{u}\}, \{\bar{x}^1, x^2, \bar{u}\}, \{\bar{x}^1, \bar{x}^2, u\}\}$.

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

208 3.3 Hard Formulas for QU-Res

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

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

216 We define the product $\varphi \times C$ of a formula φ and a clause C as $\varphi \times C := \{D \cup C \mid D \in \varphi\}$.
 217 Our first main result follows:

218 ► **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*
 219 *QBF gadgets and χ_n a propositional formula with a set $\mathcal{C} = \{C_1, \dots, C_n\}$ of critical clauses*

220 and a set \mathcal{D} of remaining clauses. Set $T_n = \text{vars}(\chi_n)$ and let χ_n have no common variables
 221 with $\bigcup_{i \in [n]} (X_i \cup U_i)$. Then

$$222 \quad \chi_n^\Phi = \exists X_1 \dots X_n \forall U_1 \dots U_n \exists T_n \left[\bigcup_{i \in [n]} \{\varphi_i \times \{C_i\}\} \right] \cup \mathcal{D}$$

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

224 We first show that the following holds:

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

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

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

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

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

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

253 3.4 Examples

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

256 ► **Example 14** (Equality Formulas [11]). The equality formulas (Definition 4) arise from
 257 applying the equality gadgets to the simple contradiction formulas: $\text{EQ}_n = \text{SC}_n^{\text{EQ}}$.

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

$$260 \quad \text{IC}_n^{\text{EQ}} = \exists x_1, \dots, x_n \forall u_1, \dots, u_n \exists t_0, \dots, t_{n-2} \cdot$$

$$261 \quad \left(\bigcup_{i=1}^{n-2} \{ \{u_i, x_i, t_{i-1}, \bar{t}_i\}, \{ \bar{u}_i, \bar{x}_i, t_{i-1}, \bar{t}_i \} \} \right)$$

$$262 \quad \cup \{ \{u_{n-1}, x_{n-1}, \bar{t}_0\}, \{ \bar{u}_{n-1}, \bar{x}_{n-1}, \bar{t}_0 \}, \{u_n, x_n, t_{n-2}\}, \{ \bar{u}_n, \bar{x}_n, t_{n-2} \} \}.$$

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

$$266 \quad \text{EC}_n^{\text{EQ}} = \exists x_1 \dots x_n \forall u_1 \dots u_n \exists t_0 \dots t_n \cdot \left(\bigcup_{i \in [n]} \{C_{i,1}, C_{i,2}, D_i\} \right) \cup \{D_{n+1}, D_{n+2}\}$$

267 with clauses $C_{i,1} = \{x_i, u_i, t_{i-1}, \bar{t}_i\}$, $C_{i,2} = \{\bar{x}_i, \bar{u}_i, t_{i-1}, \bar{t}_i\}$, $D_i = \{\bar{t}_{i-1}, t_i\}$ for $i \in [n]$ and
268 $D_{n+1} = \{t_0, t_n\}$, $D_{n+2} = \{\bar{t}_0, \bar{t}_n\}$.

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

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

$$272 \quad \text{SC}_n^{\text{XOR}} = \exists x_1^1 x_1^2 \dots x_n^1 x_n^2 \forall u_1 \dots u_n \exists t_1 \dots t_n \cdot$$

$$273 \quad \left[\bigcup_{i \in [n]} \{ \{x_i^1, x_i^2, u_i, \bar{t}_i\}, \{x_i^1, \bar{x}_i^2, u_i, t_i\}, \{\bar{x}_i^1, x_i^2, u_i, t_i\}, \{x_i^1, \bar{x}_i^2, u_i, \bar{t}_i\} \} \right]$$

$$274 \quad \cup \{t_1, \dots, t_n\}.$$

276 3.5 Random Formulas

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

279 ► **Definition 18** (F -satisfying Assignment). For $X = \{x_1, \dots, x_a\}$, $U = \{u_1, \dots, u_b\}$ and a
280 function $F : \langle X \rangle \rightarrow \langle U \rangle$ we call an assignment $\alpha \in \langle X \cup U \rangle$ F -satisfying iff $F(x_1^\alpha \dots x_a^\alpha) =$
281 $u_1^\alpha \dots u_b^\alpha$.

282 ► **Definition 19** ($F_{a,b}$ -Gadget). An $F_{a,b}$ -gadget is built from a non-constant Boolean function
283 $F : \{0, 1\}^a \rightarrow \{0, 1\}^b$ as follows: We introduce sets of variables $X = \{x_1, \dots, x_a\}$ and $U =$
284 $\{u_1, \dots, u_b\}$. Consider F as function from $\langle X \rangle$ to $\langle U \rangle$. For any F -satisfying assignment α
285 we add the clause $\{v \mid v^\alpha = 0\} \cup \{\bar{v} \mid v^\alpha = 1\}$. We call the following QBF an $F_{a,b}$ -gadget:

$$286 \quad \text{RG}_{a,b}^F = \exists x_1 \dots x_a \forall u_1, \dots, u_b \cdot \{ \{v \mid v^\alpha = 0\} \cup \{\bar{v} \mid v^\alpha = 1\} \mid \alpha \text{ is } F\text{-satisfying} \}.$$

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

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

290 **Proof.** Obviously, any such QBF is a Σ_2^b formula. To argue for its falsity, let us consider
291 the assignment game: First, the existential player assigns the X -variables. Let α be the

292 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
 293 strategy of the universal player is now to assign U according to α . This will falsify the
 294 clause $\{v \mid v^\alpha = 0\} \cup \{\bar{v} \mid v^\alpha = 1\}$ and thus the whole QBF. Thus the strategy following F
 295 is apparently a winning strategy. The non-constancy is also clear as the function F is not
 296 constant: Suppose, there was a constant winning strategy and $\{l_1^u, \dots, l_b^u\}$ was its negation
 297 pattern on $\{u_1, \dots, u_b\}$ (i.e. $l_i^u = \bar{u}_i$ iff u_i is assigned 0 in the strategy and $l_i^u = u_i$ else). A
 298 winning strategy always falsifies a clause, so for every possible assignment to the existential
 299 variables, there needs to be a clause containing the inverse negation pattern of this assignment
 300 and $\{\bar{l}_1^u, \dots, \bar{l}_b^u\}$. Since every clause is based on a F -satisfying assignment (by definition), we
 301 see that F is constant, which violates the assumptions. \blacktriangleleft

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

304 For the construction of random formulas, we need multiple gadgets. A possible procedure
 305 to construct sequences of random gadgets is to set lower and upper bounds for a, b , for each
 306 $i \in [n]$ choose parameters a_i, b_i randomly within the bounds and then obtain a F_{a_i, b_i} -gadget
 307 from a randomly chosen non-constant function $F : \{0, 1\}^{a_i} \rightarrow \{0, 1\}^{b_i}$ (repeating this process
 308 for each index $n \in \mathbb{N}$).

309 We also want to randomly choose the propositional base formulas. Each clause of a
 310 minimally unsatisfiable formula is critical, so we focus on generating minimally unsatisfiable
 311 formulas. A full characterization of minimally unsatisfiable 2-CNFs was recently given in [3]
 312 (see also [1, 2]). We can use this characterization to obtain the propositional part of our
 313 construction (thereby restricting ourselves to 2-CNFs). This includes the IC_n formulas (the
 314 implication chain formulas), but not the SC_n formulas (simple contradiction formulas).

315 The work [1] also describes a generation procedure for special minimally unsatisfiable
 316 formulas that are 2-CNFs with deficiency one (exactly one clause more than the number
 317 of variables). Using the approach described there with a small modification (allowing C_1
 318 and C_2 to contain more than one literal) enables us to generate unsatisfiable deficiency one
 319 formulas (which are not necessarily 2-CNFs):

320 **► Lemma 21.** *Consider the following construction method:*

321 *Start with $F_0 := \{\perp\}$. Repeat the following steps for $i = 1, \dots, n$:*

322 \blacksquare *Choose a clause $C \in F_{i-1}$ at random (set $C := \{\}$ if $F_{i-1} = \perp$).*

323 \blacksquare *Choose C_1 and C_2 with $C_1 \cup C_2 = C$.*

324 \blacksquare *Build $F_i = F_{i-1} \setminus \{C\} \cup \{C_1 \cup \{v\}\} \cup \{C_2 \cup \{\bar{v}\}\}$ for some $v \notin \text{vars}(F_{i-1})$.*

325 *The formulas constructed according to this method are minimally unsatisfiable.*

326 **Proof.** We show this by induction: Clearly, $F_0 = \{\perp\}$ is minimally unsatisfiable. No we
 327 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 $C = \{\}$
 328 for F_1) and a decomposition $C_1 \cup C_2 = C$. Now we replace C by $C_1 \cup \{v\}$ and $C_2 \cup \{\bar{v}\}$. At
 329 this point it is very easy to modify a proof of resolution for F_i to one for F_{i+1} : We just have
 330 to replace any axiom C by the resolution from $C_1 \cup \{v\}$ and $C_2 \cup \{\bar{v}\}$ to C . Thus we already
 331 know that F_{i+1} is unsatisfiable.

