INF 542: Logic and Computability

Lecture 8 — D. Miller

24.11.2006

Outline

1. Review of two-sided sequent calculus
2. One-sided sequent calculus
3. Models, Herbrand models
4. Soundness theorem
5. Completeness theorem

Sequent calculus

A calculus introduced by G. Gentzen in 1936 in order to prove a fundamental theorem of logic.

A *sequent* of $\mathcal{F}$ is a triple $\Sigma : \Gamma \longrightarrow \Delta$, where Σ is a first-order signature and Γ and Δ are finite (possibly empty) multisets of Σ-formulas.

The multiset Γ is this sequent's *antecedent* and Δ is its *succedent*. The expressions Γ, B and B, Γ denote the multiset union $\Gamma \cup \{B\}$.

A first-order *signature* Σ is a set of first-order typed variables. A Σ-formula is a formula all of whose free variables are contain in the set Σ.

Sequent calculus: Initial and cut rules

$$\frac{}{\Sigma \;:\; B \;\longrightarrow B}\; \mathit{initial} \qquad \frac{\Sigma \;:\; \Delta_1 \;\longrightarrow \Gamma_1, B \qquad \Sigma \;:\; B, \Delta_2 \;\longrightarrow \Gamma_2}{\Sigma \;:\; \Delta_1, \Delta_2 \;\longrightarrow \Gamma_1, \Gamma_2}\; \mathrm{cut}$$

Sequent calculus: Structural rules

$$\frac{\Sigma \;:\; \Delta \;\longrightarrow \Gamma}{\Sigma \;:\; \Delta, B \;\longrightarrow \Gamma}\; \mathrm{weakL} \qquad \frac{\Sigma \;:\; \Delta \;\longrightarrow \Gamma}{\Sigma \;:\; \Delta \;\longrightarrow \Gamma, B}\; \mathrm{weakR}$$

$$\frac{\Sigma \;:\; \Delta, B, B \;\longrightarrow \Gamma}{\Sigma \;:\; \Delta, B \;\longrightarrow \Gamma}\; \mathrm{contrL} \qquad \frac{\Sigma \;:\; \Delta \;\longrightarrow \Gamma, B, B}{\Sigma \;:\; \Delta \;\longrightarrow \Gamma, B}\; \mathrm{contrR}$$

Sequent calculus: Introduction rules

$$\frac{\Sigma : B, \Delta \longrightarrow \Gamma}{\Sigma : B \wedge C, \Delta \longrightarrow \Gamma} \wedge L \qquad \frac{\Sigma : C, \Delta \longrightarrow \Gamma}{\Sigma : B \wedge C, \Delta \longrightarrow \Gamma} \wedge L$$

$$\frac{\Sigma : \Delta \longrightarrow \Gamma, B \qquad \Sigma : \Delta \longrightarrow \Gamma, C}{\Sigma : \Delta \longrightarrow \Gamma, B \wedge C} \wedge R$$

$$\frac{\Sigma : B, \Delta \longrightarrow \Gamma \qquad \Sigma : C, \Delta \longrightarrow \Gamma}{\Sigma : B \vee C, \Delta \longrightarrow \Gamma} \vee L$$

$$\frac{\Sigma : \Delta \longrightarrow \Gamma, B}{\Sigma : \Delta \longrightarrow \Gamma, B \vee C} \vee R \qquad \frac{\Sigma : \Delta \longrightarrow \Gamma, C}{\Sigma : \Delta \longrightarrow \Gamma, B \vee C} \vee R$$

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

$$\frac{\Sigma : \Delta, B[t/x] \longrightarrow \Gamma}{\Sigma : \Delta, \forall x\, B \longrightarrow \Gamma} \forall L \qquad \frac{\Sigma \cup \{c\} : \Delta \longrightarrow \Gamma, B[c/x]}{\Sigma : \Delta \longrightarrow \Gamma, \forall x\, B} \forall R$$

$$\frac{\Sigma \cup \{c\} : \Delta, B[c/x] \longrightarrow \Gamma}{\Sigma : \Delta, \exists x\, B \longrightarrow \Gamma} \exists L \qquad \frac{\Sigma : \Delta \longrightarrow \Gamma, B[t/x]}{\Sigma : \Delta \longrightarrow \Gamma, \exists x\, B} \exists R$$

$$\frac{}{\Sigma : \longrightarrow \top} \top R \qquad \frac{}{\Sigma : \bot \longrightarrow} \bot L$$

The Cut-Elimination Theorem

A central result in proof theory (usually desired for any proof system of any logic) is the cut-elimination theorem.

Theorem. If a sequent has a proof then it has a cut-free proof.

In other words: lemmas are not strictly speaking necessary.

