Reasoning Engines for Rigorous System Engineering

Block 3: Quantified Boolean Formulas and DepQBF

2. Basic Deduction Concepts for Quantified Boolean Formulas

Uwe Egly Florian Lonsing

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

Outline

1. A resolution calculus for QBFs in PCNF
2. Long distance resolution
3. Gentzen/sequent systems for arbitrary QBFs

Why do we need a resolution calculus for QBFs?

- We need a QSAT solver in our rapid implementation approach. Why not Q-resolution (Q-res)?
- Although you will usually not see it, but in nearly every QDPLL solver, there is Q-res inside.
- Some QDPLL solvers deliver Q-res clause proofs ("refutations") as certificates for unsatisfiability.
- Some even deliver Q-res cube "proofs" as certificates for satisfiability.
- From such proofs, one can generate witness functions (as mentioned earlier).

A resolution calculus for QBFs: The definition of resolvents

Definition (propositional resolvent)

Given two clauses C_1 and C_2 and a pivot variable p with $p \in C_1$ and $\neg p \in C_2$, *resolution* produces the resolvent $C_r = (C_1 \setminus \{p\}) \cup (C_2 \setminus \{\neg p\})$.

Definition (Q-resolution with existential pivot variable)

- Let C_1, C_2 be non-tautological clauses where $v \in C_1, \neg v \in C_2$ for an $\exists$-variable v.
- Tentative Q-resolvent of C_1 and C_2:

$$C_1 \otimes C_2 := (UR(C_1) \cup UR(C_2)) \setminus \{v, \neg v\}.$$

- If $\{x, \neg x\} \subseteq C_1 \otimes C_2$ for some variable x, then no Q-resolvent exists.
- Otherwise, the non-tautological Q-resolvent is $C := C_1 \otimes C_2$.

A resolution calculus for QBFs: The quantification level

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 (QBF with 4 quantification levels and 3 quantifier alternations)

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

An ordering between variables is defined according to their occurrence in the quantifier prefix and extended to literals. For instance,

$$x_2 < y_4 \qquad \text{as well as} \qquad x_1 < \neg x_3.$$

A resolution calculus for QBFs: Universal reduction

Definition (universal reduction (UR))

Given a clause C, UR on C produces the clause

$$UR(C) := C \setminus \{\ell \in C \mid q(\ell) = \forall \text{ and } \forall \ell' \in C \text{ with } q(\ell') = \exists : \ell' < \ell\},$$

where $<$ is the linear variable ordering given by the quantifier prefix.

- Universal reduction deletes "trailing" universal literals from clauses.
- Clauses are shortened by UR.

Example

Given $\Phi := \forall y \exists x_1 \forall z \exists x_2 . (\underbrace{x_1 \vee z}_{C}) \wedge (\neg y \vee \neg x_1) \wedge (\neg y \vee x_2)$, we have

$UR(C) := x_1$.

A resolution calculus for QBFs

Definition (Q-resolution calculus)

The Q-resolution (Q-res) calculus consists of the Q-resolution rule and the universal reduction rule.

Remark

1. *Resolution operations are only allowed over existential literals.*
2. *Tautological resolvents are never generated.*

We will relax these requirements later on.

Soundness and completeness or Q-resolution

Theorem (Kleine Büning, Karpinski, Flögel, Inf. Comput., 1995)

A QBF in PCNF without tautological clauses is false iff there is a derivation of the empty clause $\Box$ (= a refutation) in the Q-resolution calculus.

Example

Let Φ be $\exists a \forall x \exists b \forall y \exists c \,.\, C_1 \wedge \cdots \wedge C_6$ with

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

A Q-resolution refutation of Φ

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{C_1 \quad C_2}{a \lor x \lor b \lor y}\,R
    }{a \lor x \lor b}\,UR
    \qquad
    \begin{matrix}(C_3)\\ x \lor \neg b\end{matrix}
  }{
    \dfrac{a \lor x}{a}\,UR
  }\,R
  \qquad
  \dfrac{
    \dfrac{
      \dfrac{\begin{matrix}(C_4)\\ \neg y \lor c\end{matrix} \quad \begin{matrix}(C_5)\\ \neg a \lor \neg x \lor b \lor \neg c\end{matrix}}{\neg a \lor \neg x \lor b \lor \neg y}\,R
    }{\neg a \lor \neg x \lor b}\,UR
    \qquad
    \begin{matrix}(C_6)\\ \neg x \lor \neg b\end{matrix}
  }{
    \dfrac{\neg a \lor \neg x}{\neg a}\,UR
  }\,R
}{\Box}\,R
$$