332 Now, to show minimality, have a look at the single clauses. We distinguish two cases:
 333 Suppose first, we omit a clause $D \in F_i \setminus \{C\}$ from F_{i+1} . We know from induction that F_i
 334 is minimally unsatisfiable, thus $F_i \setminus \{D\}$ is satisfiable. A satisfying assignment to $F_i \setminus \{D\}$
 335 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 $C_2 \cup \{\bar{v}\}$.
 336 The second can easily be satisfied by extending the assignment to v (with the appropriate
 337 value). The resulting assignment satisfies $F_{i+1} \setminus \{D\}$.

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

341 Now SC_n can be obtained in this way.

342 Combining random QBF gadgets (according to Lemma 20) with random minimally
 343 unsatisfiable formulas, we get random QBFs, which are hard for QU-Res by Theorem 12:

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

347 Let us briefly compare our random QBFs with the hard random formulas presented in [11].
 348 The formulas in [11] resemble our formulas, but with one major difference: the QBFs in [11]
 349 are only false and hard with high probability. In contrast, we construct QBFs that are always
 350 hard and false by design. The random formulas from [11] can be understood to be based
 351 on the SC formulas. To this they add a random construction that is akin to a QBF gadget,
 352 but only yields one with high probability. Note that in our construction here, we can choose
 353 both the propositional base formulas and the QBF gadgets randomly.

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

355 ▶ **Example 23 (Random SC).** To keep the example as simple as possible, we again resort to
 356 the SC formulas. As we assemble the gadgets, we will set a and b fixed at $a = 2, b = 1$, instead
 357 of randomly choosing these parameters. Thus, all gadgets will be random $F_{1,2}$ -gadgets. There
 358 are $2^4 - 2 = 16$ such gadgets (resp. functions) from which we can choose. We construct
 359 SC_n^{RG} as follows: Let $(F_i)_{i \in [n]}$ be a sequence of randomly chosen non-constant functions
 360 $F_i : \{0, 1\}^2 \rightarrow \{0, 1\}$ for $i \in [n]$ and $\text{RG}_n = (\text{RG}_{2,1}^{F_i})_{i \in [n]}$ the sequence of the associated
 361 gadgets in variables x_i^1, x_i^2 and u_i each, i.e. $\text{RG}_{2,1}^{F_i} = \exists x_i^1 x_i^2 \forall u_i \cdot \varphi_i$. We build

$$362 \quad SC_n^{\text{RG}} = \exists x_1^1 x_1^2 \dots x_n^1 x_n^2 \forall u_1 \dots u_n \exists t_1 \dots t_n \cdot \left(\bigcup_{i \in [n]} \{\varphi_i \times \{\bar{t}_i\}\} \right) \cup \{\{t_1, \dots, t_n\}\}.$$

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

365 Their hardness follows directly from Proposition 22 and the construction of SC_n^{RG} :

366 ▶ **Corollary 24.** *Any QU-Res refutation of SC_n^{RG} has size at least 2^n .*

367 4 Formulas Separating Q-Res and LD-Q-Res

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

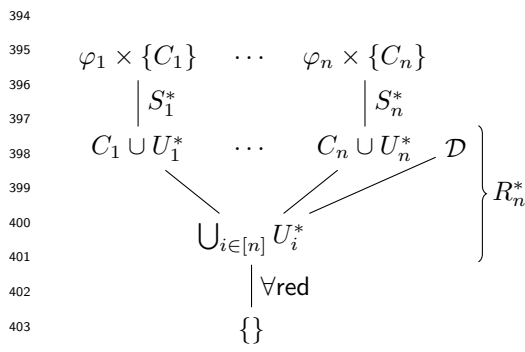
372 In fact, instead of LD-Q-Res we can even use a weaker system, so-called reductionless
 373 LD-Q-Res [13, 20, 35], which is a strict fragment of LD-Q-Res [13]. This system allows merging
 374 as in LD-Q-Res but no universal reduction, i.e., any refutation ends with a purely universal
 375 clause. In other words, it includes LD-Q-Res refutations in which all universal reductions
 376 occur at the end of the derivation.

377 ► **Theorem 25.** For $n \in \mathbb{N}$ let Φ_n be sequences of QBF gadgets with polynomial-size Q-Res
 378 refutations and χ_n propositional formulas with polynomial-size resolution refutations. Let
 379 $\Phi_n = (\phi_i)_{i \in [n]} = (\exists X_i \forall U_i \cdot \varphi_i)_{i \in [n]}$ and $\chi_n = \mathcal{C} \cup \mathcal{D}$ with critical clauses $\mathcal{C} = \{C_1, \dots, C_n\}$,
 380 additional clauses \mathcal{D} , $T_n = \text{vars}(\chi_n)$ and $\text{vars}(\chi_n) \cap \left(\bigcup_{i \in [n]} \{X_i \cup U_i\}\right) = \emptyset$. Then χ_n^Φ (as in
 381 Theorem 12) has polynomial-size refutations in reductionless LD-Q-Res.

382 **Proof.** We consider the formula χ_n^Φ . Let R_n be polynomial-size resolution refutations of χ_n
 383 and S_1, \dots, S_n polynomial-size LD-Q-Res refutations³ of the gadgets ϕ_1, \dots, ϕ_n . Let S'_i be
 384 as S_i , but without the final universal reduction steps. Let U_i^* be the set of (possibly merged)
 385 universal variables in the last clause of the resulting derivation. We can enlarge every clause
 386 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
 387 enlarge every C_i in R_n by U_i^* . This extension runs through the entire proof⁴ and we obtain
 388 a reductionless LD-Q-Res derivation R_n^* of $\bigcup_{i \in [n]} U_i^*$, which we can complete to a refutation
 389 by universal reduction. The composition of the proof is shown in Figure 3. ◀

390 By Theorem 12 (the formulas are hard for QU-Res) and Theorem 25 (which provides
 391 short LD-Q-Res refutations) the following holds:

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



405 ■ **Figure 3** Polynomial-size LD-Q-Res refuta-
 406 tions for χ_n^Φ .

407

408 For the next insight we need a result from [16]:

409 ► **Theorem 27** ([16]). For any QBF ϕ , if π is a treelike $P+\forall\text{red}$ proof of ϕ (where P is a
 410 propositional proof system), then $|\pi| \geq \rho(\phi)$ (where $\rho(\phi)$ is the strategy size from Definition 1).

411 This implies that all the formulas we have constructed so far, including the random QBFs,
 412 are hard for all tree-like $P+\forall\text{red}$ systems.

413 ► **Corollary 28.** If χ_n^Φ is a QBF as described in Theorem 12, then any refutation of χ_n^Φ in
 414 treelike $P+\forall\text{red}$ systems has length at least 2^n .

³ Note that for Σ_2^b -formulas the systems Q-Res and LD-Q-Res are equivalent. A Q-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.

415 This leads to an interesting fact:

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

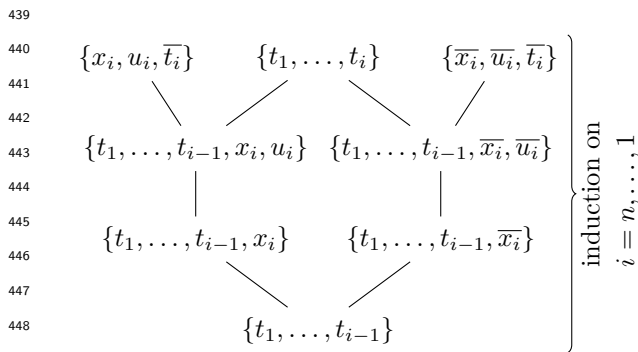
418 **Proof.** The polynomial-size reductionless LD-Q-Res refutations shown in the proof of Theo-
 419 rem 25 are treelike, as long as the resolution refutation of the propositional formula and the
 420 reductionless LD-Q-Res refutation of the gadgets are (it is easy to find examples for both).
 421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

424 This is surprising because reductionless LD-Q-Res itself is not a very strong proof system;
 425 certainly the treelike variant is not either. Reductionless LD-Q-Res does not even simulate
 426 Q-Res (the two systems are in fact incomparable [35]). This is interesting to contrast with
 427 the recent simulation of LD-Q-Res (and even stronger systems) by QBF Frege [24]. The
 428 simulation there is quite non-trivial and highly dag-like. Proposition 29 above means that it
 429 cannot be strengthened to a tree-preserving simulation.

