Fixed points and proof theory

Dale Miller

INRIA-Saclay & LIX, École Polytechnique
Palaiseau, France

FICS 2010, 21 August 2010

Joint work with David Baelde. See LPAR 2007; Baelde's 2008 PhD; ACM-BCS-Visions Conference 2010; extended journal submission.

Outline

1. Primer on sequent calculus proofs and focused proofs
2. Fixed points: unfolding only
3. Fixed points: induction and co-induction rules
4. Some applications

Propositional classical logic

Let us start some place very familiar.

The only connectives: $\wedge$, $\vee$, t, f.

$B^{\perp}$ denotes the negation normal form of the negation of B.

We have no atomic formulas (in the entire talk!). *Atoms are undefined formulas*. We give recursive definitions to everything.

We first present a proof system using one-sided sequents $\vdash \Delta$, where Δ is a *multiset* of formulas.

The proof system contains:

- two *structural* rules (weakening and contraction),
- two *identity* rules (initial and cut),
- the *multiplicative* introduction rules, and
- the *additive* introduction rules.

A unfocused proof system for classical logic

Structural: $\dfrac{\vdash B, B, \Delta}{\vdash B, \Delta}\ \mathit{contract}$ $\qquad$ $\dfrac{\vdash \Delta}{\vdash B, \Delta}\ \mathit{weaken}$

Identity: $\dfrac{}{\vdash B, B^{\perp}}\ \mathit{initial}$ $\qquad$ $\dfrac{\vdash \Delta_1, B \quad \vdash B^{\perp}, \Delta_2}{\vdash \Delta_1, \Delta_2}\ \mathit{cut}$

Multiplicative: $\dfrac{\vdash B_1, \Delta_1 \quad \vdash B_2, \Delta_2}{\vdash B_1 \wedge B_2, \Delta_1, \Delta_2}\ \wedge$ $\qquad$ $\dfrac{\vdash B_1, B_2, \Delta}{\vdash B_1 \vee B_2, \Delta}\ \vee^{*}$

$\dfrac{}{\vdash t}\ t$ $\qquad$ $\dfrac{\vdash \Delta}{\vdash f, \Delta}\ f^{*}$

Additive: $\dfrac{\vdash B_1, \Delta \qquad \vdash B_2, \Delta}{\vdash B_1 \wedge B_2, \Delta}\ \wedge^{*}$ $\qquad$ $\dfrac{\vdash B_i, \Delta}{\vdash B_1 \vee B_2, \Delta}\ \vee_i$

$\dfrac{}{\vdash t, \Delta}\ t^{*}$ $\qquad$ —

Both identity rules can be eliminated! The $*$ rules are invertible.

Two versions of the connectives

Given the structural rules, the additive rule and the multiplicative rule for the same connective are inter-admissible.

Annotate the connectives of the invertible rules as negative ($\wedge^-$ and $\vee^-$) and annotate the connectives in not-necessarily-invertible rules as positive ($\wedge^+$ and $\vee^+$).

Similarly, annotate their units (t^-, f^-, t^+, f^+).

An annotated formula is *negative* if its top-level logical connective is annotated negatively: likewise for *positive*.

Given a formula B let $\hat{B}$ be any *polarization* of B in which every logical connectives in B is given either a plus or a minus annotation. Then:

> *B is provable (in the unannotated proof system) if and only if $\hat{B}$ is provable (in the annotated proof system).*

Proof search with unfocused proof search

... is simply ridiculous. There are just too many ways to build proofs and most of them differ in truly minor ways.

One wants a tight correspondence between the application of inference rules and “actions” within a computation.

An early taming of the sequent calculus used *uniform proofs* [Miller et.al, 91] which contained the two “phases” of *goal-reduction* and *backchaining* (a proof-theoretic foundation for logic programming).

Andreoli’s *focused proof system* [1992] generalize that earlier work to a full, rich logic (linear logic).

An important message of this talk: Focused proof systems are an essential normal form for the application of sequent calculus.

The LKF focused proof system

We present a focused proof system for *annotated* propositional classical logic that is derived from the LKF proof system of Liang and Miller [2007].

Let P denote a positive formula, N a negative formula, and Θ a multiset of positive formulas, and Γ is a list of formulas.

Sequents in the focused proof system are of the form

- $\vdash \Theta \Uparrow \Gamma$ (negative or asynchronous phase)
- $\vdash \Theta \Downarrow B$ (positive or synchronous phase)

The inference rules used in the negative phase are invertible.