Example (again)

Let Φ be $\exists a \forall x \exists b \forall y \exists c\,.\,C_1 \land \cdots \land C_6$ with

C_1:	$a \lor b \lor y \lor c$	C_2:	$a \lor x \lor b \lor y \lor \neg c$
C_3:	$x \lor \neg b$	C_4:	$\neg y \lor c$
C_5:	$\neg a \lor \neg x \lor b \lor \neg c$	C_6:	$\neg x \lor \neg b$

A resolution calculus for QBFs (cont'd)

Is the following rule allowed/sound?

Definition (QU-resolution with universal pivot variable)

- Let C_1, C_2 be non-tautological clauses where $v \in C_1, \neg v \in C_2$ for an $\forall$-variable v.
- Tentative QU-resolvent of C_1 and C_2:
$$C_1 \otimes C_2 := (UR(C_1) \cup UR(C_2)) \setminus \{v, \neg v\}.$$
- If $\{x, \neg x\} \subseteq C_1 \otimes C_2$ for some variable x, then no QU-resolvent exists.
- Otherwise, the non-tautological QU-resolvent is $C := C_1 \otimes C_2$.

A resolution calculus for QBFs (cont'd)

Is the following rule allowed/sound?

Definition (QU-resolution with universal pivot variable)

- Let C_1, C_2 be non-tautological clauses where $v \in C_1, \neg v \in C_2$ for an $\forall$-variable v.
- Tentative QU-resolvent of C_1 and C_2:
$$C_1 \otimes C_2 := (UR(C_1) \cup UR(C_2)) \setminus \{v, \neg v\}.$$
- If $\{x, \neg x\} \subseteq C_1 \otimes C_2$ for some variable x, then no QU-resolvent exists.
- Otherwise, the non-tautological QU-resolvent is $C := C_1 \otimes C_2$.

YES. Q-resolution can be extended by this rule yielding QU-resolution!

A stronger resolution calculus for QBFs

Definition (QU-resolution calculus)

The Q-resolution (Q-res) calculus consists of the Q-resolution rule, the QU-resolution rule and the universal reduction rule.

- The QU-resolution calculus is a slight extension of the Q-resolution calculus, but . . .
- it has the potential to enable shorter proofs.

➥ We will demonstrate this in the following.

A hard class of formulas for Q-resolution

Definition (Class $(\Psi_k)_{k \geq 1}$ of unsatisfiable QBFs)

$$\Psi_{(k \geq 1)} := \exists d_1 \exists e_1 \forall x_1 \exists d_2 \exists e_2 \forall x_2 \cdots \exists d_k \exists e_k \forall x_k \exists f_1 \cdots \exists f_k .$$

$$(\overline{d_1} \vee \overline{e_1}) \quad \wedge \qquad (1)$$

$$(d_k \vee \overline{x_k} \vee \overline{f_1} \vee \cdots \vee \overline{f_k}) \quad \wedge \qquad (2)$$

$$(e_k \vee x_k \vee \overline{f_1} \vee \cdots \vee \overline{f_k}) \quad \wedge \qquad (3)$$

$$\bigwedge_{j=1}^{k-1} (d_j \vee \overline{x_j} \vee \overline{d_{j+1}} \vee \overline{e_{j+1}}) \quad \wedge \qquad (4)$$

$$\bigwedge_{j=1}^{k-1} (e_j \vee x_j \vee \overline{d_{j+1}} \vee \overline{e_{j+1}}) \quad \wedge \qquad (5)$$

$$\bigwedge_{j=1}^{k} (\overline{x_j} \vee f_j) \quad \wedge \qquad (6)$$

$$\bigwedge_{j=1}^{k} (x_j \vee f_j) \qquad (7)$$

A hard class of formulas for Q-resolution

Theorem (Kleine Büning, Karpinski, Flögel, Inf. Comput., 1995)

Any Q-resolution proof of Ψ_k *has at least* 2^k *resolution steps.*

Result is a bit surprising, because

- the existential part (in black) is Horn and
- propositional Horn clause sets have short (unit) resolution proofs.
- Short proofs are possible for Horn clause sets containing $\forall$ variables.