430 **5 Construction of Separating Formulas between Q-Res and QU-Res**

431 We now want to construct QBFs that separate Q-Res and QU-Res. As an intermediate step,
 432 we will build QBFs that are easy for Q-Res but have exponential strategy size. We will use
 433 the equality QBFs from the previous sections as running example, and, in fact, only change
 434 the prefix (and add some conditions on the underlying propositional formulas for the general
 435 case). We will then use such false QBFs with exponential strategy size and short Q-Res
 436 refutations to construct a large class of formulas to separate Q-Res from QU-Res.

437 **5.1 Formulas with Exponential Strategy Size and Short Q-Res**
 438 **Refutations**



450 ■ **Figure 4** Polynomial-size Q-Res refutation of ${}^{11}\text{SC}_n^{\text{EQ}}$.

439 First we will look at Examples 14, 16, and 17 from Section 3.4 and show
 440 how to obtain formulas from them that are easy for Q-Res but still have
 441 exponential strategy size. The key point here is the prefix – while we
 442 leave the matrix unchanged, we resort the Σ_3^b prefix into an unrestricted
 443 prefix. Roughly speaking, we do this by arranging the ‘crucial’ variables
 444 of each critical clause into a separate existential block to the right of the
 445 variables of the associated gadget, and

452 the remaining propositional variables into the leftmost existential block. In most of the
 453 examples already given, it is intuitively easy to identify the ‘crucial’ variables of a clause; in
 454 the general case, this is somewhat more involved⁵, as is to determine the appropriate order of

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

455 the critical clauses (i.e., of their variables in the prefix), which is not arbitrary. We therefore
 456 only verify the desired properties for Examples 14, 16, and 17 from Section 3.4 here, further
 457 details are given in Section 5.2.

458 We start with the equality formulas. These were already modified in the desired way to
 459 the *interleaved equality formulas* [11], which have the same matrix as the equality formulas,
 460 but with an interleaved prefix (this also inspired our general construction). We adopt the
 461 name ‘interleaved’ also for our other examples and denote the interleaved variant of a Σ_3^b -QBF
 462 χ_n^Φ by ${}^{\text{il}}\chi_n^\Phi$. We will give short Q-Res refutations for each example.

463 ► **Example 30** (Interleaved Equality [11]). We build ${}^{\text{il}}\text{SC}_n^{\text{EQ}}$ from SC_n^{EQ} by reordering the
 464 prefix in a natural way according to the indices:

$$\begin{aligned} 465 \quad \text{SC}_n^{\text{EQ}} &= \exists x_1 \dots x_n \forall u_1 \dots u_n \exists t_1, \dots, t_n \cdot \psi \\ 466 \quad {}^{\text{il}}\text{SC}_n^{\text{EQ}} &= (\exists x_1 \forall u_1 \exists t_1) \dots (\exists x_n \forall u_n \exists t_n) \cdot \psi \\ 467 \quad \psi &= \bigcup_{i \in [n]} \{ \{ \bar{t}_i, x_i, u_i \}, \{ \bar{t}_i, \bar{x}_i, \bar{u}_i \} \} \cup \{ t_1, \dots, t_n \}. \end{aligned}$$

469 The Q-Res refutation shown in Figure 4 follows closely the resolution proof of SC_n .

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

$$\begin{aligned} 472 \quad \text{EC}_n^{\text{EQ}} &= \exists x_1 \dots x_n \forall u_1 \dots u_n \exists t_0 \dots t_n \cdot \psi \\ 473 \quad {}^{\text{il}}\text{EC}_n^{\text{EQ}} &= \exists t_0 (\exists x_1 \forall u_1 \exists t_1) \dots (\exists x_n \forall u_n \exists t_n) \cdot \psi \\ 474 \quad \psi &= \left(\bigcup_{i \in [n]} \{ C_{i,1}, C_{i,2}, D_i \} \right) \cup \{ D_{n+1}, D_{n+2} \} \end{aligned}$$

475 with Clauses

$$\begin{aligned} 476 \quad C_{i,1} &= \{ x_i, u_i, t_{i-1}, \bar{t}_i \} & D_i &= \{ \bar{t}_{i-1}, t_i \} & i \in [n] \\ 477 \quad C_{i,2} &= \{ \bar{x}_i, \bar{u}_i, t_{i-1}, \bar{t}_i \} \\ 478 \quad D_{n+1} &= \{ t_0, t_n \} & D_{n+2} &= \{ \bar{t}_0, \bar{t}_n \}. \end{aligned}$$

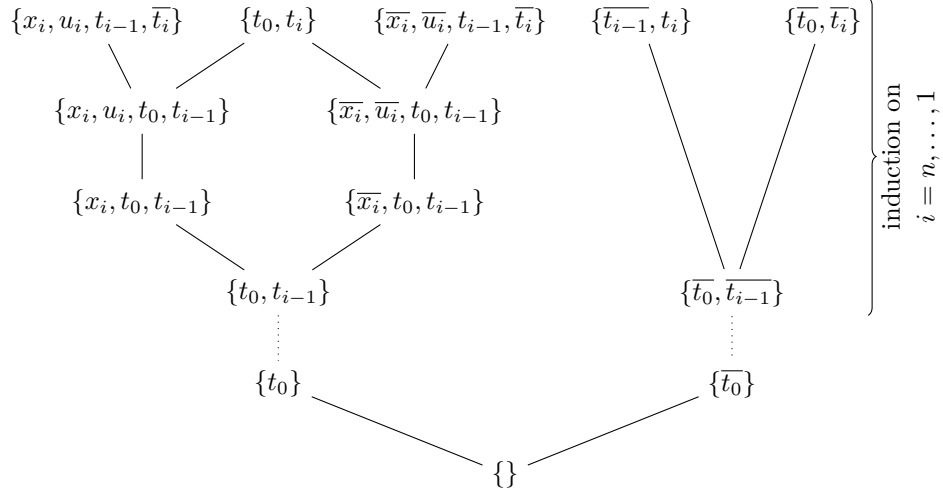
479 The Q-Res refutation (see Figure 5) is structurally similar to the resolution proof for EC_n
 480 here as well, although it can be seen quite clearly that only one side of the proof is blown up
 481 by the refutations of the gadgets, which is due to the choice of the critical clauses.

482 We now consider using XOR gadgets:

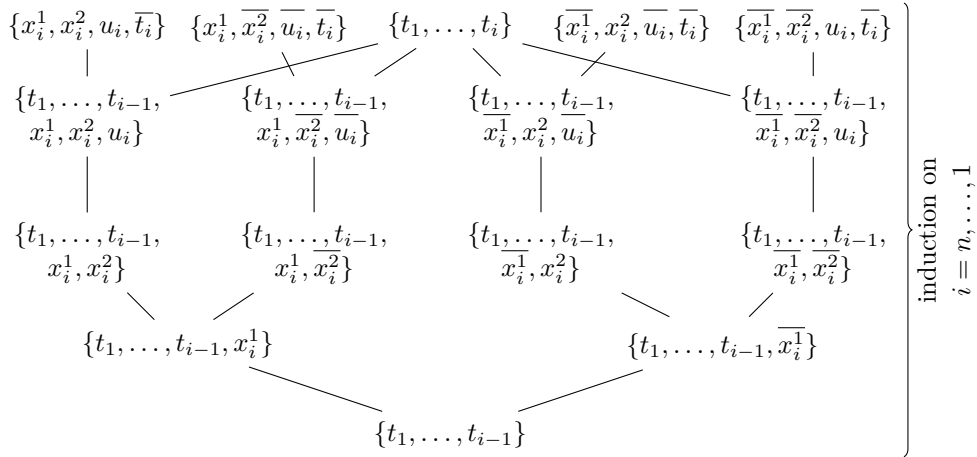
483 ► **Example 32** (Interleaved XOR). For ${}^{\text{il}}\text{SC}_n^{\text{XOR}}$, the existential blocks in the prefix each
 484 comprise two existential variables, as specified by the XOR gadget. The matrix remains the
 485 same as for SC_n^{XOR} :

$$\begin{aligned} 486 \quad \text{SC}_n^{\text{XOR}} &= \exists x_1^1 x_1^2 \dots x_n^1 x_n^2 \forall u_1 \dots u_n \exists t_1 \dots t_n \cdot \psi \\ 487 \quad {}^{\text{il}}\text{SC}_n^{\text{XOR}} &= (\exists x_1^1 x_1^2 \forall u_1 \exists t_1) \dots (\exists x_n^1 x_n^2 \forall u_n \exists t_n) \cdot \psi \\ 488 \quad \psi &= \left[\bigcup_{i \in [n]} \left\{ \{ x_i^1, x_i^2, u_i, \bar{t}_i \}, \{ x_i^1, \bar{x}_i^2, u_i, \bar{t}_i \}, \{ \bar{x}_i^1, x_i^2, u_i, \bar{t}_i \}, \{ \bar{x}_i^1, \bar{x}_i^2, u_i, \bar{t}_i \} \right\} \right] \\ 489 \quad &\cup \{ t_1, \dots, t_n \}. \end{aligned}$$

490 The Q-Res refutations are made slightly more complex by the gadgets, but even here the
 491 structure of the resolution proof of SC shines through, as you can see in Figure 6.



