Focused sequent calculus proof systems

Dale Miller

Inria Saclay & LIX, École Polytechnique
Palaiseau, France

Workshop on Proof Theory and its Applications
Ghent, 6 September 2018

The sequent calculus

I assume everyone here is familiar with Gentzen's LJ and LK sequents. I mention only some highlights.

- Gentzen used lists as the left and right contexts. He also used the exchange rule.
- In this talk, contexts will be either multisets or lists: exchange is never used.
- Proofs without cuts are *analytic* (involving only subformulas): there are no cut-free proofs of false.
- Introducing the cut rule meant that all of first-order logic was captured. Cut-elimination was a kind of completeness result: analytic proofs were sufficient.

Unity of logic

LJ proofs are LK proofs in which the right hand side has at most one formula.

Gentzen's sequent calculus work was an early attempt at a "unity of logic". Making structure rules explicit (especially on the right) is critical.

Girard logic takes the add rule explicit also on the left. Linear logic and sequent calculus:

Sequent calculus is an appealing tool to study proof theory and computational logic since it captures and relates these three logics.

Applications of sequent calculus

Besides cut-elimination and the consistency of classical and intuitionistic logics, sequent calculus has been used in:

Proof theory

- Herbrand's theorem
- Midsequent theorem
- Interpolation
- Negative translations

Computer Science

- foundations for logic programming:
- explicit substitutions in the λ-calculus
- syntactic correctness of Skolemization
- etc.

However: Sequent calculus proofs are chaotic, painful, etc

Sequent calculus proofs are formless.

Any structure they might contain about a proof needs to be pulled out by extensive inference-rule permutation arguments.

It is common to say that

- a sequent calculus proof is a *computation of a proof* while
- a natural deduction proof is the *actual proof*.

We can be more sophisticated than that in this talk.

Permutation of inference rules illustrated

Let Γ be a multiset of 998 formulas and consider searching for a proof of the sequent $\Gamma, B_1 \vee B_2, C_1 \wedge C_2 \vdash A$.

There are 1000 choices for the left introduction rule to attempt this proof and the resulting premises can be attempted using 1000 left-introduction rules.

For example,

$$\dfrac{\dfrac{\Gamma, B_1, C_1, C_2 \vdash A}{\Gamma, B_1, C_1 \wedge C_2 \vdash A}\,\wedge L \quad \dfrac{\Gamma, B_2, C_1, C_2 \vdash A}{\Gamma, B_2, C_1 \wedge C_2 \vdash A}\,\wedge L}{\Gamma, B_1 \vee B_2, C_1 \wedge C_2 \vdash A}\,\vee L$$

is one is about a million choices.

- Another choice switches the order of $\vee L$ and $\wedge L$: that switch is **not important**.
- Also these two inference rules are *invertible* and can be applied automatically; without needing to reconsider them.

Problems with the sequent calculus

Inference rules in the sequent calculus are

- too tiny,
- too independent from each other, and
- not the right inference rules is many settings.

For example, it is more common to need inference rules such as one of the following pairs of rules.

$$\frac{\Gamma \vdash \mathit{adj}\ x\ y}{\Gamma \vdash \mathit{path}\ x\ y} \qquad \frac{\Gamma \vdash \mathit{path}\ x\ z \quad \Gamma \vdash \mathit{path}\ z\ y}{\Gamma \vdash \mathit{path}\ x\ y}$$

$$\frac{\Gamma, \mathit{adj}\ x\ y, \mathit{path}\ x\ y \vdash A}{\Gamma, \mathit{adj}\ x\ y \vdash A} \qquad \frac{\Gamma, \mathit{path}\ x\ z, \mathit{path}\ z\ y, \mathit{path}\ x\ y \vdash A}{\Gamma, \mathit{path}\ x\ z, \mathit{path}\ z\ y \vdash A}$$

NB: these inference rules mention no occurrences of logical connectives.