➥ Universal non-Horn part forces exponential proof length!

QU-resolution and the class $(\Psi_k)_{k \geq 1}$

- In general: QU-res allows to derive clauses which Q-res cannot derive.
- In particular for formula Ψ_k: QU-res allows to derive unit clauses.
- Key observation: unit clauses f_i $(1 \leq i \leq k)$ obtained by QU-resolution allow for short proofs of Ψ_k.

Proposition (Van Gelder 2012)

Every formula Ψ_k has a QU-resolution proof with $\mathcal{O}(k)$ resolution steps.

Short QU-res proofs for Ψ_k ($k \geq 1$)

Example (Ψ_2 in QDIMACS format)

```
c k=2
p cnf 8 9
e 1 2 0
a 3 0
e 4 5 0
a 6 0
e 7 8 0
-1 -2 0
1 -3 -4 -5 0
2  3 -4 -5 0
4 -6 -7 -8 0
5  6 -7 -8 0
 3 7 0
-3 7 0
 6 8 0
-6 8 0
```

- Derive new unit clauses from all the binary clauses by QU-resolution over universal variables. The result are two clauses f_1 and f_2 (7 0) and (8 0).
- Observe: the unit clauses resulting from the previous step cannot be derived by Q-res.
- We derive (4 0) and (5 0) by Q-resolutions and UR.
- Use the new unit clauses to successively shorten all the clauses of size four by unit resolution and universal reduction. Further unit clauses can be obtained this way.
- Finally the empty clause is derived using (−1 −2 0).
- This resolution strategy can be applied to Ψ_k for all k.

Outline

Motivation

Resolution so far:

- Resolvents with existential or universal pivot variables
- Q(U)-resolvents are non-tautological
  (i.e., clause which does not contain v and $\neg v$ for some variable v).

How do we continue?

- We extend the concept by allowing (certain) tautological resolvents
  - It was first used in the clause learning procedure of yquaffle (Zhang and Malik, 2002)
  - Recently it was formalized as a calculus (Balabanov and Jiang, 2012)
  - Implemented in the solver DepQBF (E., Lonsing, Widl 2013)
- We show that an exponential speed-up in proof length is possible.

Long distance Q-resolution: The basic idea

Definition

Two clauses C and D have distance $k \geq 1$ if there are literals $\ell_1, \ldots, \ell_k$ such that, for all $1 \leq i \leq k$, literal ℓ_i occurs in C and the dual of ℓ_i occurs in D. If there is no such literal then the clauses have distance 0.

- The usual resolution rules require two parent clauses of distance 1.
- Tentatively, we allow two parent clauses of distance ≥ 1, provided
  1. the pivot (say ℓ_1) is existential,
  2. all other literals $\ell_2, \ldots, \ell_k$ are universal, and
  3. $\ell_1 < \ell_i$ for all $i = 2, \ldots, k$ ("the pivot is minimal in $\ell_1, \ell_2, \ldots, \ell_k$").
- A more precise description follows later.

Long distance Q-resolution: Some examples

Φ: $\exists a \forall x \exists b \forall y \exists c.\ C_1 \wedge C_2 \wedge C_3 \wedge C_4$

$$\frac{a \vee x \vee \neg b \vee y \vee \neg c \qquad \neg a \vee \neg x \vee \neg b \vee \neg c}{x^* \vee \neg b \vee y \vee \neg c}\ R$$

- The two parent clauses have distance 2 (based on a and x).
- The pivot variable is a, $a < x$ and x^* is a shorthand for $x \vee \neg x$.

$$\frac{x^* \vee \neg b \vee \neg c \qquad b \vee \neg c}{x^* \vee \neg c}\ R$$

- The two parent clauses have distance 1 (based on b).
- The pivot variable is b and no level restriction is required here.

