Assignment 8 Solutions: Cut Admissibility, Meta-Interpreters

15-317: Constructive Logic

Out: Thursday, October 30, 2008
Due: Tuesday, November 11, 2008, before class

1 Cut and Identity

Recall the rules for disjunction and implication:

$$\frac{\Gamma \Longrightarrow A}{\Gamma \Longrightarrow A \vee B}\ \vee R_1 \qquad \frac{\Gamma \Longrightarrow B}{\Gamma \Longrightarrow A \vee B}\ \vee R_2 \qquad \frac{\Gamma, A \vee B, A \Longrightarrow C \quad \Gamma, A \vee B, B \Longrightarrow C}{\Gamma, A \vee B \Longrightarrow C}\ \vee L$$

$$\frac{\Gamma, A \Longrightarrow B}{\Gamma \Longrightarrow A \supset B}\ \supset R \qquad \frac{\Gamma, A \supset B \Longrightarrow A \quad \Gamma, A \supset B, B \Longrightarrow C}{\Gamma, A \supset B \Longrightarrow C}\ \supset L$$

1.1 Identity

Identity: For all A and Γ, the sequent $\Gamma, A \Longrightarrow A$ is derivable.

Task 1 (10 pts).
Prove the $\supset$ case:
Assume

- $\Gamma, A \Longrightarrow A$ for all Γ
- $\Gamma, B \Longrightarrow B$ for all Γ

and show $\Gamma, A \supset B \Longrightarrow A \supset B$ for all Γ.

$$\dfrac{\dfrac{\overset{IH}{\Gamma, A \supset B, A \Longrightarrow A} \quad \overset{IH}{\Gamma, A \supset B, A, B \Longrightarrow B}}{\Gamma, A \supset B, A \Longrightarrow B}\ \supset L}{\Gamma, A \supset B \Longrightarrow A \supset B}\ \supset R$$

1.2 Principal Cuts

- **Weakening:** If $\Gamma \Longrightarrow C$ then $\Gamma, A \Longrightarrow C$.
- **Cut:** If $\Gamma \Longrightarrow A$ and $\Gamma, A \Longrightarrow C$ then $\Gamma \Longrightarrow C$.

Task 2 (10 pts). Prove the principal cut case for $\supset$:

Given

$$\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma, A \Longrightarrow B\end{array}}{\Gamma \Longrightarrow A \supset B} \supset R \qquad \mathcal{E} = \dfrac{\begin{array}{c}\mathcal{E}_1\\ \Gamma, A \supset B \Longrightarrow A\end{array} \quad \begin{array}{c}\mathcal{E}_2\\ \Gamma, A \supset B, B \Longrightarrow C\end{array}}{\Gamma, A \supset B \Longrightarrow C} \supset L$$

construct a derivation of $\Gamma \Longrightarrow C$.

Proof.

$$\begin{array}{ll} \mathcal{E}_1' :: \Gamma \Longrightarrow A & \text{IH on } (A \supset B, \mathcal{D}, \mathcal{E}_1) \\ \mathcal{D}' :: \Gamma, B \Longrightarrow A \supset B & \text{weakening on } \mathcal{D} \\ \mathcal{E}_2' :: \Gamma, B \Longrightarrow C & \text{IH on } (A \supset B, \mathcal{D}', \mathcal{E}_2) \\ \mathcal{D}_1' :: \Gamma \Longrightarrow B & \text{IH on } (A, \mathcal{E}_1', \mathcal{D}_1) \\ \Gamma \Longrightarrow C & \text{IH on } (B, \mathcal{D}_1', \mathcal{E}_2') \end{array}$$

□

Task 3 (5 pts). Prove a commutative cut case for $\vee$:

From

$$\dfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma, B_1 \vee B_2, B_1 \Longrightarrow A_1 \supset A_2\end{array} \quad \begin{array}{c}\mathcal{D}_2\\ \Gamma, B_1 \vee B_2, B_2 \Longrightarrow A_1 \supset A_2\end{array}}{\Gamma, B_1 \vee B_2 \Longrightarrow A_1 \supset A_2} \vee L \qquad \begin{array}{c}\mathcal{E}\\ \Gamma, B_1 \vee B_2, A_1 \supset A_2 \Longrightarrow C\end{array}$$

derive $\Gamma, B_1 \vee B_2 \Longrightarrow C$.

Proof. First, weaken $\mathcal{E}$ with B_1, and then cut with $\mathcal{D}_1$ to get $\Gamma, B_1 \vee B_2, B_1 \Longrightarrow C$. Symmetrically, get $\Gamma, B_1 \vee B_2, B_2 \Longrightarrow C$. Then apply $\vee L$. □

2 Counting Proofs

In class, we defined an interpreter for Prolog that made subgoal order and backtracking explicit. In this problem, you will extend this interpreter to count the number of proofs of a proposition.

