On Sequent Systems and Resolution for Quantified Boolean Formulas

Uwe Egly

Knowledge-Based Systems Group
Institute of Information Systems
Vienna University of Technology
Outline

Introduction

Calculi for QBFs
  Sequent calculi
  A resolution calculus

Comparing sequent systems with Q-resolution

Conclusion
A calculus $P_1$ polynomially simulates ($p$-simulates) another calculus $P_2$ if there is a polynomial $p$ such that for every natural number $n$ and every formula $\varphi$, the following holds.

If there is a proof of $\varphi$ in $P_2$ of size $n$, then there is a proof of $\varphi$ (or a suitable translation of it) in $P_1$ whose size is less than $p(n)$. 

Sequent calculi for QBFs

Introduction and propositional rules

- Inference rules do not work on formulas but on sequents.
- These are pairs \((\Gamma, \Delta)\) of multisets of formulas.
- Example rules for conjunctions:

  \[
  \Gamma \vdash \Delta, \phi \quad \Gamma \vdash \Delta, \psi \\
  \Gamma \vdash \Delta, (\phi \land \psi) \quad ^\land r \\
  \phi, \psi, \Gamma \vdash \Delta \\
  (\phi \land \psi), \Gamma \vdash \Delta \quad ^\land l
  \]

- Similar rules for other binary connectives and negation.

- Axioms are sequents of the form \(\phi, \Gamma \vdash \Delta, \phi\).

- An important (redundant) rule is cut:

  \[
  \Gamma \vdash \Delta, \phi \quad \phi, \Gamma \vdash \Delta \\
  \Gamma \vdash \Delta \quad ^\text{cut}
  \]
Sequent calculi for QBFs
From propositional formulas to QBFs

- We extend propositional LK\textsubscript{cut} by different quantifier rules
- Strong quantifier rules (i.e., with eigenvariable conditions)
  \[
  \frac{\Gamma \vdash \Delta, \Phi\{p/q\}}{\Gamma \vdash \Delta, (\forall p \Phi)} \quad \forall r_e
  \]
  \[
  \frac{\Phi\{p/q\}, \Gamma \vdash \Delta}{(\exists p \Phi), \Gamma \vdash \Delta} \quad \exists l_e
  \]
- Weak quantifier rules (\(\Psi\) is any QBF)
  \[
  \frac{\Phi\{p/\Psi\}, \Gamma \vdash \Delta}{(\forall p \Phi), \Gamma \vdash \Delta} \quad \forall l
  \]
  \[
  \frac{\Gamma \vdash \Delta, \Phi\{p/\Psi\}}{\Gamma \vdash \Delta, (\exists p \Phi)} \quad \exists r
  \]
- The resulting (cut-free) calculus for QBFs is sound and complete
Sequent calculi for QBFs
Different extensions and refinements

- **Krajíček and Pudlák (KP):**
  - Restrict the number of quantifier alternations of all formulas in a proof $\iff KP_i$
  - Incomplete in general for fixed $i$

- **Cook and Morioka (CM):**
  - Restrict $\psi$ in $\forall l$ and $\exists r$ to a propositional formula
  - Restrict the number of quantifier alternations of cut formulas in a proof ($\iff CM_i$)
  - Complete (but proofs might become shorter with increasing $i$)

**Theorem (Cook and Morioka, 2005)**

$CM_i$ and $KP_i$ are $p$-equivalent for proving $(\Sigma^q_i \cup \Pi^q_i)$-formulas.
Sequent calculi for QBFs
Refinements of the quantifier rules and calculi

- $\forall f$ and $\exists f$: Restrict $\Psi$ in $\forall$, $\exists$ to a **propositional formula**
  $G_{qfe}$ ($G_{qfe}^*$) is the (tree) calculus without cut

- $\forall v$ and $\exists v$: Restrict $\Psi$ in $\forall$, $\exists$ to a **variable** and $\bot$, $\top$
  $G_{qve}$ ($G_{qve}^*$) is the (tree) calculus without cut

**Proposition**

$G_{qve}$ with *propositional cut* cannot p-simulate $G_{qfe}^*$

Can cuts with more complex cut formulas improve the situation?
The power of $\forall l_f$ and $\exists r_f$

Proposition

Let $Gqxe_i^*$ ($x \in \{f, v\}$) be $Gqxe$ with proofs in tree form and cut formulas from $(\Sigma_i^q \cup \Pi_i^q)$. $Gqve_i^*$ p-simulates $Gqfe_i^*$ for $i > 0$.

