Consistency and cut elimination: two ways to restrict Resolution

Gilles Dowek

A proof search method

Polarized resolution modulo

A restriction of Resolution

That is complete under some conditions

Why restricting Resolution?

A, $A \Rightarrow B$, $B \Rightarrow C$, $C \Rightarrow D$, $D \Rightarrow E$, E?

A, $\neg A \vee B$, $\neg B \vee C$, $\neg C \vee D$, $\neg D \vee E$, $\neg E$

Many ways to derive the empty clause $\perp$.

Resolution with set of support, Ordered resolution, ...

I. From Resolution to Equational resolution

An example

Assume $+$ associative, $P((a+b)+c)+(d+e)$

Try to prove $P(a+(b+(c+d)+e))$

Many ways to use the associativity axiom

Instead: orient associativity $x+(y+z) \longrightarrow (x+y)+z$ and normalize

$P((((a+b)+c)+d)+e)$

$P((((a+b)+c)+d)+e)$

Another example

Assume $P((a+b)+c)$ try to prove $\exists z\, P(a+z)$

$$(X+Y)+Z = X+(Y+Z)$$

$$\neg X = Y \vee \neg P(X) \vee P(Y)$$

$$P((a+b)+c)$$

$$\neg P(a+Z)$$

Another example

Assume $P((a+b)+c)$ try to prove $\exists z\ P(a+z)$

$$P((a+b)+c)$$

$$\neg P(a+Z)$$

Replace unification by equational unification modulo associativity

Deduction modulo

Proving soundness and completeness

$\Gamma, \text{Assoc} \vdash C$ iff $cl(\Gamma, \neg C) \rightsquigarrow_{\text{Assoc}} \perp$

Deduction modulo

Proving soundness and completeness

$$\Gamma, \text{Assoc} \vdash C \quad \text{iff} \quad \Gamma \vdash_{\text{Assoc}} C \quad \text{iff} \quad cl(\Gamma, \neg C) \rightsquigarrow_{\text{Assoc}} \perp$$

$\vdash_{\text{Assoc}}$?

$$\dfrac{\overline{P((a+b)+c) \vdash_{\text{Assoc}} P(a+(b+c))}\ \text{axiom}}{P((a+b)+c) \vdash_{\text{Assoc}} \exists x\, P(a+x)}\ \exists\text{-right}$$

Completeness

The completeness of Resolution:

(1) If the sequent $\Gamma \vdash C$ has a proof then it has a cut free proof

(2) If the sequent $\Gamma \vdash C$ has a cut free proof then
$cl(\Gamma, \neg C) \rightsquigarrow \bot$ (simple induction)

Both lemmas generalize to Deduction modulo associativity

II. From Equational resolution to Resolution modulo

Rewrite rules

Rewrite rules on terms

$$x + (y + z) \longrightarrow (x + y) + z$$

Or

$$0 + y \longrightarrow y$$

$$S(x) + y \longrightarrow S(x + y)$$

$X + 2 = 4$

More rewrite rules

What about the rewrite rule

$$x \subseteq y \longrightarrow \forall z \left(z \in x \Rightarrow z \in y\right)$$

?

PA, HOL, Z

Resolution modulo (2003)

Term rewrite rules used by the (equational) unification algorithm

But proposition rewrite rules used to directly rewrite (narrow) clauses

Resolution modulo

$$P \longrightarrow (Q \Rightarrow R)$$

P

Q

$\neg R$

Besides the Resolution rule, another rule:

from P derive $Q \Rightarrow R$

Dynamic clausification

But $Q \Rightarrow R$ not a clause: put it in clause form

P

Q

$\neg R$

$\neg Q \vee R$

R

$\perp$

Dynamic clausification

In general: skolemization

$$P(x) \longrightarrow \exists y\, Q(x, y)$$

from $P(X)$ derive $Q(X, f(X))$

Terrible to prove complete, horrible to implement

III. From Resolution modulo to Polarized resolution modulo

Transforming rewrite rules

Why not transform the rule into

$$P \longrightarrow (\neg Q \vee R)$$

?

Because P can also occur negatively in a clause

e.g. $\neg P \vee S$ rewrites to $\neg(Q \Rightarrow R) \vee S$

i.e. $Q \vee S$, $\neg R \vee S$

To transform the rewrite rules

polarize them

$$P \longrightarrow_{-} (\neg Q \vee R)$$

$$P \longrightarrow_{+} \neg Q$$

$$P \longrightarrow_{+} \neg\neg R$$

so that a clause always rewrites to a clause

IV. A restriction of (equational) Resolution?

One-way clauses

$$P \longrightarrow_{-} (\neg Q \vee R)$$

Transforms the clause $P \vee S$ into $\neg Q \vee R \vee S$

What is the difference with the clause $\neg P \vee \neg Q \vee R$?

$$\underline{\neg P} \vee \neg Q \vee R$$

Social rules

Resolution between two one-way clauses is prohibited

Resolution between an ordinary clause and a one-way clause is permitted only if the resolved literal is the selected one

A restriction of (equational) Resolution

A rewrite rule $P \longrightarrow_{\_} (\neg Q \vee R)$

A one-way clause $\underline{\neg P} \vee \neg Q \vee R$

An axiom $P \Rightarrow (\neg Q \vee R)$

A clause $\neg P \vee \neg Q \vee R$

More restricted than Resolution with set of support

In Resolution with set of support

Resolution between two theory clauses is prohibited

Resolution between an ordinary clause and a theory clause is always permitted

Restrictions of Resolution

Restrictions $\longrightarrow$ efficiency

Two choices: the clauses, the literals in the clauses

Two types of restrictions: clause restrictions (Set of support, Semantic resolution, ...),

literal restrictions (Ordered resolution, ...)

Here: mixing both both types

Completeness

The completeness of Resolution:

(1) If the sequent $\Gamma \vdash C$ has a proof then it has a cut free proof

(2) If the sequent $\Gamma \vdash C$ has a cut free proof then
$cl(\Gamma, \neg C) \leadsto \perp$ (simple induction)

Completeness

(2) If $\Gamma \vdash C$ has a cut free proof then $cl(\Gamma, \neg C) \leadsto \bot$

Generalizes to Deduction modulo and still a simple induction

But (1) not all $\mathcal{R}$ enjoy cut elimination in Deduction modulo

Polarized resolution modulo $\mathcal{R}$ complete if (and only if following Hermant) Deduction modulo $\mathcal{R}$ has the cut elimination property

Lessons learned from the completeness theorem

When can we replace the clause $\neg P \vee \neg Q \vee R$

by the one-way clause $\underline{\neg P} \vee \neg Q \vee R$?

When Deduction modulo the rule

$$P \longrightarrow_{-} \neg Q \vee R$$

has the cut elimination property

More generally

When can we replace a set of clauses by one-way clauses?

When Deduction modulo the associated rewrite system has the cut elimination property

Notice the parallel: When can we replace a set of clauses by theory clauses?

When this set is consistent

Concluding remarks

New connections between proof search methods and proof theory

(1) set of support: only consistency, here: cut elimination

(2) unlike other restrictions, Polarized resolution modulo not an instance of Ordered resolution (Gödel's theorem, with Burel)

Promising implementation (Burel)

Part of a trend in proof theory (and automated theorem proving): focus on theories (from a theory of proofs to a theory of theories)