■ **Figure 5** Polynomial-size Q-Res refutation of $^{\text{il}}\text{EC}_n^{\text{EQ}}$.



■ **Figure 6** Polynomial-size Q-Res refutation of $^{\text{il}}\text{SC}_n^{\text{XOR}}$.

492 Note, that all the universal reductions in the Q-Res refutations shown in Figures 4–6
 493 comply with the rules thanks to the variable order in the prefixes.

494 It is readily verified that the interleaved formulas inherit exponential strategy size from
 495 their Σ_3^b origins. While the winning strategies of the universal player are no longer unique
 496 for the interleaved formulas, the existential player can nevertheless continue to force a game
 497 that corresponds to the winning strategy of the associated Σ_3^b formulas, i.e., $u_i = x_i$ for all
 498 $i \in [n]$ 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
 499 gadgets. Thus, the interleaved formulas retain exponential strategy size.

500 Note that the circle formulas IC_n^{EQ} from Example 15 can not be modified this way – there
 501 are not even enough propositional t variables to build the prefix accordingly⁶.

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

505 **► Proposition 33.** *The formulas from Examples 30–32 (and all other formulas with short*
 506 *Q-Res refutations and exponential strategy size) separate treelike from dag-like Q-Res.*

507 5.2 General Construction of Formulas as in Section 5.1

508 While we show in Section 5.1 that certain variants of the previously introduced examples
 509 satisfy the required conditions, in the following we will give a general construction for such
 510 formulas that are easy for Q-Res but have exponential strategy size. We will use the same
 511 ingredients as in Section 3. In fact, we only have to change the prefix and some requirements
 512 to the underlying propositional formulas and QBF gadgets. This approach is consistent
 513 with the relationship between the examples in Section 3.4 and those in Section 5.1 (e.g the
 514 conventional equality formulas from [11] and interleaved equality).

515 Knowing this construction will enable us later to perform the construction in Section 5.3
 516 on this basis and thus to find further separating formulas between Q-Res and QU-Res.

517 We are familiar with exponential strategy size from Section 3, and we will reuse the
 518 procedure described there, refining our requirements to the propositional base formula as
 519 well as to the QBF gadget and reordering the prefix. To get short Q-Res refutations of the
 520 constructed formula, in addition to gadgets with short proofs, of course we need to use a
 521 propositional base formula with short resolution refutations. In fact, the condition is more
 522 complicated:

523 **► Definition 34** (refutation and assignment preserving formulas). *Let χ_n be a propositional*
 524 *formula with at least n clauses and short resolution proofs.*

525 *With respect to a set \mathcal{C} of critical clauses and a short refutation π of χ_n , we call a*
 526 *resolution step in π involving a clause from \mathcal{C} a \mathcal{C} -step and we call $\chi_n(\mathcal{C}, \pi)$ -refutation*
 527 *preserving, if \mathcal{C}, π satisfy the following properties:*

- 528 (i) *For any $C \in \mathcal{C}$ there is exactly one \mathcal{C} -step in π using C as axiom.*
- 529 (ii) *Every \mathcal{C} -step resolves a clause from \mathcal{C} with a clause from $\mathcal{D} = \chi_n \setminus \mathcal{C}$ or a derived clause.*
- 530 (iii) *The pivots of the \mathcal{C} -steps are pairwise different.*
- 531 (iv) *Any resolvent of a \mathcal{C} -step contains no pivot which is used in an earlier \mathcal{C} -step.*

⁶ The modification becomes straightforward if we choose $\mathcal{D} = \{\{\bar{t}_0\}, \{t_n\}\}$ and $C_i = \{t_{i-1}, \bar{t}_i\}$ 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).

532 Now let π be as described. We denote by $R = (C, D, p)$ a resolution step with parent
 533 clauses C and D over the pivot variable p . Let R_1, \dots, R_n be the sequence of \mathcal{C} -steps in
 534 π and $C_1, \dots, C_n, p_1, \dots, p_n$ the according sequences of parent clauses from \mathcal{C} respective
 535 pivot variables. Now let $t_i = p_{n+1-i}$ and $C_i^* = C_{n+1-i}$ for $i \in [n]$ (so the sequence of
 536 t -variables is exactly the one of p -variables in reverse order, as with C^* - and C -clauses).
 537 Let further $T = \text{vars}(\chi_n)$, $T_0 = T \setminus \{t_1, \dots, t_n\}$, $T_i = T_{i-1} \cup \{t_i\}$ for $i \in [n]$, $\alpha_0 \in \langle T_0 \rangle$ an
 538 assignment to the variables from T_0 and let $\alpha_i \in \langle T_i \rangle$ be like α_{i-1} on their common variables
 539 and additionally assigning a truth value to t_i for $i \in [n]$. Let $\alpha = (\alpha_0, \dots, \alpha_n)$ be built up
 540 from α_0 as described. We call χ_n $\alpha_{\mathcal{C}, \pi}$ -preserving if $C_i^* \upharpoonright_{\alpha_{i-1}}$ is critical in $\chi_n \upharpoonright_{\alpha_{i-1}}$ for any
 541 $i \in [n]$.

542 ► **Definition 35** ($\text{il}_{\chi_n}^{\Phi}$). Let χ_n be a (\mathcal{C}, π) -refutation preserving and $\alpha_{\mathcal{C}, \pi}$ -preserving proposi-
 543 tional formula with $|\mathcal{C}| = n$ and $\mathcal{D} = \chi_n \setminus \mathcal{C}$. Let t_1, \dots, t_n and C_1^*, \dots, C_n^* be the sequences
 544 of pivot variables and \mathcal{C} -parent clauses of resolution \mathcal{C} -steps in π (i.e., in reverse order) and
 545 $T_0 = \text{vars}(\chi_n) \setminus \{t_1, \dots, t_n\}$. Let further $\Phi_n = (\phi_i)_{i \in [n]} = (\mathcal{P}_i \cdot \varphi_i)_{i \in [n]}$ be a sequence of QBF
 546 gadgets. We define

$$547 \quad \text{il}_{\chi_n}^{\Phi} = \exists T_0 (\mathcal{P}_1 \exists t_1) \dots (\mathcal{P}_n \exists t_n) \cdot$$

$$548 \quad \bigcup_{i \in [n]} [\varphi_i \times \{C_i^*\}] \cup \mathcal{D}.$$

$$549$$

550 ► **Lemma 36.** For $n \in \mathbb{N}$ let Φ_n be a sequence of n QBF gadgets and χ_n a propositional
 551 formula with polynomial-size resolution refutations. Let χ_n be (\mathcal{C}, π) -refutation preserving
 552 with $|\mathcal{C}| \geq n$. Then $\text{il}_{\chi_n}^{\Phi}$ has polynomial-size Q-Res refutations.

553 **Proof.** Let $\Phi_n = (\phi_i)_{i \in [n]} = (\mathcal{P}_i \cdot \varphi_i)_{i \in [n]}$ be a sequence of QBF gadgets, χ_n (\mathcal{C}, π) -refutation
 554 preserving with polynomial-size resolution refutations, $\mathcal{D} = \chi_n \setminus \mathcal{C}$, C_1^*, \dots, C_n^* and t_1, \dots, t_n
 555 the sequences of axioms and pivots as described above and $T_0 = \text{vars}(\chi_n) \setminus \{t_1, \dots, t_n\}$. We
 556 consider the \mathcal{C} -steps performed in π and show, that the resolvents can be derived in only a
 557 few more steps using axioms from $\text{il}_{\chi_n}^{\Phi}$ and Q-Res.

558 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
 559 are resolved with each other in π to the resolvent E . t_i is the pivot element to this resolution
 560 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
 561 D , we obtain $\varphi_i \times \{E\}$, thereby eliminating the pivot t_i . Since ϕ_i and χ_n are variable disjoint
 562 and all the T -variables are existential, this is easily possible. Since χ_n is (\mathcal{C}, π) -refutation
 563 preserving, E does not contain any variable t_j with $j > i$. Now we can use the refutation
 564 of φ_i (note that its size is constant since the size of the gadget is independent from n) by
 565 extending each clause in it by E . Since $\varphi_i \times \{E\}$ only contains variables from \mathcal{P}_i and T ,
 566 reduction steps within the derivation could – corresponding to the prefix – only be blocked
 567 by variables t_j , $j \geq i$. However, these are not contained in $\varphi_i \times \{E\}$. So at the end of the
 568 derivation we get the clause E instead of the empty clause – as desired.

