On Sequent Systems and Resolution for Quantified Boolean Formulas

Uwe Egly

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

Outline

How to compare calculi?

Polynomial simulations

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 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 $p(n)$.

Sequent calculi for QBFs

Introduction and propositional rules

- Inference rules do not work on formulas but on sequents
- These are pairs (Γ, Δ) of multisets of formulas
- Example rules for conjunctions

$$\frac{\Gamma \vdash \Delta, \Phi \quad \Gamma \vdash \Delta, \Psi}{\Gamma \vdash \Delta, (\Phi \wedge \Psi)} \wedge r \qquad \frac{\Phi, \Psi, \Gamma \vdash \Delta}{(\Phi \wedge \Psi), \Gamma \vdash \Delta} \wedge l$$

- 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

$$\frac{\Gamma \vdash \Delta, \Phi \quad \Phi, \Gamma \vdash \Delta}{\Gamma \vdash \Delta} \mathit{cut}$$

Sequent calculi for QBFs

From propositional formulas to QBFs

- We extend propositional $\mathrm{LK_{cut}}$ by different quantifier rules
- Strong quantifier rules (i.e., with eigenvariable conditions)

$$\frac{\Gamma \vdash \Delta, \Phi\{p/q\}}{\Gamma \vdash \Delta, (\forall p\, \Phi)}\ \forall r_e \qquad \frac{\Phi\{p/q\}, \Gamma \vdash \Delta}{(\exists p\, \Phi), \Gamma \vdash \Delta}\ \exists l_e$$

- Weak quantifier rules (Ψ is any QBF)

$$\frac{\Phi\{p/\Psi\}, \Gamma \vdash \Delta}{(\forall p\, \Phi), \Gamma \vdash \Delta}\ \forall l \qquad \frac{\Gamma \vdash \Delta, \Phi\{p/\Psi\}}{\Gamma \vdash \Delta, (\exists p\, \Phi)}\ \exists r$$

- 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 ➥ KP_i
  - Incomplete in general for fixed i
- Cook and Morioka (CM):
  - Restrict Ψ in $\forall l$ and $\exists r$ to a propositional formula
  - Restrict the number of quantifier alternations of cut formulas in a proof (➥ 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* $(\Sigma_i^q \cup \Pi_i^q)$*-formulas.*

Sequent calculi for QBFs

Refinements of the quantifier rules and calculi

- $\forall l_f$ and $\exists r_f$: Restrict Ψ in $\forall l$, $\exists r$ to a propositional formula
  Gqfe (Gqfe*) is the (tree) calculus without cut
- $\forall l_v$ and $\exists r_v$: Restrict Ψ in $\forall l$, $\exists r$ to a variable and $\bot, \top$
  Gqve (Gqve*) is the (tree) calculus without cut

Proposition

Gqve *with propositional cut cannot p-simulate* Gqfe*

Can cuts with more complex cut formulas improve the situation?

The power of $\forall l_f$ and $\exists r_f$

Proposition

Let Gqxe_i^* *(*$\mathrm{x} \in \{\mathrm{f}, \mathrm{v}\}$*) 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

$$\dfrac{\begin{array}{c}\beta\\ \Gamma \vdash \Delta, \Phi\{p/B\}\end{array}}{\Gamma \vdash \Delta, (\exists p\,\Phi)}\ \exists r_f \qquad \Bigg| \qquad \dfrac{\begin{array}{c}\alpha(\varepsilon(B))\\ \vdash \exists x\,(x \leftrightarrow B)\end{array} \qquad \dfrac{\dfrac{\begin{array}{c}\beta'\\ q \leftrightarrow B, \Gamma \vdash \Delta, \Phi\{p/q\}\end{array}}{q \leftrightarrow B, \Gamma \vdash \Delta, \exists p\,\Phi}\ \exists r_v}{\exists x\,(x \leftrightarrow B), \Gamma \vdash \Delta, \exists p\,\Phi}\ \exists l_e}{\Gamma \vdash \Delta, \exists p\,\Phi}\ cut$$

$\varepsilon(B)$ 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 φ in PCNF is false iff there is a Q-resolution refutation from φ.

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: $\underbrace{\forall x_1 \forall x_2}_{\text{level 1}} \underbrace{\exists y_1 \exists y_2 \exists y_3}_{\text{level 2}} \underbrace{\forall x_3}_{\text{level 3}} \underbrace{\exists y_4}_{\text{level 4}}$

Definition (Forall reduction rule $\forall$R)

Let $C \vee \ell \vee D$ be a non-tautological clause, ℓ a universal literal and no other literal in C, D has higher level. With

$$\frac{C \vee \ell \vee D}{C \vee D} \; \forall\text{R}$$

we can derive $C \vee D$ from $C \vee \ell \vee D$.