The LKF focused proof system

Structural: $\dfrac{\vdash \Theta, P \Uparrow \Gamma}{\vdash \Theta \Uparrow \Gamma, P}$ *Store* $\quad \dfrac{\vdash \Theta \Uparrow N}{\vdash \Theta \Downarrow N}$ *Release* $\quad \dfrac{\vdash P, \Theta \Downarrow P}{\vdash P, \Theta \Uparrow \cdot}$ *Focus*

Neg phase: $\dfrac{}{\vdash \Theta \Uparrow \Gamma, t^-} \quad \dfrac{\vdash \Theta \Uparrow \Gamma, A \quad \vdash \Theta \Uparrow \Gamma, B}{\vdash \Theta \Uparrow \Gamma, A \wedge^- B}$

$\dfrac{\vdash \Theta \Uparrow \Gamma}{\vdash \Theta \Uparrow \Gamma, f^-} \quad \dfrac{\vdash \Theta \Uparrow \Gamma, A, B}{\vdash \Theta \Uparrow \Gamma, A \vee^- B}$

Pos phase: $\dfrac{}{\vdash \Theta \Downarrow t^+} \quad \dfrac{\vdash \Theta \Downarrow A \quad \vdash \Theta \Downarrow B}{\vdash \Theta \Downarrow A \wedge^+ B}$

– $\quad \dfrac{\vdash \Theta \Downarrow A_i}{\vdash \Theta \Downarrow A_1 \vee^+ A_2}$

Contraction occurs only in the *Focus* rule and only on *positives*.
Negatives are treated *linearly* !

LKF is sound and complete for classical logic

Theorem

Let B be a propositional formula and let $\hat{B}$ be a polarization of B. Then B is provable in classical logic if and only if there is an LKF proof of $\vdash \cdot \Uparrow \hat{B}$.

Notice that polarization does not affect provability but it does affect the shape of possible LKF proofs.

If one uses only negative connectives, then

- most of the proof is one $\Uparrow$ phase, and
- the proof is exponential in size.

Invertibility can be expensive. If one uses positive connectives, some "cleverness" can be inserted into the proof and you might find much smaller proofs.

Macro-rules vs Micro-rules

Focused proof allow us to change the size of inference rules.
Micro-rule: an introduction rule
Macro-rule: an entire phase (collect all adjacent $\Uparrow$ or $\Downarrow$).

The following is a positive macro-rule:

$$\dfrac{\dfrac{\vdash \Theta, P \Uparrow N_1 \quad \cdots \quad \vdash \Theta, P \Uparrow N_n}{\cdots \text{ only } \Downarrow \text{ sequents here } \cdots}}{\dfrac{\vdash \Theta, P \Downarrow P}{\vdash \Theta, P \Uparrow \cdot}}$$

Specifically: the macro-rule is has conclusion $\vdash \Theta, P \Uparrow \cdot$ and $n \geq 0$ premises $\vdash \Theta, P \Uparrow N_1, \ldots, \vdash \Theta, P \Uparrow N_n$.

Similarly, there are negative macro-rules with conclusion, say, $\vdash \Theta, P \Uparrow N_i$, and with $m \geq 0$ premises of the form $\vdash \Theta, P, \mathcal{C} \Uparrow \cdot$, where $\mathcal{C}$ is a multiset of positive formulas.

Macro-rules automatically satisfy cut and initial elimination.

Breaking macro-rules with delays

Large macro rules can easily be broken up, if desired, by the use of *delays*, which can be defined as follows:

$$\partial^+(B) = B \wedge^+ t^+ \quad \text{and} \quad \partial^-(B) = B \wedge^- t^-.$$

Clearly, B, $\partial^-(B)$, and $\partial^+(B)$ are all logically equivalent but $\partial^-(B)$ is always negative and $\partial^+(B)$ is always positive.

Insert $\partial^-(\cdot)$ into a formula to break a positive phase. Insert $\partial^+(\cdot)$ into a formula to break a negative phase.

By inserting many delay operators, a focused proof can be made to emulate an unfocused proof.

Fixed points and first-order structure

We now add to propositional classical logic

- the fixed point constructors μ and ν,
- the first-order quantifiers $\forall$ and $\exists$, and
- the equality / in-equality relations on first-order terms $=$ and $\neq$.

Each pair of these connectives are de Morgan duals.