569 Figure 7 illustrates the procedure using an equality sub-formula $\mathcal{P}_i \cdot \varphi_i = \exists x_i \forall u_i \cdot$
 570 $\{\{x_i, u_i\}, \{\bar{x}_i, \bar{u}_i\}\}$.

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

576 ▶ **Lemma 37.** For $n \in \mathbb{N}$ let Φ_n be a sequence of n QBF gadgets and χ_n a propositional
 577 formula with polynomial-size resolution refutations. Let χ_n be $\alpha_{\mathcal{C},\pi}$ -preserving with $|\mathcal{C}| \geq n$.
 578 Then ${}^{\text{ll}}\chi_n^\Phi$ has exponential strategy size.

579 **Proof.** We can use a similar argumentation as in Theorem 12 to show, that any winning
 580 strategy for ${}^{\text{ll}}\chi_n^\Phi$ is based on a combination of winning strategies for the ϕ_i formulas (but
 581 we have to take into account that the prefix does not collect the T -variables at the end and
 582 therefore need the $\alpha_{\mathcal{C},\pi}$ -preserving property.).

583 Let χ_n be $\alpha_{\mathcal{C},\pi}$ -preserving with respect to a critical set \mathcal{C} with size $|\mathcal{C}| = n$ and a resolution
 584 refutation π and let $\Phi_n = (\phi_i)_{i \in [n]} = (\mathcal{P}_i \cdot \varphi_i)_{i \in [n]}$ be a sequence of QBF gadgets. It is
 585 obvious, that assigning u_i according to a winning strategy for ϕ_i for each $i \in [n]$ is a universal
 586 winning strategy on ${}^{\text{ll}}\chi_n^\Phi$ with exponential size (since the gadgets are non-constant). We
 587 assume (for contradiction), there is a winning strategy S assigning u_i different from any
 588 winning strategy for ϕ_i for some $i \in [n]$ (we consider the smallest i with this property).
 589 Then all clauses from $\varphi_i \times \{C_i^*\}$ are satisfied (since φ_i is satisfied). We assume that the
 590 existential player has followed α_{i-1} on T_0 and t_1, \dots, t_{i-1} . But since χ_n is $\alpha_{\mathcal{C},\pi}$ -preserving,
 591 we know $C_i^* \upharpoonright_{\alpha_{i-1}}$ is critical in $\chi_n \upharpoonright_{\alpha_{i-1}}$. That means $\chi_n \upharpoonright_{\alpha_{i-1}} \setminus \{C_i^* \upharpoonright_{\alpha_{i-1}}\}$ is satisfiable with
 592 some assignment α' to the remaining variables t_i, \dots, t_n . Since the clauses $\varphi_i \times \{C_i^*\}$ are
 593 already satisfied by the universal assignment, the existential player wins the assignment game
 594 with α' and an arbitrary assignment to the remaining existential variables. Thus S is not a
 595 winning strategy. ◀

596 The formulas for simple con-
 597 tradiction and equivalence chain
 598 from Section 3 are refutation and
 599 $\alpha_{\mathcal{C},\pi}$ -preserving, where the naming
 600 of the clauses identifies \mathcal{C} and \mathcal{D}
 601 and the related π and α should be
 602 obvious. While interleaved equal-
 603 ity formulas ([11]) are an instan-
 604 tiation of ${}^{\text{ll}}\chi_n^\Phi$ -formulas already
 605 known from literature, we present
 606 some new examples in Section 5.1.

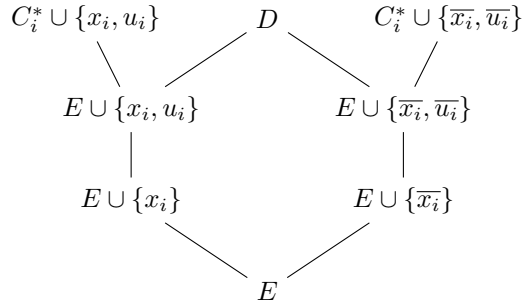
607 ▶ **Theorem 38.** For $n \in \mathbb{N}$ let Φ_n
 608 be a sequence of n QBF gadgets
 609 and χ_n a propositional formula with polynomial-size resolution refutations. Let χ_n be (\mathcal{C}, π) -
 610 refutation preserving and $\alpha_{\mathcal{C},\pi}$ -preserving with $|\mathcal{C}| \geq n$. Then ${}^{\text{ll}}\chi_n^\Phi$ separate tree-like from
 611 dag-like Q-Res.

612 **Proof.** This follows immediately from Lemmas 37 and 47 and Proposition 33. ◀

613 5.3 Separating Formulas

614 In the second step we will use the QBFs with short Q-Res refutations and exponential strategy
 615 size to construct separating formulas between Q-Res and QU-Res. Our method is inspired by
 616 the structure of the KBKF formulas [31]. We first define the concept of target clauses.

617 ▶ **Definition 39 (Target Clauses).** For a false QBF $\phi = \mathcal{P} \cdot \varphi$ let F be a set of clauses such
 618 that the existential player has a strategy to never lose on clauses from $\phi \setminus F$ in any assignment
 619 game (regardless of the strategy chosen by the universal player), i.e., the existential player
 620 will always lose on clauses in F . We call F a set of target clauses.



613 ■ **Figure 7** Q-Res derivation of the resolvent E from $\text{EQ} \times_i^*$.

621 Notice that F is in general not unique. It is always possible to choose $F = \varphi$. Based on
 622 this, the construction is remarkably simple:

623 ► **Definition 40** (Tail Construction). *Let $\phi = \mathcal{P} \cdot \varphi$ be a false QBF with universal variables*
 624 *$\text{vars}_{\forall}(\phi) = \{u_1, \dots, u_n\}$ and $\{e_1, \dots, e_n\} \cap \text{vars}(\phi) = \emptyset$. Let further F be a set of target*
 625 *clauses for ϕ . Then we call*

$$\begin{aligned} \phi^* &= \mathcal{P}^* \cdot \varphi^* \\ &= \mathcal{P} \exists e_1 \dots e_n \cdot \left(\bigcup_{C \in \varphi \setminus F} \{C\} \right) \cup \left(\bigcup_{C \in F} \{C \cup \{\bar{e}_i : i \in [n]\}\} \right) \cup \left(\bigcup_{i \in [n]} \{\{u_i, e_i\}, \{\bar{u}_i, e_i\}\} \right) \end{aligned}$$

627 the tailed version ϕ^* of ϕ .

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

631 ► **Theorem 41.** *Let ϕ_n^* be tailed versions of formulas ϕ_n as described in Definition 40, where*
 632 *ϕ_n requires super-polynomial strategy size, but has polynomial-size Q-Res refutations. Then*
 633 *ϕ_n^* separates Q-Res from QU-Res, i.e., ϕ_n^* requires super-polynomial size Q-Res refutations,*
 634 *but has polynomial-size QU-Res refutations.*

635 We will split the proof of Theorem 41 into two parts, first showing hardness for Q-Res of
 636 the constructed formula and afterwards constructing short QU-Res proofs.

637 To show this, we modify ϕ^* once more, similarly as described in [6] for the KBKF formulas.
 638 That is, we use new variables v_1, \dots, v_n and put them into the formula as copies of the
 639 universal variables u_1, \dots, u_n . While Balabanov, Widl, and Jiang create $\forall u_i v_i$ from each $\forall u_i$
 640 in the prefix, we group the universal copies in a (possibly additional) universal quantification
 641 block to the right of \mathcal{P} (and to the left of the existential tail variables), similarly as in [11],
 642 i.e., $\mathcal{P}^* = \mathcal{P} \exists e_1 \dots e_n$ becomes $\mathcal{P}' = \mathcal{P} \forall v_1 \dots v_n \exists e_1 \dots e_n$. In addition, the occurrences of u_i
 643 in the matrix are effectively doubled, i.e., φ' contains for each clause $C \in \varphi^*$ the extended
 644 clause $C \cup \{v_i : u_i \in C\} \cup \{\bar{v}_i : \bar{u}_i \in C\}$.

