A Little Blocked Literal Goes a Long Way*

Benjamin Kiesl[1], Marijn J.H. Heule[2], and Martina Seidl[3]

[1] Institute of Information Systems, Vienna University of Technology
[2] Department of Computer Science, The University of Texas at Austin
[3] Institute for Formal Models and Verification, JKU Linz

Abstract. Q-resolution is a generalization of propositional resolution that provides the theoretical foundation for search-based solvers of quantified Boolean formulas (QBFs). Recently, it has been shown that an extension of Q-resolution, called long-distance resolution, is remarkably powerful both in theory and in practice. However, it was unknown how long-distance resolution is related to QRAT, a proof system introduced for certifying the correctness of QBF-preprocessing techniques. We show that QRAT polynomially simulates long-distance resolution. Two simple rules of QRAT are crucial for our simulation—*blocked-literal addition* and *blocked-literal elimination*. Based on the simulation, we implemented a tool that transforms long-distance-resolution proofs into QRAT proofs. In a case study, we compare long-distance-resolution proofs of the well-known Kleine Büning formulas with corresponding QRAT proofs.

1 Introduction

Quantified Boolean formulas (QBF) [19] extend propositional formulas with existential and universal quantifiers over the propositional variables. These quantifiers lead to increased expressiveness, which makes QBF attractive for reasoning problems in areas such as formal verification and artificial intelligence [3].

To obtain a better understanding of the strengths and limitations of different QBF-solving approaches, their underlying proof systems have been extensively analyzed, providing a comprehensive proof-complexity landscape for QBF [6, 10, 9, 4, 16]. Two kinds of proof systems have received particular attention: instantiation-based proof systems [5, 6], which provide the foundation for expansion-based solvers like `RAReQS` [18], and resolution-based proof systems [16, 20, 26, 1, 24, 2, 7, 17, 23], which provide the foundation for search-based solvers like `DepQBF` [22]. Apart from these, also sequent systems have been studied [10, 8]. There is, however, another practically useful proof system—quite different from the aforementioned ones—whose place in the complexity landscape was still unclear: the QRAT proof system [15].

The QRAT proof system is a generalization of DRAT [25] (the de-facto standard for proofs in practical SAT solving) that has its strengths when it comes

* This work has been supported by the Austrian Science Fund (FWF) under projects W1255-N23 and S11408-N23, and by the National Science Foundation (NSF) under grant number CCF-1618574.

to preprocessing: Many QBF solvers use preprocessing techniques to simplify a QBF before they actually evaluate its truth. With the QRAT system, it is possible to certify the correctness of virtually all preprocessing simplifications performed by state-of-the-art QBF solvers and preprocessors. Additionally, there exist efficient tools for checking the correctness of QRAT proofs as well as for extracting winning strategies (so-called *Skolem functions*) from QRAT proofs of satisfiability [15].

It can be easily seen that QRAT simulates the basic Q-resolution calculus [20] that allows only resolution upon existential variables. Likewise, it simulates the calculus QU-Res [24], which extends Q-resolution by allowing resolution upon universal variables. So far, however, it was unclear how QRAT is related to the long-distance-resolution calculus [26, 1]—a calculus that is particularly popular because it allows for short proofs both in theory and in practice [11].

In this paper, we prove that QRAT can polynomially simulate the long-distance-resolution calculus. For our simulation, we need only Q-resolution and universal reduction together with blocked-literal elimination and blocked-literal addition using fresh variables [14, 21]. These four rules are allowed in QRAT. To illustrate the power of blocked literals, we present handcrafted QRAT proofs of the formulas commonly used to display the strength of long-distance resolution—the well-known *Kleine Büning formulas* [20]. Our proofs are slightly smaller than the long-distance resolution proofs of these formulas described by Egly et al. [11].

To put our simulation into practice, we implemented a tool that transforms long-distance-resolution proofs into QRAT proofs. With this tool it is now possible to obtain QRAT proofs that certify the correctness of both the preprocessing and the actual solving, even when using a QBF solver based on long-distance resolution. We used our tool to transform long-distance-resolution proofs of the Kleine Büning formulas into QRAT proofs. We compare the resulting proofs with the handcrafted QRAT proofs as well as with the original proofs. Rounding off the picture, we locate QRAT in the proof-complexity landscape of resolution-based proof systems and discuss open questions.

2 Preliminaries

In the following, we introduce the background required to understand the rest of the paper. A *literal* is either a variable x (a *positive literal*) or the negation $\bar{x}$ of a variable x (a *negative literal*). The complement $\bar{l}$ of a literal l is defined as $\bar{x}$ if $l = x$ and as x if $l = \bar{x}$. A *clause* is a disjunction of literals. A (*propositional*) *formula* in *conjunctive normal form* (CNF) is a conjunction of clauses. A clause can be seen as a set of literals and a formula can be seen as a set of clauses.

A *quantifier prefix* has the form $Q_1 X_1 \dots Q_q X_q$, where all the X_i are mutually disjoint sets of variables, $Q_i \in \{\forall, \exists\}$, and $Q_i \neq Q_{i+1}$. A *quantified Boolean formula* (QBF) ϕ in *prenex conjunctive normal form* (PCNF) is of the form $\Pi.\psi$ where Π is a quantifier prefix and ψ, called the *matrix* of ϕ, is a propositional formula in CNF. The quantifier $Q(\Pi, l)$ of a literal l is Q_i if $var(l) \in X_i$. Let $Q(\Pi, l) = Q_i$ and $Q(\Pi, k) = Q_j$, then $l \leq_\Pi k$ if $i \leq j$, and $l <_\Pi k$ if $i < j$.

Using the truth constants 1 (*true*) and 0 (*false*), a QBF $\forall x \Pi.\psi$ is false iff at least one of $\Pi.\psi[x/1]$ and $\Pi.\psi[x/0]$ is false where $\Pi.\psi[x/t]$ is obtained from $\Pi.\psi$ by replacing all occurrences of x in ψ by t and removing x from Π. Respectively, a QBF $\exists x \Pi.\psi$ is false iff both $\Pi.\psi[x/1]$ and $\Pi.\psi[x/0]$ are false. If the matrix ψ of ϕ contains the empty clause (denoted by $\bot$) after eliminating the truth constants according to standard rules, then ϕ is false. If ψ is empty, ϕ is true.

2.1 Resolution-Based Calculi

In resolution-based calculi, a proof P of a QBF $\Pi.\psi = \Pi.C_1 \wedge \cdots \wedge C_m$ is a sequence $C_{m+1}, \ldots, C_n$ of clauses with $C_n = \bot$ and for every C_i $(m+1 \leq i \leq n)$, it holds that C_i has been derived from clauses in ψ or from earlier clauses in P (i.e., from clauses with index strictly smaller than i) by applications of either the $\forall$-*red* rule (also called *universal reduction*) or instantiations of the *resolution* rule which are defined as follows:

$$\frac{C \vee x}{C}\ (\forall\text{-red}) \qquad \frac{C \vee l \qquad D \vee \bar{l}}{C \vee D}\ (\text{resolution})$$

The rule $\forall$-red is only applicable if the literal x is universal and if for every existential literal $l \in C$, it holds that $l <_\Pi x$. In the resolution rule, the resolvent $C \vee D$ is derived from its two antecedent clauses. We assume that no clause in ψ contains complementary literals, otherwise the $\forall$-red rule is unsound.