Long distance Q-resolution: Some examples (cont'd)

$\Phi: \quad \exists a \forall x \exists b \forall y \exists c.\ C_1 \wedge C_2 \wedge C_3 \wedge C_4$

$$\frac{a \vee x \vee \neg b \vee y \vee \neg c \qquad \neg a \vee \neg x \vee \neg b \vee \neg y \vee \neg c}{x^* \vee \neg b \vee y^* \vee \neg c}\ R$$

- The two parent clauses have distance 3 (based on a, x and y).
- The pivot variable is a and $a < x$ as well as $a < y$ holds.

$$\frac{a \vee x \vee \neg b \vee y \vee \neg c \qquad a \vee \neg x \vee b \vee \neg y \vee \neg c}{a \vee x^* \vee y^* \vee \neg c}\ R$$

- The two parent clauses have distance 3 (based on b, x and y).
- The pivot variable is b, $b < y$, but $b \not< x$ hold.
- This is a faulty application of long distance resolution!

Long distance Q-resolution: The restriction on the pivot

$\Phi: \quad \forall x \, \exists a. \, (\neg x \vee a) \wedge (x \vee \neg a)$

- Φ is true! Simply set a to the same value as x.
- Without the restriction on the pivot, we can derive the empty clause!

$$\dfrac{\dfrac{\neg x \vee a \qquad x \vee \neg a}{x^*} \; R?}{\Box} \; UR$$

- The two parent clauses of $R?$ have distance 2 (based on a and x).
- The pivot variable is a and $a \not< x$ holds.

➥ Ordering restrictions are important for correctness!

The long distance Q-resolution (LDQ) calculus for QBFs

Notations

- The $\exists$ variable p is the pivot element of the resolutions.
- The variable x is universal.
- x^* is a shorthand for $x \vee \neg x$. x^* is called the merged literal.
- X^l, X^r are sets of universal literals (merged or unmerged), such that
  - for each literal $m \in X^l$ (with variable x), it holds that if m is not a merged literal, then the dual of m is in X^r, and otherwise
  - either of $x \in X^r$, $\neg x \in X^r$, $x^* \in X^r$, and
  - X^r does not contain any additional literal.
- X^* contains the merged literals of each literal in X^l.

The long distance Q-resolution (LDQ) calculus for QBFs

Resolution rule R_1

$$\frac{C^l \vee p \qquad C^r \vee \neg p}{C^l \vee C^r} \; R_1$$

For all literals $m \in C^l$ it holds that the dual of m is not in C^r.

Resolution rule R_2

$$\frac{C^l \vee p \vee X^l \qquad C^r \vee \neg p \vee X^r}{C^l \vee C^r \vee X^*} \; [R_2]$$

For all literals $m \in X^r$ it holds that $p < m$, for all literals $m \in C^l$ it holds that the dual of m is not in C^r.

Universal reduction rule UR

$$\frac{C \vee x'}{C} \; [UR]$$

For $x' \in \{x, \neg x, x^*\}$ and for any $\exists$ variable $e \in C$ it holds that $e < x'$.

Symmetric rules are omitted!

Examples for R_2 with Φ: $\exists a \forall x \exists b \forall y \exists c.\ C_1 \wedge C_2 \wedge C_3 \wedge C_4$

$$\frac{a \vee x \vee \neg b \vee y \vee \neg c \qquad \neg a \vee \neg x \vee \neg b \vee \neg c}{x^* \vee \neg b \vee y \vee \neg c}\ R_2$$

- The two parent clauses have distance 2 (based on a and x).
- The pivot variable is a and $C^l = \{\neg b, y, \neg c\}$ and $C^r = \{\neg b, \neg c\}$.
- $a < x$, $X^l = \{x\}$, $X^r = \{\neg x\}$ and $X^* = \{x^*\}$.

$$\frac{x^* \vee \neg b \vee y \vee \neg c \qquad b \vee \neg y \vee \neg c}{x^* \vee y^* \vee \neg c}\ R_2$$

- The two parent clauses have distance 2 (based on b and y).
- The pivot variable is b and $C^l = \{x^*, \neg c\}$ and $C^r = \{\neg c\}$.
- $b < y$, $X^l = \{y\}$, $X^r = \{\neg y\}$ and $X^* = \{y^*\}$.
- Since x^* is not in X^l or X^r, $b < y$ is sufficient for correctness.