► **Definition 42** (ϕ'). *For any QBF $\phi^* = \mathcal{P}^* \cdot \varphi^*$ constructed from a QBF $\phi = \mathcal{P} \cdot \varphi$ following*
Definition 40 we define

$$\phi' = \mathcal{P}' \cdot \varphi' = \mathcal{P} \forall v_1 \dots v_n \exists e_1 \dots e_n \cdot \left(\bigcup_{C \in \varphi^*} C \cup \{v_i : u_i \in C\} \cup \{\bar{v}_i : \bar{u}_i \in C\} \right).$$

645 Moving the universal variable copies to the right into a common universal block can only
 646 shorten QU-Res refutations, since it might enable additional universal reductions, but can
 647 never block a reduction previously possible. We then use Theorem 3 to show that ϕ' requires
 648 long QU-Res proofs. To do so, we first show:

649 ► **Lemma 43.** *Let ϕ^* be a QBF constructed from ϕ following Definition 40 and let ϕ' be as*
 650 *described in Definition 42. Then in the assignment game for ϕ' the existential player can*
 651 *force the universal player to*

- 652 (i) *follow a winning strategy for ϕ on u_1, \dots, u_n and*
- 653 (ii) *assign $v_i = u_i$ for every $i \in [n]$.*

654 **Proof.** We first show (i). Consider the assignment game on \mathcal{P} . If the universal player does
 655 not use a winning strategy on ϕ , he will lose on ϕ . Thus the assignment α constructed on
 656 \mathcal{P} satisfies φ and thus all the clauses $\bigcup_{C \in \phi} \{C \cup \{\bar{e}_i : i \in [n]\} \cup \{v_i \mid u_i \in C\} \cup \{\bar{v}_i \mid \bar{u}_i \in C\}\}$,
 657 because these are just weakenings of clauses from φ . The remaining clauses are
 658 $\bigcup_{i \in [n]} \{\{u_i, v_i, e_i\}, \{\bar{u}_i, \bar{v}_i, e_i\}\}$, which can easily be satisfied by $e_i = 1$ for $i \in [n]$. Hence the
 659 existential player wins the assignment game.

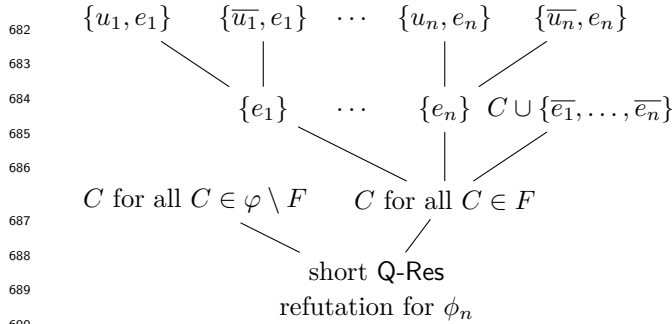
660 For (ii) again we consider the game on \mathcal{P} and assume that the existential player plays
 661 according to his strategy on ϕ to only lose on clauses in F . Since F is a target set, we
 662 know that such a strategy exists. Let α be the assignment constructed on \mathcal{P} (by both the
 663 existential and the universal player). By definition of target clauses α does not falsify any
 664 clause $C \in \varphi \setminus \{F\}$; these are also part of ϕ^* . α also satisfies the corresponding clauses in ϕ' ,
 665 which are $\{C \cup \{v_i \mid u_i \in C\} \cup \{\bar{v}_i \mid \bar{u}_i \in C\} \mid C \in \varphi \setminus \{F\}\}$. Thus, the remaining clauses are
 666 those resulting from $C \in F$, $\bigcup_{C \in F} \{C \cup \{\bar{e}_i : i \in [n]\} \cup \{v_i \mid u_i \in C\} \cup \{\bar{v}_i \mid \bar{u}_i \in C\}\}$ and
 667 the additional clauses $\bigcup_{i \in [n]} \{\{u_i, v_i, e_i\}, \{\bar{u}_i, \bar{v}_i, e_i\}\}$. Now assume towards a contradiction
 668 that the universal player assigns $v_j \neq u_j$ for some $j \in [n]$ (let j be the first index for
 669 which this applies). Then the existential player can assign $e_j = 0$ without falsifying any
 670 of these clauses. This immediately satisfies every clause originating from a clause in F .
 671 All the clauses $\{u_j, v_j, e_j\}, \{\bar{u}_j, \bar{v}_j, e_j\}$ with $j < i$ are already satisfied and thus only the
 672 clauses $\{u_j, v_j, e_j\}, \{\bar{u}_j, \bar{v}_j, e_j\}$ with $j > i$ remain. But now the existential player can win the
 673 assignment game by simply assigning $e_j = 1$ for each $j > i$. \blacktriangleleft

674 **► Lemma 44.** Let ϕ , ϕ^* , and ϕ' be as in Lemma 43. Then QU-Res proof size of ϕ' is at
 675 least $\rho(\phi)$.

676 **Proof.** According to Lemma 43 the universal player has to assign u_1, \dots, u_n according to
 677 a ϕ -strategy and $v_i = u_i$ for $i \in [n]$. Thus the cost of ϕ' is at least $\rho(\phi)$, because the
 678 whole strategy is pooled in the last universal block. Now we can use the cost/size argument
 679 (Theorem 3) and obtain that proof size of ϕ' in QU-Res is at least $\rho(\phi)$. \blacktriangleleft

680 We can now prove the lower bound for ϕ^* , following an approach described in [11].

681



691 **■ Figure 8** Polynomial-size QU-Res refutations for ϕ^* .

692

693

694

695 ence to QU-Res). But then we can construct a Q-Res proof π' for ϕ' by just doubling all
 696 reduction steps in π in the sense of introducing an additional reduction step for v_i as soon
 697 as u_i is reduced. That is always possible, because v_i is never quantified left from u_i . The
 698 remainder of the proof can be left unchanged, since the variable copies (v_i, \bar{v}_i) cannot cause
 699 any tautologies that would not also be caused by the originals (u_i, \bar{u}_i) . The proof constructed

695 **► Lemma 45.** Let $\phi^* = \mathcal{P}^* \cdot \varphi^*$ be
 696 a QBF constructed from $\phi = \mathcal{P} \cdot \varphi$
 697 according to Definition 40. Then
 698 proof size of ϕ^* in Q-Res is at least
 699 $\frac{1}{2}\rho(\phi)$.

Proof. Suppose that proof size
 of ϕ^* 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 vari-
 ables must be reduced by universal
 reduction in π (there is no other
 option, which is the decisive differ-

700 in this way remains in the same order of magnitude as the original one, more precisely
 701 $|\pi'| \leq 2|\pi| < \rho(\phi)$ in contradiction to the above observation of Lemma 44. Thus any Q-Res
 702 refutations for ϕ^* has size at least $\frac{1}{2}\rho(\phi)$. ◀

703 Lemma 45 in combination with the conditions from Theorem 41 (i.e., exponential strategy
 704 size of ϕ_n) implies Q-Res-hardness of ϕ_n^* :

705 ▶ **Corollary 46** (ϕ_n^* is Hard for Q-Res). *Let ϕ_n^* be tailed versions constructed from ϕ_n following
 706 the rules and conditions from Theorem 41. Then ϕ_n^* is hard for Q-Res.*

707 Let us now prove the upper bound stated in Theorem 41:

708 ▶ **Lemma 47** (ϕ_n^* has Short QU-Res Refutations). *If ϕ_n^* are QBFs constructed from ϕ_n
 709 following the rules and conditions from Theorem 41, then ϕ_n^* has short QU-Res refutations.*

710 **Proof.** $\phi_n = \mathcal{P} \cdot \varphi_n$ has by assumption short Q-Res proofs. ϕ_n^* additionally contains the
 711 clauses $\{u_i, e_i\}$ and $\{\bar{u}_i, e_i\}$ for all $i \in [n]$, from which we can get all the unit clauses
 712 $\{e_i\}, i \in [n]$ in only n universal resolution steps (available in QU-Res). We then remove all
 713 the \bar{e}_i literals from the clauses originated from F in $|F| \cdot n$ resolution steps. Together with
 714 the unchanged clauses from $\varphi_n \setminus F$ we now have all clauses from φ_n and can proceed with
 715 the short Q-Res refutation of ϕ_n . The proof of ϕ_n is extended by $(|F| + 1) \cdot n \leq (|\varphi_n| + 1) \cdot n$
 716 steps. Therefore we get a polynomial-size QU-Res refutation of ϕ_n^* . The composition of the
 717 proof is shown in Figure 8. ◀

718 **Proof of Theorem 41.** The theorem follows from Corollary 46 and Lemma 47. ◀

719 5.4 Examples

720 We illustrate our construction on the interleaved equality formulas from [11], which we
 721 already discussed in Section 5.1:

722 ▶ **Example 48** (Tailed Equality). We first need suitable formulas, on which we can use the
 723 tail construction:

$$724 \quad \phi_n = (\exists x_1 \forall u_1 \exists t_1) \dots (\exists x_n \forall u_n \exists t_n) \cdot \left(\bigcup_{i \in [n]} \{ \{x_i, u_i, \bar{t}_i\}, \{\bar{x}_i, \bar{u}_i, \bar{t}_i\} \} \right) \cup \{ \{t_1, \dots, t_n\} \}.$$

