

On the Relation between Resolution Calculi for QBFs and First-order Formulas^{*}

Uwe Egly

Institut für Informationssysteme 184/3, Technische Universität Wien,
Favoritenstrasse 9–11, A-1040 Vienna, Austria
email: uwe@kr.tuwien.ac.at

Abstract. Quantified Boolean formulas (QBFs) generalize propositional formulas by admitting quantifications over propositional variables. QBFs can be viewed as (restricted) formulas of first-order predicate logic and easy translations from QBFs to first-order formulas exist. We analyze the effect of such translations on the complexity of resolution proofs. More precisely, we show that there are families $(\Phi_i)_{i \geq 1}$ and $(\Omega_i)_{i \geq 1}$ of short QBFs for which any resolution refutation of Φ_i or Ω_i in Q-resolution, QU-resolution, LDQ-resolution and LDQU-resolution has size super-polynomial in i , but the translated versions of Φ_i and Ω_i possess short first-order resolution refutations. We use $(\Phi_i)_{i \geq 1}$ and $(\Omega_i)_{i \geq 1}$ to exponentially separate two closely related translations of QBFs to first-order formulas. Moreover we show a polynomial simulation of QU-resolution by first-order resolution (together with a translation) and we discuss how first-order predicate logic can be used to succinctly represent refutations of QBFs obtained by expanding some universal quantifiers.

1 Preliminaries

We assume familiarity with the basic concepts of propositional and first-order logic as well as quantified Boolean formulas. Especially we assume familiarity with resolution and skolemization in first-order logic [7], Q-resolution (Q-res) [6], long distance Q-resolution (LDQ-res) [1, 3] together with their extended versions QU-res and LDQU-res allowing also distance one resolutions over *universal* variables. We consider resolution derivations not restricted to tree form. As an example, we present the definition of a first-order resolution deduction of a clause C from a set $\mathcal{C}$ of input clauses.

A sequence $C_1, \dots, C_n$ is called *R₁-deduction* (first-order resolution deduction) of a clause C from $\mathcal{C}$ if $C_n = C$ and for all $i = 1, \dots, n$, one of the following conditions hold.

1. C_i is an input clause from $\mathcal{C}$.
2. C_i is a factor of a C_j for $j < i$.
3. C_i is a resolvent of a variant of C_j and a variant of C_k for $j, k < i$.

An *R₁-refutation* of $\mathcal{C}$ is an R₁-deduction of the empty clause $\square$ from $\mathcal{C}$. The *size* of a deduction is given by $\sum_{i=1}^n \text{size}(C_i)$, where $\text{size}(C_i)$ is the number of character occurrences in C_i .

^{*} The work was supported by the Austrian Science Foundation (FWF) under grant S11409-N23.

We introduce the translation from (closed) QBFs to (closed) first-order formulas and variants of this translation from [9] (we use Q^b to denote the Boolean quantifier Q).

$$\llbracket \perp \rrbracket_p^f = p(f_\perp) \quad \llbracket \top \rrbracket_p^f = p(f_\top) \quad \llbracket x \rrbracket_p^f = p(x)$$

$$\llbracket \neg \Phi \rrbracket_p^f = \neg \llbracket \Phi \rrbracket_p^f \quad \llbracket \Phi_1 \circ \Phi_2 \rrbracket_p^f = \llbracket \Phi_1 \rrbracket_p^f \circ \llbracket \Phi_2 \rrbracket_p^f \quad \llbracket Q^b x \Phi \rrbracket_p^f = Qx \llbracket \Phi \rrbracket_p^f$$

The connective $\circ$ is a binary connective present in both languages and $Q \in \{\forall, \exists\}$. The symbols p and f do not occur in the source QBF; p is a unary predicate symbol and f is used to construct (Skolem) constant and function symbols by indices.

The translations can be extended first to $Sk\llbracket \Phi \rrbracket_p^f$ generating a skolemized version of $\llbracket \Phi \rrbracket_p^f$.