The most basic resolution-based calculus for QBF is the *Q-resolution calculus* (Q-Res) [20]. It uses the resolution rule *Q-res* which requires that (1) l is existential and (2) C does not contain a literal x such that $\bar{x} \in D$. In contrast, the *long-distance-resolution calculus* (LQ-Res) [26, 1] uses a less restrictive variant of the resolution rule, called *LQ-res*, which requires that (1) l is existential and (2) for every literal $x \in C$ such that $\bar{x} \in D$, it holds that x is universal and $l <_\Pi x$. Note that every Q-res step is also an LQ-res step. In the rest of the paper, we refer to resolution steps as LQ-res steps only if they are not Q-res steps, otherwise we refer to them as Q-res steps. Note that in the literature a complementary pair $x, \bar{x}$ is also represented by a so-called *merged literal* x^*.

Example 1. Consider the QBF $\phi = \exists a \forall x \exists b \exists c.(\bar{a} \vee \bar{x} \vee c) \wedge (\bar{x} \vee b \vee \bar{c}) \wedge (a \vee x \vee b) \wedge (\bar{b})$. The following is a long-distance-resolution proof of ϕ: $\bar{a} \vee \bar{x} \vee b$, $x \vee \bar{x} \vee b$, $x \vee \bar{x}$, x, $\bot$. We explain this proof in more detail later (also see Fig. 1 on page 5).

2.2 The QRAT Proof System Light

In this paper, we do not need the power of the full QRAT proof system [15]. We therefore introduce only a very restricted version of QRAT that is sufficient for the simulation of the long-distance-resolution calculus.

One of the main concepts in this variant of QRAT is the concept of a *blocked literal*. For the definition of blocked literals, we first have to introduce so-called *outer resolvents*. Given two clauses $C \vee x, D \vee \bar{x}$ of a QBF $\Pi.\psi$, the outer resolvent $C \vee x \bowtie^x_\Pi D \vee \bar{x}$ of $C \vee x$ with $D \vee \bar{x}$ upon x is the clause consisting of all literals in C together with those literals of D that occur outer to x, i.e., the outer resolvent is the clause $C \cup \{l \mid l \in D \text{ and } l \leq_\Pi x\}$. We can now define blocked literals:

Definition 1. *A universal literal x is* blocked *in a clause $C \vee x$ w.r.t. a QBF $\Pi.\psi$ if, for every clause $D \vee \bar{x} \in \psi \setminus \{C \vee x\}$, the outer resolvent $C \vee x \bowtie^x_\Pi D \vee \bar{x}$ contains a pair of complementary literals.*

Example 2. Let $\phi = \exists a \forall x, y \exists b.(a \vee x \vee y) \wedge (\bar{a} \vee \bar{x} \vee b) \wedge (\bar{y} \vee \bar{x} \vee b)$. The literal x is blocked in $a \vee x \vee y$ w.r.t. ϕ: There are two outer resolvents of $a \vee x \vee y$ upon x, namely $a \vee y \vee \bar{a}$, obtained by resolving with $\bar{a} \vee \bar{x} \vee b$, and $a \vee y \vee \bar{y}$, obtained by resolving with $\bar{y} \vee \bar{x} \vee b$. Both contain a pair of complementary literals. □

If a literal is blocked in a clause, its removal is called *blocked-literal elimination* (BLE) [14]. If, after adding a literal to a clause, the literal is blocked in that clause, then this addition is called *blocked-literal addition* (BLA). Both BLE and BLA do not change the truth value of a formula.

In our restricted variant of QRAT, a *derivation* for a QBF ϕ is a sequence $M_1, \ldots, M_n$ of proof steps. Starting with $\phi_0 = \phi$, every M_i modifies ϕ_{i-1} in one of the following four ways, which results in a new formula ϕ_i: (1) It adds to ϕ_{i-1} a clause that is derived from two clauses in ϕ_{i-1} via a resolution step. (2) It adds to ϕ_{i-1} a clause C that is obtained from a clause $C \vee x \in \phi_{i-1}$ by a $\forall$-red step, with the additional restriction that C does not contain $\bar{x}$. (3) It adds a blocked literal to a clause in ϕ_{i-1}. (4) It removes a blocked literal from a clause in ϕ_{i-1}.

A QRAT derivation $M_1, \ldots, M_n$ therefore gradually derives new formulas $\phi_1, \ldots, \phi_n$ from the starting formula ϕ. If the final formula ϕ_n contains the empty clause $\bot$, then the derivation is a (*refutation*) *proof* of ϕ. Note that the $\forall$-red rule in QRAT is more restricted than the $\forall$-red rule from the resolution-based calculi, making it sound also when clauses contain complementary literals.

To simplify the presentation, we do not specify how the modification steps M_i are represented syntactically. We also do not include clause deletion. Note that certain proof steps can modify the quantifier prefix by introducing new or removing existing variables. Note also that Q-resolution proofs do not contain complementary literals, so they can be simply rewritten into QRAT proofs using only Q-res and $\forall$-red steps. Finally, we want to highlight that for our simulation, we do not need the unrestricted resolution rule; the Q-res rule suffices.

3 Illustration of the Simulation

We start by illustrating on an example how our restricted variant of QRAT can simulate the long-distance-resolution calculus. As already mentioned, the $\forall$-red rule used in QRAT is more restricted than the one in the long-distance-resolution calculus because it does not allow us to remove a literal x from a clause that contains $\bar{x}$. This means that once we derive a clause that contains both a literal x and its complement $\bar{x}$, we cannot simply get rid of the two literals by using the $\forall$-red rule. We therefore want to avoid the derivation of clauses with complementary literals entirely. Now, the only way the long-distance-resolution calculus can derive such clauses is via resolution (LQ-res) steps. So to avoid the complementary literals, we eliminate them already before performing the resolution steps. We demonstrate this on an example:

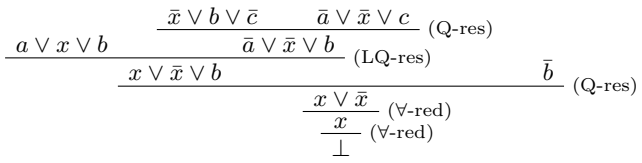

Fig. 1. LQ-res proof of QBF $\phi = \exists a \forall x \exists b \exists c.(\bar{a} \vee \bar{x} \vee c) \wedge (\bar{x} \vee b \vee \bar{c}) \wedge (a \vee x \vee b) \wedge (\bar{b})$.

Example 3. Consider the QBF $\phi = \exists a \forall x \exists b \exists c.(\bar{a} \vee \bar{x} \vee c) \wedge (\bar{x} \vee b \vee \bar{c}) \wedge (a \vee x \vee b) \wedge (\bar{b})$ from Example 1. To increase readability, we illustrate its long-distance-resolution proof as a proof tree in Fig. 1. To simulate this proof with QRAT, we first add the resolvent $\bar{a} \vee \bar{x} \vee b$ to ϕ via a Q-res step to obtain the new formula ϕ'. Now we cannot simply perform the next derivation step (the LQ-res step) because the resulting resolvent $x \vee \bar{x} \vee b$ would contain complementary literals. To deal with this, we try to eliminate x from the clause $a \vee x \vee b$. This is where the addition and elimination of blocked literals come into play.

We cannot yet eliminate x from ϕ' because x is not blocked in $a \vee x \vee b$ with respect to ϕ': For x to be blocked, all outer resolvents of $a \vee x \vee b$ upon x must contain complementary literals. The clauses that can be resolved with $a \vee x \vee b$ are $\bar{a} \vee \bar{x} \vee c$, $\bar{a} \vee \bar{x} \vee b$, and $\bar{x} \vee b \vee \bar{c}$. While the outer resolvents with the former two clauses contain the complementary literals a and $\bar{a}$, the outer resolvent $a \vee b$, obtained by resolving with $\bar{x} \vee b \vee \bar{c}$, does not contain complementary literals.

