Finding Unity in Computational Logic

Dale Miller

INRIA-Saclay & LIX, École Polytechnique
Palaiseau, France

ISCL: International School on Computational Logic
Bertinoro, 11-15 April 2011

Lecture 3: Some slides about proof theory for logic programming.

A single proof system for classical and intuitionistic logic

Sequents are of the form $\Sigma\colon \Gamma \vdash \Delta$, where Γ is a *set* of formulas and Δ is a *multiset* of formulas.

Weakening and contraction on the left is "built in" and is explicit on the right.

Structural rules

$$\frac{\Sigma\colon \Gamma \vdash \Delta}{\Sigma\colon \Gamma \vdash \Delta, B}\ wR \qquad \frac{\Sigma\colon \Gamma \vdash \Delta, B, B}{\Sigma\colon \Gamma \vdash \Delta, B}\ cR$$

Identity rules

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

The introduction rules

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

$$\frac{\Sigma\colon \Gamma \vdash \Delta, B \qquad \Sigma\colon \Gamma \vdash \Delta, C}{\Sigma\colon \Gamma \vdash \Delta, B \wedge C}\ \wedge R \qquad \frac{}{\Sigma\colon \Gamma \vdash \top}\ \top R$$

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

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

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

The introduction rules (the quantifiers)

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

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

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.

Exercise 8 (page 17)

Provide a **C**-proof only if there is no **I**-proof. Assume that the signature for non-logical constants is $\{p\colon o,\ q\colon o,\ r\colon i \to o,\ s\colon i \to i \to o,\ a\colon i,\ b\colon i\}$.

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: $\neg B = (B \supset \bot)$.

Cut elimination: permuting a cut up

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

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

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

The cut rule is on a smaller formula.

Cut elimination: permuting a cut up

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

This part of the proof can be changed locally to

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

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

Cut elimination: permuting a cut away

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

Rewrite this proof to the following.

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

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.

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. But 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.

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. But 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.

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

If you are using cut-free proofs, you are probably modeling computation (like modeling the execution of a Turing machine).

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 select to introduce?
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 select to introduce?
Solution: Good question. We concentrate on this question soon.

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 select to introduce?
Solution: Good question. We concentrate on this question soon.

Horn clauses: three presentations

$$\begin{aligned} G ::= &\quad A \mid G \wedge G \\ D ::= &\quad A \mid G \supset A \mid \forall x\, D. \end{aligned} \tag{1}$$

Program clauses in this style presentation are formulas of the form

$$\forall x_1 \ldots \forall x_n (A_1 \wedge \cdots \wedge A_m \supset A_0),$$

Horn clauses: three presentations

$$\begin{aligned} G &::= \quad A \mid G \wedge G \\ D &::= A \mid G \supset A \mid \forall x\, D. \end{aligned} \tag{1}$$

Program clauses in this style presentation are formulas of the form

$$\forall x_1 \ldots \forall x_n (A_1 \wedge \cdots \wedge A_m \supset A_0),$$

Disjunction and existentials can be permitted in goal formulas.

$$\begin{aligned} G &::= \top \mid A \mid G \wedge G \mid G \vee G \mid \exists x\, G \\ D &::= A \mid G \supset D \mid D \wedge D \mid \forall x\, D. \end{aligned} \tag{2}$$

Horn clauses: three presentations

$$\begin{aligned} G &::= \quad A \mid G \wedge G \\ D &::= \quad A \mid G \supset A \mid \forall x\ D. \end{aligned} \tag{1}$$

Program clauses in this style presentation are formulas of the form

$$\forall x_1 \ldots \forall x_n (A_1 \wedge \cdots \wedge A_m \supset A_0),$$

Disjunction and existentials can be permitted in goal formulas.

$$\begin{aligned} G &::= \quad \top \mid A \mid G \wedge G \mid G \vee G \mid \exists x\ G \\ D &::= \quad A \mid G \supset D \mid D \wedge D \mid \forall x\ D. \end{aligned} \tag{2}$$

A compact presentation of Horn clauses and goals is:

$$\begin{aligned} G &::= \quad A \\ D &::= \quad A \mid A \supset D \mid \forall x\ D. \end{aligned} \tag{3}$$

No occurrences of logical connectives to the left of an implication.

Horn clauses in classical and intuitionistic logic

Let Σ be a signature, let $\mathcal{P}$ be a set of Horn clauses, and let Γ be a multiset Horn goals.