Definition 1. Let Φ be a closed QBF in prenex conjunctive normal form (PCNF) with matrix M and let $\llbracket \Phi \rrbracket_p^f$ be its closed first-order translation. For any existential variable a in the quantifier prefix of Φ , let $dep(a)$ be the sequence of universal variables left of a (in exactly the same order in which they occur in the prefix). Let f_a be the Skolem function symbol associated to a . We call $\forall \llbracket M \rrbracket_p^f \sigma$ the skolemized form of $\llbracket \Phi \rrbracket_p^f$ and denote it by $Sk\llbracket \Phi \rrbracket_p^f$, where the substitution σ is as follows.

$$\sigma = \{a \setminus f_a(dep(a)) \mid \text{for all existential variables } a \text{ in } \Phi\}.$$

Since we interpret over a two-element domain, proper Skolem function symbols can be eliminated by introducing new predicate symbols.

Definition 2. Let Φ be a closed QBF in PCNF with matrix M and let $\llbracket \Phi \rrbracket_p^f$ be its closed first-order translation. Replace in $Sk\llbracket \Phi \rrbracket_p^f$ any occurrence of a predicate of the form $p(f_b(X))$ by $p_b(X)$ where f_b is a proper function symbol (i.e., its arity is greater than 0) and X is a non-empty list of universal variables. The formula resulting after all possible replacements is the ERP formula $EPR\llbracket \Phi \rrbracket_p^f$.

We will see later that the first-order translation and the EPR translation have different proof-theoretical properties because some resolution operations are blocked by different predicate symbols.

Proposition 1. Let Φ be a closed QBF.

$$\begin{aligned} \Phi \text{ is satisfiable} & \quad \text{iff} \quad \llbracket \Phi \rrbracket_p^f \wedge p(f_\top) \wedge \neg p(f_\perp) \text{ is satisfiable.} \\ \Phi \text{ is satisfiable} & \quad \text{iff} \quad Sk\llbracket \Phi \rrbracket_p^f \wedge p(f_\top) \wedge \neg p(f_\perp) \text{ is satisfiable.} \\ \Phi \text{ is satisfiable} & \quad \text{iff} \quad EPR\llbracket \Phi \rrbracket_p^f \wedge p(f_\top) \wedge \neg p(f_\perp) \text{ is satisfiable.} \end{aligned}$$

We conclude this section with two simple observations.

- O1 Let Φ be a (closed) QBF. Then $\Phi \cong \llbracket \Phi \rrbracket_p^f$, i.e., Φ and $\llbracket \Phi \rrbracket_p^f$ are isomorphic.
- O2 Let Φ be a closed QBF in PCNF with matrix M and let M' be the matrix of $Sk\llbracket \Phi \rrbracket_p^f$ or $EPR\llbracket \Phi \rrbracket_p^f$. Then $M \cong M'$.

We will use the isomorphism between the QBF and its skolemized first-order and EPR translation to construct first-order resolution refutations from Q-resolution refutations.

2 Exponential separation of resolution calculi

We constructed in [2] a family $(\Phi_n)_{n \geq 1}$ of short closed QBFs in PCNF for which any Q-res refutation of Φ_n is super-polynomial. The formula Φ_n is

$$\exists^b X_n \forall^b Y_n \exists^b Z_n (\text{TPHP}_n^{Y_n, Z_n} \wedge \text{CPHP}_n^{X_n}) .$$

$\text{CPHP}_n^{X_n}$ is the pigeon hole formula for n holes and $n + 1$ pigeons in *conjunctive* normal form and denoted over the variables $X_n = \{x_{1,1}, \dots, x_{n+1,n}\}$. Variable $x_{i,j}$ is intended to denote that pigeon i is sitting in hole j . $\text{CPHP}_n^{X_n}$ is

$$\left(\bigwedge_{i=1}^{n+1} \left(\bigvee_{j=1}^n x_{i,j} \right) \right) \wedge \left(\bigwedge_{j=1}^n \bigwedge_{1 \leq i_1 < i_2 \leq n+1} (\neg x_{i_1,j} \vee \neg x_{i_2,j}) \right) .$$

The number of clauses in $\text{CPHP}_n^{X_n}$ is $l_n = (n + 1) + n^2(n + 1)/2$ and $\text{size}(\text{CPHP}_n^{X_n})$ is $O(n^3)$. The formula $\text{TPHP}_n^{Y_n, Z_n}$ is obtained from the pigeon hole formula in *disjunctive* normal form, $\text{DPHP}_n^{Y_n}$, by a structure-preserving polarity-sensitive translation to clause form [8]. The formula $\text{DPHP}_n^{Y_n}$ is the negation of $\text{CPHP}_n^{Y_n}$ where negation has been pushed in front of atoms and double-negation elimination has been applied. The following description of the construction of $\text{TPHP}_n^{Y_n, Z_n}$ has been taken from [2].

