Sequent Calculus: overview and recent developments (Part 1)

Dale Miller

INRIA Saclay & Ecole Polytechnique, France

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

Topics in classical and intuitionistic proof theory with applications to computation.

Interests in the Sequent Calculus

For mathematical logic:

- Gentzen's proof of consistency of first order logics and Peano Arithmetic. Ordinal analysis.

For logic more generally:

- One of several frameworks for describing proofs in many logics.

For computer science:

- A framework for computational logic, especially those involving classical logic.

Many roles of logic in computation

Computation-as-model: Computations happens, *i.e.*, states change, communications occur, *etc*. Logic is used to make statements *about* computation. *E.g.*, Hoare triples, modal logics.

Computation-as-deduction: Elements of logic are used to model elements of computation directly.

Many roles of logic in computation

Computation-as-model: Computations happens, *i.e.*, states change, communications occur, *etc*. Logic is used to make statements *about* computation. *E.g.*, Hoare triples, modal logics.

Computation-as-deduction: Elements of logic are used to model elements of computation directly.

Proof normalization. Programs are proofs and computation is proof normalization (λ-conversion, cut-elimination). A foundations for functional programming. Curry-Howard Isomorphism.

Proof search. Programs are theories and computation is the search for sequent proofs. A foundations for logic programming, model checking, and theorem proving.

We focus on two logics

There are great many "logics" used in practice and in research.

Implemented computational logic systems demand selecting one of two logics: *Classical Logic* and *Intuitionistic Logic*.

These two choices covers a large percentage of existing computational systems based on logic.

Although **Linear Logic** lies *behind* these two logics, we will speak about this logic only indirectly.

We focus on two logics

There are great many "logics" used in practice and in research.

Implemented computational logic systems demand selecting one of two logics: *Classical Logic* and *Intuitionistic Logic*.

These two choices covers a large percentage of existing computational systems based on logic.

Although **Linear Logic** lies *behind* these two logics, we will speak about this logic only indirectly.

Given our focus on proofs, the choice of

propositional vs first-order vs higher-order

logic is not a concern here: HO logic can directly support both all three.

Logics with recursive definitions

We will eventually add recursive definitions to classical logic (using a fixed point connective). We identify three different activities viz a viz the use of fixed points.

- computation (*a la* logic programming): "There a exists a path in an unfolding."
- model checking: "For all paths, there exist a path."
- theorem prover: Use rules for induction and co-induction instead of just unfold.

Sequent calculus provides a common framework for mixing

- computation and deduction, and
- model checking and theorem proving.

Terms and formulas

Formally, we use Church's Simple Theory of Types [1940] to encode terms and formulas.

Informally, terms and formulas are first-order with occasional and natural uses of higher-order abstractions via λ-abstraction.

Equality via α-conversion useful for comparing formulas.

Equality via β-conversion useful for specifying substitution.

Sequents

Sequents are triples $\Sigma : \Gamma \vdash \Delta$ where

- Σ, the *signature* of the sequent, is a set of (eigen) variables (with scope over the sequent);
- Γ, the *left-hand-side*, is a multiset of formulas; and
- Δ, the *right-hand-side*, is a multiset of formulas.

NB: Gentzen used lists instead of multisets.

Inference rules: two structural rules

There are two sets of these: *contraction, weakening*.

$$\frac{\Sigma : \Gamma, B, B \vdash \Delta}{\Sigma : \Gamma, B \vdash \Delta}\ cL \qquad \frac{\Sigma : \Gamma \vdash \Delta, B, B}{\Sigma : \Gamma \vdash \Delta, B}\ cR$$

$$\frac{\Sigma : \Gamma \vdash \Delta}{\Sigma : \Gamma, B \vdash \Delta}\ wL \qquad \frac{\Sigma : \Gamma \vdash \Delta}{\Sigma : \Gamma \vdash \Delta, B}\ wR$$

NB: Gentzen's use of lists of formulas required him to also have an *exchange* rule.