Now we use a feature of QRAT to make x blocked in $a \vee x \vee b$: We add a new literal x' (which goes to the same quantifier block as x) to $a \vee x \vee b$ to turn it into $a \vee x' \vee x \vee b$. The addition of x' is clearly a blocked-literal addition as there are no outer resolvents of $a \vee x' \vee x \vee b$ upon x'. Likewise, we add the complement $\bar{x}'$ of x' to $\bar{x} \vee b \vee \bar{c}$ to turn it into $\bar{x}' \vee \bar{x} \vee b \vee \bar{c}$. Again this is a blocked-literal addition since $a \vee x' \vee x \vee b$ (which is the only clause containing the complement x' of $\bar{x}'$) contains x while $\bar{x}' \vee \bar{x} \vee b \vee \bar{c}$ contains $\bar{x}$.

Now the complementary pair $x', \bar{x}'$ is contained in the outer resolvent of $a \vee x' \vee x \vee b$ with $\bar{x}' \vee \bar{x} \vee b \vee \bar{c}$ upon x. Thus, the literal x becomes blocked in $a \vee x' \vee x \vee b$ and so we can remove it to obtain $a \vee x' \vee b$. We have thus replaced x in $a \vee x \vee b$ by x' and now we can resolve $a \vee x' \vee b$ with $\bar{a} \vee \bar{x} \vee b$ upon a to obtain the resolvent $x' \vee \bar{x} \vee b$ (instead of $x \vee \bar{x} \vee b$ as in the original proof). Finally, we resolve $x' \vee \bar{x} \vee b$ with $\bar{b}$ to obtain $x' \vee \bar{x}$ from which we derive the empty clause $\bot$ via ∀-red steps. □

To summarize, we start by adding clauses of a given long-distance-resolution proof to our formula until we bump into an LQ-res step. To avoid complementary literals in the resolvent of the LQ-res step, we then use blocked-literal addition and blocked-literal elimination to replace these literals. After this, we can derive a resolvent without complementary literals and move on until we encounter the next LQ-res step, which we again eliminate. We repeat this procedure until the whole long-distance-resolution proof is turned into a QRAT proof.

Note that the modification of existing clauses has an impact on later derivations. For instance, by replacing $a \vee x \vee b$ in the above example with $a \vee x' \vee b$, we not only affected the immediate resolvent $x \vee \bar{x} \vee b$, which we turned into $x' \vee \bar{x} \vee b$, but also the later resolvent $x \vee \bar{x}$, which became $x' \vee \bar{x}$. We therefore have to show that these modifications are harmless in the sense that they do not lead to an invalid proof. We do so in the next section, where we define our simulation in detail before proving that it indeed produces a valid QRAT proof.

4 Simulation

We first describe our simulation procedure on a high level before we specify the details and prove its correctness. As we have seen, given a long-distance-resolution proof, we can use QRAT to derive all clauses up to the first LQ-res step. The crucial part of the simulation is then the elimination of complementary literals from this LQ-res step, which might involve the modification of several clauses via the addition and elimination of blocked literals.

Let $\phi = \Pi.C_1 \wedge \cdots \wedge C_m$ be a QBF and $P = C_{m+1}, \ldots, C_r, \ldots, C_n$ be a long-distance-resolution proof of ϕ where C_r is the first clause derived via an LQ-res step. If there is no such C_r, the proof can be directly translated to QRAT. Otherwise, in a first step, our procedure produces a QRAT derivation that adds all the clauses $C_{m+1}, \ldots, C_{r-1}$ to ϕ by using Q-res and $\forall$-red steps. It then uses blocked-literal addition and blocked-literal elimination to avoid complementary literals in the resolvent C_r, which it thereby turns into a different resolvent C'_r. After this, it adds C'_r to ϕ via a Q-res step. The result is a QRAT derivation of a formula ϕ' from ϕ. We explain this first step in Section 4.1.

In a second step, the procedure first removes all the clauses $C_{m+1}, \ldots, C_r$ from P since they—or their modified variants—are now all contained in ϕ'. As several clauses have been modified via blocked-literal addition and blocked-literal elimination in the first step, it then propagates these modifications through the remaining part of P. This turns P into a long-distance resolution proof P' of ϕ'. We explain this second step in Section 4.2.

By repeating these two steps for every LQ-res step, we finally obtain a QRAT proof of ϕ. Thus, we have to show that after the above two steps (i.e., after one iteration of our procedure), ϕ' is obtained by a valid QRAT derivation and the proof P' is a valid long-distance-resolution proof of ϕ' that is shorter than P. The correctness of the simulation follows then simply by induction.

To simplify the presentation, we assume that the long-distance resolvent C_r contains only one pair of complementary literals, i.e., $C_r = C \vee D \vee x \vee \bar{x}$ was derived from two clauses $C \vee l \vee x$ and $D \vee \bar{l} \vee \bar{x}$ where C does not contain a literal k such that $\bar{k}$ is contained in D. Although this assumption leads to a loss of generality, we show later that our argument can be easily extended to the more general case where C and D are allowed to contain multiple pairs of complementary literals.

4.1 QRAT Derivation of the Formula ϕ'

Below we describe the QRAT derivation of ϕ' from ϕ. Initially, $\phi' = \phi$.

1. Add the clauses $C_{m+1}, \dots C_{r-1}$ to ϕ' via Q-res and $\forall$-red steps.
2. Consider the LQ-res step that derived $C_r = C \vee D \vee x \vee \bar{x}$ from two clauses $C \vee l \vee x$ and $D \vee \bar{l} \vee \bar{x}$:
$$\frac{C \vee l \vee x \qquad D \vee \bar{l} \vee \bar{x}}{C \vee D \vee x \vee \bar{x}}\ \text{(LQ-res)}$$
Towards making x blocked in $C \vee l \vee x$, add a new literal x' (that goes to the same quantifier block as x) to $C \vee l \vee x$ to turn it into $C \vee l \vee x' \vee x$.
3. Add $\bar{x}'$ to each clause $C_i \in \phi'$ for which (1) $\bar{x} \in C_i$, and (2) the outer resolvent of $C \vee l \vee x' \vee x$ and C_i upon x is not a tautology.
4. Now x is a blocked literal in $C \vee l \vee x' \vee x$. Eliminate it to obtain $C \vee l \vee x'$.
5. Add the clause $C \vee D \vee x' \vee \bar{x}$ to ϕ' by performing a Q-res step of $C \vee l \vee x'$ and $D \vee \bar{l} \vee \bar{x}$ upon l.

To see that this results in a valid QRAT derivation, observe the following: In step 2, the addition of x' is a blocked-literal addition, since $\bar{x}'$ is not contained in any of the clauses. In step 3, for every C_i with $\bar{x} \in C_i$, the addition of $\bar{x}'$ is a blocked-literal addition as only $C \vee l \vee x' \vee x$ can be resolved with C_i upon $\bar{x}'$ and the corresponding outer resolvent contains x and $\bar{x}$. Note that instead of eliminating x from $C \vee l \vee x$, we could have also eliminated $\bar{x}$ from $D \vee \bar{l} \vee \bar{x}$. It remains to modify the long-distance-resolution proof P of ϕ so that it becomes a valid proof of ϕ'.

4.2 Modification of the Long-Distance-Resolution Proof

We next turn the proof $P = C_{m+1}, \dots, C_r, \dots, C_n$ of ϕ into a proof P' of ϕ'. First, we remove the clauses $C_{m+1}, \dots, C_r$ from P since ϕ' already contains variants $C'_{m+1}, \dots, C'_r$ of these clauses. Second, since we have modified the clauses in ϕ', we have to propagate these modifications through the remaining proof.