We use new variables of the form $z_{i_1, i_2, j}$ for disjuncts in $\text{DPHP}_n^{Y_n}$. For the first $n + 1$ disjuncts of the form $\bigwedge_{j=1}^n \neg y_{i,j}$ with $1 \leq i \leq n + 1$, we use variables $z_{1,0,0}, \dots, z_{n+1,0,0}$. For the second part, for any $1 \leq j \leq n$ and the $n(n + 1)/2$ disjuncts, we use

$$z_{1,2,j}, \dots, z_{1,n+1,j}, z_{2,3,j}, \dots, z_{2,n+1,j}, \dots, z_{n,n+1,j} .$$

The set of these variables for DPHP_n is denoted by Z_n . Due to this construction, we can speak about the conjunction corresponding to the variable $z_{i_1, i_2, j}$.

We construct the conjunctive normal form $\text{TPHP}_n^{Y_n, Z_n}$ of $\text{DPHP}_n^{Y_n, Z_n}$ as follows. First, we take the clause $D_n^{Z_n} = \bigvee_{z \in Z_n} \neg z$ over all variables in Z_n . The formula $P_n^{Y_n, Z_n}$ for the first $(n + 1)$ disjuncts of $\text{DPHP}_n^{Y_n}$ is of the form

$$\bigwedge_{i=1}^{n+1} \bigwedge_{j=1}^n (z_{i,0,0} \vee \neg y_{i,j}) .$$

For the remaining $n^2(n + 1)/2$ disjuncts of $\text{DPHP}_n^{Y_n}$, we have the formula $Q_n^{Y_n, Z_n}$

$$\bigwedge_{j=1}^n \bigwedge_{1 \leq i_1 < i_2 \leq n+1} ((z_{i_1, i_2, j} \vee y_{i_1, j}) \wedge (z_{i_1, i_2, j} \vee y_{i_2, j})) .$$

Then $\text{TPHP}_n^{Y_n, Z_n}$ is $D_n^{Z_n} \wedge P_n^{Y_n, Z_n} \wedge Q_n^{Y_n, Z_n}$ and $\text{size}(\text{TPHP}_n^{Y_n, Z_n})$ is $O(n^3)$.

It is easy to check that

$$\text{DPHP}_n^{Y_n} \equiv \exists^b Z_n \text{TPHP}_n^{Y_n, Z_n}$$

holds.

We use a second family $(\Omega)_{i \geq 1}$ of QBFs where Ω_n is

$$\forall^b Y_n \exists^b Z_n \exists^b X_n (\text{TPHP}_n^{Y_n, Z_n} \wedge \text{CPHP}_n^{X_n}) .$$

The difference between the logically equivalent formulas Φ_n and Ω_n is the quantifier prefix. The number of quantifier alternations is 2 in Φ_n , whereas it is 1 in Ω_n .

Proposition 2. *Any refutation of Φ_n and Ω_n in Q-res, QU-res, LDQ-res, and LDQU-res has size super-polynomial in n .*

The first part concerning Φ_n is part of Proposition 3 in [2], the second part concerning Ω_n can be proved similarly. The proof is based on the fact that (i) the two conjuncts of the QBFs Φ_n and Ω_n belong to languages with different alphabets and (ii) that the alphabets cannot be made identical by instantiation of quantifiers in Q-res, QU-res, LDQ-res or LDQU-res. Therefore we have to refute either $\text{TPHP}_n^{Y_n, Z_n}$ or $\text{CPHP}_n^{X_n}$ under the given quantifier prefix. Since $\forall^b Y_n \exists^b Z_n \text{TPHP}_n^{Y_n, Z_n}$ is true, there is no refutation in the above calculi and we have to turn to $\exists^b X_n \text{CPHP}_n^{X_n}$. But then, we essentially have to refute $\text{CPHP}_n^{X_n}$ with propositional resolution and consequently, by Haken's famous result [4], any refutation of $\text{CPHP}_n^{X_n}$ in Q-res, QU-res, LDQ-res or LDQU-res has size super-polynomial in n .