Inference rules: two identity rules

There are exactly two: *initial, cut*.

$$\frac{}{\Sigma\colon B \vdash B}\ init \qquad \frac{\Sigma\colon \Gamma_1 \vdash \Delta_1, B \qquad \Sigma\colon B, \Gamma_2 \vdash \Delta_2}{\Sigma\colon \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ cut$$

Notice the repeated use of the variable B in these rules.

In general: all instances of both of these rules can be *eliminated* except for *init* when B is atomic.

Inference rules: introduction rules (some examples)

$$\frac{\Sigma : \Gamma, B_i \vdash \Delta}{\Sigma : \Gamma, B_1 \wedge B_2 \vdash \Delta} \wedge L \qquad \frac{\Sigma : \Gamma \vdash \Delta, B \qquad \Sigma : \Gamma \vdash \Delta, C}{\Sigma : \Gamma \vdash \Delta, B \wedge C} \wedge R$$

$$\frac{\Sigma : \Gamma, B \vdash \Delta \qquad \Sigma : \Gamma, C \vdash \Delta}{\Sigma : \Gamma, B \vee C \vdash \Delta} \vee L \qquad \frac{\Sigma : \Gamma \vdash \Delta, B_i}{\Sigma : \Gamma \vdash \Delta, B_1 \vee B_2} \vee R$$

$$\frac{\Sigma : \Gamma_1 \vdash \Delta_1, B \qquad \Sigma : \Gamma_2, C \vdash \Delta_2}{\Sigma : \Gamma_1, \Gamma_2, B \supset C \vdash \Delta_1, \Delta_2} \supset L \qquad \frac{\Sigma : \Gamma, B \vdash \Delta, C}{\Sigma : \Gamma \vdash \Delta, B \supset C} \supset R$$

$$\frac{\Sigma \vdash t : \tau \qquad \Sigma : \Gamma, B[t/x] \vdash \Delta}{\Sigma : \Gamma, \forall_\tau x\, B \vdash \Delta} \forall L \qquad \frac{\Sigma, y : \tau \ : \ \Gamma \vdash \Delta, B[y/x]}{\Sigma : \Gamma \vdash \Delta, \forall_\tau x\, B} \forall R$$

$$\frac{\Sigma, y : \tau \ : \ \Gamma, B[y/x] \vdash \Delta}{\Sigma : \Gamma, \exists_\tau x\, B \vdash \Delta} \exists L \qquad \frac{\Sigma \vdash t : \tau \qquad \Sigma : \Gamma \vdash \Delta, B[t/x]}{\Sigma : \Gamma \vdash \Delta, \exists_\tau x\, B} \exists R$$

Additive vs multiplicative inference rules

Inference rules with two or more premises are classified as follows:

Additive: side formulas are the same in premises and conclusion.

$$\frac{\Sigma\colon \Gamma, B \vdash \Delta \qquad \Sigma\colon \Gamma, C \vdash \Delta}{\Sigma\colon \Gamma, B \vee C \vdash \Delta}\ \vee L$$

Multiplicative: side formulas in premises accumulate.

$$\frac{\Sigma\colon \Gamma_1 \vdash \Delta_1, B \quad \Sigma\colon \Gamma_2, C \vdash \Delta_2}{\Sigma\colon \Gamma_1, \Gamma_2, B \supset C \vdash \Delta_1, \Delta_2}\ \supset L$$

These versions are inter-admissible in the presence of contraction and weakening. In linear logic, these adjectives applied to connectives as well.

Permutations of inference rules

$$\dfrac{\dfrac{\Sigma\colon \Gamma, p, r \vdash s, \Delta \qquad \Sigma\colon \Gamma, q, r \vdash s, \Delta}{\Sigma\colon \Gamma, p \vee q, r \vdash s, \Delta}\ \vee L}{\Sigma\colon \Gamma, p \vee q \vdash r \supset s, \Delta}\ \supset R$$

$$\dfrac{\dfrac{\Sigma\colon \Gamma, p, r \vdash s, \Delta}{\Sigma\colon \Gamma, p \vdash r \supset s, \Delta}\ \supset R \qquad \dfrac{\Sigma\colon \Gamma, q, r \vdash s, \Delta}{\Sigma\colon \Gamma, q \vdash r \supset s, \Delta}\ \supset R}{\Sigma\colon \Gamma, p \vee q \vdash r \supset s, \Delta}\ \vee L$$