Proposition. If $\Sigma : \mathcal{P} \vdash \Gamma$ has a cut-free **C**-proof then there is a $G \in \Gamma$ such that $\Sigma : \mathcal{P} \vdash G$ has an **I**-proof.

Proved by a simple induction on the structure of **C**-proofs.

Let Σ be a signature, let $\mathcal{P}$ be a set of Horn clauses, and let Γ be a multiset Horn goals.

Proposition. If $\Sigma : \mathcal{P} \vdash \Gamma$ has a cut-free **C**-proof then there is a $G \in \Gamma$ such that $\Sigma : \mathcal{P} \vdash G$ has an **I**-proof.

Proved by a simple induction on the structure of **C**-proofs.

Proposition. Any set of Horn clauses is consistent.
Proof. By the above Proposition, $\Sigma; \mathcal{P} \vdash_C \quad$ is impossible.

hereditary Harrop formulas: three presentations

$$
\begin{aligned}
G &::= \quad A \mid G \wedge G \mid D \supset G \mid \forall_\tau x.G \\
D &::= \quad A \mid G \supset A \mid \forall x.D
\end{aligned} \tag{4}
$$

Again, disjunctions and existentials are allowed in goal formulas.

$$
\begin{aligned}
G &::= \quad \top \mid A \mid G \wedge G \mid G \vee G \mid \exists x.G \mid D \supset G \mid \forall x.G \\
D &::= \quad A \mid G \supset D \mid D \wedge D \mid \forall x.D
\end{aligned} \tag{5}
$$

A more compact presentation is:

$$
\begin{aligned}
G &::= \quad A \mid D \supset G \mid G \wedge G \mid \forall x.G \\
D &::= \quad A \mid G \supset D \mid D \wedge D \mid \forall x.D
\end{aligned} \tag{6}
$$

These provide a foundation for the λProlog programming language.

A new proof system for intuitionistic logic: right rules

The single conclusion version of the rules we listed before.

$$\frac{\Sigma\colon \Gamma \vdash B \qquad \Sigma\colon \Gamma \vdash C}{\Sigma\colon \Gamma \vdash B \wedge C}\ \wedge R \qquad \frac{}{\Sigma\colon \Gamma \vdash \top}\ \top R$$

$$\frac{\Sigma\colon \Gamma \vdash B}{\Sigma\colon \Gamma \vdash B \vee C}\ \vee R \qquad \frac{\Sigma\colon \Gamma \vdash C}{\Sigma\colon \Gamma \vdash B \vee C}\ \vee R$$

$$\frac{\Sigma\colon B, \Gamma \vdash C}{\Sigma\colon \Gamma \vdash B \supset C}\ \supset R$$

$$\frac{\Sigma, c\colon i\ \colon \Gamma \vdash B[c/x]}{\Sigma\colon \Gamma \vdash \forall x\ B}\ \forall R \qquad \frac{\Sigma\colon \Gamma \vdash B[t/x]}{\Sigma\colon \Gamma \vdash \exists x\ B}\ \exists R$$

A new proof system for intuitionistic logic: left rules

$$\frac{\Sigma : \mathcal{P} \xrightarrow{D} A}{\Sigma : \mathcal{P} \vdash A}\ \textit{decide} \qquad \frac{}{\Sigma : \mathcal{P} \xrightarrow{A} A}\ \textit{init}$$

$$\frac{\Sigma : \mathcal{P} \xrightarrow{D_1} A}{\Sigma : \mathcal{P} \xrightarrow{D_1 \wedge D_2} A}\ \wedge L \qquad \frac{\Sigma : \mathcal{P} \xrightarrow{D_2} A}{\Sigma : \mathcal{P} \xrightarrow{D_1 \wedge D_2} A}\ \wedge L$$

$$\frac{\Sigma : \mathcal{P} \vdash G \qquad \Sigma : \mathcal{P} \xrightarrow{D} A}{\Sigma : \mathcal{P} \xrightarrow{G \supset D} A}\ \supset L \qquad \frac{\Sigma : \mathcal{P} \xrightarrow{D[t/x]} A}{\Sigma : \mathcal{P} \xrightarrow{\forall_\tau x.D} A}\ \forall L$$

These rules capture the notions of *goal-directed search* and *backchaining*.

Now, the bigger questions

- Can we provide restrictions on proofs to more of logic?
- Can we account for *program-directed search* (more generally called bottom-up search)?
- Can we account for *all* of intuitionistic logic? and classical logic?