Outline

The general idea of the exponential separation

We want to construct a family $(\varphi_n)_{n>1}$ of QBFs, such that

- φ_n has a short (cut-free tree) proof in Gqve*, 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)

$$\mathrm{CPHP}_n^{X_n}: \quad \left(\bigwedge_{i=1}^{n+1} \big(\bigvee_{j=1}^{n} x_{i,j}\big)\right) \wedge \left(\bigwedge_{j=1}^{n} \bigwedge_{1\leq i_1<i_2\leq n+1} (\neg x_{i_1,j} \vee \neg x_{i_2,j})\right)$$

$$\mathrm{DPHP}_n^{X_n}: \quad \left(\bigvee_{i=1}^{n+1} \bigwedge_{j=1}^{n} \neg x_{i,j}\right) \vee \left(\bigvee_{j=1}^{n} \bigvee_{1\leq i_1<i_2\leq n+1} (x_{i_1,j} \wedge x_{i_2,j})\right)$$

The general idea of the exponential separation

We know from the literature that

1. any sequence R-refutation of $\mathrm{CPHP}_n^{X_n}$ is exponential and
2. any cut free sequent proof of $\mathrm{DPHP}_n^{X_n}$ is exponential

Intuitively, we want to use ψ_n which is

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

- No problem for a (cut-free) sequent proof in Gqve*, because we obtain $\mathrm{DPHP}_n^{C_n} \rightarrow \mathrm{DPHP}_n^{C_n}$ 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 (➥ $\exists Z_n\, \mathrm{TPHP}_n^{Y_n,Z_n}$, where $\mathrm{DPHP}_n^{Y_n} \equiv \exists Z_n\, \mathrm{TPHP}_n^{Y_n,Z_n}$ holds)

An exponential separation of Gqve* and Q-resolution

Proposition

Let $\varphi_n = \forall X_n \exists Y_n \forall Z_n \left(\mathrm{TPHP}_n^{Y_n, Z_n} \rightarrow \mathrm{DPHP}_n^{X_n}\right)$. *Then there exists a proof of* $\vdash \varphi_n$ *in* Gqve* *of size polynomial in n.*

Essentially prove $\mathrm{TPHP}_n^{C_n, Z_n} \rightarrow \mathrm{DPHP}_n^{C_n}$ which is easy!

An exponential separation of Gqve* and Q-resolution

Proposition

Let $\varphi_n = \forall X_n \exists Y_n \forall Z_n \left(\mathrm{TPHP}_n^{Y_n,Z_n} \rightarrow \mathrm{DPHP}_n^{X_n}\right)$*. Then any* Q-res *refutation of the negation of* φ_n*, i.e.,*

$$\exists X_n \forall Y_n \exists Z_n \left(\mathrm{TPHP}_n^{Y_n,Z_n} \wedge \mathrm{CPHP}_n^{X_n}\right)$$

has exponential size.

> Since $\mathrm{DPHP}_n^{Y_n}$ is valid and $\mathrm{DPHP}_n^{Y_n} \equiv \exists Z_n\, \mathrm{TPHP}_n^{Y_n,Z_n}$ holds, we have to refute $\mathrm{CPHP}_n^{X_n}$ which is hard!

Conclusion

- 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 ∃PR)

Let $A\colon C_1 \vee x \vee C_2$ and $B\colon C_3 \vee \neg x \vee C_4$ be two clauses, where the C_i are possibly empty subclauses and x is an $\exists$ variable. With

$$\frac{C_1 \vee x \vee C_2 \qquad\qquad C_3 \vee \neg x \vee C_4}{C_1 \vee C_2 \vee C_3 \vee C_4}\ \exists\mathrm{PR}$$

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

Definition (Propositional factoring rule PF)

Let $A\colon C_1 \vee \ell \vee C_2 \vee \ell \vee C_3$ be a clause with possibly empty subclauses C_1, C_2, C_3 and let ℓ be a literal. With

$$\frac{C_1 \vee \ell \vee C_2 \vee \ell \vee C_3}{C_1 \vee \ell \vee C_2 \vee C_3}\ \mathrm{PF}$$

we derive the factor $C_1 \vee \ell \vee C_2 \vee C_3$ of A.

The general idea of the exponential separation

- Introduce fresh variables $z_{i_1,i_2,j}$ for the disjuncts in $\mathrm{DPHP}_n^{X_n}$
- 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 $\bigvee_{1 \le i_1 < i_2 \le n+1} (x_{i_1,j} \wedge x_{i_2,j})$, 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 $\mathrm{DPHP}_n^{X_n}$
- $\mathrm{TPHP}_n^{Y_n,Z_n}$ is $D_n^{Z_n} \wedge P_n^{Y_n,Z_n} \wedge Q_n^{Y_n,Z_n}$ and its size is $O(n^3)$

The general idea of the exponential separation

$$\begin{aligned}
\mathrm{TPHP}_n^{Y_n,Z_n} &= D_n^{Z_n} \wedge P_n^{Y_n,Z_n} \wedge Q_n^{Y_n,Z_n} \\
D_n^{Z_n} &= \bigvee_{z \in Z_n} \neg z \\
P_n^{Y_n,Z_n} &= \bigwedge_{i=1}^{n+1} \bigwedge_{j=1}^{n} (z_{i,0,0} \vee \neg y_{i,j}) \\
Q_n^{Y_n,Z_n} &= \bigwedge_{j=1}^{n} \bigwedge_{1 \le i_1 < i_2 \le n+1} \big((z_{i_1,i_2,j} \vee y_{i_1,j}) \wedge (z_{i_1,i_2,j} \vee y_{i_2,j})\big)
\end{aligned}$$

$$\boxed{\varphi_n = \forall X_n \exists Y_n \forall Z_n \big(\mathrm{TPHP}_n^{Y_n,Z_n} \to \mathrm{DPHP}_n^{X_n}\big)}$$