Sequent Calculus: overview and recent developments (Part 2)

Dale Miller

INRIA Saclay & Ecole Polytechnique, France

PLS8: 8th Panhellenic Logic Symposium, Ioannina, Greece,
July 4-8, 2011

Presenting and applying a focused proof system for classical logic.

Invertible rules and the negative phase

Some inference rules are *invertible*, *e.g.*,

$$\frac{A, \Gamma \longrightarrow B}{\Gamma \longrightarrow A \supset B} \qquad \frac{\Gamma \longrightarrow A \qquad \Gamma \longrightarrow B}{\Gamma \longrightarrow A \wedge B} \qquad \frac{\Gamma \longrightarrow B[y/x]}{\Gamma \longrightarrow \forall x.B}$$

First focusing principle: when proving a sequent, apply invertible rules exhaustively and in any order.

This is the *negative phase* of proof search: if formulas are "processes" in an "environment," then these formulas "evolve" without communications ("asynchronously") with the environment.

Non-invertible rules and the positive phase

Some inference rules are not generally invertible, *e.g.*,

$$\frac{\Gamma_1 \longrightarrow A \quad \Gamma_2 \longrightarrow B}{\Gamma_1, \Gamma_2 \longrightarrow A \wedge B} \qquad \frac{\Gamma \longrightarrow B[t/x]}{\Gamma \longrightarrow \exists x.B}$$

Some *backtracking* is generally necessary within proof search using these inference rules.

Second focusing principle: non-invertible rules are applied in a "chain-like" fashion.

This is the *positive phase* of proof search.

Extending the neg/pos distinction to atoms

Focusing proof systems generally extend the neg/pos distinction to atoms.

We shall assume that somehow all atoms are given a *bias*, that is, they are either positive or negative.

A *positive formula* is either a positive atom or has a top-level connective whose right-introduction rule is not invertible.

A *negative formula* is either a negative atom or has a top-level connective whose right-introduction rules is invertible.

Various focusing-like proof system

Uniform proofs [M, Nadathur, Scedrov, 1987] describes goal-directed search and backchaining (in higher-order logic).

LLF: [Andreoli, 1992]: a focused proof system for linear logic.

LKT/LKQ/LK$^{\eta}$: focusing systems for classical logic [Danos, Joinet, Schellinx,1993]

LJQ [Herbelin, 1995] permits forward-chaining proof. *LJQ′* [Dyckhoff & Lengrand, 2007] extends it.

λRCC [Jagadeesan, Nadathur, Saraswat, 2005] mixes forward chaining and backward chaining (in a subset of intuitionistic logic).

LJF [Liang & M, 2009] allows forward and backward proof in all of intuitionistic logic. LJT, LJQ, λRCC, and LJ are subsystems.

LKF (following) provides focusing for all of classical logic.

The full picture behind focusing

Andreoli (1992) was the first to give a focused proof system for a full logic (linear logic).

The proof system for MALL (multiplicative-additive linear logic) is remarkably elegant and unambiguous.

Some complexity arises from using the exponentials (!, ?): in particular, exponentials terminate focusing phases.

We now present two comprehensive focused proof systems for classical logic.

- LKF for *classical logic*
- LKF for *classical logic* with fixed points and equality

Classical logic and one-sided sequents

Two conventions for dealing with classical logic.

- Formulas are in *negation normal form*.
  - $B \supset C$ is replaced with $\neg B \vee C$,
  - negations are pushed to the atoms
- Sequents will be one-sided. In particular, the two sided sequent

$$\Sigma : B_1, \ldots, B_n \vdash C_1, \ldots, C_m$$

will be converted to

$$\Sigma : \quad \vdash \neg B_1, \ldots, \neg B_n, C_1, \ldots, C_m.$$

We also drop the "$\Sigma :$ " prefix on sequents.

LKF: Focusing for Classical Logic

Formulas are *polarized* as follows.

- atoms are assigned bias (either $+$ or $-$), and
- $\wedge$ $\vee$, t, and f are annotated with either $+$ or $-$.
  Thus: $\wedge^-$, $\wedge^+$, $\vee^-$, $\vee^+$, t^-, t^+, f^-, f^+.