725 As mentioned in Section 5.1, these are exactly the ${}^{\text{ll}}\text{SC}_n^{\text{EQ}}$ -formulas, i.e., they have expo-
 726 nential strategy size and short Q-Res refutations. Thus, $(\phi_i)_{i \in \mathbb{N}}$ meets the requirements for
 727 constructing separating formulas according to the above method. The existential player
 728 has a strategy to satisfy all clauses except for $\{x_n, u_n, \bar{t}_n\}$, $\{\bar{x}_n, \bar{u}_n, \bar{t}_n\}$ and $\{t_1, \dots, t_n\}$ in
 729 any game (by just setting $t_i = 0$ for $i < n$). With $u_n = x_n$ we get the following possible
 730 assignments:

- 731 ■ $x_n = u_n = 1, t_n = 1$ falsifies $\{\bar{x}_n, \bar{u}_n, \bar{t}_n\}$,
- 732 ■ $x_n = u_n = 0, t_n = 1$ falsifies $\{x_n, u_n, \bar{t}_n\}$ and
- 733 ■ $x_n = u_n, t_n = 0$ falsifies $\{t_1, \dots, t_n\}$.

734 The remaining two clauses are satisfied in each case. Thus there are three possibilities for a
 735 minimal set F of target clauses, containing one of these three clauses. The most intuitive
 736 choice for F is $F = \{ \{t_1, \dots, t_n\} \}$. The tail construction then leads to the following formulas,

737 separating Q-Res and QU-Res:

$$738 \quad \phi_n^* = {}^{t1} \text{SC}_n^{\text{EQ}} = (\exists x_1 \forall u_1 \exists t_1) \dots (\exists x_n \forall u_n \exists t_n) \exists e_1 \dots e_n \cdot$$

$$739 \quad \left(\bigcup_{i \in [n]} \{ \{x_i, u_i, \bar{t}_i\}, \{\bar{x}_i, \bar{u}_i, \bar{t}_i\}, \{u_i, e_i\}, \{\bar{u}_i, e_i\} \} \right)$$

$$740 \quad \cup \{ \{t_1, \dots, t_n, \bar{e}_1, \dots, \bar{e}_n\} \}.$$

742 Interestingly, the KBKF formulas [31] correspond to the tail construction (they actually
743 inspired our construction):

744 ► **Example 49** (KBKF). The KBKF formulas presented in [31] are defined as

$$745 \quad \phi_n^* = \text{KBKF}_n = \exists y_0 (\exists y_1 y'_1 \forall u_1) \dots (\exists y_n y'_n \forall u_n) \exists y_{n+1} \dots y_{n+n} \cdot \bigcup_{i \in [0 \dots 2n]} \{C_i, C'_i\}$$

746 where the matrix clauses are defined as follows:

$$747 \quad C_0 = \{\bar{y}_0\} \qquad C'_0 = \{y_0, \bar{y}_1, \bar{y}'_1\}$$

$$748 \quad C_k = \{y_k, \bar{u}_k, \bar{y}_{k+1}, \bar{y}'_{k+1}\} \qquad C'_k = \{y'_k, u_k, \bar{y}_{k+1}, \bar{y}'_{k+1}\}$$

$$749 \quad C_n = \{y_n, \bar{u}_n, \bar{y}_{n+1}, \dots, \bar{y}_{n+n}\} \qquad C'_n = \{y'_n, u_n, \bar{y}_{n+1}, \dots, \bar{y}_{n+n}\}$$

$$750 \quad C_{n+t} = \{\bar{u}_t, y_{n+t}\} \qquad C'_{n+t} = \{u_t, y_{n+t}\}$$

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

$$756 \quad \phi_n = \exists y_0 (\exists y_1 y'_1 \forall u_1) \dots (\exists y_n y'_n \forall u_n) \cdot \bigcup_{i \in [0 \dots n]} \{C_i, C'_i\}$$

757 with

$$758 \quad C_0 = \{\bar{y}_0\} \qquad C'_0 = \{y_0, \bar{y}_1, \bar{y}'_1\}$$

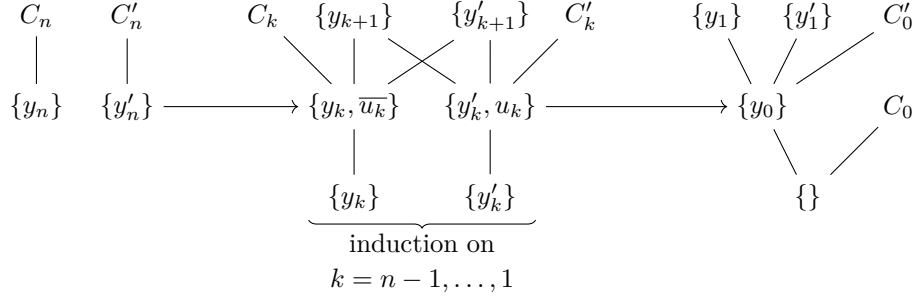
$$759 \quad C_k = \{y_k, \bar{u}_k, \bar{y}_{k+1}, \bar{y}'_{k+1}\} \qquad C'_k = \{y'_k, u_k, \bar{y}_{k+1}, \bar{y}'_{k+1}\}$$

$$760 \quad C_n = \{y_n, \bar{u}_n\} \qquad C'_n = \{y'_n, u_n\}$$

761

763 for $1 \leq k < n$.

764 ϕ_n is also a false QBF and the existential player can force the universal player to follow
765 the same strategy as in KBKF: setting $u_k = y'_k$ for each $k \in [n]$. (Note that this is not
766 a unique winning strategy, since the existential player could leave the universal player a
767 wide range of freedom in assigning the universal variables.) To force the universal player
768 assigning variables according to the KBKF-strategy, the existential player will assign $y_0 = 0$
769 and $y'_k \neq y_k$ in every round $k \in [n]$. The last remaining clauses are $C_n = \{y_n, \bar{u}_n\}$ and
770 $C'_n = \{y'_n, u_n\}$, and every so constructed assignment falsifies exactly one of them: $y_n = 0$,
771 $y'_n = 1 = u_n$ falsifies C_n and $y_n = 1, y'_n = 0 = u_n$ falsifies C'_n ; in each case the other clause
772 is satisfied. Thus it is sufficient for the set F of target clauses to contain one of the two
773 clauses. For KBKF $F = \{C_n, C'_n\}$ was chosen (which is not minimal), which makes the tail
774 construction generating just the KBKF formulas. Polynomial-size Q-Res refutations of ϕ_n
775 are shown in Figure 9.



■ **Figure 9** Polynomial-size Q-Res refutation of the base formulas ϕ_n of KBKF_n .

776 Hence $(\phi_i)_{i \in \mathbb{N}}$ has exponential strategy size and short Q-Res refutations, thus satisfying
 777 the conditions of the tail construction. It follows immediately, that the KBKF formulas
 778 separate Q-Res from QU-Res.

779 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
 780 be removed from one of the clauses C_n or C'_n without affecting the separation property.

781 6 Conclusion and Open Problems

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

788 A related question is which exact class of formulas can be generated by our construction.
 789 As we always import hardness via the size-cost method, one might aim for a construction
 790 that yields all such formulas. We do not achieve this yet, as one can even find Σ_3^b -formulas
 791 with high costs that do not stem from our method. Of course there are also further sources
 792 of hardness. E.g. the parity formulas [15] are hard for QU-Res, but have small cost. Finding
 793 general constructions for other QBF families, where hardness does not originate from cost,
 794 also appears interesting for future work.

795 — References —

- 796 1 Hoda Abbasizanjani. *The combinatorics of minimal unsatisfiability: connecting to graph theory*.
 797 dissertation, Department of Computer Science, Swansea University, 2021.
- 798 2 Hoda Abbasizanjani and Oliver Kullmann. Minimal unsatisfiability and minimal strongly
 799 connected digraphs. In Olaf Beyersdorff and Christoph M. Wintersteiger, editors, *Theory*
 800 *and Applications of Satisfiability Testing (SAT)*, volume 10929 of *Lecture Notes in Computer*
 801 *Science*, pages 329–345. Springer, 2018.
- 802 3 Hoda Abbasizanjani and Oliver Kullmann. Classification of minimally unsatisfiable 2-
 803 cnfs. *CoRR*, abs/2003.03639, 2020. URL: <https://arxiv.org/abs/2003.03639>, arXiv:
 804 2003.03639.
- 805 4 Albert Atserias, Johannes Klaus Fichte, and Marc Thurley. Clause-learning algorithms with
 806 many restarts and bounded-width resolution. *J. Artif. Intell. Res.*, 40:353–373, 2011.
- 807 5 Valeriy Balabanov and Jie-Hong R. Jiang. Unified QBF certification and its applications.
 808 *Formal Methods in System Design*, 41(1):45–65, 2012.

