Focused proof systems for Classical Logics

Dale Miller

INRIA-Saclay & LIX, École Polytechnique
Palaiseau, France

Bertinoro, 11-15 April 2011

Lecture 5: Normal forms for classical logic proofs
Main reference: Liang & M. Focusing and polarization in linear, intuitionistic, and classical logics. TCS, 2009.

LKF: Focusing for Classical Logic

Classical logic is polarized as follow:

1. $B \supset C$ is replaced with $\neg B \vee C$,
2. negations are pushed to the atoms,
3. atoms are assigned bias (either $+$ or $-$), and
4. $\wedge$ $\vee$, $\top$, and $\bot$ are annotated with either $+$ or $-$.

LKF is a focused, one-sided sequent calculus with the sequents

$$\vdash \Theta \Uparrow \Gamma \qquad \text{and} \qquad \vdash \Theta \Downarrow B$$

Here, Θ is a multiset of positive formulas and negative literals, Γ is a multiset of formulas, and B is a formula.

LKF : focused proof systems for classical logic

$$\frac{}{\vdash \Theta \Uparrow \Gamma, t^-} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A \qquad \vdash \Theta \Uparrow \Gamma, B}{\vdash \Theta \Uparrow \Gamma, A \wedge^- B}$$

$$\frac{\vdash \Theta \Uparrow \Gamma}{\vdash \Theta \Uparrow \Gamma, f^-} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A, B}{\vdash \Theta \Uparrow \Gamma, A \vee^- B} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A[y/x]}{\vdash \Theta \Uparrow \Gamma, \forall x A}$$

LKF : focused proof systems for classical logic

$$\frac{}{\vdash \Theta \Uparrow \Gamma, t^-} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A \qquad \vdash \Theta \Uparrow \Gamma, B}{\vdash \Theta \Uparrow \Gamma, A \wedge^- B}$$

$$\frac{\vdash \Theta \Uparrow \Gamma}{\vdash \Theta \Uparrow \Gamma, f^-} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A, B}{\vdash \Theta \Uparrow \Gamma, A \vee^- B} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A[y/x]}{\vdash \Theta \Uparrow \Gamma, \forall x A}$$

$$\frac{}{\vdash \Theta \Downarrow t^+} \qquad \frac{\vdash \Theta \Downarrow A \qquad \vdash \Theta \Downarrow B}{\vdash \Theta \Downarrow A \wedge^+ B} \qquad \frac{\vdash \Theta \Downarrow A_i}{\vdash \Theta \Downarrow A_1 \vee^+ A_2} \qquad \frac{\vdash \Theta \Downarrow A[t/x]}{\vdash \Theta \Downarrow \exists x A}$$

LKF : focused proof systems for classical logic

$$\frac{}{\vdash \Theta \Uparrow \Gamma, t^-} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A \qquad \vdash \Theta \Uparrow \Gamma, B}{\vdash \Theta \Uparrow \Gamma, A \wedge^- B}$$

$$\frac{\vdash \Theta \Uparrow \Gamma}{\vdash \Theta \Uparrow \Gamma, f^-} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A, B}{\vdash \Theta \Uparrow \Gamma, A \vee^- B} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A[y/x]}{\vdash \Theta \Uparrow \Gamma, \forall x A}$$

$$\frac{}{\vdash \Theta \Downarrow t^+} \qquad \frac{\vdash \Theta \Downarrow A \qquad \vdash \Theta \Downarrow B}{\vdash \Theta \Downarrow A \wedge^+ B} \qquad \frac{\vdash \Theta \Downarrow A_i}{\vdash \Theta \Downarrow A_1 \vee^+ A_2} \qquad \frac{\vdash \Theta \Downarrow A[t/x]}{\vdash \Theta \Downarrow \exists x A}$$

Init	Store	Release	Decide
$\dfrac{}{\vdash \neg P_a, \Theta \Downarrow P_a}$	$\dfrac{\vdash \Theta, C \Uparrow \Gamma}{\vdash \Theta \Uparrow \Gamma, C}$	$\dfrac{\vdash \Theta \Uparrow N}{\vdash \Theta \Downarrow N}$	$\dfrac{\vdash P, \Theta \Downarrow P}{\vdash P, \Theta \Uparrow \cdot}$

P positive; P_a positive literal; N negative;
C positive formula or negative literal

About the structural rules in LKF

The only form of *contraction* is in the Decide rule

$$\frac{\vdash P, \Theta \Downarrow P}{\vdash P, \Theta \Uparrow \cdot}$$

The only occurrence of *weakening* is in the Init rule.

$$\frac{}{\vdash \neg P_a, \Theta \Downarrow P_a}$$

Thus: negative non-atomic formulas are treated *linearly!*

Only positive formulas are contracted.

