Short Proofs for Some Symmetric Quantified Boolean Formulas[☆]

Manuel Kauers[a], Martina Seidl[b]

[a] *Institute for Algebra, J. Kepler University Linz, Austria*
[b] *Institute for Formal Models and Verification, J. Kepler University Linz, Austria*

Abstract

We exploit symmetries to give short proofs for two prominent formula families of QBF proof complexity theory. On the one hand, we employ symmetry breakers. On the other hand, we enrich the (relatively weak) QBF resolution calculus Q-Res with the symmetry rule and obtain separations to powerful QBF calculi.

Keywords: Automated Theorem Proving, Proof Complexity, QBF

1. Introduction

A Quantified Boolean Formula (QBF) is a formula of the form $P.\phi$, where ϕ is a propositional formula, say in the variables $x_1, \dots, x_n$, and P is a quantifier prefix $P = Q_1x_1Q_2x_2 \cdots Q_nx_n$ with $Q_i \in \{\forall, \exists\}$. From QBF proof complexity theory, it is known that the shortest proof of certain QBFs may have exponential size in a resolution-based calculus [7, 4]. We consider here two families of QBFs (cf. Section 2) which play a prominent role in QBF proof complexity for separating various calculi. We make the observation that short proofs can be obtained if we take into account the symmetries of the formulas. In Section 3, we do so by using symmetry breakers. In Section 4, we enrich the oldest variant of the resolution calculus for QBF, Q-Res [6], by a *symmetry rule*, generalizing an idea reported in [8, 9] for SAT. In both cases, it turns out that the proof sizes for both families of formulas shrinks from exponential to linear. As consequences, we obtain separation results between Q-Res with the symmetry rule and powerful proof systems like IR-calc [4] and LQU$^+$ [2] (cf. Section 5).

Let us recall some basic facts and fix some notation. We only consider QBFs $P.\phi$ where ϕ is in conjunctive normal form (CNF), i.e., ϕ is a conjunction of clauses, each clause being a disjunction of literals, each literal being a variable or a negated variable, i.e., if x is a variable, x and $\bar{x}$ are literals. We also view clauses as sets of literals. The prefix $P = Q_1x_1 \dots Q_nx_n$ imposes an order $<_P$ on its variables: $x_i <_P x_j$ if $i < j$. The Q-Res calculus [6] applies the following rules on a QBF $P.\phi$:

- A Any non-tautological clause of ϕ can be derived.
- R From the already derived clauses $C \vee x$ and $C' \vee \bar{x}$ with existentially quantified variable x and C, C' such that $C \cup C'$ is not a tautology, the clause $C \vee C'$ can be derived.
- U Let $C \vee l$ be an already derived clause where l is a universal literal, $\bar{l} \notin C$ and all existential literals $k \in C$ are such that $k <_P l$. Then the clause C can be derived.

In the following, we will not mention the application of the axiom rule A explicitly. We write $C_1,\ C_2 \xrightarrow{\text{R}} C$ and $D_1 \xrightarrow{\text{U}} D$ for the application of R and U. A refutation of a QBF $P.\phi$ is the consecutive application of the resolution rule R and the universal reduction rule U until the empty clause is derived. Q-Res is sound and complete [6].

Finally, let us recall the notion of (syntactic) symmetries for QBFs [5]. A bijective map σ from the set $\{x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n\}$ of literals to itself is called admissible for a prefix $P = Q_1x_1 \dots Q_nx_n$ if for all $x \in \{x_1, \dots, x_n\}$ we have $\overline{\sigma(x)} = \sigma(\bar{x})$ and x, $\sigma(x)$ belong to the same quantifier block, i.e., for all $i, j \in \{1, \dots, n\}$ we have $\sigma(x_i) \in \{x_j, \bar{x}_j\}$ only if $Q_{\min(i,j)} = Q_{\min(i,j)+1} = \cdots = Q_{\max(i,j)}$. An admissible function σ is called a symmetry for a QBF

[☆] Parts of this work were supported by the Austrian Science Fund (FWF) under grant numbers NFN S11408-N23 (RiSE), and SFB F5004.