An LDQ-resolution proof of Φ

$\Phi: \quad \exists a \forall x \exists b \forall y \exists c.\ C_1 \wedge C_2 \wedge C_3 \wedge C_4$

$$\dfrac{\overset{(C_1)}{a \vee x \vee \neg b \vee y \vee \neg c} \qquad \overset{(C_2)}{\neg a \vee \neg x \vee \neg b \vee \neg c}}{x^* \vee \neg b \vee y \vee \neg c}\ R$$

$$\dfrac{x^* \vee \neg b \vee y \vee \neg c \qquad \overset{(C_3)}{b \vee \neg y \vee \neg c}}{x^* \vee y^* \vee \neg c}\ R$$

$$\dfrac{x^* \vee y^* \vee \neg c \qquad \overset{(C_4)}{c}}{x^* \vee y^*}\ R$$

$$\dfrac{x^* \vee y^*}{\Box}\ UR$$

Short LDQ-resolution proofs of Ψ_k

Definition (Class $(\Psi_k)_{k\geq 1}$ of unsatisfiable QBFs from Kleine Büning op. cit.)

$\Psi_{(k\geq 1)} := \exists d_1 \exists e_1 \forall x_1 \exists d_2 \exists e_2 \forall x_2 \cdots \exists d_k \exists e_k \forall x_k \exists f_1 \cdots \exists f_k.$

$$
\begin{array}{rcl}
(\overline{d_1} \vee \overline{e_1}) & \wedge & \\
(d_k \vee \overline{x_k} \vee \overline{f_1} \vee \cdots \vee \overline{f_k}) & \wedge & (e_k \vee x_k \vee \overline{f_1} \vee \cdots \vee \overline{f_k}) \quad \wedge \\
\bigwedge_{j=1}^{k-1} (d_j \vee \overline{x_j} \vee \overline{d_{j+1}} \vee \overline{e_{j+1}}) & \wedge & \bigwedge_{j=1}^{k-1} (e_j \vee x_j \vee \overline{d_{j+1}} \vee \overline{e_{j+1}}) \quad \wedge \\
\bigwedge_{j=1}^{k} (\overline{x_j} \vee f_j) & \wedge & \bigwedge_{j=1}^{k} (x_j \vee f_j)
\end{array}
$$

Theorem (E., Lonsing, Widl 2013)

There are LDQ- resolution proofs for Ψ_k with $O(k)$ clauses.

Short LDQ-resolution proofs for Ψ_k ($k \geq 1$)

Example (Ψ_2 in QDIMACS format)

```
c k=2
p cnf 8 9
e 1 2 0
a 3 0
e 4 5 0
a 6 0
e 7 8 0
-1 -2 0
1 -3 -4 -5 0
2  3 -4 -5 0
4 -6 -7 -8 0
5  6 -7 -8 0
 3 7 0
-3 7 0
 6 8 0
-6 8 0
```

- Derive (5 6 -7 0) from (5 6 -7 -8 0) and (6 8 0).
- Derive (4 -6 -7 0) from (4 -6 -7 -8 0) and (-6 8 0).
- Use both to derive (2 3 6^* -7 0) from (2 3 -4 -5 0). Observe that $4 < 6$ and $5 < 6$.
- Similarly, derive (1 -3 6^* -7 0).
- Derive (2 3 6^* 0) from (2 3 6^* -7 0) and (3 7 0).
- Derive (1 -3 6^* 0) from (1 -3 6^* -7 0) and (-3 7 0).
- Use (-1 -2 0) to derive (3^* 6^* 0). Observe that $1 < 3$, $1 < 6$, $2 < 3$ and $2 < 6$.
- Universal reduction applied to (3^* 6^* 0) results $\square$.
- This resolution strategy can be applied to Ψ_k for all k.

LDQ-resolution in DepQBF: Some experimental results

- Preprocessed benchmarks from QBF Evaluation 2012.
- DepQBF with traditional Q-resolution solves more benchmarks:

QBFEVAL'12-pre (276 formulas)	
DepQBF	120 (62 sat, 58 unsat)
DepQBF-LDQ	117 (62 sat, 55 unsat)

- LDQ-resolution (DepQBF-LDQ) results in shorter proofs:

115 solved by both:	DepQBF-LDQ	DepQBF
Avg. assignments	13.7×10^6	14.4×10^6
Avg. backtracks	43,676	50,116
Avg. resolutions	573,245	899,931
Avg. learn.clauses	31,939 (taut: 5,571)	36,854
Avg. run time	51.77	57.78

- Still missing: much more detailed experimental analysis.