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

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

Store

$$\frac{\vdash \Theta, C \Uparrow \Gamma}{\vdash \Theta \Uparrow \Gamma, C}$$

Release

$$\frac{\vdash \Theta \Uparrow N}{\vdash \Theta \Downarrow N}$$

Decide

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

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* (in the sense of linear logic).

Only positive formulas are contracted.

The abstraction behind focused proofs

We can ignore the internal structure of phases and consider only their boundaries.

We can now move from *micro-rules* (introduction rules) to *macro-rules* (pos or neg phases).

The *decide depth* of an LKF proofs is the maximum number of *Decide* rules along any path starting from the end-sequent.

This measures counts "bi-poles": one positive phase followed by a negative phase.

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*.

Recall the Fibonacci series example: one specification yielded an exponential time algorithm or a linear time algorithm depending only on bias assignment.

An example

Let a, b, c be positive atoms and let Θ contain the formula $a \wedge^+ b \wedge^+ \neg c$.

$$\dfrac{\dfrac{}{\vdash \Theta \Downarrow a}\ \textit{Init} \quad \dfrac{}{\vdash \Theta \Downarrow b}\ \textit{Init} \quad \dfrac{\dfrac{\vdash \Theta, \neg c \Uparrow \cdot}{\vdash \Theta \Uparrow \neg c}}{\vdash \Theta \Downarrow \neg c}\ \textit{Release}}{\dfrac{\vdash \Theta \Downarrow a \wedge^+ b \wedge^+ \neg c}{\vdash \Theta \Uparrow \cdot}\ \textit{Decide}}\ \textit{and}$$

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

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

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.

$$\dfrac{\dots \quad \dfrac{\dfrac{}{\vdash L_1, \dots, L_n \Downarrow L_i}\ \mathit{Init}}{\vdash L_1, \dots, L_n \Uparrow \cdot}\ \mathit{Decide} \quad \dots}{\vdots}$$
$$\vdash \cdot \Uparrow B$$

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

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).

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

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

Positives allow "clever" choices

To illustrate the trade-off between proof-size and proof-checking time consider the following simple example.

Let B be a propositional formula with a large conjunctive normal form. Let B^- (respectively, B^+) be the result of annotating all the connectives in B negative (respectively, positively).

Consider the tautology $C = (p \vee B) \vee \neg p$.

A *negative focused proof* results from computing the conjunctive normal form of C and then observing that each disjunct is trivial.

There are many *positive focused proof* but one has decide depth 2: first move through C to pick $\neg p$ and then move again through C to pick p.

Herbrand's Theorem proved

Herbrand's Theorem.
Let B be a quantifier-free first-order formula. $\exists \bar{x}.B$ is a theorem 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.

This theorem is easily proved by the completeness of LKF.

Arithmetic via equality and fixed points

We shall add

- first-order *term equality*
  following Girard [1992] and Schroeder-Heister [1993], and
- *fixed points* (for recursive definitions)
  following Baelde, McDowell, M, Tiu [1996-2008].

They will both be *logical connectives:* that is, they are defined by introduction rules.

Equality as logical connective

Introductions in an unfocused setting.

$$\frac{}{\vdash \Theta, t = t} \qquad \frac{}{\vdash \Theta, s \neq t}\ \ddagger \qquad \frac{\vdash \Theta\sigma}{\vdash \Theta, s \neq t}\ \dagger$$

$\ddagger$ s and t are not unifiable.

$\dagger$ s and t to be unifiable and σ to be their mgu

Equality as logical connective

Introductions in an unfocused setting.

$$\frac{}{\vdash \Theta, t = t} \qquad \frac{}{\vdash \Theta, s \neq t}\ \ddagger \qquad \frac{\vdash \Theta\sigma}{\vdash \Theta, s \neq t}\ \dagger$$

$\ddagger$ s and t are not unifiable.
$\dagger$ s and t to be unifiable and σ to be their mgu

Introductions in a focused setting.

$$\frac{}{\vdash \Theta \Downarrow t = t} \qquad \frac{}{\vdash \Theta \Uparrow \Gamma, s \neq t}\ \ddagger \qquad \frac{\vdash \Theta\sigma \Uparrow \Gamma\sigma}{\vdash \Theta \Uparrow \Gamma, s \neq t}\ \dagger$$

N.B. Unification was used before to *implement* inference rules: here, unification is in the *definition* of the rule.