Email addresses: manuel.kauers@jku.at (Manuel Kauers), martina.seidl@jku.at (Martina Seidl)

$P.\phi$ if applying σ to all literals in ϕ maps ϕ to itself (up to reordering clauses and literals).

2. Formula Families

We consider the following two families of formulas.

Definition 1 ([6]). *For $n \in \mathbb{N}$, the formula* KBKF_n *is defined by the prefix*

$$\exists x_1 y_1 \forall a_1 \exists x_2 y_2 \forall a_2 \dots \exists x_n y_n \forall a_n \exists z_1 \dots z_n$$

and the following clauses:

- $C_1 = (\bar{x}_1 \vee \bar{y}_1)$
- *for* $j = 1, \dots, n-1$*:*
  $C_{2j} = (x_j \vee \bar{a}_j \vee \bar{x}_{j+1} \vee \bar{y}_{j+1})$
  $C_{2j+1} = (y_j \vee a_j \vee \bar{x}_{j+1} \vee \bar{y}_{j+1})$.
- $C_{2n} = (x_n \vee \bar{a}_n \vee \bar{z}_1 \vee \dots \vee \bar{z}_n)$,
  $C_{2n+1} = (y_n \vee a_n \vee \bar{z}_1 \vee \dots \vee \bar{z}_n)$
- *for* $j = 1, \dots, n$*:*
  $B_{2j-1} = (a_j \vee z_j)$ *and* $B_{2j} = (\bar{a}_j \vee z_j)$.

For every $n \in \mathbb{N}$, the formula KBKF_n is false, and it is known [6, 4, 3] that any Q-Res refutation needs a number of steps which is at least exponential in n.

Definition 2 ([4]). *For $n \in \mathbb{N}$ with $n > 1$, the formula* QUPARITY_n *is defined by the prefix*

$$\exists x_1 \dots x_n \forall a_1 a_2 \exists y_2 \dots y_n$$

and the following clauses:

- $A_2 = (\bar{x}_1 \vee \bar{x}_2 \vee \bar{y}_2 \vee a_1 \vee a_2)$
  $B_2 = (\bar{x}_1 \vee x_2 \vee y_2 \vee a_1 \vee a_2)$
  $C_2 = (x_1 \vee \bar{x}_2 \vee y_2 \vee a_1 \vee a_2)$
  $D_2 = (x_1 \vee x_2 \vee \bar{y}_2 \vee a_1 \vee a_2)$
- *for* $j = 3, \dots, n$*:*
  $A_j = (\bar{y}_{j-1} \vee \bar{x}_j \vee \bar{y}_j \vee a_1 \vee a_2)$
  $B_j = (\bar{y}_{j-1} \vee x_j \vee y_j \vee a_1 \vee a_2)$
  $C_j = (y_{j-1} \vee \bar{x}_j \vee y_j \vee a_1 \vee a_2)$
  $D_j = (y_{j-1} \vee x_j \vee \bar{y}_j \vee a_1 \vee a_2)$
- $E_1 = (a_1 \vee a_2 \vee y_n)$ *and* $E_2 = (\bar{a}_1 \vee \bar{a}_2 \vee \bar{y}_n)$
- *for* $i = 2, \dots, n$, A'_i, B'_i, C'_i, D'_i *are obtained from* A_i, B_i, C_i, D_i *by replacing* $a_1 \vee a_2$ *by* $\bar{a}_1 \vee \bar{a}_2$.

QUPARITY_n is a variant of the QPARITY_n family [4] which encodes $\exists x_1 \dots x_n \forall z. z \neq x_1 \oplus \dots \oplus x_n$, where $\oplus$ stands for exclusive or. Obviously all these formulas are false. Refuting QPARITY_n needs an exponential number of steps in the calculus Q-Res, but not in the stronger calculus LQU^+. We use QUPARITY_n instead of QPARITY_n because for this family, also LQU^+ needs exponentially many steps [4]. This will be used in Section 5.