The connectives μ and ν are really a collection $\{\mu_n\}_{n\geq 0}$ and $\{\nu_n\}_{n\geq 0}$ such that the simple type of μ_n and of ν_n is $\tau_n \to \tau_n$, where τ_n is $i \to \ldots \to i \to o$ (n occurrences of the type i).

All six of these constants are *logical connectives*: they all have introduction rules and the cut and initial rules can be eliminated.

Inference rules for quantifiers, equality, fixed points

Fixed points:
$$\frac{\vdash B(\nu B)\bar{u}, \Delta}{\vdash \nu B \bar{u}, \Delta} \qquad \frac{\vdash B(\mu B)\bar{u}, \Delta}{\vdash \mu B \bar{u}, \Delta}$$

Quantifiers:
$$\frac{\vdash B[t/x], \Delta}{\vdash \exists x.B, \Delta} \qquad \frac{\vdash B[y/x], \Delta}{\vdash \forall x.B, \Delta}$$

Equality:
$$\frac{\vdash \Delta\sigma}{\vdash u \neq v, \Delta}\ \dagger \qquad \frac{}{\vdash u \neq v, \Delta}\ \ddagger \qquad \frac{}{\vdash u = u}$$

Provisos: $\dagger$: u and v have mgu σ $\quad$ $\ddagger$: u and v are not unifiable

Inference rules for quantifiers, equality, fixed points

Fixed points:
$$\frac{\vdash B(\nu B)\bar{u}, \Delta}{\vdash \nu B\bar{u}, \Delta} \qquad \frac{\vdash B(\mu B)\bar{u}, \Delta}{\vdash \mu B\bar{u}, \Delta}$$

Quantifiers:
$$\frac{\vdash B[t/x], \Delta}{\vdash \exists x.B, \Delta} \qquad \frac{\vdash B[y/x], \Delta}{\vdash \forall x.B, \Delta}$$

Equality:
$$\frac{\vdash \Delta\sigma}{\vdash u \neq v, \Delta}\ \dagger \qquad \frac{}{\vdash u \neq v, \Delta}\ \ddagger \qquad \frac{}{\vdash u = u}$$

Provisos: $\dagger$: u and v have mgu σ $\qquad$ $\ddagger$: u and v are not unifiable

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

$$\frac{\vdash \Theta \Downarrow B[t/x]}{\vdash \Theta \Downarrow \exists x.B} \qquad \frac{\vdash \Theta \Uparrow \Gamma, B[y/x]}{\vdash \Theta \Uparrow \Gamma, \forall x.B}$$

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

Least and Greatest Fixed points?

The two fixed points constructors have identical rules: unfolding. Hence, they are equivalent and *self-dual*:

$$(\mu\lambda p\lambda\bar{x}.(Bp\bar{x}))^{\perp} \equiv (\mu\lambda p\lambda\bar{x}.(Bp\bar{x})^{\perp})$$

$$(\nu\lambda p\lambda\bar{x}.(Bp\bar{x}))^{\perp} \equiv (\nu\lambda p\lambda\bar{x}.(Bp\bar{x})^{\perp})$$

Such equivalences are only provable if all unfoldings terminate.

We arbitrarily classify μ as positive and ν as negative.

We separate these constructor later when we introduce the (higher-order) rules for *induction* and *co-induction*.

Examples

The following Horn clauses (Prolog program) defines two predicates on natural numbers.

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

The predicate *nat* can be written as the fixed point

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

and *leq* (less-than-or-equal) can be written as the fixed point

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

Horn clause specification can be made into *purely positive* fixed point specifications.

Engineering of inference rules

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 and n are natural numbers and where both N_1 and N_2 are negative formulas.

There are exactly two possible macro rules with this conclusion:

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

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

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

The inference rules for labeled transitions

One step transitions $P \xrightarrow{A} Q$ are often given as

- a table to encode finite state machines, or
- a collection of syntax-directed SOS inference rules, such as

$$\frac{P_i \xrightarrow{A} R}{P_1 + P_2 \xrightarrow{A} R}\ i{=}1{,}2 \qquad \frac{}{a.P \xrightarrow{a} P} \qquad \cdots$$

In either case, Horn clauses can describe $P \xrightarrow{A} Q$. For example,

$$\begin{aligned} \forall P_1, P_2, A, R\ [\ P_1 \xrightarrow{A} R \ &\supset\ P_1 + P_2 \xrightarrow{A} R\ ] \\ \forall P_1, P_2, A, R\ [\ P_2 \xrightarrow{A} R \ &\supset\ P_1 + P_2 \xrightarrow{A} R\ ] \\ \forall P, A\ [\ t \ &\supset\ A.P \xrightarrow{A} P\ ] \end{aligned}$$

Hence, $\cdot \dot{\longrightarrow} \cdot$ can be defined as a purely positive fixed point.