A better perspective on sequent calculus proofs

Describe this situation to a computer scientist and he will say

> *Give sequent calculus the distinguished role of* assembly language *for proof systems. Our job is to* compile *a wide range of inference rules into that assembly language.*

Describe this situation to a proof theorist and she will say

> *We need to develop an approach to synthetic inference rules.*

Hopefully,

- the results from both perspectives formally yields the same thing, and
- the good properties (e.g., cut-elimination) also hold for the higher-level proof systems.

Main ingredients in focused proof systems

- Specific control on weakening and contraction
- Additive and multiplicative distinctions for some inference rules becomes apparent (and we want both).

$$\frac{\Gamma \vdash B_1 \quad \Gamma \vdash B_2}{\Gamma \vdash B_1 \wedge B_2} \quad \text{additive vs multiplicative} \quad \frac{\Gamma_1 \vdash B_1 \quad \Gamma_2 \vdash B_2}{\Gamma_1, \Gamma_2 \vdash B_1 \wedge B_2}$$

- Identify and always apply invertible introduction rules.
- The non-invertible rules can consume external information. Chain these rules one after another.

$$\frac{\Gamma \vdash B_i}{\Gamma \vdash B_0 \vee B_1} \text{ needs a bit from an oracle}$$

The first focused proof system with these ingredients was given by Andreoli in JLC, 1992.

Polarization terminology: an apology

- invertible — asynchronous — negative — $\Uparrow$
- non-invertible — synchronous — positive — $\Downarrow$

Do not confuse with "negative occurrence" and "positive occurrence".

In linear logic, the de Morgan dual of an asynchronous connective is a synchronous connective.

In classical and intuitionistic logic, the polarized connectives are the following:

- positive: $\exists$, $\wedge^+$, t^+, $\vee^+$, f^+,
- negative: $\forall$, $\wedge^-$, t^-,
  - In classical logic: $\vee^-$, f^-,
  - In intuitionistic logic: $\supset$,

Even atomic formulas are polarized

$$\frac{\Gamma \vdash a \qquad \Gamma, b \vdash G}{\Gamma, a \supset b \vdash G} \text{ where } a, b \text{ are atoms}$$

Negative protocol: The right branch is trivial; i.e., $b = G$.
Continue with $\Gamma \vdash a$ (backward chaining).
Positive protocol: The left branch is trivial; i.e., $\Gamma = \Gamma', a$.
Continue with $\Gamma', a, b \vdash G$ (forward chaining).

Let Γ contain $\mathit{fib}(0, 0)$, $\mathit{fib}(1, 1)$, and

$$\forall n \forall f \forall f' [\mathit{fib}(n, f) \supset \mathit{fib}(n + 1, f') \supset \mathit{fib}(n + 2, f + f')].$$

The nth Fibonacci number is F iff $\Gamma \vdash \mathit{fib}(n, F)$.

Negative protocol: the unique proof is *exponential* in n.
Positive protocol: the shortest proof is *linear* in n.

LJF: Two kinds of focused sequent

$\Downarrow$ sequents, used to specify the formula under focus

$\Gamma \Downarrow B \vdash E$ with a left focus on B
$\Gamma \vdash B \Downarrow$ with a right focus on B

If such a sequent is the conclusion of an introduction rule, then that rule introduced B.

$\Uparrow$ sequents used with invertible introduction rules

$\Gamma \Uparrow \Theta \vdash \Delta_1 \Uparrow \Delta_2$
The multiset union of Δ_1 and Δ_2 contains at most one formula.
The two zones Θ and Δ_1 are treated as *lists*: if the zone Θ is non-empty, introduce the first member of Θ; otherwise introduce the first member of Δ_1.

The sequent $\Gamma \Uparrow \cdot \vdash \cdot \Uparrow \Delta$ is called a *border* sequent.

