Light Polarized Translations in Deduction Modulo

Olivier Hermant

ISEP

May 11, 2012

Deduction modulo [Dowek, Hardin & Kirchner]

Original idea: *combine automated theorem proving with rewriting*

Generalized to: *combine any first-order deduction process with rewriting*

Deduction modulo [Dowek, Hardin & Kirchner]

Original idea: *combine automated theorem proving with rewriting*

Generalized to: *combine any first-order deduction process with rewriting*

Example: Classical Sequent Calculus Modulo

- first-order logic: function and predicate symbols, logical connectors $\wedge, \vee, \Rightarrow$, quantifiers $\forall, \exists$ and constants $\top, \bot$

$$\text{LK} \quad + \quad \frac{\Gamma \vdash A, \Delta}{\Gamma \vdash B, \Delta}\ \textsc{Conv-R} \quad + \quad \frac{\Gamma, A \vdash \Delta}{\Gamma, B \vdash \Delta}\ \textsc{Conv-L}$$

- where Conv rules are applicable whenever $A \equiv B$, the congruence generated by rewriting.

Generating the congruence

Proposition Rewrite System

$P \longrightarrow A$ where P is an atomic formula, A is a formula and the free variables of A are contained in P.

A proposition rewrite system $\mathcal{R}$ is a collection of such rewrite rules.

One-step Rewriting formulæ

A formula B rewrites in one step to C, noted $B \longrightarrow C$ if:

- there is a rewrite rule $P \longrightarrow A \in \mathcal{R}$, a substitution σ, $B = P\sigma$ and $C = A\sigma$.
- $B = B_1 \square B_2$, $\square$ is one of the connectives $\vee, \wedge, \Rightarrow$ and: $B_1 \longrightarrow B_1'$ and $C = B_1' \square B_2$; or $B_2 \longrightarrow B_2'$ and $C = B_1 \square B_2'$.
- etc ...

Generating the congruence

Rewriting formulæ

A formula A rewrites in one step to B, noted $A \longrightarrow^* B$ if:

- A is B
- $A \longrightarrow^* A'$ and $A' \longrightarrow B$

Congruence

Two formula A and B are congruent, noted $A \equiv B$ iff:

- $A \longrightarrow^* B$ or $B \longrightarrow^* A$
- there exists A' such that $A \equiv A'$ and: $A' \longrightarrow^* B$ or $B \longrightarrow^* A'$.

Deduction System I: classical sequent calculus

$$\frac{}{\Gamma, A \vdash A, \Delta}\text{ axiom} \qquad \frac{\Gamma_1 \vdash A, \Delta_1 \qquad \Gamma_2, A \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\text{ cut}$$

$$\frac{\Gamma_1 \vdash A, \Delta_1 \qquad \Gamma_2 \vdash B, \Delta_2}{\Gamma_1, \Gamma_2 \vdash A \wedge B, \Delta_1, \Delta_2}\ \wedge\text{-r} \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ \wedge\text{-l}$$

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \Rightarrow B, \Delta}\ \Rightarrow\text{-r} \qquad \frac{\Gamma_1, B \vdash \Delta_1 \qquad \Gamma_2 \vdash A, \Delta_2}{\Gamma_1, \Gamma_2, A \Rightarrow B \vdash \Delta_1, \Delta_2}\ \Rightarrow\text{-l}$$

$$\frac{\Gamma \vdash A[x], \Delta}{\Gamma \vdash \forall x A[x], \Delta}\ \forall\text{-r, } x \text{ fresh} \qquad \frac{\Gamma, A[t] \vdash \Delta}{\Gamma, \forall x A[x] \vdash \Delta}\ \forall\text{-l, any } t$$

Deduction System I: classical sequent calculus

$$\frac{}{\Gamma, A \vdash B, \Delta} \text{ axiom, } A \equiv B \qquad \frac{\Gamma_1 \vdash A, \Delta_1 \qquad \Gamma_2, B \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} \text{ cut, } A \equiv B$$

$$\frac{\Gamma_1 \vdash A, \Delta_1 \qquad \Gamma_2 \vdash B, \Delta_2}{\Gamma_1, \Gamma_2 \vdash C, \Delta_1, \Delta_2} \wedge\text{-r, } C \equiv A \wedge B \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, C \vdash \Delta} \wedge\text{-l, } C \equiv A \wedge B$$