Permutations of inference rules (continued)

$$\dfrac{\dfrac{\Sigma\colon \Gamma_1, r \vdash \Delta_1, p \qquad \Sigma\colon \Gamma_2, q \vdash \Delta_2, s}{\Sigma\colon \Gamma_1, \Gamma_2, p \supset q, r \vdash \Delta_1, \Delta_2, s}\ \supset\mathrm{L}}{\Sigma\colon \Gamma_1, \Gamma_2, p \supset q \vdash \Delta_1, \Delta_2, r \supset s}\ \supset\mathrm{R}$$

To switch the order of these two inference rules requires introduction some weakenings and a contraction.

$$\dfrac{\dfrac{\dfrac{\dfrac{\Sigma\colon \Gamma_1, r \vdash \Delta_1, p}{\Sigma\colon \Gamma_1, r \vdash \Delta_1, p, s}\ wR}{\Sigma\colon \Gamma_1 \vdash \Delta_1, p, r \supset s}\ \supset\mathrm{R} \qquad \dfrac{\dfrac{\Sigma\colon \Gamma_2, q \vdash \Delta_2, s}{\Sigma\colon \Gamma_2, q, r \vdash \Delta_2, s}\ wL}{\Sigma\colon \Gamma_2, q \vdash \Delta_2, r \supset s}\ \supset\mathrm{R}}{\Sigma\colon \Gamma_1, \Gamma_2, p \supset q \vdash \Delta_1, \Delta_2, r \supset s, r \supset s}\ \supset\mathrm{L}}{\Sigma\colon \Gamma_1, \Gamma_2, p \supset q \vdash \Delta_1, \Delta_2, r \supset s}\ cR$$

Provability defined

A **C**-proof (*classical proof*) is any proof using these inference rules.

An **I**-proof (*intuitionistic proof*) is a **C**-proof in which the right-hand side of all sequents contain either 0 or 1 formula.

Let Σ be a given first-order signature over S, let Δ be a finite set of Σ-formulas, and let B be a Σ-formula.

Write $\Sigma; \Delta \vdash_C B$ and $\Sigma; \Delta \vdash_I B$ if the sequent $\Sigma : \Delta \longrightarrow B$ has, respectively, a **C**-proof or an **I**-proof.

Some Exercises

Provide a **C**-proof only if there is no **I**-proof.

1. $[p \wedge (p \supset q) \wedge ((p \wedge q) \supset r)] \supset r$
2. $(p \supset q) \supset (\neg q \supset \neg p)$
3. $(\neg q \supset \neg p) \supset (p \supset q)$
4. $p \vee (p \supset q)$
5. $((r\ a \wedge r\ b) \supset q) \supset \exists x(r\ x \supset q)$
6. $((p \supset q) \supset p) \supset p$ (Pierce's formula)
7. $\exists y \forall x\ (r\ x \supset r\ y)$
8. $\forall x \forall y\ (s\ x\ y) \supset \forall z\ (s\ z\ z)$

N.B. Negation is defined: $\neg B = (B \supset f)$.

Cut elimination: permuting a cut up

$$\dfrac{\dfrac{\dfrac{\Xi_1}{\Sigma\colon \Gamma_1 \vdash A_1, \Delta_1} \quad \dfrac{\Xi_2}{\Sigma\colon \Gamma_1 \vdash A_2, \Delta_1}}{\Sigma\colon \Gamma_1 \vdash A_1 \wedge A_2, \Delta_1}\ \wedge R \qquad \dfrac{\dfrac{\Xi_3}{\Sigma\colon \Gamma_2, A_i \vdash \Delta_2}}{\Sigma\colon \Gamma_2, A_1 \wedge A_2 \vdash \Delta_2}\ \wedge L}{\Sigma\colon \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ cut$$

Here, $i \in \{1, 2\}$. Change this fragment to

$$\dfrac{\dfrac{\Xi_i}{\Sigma\colon \Gamma_1 \vdash A_i, \Delta_1} \quad \dfrac{\Xi_3}{\Sigma\colon \Gamma_2, A_i \vdash \Delta_2}}{\Sigma\colon \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ cut$$

The cut rule is on a smaller formula.