Assume, for instance, that in P the clause C_{r+1} has been obtained by resolving a clause C_i with a clause C_j. Both C_i and C_j might have been affected by blocked-literal additions so that they are now different clauses $C'_i, C'_j \in \phi'$. To account for these modifications of C_i and C_j, we replace C_{r+1} in P by the resolvent of C'_i and C'_j. Moreover, in cases where P removes x from a clause via a $\forall$-red step, we now also remove x'. Analogously for $\bar{x}'$ and $\bar{x}$.

To formalize these modifications, we first assign to every clause C_i with $1 \leq i \leq r$ its corresponding clause of ϕ' as follows:

$$C'_i = \begin{cases} C_i \cup \{\bar{x}'\} & \text{if } \bar{x} \in C_i \text{ and the outer resolvent of } C \vee l \vee x \vee x' \\ & \text{and } C_i \text{ upon } x \text{ is not a tautology;} \\ (C_i \setminus \{x\}) \cup \{x'\} & \text{if } C_i = C_r \text{ or } C_i = C \vee l \vee x; \\ C_i & \text{otherwise.} \end{cases}$$

Note that, by construction, $C'_i \in \phi'$ for $1 \leq i \leq r$. For every i such that $r < i \leq n$, we step-by-step, starting with $i = r + 1$, define C'_i based on the derivation rule that was used for deriving C_i in P. We distinguish between clauses derived by resolution steps and clauses derived by $\forall$-red steps:

Case 1: C_i has been derived via a resolution step of two clauses $C_j = C \vee l$ and $C_k = D \vee \bar{l}$ upon l, i.e., $C_i = C \vee D$. We define $C'_i = C'_j \setminus \{l\} \vee C'_k \setminus \{\bar{l}\}$.

Case 2: C_i has been derived from a clause C_j via a $\forall$-red step. If the $\forall$-red step removes a literal l with $var(l) \neq var(x)$, we define $C'_i = C'_j \setminus \{l\}$. If it removes x, we define $C'_i = C'_j \setminus \{x, x'\}$, and if it removes $\bar{x}$, we define $C'_i = C'_j \setminus \{\bar{x}, \bar{x}'\}$.

Note that $\forall$-red steps of x and $\bar{x}$ in P' might remove two literals at once. Although such $\forall$-red steps do not constitute valid derivation steps in a strict sense, this is not a serious problem: These steps can be easily rewritten into two distinct $\forall$-red steps since x and x' are in the same quantifier block. For instance, the left step below can be rewritten into the two steps on the right:

$$\frac{C \vee x \vee x'}{C}\ (\forall\text{-red}) \qquad \frac{\dfrac{C \vee x \vee x'}{C \vee x}\ (\forall\text{-red})}{C}\ (\forall\text{-red})$$

Next, we show that the resulting proof P' is—apart from the minor detail just mentioned—a valid long-distance-resolution proof of ϕ'.

4.3 Correctness of the Simulation

To prove the correctness of our simulation, we first introduce a lemma that guarantees that the modified long-distance-resolution proof P' has a similar structure as the original proof P:

Lemma 1. *Let $\phi' = \Pi'.C'_1 \wedge \cdots \wedge C'_r$ and $P' = C'_{r+1}, \ldots, C'_n$ be obtained from $\phi = \Pi.C_1 \wedge \cdots \wedge C_m$ and $P = C_{m+1}, \ldots, C_r, \ldots, C_n$ as defined above. Then, for every clause C'_i with $1 \leq i \leq n$, the following holds: (1) If x' or x is in C'_i, then $x \in C_i$. (2) If $\bar{x}'$ or $\bar{x}$ is in C'_i, then $\bar{x} \in C_i$. (3) C'_i agrees with C_i on all literals whose variables are different from x and x', i.e., $C'_i \setminus \{x, \bar{x}, x', \bar{x}'\} = C_i \setminus \{x, \bar{x}\}$.*

Proof. By induction on i.

Base Case ($i \leq r$): The claim holds by the definition of C'_i.

Induction Step ($r < i$): Consider the clause C_i in P that corresponds to C'_i. We proceed by a case distinction based on how C_i was derived in P.

Case 1: C_i is a resolvent $C_j \setminus \{l\} \vee C_k \setminus \{\bar{l}\}$ of two clauses C_j, C_k. In this case, $C'_i = C'_j \setminus \{l\} \vee C'_k \setminus \{\bar{l}\}$. By the induction hypothesis, the statement holds for C'_j and C'_k. Now, if C'_i contains x' or x, then at least one of C'_j and C'_k must contain x' or x and thus one of C_j and C_k must contain x, hence $x \in C_i$. Analogously, if C'_i contains $\bar{x}'$ or $\bar{x}$, then C_i contains $\bar{x}$. Now, C'_j agrees with C_j on all literals

whose variables are different from x and x', and the same holds for C'_k and C_k. Thus, C'_i agrees with C_i on all literals whose variables are different from x and x'.

Case 2: C_i has been derived from a clause C_j via a $\forall$-red step, i.e., $C_i = C_j \setminus \{y\}$ for some universal literal y. By the induction hypothesis, the statement holds for C'_j. If $var(y) \neq var(x')$, then $C'_i = C'_j \setminus \{y\}$ and thus the claim holds. If $y = x$, then $C'_i = C'_j \setminus \{x, x'\}$ and thus the claim holds too. The case where $y = \bar{x}$ is analogous to the case where $y = x$. □

We can now show that the proof P', produced by our simulation procedure, is a valid long-distance-resolution proof of ϕ':

Theorem 2. *Let $\phi' = \Pi'.C'_1 \wedge \cdots \wedge C'_r$ and $P' = C'_{r+1}, \ldots, C'_n$ be obtained from $\phi = \Pi.C_1 \wedge \cdots \wedge C_m$ and $P = C_{m+1}, \ldots, C_r, \ldots, C_n$ by our procedure. Then, P' is a valid long-distance-resolution proof of ϕ'.*

Proof. We have to show that every clause C'_i in P' has been derived from clauses in $C'_1, \ldots, C'_{i-1}$ via a valid application of a derivation rule and that $C'_n = \bot$. To show that every clause in P' has been derived via a valid application of a derivation rule, let C'_i be a clause in P'. We proceed by a case distinction based on the rule via which its counterpart C_i has been derived in P:

Case 1: C_i has been derived from two clauses C_j, C_k via a Q-res step or an LQ-res step upon some existential literal l. In this case, $C'_i = C'_j \setminus \{l\} \vee C'_k \setminus \{\bar{l}\}$. We have to show that $l \in C'_j$, $\bar{l} \in C'_k$, and for every literal $l' \in C'_j$ such that $l' \neq l$ and $\bar{l}' \in C'_k$, it holds that l' is universal and $l <_{\Pi'} l'$. By Lemma 1, C'_j agrees with C_j on all literals whose variables are different from the universal literals x and x'. Likewise for C'_k and C_k. Therefore, $l \in C'_j$ and $\bar{l} \in C'_k$.

Now, assume C'_j contains a literal l' such that $l' \neq l$ and $\bar{l}' \in C'_k$. If the variable of l' is different from x and x', then it must be the case that l' is universal and $l <_{\Pi'} l'$, for otherwise the derivation of C_i in P were not valid. Assume thus that the variable of l' is either x or x'. If l' is either x or x', then Lemma 1 implies that C_j contains x and also, since $\bar{l}' \in C'_k$, that C_k contains $\bar{x}$. Therefore, it holds that $l <_{\Pi'} x$ (since otherwise the derivation of C_i in P were not valid) and since x' and x are in the same quantifier block, it also holds that $l <_{\Pi'} x'$, hence $l <_{\Pi'} l'$. The case where l' is $\bar{x}$ or $\bar{x}'$ is symmetric.