LJF: Asynchronous Introduction Rules

$$\frac{\Gamma \Uparrow B_1 \vdash B_2 \Uparrow}{\Gamma \Uparrow \cdot \vdash B_1 \supset B_2 \Uparrow} \qquad \frac{\Gamma \Uparrow \cdot \vdash B_1 \Uparrow \quad \Gamma \Uparrow \cdot \vdash B_2 \Uparrow}{\Gamma \Uparrow \cdot \vdash B_1 \wedge^- B_2 \Uparrow} \qquad \frac{}{\Gamma \Uparrow \cdot \vdash t^- \Uparrow}$$

$$\frac{}{\Gamma \Uparrow \Theta, f^+ \vdash \Delta_1 \Uparrow \Delta_2} \qquad \frac{\Gamma \Uparrow \Theta, B_1 \vdash \Delta_1 \Uparrow \Delta_2 \quad \Gamma \Uparrow \Theta, B_2 \vdash \Delta_1 \Uparrow \Delta_2}{\Gamma \Uparrow \Theta, B_1 \vee^+ B_2 \vdash \Delta_1 \Uparrow \Delta_2}$$

$$\frac{\Gamma \Uparrow \Theta, B_1, B_2 \vdash \Delta_1 \Uparrow \Delta_2}{\Gamma \Uparrow \Theta, B_1 \wedge^+ B_2 \vdash \Delta_1 \Uparrow \Delta_2} \qquad \frac{\Gamma \Uparrow \Theta \vdash \Delta_1 \Uparrow \Delta_2}{\Gamma \Uparrow \Theta, t^+ \vdash \Delta_1 \Uparrow \Delta_2}$$

$$\frac{\Gamma \Uparrow \cdot \vdash [y/x]B \Uparrow}{\Gamma \Uparrow \cdot \vdash \forall x.B \Uparrow}\ \dagger \qquad \frac{\Gamma \Uparrow \Theta, [y/x]B \vdash \Delta_1 \Uparrow \Delta_2}{\Gamma \Uparrow \Theta, \exists x.B \vdash \Delta_1 \Uparrow \Delta_2}\ \dagger$$

Here, Γ and Δ_2 ranges over multisets of polarized formulas,
Θ and Δ_1 ranges over *lists* of polarized formulas

† The usual eigenvariable restriction applies to y.

LJF: Synchronous Introduction Rules

$$\frac{\Gamma \Downarrow [t/x]B \vdash E}{\Gamma \Downarrow \forall x.B \vdash E} \qquad \frac{\Gamma \vdash [t/x]B \Downarrow}{\Gamma \vdash \exists x.B \Downarrow}$$

$$\frac{\Gamma \vdash B_i \Downarrow}{\Gamma \vdash B_1 \vee^+ B_2 \Downarrow} \qquad \frac{\Gamma \Downarrow B_i \vdash E}{\Gamma \Downarrow B_1 \wedge^- B_2 \vdash E}\ i \in \{1,2\}$$

$$\frac{\Gamma \vdash B_1 \Downarrow \quad \Gamma \Downarrow B_2 \vdash E}{\Gamma \Downarrow B_1 \supset B_2 \vdash E}$$

$$\frac{}{\Gamma \vdash t^+ \Downarrow}\ \ddagger \qquad \frac{\Gamma \vdash B_1 \Downarrow \quad \Gamma \vdash B_2 \Downarrow}{\Gamma \vdash B_1 \wedge^+ B_2 \Downarrow}$$

Here, E denotes either a positive formula or a negative atom.

LJF: Identity rules and Structural rules

Initial: $\dfrac{N \text{ atomic}}{\Gamma \Downarrow N \vdash N}\, I_l \qquad \dfrac{P \text{ atomic}}{\Gamma, P \vdash P \Downarrow}\, I_r$

Cut: $\dfrac{\Gamma \Uparrow \cdot \vdash B \Uparrow \cdot \qquad \Gamma \Uparrow B \vdash \cdot \Uparrow E}{\Gamma \Uparrow \cdot \vdash \cdot \Uparrow E}\, Cut$

Decide: $\dfrac{\Gamma, N \Downarrow N \vdash E}{\Gamma, N \Uparrow \cdot \vdash \cdot \Uparrow E}\, D_l \qquad \dfrac{\Gamma \vdash P \Downarrow}{\Gamma \Uparrow \cdot \vdash \cdot \Uparrow P}\, D_r$