Outline

Why yet another inference system?

- Sequent systems have been introduced by G. Gentzen in 1934/35.
- Theorem proving for "non-normal forms" are easily possible (not only for QBFs; also for propositional/FO/non-classical logic).
- Vast amount of proof-theoretical knowledge about them (like, e.g., cut elimination).
- Tableau systems (a variant of Gentzen systems) are often used in implementations.

Sequents

Sequent systems do not work on formulas, but on sequents.

Definition (Sequent)

A sequent S is an ordered pair of the form $\Gamma \vdash \Delta$, where Γ (antecedent) and Δ (succedent) are finite multisets of formulas. We write "$\vdash \Delta$" or "$\Gamma \vdash$" whenever Γ or Δ is the empty sequence, respectively.

Intuitively, a sequent states that

"if all formulas in Γ are true, then at least one formula in Δ is true."

An example for a (true) sequent is:

$$\Phi, \Psi_1 \vdash \Psi_2, \Phi$$

The propositional rules of a sequent calculus for QBFs

$$\frac{\Gamma \vdash \Delta}{\Phi, \Gamma \vdash \Delta}\ wl \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \Phi}\ wr$$

$$\frac{\Gamma_1, \Phi, \Phi, \Gamma_2 \vdash \Delta}{\Gamma_1, \Phi, \Gamma_2 \vdash \Delta}\ cl \qquad \frac{\Gamma \vdash \Delta_1, \Phi, \Phi, \Delta_2}{\Gamma \vdash \Delta_1, \Phi, \Delta_2}\ cr$$

$$\frac{\Gamma \vdash \Delta, \Phi}{\neg\Phi, \Gamma \vdash \Delta}\ \neg l \qquad \frac{\Phi, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg\Phi}\ \neg r$$

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

$$\frac{\Phi, \Gamma \vdash \Delta \qquad \Psi, \Gamma \vdash \Delta}{\Phi \vee \Psi, \Gamma \vdash \Delta}\ \vee l \qquad \frac{\Gamma \vdash \Delta, \Phi, \Psi}{\Gamma \vdash \Delta, \Phi \vee \Psi}\ \vee r$$

$$\frac{\Gamma \vdash \Delta, \Phi \qquad \Psi, \Gamma \vdash \Delta}{\Phi \rightarrow \Psi, \Gamma \vdash \Delta}\ \rightarrow l \qquad \frac{\Phi, \Gamma \vdash \Delta, \Psi}{\Gamma \vdash \Delta, \Phi \rightarrow \Psi}\ \rightarrow r$$

Example: A sequent proof for $\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)$

$$\frac{}{\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)}$$

Example: A sequent proof for $\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)$

$$\dfrac{\overline{\neg(a \vee b) \vdash \neg a \wedge \neg b}}{\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)} \rightarrow r$$

Example: A sequent proof for $\vdash (\neg(a \lor b)) \to (\neg a \land \neg b)$

$$\dfrac{\dfrac{\overline{\vdash a \lor b,\ \neg a \land \neg b}}{\neg(a \lor b) \vdash \neg a \land \neg b}\ \neg l}{\vdash (\neg(a \lor b)) \to (\neg a \land \neg b)}\ \to r$$

Example: A sequent proof for $\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash a,\ b,\ \neg a \wedge \neg b}}{\vdash a \vee b,\ \neg a \wedge \neg b}\ \vee r}{\neg(a \vee b) \vdash \neg a \wedge \neg b}\ \neg l}{\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)}\ \rightarrow r$$

Example: A sequent proof for $\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\overline{\vdash a,\ b,\ \neg a} \qquad \overline{\vdash a,\ b,\ \neg b}}{\vdash a,\ b,\ \neg a \wedge \neg b}\ \wedge r}{\vdash a \vee b,\ \neg a \wedge \neg b}\ \vee r}{\neg(a \vee b) \vdash \neg a \wedge \neg b}\ \neg l}{\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)}\ \rightarrow r
$$