In the following we show that $Sk \llbracket \Omega_n \rrbracket_p^f$ has a short refutation in R_1 . We use $f_{x_{i,j}}$ to denote the Skolem function symbol corresponding to $x_{i,j} \in X_n$ and $f_{z_{i,j,k}}$ to denote the Skolem function symbols corresponding to $z_{i,j,k} \in Z_n$. All the Skolem function symbols have arity $|Y_n| = n(n+1)$. Let $\overline{F}$ denote the formula F under the first-order translation and skolemization. We have

$$\begin{aligned} \overline{\text{CPHP}_n^{X_n}} : & \left(\bigwedge_{i=1}^{n+1} \left(\bigvee_{j=1}^n p(f_{x_{i,j}}(Y_n)) \right) \right) \wedge \\ & \left(\bigwedge_{j=1}^n \bigwedge_{1 \leq i_1 < i_2 \leq n+1} (\neg p(f_{x_{i_1,j}}(Y_n)) \vee \neg p(f_{x_{i_2,j}}(Y_n))) \right) . \end{aligned}$$

From $\text{TPHP}_n^{Y_n, Z_n}$ we have

$$\begin{aligned} \overline{D_n^{Z_n}} : & \bigvee_{z \in Z_n} \neg p(f_z(Y_n)) \\ \overline{P_n^{Y_n, Z_n}} : & \bigwedge_{i=1}^{n+1} \bigwedge_{j=1}^n (p(f_{z_{i,0,0}}(Y_n)) \vee \neg p(y_{i,j})) \\ \overline{Q_n^{Y_n, Z_n}} : & \bigwedge_{j=1}^n \bigwedge_{1 \leq i_1 < i_2 \leq n+1} ((p(f_{z_{i_1, i_2, j}}(Y_n)) \vee p(y_{i_1, j})) \wedge \\ & (p(f_{z_{i_1, i_2, j}}(Y_n)) \vee p(y_{i_2, j}))) . \end{aligned}$$

The refutation of $Sk \llbracket \Omega_n \rrbracket_p^f$ is constructed as follows.

1. We use $\overline{P_n^{Y_n, Z_n}}$ together with the first $n + 1$ clauses from $\overline{\text{C PHP}_n^{X_n}}$ to derive $p(f_{z_{i,0,0}}(Y'_n))\mu_i$ (for all $i = 1, \dots, n + 1$). The derivation consists of $O(n^2)$ clauses and applies resolution and factoring. The substitution μ_i is

$$\bigcup_{j=1}^n \{y'_{i,j} \setminus f_{x_{i,j}}(Y_n)\}.$$

2. We use $\overline{Q_n^{Y_n, Z_n}}$ together with the binary clauses from $\overline{\text{C PHP}_n^{X_n}}$ to derive the clause $p(f_{z_{i_1, i_2, j}}(Y_n))\nu_{i_1, i_2, j}$ (for all $j = 1, \dots, n$ and i_1, i_2 with $1 \leq i_1 < i_2 \leq n + 1$). The derivation consists of $O(n^3)$ clauses and applies resolution and factoring. The substitution $\nu_{i_1, i_2, j}$ is

$$\{y_{i_1, j} \setminus f_{x_{i_1, j}}(Y_n)\sigma_{i_1, i_2, j}, y_{i_2, j} \setminus f_{x_{i_2, j}}(Y_n)\sigma_{i_1, i_2, j}\},$$

where $\sigma_{i_1, i_2, j}$ is a variable renaming from the variant generation in resolution.

3. We use $\overline{D_n^{Z_n}}$ together with the derived instance of $p(f_{z_{k,l,m}}(Y_n))$ to derive $\square$ by resolution. Since any variable $y_{i,j}$ is assigned to a variant of $f_{x_{i,j}}(Y_n)$ for all $i = 1, \dots, n + 1$ and all $j = 1, \dots, n$, all resolution steps are possible. The derivation consists of $O(n^3)$ clauses.

The formula $Sk\llbracket \Phi_n \rrbracket_p^f$ can be refuted similarly in R_1 by replacing variants of the form $f_{x_{i,j}}(Y_n)$ by $a_{i,j}$.

