1. Introduction

A Quantified Boolean Formula (QBF) is a formula of the form $P.\phi$, where $\phi$ is a propositional formula, say in the variables $x_1, \ldots, x_n$, and $P$ is a quantifier prefix $P = Q_1 x_1 Q_2 x_2 \cdots Q_n x_n$ 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 \cite{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 \cite{6}, by a symmetry rule, generalizing an idea reported in \cite{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-cal\cite{4} and LQU\cite{1}[cf. Section 5]. Let us recall some basic facts and fix some notation. We only consider QBFs $P.\phi$ where $\phi$ is in conjunctive normal form (CNF), i.e., $\phi$ 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 $P = Q_1 x_1 \cdots Q_n x_n$ imposes an order $<_P$ on its variables: $x_i <_P x_j$ if $i < j$. The Q-Res calculus \cite{6} applies the following rules on a QBF $P.\phi$:

1. Any non-tautological clause of $\phi$ can be derived.
2. From the already derived clauses $C \lor x$ and $C' \lor \bar{x}$ with existentially quantified variable $x$ and $C, C'$ such that $C \lor C'$ is not a tautology, the clause $C \lor C'$ can be derived.
3. Let $C \lor l$ be an already derived clause where $l$ is a universal literal, $l \notin C$ 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 $C_1, C_2 \Rightarrow R C$ and $D_1 \Rightarrow U D$ 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 \cite{6}. A bijective map $\sigma$ from the set $\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}$ of literals to itself is called admissible for a prefix $P = Q_1 x_1 \cdots Q_n x_n$ if for all $x \in \{x_1, \ldots, x_n\}$ we have $\sigma(x) = \sigma(\bar{x})$ and $x, \sigma(x)$ belong to the same quantifier block, i.e., for all $i,j \in \{1, \ldots, n\}$ 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 $\sigma$ is called a symmetry for a QBF.
2. Formula Families

We consider the following two families of formulas.

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

\[
\exists x_1 y_1 \forall a_1 \exists x_2 y_2 \forall a_2 \ldots \exists x_n y_n \forall a_n \exists z_1 \ldots z_n
\]

and the following clauses:

- \( C_1 = (\bar{x}_1 \lor \bar{y}_1) \)
- for \( j = 1, \ldots, n - 1 \):
  - \( C_{2j} = (x_j \lor \bar{a}_j \lor \bar{x}_{j+1} \lor \bar{y}_{j+1}) \)
  - \( C_{2j+1} = (y_j \lor \bar{a}_j \lor \bar{x}_{j+1} \lor \bar{y}_{j+1}) \)
- \( C_{2n} = (x_n \lor \bar{a}_n \lor \bar{x}_1 \lor \ldots \lor z_n) \),
  - \( C_{2n+1} = (y_n \lor \bar{a}_n \lor \bar{x}_1 \lor \ldots \lor z_n) \)
- for \( j = 1, \ldots, n \):
  - \( B_{2j-1} = (a_j \lor z_j) \) and \( B_{2j} = (\bar{a}_j \lor z_j) \).

For every \( n \in \mathbb{N} \), the formula \( \text{KBKF}_n \) 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 \( \text{QUPARITY}_n \) is defined by the prefix

\[
\exists x_1 \ldots x_n \forall a_1 a_2 \exists y_2 \ldots y_n
\]

and the following clauses:

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

**QUPARITY** \( n \) is a variant of the QPARITY \( n \) family [4] which encodes \( \exists x_1 \ldots x_n \forall z. z \neq x_1 \oplus \cdots \oplus x_n \), 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 \( \psi \) over the variables of \( P \) such that when \( P, \phi \) is true, so is \( P, (\phi \land \psi) \). Typically, \( \psi \) is chosen in such a manner that \( P, (\phi \land \psi) \) 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

\[
\psi = \bigwedge_{i=1}^{n} \bigwedge_{j<i} \big( (\bigwedge_{x_j \leftrightarrow \sigma(x_j)} (x_i \rightarrow \sigma(x_i))) \big)
\]

is a symmetry breaker for any QBF \( P, \phi \).

For the formulas \( \text{KBKF}_n \) (Def. 1), we have for every \( i = 1, \ldots, n \) the symmetry \( \sigma_i = (x_1 y_1)(\bar{x}_i \bar{y}_i)(a_i \bar{a}_i) \) 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,

\[
\psi_n = (\bar{x}_1 \lor y_1) \land \cdots \land (\bar{x}_n \lor y_n)
\]

is a symmetry breaker for KBKF \( n \).

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

The proof proceeds as follows.

