# Proof Theory Seminar
# Assignment 2

Instructor: Deepak Garg

Out: May 3, 2012
Due: May 14, 2012

Please submit your solutions on the due date before class. Both typeset and handwritten solutions are acceptable, either in hardcopy or by email. For help with LaTeX macros, contact the instructor.

## Problem 1: Proofs

Give sequent calculus proofs for the following sequents of intuitionistic logic. The notation $\Rightarrow \varphi$ means $\cdot \Rightarrow \varphi\ \mathsf{conc}$, where $\cdot$ is the empty set.

1. $\Rightarrow (\varphi_1 \supset (\varphi_2 \supset \varphi_3)) \supset ((\varphi_1 \supset \varphi_2) \supset (\varphi_1 \supset \varphi_3))$
2. $\Rightarrow ((\varphi_1 \supset \varphi_2) \vee (\varphi_1 \supset \varphi_3)) \supset (\varphi_1 \supset (\varphi_2 \vee \varphi_3))$

## Problem 2: Formal Proof of Unprovability

In this problem, we will explore formal proofs of unprovability of sequents. Often, such proofs rely on existence of *cycles*: Trying to construct a proof of a sequent backwards brings us back to the same sequent and hence we conclude that there is no proof. For example, suppose we try to find a proof of the (unprovable) sequent $\varphi_1 \supset \varphi_2\ \mathsf{hyp} \Rightarrow \varphi_1\ \mathsf{conc}$. By analyzing the possible rules that can be used to prove this sequent, we determine that any proof of it, if one were to exist, must have the following form:

$$\dfrac{\begin{array}{c}\vdots\\ \varphi_1 \supset \varphi_2\ \mathsf{hyp} \Rightarrow \varphi_1\ \mathsf{conc}\end{array} \qquad \begin{array}{c}\vdots\\ \varphi_1 \supset \varphi_2\ \mathsf{hyp}, \varphi_2\ \mathsf{hyp} \Rightarrow \varphi_1\ \mathsf{conc}\end{array}}{\varphi_1 \supset \varphi_2\ \mathsf{hyp} \Rightarrow \varphi_1\ \mathsf{conc}}\ {\supset}\mathrm{L}$$

Observe that the first premise is exactly the same as the conclusion and it is clear that no matter how hard we try, we won't find a proof because when we try to prove the first premise the same pattern will repeat. The question is: Can we formalize this informal intuition to *prove* that this sequent has no proof? The answer is yes: There exists a proof of unprovability based on an *infinite descent argument*.

Define the depth of a proof $\mathcal{D}$, written $\mathrm{depth}(\mathcal{D})$, as the depth of the tree corresponding to $\mathcal{D}$, i.e., the number of rules in the longest path in $\mathcal{D}$ starting from its conclusion and ending at a leaf. Here's how the infinite descent argument works. Suppose, for the sake of contradiction, that the sequent $\varphi_1 \supset \varphi_2\ \mathsf{hyp} \Rightarrow \varphi_1\ \mathsf{conc}$ has a proof. Choose a proof $\mathcal{D}$ of the sequent which has minimum depth among all proofs of the sequent. Let $\mathrm{depth}(\mathcal{D}) = d$. By case analysis of inference rules, we determine that the proof $\mathcal{D}$ must have the form above and that the first premise of its last rule is also a proof of the same sequent. Because the depth of $\mathcal{D}$ is $d$, the depth of its first premise is at most $d-1$. This is a contradiction because we assumed that no proof of the sequent has a depth less than $d$. Hence, our assumption is incorrect and $\varphi_1 \supset \varphi_2 \;\mathsf{hyp} \Rightarrow \varphi_1 \;\mathsf{conc}$ has no proof. QED.