Cut elimination: permuting a cut up

$$\dfrac{\dfrac{\begin{matrix}\Xi_1\\ \Sigma\colon \Gamma_1, A_1 \vdash A_2, \Delta_1\end{matrix}}{\Sigma\colon \Gamma_1 \vdash A_1 \supset A_2, \Delta_1}\supset R \qquad \dfrac{\begin{matrix}\Xi_2\\ \Sigma\colon \Gamma_2 \vdash A_1, \Delta_2\end{matrix} \quad \begin{matrix}\Xi_3\\ \Sigma\colon \Gamma_3, A_2 \vdash \Delta_3\end{matrix}}{\Sigma\colon \Gamma_2, \Gamma_3, A_1 \supset A_2 \vdash \Delta_2, \Delta_3}\supset L}{\Sigma\colon \Gamma_1, \Gamma_2, \Gamma_3 \vdash \Delta_1, \Delta_2, \Delta_3}\ cut$$

This part of the proof can be changed locally to

$$\dfrac{\dfrac{\begin{matrix}\Xi_2\\ \Sigma\colon \Gamma_2 \vdash A_1, \Delta_2\end{matrix} \quad \begin{matrix}\Xi_1\\ \Sigma\colon \Gamma_1, A_1 \vdash A_2, \Delta_1\end{matrix}}{\Sigma\colon \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, A_2}\ cut \qquad \begin{matrix}\Xi_3\\ \Sigma\colon \Gamma_3, A_2 \vdash \Delta_3\end{matrix}}{\Sigma\colon \Gamma_1, \Gamma_2, \Gamma_3 \vdash \Delta_1, \Delta_2, \Delta_3}\ cut$$

Although there are now two cut rules, they are on smaller formulas.

Cut elimination: permuting a cut away

$$\dfrac{\dfrac{\Xi}{\Sigma\colon \Gamma_1 \vdash \Delta, B} \qquad \dfrac{}{\Sigma\colon \Gamma_2, B \vdash B}\ init}{\Sigma\colon \Gamma_1, \Gamma_2 \vdash \Delta, B}\ cut$$

Rewrite this proof to the following.

$$\dfrac{\dfrac{\Xi}{\Sigma\colon \Gamma_1 \vdash \Delta_1, B}}{\Sigma\colon \Gamma_1, \Gamma_2 \vdash \Delta_1, B}\ wL$$

We have removed one occurrence of the cut rule.

N.B. *wL* is not an official rule: one must show that it is admissible.

Cut elimination

Theorem. If a sequent has a **C**-proof (respectively, **I**-proof) then it has a cut-free **C**-proof (respectively, **I**-proof).

This theorem was stated and proved by Gentzen 1935.

Gentzen invented the sequent calculus so that he could formulate one proof of this *Hauptsatz* for both classical *and* intuitionistic logic.

Structural rules were key to describing the difference between these two logics.

Cut elimination

Theorem. If a sequent has a **C**-proof (respectively, **I**-proof) then it has a cut-free **C**-proof (respectively, **I**-proof).

This theorem was stated and proved by Gentzen 1935.

Gentzen invented the sequent calculus so that he could formulate one proof of this *Hauptsatz* for both classical *and* intuitionistic logic.

Structural rules were key to describing the difference between these two logics.

Think to all the other ways you know for describing the difference between them (excluded middle, constructive vs non-constructive, Kripke semantics, etc).

Consequences of cut elimination

Theorem. Logic is consistency: It is impossible for there to be a proof of B and $\neg B$.

Proof. Assume that $\vdash B$ and $B \vdash$ have proofs. By cut, $\vdash$ has a proof. Thus, it also has a cut-free proof, but this is impossible.

Theorem. A cut-free proof system of a sequent is composed only of subformula of formulas in the root sequent.

Proof. Simple inspection of all rules other than cut. (Assuming first-order quantification here.)

Should I eliminate cuts in general?

Consequences of cut elimination

Theorem. Logic is consistency: It is impossible for there to be a proof of B and $\neg B$.