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash C, \Delta} \Rightarrow\text{-r, } C \equiv A \Rightarrow B \qquad \frac{\Gamma_1, B \vdash \Delta_1 \qquad \Gamma_2 \vdash A, \Delta_2}{\Gamma_1, \Gamma_2, C \vdash \Delta_1, \Delta_2} \Rightarrow\text{-l, } C \equiv A \Rightarrow B$$

$$\frac{\Gamma \vdash A[x], \Delta}{\Gamma \vdash C, \Delta} \forall\text{-r, } x \text{ fresh, } C \equiv \forall x A[x] \qquad \frac{\Gamma, A[t] \vdash \Delta}{\Gamma, C \vdash \Delta} \forall\text{-l, any } t\text{, } C \equiv \forall x A[x]$$

Deduction System II: intuitionistic natural deduction

$$\frac{}{\Gamma, A \vdash A}\text{axiom}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\wedge\text{-i} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\wedge\text{-e1} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\wedge\text{-e2}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\Rightarrow\text{-i} \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\Rightarrow\text{-e}$$

$$\frac{\Gamma \vdash A[x]}{\Gamma \vdash \forall x A[x]}\forall\text{-i}, x \text{ free} \qquad \frac{\Gamma \vdash \forall x A[x]}{\Gamma \vdash A[t]}\forall\text{-e, any } t$$

Rewriting relation

- on terms:

$$\begin{array}{rcl} x + 0 & \longrightarrow & x \\ x + S(y) & \longrightarrow & S(x + y) \end{array}$$

- on atomic formulæ:

$$\begin{array}{rcl} Null(0) & \longrightarrow & \top \\ Null(S(x)) & \longrightarrow & \bot \\ A & \longrightarrow & A \Rightarrow A \end{array}$$

(the last one is very bad)

Examples of theories expressed in Deduction Modulo

- arithmetic
- Zermelo's set theory
- a subset of B set theory
- simple type theory (HOL)

What about cut-elimination ?

$$\begin{cases} \vdash \text{even}(0) \\ \text{even}(n) \vdash \text{even}(n+2) \end{cases}$$

$$\text{Cut}\ \dfrac{\dfrac{}{\vdash \text{even}(0)} \quad \dfrac{}{\text{even}(0) \vdash \text{even}(2)}}{\vdash \text{even}(2)}$$

- axiomatic cuts

What about cut-elimination ?

$$\begin{cases} x + 0 & \rightarrow & x \\ x + s(y) & \rightarrow & s(x + y) \\ \\ \text{even}(0) & \rightarrow & \top \\ \text{even}(x + 2) & \rightarrow & \text{even}(x) \end{cases}$$

$$\dfrac{\overline{\vdash \top}}{\vdash \text{even}(2)}\ \textsc{Conv-r}$$

or even:

$$\dfrac{\overline{\vdash \top}}{\vdash \text{even}(4)}\ \textsc{Conv-r}$$

$$\vdots$$

Cut-elimination implies consistency…
and we must pay the prize

Consistency $\Leftarrow$ / $\not\Rightarrow$ Cut elimination $\Leftarrow$ / $\not\Rightarrow$ Normalization

- minimal counterexample : $A \rightarrow A \Rightarrow B$
- convergent counterexample : $\begin{cases} R \in R & \rightarrow \forall y. y \simeq R \Rightarrow y \in R \Rightarrow B \\ y \simeq z & \rightarrow \forall y. (x \in y \Rightarrow z \in y) \end{cases}$

- minimal counterexample : $A \rightarrow A \Rightarrow A$
- convergent counterexample : $\begin{cases} R \in R & \rightarrow \forall y. y \simeq R \Rightarrow y \in R \Rightarrow A \Rightarrow A \\ y \simeq z & \rightarrow \forall y. (x \in y \Rightarrow z \in y) \end{cases}$

Polarized Deduction Modulo

Positive and Negative Occurrences

A occurs positively (resp. negatively) in a formula C if C is:

- A (resp. no valid condition)
- $C_1 \square C_2$, $\square$ is $\vee, \wedge$ and A occurs positively (resp. negatively) in C_1 or C_2
- $C_1 \Rightarrow C_2$, and A occurs positively (resp. negatively) in C_2 or negatively (resp. positively) in C_1
- $\neg C_1$ and A occurs negatively (resp. positively) in C_1.
- etc ...