- 809 6 Valeriy Balabanov, Magdalena Widl, and Jie-Hong R. Jiang. QBF resolution systems and
810 their proof complexities. In *Proc. Theory and Applications of Satisfiability Testing (SAT)*,
811 pages 154–169, 2014.
- 812 7 P. Beame and T. Pitassi. Simplified and improved resolution lower bounds. In *Proc. 37th*
813 *IEEE Symposium on the Foundations of Computer Science*, pages 274–281. IEEE Computer
814 Society Press, 1996.
- 815 8 Paul Beame, Henry A. Kautz, and Ashish Sabharwal. Towards understanding and harnessing
816 the potential of clause learning. *J. Artif. Intell. Res. (JAIR)*, 22:319–351, 2004.
- 817 9 Olaf Beyersdorff and Joshua Blinkhorn. Lower bound techniques for QBF expansion. *Theory*
818 *Comput. Syst.*, 64(3):400–421, 2020.
- 819 10 Olaf Beyersdorff and Joshua Blinkhorn. A simple proof of QBF hardness. *Information*
820 *Processing Letters*, 168, 2021.
- 821 11 Olaf Beyersdorff, Joshua Blinkhorn, and Luke Hinde. Size, cost, and capacity: A semantic
822 technique for hard random QBFs. *Logical Methods in Computer Science*, 15(1), 2019.
- 823 12 Olaf Beyersdorff, Joshua Blinkhorn, and Meena Mahajan. Hardness characterisations and
824 size-width lower bounds for QBF resolution. In *Proc. ACM/IEEE Symposium on Logic in*
825 *Computer Science (LICS)*, pages 209–223. ACM, 2020.
- 826 13 Olaf Beyersdorff, Joshua Blinkhorn, and Meena Mahajan. Building strategies into QBF proofs.
827 *J. Autom. Reasoning*, 65(1):125–154, 2021.
- 828 14 Olaf Beyersdorff and Benjamin Böhm. Understanding the Relative Strength of QBF CDCL
829 Solvers and QBF Resolution. In *12th Innovations in Theoretical Computer Science Conference*
830 *(ITCS 2021)*, volume 185 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages
831 12:1–12:20, 2021.
- 832 15 Olaf Beyersdorff, Leroy Chew, and Mikolás Janota. New resolution-based QBF calculi and
833 their proof complexity. *ACM Transactions on Computation Theory*, 11(4):26:1–26:42, 2019.
- 834 16 Olaf Beyersdorff and Luke Hinde. Characterising tree-like Frege proofs for QBF. *Inf. Comput.*,
835 268, 2019.
- 836 17 Olaf Beyersdorff, Luke Hinde, and Ján Pich. Reasons for hardness in QBF proof systems.
837 *ACM Transactions on Computation Theory*, 12(2), 2020.
- 838 18 Olaf Beyersdorff, Mikolás Janota, Florian Lonsing, and Martina Seidl. Quantified boolean
839 formulas. In Armin Biere, Marijn Heule, Hans van Maaren, and Toby Walsh, editors, *Handbook*
840 *of Satisfiability*, Frontiers in Artificial Intelligence and Applications, pages 1177–1221. IOS
841 Press, 2021.
- 842 19 Olaf Beyersdorff, Luca Pulina, Martina Seidl, and Ankit Shukla. Qbffam: A tool for generating
843 QBF families from proof complexity. In Chu-Min Li and Felip Manyà, editors, *Theory and*
844 *Applications of Satisfiability Testing (SAT)*, volume 12831 of *Lecture Notes in Computer*
845 *Science*, pages 21–29. Springer, 2021.
- 846 20 Nikolaj Bjørner, Mikolás Janota, and William Klieber. On conflicts and strategies in QBF.
847 In Ansgar Fehnker, Annabelle McIver, Geoff Sutcliffe, and Andrei Voronkov, editors, *20th*
848 *International Conferences on Logic for Programming, Artificial Intelligence and Reasoning*
849 *LPAR 2015*, volume 35 of *EPiC Series in Computing*, pages 28–41. EasyChair, 2015.
- 850 21 Maria Luisa Bonet, Juan Luis Esteban, Nicola Galesi, and Jan Johannsen. On the rel-
851 ative complexity of resolution refinements and cutting planes proof systems. *SIAM J.*
852 *Comput.*, 30(5):1462–1484, 2000. URL: <http://dx.doi.org/10.1137/S0097539799352474>,
853 doi:10.1137/S0097539799352474.
- 854 22 Sam Buss and Jakob Nordström. Proof complexity and SAT solving. In Armin Biere, Marijn
855 Heule, Hans van Maaren, and Toby Walsh, editors, *Handbook of Satisfiability*, Frontiers in
856 Artificial Intelligence and Applications, pages 233–350. IOS Press, 2021.
- 857 23 Leroy Chew. *QBF proof complexity*. PhD thesis, University of Leeds, Leeds, 2017.
- 858 24 Leroy Chew and Friedrich Slivovsky. Towards uniform certification in QBF. *Electron. Collo-*
859 *quium Comput. Complex.*, 2021. To appear at STACS 2022. URL: [https://eccc.weizmann.
860 ac.il/report/2021/144](https://eccc.weizmann.ac.il/report/2021/144).

- 861 25 Judith Clymo. *Proof Complexity for Quantified Boolean Formulas*. PhD thesis, School of
862 Computing, University of Leeds, 2021.
- 863 26 Stephen A. Cook and Phuong Nguyen. *Logical Foundations of Proof Complexity*. Cambridge
864 University Press, 2010.
- 865 27 Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof
866 systems. *The Journal of Symbolic Logic*, 44(1):36–50, 1979.
- 867 28 Uwe Egly, Florian Lonsing, and Magdalena Widl. Long-distance resolution: Proof generation
868 and strategy extraction in search-based QBF solving. In *Proc. Logic for Programming, Artificial
869 Intelligence, and Reasoning (LPAR)*, pages 291–308, 2013.
- 870 29 Amin Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308,
871 1985.
- 872 30 Mikolás Janota and Joao Marques-Silva. Expansion-based QBF solving versus Q-resolution.
873 *Theor. Comput. Sci.*, 577:25–42, 2015.
- 874 31 Hans Kleine Büning, Marek Karpinski, and Andreas Flögel. Resolution for quantified Boolean
875 formulas. *Inf. Comput.*, 117(1):12–18, 1995.
- 876 32 Jan Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, volume 60 of
877 *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, Cambridge,
878 1995.
- 879 33 Jan Krajíček. *Proof complexity*, volume 170 of *Encyclopedia of Mathematics and Its Applications*.
880 Cambridge University Press, 2019.
- 881 34 Florian Lonsing, Uwe Egly, and Allen Van Gelder. Efficient clause learning for quantified
882 Boolean formulas via QBF pseudo unit propagation. In *Proc. International Conference on
883 Theory and Applications of Satisfiability Testing (SAT)*, pages 100–115, 2013.
- 884 35 Tomáš Peitl, Friedrich Slivovsky, and Stefan Szeider. Proof complexity of fragments of long-
885 distance Q-resolution. In Mikolás Janota and Inês Lynce, editors, *Theory and Applications of
886 Satisfiability Testing - SAT 2019 - 22nd International Conference, SAT, Proceedings*, volume
887 11628 of *Lecture Notes in Computer Science*, pages 319–335. Springer, 2019.
- 888 36 Knot Pipatsrisawat and Adnan Darwiche. On the power of clause-learning SAT solvers as
889 resolution engines. *Artif. Intell.*, 175(2):512–525, 2011.
- 890 37 Nathan Segerlind. The complexity of propositional proofs. *Bulletin of Symbolic Logic*,
891 13(4):417–481, 2007.
- 892 38 M. Sipser. *Introduction to the Theory of Computation*. Course Technology, 2nd edition,
893 February 2005.
- 894 39 Alasdair Urquhart. Hard examples for resolution. *J. ACM*, 34(1):209–219, 1987.
- 895 40 Allen Van Gelder. Contributions to the theory of practical quantified Boolean formula solving.
896 In *Proc. Principles and Practice of Constraint Programming (CP)*, pages 647–663, 2012.
- 897 41 Lintao Zhang and Sharad Malik. Conflict driven learning in a quantified Boolean satisfiability
898 solver. In *Proc. IEEE/ACM International Conference on Computer-aided Design (ICCAD)*,
899 pages 442–449, 2002.