Proposition 3. *Let $(\Phi_n)_{n \geq 1}$ and $(\Omega_n)_{n \geq 1}$ be the families of closed QBFs defined above. Then $\llbracket \Phi_n \rrbracket_p^f$ and $\llbracket \Omega_n \rrbracket_p^f$ have short tree refutations in R_1 consisting of $O(n^3)$ clauses. Moreover the size of the refutation is polynomial in n .*

Theorem 1. *The calculi Q-res, QU-res, LDQ-res, or LDQU-res cannot polynomially simulate R_1 with the translation $Sk\llbracket \cdot \rrbracket_p^f$ or $EPR\llbracket \cdot \rrbracket_p^f$.*

We use $(\Phi_n)_{n \geq 1}$ and $(\Omega_n)_{n \geq 1}$ to exponentially separate the first-order translation with skolemization from the ERP translation.

Proposition 4. *Let $(\Omega_n)_{n \geq 1}$ be the family of closed QBFs defined above and let Ω'_n be the EPR formula $EPR\llbracket \Omega_n \rrbracket_p^f \wedge p(f_\top) \wedge \neg p(f_\perp)$. Then any R_1 -refutation of Ω'_n has size super-polynomial in n .*

Proof (Sketch). Similar arguments as in Proposition 3 in [2] apply, because the EPR translations of $\text{TPHP}_n^{Y_n, Z_n}$ and $\text{C PHP}_n^{X_n}$ are denoted in different languages and literals from the former cannot be resolved with literals from the latter. The reason here are the different first-order predicate symbols used to represent universal and existential literals. For universal literals, the unary predicate symbol is p , for existential literals, the predicate symbol is p_b where b is the atom of the literal. Again, the pigeonhole formula has to be refuted. Consequently, the (essentially propositional) resolution proof has size super-polynomial in n . $\square$

Theorem 2. *R_1 with translation $EPR\llbracket \cdot \rrbracket_p^f$ cannot polynomially simulate R_1 with translation $Sk\llbracket \cdot \rrbracket_p^f$.*

3 Polynomial simulations of resolution calculi

In this section we show that the first-order resolution calculus R_1 polynomially simulates QU-res and therefore also Q-res. Moreover we discuss how R_1 can simulate effects of universal expansion.

Let P_1 and P_2 be two proof systems. Then P_1 *polynomially simulates* (p-simulates) P_2 if there is a polynomial p such that for every natural number n and every formula φ , the following holds. If there is a proof of φ in P_2 of size n , then there is a proof of φ (or a suitable translation of it) in P_1 whose size is less than $p(n)$.

Proposition 5. R_1 *polynomially simulates* QU-res.

Proof. Let $\Phi: Q^b M$ be a QBF in PCNF with quantifier prefix Q^b and matrix M . Consider the first-order translation $\llbracket \Phi \rrbracket_p^f$ of Φ and $Sk\llbracket \Phi \rrbracket_p^f$ (the skolemized form of $\llbracket \Phi \rrbracket_p^f$). Then every literal in M has an isomorphic counterpart in M' , the matrix of $Sk\llbracket \Phi \rrbracket_p^f$. We employ this isomorphism in the following.

Let $C_1, \dots, C_n$ be a QU-res deduction of C_n . For any clause C_i ($1 \leq i \leq n$) of the form $L_{i,1} \vee \dots \vee L_{i,m_i}$ generate a first-order clause D_i of the form $K_{i,1} \vee \dots \vee K_{i,m_i}$ where $K_{i,j} \cong L_{i,j}$ (i.e., $K_{i,j}$ is the isomorphic counterpart of $L_{i,j}$) for $j = 1, \dots, m_i$. We show by induction on n that there exists an R_1 deduction $p(f_\top), \neg p(f_\perp), E_1, \dots, E_n$ of E_n from $Sk\llbracket \Phi \rrbracket_p^f \wedge p(f_\top) \wedge \neg p(f_\perp)$ such that the following holds for $i = 1, \dots, n$.

1. E_i is non-tautological.
2. $D_i = E_i\sigma$ for some variable substitution σ .

Condition 2 implies that all E_i are not instantiated with non-variable terms.

Base: $n = 1$. Then C_1 is an input clause from M , C_1 is non-tautological by assumption (of QU-res), and D_1 is a first-order input clause with $C_1 \cong D_1$. Take $E_1 = D_1$ and $D_1 = E_1\sigma$ where σ is the empty substitution denoted by ϵ .

IH: Suppose $n \geq 1$ and for all $k \leq n$, we have based on $C_1, \dots, C_k$ an R_1 deduction $p(f_\top), \neg p(f_\perp), E_1, \dots, E_k$ of E_k from $Sk\llbracket \Phi \rrbracket_p^f \wedge p(f_\top) \wedge \neg p(f_\perp)$ such that conditions 1. and 2. hold.