3. Symmetry Breakers

A symmetry breaker for $P.\phi$ is a certain Boolean formula ψ over the variables of P such that when $P.\phi$ is true, so is $P.(\phi \wedge \psi)$. Typically, ψ is chosen in such a manner that $P.(\phi \wedge \psi)$ has fewer symmetries than $P.\phi$, hence the name symmetry breaker. A detailed discussion on symmetry breakers for QBF can be found in [5]. Given the prefix $P = Q_1 x_1 \cdots Q_n x_n$ and a set S of symmetries for QBF $P.\phi$, it was shown in [1, 5] that

$$\psi = \bigwedge_{\substack{i=1 \\ Q_i = \exists}}^{n} \bigwedge_{\sigma \in S} \Bigg(\Big(\bigwedge_{j<i} (x_j \leftrightarrow \sigma(x_j)) \Big) \rightarrow (x_i \rightarrow \sigma(x_i)) \Bigg)$$

is a symmetry breaker for any QBF $P.\phi$.

For the formulas KBKF_n (Def. 1), we have for every $i = 1, \dots, n$ the symmetry $\sigma_i = (x_i\ y_i)(\bar{x}_i\ \bar{y}_i)(a_i\ \bar{a}_i)$ which exchanges the variables x_i, y_i, the literals $\bar{x}_i, \bar{y}_i$, and the literals $a_i, \bar{a}_i$. Therefore,

$$\psi_n = (\bar{x}_1 \vee y_1) \wedge \dots \wedge (\bar{x}_n \vee y_n)$$

is a symmetry breaker for KBKF_n.

Proposition 1. *For $n \in \mathbb{N}$, write KBKF_n as $P_n.\phi_n$ and let ψ_n be the symmetry breaker from above. Then $P_n.(\phi_n \wedge \psi_n)$ has a refutation proof with no more than $4n$ steps.*

The proof proceeds as follows.

- $C_1,\ (\bar{x}_1 \vee y_1) \xrightarrow{\text{R}} U_0 := \bar{x}_1$.
- for $j = 1, \dots, n-1$, do
  $C_{2j},\ U_{j-1} \xrightarrow{\text{R}} \tilde{U}_j := (\bigvee_{i=1}^{j} \bar{a}_i \vee \bar{x}_{j+1} \vee \bar{y}_{j+1})$.
  $\tilde{U}_j,\ (\bar{x}_{j+1} \vee y_{j+1}) \xrightarrow{\text{R}} U_j := (\bigvee_{i=1}^{j} \bar{a}_i \vee \bar{x}_{j+1})$.
  Then $U_{n-1} = (\bar{a}_1 \vee \dots \vee \bar{a}_{n-1} \vee \bar{x}_n)$.
- $C_{2n},\ U_{n-1} \xrightarrow{\text{R}} V_0 := (\bigvee_{i=1}^{n} \bar{a}_i \vee \bar{z}_1 \vee \dots \vee \bar{z}_n)$.

- for $j = 1, \ldots, n$, do
  $V_{j-1},\ B_{2j} \xrightarrow{\text{R}} V_j := (\bigvee_{i=1}^{n} \bar{a}_i \vee \bigvee_{i=j+1}^{n} \bar{z}_i)$.
  Then $W_0 := V_n = (\bar{a}_1 \vee \cdots \vee \bar{a}_n)$.
- for $j = 1, \ldots, n$, do
  $W_{j-1} \xrightarrow{\text{U}} W_j := (\bar{a}_{j+1} \vee \cdots \vee \bar{a}_n)$.
  W_n is the empty clause.