Case 2: C_i has been derived from a clause C_j via a $\forall$-red step, that is, by removing a universal literal y such that for every existential literal $l' \in C_j$, it holds that $l' <_{\Pi} y$. If $var(y) \neq x$, then $C'_j = C'_i \setminus \{y\}$ and since, by Lemma 1, C'_i coincides with C_i on all existential variables, it holds for every existential literal $l' \in C'_i$ that $l' <_{\Pi'} y$. If $var(y) = x$, then C'_j is of the form $C'_i \setminus \{x, x'\}$ or $C'_i \setminus \{\bar{x}, \bar{x}'\}$. Now, x and x' are in the same quantifier block and thus, with the same argument as for $var(y) = x$, it holds for every existential literal $l' \in C'_j$ that $l' <_{\Pi'} y$.

Finally, to see that $C'_n = \bot$, observe the following: By Lemma 1, since x and $\bar{x}$ are not in C_n, it follows that x' and $\bar{x}'$ are not in C'_n. Moreover, again by Lemma 1, C_n and C'_n agree on all other literals. Therefore, $C'_n = C_n = \bot$. □

We can also show that our simulation does not introduce new LQ-res steps. Hence, if a long-distance-resolution proof contains n LQ-res steps, our simulation terminates after at most n iterations (the proof is omitted due to space reasons):

Theorem 3. *Let P' be obtained from $\phi = \Pi.\psi$ and P by our procedure. Then, P' contains fewer LQ-res steps than P.*

4.4 Clashes of Several Universal Literals

Until now, we assumed that LQ-res steps involve only one pair of complementary universal literals. When multiple such pairs are involved, the procedure changes only slightly: Instead of eliminating only a single literal from one of the clauses that are involved in the LQ-res step, we now eliminate several of them. If we start with the outermost one and gradually move inwards, we ensure that at most one blocked literal is added per clause. We illustrate this on an example. Consider the QBF $\phi = \exists a \exists b \forall x \exists c \forall y \exists d.(b \vee x \vee c \vee y \vee d) \wedge (a \vee \bar{x} \vee c) \wedge (\bar{a} \vee \bar{b} \vee \bar{y} \vee d)$ and the following derivations in a long-distance-resolution proof:

$$\dfrac{b \vee x \vee c \vee y \vee d \qquad \dfrac{a \vee \bar{x} \vee c \qquad \bar{a} \vee \bar{b} \vee \bar{y} \vee d}{\bar{b} \vee \bar{x} \vee c \vee \bar{y} \vee d}\ \text{(Q-res)}}{x \vee \bar{x} \vee c \vee y \vee \bar{y} \vee d}\ \text{(LQ-res)}$$

In the LQ-res step, there are two pairs of complementary universal literals, namely $x, \bar{x}$ and $y, \bar{y}$. We therefore try to get rid of both x and y in the left antecedent $L = b \vee x \vee c \vee y \vee d$ of the LQ-res step. As in the case where only one literal is removed, we start by deriving in QRAT all clauses that occur before the LQ-res step. In this case, we add $\bar{b} \vee \bar{x} \vee c \vee \bar{y} \vee d$ to ϕ via a Q-res step and denote the resulting formula by ϕ'.

Now we want to remove x from L via blocked-literal elimination. In order for x to be blocked in ϕ', all outer resolvents of L upon x have to be tautologies. The formula ϕ' contains two clauses that can be resolved with L upon x, namely $\bar{b} \vee \bar{x} \vee c \vee \bar{y} \vee d$ and $a \vee \bar{x} \vee c$. As the first clause contains $\bar{b}$ and L contains b, the corresponding outer resolvent upon x contains $b, \bar{b}$. But there are no complementary literals in the outer resolvent $a \vee b$ with the second clause. We therefore add a fresh literal x' to L and add its complement $\bar{x}'$ to $\bar{a} \vee \bar{x} \vee c$ to obtain $\phi' = \exists a \exists b \forall x \forall x' \exists c \forall y \exists d.(b \vee x \vee x' \vee c \vee y \vee d) \wedge (a \vee \bar{x} \vee \bar{x}' \vee c) \wedge (\bar{a} \vee \bar{b} \vee \bar{y} \vee d) \wedge (\bar{b} \vee \bar{x} \vee c \vee \bar{y} \vee d)$.

We can now remove the blocked literal x from $(b \vee x \vee x' \vee c \vee y \vee d)$ to obtain $L' = b \vee x' \vee c \vee y \vee d$. If we now resolved L' with $\bar{b} \vee \bar{x} \vee c \vee \bar{y} \vee d$, we would get the following LQ-res step:

$$\dfrac{b \vee x' \vee c \vee y \vee d \qquad \bar{b} \vee \bar{x} \vee c \vee \bar{y} \vee d}{x' \vee \bar{x} \vee c \vee y \vee \bar{y} \vee d}\ \text{(LQ-res)}$$

Since there is still a clash of y and $\bar{y}$, we need to get rid of y in L'. We are lucky because we do not need to perform any blocked-literal additions: The only clauses in ϕ' that contain $\bar{y}$ are $\bar{a} \vee \bar{b} \vee \bar{y} \vee d$ and $\bar{b} \vee \bar{x} \vee c \vee \bar{y} \vee d$, and the outer resolvents of L' with both of them contain complementary literals. We can thus remove y from L' and use a Q-res step to add the resulting resolvent to ϕ':

$$\frac{b \vee x' \vee c \vee d \qquad \bar{b} \vee \bar{x} \vee c \vee \bar{y} \vee d}{x' \vee \bar{x} \vee c \vee \bar{y} \vee d}\ \text{(Q-res)}$$

Similarly to the case where we only eliminated one literal, we then propagate the corresponding changes through the rest of the proof to turn it into a valid long-distance resolution proof of ϕ'.

5 Complexity of the Simulation

After showing how a long-distance-resolution proof can be translated into a QRAT proof, we still have to prove that the size (the number of derivation steps) of the resulting QRAT proof is polynomial w.r.t. the size of the original proof and the formula. We have seen that the long-distance-resolution proof and the QRAT proof correspond one-to-one on resolution steps and $\forall$-red steps. Therefore, we only need to estimate the number of blocked-literal addition and blocked-literal elimination steps to obtain an upper bound on the size of the QRAT proof.

Consider a long-distance-resolution proof $C_{m+1}, \ldots, C_r, \ldots, C_n$ of a QBF $\Pi.C_1 \wedge \cdots \wedge C_m$, where C_r is the first clause that is derived via an LQ-res step:

$$\frac{C \vee l \vee x_1 \vee \cdots \vee x_k \qquad D \vee \bar{l} \vee \bar{x}_1 \vee \cdots \vee \bar{x}_k}{C_r = C \vee D \vee x_1 \vee \bar{x}_1 \vee \cdots \vee x_k \vee \bar{x}_k}\ \text{(LQ-res)}$$

We can make the following observation: To remove all the literals $x_1, \ldots, x_k$ from $C \vee l \vee x_1 \vee \cdots \vee x_k$ via blocked-literal elimination, we have to add at most one new literal of the form $\bar{x}'_i$ to every clause $C_1, \ldots, C_{r-1}$ if we start by eliminating the outermost universal literal x_1 and step-by-step work ourselves towards the innermost literal x_k. The reason this works is as follows:

Assume we have added the literal x'_1 to $C \vee l \vee x_1 \vee \cdots \vee x_k$ and the corresponding literal $\bar{x}'_1$ to another clause $C_i = C'_i \vee \bar{x}_1$ to obtain complementary literals in the outer resolvent of the resulting clauses $C \vee l \vee x_1 \vee x'_1 \vee \cdots \vee x_k$ and $C' \vee \bar{x}_1 \vee \bar{x}'_1$ upon x_1. Then, the outer resolvent of $C \vee l \vee x_1 \vee x'_1 \vee \cdots \vee x_k$ with $C' \vee \bar{x}_1 \vee \bar{x}'_1$ upon a literal x_j that is inner to x_1 (i.e., $x_1 <_\Pi x_j$) contains the complementary pair $x'_1, \bar{x}'_1$, so we have to add no further literals to $C' \vee \bar{x}_1 \vee \bar{x}'_1$.