Step: Consider $C_1, \dots, C_{n+1}, D_1, \dots, D_{n+1}$ and $E_1, \dots, E_{n+1}$.

CASE 1: C_{n+1} is an input clause. Then proceed as in the base case.

CASE 2: C_{n+1} is the consequence of a $\forall$ reduction applied to C_i ($i \leq n$). Let ℓ be the universal literal removed. Without loss of generality, let ℓ be positive and of the form x . Then there is a clause $D_i: \tilde{D}_i \vee p(x)$. Observe that the variable x does not occur in $\tilde{D}_i$. By IH, we have a non-tautological clause $E_i: \tilde{E}_i \vee p(y)$ and a variable substitution σ with $D_i = E_i\sigma$. E_{n+1} is obtained from E_i and $\neg p(f_\perp)$ by resolution resulting in $\tilde{E}_i$. Then $D_{n+1} = E_{n+1}\sigma$ and E_{n+1} is non-tautological because E_i is non-tautological.

CASE 3: C_{n+1} is a factor of C_i ($i \leq n$). Then there is a clause $D_i: \tilde{D}_i \vee \ell(t) \vee \ell(t)$ where $\ell(t)$ is a literal with predicate symbol p with a term t as argument. By IH, we have a non-tautological clause E_i and a variable substitution σ with $D_i = E_i\sigma$. If t is a

constant, then E_{n+1} is E_i with one occurrence of $\ell(t)$ removed, E_i is non-tautological and so is E_{n+1} and $D_{n+1} = E_{k+1}\sigma$.

Let the term t be of the form $f(\mathbf{X})$. Then E_i is $\tilde{E}_i \vee \ell(f(\mathbf{Y})) \vee \ell(f(\mathbf{Z}))$ and $\sigma(u_r) = x_r$ for all $u_r \in \mathbf{Y} \cup \mathbf{Z}$. Let π be the unifier of $\{\ell(f(\mathbf{Y})), \ell(f(\mathbf{Z}))\}$ of the form $\{y_i \setminus z_i \mid \text{for all } y_i \in \mathbf{Y}\}$. The factor E_{n+1} is then $(\tilde{E}_i \vee \ell(f(\mathbf{Z})))\pi$ and $D_{n+1} = E_{k+1}\sigma$ holds.

We argue in the following that E_{n+1} is non-tautological. Suppose E_{n+1} is tautological. Then, since $D_{n+1} = E_{n+1}\sigma$, D_{n+1} is tautological which in turn implies that C_{n+1} is tautological. But this is impossible by the definition of Q-res and QU-res.

Let t be a variable x . Then this case is similar to the case $t = f(x)$.

CASE 4: C_{n+1} is a Q-resolvent of C_i and C_j ($i, j \leq n$) upon the existential variable e . Then there are two clause $D_i: \tilde{D}_i \vee p(t_e)$ and $D_j: \tilde{D}_j \vee \neg p(t_e)$. By IH, we have non-tautological clauses E_i with $D_i = E_i\sigma_1$ and E_j with $D_j = E_j\sigma_2$ where σ_1 as well as σ_2 are variable substitutions.

SUBCASE 4.1: t_e is a functional term $f_e(\mathbf{X})$. Then

$E_i: \tilde{E}_i \vee p(f_e(\mathbf{Y}))$ and $\sigma_1(y_r) = x_r$ for all $y_r \in \mathbf{Y}$;

$E_j: \tilde{E}_j \vee \neg p(f_e(\mathbf{Z}))$ and $\sigma_2(z_r) = x_r$ for all $z_r \in \mathbf{Z}$.

Let μ be a renaming substitution such that $E_i\mu$ and E_j are variable-disjoint. In order to construct the resolvent, we have to compute the most general unifier (mgu) π of $\{p(f_e(\mathbf{Y}))\mu, p(f_e(\mathbf{Z}))\}$, which is $\{\mu(y_r) \setminus z_r \mid \text{for all } y_r \in \mathbf{Y}\}$. The unifier π is a matcher; it affects only variables from $E_i\mu$. The resolvent E_{n+1} is then $\tilde{E}_i\mu\pi \vee \tilde{E}_j$.