For the formulas QUPARITY_n, the argument is similar. In this case, we have the symmetries $\sigma_1 = (x_1\ x_2)(\bar{x}_1\ \bar{x}_2)$ and

$$\sigma_i = (x_i\ \bar{x}_i)(a_1\ \bar{a}_1)(a_2\ \bar{a}_2)(y_i\ \bar{y}_i) \cdots (y_n\ \bar{y}_n)$$

for every $i = 2, \ldots, n$. There are some further symmetries which we will not need. The symmetries $\sigma_1, \ldots, \sigma_n$ give rise to the symmetry breaker

$$\psi_n = (\bar{x}_1 \vee x_2) \wedge \bar{x}_2 \wedge \cdots \wedge \bar{x}_n$$

for QUPARITY_n.

Proposition 2. *For $n \in \mathbb{N}$ with $n > 1$, write QUPARITY_n as $P_n.\phi_n$, and let ψ_n be the symmetry breaker from above. Then $P_n.(\phi_n \wedge \psi_n)$ has a refutation proof with no more than $2n + 1$ steps.*

The proof proceeds as follows.

- $D_2,\ (\bar{x}_1 \vee x_2) \xrightarrow{\text{R}} U_1 := (x_2 \vee \bar{y}_2 \vee a_1 \vee a_2)$.
- $U_1,\ \bar{x}_2 \xrightarrow{\text{R}} U_2 := (\bar{y}_2 \vee a_1 \vee a_2)$.
- for $j = 3, \ldots, n$, do
  $D_j,\ \bar{x}_j \xrightarrow{\text{R}} \tilde{D}_j := (y_{j-1} \vee \bar{y}_j \vee a_1 \vee a_2)$.
- for $j = 3, \ldots, n$, do
  $U_{j-1},\ \tilde{D}_j \xrightarrow{\text{R}} U_j := (\bar{y}_j \vee a_1 \vee a_2)$.
- $U_n = (\bar{y}_n \vee a_1 \vee a_2),\ E_1 \xrightarrow{\text{R}} (a_1 \vee a_2)$.
- $(a_1 \vee a_2) \xrightarrow{\text{U}} a_2 \xrightarrow{\text{U}}$ empty clause.

4. The Symmetry Rule

As an alternative to using symmetry breakers, we can enrich the calculus Q-Res as introduced in Section 1 to the calculus Q-Res+S by adding the following rule, which allows us to exploit symmetries of the input formula $P.\phi$ within the proof.

S From an already derived clause C and a symmetry σ of $P.\phi$, the clause $\sigma(C)$ can be derived.

Several variants of this rule have been proposed for SAT in [8, 9], but to our knowledge it has not yet been considered in the context of QBF. However, it is easy to see that the rule also works for QBF.

Proposition 3. *Let $P.\phi$ be a QBF, and suppose that C is a clause which can be derived from ϕ using the rules S, R, U. Then it can also be derived using only the rules R, U.*

Proof. Suppose otherwise. Then there are clauses which can be derived with S, R, U but not with R, U alone. Let C be such a clause, and consider a derivation of C with a minimal number of applications of S. The rule S is used at least once during the derivation. Consider its earliest application, suppose this application derives $\sigma(D)$ from the clause D. If we can show that $\sigma(D)$ can also be derived using only R and U, then we can eliminate this first application of S in the derivation of C and obtain a contradiction to the assumed minimality.

To show that $\sigma(D)$ can be derived using only R and U, observe first that D was derived only using R and U. For an admissible function σ, we have $\overline{\sigma(x)} = \sigma(\bar{x})$ for every variable x. Therefore, if a clause E can be derived by R from two clauses E_1 and E_2, we can derive $\sigma(E)$ by R from $\sigma(E_1)$ and $\sigma(E_2)$. Furthermore, an admissible function cannot permute literals across quantifier blocks, which implies that if F can be derived by U from F_1, then $\sigma(F)$ can be derived by U from $\sigma(F_1)$. Finally, when σ is a symmetry of ϕ and G is a clause of ϕ, then also $\sigma(G)$ is a clause of ϕ. By combining these three observations, it follows that applying σ to all clauses appearing in the derivation of D yields a derivation of $\sigma(D)$. This completes the proof. ☐

According to the previous proposition, with S we cannot derive any clause that we cannot also derive without. Therefore, soundness of Q-Res+S follows from soundness of Q-Res. Next, we illustrate that Q-Res+S allows for shorter proofs than Q-Res. For the application of S, we write $C,\ \sigma \xrightarrow{\text{S}} D$.