2.1 Base rules

We assume that every atomic proposition P is defined by exactly one clause $P \leftarrow B$.

$$\dfrac{P \leftarrow B \quad B\,\mathsf{true}}{P\,\mathsf{true}} \qquad \dfrac{}{\top\,\mathsf{true}} \qquad \dfrac{A\,\mathsf{true} \quad B\,\mathsf{true}}{A \wedge B\,\mathsf{true}} \qquad \dfrac{A\,\mathsf{true}}{A \vee B\,\mathsf{true}} \qquad \dfrac{B\,\mathsf{true}}{A \vee B\,\mathsf{true}} \qquad \text{(no rule } \bot\,\mathsf{true}\text{)}$$

2.2 Abstract machine

Recall that S, the success stack, is a conjunction of propositions, and F, the failure stack, is a disjunction of propositions of the form $(B \wedge S)$.

$$\dfrac{P \leftarrow B \quad B/S/F}{P/S/F} \qquad \dfrac{}{\top/\top/F} \qquad \dfrac{B/S/F}{\top/(B \wedge S)/F} \qquad \dfrac{A/(B \wedge S)/F}{A \wedge B/S/F}$$

$$\dfrac{A/S/(B \wedge S) \vee F}{A \vee B/S/F} \qquad \text{(no rule } \bot/S/\bot\text{)} \qquad \dfrac{B/S/F}{\bot/S'/(B \wedge S) \vee F}$$

2.3 Counting Proofs

For these rules for these connectives, we can easily count the number of proofs a proposition has:

$$\begin{aligned}
|P| &= |B| \text{ where } P \leftarrow B \\
|\top| &= 1 \\
|A \wedge B| &= |A| * |B| \\
|\bot| &= 0 \\
|A \vee B| &= |A| + |B|
\end{aligned}$$

This definition makes sense if we assume that atoms are not defined recursively: recursive clauses can lead to propositions with infinitely many proofs. E.g. $\mathtt{nat} \leftarrow (\top \vee \mathtt{nat})$ has one proof for each natural number.

Theorem 1. *There are $|A|$ many derivations of $A\,\mathsf{true}$.*

Task 1 (7 pts). Extend the interpreter so that it counts the number of proofs of a proposition as it proves it: Define a judgement $A/S/F \mid n$ such that $(A \wedge S) \vee F$ has n proofs. Fill in the ?'s in the following rules:

$$\frac{P \leftarrow B \quad B/S/F \mid n}{P/S/F \mid n} \qquad \frac{}{\top/\top/\bot \mid 1} \qquad \frac{B/S/F \mid n}{\top/\top/((B \wedge S) \vee F) \mid n+1} \qquad \frac{B/S/F \mid n}{\top/(B \wedge S)/F \mid n} \qquad \frac{A/(B \wedge S)/F \mid n}{A \wedge B/S/F \mid n}$$

$$\frac{A/S/(B \wedge S) \vee F \mid n}{A \vee B/S/F \mid n} \qquad \frac{}{\bot/S/\bot \mid 0} \qquad \frac{B/S/F \mid n}{\bot/S'/(B \wedge S) \vee F \mid n}$$

Task 2 (8 pts). Prove your revised interpreter sound by induction on the rules:

Theorem 2. *If $A/S/F \mid n$ then $|(A \wedge S) \vee F| = n$.*

You may use whatever properties of arithmetic you require (e.g. associativity of $*$, distributivity of $*$ over $+$).

- $$\frac{}{\top/\top/\bot \mid 1}$$

  To show: $|(\top \wedge \top) \vee \bot| = 1 * 1 + 0 = 1$.

- $$\frac{B/S/F \mid n}{\top/\top/((B \wedge S) \vee F) \mid n+1}$$

  IH: $|(B \wedge S) \vee F| = n$.

  To show: $|\top \wedge \top \vee ((B \wedge S) \vee F)| = 1 * 1 + |(B \wedge S) \vee F| = 1 + n$.

- $$\frac{A/(B \wedge S)/F \mid n}{A \wedge B/S/F \mid n}$$

  IH: $|A \wedge (B \wedge S) \vee F| = n$

  TS: $|(A \wedge B) \wedge S \vee F| = n$.

  But $|A \wedge (B \wedge S) \vee F|$ = $|A| * (|B| * |S|) + |F|$ = $(|A| * |B|) * |S| + |F|$ = $|(A \wedge B) \wedge S \vee F| = n$.

The remaining cases are similar.