An analogy from programming language: Instead of calling a subroutine, you can "in-line" the routine.

Of course, one expects the size of programs (and cut-free proofs) to grow greatly.

Cut-elimination, mathematics, and computation

Cut-free proofs of mathematically interesting theorems “do not exist in nature”. They only exist “in principle”.

The cut-elimination theorem helps to validate a logic as well designed and as consistent.

Proofs without cut have the *subformula property*: any formula in any sequent in a cut-free proof is a subformula of a formula in the end-sequent.

A one-sided sequent calculus for classical logic

Doing meta-theory about proof systems will be easier if we simplify formulas and proofs.

A formula is in *negation normal form* (nnf) if it contains no occurrences of $\supset$ and if negations have only atomic scope.

Any formula can be rewritten to a classically equivalent formula that is in negation normal form by rewriting it by a series of simple equivalences. For example, $\neg\neg B \equiv B$ and $\neg(A \wedge B) \equiv (\neg A \vee \neg B)$.

Now replace the two-side sequent $\Sigma \,:\, \Gamma \longrightarrow \Delta$ with the one-side sequent $\Sigma \,:\, \longrightarrow \neg\Gamma, \Delta$, but this time, assume that all formulas are in negation normal form.

If we write $\neg B$ in a sequent, we mean the negation normal form of $\neg B$.

One-sided sequent proof system

$$\frac{\Sigma : \longrightarrow \Gamma, B \qquad \Sigma : \longrightarrow \Gamma, C}{\Sigma : \longrightarrow \Gamma, B \wedge C}\ \wedge R \qquad \frac{}{\Sigma : \longrightarrow \Gamma, \top}\ \top R$$

$$\frac{\Sigma : \longrightarrow \Gamma, B, C}{\Sigma : \longrightarrow \Gamma, B \vee C}\ \vee R \qquad \frac{\Sigma : \longrightarrow \Gamma}{\Sigma : \longrightarrow \Gamma, \bot}\ \bot R$$

$$\frac{\Sigma \cup \{c\} : \longrightarrow \Gamma, B[c/x]}{\Sigma : \longrightarrow \Gamma, \forall x\ B}\ \forall R \qquad \frac{\Sigma : \longrightarrow \Gamma, B[t/x]}{\Sigma : \longrightarrow \Gamma, \exists x\ B}\ \exists R$$

$$\frac{}{\Sigma : \longrightarrow \Gamma, B, \neg B}\ \text{initial} \qquad \frac{\Sigma : \longrightarrow \Gamma_1, B \qquad \Sigma : \longrightarrow \Gamma_2, \neg B}{\Sigma : \longrightarrow \Gamma_1, \Gamma_2}\ \text{cut}$$

We have organized things so that structural rules are not needed.

All inference rules are now invertible except for the $\exists$R rule. To retain invertibility, one must ensure that $\exists x\ B$ occurs in the upper premise as well as the lower premise (via an implicit use of the contraction rule).

Models for first-order logic

But what do formulas mean? While there are many ways to answer this, a common approach uses the notion of *models*.

We must specify the *domain of quantification*: a set of objects about which quantified variables range and terms denote.

An *interpretation* is a pair $\langle \mathcal{D}, I \rangle$ where $\mathcal{D}$ is a *non-empty* set that serves as the domain of quantification and where I is a mapping from both function and predicate constants to functions:

If f is a function constant of arity n then $I(f) : \mathcal{D}^n \to \mathcal{D}$.

If $n = 0$, then $I(f)$ is some particular element of $\mathcal{D}$.

If p is a predicate constant of arity n then $I(p) : \mathcal{D}^n \to \{\mathtt{t}, \mathtt{f}\}$ (the characteristic function for a subset of $\mathcal{D}^n$.

If $n = 0$ then $I(p)$ is a member of $\{\mathtt{t}, \mathtt{f}\}$.

Variable assignments

A *variable assignment* is a function ϕ from some set variables (the *domain* of ϕ, $\mathrm{dom}(\phi)$) to $\mathcal{D}$.

Let ϕ be a term assignment and let $d \in \mathcal{D}$. By $\phi[d/x]$ we denote the term assignment that is defined for x to have value d. For all values in $\mathrm{dom}(\phi) - \{x\}$, the functions ϕ and $\phi[x/d]$ are identical.

Given an interpretation I and an assignment ϕ, we define the mapping I_ϕ of terms to $\mathcal{D}$ as follows:

If x is a variable, then $I_\phi(x) = \phi(x)$

If f is an n-ary function symbol, then

$$I_\phi(f(t_1, \ldots, t_n)) = I(f)(I_\phi(t_1), \ldots, I_\phi(t_n)),$$

A formula or term is *closed* if it contains no free variables. A formula that is closed is also called a *sentence*.