Proposition 4. *For every $n \in \mathbb{N}$, the formula KBKF_n can be refuted by no more than $5n$ applications of S, R, U.*

We proceed as follows by using the symmetries of the form $\sigma_i = (x_i\ y_i)(\bar{x}_i\ \bar{y}_i)(a_i\ \bar{a}_i)$ for $i = 1, \ldots, n$.

- set $U_{n+1} = C_{2n+1}$.

- for $j = n, \dots, 1$, do

  $U_{j+1},\ B_{2j-1} \xrightarrow{\mathrm{R}} U_j \ := \ (y_n \vee \bigvee_{i=j}^{n} a_i \vee \bigvee_{i=1}^{j-1} \bar{z}_i)$.

- set $W_n := U_1 = (y_n \vee a_1 \vee \cdots \vee a_n)$.

- for $j = n, \dots, 2$, do

  $W_j \xrightarrow{\mathrm{U}} V_j := (y_j \vee \bigvee_{i=1}^{j-1} a_i)$.
  $V_j,\ \sigma_j \xrightarrow{\mathrm{S}} V_j' := (x_j \vee \bigvee_{i=1}^{j-1} a_i)$.
  $V_j',\ C_{2j-1} \xrightarrow{\mathrm{R}} V_j'' := (y_{j-1} \vee \bar{y}_j \vee \bigvee_{i=1}^{j-1} a_i)$.
  $V_j'',\ V_j \xrightarrow{\mathrm{R}} W_{j-1} := (y_{j-1} \vee \bigvee_{i=1}^{j-1} a_i)$.

- $W_1 = (y_1 \vee a_1) \xrightarrow{\mathrm{U}} V_1 = y_1$.

- $V_1,\ \sigma_1 \xrightarrow{\mathrm{S}} V_1' := x_1$.

- $V_1',\ C_1 \xrightarrow{\mathrm{R}} V_1'' := \bar{y}_1$.

- $V_1'',\ V_1 \xrightarrow{\mathrm{R}}$ empty clause.

Proposition 5. *For every $n \in \mathbb{N}$ with $n > 1$, the formula* $\mathrm{QUPARITY}_n$ *can be refuted by no more than $3n + 2$ applications of S, R, U.*

Recall from Section 4 that $\mathrm{QUPARITY}_n$ has the symmetries $\sigma_1 = (x_1\ x_2)(\bar{x}_1\ \bar{x}_2)$ and $\sigma_i = (x_i\ \bar{x}_i)(a_1\ \bar{a}_1)(a_2\ \bar{a}_2)(y_i\ \bar{y}_i)\cdots(y_n\ \bar{y}_n)$ for $i > 1$.

- $D_n,\ E_1 \xrightarrow{\mathrm{R}} U_n := (y_{n-1} \vee x_n \vee a_1 \vee a_2)$.

- for $j = n-1, \dots, 3$, do

  $D_j,\ U_{j+1} \xrightarrow{\mathrm{R}} U_j := (y_{j-1} \vee \bigvee_{i=j}^{n} x_i \vee a_1 \vee a_2)$.

- $D_2,\ U_3 \xrightarrow{\mathrm{R}} U_2 := (\bigvee_{i=1}^{n} x_i \vee a_1 \vee a_2)$.

- $U_2 \xrightarrow{\mathrm{U}} \bigvee_{i=1}^{n} x_i \vee a_1 \xrightarrow{\mathrm{U}} V_n := \bigvee_{i=1}^{n} x_i$.