Formally, $\cdot \dot{\longrightarrow} \cdot$ is not a predicate and $P \xrightarrow{A} Q$ is not an atomic formula.

The inference rules for simulation

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

Here, the implication $B \supset C$ is an abbreviation for $B^{\perp} \vee^{-} C$.
As a fixed point expression, *sim* relation is:

$$\nu \lambda s \lambda P \lambda Q. \forall P' \forall A[P \xrightarrow{A} P' \supset \exists Q'[Q \xrightarrow{A} Q' \wedge s\ P'\ Q']]$$

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'.

The resulting focused proof system (using the macro-rules) is aligned directly with the structure of the actual (model-checking) problem.

Rules for Induction and co-induction

Unfolding is limited: we cannot prove $\forall n.nat\ n \supset nat\ n$. We need rules for *induction / co-induction*.

$$\frac{\vdash \Gamma, B(\mu B)\bar{u}}{\vdash \Gamma, \mu B\bar{u}}\ \mu \qquad \frac{\vdash \Gamma, S\bar{u} \quad \vdash BSx, (Sx)^{\perp}}{\vdash \Gamma, \nu B\bar{u}}\ \nu \qquad \frac{}{\vdash \mu B\bar{u}, \nu\bar{B}\bar{u}}\ \mu\nu$$

S ranges over closed term of type τ_n. x is an eigenvariable.

With these rules, μ and ν are different: μ builds the least fixed point and ν builds the greatest fixed point.

The *negation* $\overline{B}$ of a body B is defined as $\lambda p.\lambda\vec{x}.(B(\lambda\vec{x}.(p\vec{x})^{\perp})\vec{x})^{\perp}$.

We shall assume that *all bodies are monotonic*: the expression $Bp\bar{t}$ does not contain any negated instance of p.

Induction and co-induction in two-sided sequents

If we write these rules as two-sided, single-conclusion sequents, they might look more familiar.

$$\frac{\Gamma \vdash B(\mu B)\bar{u}}{\Gamma \vdash \mu B\bar{u}} \qquad \frac{BS\vec{x} \vdash S\vec{x} \quad \Gamma, S\vec{t} \vdash G}{\Gamma, \mu B\vec{t} \vdash G}\ \mu L \qquad \frac{}{\mu B\bar{u} \vdash \mu B\bar{u}}$$

$$\frac{\Gamma, B(\nu B)\bar{u} \vdash G}{\Gamma, \nu B\bar{u} \vdash G} \qquad \frac{S\vec{x} \vdash BS\vec{x} \quad \Gamma \vdash S\vec{t}}{\Gamma \vdash \nu B\vec{t}}\ \nu R \qquad \frac{}{\nu B\bar{u} \vdash \nu B\bar{u}}$$

The $\mu\nu$ rule is the only form of the initial rule that we shall need in this proof system.

Informally: when trying to prove $\forall n.nat(n) \supset B(n)$ by induction, one tries to reduce $B(j+1)$ to the inductive assumption $B(j)$. Thus, you need to know if your current reduction *equals* $B(j)$.

Focused version of the induction and co-induction rules

$$\frac{\vdash \Gamma \Uparrow S\bar{t}, \Delta \quad \vdash \Uparrow BS\vec{x}, S\vec{x}^{\perp}}{\vdash \Gamma \Uparrow \nu B\bar{t}, \Delta}\ \vec{x} \text{ new} \qquad \frac{\vdash \Gamma, \nu B\bar{t} \Uparrow \Delta}{\vdash \Gamma \Uparrow \nu B\bar{t}, \Delta}$$

$$\frac{\vdash \Gamma \Downarrow B(\mu B)\vec{x}}{\vdash \Gamma \Downarrow \mu B\vec{x}} \qquad \frac{}{\vdash \nu\overline{B}\vec{x} \Downarrow \mu B\vec{x}}$$

Unfolding of ν is easily proved from the co-induction rule.

$$\frac{\vdash \Gamma \Uparrow B(\nu B)\vec{x}}{\vdash \Gamma \Uparrow \nu B\vec{x}}$$

Notice that in the negative (invertible) phase, there is a choice in the treatment of ν. One either

- does a co-induction (includes unfolding) or
- freezes it (store it to eventually match in the $\mu\nu$ rule.