Now to the problem: Prove formally that the sequent $\cdot \Rightarrow (\varphi_1 \supset (\varphi_2 \vee \varphi_3)) \supset ((\varphi_1 \supset \varphi_2) \vee (\varphi_1 \supset \varphi_3)) \;\mathsf{conc}$ has no proof. [Hint: In addition to infinite descent, you may want to use the fact that contraction is admissible in the sequent calculus and it is structure-preserving (and, hence, also depth-preserving).]

# Problem 3: Admissibility of Cut

**Proof cases** We discussed in class a proof of the following metatheoretic property of the sequent calculus, called admissibility of cut.

- (Admissibility of cut) If $\mathcal{D} :: \Gamma \Rightarrow \varphi \;\mathsf{conc}$ and $\mathcal{E} :: \Gamma, \varphi \;\mathsf{hyp} \Rightarrow \psi \;\mathsf{conc}$, then there exists $\mathcal{F} :: \Gamma \Rightarrow \psi \;\mathsf{conc}$.

The proof of this property is by induction on the order $\langle \varphi, [\mathcal{D}, \mathcal{E}] \rangle$, i.e., the lexicographic order that gives higher priority to $\varphi$ and lower but equal priority to $\mathcal{D}$ and $\mathcal{E}$. We saw in class some of the cases of this proof and also how they could be grouped to reduce the size of the proof. Now, show the following cases of this proof:

1. $\mathcal{D}$ ends in the rule ($\supset$L). How $\mathcal{E}$ ends is irrelevant, as all such cases can be handled uniformly.

2. $\mathcal{E}$ ends in the rule ($\vee$R$_1$). Here, it is irrelevant how $\mathcal{D}$ ends.

3. $\mathcal{E}$ ends in the rule ($\supset$L), but the cut formula $\varphi$ is not principal in the rule. Again, it is irrelevant here how $\mathcal{D}$ ends.

4. $\mathcal{D}$ ends in the rule ($\wedge$R) and $\mathcal{E}$ ends in the rule ($\wedge$L$_1$) and the cut formula is principal in the rule ($\wedge$L$_1$).

**Base case?** The proof of admissibility of cut is by lexicographic induction on $\langle \varphi, [\mathcal{D}, \mathcal{E}] \rangle$, but we only case analyze $\mathcal{D}$ and $\mathcal{E}$. This means that we never *explicitly* consider the base case where $\varphi$ is an atomic formula. However, this base case is *implicitly* considered in the proof. The objective of this problem is to explore where the base case appears in the proof.

More precisely, when $\varphi$ is *restricted* to atomic formulas, admissibility of cut can be proved using induction on $\mathcal{E}$ alone. Show the following cases of this proof: (init), ($\vee$R$_1$), ($\supset$L) *and* explain where in the general proof of admissibility of cut each of these cases is covered (so, in the general proof of admissibility of cut, there is really no need to write an explicit proof of the base case where $\varphi$ is an atom).

# Problem 4: Alternate ($\supset$L) rule

A plausible, but incorrect, way to write the left rule for implication in the sequent calculus is the following:

$$\frac{\Gamma, \varphi_1 \;\mathsf{hyp}, \varphi_1 \supset \varphi_2 \;\mathsf{hyp}, \varphi_2 \;\mathsf{hyp} \Rightarrow \psi \;\mathsf{conc}}{\Gamma, \varphi_1 \;\mathsf{hyp}, \varphi_1 \supset \varphi_2 \;\mathsf{hyp} \Rightarrow \psi \;\mathsf{conc}} \supset\text{L'}$$

The difference between the usual ($\supset$L) rule and the one above is that the usual rule requires a proof of $\varphi_1 \;\mathsf{conc}$ as the first premise, whereas this rule requires $\varphi_1 \;\mathsf{hyp}$ as an explicit hypothesis. Let us call the standard sequent calculus with the rule ($\supset$L) SC and a sequent calculus in which ($\supset$L) is replaced with ($\supset$L'), SC'.