Release: $\dfrac{\Gamma \Uparrow P \vdash \cdot \Uparrow E}{\Gamma \Downarrow P \vdash E}\, R_l \qquad \dfrac{\Gamma \Uparrow \cdot \vdash N \Uparrow \cdot}{\Gamma \vdash N \Downarrow}\, R_r$

Store: $\dfrac{\Gamma, C \Uparrow \Theta \vdash \Delta_1 \Uparrow \Delta_2}{\Gamma \Uparrow \Theta, C \vdash \Delta_1 \Uparrow \Delta_2}\, S_l \qquad \dfrac{\Gamma \Uparrow \cdot \vdash \cdot \Uparrow E}{\Gamma \Uparrow \cdot \vdash E \Uparrow \cdot}\, S_r$

Here, P is a positive formula; N is a negative formula; C is either a negative formula or a positive atom; and B is an unrestricted polarized formula.

How to polarize a formula

- atomic formulas are labeled either "positive" or "negative"
- replace all occurrences of true with either t^+ or t^- and of conjunction with either $\wedge^+$ or $\wedge^-$. (If there are n occurrences of truth and conjunction in B, there are 2^n ways to do this replacement.)
- rename false and disjunction as f^+ and $\vee^+$

positive connectives are f^+, $\vee^+$, t^+, $\wedge^+$, and $\exists$
negative connectives are t^-, $\wedge^-$, $\supset$, and $\forall$.

A formula is *positive* if it is a positive atom or has a top-level positive connective; a formula is *negative* if it is a negative atom or has a top-level negative connective.

Formal results about **LJF**

Theorem: Let B be a first-order intuitionistic logic formula.

- If $\vdash B$ then for every polarization $\hat{B}$ of B, $\cdot \Uparrow \cdot \vdash \hat{B} \Uparrow \cdot$.
- If $\hat{B}$ is a polarized version of B and $\cdot \Uparrow \cdot \vdash \hat{B} \Uparrow \cdot$, then $\vdash B$.

Proof: See Liang & M [TCS 2009]. Based on linear logic.

Polarization does not affect provability but can make a big impact on the structure of proofs.

LJF generalizes the MJ sequent system of J. M. Howe's 1998 PhD. The completeness of **LJF** yields the completeness:

- LJT [Herbelin's PhD, 1995]
- LJQ/LJQ' [Dyckhoff & Lengrand, CiE, 2006]
- λRCC [Jagadeesan, Nadathur & Saraswat, 2005, FSTTCS]
- **LKF**, a focused proof system for classical logic

Synthetic rules

Synthetic rules result from looking only at border sequents. That is, a synthetic rule is built from a collect of focused rules in which the conclusion and the premises are border sequents.

$$\dfrac{\begin{array}{ccc} \ldots & \Gamma_i \Uparrow \cdot \vdash \cdot \Uparrow \Delta_i & \ldots \\ \ldots & \Uparrow & \ldots \\ \ldots & \vdots & \ldots \\ \ldots & \Downarrow & \ldots \end{array}}{\Gamma \Uparrow \cdot \vdash \cdot \Uparrow \Delta}\ \textit{decide}$$

The corresponding synthetic rule is of the form

$$\dfrac{\ldots \quad \Gamma_i \vdash \Delta_i \quad \ldots}{\Gamma \vdash \Delta}$$

Of course, the polarized formulas here need to be replaced by their corresponding unpolarized form.

Geometric formulas

$$\forall \overline{z}(P_1 \wedge \ldots \wedge P_m \supset$$

$$(\exists x_1(Q_{11} \wedge \ldots \wedge Q_{1k_1}) \vee \ldots \vee \exists x_n(Q_{n1} \wedge \ldots \wedge Q_{nk_n})))$$

This geometric formula can be polarized in **LJF** as

$$\forall \overline{z}(P_1 \wedge^+ \ldots \wedge^+ P_m \supset$$

$$(\exists x_1(Q_{11} \wedge^+ \ldots \wedge^+ Q_{1k_1}) \vee^+ \ldots \vee^+ \exists x_n(Q_{n1} \wedge^+ \ldots \wedge^+ Q_{nk_n})))$$