Interpretation of formulas

We write $\langle \mathcal{D}, I \rangle \models_\phi B$ to denote that the formula B is true (is satisfied) in the interpretation $\langle \mathcal{D}, I \rangle$ and the term assignment ϕ.

When $\mathcal{D}$ is understood, we shall simply write $I \models_\phi B$.

- if B is $p(t_1, \ldots, t_n)$ and $I(p)(I_\phi(t_1), \ldots, I_\phi(t_n)) = \mathtt{t}$ then $I \models_\phi B$;
- $I \models_\phi B_1 \wedge B_2$ if $I \models_\phi B_1$ and $I \models_\phi B_2$;
- $I \models_\phi B_1 \vee B_2$ if $I \models_\phi B_1$ or $I \models_\phi B_2$;
- $I \models_\phi \neg B$ hold if $I \models_\phi B$ does not hold;
- $I \models B_1 \supset B_2$ if not $I \models_\phi B_1$ or $I \models_\phi B_2$;
- $I \models_\phi \forall x.B$ if for all $d \in \mathcal{D}$, $I \models_{\phi'} B$, where ϕ' is $\phi[d/x]$; and
- $I \models_\phi \exists x.B$ if for some $d \in \mathcal{D}$, $I \models_{\phi'} B$, where ϕ' is $\phi[d/x]$.

Models of sentences

B is *satisfiable* if there is an interpretation $\langle \mathcal{D}, I \rangle$ and a term assignment ϕ such that $\langle \mathcal{D}, I \rangle \models_\phi B$. The formula B is *valid* if for every interpretation $\langle \mathcal{D}, I \rangle$ and a term assignment, we have $\langle \mathcal{D}, I \rangle \models_\phi B$.

If B is a sentence then we write $I \models B$ to denote $I \models_\phi B$ where ϕ is the unique term assignment with an empty domain.

An interpretation $\langle \mathcal{D}, I \rangle$ that makes a sentence B true ($\langle \mathcal{D}, I \rangle \models B$) is said to be a *model* for that sentence.

Herbrand interpretations and models

A *Herbrand interpretation* is a first-order interpretation $\langle \mathcal{D}, I \rangle$ where $\mathcal{D}$ is the set of closed terms (over a fixed set of function constants) and

$$I_\phi(f(t_1, \ldots, t_n)) = f(I_\phi(t_1), \ldots, I_\phi(t_n)).$$

It is easy to see that in such an interpretation, term assignments become just substitutions and that $I_\phi(t) = \phi(t)$.

When specifying a Herbrand interpretation, one only needs to specify the interpretation of predicate symbols.

Equivalently: a Herbrand interpretation is specify a set of closed, atomic formulas, say $\mathcal{H}$. Here, $I(p(t_1, \ldots, t_n)) = \mathtt{t}$ if and only if $p(t_1, \ldots, t_n) \in \mathcal{H}$.

Herbrand models are somethings called *term models* since the domain of individuals are terms instead of more abstract objects. For example, in a Herbrand model, the terms $1 + 2$, $2 + 1$, and 3 are three different terms (i.e., syntactic expressions).

Soundness of sequent calculus

Let $\mathcal{M}$ be a Herbrand interpretation and let $\Sigma : \Gamma$ be a sequent, where $\Sigma = \{x_1, \ldots, x_n\}$. We say that $\Sigma : \Gamma$ is *satisfiable* in $\mathcal{M}$ if for every list of terms $t_1, \ldots, t_n$ there is an $F \in \Gamma$ such that $M \models F[t_1/x_1, \ldots, t_n/x_n]$.

We write $\mathcal{M} \models \Sigma : \Gamma$ if $\Sigma : \Gamma$ is satisfiable in $\mathcal{M}$.

A sequent is *unsatisfiable* in $\mathcal{M}$ if it is not satisfiable.

The sequent $\Sigma : \Gamma$ is *valid*, denoted as $\models \Sigma : \Gamma$ if for every interpretation $\mathcal{M}$ we have $\mathcal{M} \models \Sigma : \Gamma$.

The Soundness Theorem: If the sequent $\Sigma : \Gamma$ is provable then it is valid.

This is a fairly straightforward proof by induction on the structure of proofs.

The Completeness Theorem

Proving the converse to soundness, namely, completeness is much more involved.

The Completeness Theorem: If the sequent $\Sigma : \Gamma$ is valid then it is provable.

In fact, we will prove the contrapositive of this statement, namely, that if a sequent does not have a proof then it is not valid. We shall show that an unprovable sequent has a counter-model (an interpretation in which it is false) that is also a Herbrand interpretation.

How can we know that a sequent does not have a proof?