- \( C_1, (\bar{x}_1 \lor y_1) \xrightarrow{R} U_0 := \bar{x}_1 \).
- for \( j = 1, \ldots, n - 1 \), do
  - \( C_{2j}, U_{j-1} \xrightarrow{R} \bar{U}_j := (\bigvee_{i=1}^{j} \bar{a}_i \lor \bar{x}_j \lor \bigvee_{j+1}^{n} \bar{y}_{j+1}). \)
  - \( \bar{U}_j, (\bar{x}_{j+1} \lor \bigvee_{j+1}^{n} y_{j+1}) \xrightarrow{R} U_j := (\bigvee_{i=1}^{j} \bar{a}_i \lor \bar{x}_{j+1}). \)
  - Then \( U_{n-1} := (\bar{a}_1 \lor \cdots \lor \bar{a}_{n-1} \lor \bar{x}_n). \)
- \( C_{2n}, U_{n-1} \xrightarrow{R} V_0 := (\bigvee_{i=1}^{n} \bar{a}_i \lor \bar{x}_1 \lor \cdots \lor \bar{x}_n). \)
• for \( j = 1, \ldots, n \), do
  \[ V_{j-1}, \ B_{2j} \xrightarrow{R} V_j := (\lor^{n}_{i=1} \bar{a}_i \lor \lor^{n}_{i=j+1} \bar{x}_i). \]
  Then \( W_0 := V_n = (\lor a_1 \lor \cdots \lor a_n) \).

• for \( j = 1, \ldots, n \), do
  \[ W_{j-1} \xrightarrow{U} W_j := (\lor a_{j+1} \lor \cdots \lor a_n). \]
  \( W_n \) is the empty clause.

For the formulas \( Q\text{PARITY}_n \), the argument is similar. In this case, we have the symmetries
\[ \sigma_i = (x_i \bar{x}_i)(a_1 \bar{a}_1)(a_2 \bar{a}_2)(y_i \bar{y}_i) \cdots (y_n \bar{y}_n) \]
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
\[ \psi_n = (\bar{x}_1 \lor x_2) \lor \cdots \lor \bar{x}_n \]
for \( Q\text{PARITY}_n \).

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

The proof proceeds as follows.

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

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 \( \sigma \) 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 \( \phi \) 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 \( \sigma \), we have \( \sigma(\bar{x}) = \sigma(\bar{x}) \) 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 \( \sigma \) is a symmetry of \( \phi \) and \( G \) is a clause of \( \phi \), then also \( \sigma(G) \) is a clause of \( \phi \). By combining these three observations, it follows that applying \( \sigma \) 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 \( C, \ \sigma \xrightarrow{S} D \).

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

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

- set \( U_{n+1} = C_{2n+1} \).
for $j = n, \ldots, 1$, do

\[ U_{j+1}, B_{2j-1} \xrightarrow{R} U_j := (y_n \lor \lor_{i=j}^n a_i \lor \lor_{i=1}^{j-1} x_i). \]

- set $W_n := U_1 := (y_n \lor a_1 \lor \cdots \lor a_n)$.
- for $j = n, \ldots, 2$, do

\[ W_j \xrightarrow{U} V_j := (y_j \lor \lor_{i=1}^{j-1} a_i), \]

\[ V_j, \sigma_j \xrightarrow{S} V'_j := (x_j \lor \lor_{i=1}^{j-1} a_i), \]

\[ V''_j := (y_j \lor \lor_{i=1}^{j-1} a_i). \]

- $W_1 = (y_1 \lor a_1) \xrightarrow{U} V_1 = y_1$.
- $V_1, \sigma_1 \xrightarrow{S} V'_1 := x_1$.
- $V'_1 \xrightarrow{C_1} V''_1 := \bar{y}_1$.
- $V''_1, V_1 \xrightarrow{R} \text{empty clause.}$

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

Recall from Section 4 that $\text{QUPARITY}_n$ has the symmetries $\sigma_1 = (x_1 x_2)(\bar{x}_1 \bar{x}_2)$ and $\sigma_i = (x_1 x_i)(a_1 a_i)(a_2 a_2)(y_1 y_i) \cdots (y_n y_n)$ for $i > 1$.

- $D_n$, $E_1 \xrightarrow{R} U_n := (y_{n-1} \lor x_n \lor a_1 \lor a_2)$.
- for $j = n-1, \ldots, 3$, do

\[ D_j, U_{j+1} \xrightarrow{R} U_j := (y_{j-1} \lor \lor_{i=j}^n x_i \lor a_1 \lor a_2). \]

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

\[ \lor_{i=1}^n x_i \lor a_1 \lor a_2 \xrightarrow{U} V_n := \lor_{i=1}^n x_i. \]

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

\[ V_j, \sigma_j \xrightarrow{S} W_j := (x_1 \lor \cdots \lor x_{j-1} \lor \bar{x}_j). \]

\[ V_j, W_j \xrightarrow{R} V_{j-1} := (x_1 \lor \cdots \lor x_{j-1}). \]

- $V_1 = x_1$, $\sigma_1 \xrightarrow{S} W_1 := x_2$.
- $W_1, \sigma_2 \xrightarrow{S} W_2 := \bar{x}_2$.

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

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 $\text{LQU}^+$ are strictly stronger than Q-Res. The addition of the symmetry rule changes the situation. While the 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 $C_{2j} \lor b_j$. 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, 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.