Polarized Rewrite System

We split the rewrite system $\mathcal{R}$ into two sets $\mathcal{R}^+$ and $\mathcal{R}^-$:

$$\begin{array}{ccc} P_1 & \longrightarrow_+ & A_1 \\ P_2 & \longrightarrow_- & A_2 \\ & \vdots & \end{array}$$

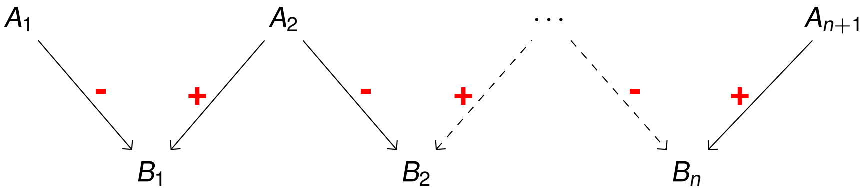
One-step positive rewriting

A formula B rewrites in one step positively to C (written $B \longrightarrow^+ C$) if:

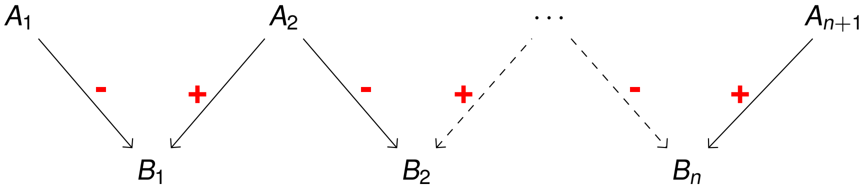
- it rewrites in in one step to C,
- we use a positive rewrite rule $P_1 \longrightarrow_+ A_1$ (resp. negative rewrite rule $P_2 \longrightarrow_+ A_2$),
- and the rewritten instance of P_1 occurs positively (resp. negatively) in B

Define as well $B \longrightarrow_- C$, $B \longrightarrow_-^* C$ and $B \longrightarrow_+^* C$.

Note on $\equiv$



Note on $\equiv$



This defines a form of congruence:

Negative and positive congruence

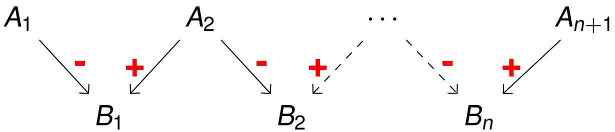
$A \equiv_- B$ iff:

- A is B; or
- $A \equiv_- C$, and $B \longrightarrow^+ C$ or $C \longrightarrow^- B$; or
- $C \equiv_- B$, and $C \longrightarrow^+ A$ or $A \longrightarrow^- C$.

$A \equiv_+ B$ is defined the same way, or directly as: $B \equiv_- A$.

Transitive, reflexive but not symmetric !

Note on $\equiv$



This definition (and the picture) accounts for:

$$\dfrac{\dfrac{}{A_1 \vdash B_1}\; A_1 \longrightarrow_- B_{1+} \longleftarrow B_1 \qquad \dfrac{\vdots}{A_2 \vdash A_{n+1}}}{A_1 \vdash A_{n+1}}\ \text{cut},\ A_{2-} \longleftarrow A_2 \longrightarrow_+ B_1$$

Or, less symmetrically, to:

$$\dfrac{\dfrac{}{A_1 \vdash B_1}\; A_1 \longrightarrow_- B_{1+} \longleftarrow B_1 \qquad \dfrac{\dfrac{}{B_2 \vdash A_3}\; B_2 \longrightarrow_- B_{2+} \longleftarrow A_3 \qquad \dfrac{\vdots \qquad \dfrac{\vdots}{B_4 \vdash A_{n+1}}}{B_3 \vdash A_{n+1}}}{B_2 \vdash A_{n+1}}\ \text{cut},\ A_{3-} \longleftarrow A_3 \longrightarrow_- B_3}{A_1 \vdash A_{n+1}}\ \text{cut},\ B_{1+} \longleftarrow A_{2-} \longrightarrow B_2$$