Hence, the number of blocked-literal additions for literals of the form $\bar{x}'_i$ is bounded by the number of clauses, that is, by n. Moreover, for every addition of a literal $\bar{x}'_i$ to some clause, there is at most one addition of the corresponding literal x'_i. Therefore, there are at most $2n$ blocked-literal additions per LQ-res step. Now, for every addition of a literal x'_i, there is exactly one elimination of the corresponding literal x_i. Thus, overall there are at most $3n$ blocked-literal additions and eliminations for every LQ-res step. Since the number of LQ-res steps is bounded by the number of clauses in the proof, the size of the QRAT derivation is at most $3n^2$. It follows that whenever a QBF has a long-distance-resolution proof of polynomial size, it also has a polynomial-size QRAT proof:

Theorem 4. *The* QRAT *proof system polynomially simulates the long-distance-resolution calculus.*

6 Evaluation

We now know that QRAT can polynomially simulate long-distance resolution. But what does it mean in practice? Can we have short QRAT proofs for formulas that have short long-distance-resolution proofs? To answer this question at least partly, we consider the formulas well-known for having short long-distance-resolution proofs while only having long Q-resolution proofs—the Kleine Büning formulas [20]. A Kleine Büning formula of size n, in short $KBKF_n$, has the prefix $\exists a_0, a_1, b_1 \forall x_1 \exists a_2, b_2 \forall x_2 \ldots \exists a_n, b_n \forall x_n \exists c_1, c_2, \ldots, c_n$ and the following clauses:

I :	$\bar{a}_0$	I' : $a_0 \vee \bar{a}_1 \vee \bar{b}_1$	
A_i :	$a_i \vee \bar{x}_i \vee \bar{a}_{i+1} \vee \bar{b}_{i+1}$	B_i : $b_i \vee x_i \vee \bar{a}_{i+1} \vee \bar{b}_{i+1}$	for $i \in \{1..n-1\}$
C :	$a_n \vee \bar{x}_n \vee \bar{c}_1 \vee \cdots \vee \bar{c}_n$	C' : $b_n \vee x_n \vee \bar{c}_1 \vee \cdots \vee \bar{c}_n$	
X_i :	$\bar{x}_i \vee c_i$	X'_i : $x_i \vee c_i$	for $i \in \{1..n\}$

We can reduce a formula $KBKF_n$ to a formula $KBKF_{n-1}$ by using only Q-res, blocked-literal elimination, and clause-deletion steps[4] (no $\forall$-red steps or resolution upon universal literals). To do so, we use the clauses A_n, B_n, C, C', X_n, and X'_n of $KBKF_n$ to construct the clauses C and C' of $KBKF_{n-1}$. The required 12 steps are shown below. The last two clauses (11 and 12) respectively correspond to the clauses C and C' of $KBKF_{n-1}$.

1.	$a_n \vee \bar{x}_n \vee \bar{c}_1 \vee \cdots \vee \bar{c}_{n-1}$	(Q-res of C and X_n)
2.	$b_n \vee x_n \vee \bar{c}_1 \vee \cdots \vee \bar{c}_{n-1}$	(Q-res of C' and X'_n)
3.		(delete C, C', X_n, X'_n)
4.	$a_{n-1} \vee \bar{x}_{n-1} \vee \bar{b}_n \vee \bar{x}_n \vee \bar{c}_1 \vee \cdots \vee \bar{c}_{n-1}$	(Q-res of 1 and A_{n-1})
5.	$b_{n-1} \vee x_{n-1} \vee \bar{a}_n \vee x_n \vee \bar{c}_1 \vee \cdots \vee \bar{c}_{n-1}$	(Q-res of 2 and B_{n-1})
6.	$a_{n-1} \vee \bar{x}_{n-1} \vee \bar{b}_n \vee \bar{c}_1 \vee \cdots \vee \bar{c}_{n-1}$	(BLE of $\bar{x}_n$ from 4)
7.	$b_{n-1} \vee x_{n-1} \vee \bar{a}_n \vee \bar{c}_1 \vee \cdots \vee \bar{c}_{n-1}$	(BLE of x_n from 5)
8.	$a_{n-1} \vee \bar{x}_{n-1} \vee x_n \vee \bar{c}_1 \vee \cdots \vee \bar{c}_{n-1}$	(Q-res of 6 and B_{n-1})
9.	$b_{n-1} \vee x_{n-1} \vee \bar{x}_n \vee \bar{c}_1 \vee \cdots \vee \bar{c}_{n-1}$	(Q-res of 7 and A_{n-1})
10.		(delete 4, 5, 6, 7, A_{n-1}, B_{n-1})
11.	$a_{n-1} \vee \bar{x}_{n-1} \vee \bar{c}_1 \vee \cdots \vee \bar{c}_{n-1}$	(BLE of x_n from 8)
12.	$b_{n-1} \vee x_{n-1} \vee \bar{c}_1 \vee \cdots \vee \bar{c}_{n-1}$	(BLE of $\bar{x}_n$ from 9)

Table 1 shows the sizes of the Kleine Büning formulas as well as of the corresponding long-distance-resolution proofs (in the QRP format) and QRAT proofs. The latter are obtained by the construction mentioned in this section. The size of both types of proofs is linear in the size of the formula. Although QRAT proofs use about twice as many proof steps (including deletion steps), the file size of QRAT proofs is smaller. The explanation for this is that long-distance-resolution proofs increase the length of clauses, while QRAT proofs decreases their length.

Short proofs of the $KBKF$ formulas can also be obtained by using resolution upon universal variables as in the calculus QU-Res [24]. There is, however, a variant of the $KBKF$ formulas, called $KBKF_n{-}qu$ [2], which has only exponential proofs in the QU-Res calculus. A $KBKF_n{-}qu$ formula is obtained from $KBKF_n$

[4] Clause deletion was not used in the simulation, but is allowed in the QRAT system.

Table 1. The size of Kleine Büning formulas in the number of variables (#var) and clauses (#cls). Additionally, the size of their long-distance-resolution proofs (in the QRP format) in the number of Q-res steps (#Q), LQ-res steps (#L), ∀-red steps (#∀), and the file size in KB (ignoring the part that represents the formula). On the right, the number of Q-res (#Q), BLE (#B), and deletion (#D) steps as well as the file size for the manual QRAT proofs.

	input		LD proofs (QRP)				QRAT proofs			
formula	#var	#cls	#Q	#L	#∀	file size	#Q	#B	#D	file size
$KBKF_{10}$	41	42	41	18	38	6	57	38	92	6
$KBKF_{50}$	201	202	201	98	198	138	297	198	492	112
$KBKF_{100}$	401	402	401	198	398	573	597	398	992	421
$KBKF_{200}$	801	802	801	398	798	2321	1197	798	1992	1627
$KBKF_{500}$	2001	2002	2001	998	1998	16 259	2997	1998	4992	11 890

by adding a universal literal y_i (occurring in the same quantifier block as x_i) to every clause in $KBKF_n$ that contains x_i, and a literal $\bar{y}_i$ to every clause in $KBKF_n$. For these formulas, blocked-literal elimination can remove all the y_i and $\bar{y}_i$ literals, which reduces a $KBKF_n{-}qu$ formula to a $KBKF_n$ formula that can then be efficiently proved using resolution upon universal literals.