Some theorems about equality

Equality is an equivalence relation...

- $\forall x\,[x = x]$
- $\forall x, y\,[x = y \supset y = x]$
- $\forall x, y, z\,[x = y \wedge y = z \supset x = z]$

and a congruence.

- $\forall x, y\,[x = y \supset (f\ x) = (f\ y)]$
- $\forall x, y\,[x = y \supset (p\ x) \supset (p\ y)]$

Let 0 denote zero and s denote successor.

- $\forall x\,[0 \neq (s\ x)]$
- $\forall x, y\,[(s\ x) = (s\ y) \supset x = y]$

A hint of model checking

Encode a non-empty set of first order terms $S = \{s_1, \ldots, s_n\}$ ($n \geq 1$) as the one-place predicate

$$\hat{S} = [\lambda x.\ x = s_1 \vee^+ \cdots \vee^+ x = s_n]$$

If S is empty, then define $\hat{S}$ to be $[\lambda x.\ f^+]$. Notice that

$$s \in S \quad \text{if and only if} \quad \vdash \hat{S}\ s.$$

A hint of model checking

Encode a non-empty set of first order terms $S = \{s_1, \ldots, s_n\}$ ($n \geq 1$) as the one-place predicate

$$\hat{S} = [\lambda x.\ x = s_1 \vee^+ \cdots \vee^+ x = s_n]$$

If S is empty, then define $\hat{S}$ to be $[\lambda x.\ f^+]$. Notice that

$$s \in S \quad \text{if and only if} \quad \vdash\ \hat{S}\ s.$$

The statement

$$\forall x \in \{s_1, \ldots, s_n\}.P(x) \quad \text{becomes} \quad \forall x.[\hat{S}x \supset Px].$$

$$\frac{\vdash P(s_1) \Uparrow \cdot}{\vdash P(x) \Uparrow x \neq s_1} \quad \cdots \quad \frac{\vdash P(s_n) \Uparrow \cdot}{\vdash P(x) \Uparrow x \neq s_n}$$
$$\vdash \cdot \Uparrow \forall x.[x \neq s_1 \wedge^- \cdots \wedge^- x \neq s_n] \vee^- P(x)$$

Fixed Points as connectives

The *fixed points* operators μ and ν are De Morgan duals and simply unfold.

$$\frac{\vdash \Theta \Uparrow \Gamma, B(\nu B)\bar{t}}{\vdash \Theta \Uparrow \Gamma, \nu B \bar{t}} \qquad \frac{\vdash \Theta \Downarrow B(\mu B)\bar{t}}{\vdash \Theta \Downarrow \mu B \bar{t}}$$

B is a formula with $n \geq 0$ variables abstracted; $\bar{t}$ is a list of n terms.

Here, μ denotes neither the least nor the greatest fixed point. That distinction arises if we add induction and co-induction.

Examples of fixed points

Natural numbers: terms over 0 for zero and s for successor. Two ways to define predicates over numbers.

$$\begin{array}{rcl} \mathit{nat}\ 0 & :- & \mathit{true}. \\ \mathit{nat}\ (s\ X) & :- & \mathit{nat}\ X. \\ \mathit{leq}\ 0\ Y & :- & \mathit{true}. \\ \mathit{leq}\ (s\ X)\ (s\ Y) & :- & \mathit{leq}\ X\ Y. \end{array}$$

These logic programs can be given as fixed point expressions.

$$\mathit{nat} = \mu(\lambda p \lambda x.(x = 0) \vee^{+} \exists y.(s\ y) = x \wedge^{+} p\ y)$$

$$\mathit{leq} = \mu(\lambda q \lambda x \lambda y.(x = 0) \vee^{+} \exists u \exists v.(s\ u) = x \wedge^{+} (s\ v) = y \wedge^{+} q\ u\ v).$$

Horn clauses can be made into fixed point specifications (mutual recursions requires standard encoding techniques).