Confluence as a cut elimination property [Dowek]

Polarized Sequent Calculus Modulo

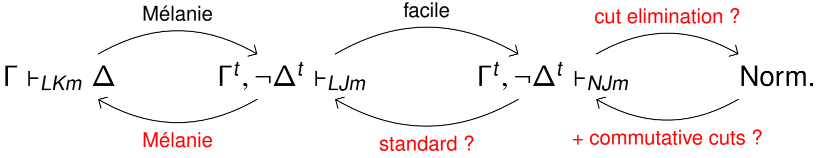
$$\frac{}{\Gamma, A \vdash B, \Delta} \text{ axiom, } A \rightarrow^*_- C^*_- \leftarrow B \qquad \frac{\Gamma_1 \vdash A, \Delta_1 \qquad \Gamma_2, B \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} \text{ cut, } A^*_+ \leftarrow C \rightarrow^*_- B$$

$$\frac{\Gamma_1 \vdash A, \Delta_1 \qquad \Gamma_2 \vdash B, \Delta_2}{\Gamma_1, \Gamma_2 \vdash C, \Delta_1, \Delta_2} \wedge\text{-r, } C \rightarrow^*_+ A \wedge B \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, C \vdash \Delta} \wedge\text{-l, } C \rightarrow^*_- A \wedge B$$

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash C, \Delta} \Rightarrow\text{-r, } C \rightarrow^*_+ A \Rightarrow B \qquad \frac{\Gamma_1, B \vdash \Delta_1 \qquad \Gamma_2 \vdash A, \Delta_2}{\Gamma_1, \Gamma_2, C \vdash \Delta_1, \Delta_2} \Rightarrow\text{-l, } C \rightarrow^*_- A \Rightarrow B$$

$$\frac{\Gamma \vdash A[x], \Delta}{\Gamma \vdash C, \Delta} \forall\text{-r, } x \text{ fresh, } C \rightarrow^*_+ \forall x A[x] \qquad \frac{\Gamma, A[t] \vdash \Delta}{\Gamma, C \vdash \Delta} \forall\text{-l, any } t,\ C \rightarrow^*_- \forall x A[x]$$

Eliminating cuts



The translation way through normalization.

polarize-translating the rewrite rules

Translation of a rewrite system $\mathcal{R}^{\odot}$

$$P_1 \longrightarrow_+ A_1 \quad \hookrightarrow \quad P_1 \longrightarrow_+ A_1^n$$
$$P_2 \longrightarrow_- A_2 \quad \hookrightarrow \quad P_2 \longrightarrow_- A_2^p$$

Results

if $\Gamma \vdash \Delta$ in $LK_{\equiv}$ modulo $\mathcal{R}$, then $\Gamma^g, \neg\Delta^d \vdash$ in $LJ_{\equiv}$ modulo $\mathcal{R}^{\odot}$

Proof. Mélanie's work (extension).

If $\Gamma \vdash A$ in polarized $LJ_{\equiv}$ modulo $\mathcal{R}$ then $\Gamma \vdash A$ in polarized Natural Deduction modulo $\mathcal{R}$

If $\Gamma \vdash A$ in polarized Natural Deduction modulo $\mathcal{R}$ with a proof free of cuts and of commutative cuts, then $\Gamma \vdash A$ in polarized $LJ_{\equiv}$ modulo $\mathcal{R}$ with a cut-free proof.

If $\Gamma^g, \neg\Delta^d \vdash$ in polarized $LJ_{\equiv}$ modulo $\mathcal{R}^{\odot}$ without cut, then $\Gamma \vdash \Delta$ in polarized $LK_{\equiv}$ modulo $\mathcal{R}$ without cut.

Proof. Mélanie's work (extension).

Further work

- achieve the plan
- is there a SC criterion for polarized DM ?