We show that there exists a variable substitution σ such that $D_{n+1} = E_{n+1}\sigma$. First observe that $D_i = E_i\mu\{\mu(u) \setminus \sigma_1(u) \mid \text{for all } u \in \text{var}(E_i)\}$. Then

$$\tilde{D}_i = \tilde{E}_i\mu\pi\{\pi(\mu(u)) \setminus \sigma_1(u) \mid \text{for all } u \in \text{var}(E_i)\}$$

follows. For all $y_i \in \mathbf{Y}$, we have $\pi(\mu(y_i)) = z_i$, $\sigma_1(y_i) = x_i$ and $\sigma_2(z_i) = x_i$. Then

$$\begin{aligned} \tilde{D}_i \vee \tilde{D}_j &= \tilde{E}_i\mu\pi\{\pi(\mu(u)) \setminus \sigma_1(u) \mid \text{for all } u \in \text{var}(E_i)\} \vee \tilde{E}_j\sigma_2 \\ &= (\tilde{E}_i\mu\pi \vee \tilde{E}_j)\sigma \end{aligned}$$

where σ is

$$\{\mu(u) \setminus \sigma_1(u) \mid \text{for all } u \in \text{var}(E_i) \setminus \mathbf{Y}\} \cup \{v \setminus \sigma_2(v) \mid \text{for all } v \in \text{var}(E_j)\}.$$

Therefore $D_{n+1} = E_{n+1}\sigma$.

SUBCASE 4.2: t_e is a constant. Similar to SUBCASE 4.1 but with an empty mgu π .

The clause E_{n+1} from both subcases is non-tautological by the same reason as in CASE 3.

CASE 5: C_{n+1} is a Q-resolvent of C_i and C_j ($i, j \leq k$) upon the universal variable u . Similar to SUBCASE 4.1. $\square$

The following example illustrates how first-order resolution is able to mimic effects of universal expansion. It is unknown whether QU-res polynomially simulates universal expansion.

Example 1 (Simulation of universal expansion). Let Φ be a QBF with quantifier prefix $\exists^b a \forall^b x \exists^b b \exists^b c \exists^b d$ and matrix M in CNF containing the following clauses:

$$\begin{array}{lll} C_1: a \vee x \vee b \vee c & C_2: \neg a \vee \neg x \vee b \vee c & C_3: x \vee \neg b \vee c \\ C_4: \neg x \vee \neg b \vee d & C_5: \neg c \vee d & C_6: \neg d \end{array}$$

We expand the $\forall^b$ quantifier and obtain Φ_e with the new expanded quantifier prefix $\exists^b a \exists^b b \exists^b b' \exists^b c \exists^b c' \exists^b d \exists^b d'$ and the following clauses:

$$\begin{array}{llll} D_1: a \vee b \vee c & D_2: \neg a \vee b' \vee c' & D_3: \neg b \vee c & D_4: \neg b' \vee d' \\ D_5: \neg c \vee d & D_6: \neg c' \vee d' & D_7: \neg d & D_8: \neg d' \end{array}$$

A Q-resolution refutation of Φ_e (in linear form) is as follows:

$D_1, D_2, b \vee b' \vee c \vee c', D_3, b' \vee c \vee c \vee c', b' \vee c \vee c', D_4, c \vee c' \vee d', D_5, c' \vee d \vee d', D_6, d \vee d' \vee d', d \vee d', D_7, d', D_8, \square$

There exists no LDQ-res refutation for the original (unexpanded) formula) of the same structure, because the second resolution step (upon b) would fail. Translating Φ results in a first-order formula Φ_f (in skolemized form) and adding $p(f_\top)$ and $\neg p(f_\perp)$ yields the following clauses:

$$\begin{array}{ll} F_1: p(a) \vee p(x) \vee p(f_b(x)) \vee p(f_c(x)) & F_2: \neg p(a) \vee \neg p(x) \vee p(f_b(x)) \vee p(f_c(x)) \\ F_3: p(x) \vee \neg p(f_b(x)) \vee p(f_c(x)) & F_4: \neg p(x) \vee \neg p(f_b(x)) \vee p(f_d(x)) \\ F_5: \neg p(f_c(x)) \vee p(f_d(x)) & F_6: \neg p(f_d(x)) \\ F_7: p(f_\top) & F_8: \neg p(f_\perp) \end{array}$$

We use resolution to compute clauses F_9 to F_{12} corresponding to D_1 to D_4 as follows.