- for $j = n, \dots, 2$, do

  $V_j,\ \sigma_j \xrightarrow{\mathrm{S}} W_j := (x_1 \vee \cdots \vee x_{j-1} \vee \bar{x}_j)$.
  $V_j,\ W_j \xrightarrow{\mathrm{R}} V_{j-1} := (x_1 \vee \cdots \vee x_{j-1})$.

- $V_1 = x_1,\ \sigma_1 \xrightarrow{\mathrm{S}} W_1 := x_2$.

- $W_1,\ \sigma_2 \xrightarrow{\mathrm{S}} W_2 := \bar{x}_2$.

- $W_1,\ W_2 \xrightarrow{\mathrm{R}}$ empty clause.

5. Consequences

From recent results, it is known that plain Q-Res is rather weak (for a fine-grained comparison of QBF proof systems see [4]). Both, the expansion-based proof system IR-calc and the CDCL-based proof system LQU^+ are strictly stronger than Q-Res. The addition of the symmetry rule changes the situation. While the $\mathrm{QUPARITY}_n$ formulas are hard for LQU^+ and the KBKF_n formulas are hard for IR-calc, we have shown that both are easy for Q-Res+S. Now one may ask if Q-Res+S is strictly stronger than IR-calc or LQU^+. The answer is clearly "no". For KBKF_n, the application of the symmetry rule can be hindered by introducing n universally quantified variables b_i which are placed between x_i and y_i in the prefix, and changing each clause C_{2j} to $C_{2j} \vee b_j$. For this modified formula, LQU^+ can still find a short proof, but Q-Res+S can only apply R and U, hence it falls back to Q-Res which does not exhibit short proofs for KBKF_n. In a similar way, $\mathrm{QUPARITY}_n$ can be modified such that these formulas remain simple for IR-calc, but become hard for Q-Res+S.

Proposition 6. *Q-Res+S and IR-calc are incomparable, and so are Q-Res+S and LQU^+.*

For the future, the effects of adding S to more powerful proof systems than Q-Res remain to be investigated.

Acknowledgments. Parts of this work were supported by the Austrian Science Fund (FWF) under grant numbers NFN S11408-N23 (RiSE), Y464-N18, and SFB F5004.

[1] Gilles Audemard, Said Jabbour, and Lakhdar Sais. Efficient symmetry breaking predicates for Quantified Boolean Formulae. In *Proc. of Workshop on Symmetry and Constraint Satisfaction Problems*, 2007.

[2] Valeriy Balabanov, Magdalena Widl, and Jie-Hong R. Jiang. QBF resolution systems and their proof complexities. In *SAT*, volume 8561 of *Lecture Notes in Computer Science*, pages 154–169. Springer, 2014.

[3] Olaf Beyersdorff, Joshua Blinkhorn, and Luke Hinde. Size, cost and capacity: A semantic technique for hard random qbfs. In *ITCS*, volume 94 of *LIPIcs*, pages 9:1–9:18. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018.

[4] Olaf Beyersdorff, Leroy Chew, and Mikolás Janota. Proof complexity of resolution-based QBF calculi. In *STACS*, volume 30 of *LIPIcs*, pages 76–89. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2015.

[5] Manuel Kauers and Martina Seidl. Symmetries of Quantified Boolean Formulas. *CoRR*, abs/1802.03993 (preprint; accepted for SAT'18), 2018.

[6] Hans Kleine Büning, Marek Karpinski, and Andreas Flögel. Resolution for quantified boolean formulas. *Inf. Comput.*, 117(1):12–18, 1995.

[7] Hans Kleine Büning and Theodor Lettmann. *Aussagenlogik - Deduktion und Algorithmen*. Leitfäden und Monographien der Informatik. Teubner, 1994.

[8] Balakrishnan Krishnamurthy. Short proofs for tricky formulas. *Acta Inf.*, 22(3):253–275, 1985.

[9] Alasdair Urquhart. The symmetry rule in propositional logic. *Discrete Applied Mathematics*, 96-97:177–193, 1999.