In addition to the handcrafted QRAT proofs, we implemented a tool (called `ld2qrat`) that, based on our simulation, transforms long-distance-resolution proofs into QRAT proofs. We used `ld2qrat` to transform the long-distance-resolution proofs of the $KBKF_n$ formulas (by Egly et al. [11]) into QRAT proofs and validated the correctness of these proofs with the proof checker `QRAT-trim`. In the plain mode, `ld2qrat` closely follows our simulation. Additionally, it features two optimizations: (1) Given an LQ-res step upon l with the antecedents $C \vee l \vee x$ and $D \vee \bar{l} \vee \bar{x}$, if one of x or $\bar{x}$ is already a blocked literal, it is removed with blocked-literal elimination. This avoids the introduction of new variables. (2) Clauses are deleted as soon as they are not needed later in the proof anymore.

Table 2 shows properties of the QRAT proofs produced by `ld2qrat` from the long-distance-resolution proofs of the $KBKF$ formulas. On the left are the sizes of proofs obtained without the clause-deletion optimization. On the right are the sizes of proofs with this optimization. A (least squares) regression analysis confirms that the length (number of steps) of the QRAT proofs without deletion is quadratically related to the length of the corresponding long-distance-resolution proofs: The function $f(x) = 0.22x^2 - 4.48x + 54.58$ (where x is the length of the long-distance-resolution proof and $f(x)$ is the length of the QRAT proof) fits the data from the above tables perfectly (the error term R^2 of the regression is 1).

7 QRAT in the Complexity Landscape

After the analysis of QRAT in theory and practice, we now locate it in the proof-complexity landscape of resolution-based calculi for QBF, which is shown in Fig. 2. Besides the long-distance-resolution calculus LQ-Res, another well-known proof system is the calculus QU-Res [24], which extends the basic Q-resolution

Table 2. Comparison of the QRAT proofs obtained by applying `ld2qrat` to long-distance-resolution proofs (in the QRP format) of the Kleine Büning formulas. The file size is given in KB and the time for translating the proof (time) is given in seconds.

	QRP to QRAT w/o deletion				QRP to QRAT w/ deletion			
formula	#var	#step	file size	time	#var	#step	file size	time
$KBKF_{10}$	59	1690	103	0.07	59	448	26	0.01
$KBKF_{50}$	299	52 170	18 774	0.45	299	6288	2227	0.12
$KBKF_{100}$	599	214 270	154 299	3.77	599	22 588	16 192	0.86
$KBKF_{200}$	1199	868 470	1 309 559	30.70	1199	85 188	126 375	7.95
$KBKF_{500}$	2999	5 471 070	23 622 369	497.32	2999	512 988	2 229 195	124.10

calculus (Q-Res) by allowing resolution upon universals literals if the resulting resolvent does not contain complementary literals. As QRAT also allows resolution upon universal literals, it simulates QU-Res. Balabanov et al. [2] showed the incomparability between LQ-Res and QU-Res by exponential separations. It thus follows that QRAT is strictly stronger than both LQ-Res and QU-Res.

Another system that is stronger than both LQ-Res and QU-Res is the calculus LQU$^+$-Res [2], which extends LQ-Res by allowing (long-distance) resolution upon universals literals. We know that either QRAT is strictly stronger than LQU$^+$-Res or the two systems are incomparable: On purely existentially-quantified formulas, LQU$^+$-Res boils down to ordinary propositional resolution (without complementary literals in resolvents) whereas the QRAT system boils down to the RAT system [25]. As the RAT system is strictly stronger than resolution—there exist polynomial-size RAT proofs of the well-known pigeon hole formulas [13] while resolution proofs of these formulas are necessarily exponential in size [12]—LQU$^+$-Res cannot simulate QRAT.

On the other hand, QRAT might be able to simulate LQU$^+$-Res, but not with our simulation of the long-distance-resolution calculus, because the simulation cannot convert all LQU$^+$-Res proofs into QRAT proofs. To see this, consider the QBF $\exists a \forall x \forall y \exists b.(a \vee x \vee b) \wedge (\bar{a} \vee \bar{x} \vee b) \wedge (x \vee \bar{b}) \wedge (\bar{x} \vee \bar{y} \vee \bar{b})$ with the following LQU$^+$-Res proof [2]: $x \vee \bar{x} \vee b,\ \bar{y} \vee \bar{b},\ x \vee \bar{x} \vee \bar{y},\ x \vee \bar{x},\ x,\ \bot$. The proof can be illustrated as follows:

$$\dfrac{\dfrac{\dfrac{\dfrac{a \vee x \vee b \qquad \bar{a} \vee \bar{x} \vee b}{x \vee \bar{x} \vee b}\,\text{(LQ-res)} \qquad \dfrac{x \vee \bar{b} \qquad \bar{x} \vee \bar{y} \vee \bar{b}}{\bar{y} \vee \bar{b}}\,\text{(QU-res)}}{x \vee \bar{x} \vee \bar{y}}\,\text{(Q-res)}}{x \vee \bar{x}}\,(\forall\text{-red})}{x}\,(\forall\text{-red})}{\bot}\,(\forall\text{-red})$$

In our simulation, we first replace the literal x in $a \vee x \vee b$ by x' before resolving the resulting clause $a \vee x' \vee b$ with $\bar{a} \vee \bar{x} \vee b$. The replacement of x by x' also leads to the addition of $\bar{x}'$ to $\bar{x} \vee \bar{y} \vee \bar{b}$. If we now perform the universal resolution step of $x \vee \bar{b}$ with $\bar{x} \vee \bar{x}' \vee \bar{y} \vee \bar{b}$, then we obtain the following partial proof:

$$\dfrac{\dfrac{a \vee x' \vee b \qquad \bar{a} \vee \bar{x} \vee b}{x' \vee \bar{x} \vee b}\,\text{(Q-res)} \qquad \dfrac{x \vee \bar{b} \qquad \bar{x} \vee \bar{x}' \vee \bar{y} \vee \bar{b}}{\bar{x}' \vee \bar{y} \vee \bar{b}}\,\text{(QU-res)}}{}$$

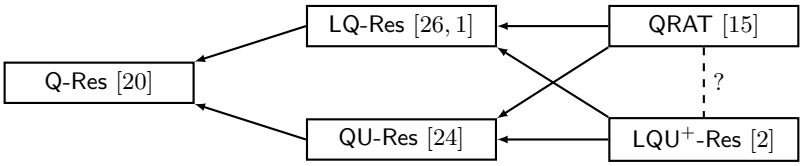

Fig. 2. Complexity landscape including QRAT. A directed edge from a proof system A to a proof system B means that A is strictly stronger than B.

The Q-res step upon b is now impossible because x' is in $x' \vee \bar{x} \vee b$ and $\bar{x}'$ is in $\bar{x}' \vee \bar{y} \vee \bar{b}$. We also cannot eliminate x' from $x' \vee \bar{x} \vee b$ via blocked-literal elimination: This would require us to add a new literal x'' to $x' \vee \bar{x} \vee b$ and to add $\bar{x}''$ to $\bar{x}' \vee \bar{y} \vee \bar{b}$ leading to the new pair $x'', \bar{x}''$ of complementary literals.

Our key result, Lemma 1, does not hold anymore when allowing resolution over universal literals. Lemma 1 guarantees that whenever a new literal $\bar{x}'$ is in a proof clause C_i' of the modified long-distance-resolution proof, then $\bar{x}$ was contained in the corresponding clause C_i in the original proof. The above example shows that resolution over universal literals destroys this property: Although $\bar{x}'$ is contained in the clause $\bar{x}' \vee \bar{y} \vee \bar{b}$, the literal x is not contained in the corresponding clause $y \vee \bar{y} \vee b$ of the original proof because we resolved it away.