Key idea for a proof: Use a quantified extension $\varepsilon(B) = \exists x (x \leftrightarrow B)$ and replace the left figure by the right one.

$\varepsilon(B)$ has a linear size proof $\alpha(\varepsilon(B))$ in $Gqve^*$
A resolution calculus for QBFs

- Q-res extends propositional resolution to QBFs
- It consists of the following rule:
  - The existential propositional resolution rule $\exists PR$
  - The propositional factoring rule $PF$
  - The forall reduction rule $\forall R$ for quantifier handling
- $\exists PR$ and $PF$ are the rules of propositional resolution
- The notions of Q-res deductions and Q-res refutations in tree or sequence form are similar to the propositional case

Theorem (Kleine Büning et al., 1995)

A (closed) QBF $\varphi$ in PCNF is false iff there is a Q-resolution refutation from $\varphi$. 
A resolution calculus for QBFs

The forall reduction rule

Definition (Quantification level)
Let \( Q \) be a sequence of quantifiers. Associate to each alternation its level as follows. The left-most quantifier block gets level 1, and each alternation increments the level.

Example:
\[
\forall x_1 \forall x_2 \exists y_1 \exists y_2 \exists y_3 \forall x_3 \exists y_4
\]
level 1 level 2 level 3 level 4

Definition (Forall reduction rule \( \forall R \))
Let \( C \lor \ell \lor D \) be a non-tautological clause, \( \ell \) a universal literal and no other literal in \( C, D \) has higher level. With
\[
\frac{C \lor \ell \lor D}{C \lor D} \quad \forall R
\]

we can derive \( C \lor D \) from \( C \lor \ell \lor D \).
Outline

Introduction

Calculi for QBFs
  Sequent calculi
  A resolution calculus

Comparing sequent systems with Q-resolution

Conclusion
The general idea of the exponential separation

We want to construct a family \((\varphi_n)_{n > 1}\) of QBFs, such that
- \(\varphi_n\) has a short (cut-free tree) proof in \(G^*_q\), but
- any sequence Q-res refutation of \(\neg \varphi_n\) is exponential

The construction is based on the pigeon hole formulas
(in CNF and in DNF for \(n\) holes and \(n + 1\) pigeons)

\[
\text{CPHP}^{X_n}_{n} : \left( \bigwedge_{i=1}^{n+1} \left( \bigvee_{j=1}^{n} x_{i,j} \right) \right) \land \left( \bigwedge_{j=1}^{n} \bigwedge_{1 \leq i_1 < i_2 \leq n+1} \neg x_{i_1,j} \lor \neg x_{i_2,j} \right)
\]

\[
\text{DPHP}^{X_n}_{n} : \left( \bigvee_{i=1}^{n+1} \bigwedge_{j=1}^{n} \neg x_{i,j} \right) \lor \left( \bigvee_{j=1}^{n} \bigvee_{1 \leq i_1 < i_2 \leq n+1} \left( x_{i_1,j} \land x_{i_2,j} \right) \right)
\]
The general idea of the exponential separation

We know from the literature that
1. any sequence R-refutation of $\text{CPHP}_n^{X_n}$ is exponential and
2. any cut free sequent proof of $\text{DPHP}_n^{X_n}$ is exponential

Intuitively, we want to use $\psi_n$ which is

$$\forall X_n \exists Y_n \left( \text{DPHP}_n^{Y_n} \rightarrow \text{DPHP}_n^{X_n} \right)$$

- No problem for a (cut-free) sequent proof in $\text{Gqve}^*$, because we obtain $\text{DPHP}_n^{C_n} \rightarrow \text{DPHP}_n^{C_n}$ by $\forall r$ and $\exists r$, but

- clausifying $\neg \psi_n$ results in exponentially many clauses.

- Use a kind of Tseitin translation to keep the CNF short
  $$(\exists Z_n \text{TPHP}_n^{Y_n,Z_n}, \text{where } \text{DPHP}_n^{Y_n} \equiv \exists Z_n \text{TPHP}_n^{Y_n,Z_n} \text{ holds})$$
An exponential separation of $G_{qve}^*$ and Q-resolution

Proposition

Let $\varphi_n = \forall X_n \exists Y_n \forall Z_n (TPHP_{n}^{Y_n, Z_n} \rightarrow DPHP_{n}^{X_n})$. Then there exists a proof of $\vdash \varphi_n$ in $G_{qve}^*$ of size polynomial in $n$.