Putting computation into an inference rule

Consider proving the positive focused sequent

$$\vdash \Theta \Downarrow (\mathit{leq}\ m\ n \wedge^+ N_1) \vee^+ (\mathit{leq}\ n\ m \wedge^+ N_2),$$

where m, n are natural numbers and N_1, N_2 are negative formulas. There are exactly two possible macro rules:

$$\frac{\vdash \Theta \Downarrow N_1}{\vdash \Theta \Downarrow (\mathit{leq}\ m\ n \wedge^+ N_1) \vee^+ (\mathit{leq}\ n\ m \wedge^+ N_2)} \text{ for } m \leq n$$

$$\frac{\vdash \Theta \Downarrow N_2}{\vdash \Theta \Downarrow (\mathit{leq}\ m\ n \wedge^+ N_1) \vee^+ (\mathit{leq}\ n\ m \wedge^+ N_2)} \text{ for } n \leq m$$

A macro inference rule can contain an entire Prolog-style computation.

One step transitions in CCS

As inference rules in SOS (structured operational semantics):

$$\frac{}{A.P \xrightarrow{A} P} \qquad \frac{P \xrightarrow{A} R}{P + Q \xrightarrow{A} R} \qquad \frac{Q \xrightarrow{A} R}{P + Q \xrightarrow{A} R}$$

$$\frac{P \xrightarrow{A} P'}{P|Q \xrightarrow{A} P'|Q} \qquad \frac{Q \xrightarrow{A} Q'}{P|Q \xrightarrow{A} P|Q'}$$

These can easily be written as Prolog clauses and as a fixed point definition.

The engineering of proof systems (cont)

Consider proofs involving simulation.

$$sim\ P\ Q \ \equiv\ \forall P' \forall A[\ P \xrightarrow{A} P' \supset \exists Q'\ [Q \xrightarrow{A} Q' \wedge sim\ P'\ Q']].$$

Typically, $P \xrightarrow{A} P'$ is given as a table or as a recursion on syntax (*e.g.*, CCS): hence, as a fixed point.
The body of this expression is exactly two "macro connectives".

- $\forall P' \forall A[P \xrightarrow{A} P' \supset \cdot\ ]$ is a negative "macro connective". There are no choices in expanding this macro rule.
- $\exists Q'[Q \xrightarrow{A} Q' \wedge^{+} \cdot\ ]$ is a positive "macro connective". There can be choices for continuation Q'.

These macro-rules now match exactly the sense of simulation.

Future work: Broad spectrum proof certificates

Sequent calculus and focusing proof systems provide:

- The *atoms* of inference (the introduction rules)
- The structure of focusing provides us with the *rules of chemistry*: which atoms stick together and which do not.
- Engineered proofs system made form the *molecules* of inference.

Future work: Broad spectrum proof certificates

Sequent calculus and focusing proof systems provide:

- The *atoms* of inference (the introduction rules)
- The structure of focusing provides us with the *rules of chemistry*: which atoms stick together and which do not.
- Engineered proofs system made form the *molecules* of inference.

An approach to a general notion of *proof certificate*:

- The world's provers print their proof evidence using appropriately engineered molecules of inference.
- A universal proof checker implements only the atoms of inference and the rules of chemistry.

Future work: Broad spectrum proof certificates

Sequent calculus and focusing proof systems provide:

- The *atoms* of inference (the introduction rules)
- The structure of focusing provides us with the *rules of chemistry*: which atoms stick together and which do not.
- Engineered proofs system made form the *molecules* of inference.

An approach to a general notion of *proof certificate*:

- The world's provers print their proof evidence using appropriately engineered molecules of inference.
- A universal proof checker implements only the atoms of inference and the rules of chemistry.

See the two recent draft submissions:

- "Communicating and trusting proofs: The case for broad spectrum proof certificates"
- "A proposal for broad spectrum proof certificates"