Results about LKF

Let B be a first-order logic formula and let $\hat{B}$ result from B by placing $+$ or $-$ on t, f, $\wedge$, and $\vee$ (there are exponentially many such placements).

Theorem. B is a first-order theorem if and only if $\hat{B}$ has an LKF proof. [Liang & M, TCS 2009]

Thus the different polarizations do not change *provability* but can radically change the *proofs*.

An example

Assume that Θ contains the formula $a \wedge^+ b \wedge^+ \neg c$ and that we have a derivation that Decides on this formula.

$$\dfrac{\dfrac{}{\vdash \Theta \Downarrow a}\ \mathit{Init} \qquad \dfrac{}{\vdash \Theta \Downarrow b}\ \mathit{Init} \qquad \dfrac{\dfrac{\vdash \Theta, \neg c \Uparrow \cdot}{\vdash \Theta \Uparrow \neg c}}{\vdash \Theta \Downarrow \neg c}\ \begin{matrix}\mathit{Release}\\ \mathit{and}\end{matrix}}{\dfrac{\vdash \Theta \Downarrow a \wedge^+ b \wedge^+ \neg c}{\vdash \Theta \Uparrow \cdot}\ \mathit{Decide}}$$

This derivation is possible iff Θ is of the form $\neg a, \neg b, \Theta'$. Thus, the “macro-rule” is

$$\frac{\vdash \neg a, \neg b, \neg c, \Theta' \Uparrow \cdot}{\vdash \neg a, \neg b, \Theta' \Uparrow \cdot}$$

Two certificates for propositional logic: negative

Use $\wedge^-$ and $\vee^-$. Their introduction rules are invertible. The initial "macro-rule" is huge, having all the clauses in the conjunctive normal form of B as premises.

$$\dfrac{\cdots \quad \dfrac{\dfrac{}{\vdash L_1, \ldots, L_n \Downarrow L_i}\; Init}{\vdash L_1, \ldots, L_n \Uparrow \cdot}\; Decide \quad \cdots}{\dfrac{\vdots}{\vdash \cdot \Uparrow B}}$$

The proof certificate can specify the complementary literals for each premise or it can ask the checker to *search* for them.

Proof certificates can be tiny but require exponential time for checking.

Two certificates for propositional logic: positive

Use $\wedge^+$ and $\vee^+$. Sequents are of the form $\vdash B, \mathcal{L} \Uparrow \cdot$ and $\vdash B, \mathcal{L} \Downarrow P$, where B is the original formula to prove, P is positive, and $\mathcal{L}$ is a set of negative literals.

Macro rules are in one-to-one correspondence with $\phi \in DNF(B)$. Divide ϕ into ϕ^- (negative literals) and ϕ^+ (positive literals).

$$\dfrac{\dfrac{\{\vdash B, \mathcal{L}, N \Uparrow \cdot \quad | \quad N \in \phi^-\}}{\vdash B, \mathcal{L} \Downarrow B}}{\vdash B, \mathcal{L} \Uparrow \cdot}\ \mathit{Decide} \qquad \text{provided } \neg\phi^+ \in \mathcal{L}$$

Proof certificates are sequences of members of $DNF(B)$. Size and processing time can be reduced (in response to "cleverness").

Herbrand's Theorem proved

Let B be a quantifier-free first-order formula. $\exists \bar{x}.B$ is valid if and only if there is an $n \geq 1$ and substitutions $\theta_1, \ldots, \theta_n$ such that $B\theta_1 \vee \cdots \vee B\theta_n$ is tautologous.

It is well known that Herbrand's theory can be proved by a permutation argument based on the completeness of cut-free proofs.
Given LKF, this proof is transparent.

Other Possible Applications

Oracles as proofs: when there is no choice in searching for a proof, just continue; when there is a choice, the oracle provides information to resolve the choice. Oracles can be small but fragile certificates. Focusing should help to develop a more declarative and robust version of oracles.

Tables of lemma (M & Nigam, CSL07): polarities can be used to enforce *re-use* instead of *re-prove*.

There are close links between *games semantics* and logic provided by focused proofs. See Delande, M, & Saurin, Annals of Pure and Applied Logic, 2010.

Mixing polarities might relate to *mixing evaluation strategies* (call-by-name, call-by-value) in functional programming languages.