Essentially prove $TPHP_{n}^{C_n, Z_n} \rightarrow DPHP_{n}^{C_n}$ which is easy!
An exponential separation of $Gqve^*$ and $Q$-resolution

Proposition

Let $\varphi_n = \forall X_n \exists Y_n \forall Z_n (TPHP_{n}^{Y_n,Z_n} \rightarrow DPHP_{n}^{X_n})$. Then any $Q$-res refutation of the negation of $\varphi_n$, i.e.,

$$\exists X_n \forall Y_n \exists Z_n (TPHP_{n}^{Y_n,Z_n} \land CPHP_{n}^{X_n})$$

has exponential size.

Since $DPHP_{n}^{Y_n}$ is valid and $DPHP_{n}^{Y_n} \equiv \exists Z_n TPHP_{n}^{Y_n,Z_n}$ holds, we have to refute $CPHP_{n}^{X_n}$ which is hard!
We have shown that different quantifier rules in sequent systems have different strength.

- Exponential separation of Gqve*/Gqfe* and Q-res
- **Instantiation** was the key property to obtain short proofs
- Possible in Gqve and Gqfe, but **not** in Q-resolution
A resolution calculus for QBFs
The existential propositional resolution rule and the propositional factoring rule

Definition (Existential propositional resolution rule $\exists PR$)
Let $A: C_1 \lor x \lor C_2$ and $B: C_3 \lor \neg x \lor C_4$ be two clauses, where the $C_i$ are possibly empty subclauses and $x$ is an $\exists$ variable. With

\[
\begin{align*}
C_1 \lor x \lor C_2 & \hspace{1cm} C_3 \lor \neg x \lor C_4 \\
\hline
C_1 \hspace{0.5cm} C_2 & \hspace{1cm} C_3 \hspace{0.5cm} C_4
\end{align*}
\]

$\exists PR$

we derive the Q-resolvent $C_1 \lor C_2 \lor C_3 \lor C_4$ from $A$ and $B$.

Definition (Propositional factoring rule PF)
Let $A: C_1 \lor \ell \lor C_2 \lor \ell \lor C_3$ be a clause with possibly empty subclauses $C_1, C_2, C_3$ and let $\ell$ be a literal. With

\[
\begin{align*}
C_1 \lor \ell \lor C_2 \lor \ell \lor C_3 & \\
\hline
C_1 \hspace{0.5cm} C_2 & \hspace{0.5cm} C_3
\end{align*}
\]

$PF$

we derive the factor $C_1 \lor \ell \lor C_2 \lor C_3$ of $A$. 
The general idea of the exponential separation

- Introduce fresh variables $z_{i_1,i_2,j}$ for the disjuncts in $\text{DPHP}_n^{X_n}$
- Use $z_{1,0,0}, \ldots, z_{n+1,0,0}$ for the first $n + 1$ disjuncts $\bigwedge_{j=1}^{n} \neg x_{i,j}$
- For the $\frac{1}{2}n(n + 1)$ disjuncts $\bigvee_{1 \leq i_1 < i_2 \leq n + 1} (x_{i_1,j} \land x_{i_2,j})$, we use
  $$z_{1,2,j}, \ldots, z_{1,n+1,j}, z_{2,3,j}, \ldots, z_{2,n+1,j}, \ldots, z_{n,n+1,j}$$
- Let $Z_n$ consists of all the $z$ variables for $\text{DPHP}_n^{X_n}$
- $\text{TPHP}_{n}^{Y_n,Z_n}$ is $D_n^{Z_n} \land P_n^{Y_n,Z_n} \land Q_n^{Y_n,Z_n}$ and its size is $O(n^3)$
The general idea of the exponential separation

\[ \text{TPHP}_{n}^{Y_n, Z_n} = D_{n}^{Z_n} \land P_{n}^{Y_n, Z_n} \land Q_{n}^{Y_n, Z_n} \]

\[ D_{n}^{Z_n} = \bigvee_{z \in Z_n} \neg z \]

\[ P_{n}^{Y_n, Z_n} = \bigwedge_{i=1}^{n+1} \bigwedge_{j=1}^{n} (z_{i,0,0} \lor \neg y_{i,j}) \]

\[ Q_{n}^{Y_n, Z_n} = \bigwedge_{j=1}^{n} \bigwedge_{1 \leq i_1 < i_2 \leq n+1} ((z_{i_1, i_2, j} \lor y_{i_1, j}) \land (z_{i_1, i_2, j} \lor y_{i_2, j})) \]

\[ \varphi_n = \forall X_n \exists Y_n \forall Z_n (\text{TPHP}_{n}^{Y_n, Z_n} \rightarrow \text{DPHP}_{n}^{X_n}) \]