Here, P_i and Q_{jk} are relational atoms.
This polarized formula is a *bipole*: outermost negative connectives around positive formulas. The resulting synthetic rule:

$$\frac{\overline{Q_1}(y_1/x_1), \overline{P}, \Gamma \vdash \Delta \quad \ldots \quad \overline{Q_n}(y_n/x_n), \overline{P}, \Gamma \vdash \Delta}{\overline{P}, \Gamma \vdash \Delta}$$

See: S. Negri. Proof analysis in modal logic. J. Philos. Logic, 2005

Compiling modal logic proof systems

We can "compile" many modal logics inference rules faithfully. [The following illustrates what is possible.]

$$\frac{xRy, \Gamma \vdash \Delta, x : \Diamond A, y : A}{xRy, \Gamma \vdash \Delta, x : \Diamond A}\ R\Diamond$$

where $\Gamma' = [\Gamma]^{\partial^+}$ and $\Delta' = [\Delta]^{\partial^+}$. Compiled this into **LKF** inferences. These rule yield a synthetic rule.

$$\dfrac{\dfrac{}{\vdash \neg\Gamma', \Delta', \partial^+([\Diamond A^\circ]_x) \Downarrow R(x,y)}\ \mathit{init} \quad \dfrac{\dfrac{\dfrac{\vdash \neg\Gamma', \Delta', \partial^+([\Diamond A^\circ]_x), [A^\circ]_y{}^{\partial^+} \Uparrow \cdot}{\vdash \neg\Gamma', \Delta', \partial^+([\Diamond A^\circ]_x) \Uparrow [A^\circ]_y{}^{\partial^+}}\ \mathit{store}}{\vdash \neg\Gamma', \Delta', \partial^+([\Diamond A^\circ]_x) \Uparrow \partial^-([A^\circ]_y{}^{\partial^+})}\ \partial^-}{\vdash \neg\Gamma', \Delta', \partial^+([\Diamond A^\circ]_x) \Downarrow \partial^-([A^\circ]_y{}^{\partial^+})}\ \mathit{release}}{\dfrac{\dfrac{\dfrac{\vdash \neg\Gamma', \Delta', \partial^+([\Diamond A^\circ]_x) \Downarrow R(x,y) \wedge^+ \partial^-([A^\circ]_y{}^{\partial^+})}{\vdash \neg\Gamma', \Delta', \partial^+([\Diamond A^\circ]_x) \Downarrow \exists y(R(x,y) \wedge^+ \partial^-([A^\circ]_y{}^{\partial^+}))}\ \exists}{\vdash \neg\Gamma', \Delta', \partial^+([\Diamond A^\circ]_x) \Downarrow \partial^+(\exists y(R(x,y) \wedge^+ \partial^-([A^\circ]_y{}^{\partial^+})))}\ \partial^+}{\vdash \neg\Gamma', \Delta', \partial^+([\Diamond A^\circ]_x) \Uparrow \cdot}\ \mathit{decide}}\ \wedge^+$$

See papers by Marin, M, & Volpe in LPAR 2015, AiML 2016.