Proof. Assume that $\vdash B$ and $B \vdash$ have proofs. By cut, $\vdash$ has a proof. Thus, it also has a cut-free proof, but this is impossible.

Theorem. A cut-free proof system of a sequent is composed only of subformula of formulas in the root sequent.

Proof. Simple inspection of all rules other than cut. (Assuming first-order quantification here.)

Should I eliminate cuts in general? **NO!** Cut-free proofs of interesting mathematical statement often do not exists in nature.

If you are using cut-free proofs, you are probably modeling computation or model checking.

Addressing various choices doing proof search

Issue 1: The cut-rule can always be chosen.
Solution: Search for only cut-free proofs.

Addressing various choices doing proof search

Issue 1: The cut-rule can always be chosen.
Solution: Search for only cut-free proofs.

Issue 2: The structural rules of weakening and contraction can be applied (almost) anytime.
Solution: Build these rules into the other rules.

Addressing various choices doing proof search

Issue 1: The cut-rule can always be chosen.
Solution: Search for only cut-free proofs.

Issue 2: The structural rules of weakening and contraction can be applied (almost) anytime.
Solution: Build these rules into the other rules.

Issue 3: What term to use in the $\exists$R and $\forall$L rules?
Solution: Use logic variables and unification (standard theorem proving technology).

Addressing various choices doing proof search

Issue 1: The cut-rule can always be chosen.
Solution: Search for only cut-free proofs.

Issue 2: The structural rules of weakening and contraction can be applied (almost) anytime.
Solution: Build these rules into the other rules.

Issue 3: What term to use in the $\exists$R and $\forall$L rules?
Solution: Use logic variables and unification (standard theorem proving technology).

Issue 4: Of the thousands of non-atomic formulas in a sequent, which should be selected for introduction?
Solution:

Addressing various choices doing proof search

Issue 1: The cut-rule can always be chosen.
Solution: Search for only cut-free proofs.

Issue 2: The structural rules of weakening and contraction can be applied (almost) anytime.
Solution: Build these rules into the other rules.

Issue 3: What term to use in the $\exists$R and $\forall$L rules?
Solution: Use logic variables and unification (standard theorem proving technology).

Issue 4: Of the thousands of non-atomic formulas in a sequent, which should be selected for introduction?
Solution: Good question. We concentrate on this issue next using

focused proof systems. .

Some "focusing" behavior

Given the inference figure (a variant of ⊃L), where A is atomic.

$$\frac{\Gamma \longrightarrow G \qquad \Gamma, D \overset{\Xi}{\longrightarrow} A}{\Gamma \longrightarrow A}\text{, provided } G \supset D \in \Gamma$$

can we restrict what is the last inference rule in Ξ?
In intuitionistic logic, we can insist that Ξ ends with either

- an introduction rule for D (if D is not atomic) or
- an initial rule with $A = D$ (if D is atomic).

Backchaining as focusing behavior

Let D be the formula (for atomic A')

$$\forall \bar{x}_1(G_1 \supset \forall \bar{x}_2(G_2 \supset \cdots \forall \bar{x}_n(G_n \supset A')\ldots))$$

and consider the sequent $\Sigma\colon \Gamma, D \vdash A$, for atomic A.

We can insist that if one applies a left introduction rule on D, the it cascades into a series of $\forall$L, $\supset$L, and initial rule.

That is, there is a substitution θ such that $A = A'\theta$ and $\Sigma\colon \Gamma \vdash G_i\theta$ are provable $(i = 1, \ldots, n)$.

This cascade of introduction rules will be called a "focus".

Backward and Forward Chaining

$$\frac{\Gamma \longrightarrow a \qquad \Gamma, b \longrightarrow G}{\Gamma, a \supset b \longrightarrow G}$$ a, b are atoms, focus on $a \supset b$

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

Let G be $fib(n, f)$ and let Γ contain $fib(0, 0)$, $fib(1, 1)$, and

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

The nth Fibonacci number is F iff $\Gamma \vdash G$.
If $fib(\cdot, \cdot)$ is negative then the unique proof is *exponential* in n.
If $fib(\cdot, \cdot)$ is positive then the shortest proof is *linear* in n.