Example: A sequent proof for $\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{a \vdash a,\ b}}{\vdash a,\ b,\ \neg a}\ \neg r \qquad \overline{\vdash a,\ b,\ \neg b}}{\vdash a,\ b,\ \neg a \wedge \neg b}\ \wedge r}{\vdash a \vee b,\ \neg a \wedge \neg b}\ \vee r}{\neg(a \vee b) \vdash \neg a \wedge \neg b}\ \neg l}{\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)}\ \rightarrow r
$$

Example: A sequent proof for $\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)$

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{a \vdash a}{a \vdash a,\ b}\ wr
      }{\vdash a,\ b,\ \neg a}\ \neg r
      \qquad
      \dfrac{}{\vdash a,\ b,\ \neg b}
    }{\vdash a,\ b,\ \neg a \wedge \neg b}\ \wedge r
  }{
    \dfrac{\vdash a \vee b,\ \neg a \wedge \neg b}{\neg(a \vee b) \vdash \neg a \wedge \neg b}\ \neg l
  }\ \vee r
}{\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)}\ \rightarrow r
$$

Example: A sequent proof for $\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)$

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{a \vdash a}{a \vdash a,\ b}\ wr
      }{\vdash a,\ b,\ \neg a}\ \neg r
      \qquad
      \dfrac{
        \dfrac{}{b \vdash a,\ b}
      }{\vdash a,\ b,\ \neg b}\ \neg r
    }{\vdash a,\ b,\ \neg a \wedge \neg b}\ \wedge r
  }{
    \dfrac{\vdash a \vee b,\ \neg a \wedge \neg b}{\neg(a \vee b) \vdash \neg a \wedge \neg b}\ \neg l
  }\ \vee r
}{\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)}\ \rightarrow r
$$

Example: A sequent proof for $\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)$

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{a \vdash a}{a \vdash a,\ b}\ wr
      }{\vdash a,\ b,\ \neg a}\ \neg r
      \qquad
      \dfrac{
        \dfrac{b \vdash b}{b \vdash a,\ b}\ wr
      }{\vdash a,\ b,\ \neg b}\ \neg r
    }{\vdash a,\ b,\ \neg a \wedge \neg b}\ \wedge r
  }{
    \dfrac{\vdash a \vee b,\ \neg a \wedge \neg b}{\neg(a \vee b) \vdash \neg a \wedge \neg b}\ \neg l
  }\ \vee r
}{\vdash (\neg(a \vee b)) \rightarrow (\neg a \wedge \neg b)}\ \rightarrow r
$$

The backward proof development stops at axioms $a \vdash a$ and $b \vdash b$.

The axioms and possible quantifier rules

The axioms: $\Phi \vdash \Phi$ Ax $\quad \bot \vdash \quad \bot l \quad \vdash \top \quad \top r$

Some possible quantifier rules:

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

$$\frac{\Psi\{p/\varphi\}, \Gamma \vdash \Delta}{\forall p\, \Psi, \Gamma \vdash \Delta}\ \forall l_f \qquad \frac{\Gamma \vdash \Delta, \Psi\{p/\varphi\}}{\Gamma \vdash \Delta, \exists p\, \Psi}\ \exists r_f$$

$$\frac{\Psi\{p/\top\}, \Psi\{p/\bot\}, \Gamma \vdash \Delta}{\forall p\, \Psi, \Gamma \vdash \Delta}\ \forall l_s \qquad \frac{\Gamma \vdash \Delta, \Psi\{p/\top\}, \Psi\{p/\bot\}}{\Gamma \vdash \Delta, \exists p\, \Psi}\ \exists r_s$$

$$\frac{\Gamma \vdash \Delta, \Psi\{p/\top\} \wedge \Psi\{p/\bot\}}{\Gamma \vdash \Delta, \forall p\, \Psi}\ \forall r_s \qquad \frac{\Psi\{p/\top\} \vee \Psi\{p/\bot\}, \Gamma \vdash \Delta}{\exists p\, \Psi, \Gamma \vdash \Delta}\ \exists l_s$$

q does not occur as a free variable in the conclusion of $\forall r_e$ / $\exists l_e$.
φ is a propositional formula.