Delays: $\partial^+(B)$ and $\partial^-(B)$

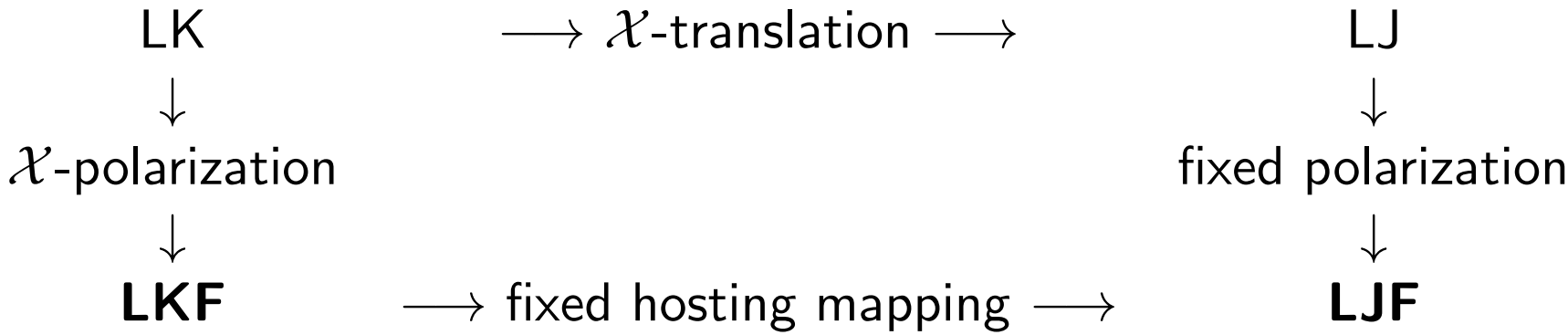
	quantifiers	additive	multiplicative
$\partial^+(B)$	$\exists x.B$	$f^+ \vee^+ B$	$t^+ \wedge^+ B$
$\partial^-(B)$	$\forall x.B$	$t^- \wedge^- B$	$f^- \vee^- B$ or $t^+ \supset B$

Here, x is not free in B.

It is natural to think of delays as 1-arty logical connectives just as units are 0-ary logical connectives.

Delays are useful for shortening $\Uparrow$ and $\Downarrow$ phases.

Negative translations



Here $\mathcal{X}$ can be picked from the set

$$\{ \text{Gödel-Gentzen, Kuroda, Krivine, Kolmogorov} \}$$

The proof structures in **LKF** and **LJF** are essentially identical.

This suggests that negative translations are, in fact, not needed: instead work inside **LKF**.

See HAL technical report by Chihani, Ilik, & M, March 2016.

Parallelism in proofs

Example:

$$D_1: \quad (a \wedge b \supset c) \qquad \frac{a, b, c \vdash}{a, b \vdash}$$

$$D_2: \quad (a \wedge d \supset e) \qquad \frac{a, d, e \vdash}{a, d \vdash}$$

$$D_3: \quad (c \wedge d \supset g) \qquad \frac{c, d, g \vdash}{c, d \vdash}$$

$$\dfrac{\dfrac{\dfrac{\Gamma, a, b, c, d, e, g \vdash E}{\Gamma, a, b, c, d, e \vdash E}\, D_3}{\Gamma, a, b, c, d \vdash E}\, D_2}{\Gamma, a, b, d \vdash E}\, D_1$$

But: D_1 and D_2 can be applied in the other order as well as in **parallel**. It is possible to allow *multifocusing*: e.g.,

$$\dfrac{\dfrac{\Gamma, a, b, c, d, e \Uparrow \cdot \vdash \cdot \Uparrow E}{\Gamma, a, b, d \Downarrow D_1, D_2 \vdash E}\, \textit{various rules}}{\Gamma, a, b, d \Uparrow \cdot \vdash \cdot \Uparrow E}\, \textit{decide}$$

Maximal multifocusing

The multifocus zone is treated linearly (no structural rules).

Soundness and completeness for *multifocusing* is trivial.
What meta-theorems can we expect about multifocusing?

(Informal) Definition: A *maximal multifocused* (MMF) proof is a multifocusing proof where no decide rule can be permuted down further in the proof.

Theorems:

- Proof nets in linear logic can be described as MMF in MALL.
- Expansion proofs in classical logic can be described as MMF in **LKF**.

Thus, instead of treating parallelism by a *revolutionary* proof system, we can *evolve* them by starting with sequent calculus.
See: Chaudhuri, Hetzl, & M, JLC, 2016; Chaudhuri, M, & Saurin IFIP TCS 2008.

Related and future topics

Redo other standard proof theory results: after proving the completeness of **LJF** and **LKF**, major permutations arguments should disappear.

Focusing in Peano/Heyting arithmetics: μMALL, μ**LJF**, μ**LKF** (?).

Computer science applications:

- Proof certificates: these are "oracles" to proof checkers. Focused proofs can structure the communications between proof checkers and the certificate.
- Separation of computation ($\Uparrow$ phase) and deduction ($\Downarrow$ phase).
- The proof theory of model checking as μMALL (Heath & M, JAR 2018).