8 Conclusion

We showed that the QRAT proof system polynomially simulates long-distance resolution. In our simulation, we used only a small subset of the QRAT rules: Q-resolution, universal reduction, blocked-literal addition, and blocked-literal elimination. Based on our simulation, we implemented a tool that transforms long-distance-resolution proofs into QRAT proofs. The tool allows to merge a QRAT derivation produced by a QBF-preprocessor with a long-distance-resolution proof produced by a search-based solver. The correctness of the resulting QRAT proof can then be checked with a proof checker such as `QRAT-trim` [15]. We evaluated the tool on long-distance-resolution proofs of the well-known Kleine Büning formulas and manually constructed QRAT proofs of these formulas that are smaller than their long-distance counterparts.

We further noted that our simulation breaks down if the long-distance-resolution calculus is extended by resolution upon universal literals, as in the calculus LQU$^+$-Res. Investigating the exact relationship between LQU$^+$-Res and QRAT therefore remains open for future work. Another open question is whether blocked-literal elimination can be polynomially simulated in LQU$^+$-Res. We also do not know whether it is possible to simulate long-distance resolution with only Q-resolution, universal reduction, clause deletion, and blocked-literal elimination (but no blocked-literal addition). Finally, what is still unclear is how QRAT relates to instantiation-based proof systems and sequent proof systems. Answers to these questions will shed more light on the proof-complexity landscape of QBF.

References

1. Balabanov, V., Jiang, J.R.: Unified QBF certification and its applications. Formal Methods in System Design 41(1), 45–65 (2012)
2. Balabanov, V., Widl, M., Jiang, J.R.: QBF resolution systems and their proof complexities. In: Proc. of the 17th Int. Conference on Theory and Applications of Satisfiability Testing (SAT 2014). LNCS, vol. 8561, pp. 154–169. Springer, Cham (2014)
3. Benedetti, M., Mangassarian, H.: QBF-based formal verification: Experience and perspectives. Journal on Satisfiability, Boolean Modeling and Computation (JSAT) 5(1-4), 133–191 (2008)
4. Beyersdorff, O., Bonacina, I., Chew, L.: Lower bounds: From circuits to QBF proof systems. In: Proc. of the 2016 ACM Conference on Innovations in Theoretical Computer Science (ITCS 2016). pp. 249–260. ACM (2016)
5. Beyersdorff, O., Chew, L., Janota, M.: On unification of QBF resolution-based calculi. In: Proc. of the 39th Int. Symposium on Mathematical Foundations of Computer Science (MFCS 2014). LNCS, vol. 8635, pp. 81–93. Springer, Heidelberg (2014)
6. Beyersdorff, O., Chew, L., Janota, M.: Proof complexity of resolution-based QBF calculi. In: Proc. of the 32nd Int. Symposium on Theoretical Aspects of Computer Science (STACS 2015). LIPIcs, vol. 30, pp. 76–89. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2015)
7. Beyersdorff, O., Chew, L., Mahajan, M., Shukla, A.: Are short proofs narrow? QBF resolution is not simple. In: Proc. of the 33rd Symposium on Theoretical Aspects of Computer Science (STACS 2016). LIPIcs, vol. 47, pp. 15:1–15:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2016)
8. Beyersdorff, O., Pich, J.: Understanding Gentzen and Frege Systems for QBF. In: Proc. of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 2016). pp. 146–155. ACM (2016)
9. Chen, H.: Proof Complexity Modulo the Polynomial Hierarchy: Understanding Alternation as a Source of Hardness. In: Proc. of the 43rd Int. Colloquium on Automata, Languages, and Programming (ICALP 2016). LIPIcs, vol. 55, pp. 94:1–94:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2016)
10. Egly, U.: On stronger calculi for QBFs. In: Proc. of the 19th Int. Conference on Theory and Applications of Satisfiability Testing (SAT 2016). LNCS, vol. 9710, pp. 419–434. Springer, Cham (2016)
11. Egly, U., Lonsing, F., Widl, M.: Long-distance resolution: Proof generation and strategy extraction in search-based QBF solving. In: Proc. of the 19th Int. Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR-19). LNCS, vol. 8312, pp. 291–308. Springer, Heidelberg (2013)
12. Haken, A.: The intractability of resolution. Theoretical Computer Science 39, 297–308 (1985)
13. Heule, M.J.H., Hunt Jr., W.A., Wetzler, N.D.: Expressing symmetry breaking in DRAT proofs. In: Proc. of the 25th Int. Conference on Automated Deduction (CADE 2015). LNCS, vol. 9195, pp. 591–606. Springer, Cham (2015)
14. Heule, M.J.H., Seidl, M., Biere, A.: Blocked literals are universal. In: Proc. of the 7th Int. NASA Symposium on Formal Methods (NFM 2015). LNCS, vol. 9058, pp. 436–442. Springer, Cham (2015)
15. Heule, M.J.H., Seidl, M., Biere, A.: Solution validation and extraction for QBF preprocessing. Journal of Automated Reasoning pp. 1–29 (2016)

16. Janota, M.: On Q-Resolution and CDCL QBF solving. In: Proc. of the 19th Int. Conference on Theory and Applications of Satisfiability Testing (SAT 2016). LNCS, vol. 9710, pp. 402–418. Springer, Cham (2016)
17. Janota, M., Grigore, R., Marques-Silva, J.: On QBF proofs and preprocessing. In: Proc. of the 19th Int. Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR-19). LNCS, vol. 8312, pp. 473–489. Springer, Heidelberg (2013)
18. Janota, M., Klieber, W., Marques-Silva, J., Clarke, E.M.: Solving QBF with counterexample guided refinement. Artificial Intelligence 234, 1–25 (2016)
19. Kleine Büning, H., Bubeck, U.: Theory of Quantified Boolean Formulas. In: Handbook of Satisfiability, pp. 735–760. IOS Press (2009)
20. Kleine Büning, H., Karpinski, M., Flögel, A.: Resolution for quantified boolean formulas. Information and Computation 117(1), 12–18 (1995)
21. Kullmann, O.: On a generalization of extended resolution. Discrete Applied Mathematics 96-97, 149–176 (1999)
22. Lonsing, F., Egly, U.: DepQBF 6.0: A search-based QBF solver beyond traditional QCDCL. CoRR abs/1702.08256 (2017)
23. Slivovsky, F., Szeider, S.: Variable dependencies and Q-resolution. In: Proc. of the 17th Int. Conference on Theory and Applications of Satisfiability Testing (SAT 2014). LNCS, vol. 8561, pp. 269–284. Springer, Cham (2014)
24. Van Gelder, A.: Contributions to the theory of practical quantified boolean formula solving. In: Proc. of the 18th Int. Conference on Principles and Practice of Constraint Programming (CP 2012). LNCS, vol. 7514, pp. 647–663. Springer, Heidelberg (2012)
25. Wetzler, N., Heule, M.J.H., Hunt Jr., W.A.: DRAT-trim: Efficient checking and trimming using expressive clausal proofs. In: Proc. of the 17th Int. Conference on Theory and Applications of Satisfiability Testing (SAT 2014). LNCS, vol. 8561, pp. 422–429. Springer, Cham (2014)
26. Zhang, L., Malik, S.: Conflict driven learning in a quantified boolean satisfiability solver. In: Proc. of the 2002 IEEE/ACM Int. Conference on Computer-aided Design (ICCAD 2002). pp. 442–449. ACM/IEEE Computer Society (2002)