$$\begin{array}{ll} F_9: & F_1, F_8, p(a) \vee p(f_b(f_\perp)) \vee p(f_c(f_\perp)) \\ F_{10}: & F_2, F_7, \neg p(a) \vee p(f_b(f_\top)) \vee p(f_c(f_\top)) \\ F_{11}: & F_3, F_8, \neg p(f_b(f_\perp)) \vee p(f_c(f_\perp)) \\ F_{12}: & F_4, F_7, \neg p(f_b(f_\top)) \vee p(f_d(f_\top)) \end{array}$$

For C_5, C_6 , no special clauses are needed in the first-order part, since F_5, F_6 are instantiated by unification. The constants in the resolvents block factoring similar to primed and unprimed variables in the QBF case. A derivation of these clauses is not necessary, because the first-order theorem prover can decide not to factor.

A first-order resolution refutation of Φ_f is as follows:

$F_9, F_{10}, p(f_b(f_\perp)) \vee p(f_b(f_\top)) \vee p(f_c(f_\perp)) \vee p(f_c(f_\top)), F_{11}, p(f_b(f_\top)) \vee p(f_c(f_\perp)) \vee p(f_c(f_\perp)) \vee p(f_c(f_\top)), p(f_b(f_\top)) \vee p(f_c(f_\perp)) \vee p(f_c(f_\top)), F_{12}, p(f_c(f_\perp)) \vee p(f_c(f_\top)) \vee p(f_d(f_\top)), F_5, p(f_c(f_\top)) \vee p(f_d(f_\perp)) \vee p(f_d(f_\top)), p(f_d(f_\perp)) \vee p(f_d(f_\top)) \vee p(f_d(f_\top)), p(f_d(f_\perp)) \vee p(f_d(f_\top)), F_6, p(f_d(f_\top)), \square$

4 Conclusion

We studied first-order resolution refutations as a representation of refutations in different Q-resolution calculi. We identified infinite families $(\Phi)_{i \geq 1}$ and $(\Omega)_{i \geq 1}$ of QBFs where Φ_i and Ω_i have only super-polynomially sized resolution refutations in Q-res,

QU-res, LDQ-res and LDQU-res, but both translations (together with first-order resolution) result in short refutations. Moreover, we have shown that slightly different translations of QBFs to first-order formulas may result in different formulas with super-polynomial differences in refutation size. Instantiation is *the* feature for obtaining short first-order refutations for our formulas and it comes for free by unification. Moreover, effects of universal expansion can be easily mimicked on the first-order level.

In future work, we will extend the polynomial simulation to long distance Q-resolution calculi.

References

1. V. Balabanov and J.-H. R. Jiang. Unified QBF certification and its applications. *Formal Methods in System Design*, 41(1):45–65, 2012.
2. U. Egly. On sequent systems and resolution for QBFs. In A. Cimatti and R. Sebastiani, editors, *SAT*, volume 7317 of *Lecture Notes in Computer Science*, pages 100–113. Springer, 2012.
3. U. Egly, F. Lonsing, and M. Widl. Long-distance resolution: Proof generation and strategy extraction in search-based QBF solving. In K. L. McMillan, A. Middeldorp, and A. Voronkov, editors, *LPAR*, volume 8312 of *Lecture Notes in Computer Science*, pages 291–308. Springer, 2013.
4. A. Haken. The intractability of resolution. *Theor. Comput. Sci.*, 39:297–308, 1985.
5. M. Janota, L. Chew, and O. Beyersdorff. On unification of QBF resolution-based calculi. *Electronic Colloquium on Computational Complexity (ECCC)*, 21:36, 2014.
6. H. Kleine Büning, M. Karpinski, and A. Flögel. Resolution for quantified Boolean formulas. *Inf. Comput.*, 117(1):12–18, 1995.
7. A. Leitsch. *The resolution calculus*. Texts in theoretical computer science. Springer, 1997.
8. D. A. Plaisted and S. Greenbaum. A structure-preserving clause form translation. *J. Symb. Comput.*, 2(3):293–304, 1986.
9. M. Seidl, F. Lonsing, and A. Biere. qbf2epr: A tool for generating EPR formulas from QBF. In P. Fontaine, R. A. Schmidt, and S. Schulz, editors, *PAAR@IJCAR*, volume 21 of *EPiC Series*, pages 139–148. EasyChair, 2012.