1. Prove that the rule ($\supset$L') is *derivable* in SC. (Hence, every theorem of SC' is a theorem of SC.)

2. Prove that the rule ($\supset$L) is *not admissible* in SC'.

   [Hint: It is enough to find a sequent which has a proof in SC, but not in SC'. For, if the rule ($\supset$L) were admissible in SC', then such a sequent could not exist.]

3. Prove that admissibility of cut does *not* hold for SC'.

   [Hint: Can you contradict (2) assuming admissibility of cut holds?]

4. Explain why the proof of admissibility of cut from class breaks on SC'. (There is no formal answer to this problem; all I am looking for is an understanding of which case(s) of the proof break or why some new cases, which cannot be completed, are needed.)

## Problem 5: Rule Invertibility

An inference rule is called invertible if the judgments in its premises have proofs whenever the judgment in the conclusion has a proof. For example, consider the rule ($\wedge$R).

$$\frac{\Gamma \Rightarrow \varphi_1 \ \mathsf{conc} \qquad \Gamma \Rightarrow \varphi_2 \ \mathsf{conc}}{\Gamma \Rightarrow \varphi_1 \wedge \varphi_2 \ \mathsf{conc}} \wedge\mathrm{R}$$

This rule is invertible because if there is a proof $\mathcal{D}$ of the conclusion, i.e., $\mathcal{D} :: \Gamma \Rightarrow \varphi_1 \wedge \varphi_2 \ \mathsf{conc}$, then we can construct a proof $\mathcal{E}_1$ of the first premise as follows (a proof of the second premise is similar):

$$\mathcal{E}_1 \quad = \quad \dfrac{\begin{array}{c}\mathcal{D}\\ \Gamma \Rightarrow \varphi_1 \wedge \varphi_2 \ \mathsf{conc}\end{array} \qquad \dfrac{\dfrac{}{\Gamma, \varphi_1 \wedge \varphi_2 \ \mathsf{hyp}, \varphi_1 \ \mathsf{hyp} \Rightarrow \varphi_1 \ \mathsf{conc}}\mathrm{init}}{\Gamma, \varphi_1 \wedge \varphi_2 \ \mathsf{hyp} \Rightarrow \varphi_1 \ \mathsf{conc}} \wedge\mathrm{L}_1}{\Gamma \Rightarrow \varphi_1 \ \mathsf{conc}} \mathrm{cut}$$

1. Explain why every left rule of the sequent calculus, except ($\supset$L), is invertible. [Hint: The answer is very easy; no cut or induction is needed.]

2. Provide a counterexample to show that ($\supset$L) is not invertible.

3. Prove that the rule ($\supset$R) is invertible.

4. Is the rule ($\vee \mathrm{R}_1$) invertible? If it is, give a proof, else give a counterexample.

5. The proof of invertibility of ($\wedge$R) shown above uses admissibility of cut. However, the result can also be proved directly by induction on $\mathcal{D}$. More precisely, we can prove by induction on $\mathcal{D}$ that: If $\mathcal{D} :: \Gamma \Rightarrow \varphi_1 \wedge \varphi_2 \ \mathsf{conc}$, then $\exists \mathcal{E}_1 :: \Gamma \Rightarrow \varphi_1 \ \mathsf{conc}$. Show the cases of this proof corresponding to the rules (init), ($\wedge$R), ($\supset$R) and ($\supset$L). (In a similar way, ($\supset$R) can also be proved invertible by induction.)

6. Combine your results from (1)–(5) to classify the rules of the sequent calculus as either invertible or non-invertible. The axioms (init), ($\top$R) and ($\bot$L) are obviously excluded from this classification because they have no premises.

## Problem 6: Canonical Proofs in Natural Deduction

Give $\beta\eta$-canonical proofs of the following hypothetical judgments. $p, q, r, s$ are atomic formulas.

1. $p \wedge q \downarrow, r \downarrow, (p \wedge q) \supset (r \supset s) \downarrow \vdash s \uparrow$
2. $p \supset (q \vee r) \downarrow, (q \vee r) \supset s \downarrow \vdash p \supset s \uparrow$