Linear logic: add exponentials or fixed points?

The logic above has two forms of "unbounded" behaviors built-in: *contraction* and *fixed points*. Do we need both?

MALL (multiplicative-additive linear logic) is the result of removing weakening and contraction from propositional classical logic.

The positive and negative version of connectives are now different. Write $\otimes$, $\&$, $\oplus$, $\parr$ instead of $\wedge^+$, $\wedge^-$, $\vee^+$, $\vee^-$.

MALL is a wonderful but weak logic.

- Girard added exponentials (!, ?) to get full linear logic. The exponentials reintroduces weakening and contraction. Elegant but not perfect solution: exponentials are not canonical, etc.
- Baelde added fixed points instead. $\mu MALL^=$.

If B is purely positive, then $\vdash !B \equiv B$. Thus, it is possible to model some of intuitionistic logic directly within $\mu MALL^=$.

Model checking: $\mu LJ^{=}$ and Bedwyr

Let $\mu LJ^{=}$ be the subset of intuitionistic logic described using the two syntactic variables $\mathcal{G}$ and $\mathcal{H}$:

$$\begin{array}{rcl} \mathcal{G} & ::= & \mathcal{G} \wedge \mathcal{G} \mid \mathcal{G} \vee \mathcal{G} \mid s = t \mid \mu(\lambda p \vec{x}.\mathcal{G} p \vec{x})\vec{t} \mid \exists x.\mathcal{G}x \\ & \mid & \forall x.\mathcal{G}x \mid \mathcal{H} \supset \mathcal{G} \mid \nu(\lambda p \vec{x}.\mathcal{G} p \vec{x})\vec{t} \\ \mathcal{H} & ::= & \mathcal{H} \wedge \mathcal{H} \mid \mathcal{H} \vee \mathcal{H} \mid s = t \mid \mu(\lambda p \vec{x}.\mathcal{H} p \vec{x})\vec{t} \mid \exists x.\mathcal{H}x \end{array}$$

Translated to $\mu MALL^{=}$ by using positive connectives where possible ($\vee^{+}$, $\wedge^{+}$) and translating $\supset$ to the $\multimap$.

The focused proof system for $\mu MALL^{=}$ on this fragment of intuitionistic provides the "operational semantics" of the Bedwyr model checker [Baelde, Gacek, Miller, Nadathur, Tiu. CADE 2007].

Bedwyr uses unfolding of fixed points, except for justifying *tabling*, which requires induction.

Theorem proving: Tac

Consider searching for only “simple” focused proofs.

- Limit the depth of proofs to only 2 or 3 macro-inference rules.
- Attempt to only use the “obvious” invariant in the induction and co-induction inference rules (use the context)

$$\frac{\Sigma;\ \Gamma, S\vec{t} \vdash G \quad \vec{x}\ ;\ BS\vec{x} \vdash S\vec{x}}{\Sigma;\ \Gamma, \mu B\vec{t} \vdash G} \quad \text{with } S := \lambda\vec{x}.\ \forall\Sigma.\ \vec{x} = \vec{t} \supset (\bigwedge \Gamma) \supset G.$$

$$\frac{\Sigma;\ \Gamma \vdash S\vec{t} \quad \vec{x}\ ;\ S\vec{x} \vdash BS\vec{x}}{\Sigma;\ \Gamma \vdash \nu B\vec{t}} \quad \text{with } S := \lambda\vec{x}.\ \exists\Sigma.\ \vec{x} = \vec{t} \wedge (\bigwedge \Gamma).$$

The first premise is trivially provable.

Such trivial (co)inductions suffice for many examples [Baelde, Miller, Snow; IJCAR 2010].

Conclusions

Focused proof systems are important technical tools in the application of proof theory to computation.

Fixed points are an interesting alternative to exponentials for adding unbounded behaviors to MALL.

The focused proof system including induction and co-induction is an important formal tool in itself. It yields an appealing and flexible normal form theorem.

Connections to *game semantics* and *cyclic proofs* should be further developed.

Focused proofs are highly customizable. They might serve well as a *broad spectrum proof certificate*.