Sequent calculi for QBFs

Take the rules for propositional logic and add quantifier rules.

- $\forall r_e$, $\exists l_e$, $\forall l_f$ and $\exists r_f$: Gqfe (Gqfe*) is the (tree) calculus
- $\forall r_e$, $\exists l_e$, $\forall l_v$ and $\exists r_v$: Restrict φ in $\forall l_f$, $\exists r_f$ to a variable and $\bot, \top$
  Gqve (Gqve*) is the (tree) calculus
- $\forall r_e$, $\exists l_e$, $\forall l_s$ and $\exists r_s$: Gqse (Gqse*) is the (tree) calculus

All these calculi are cut-free, i.e., they do not have the following rule:

$$\frac{\Gamma_1 \vdash \Delta_1, \Psi \qquad \Psi, \Gamma_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ cut$$

Ψ is the cut formula. The cut is propositional if the cut formula is.

Sequent calculi for QBFs: Some simulation result

Proposition (E. 2012)

1. Gqse *with propositional cut cannot p-simulate* Gqve*.
2. Gqve *with propositional cut cannot p-simulate* Gqfe*.
3. *Q-resolution (with proofs in dag form) cannot p-simulate* Gqve*.

The basic proof search algorithm for QBFs in NNF

- Based on DPLL (successful in SAT-/QBF-solving in (P)CNF)
- Relatively simple extension for nonprenex QBFs in NNF (implementation follows the semantics using *s* quantifier rules)

```
BOOLEAN split(QBF Φ in NNF) {

switch (simplify (Φ)):  /* simplify works inside ϕ */

   case ⊤:  return True;
   case ⊥:  return False;
   case (Φ1 ∨ Φ2):  return (split(Φ1) || split(Φ2));
   case (Φ1 ∧ Φ2):  return (split(Φ1) && split(Φ2));

   case (QX Ψ):  select x ∈ X;
      if Q = ∃ return (split(∃X Ψ[x/⊥]) || split(∃X Ψ[x/⊤]));
      if Q = ∀ return (split(∀X Ψ[x/⊥]) && split(∀X Ψ[x/⊤]));
}
```

Simplifying formulas

simplify(Φ): returns Φ' simplified wrt some equivalences:

(a) $\neg\top \Rightarrow \bot$; $\neg\bot \Rightarrow \top$;

(b) $\top \wedge \Phi \Rightarrow \Phi$; $\bot \wedge \Phi \Rightarrow \bot$; $\top \vee \Phi \Rightarrow \top$; $\bot \vee \Phi \Rightarrow \Phi$;

(c) $(Qx\,\Phi) \Rightarrow \Phi$, if $Q \in \{\forall, \exists\}$, and x does not occur in Φ;

(d) $\forall x\,(\Phi \wedge \Psi) \Rightarrow (\forall x\,\Phi) \wedge (\forall x\,\Psi)$;

(e) $\forall x\,(\Phi \vee \Psi) \Rightarrow (\forall x\,\Phi) \vee \Psi$, whenever x does not occur in Ψ;

(f) $\exists x\,(\Phi \vee \Psi) \Rightarrow (\exists x\,\Phi) \vee (\exists x\,\Psi)$;

(g) $\exists x\,(\Phi \wedge \Psi) \Rightarrow (\exists x\,\Phi) \wedge \Psi$, whenever x does not occur in Ψ.

Rewritings (d)–(g) are known as miniscoping.

Additional mechanisms

- Basic procedure clearly not sufficient for competitive solver
- Desirable extension: generalization of pruning techniques
  - Unit literal elimination
  - Pure literal elimination
  - Dependency-directed backtracking
    (works for true and false subproblems)
  - Learning

➥ `split` looks like an implementation of a sequent calculus

➥ Extensions of `split` formalized as a sequent calculus (for NNF)

➥ Such a formalization is the basis of Martina Seidl's solver `qpro`.

Conclusion (for the second part)

- We have seen different resolution concepts for QBFs in PCNF ...
- as well as sequent systems for arbitrary QBFs.
- We classified calculi wrt their ability to allow for succinct proofs.

➥ What is next:

Learn how most of the deduction concepts can be used inside QBF solvers.