Lecture Notes on
Propositional Theorem Proving

15-317: Constructive Logic
Frank Pfenning

Lecture 12
October 8, 2009

1 Introduction

The inversion calculus from the last lecture constitutes a significant step forward, but it still has the problem that in the $\supset L$ rule, the principal formula has to be copied to the first premise. Therefore, the first premise may not be smaller than the conclusion.

We now have two basic choices. One is to refine the idea of loop-checking and make it as efficient as possible. We will not pursue this option here, although it can be done fruitfully [How98, Chapter4].

The second choice is to refine our analysis of the rules to see if we can design a calculus were all premises are smaller than the conclusion in some well-founded ordering. For this purpose we return to the restrictive sequent calculus and postpone for the moment a discussion of inversion. Dyckhoff [Dyc92] noticed that we can make progress by considering the possible forms of the antecedent of the implication. In each case we can write a special-purpose rule for which the premises are smaller than conclusion. The result is a beautiful calculus which Dyckhoff calls *contraction-free* because there is no rule of contraction, and, furthermore, the principal formula of each left rule is consumed as part of the rule application rather than copied to any premise.

We repeat the rules of the restrictive sequent calculus here for reference.

$$\frac{}{\Gamma, P \longrightarrow P}\ \text{init}$$

$$\frac{\Gamma \longrightarrow A \quad \Gamma \longrightarrow B}{\Gamma \longrightarrow A \wedge B}\ \wedge R \qquad \frac{\Gamma, A, B \longrightarrow C}{\Gamma, A \wedge B \longrightarrow C}\ \wedge L$$

$$\frac{}{\Gamma \longrightarrow \top}\ \top R \qquad \frac{\Gamma \longrightarrow C}{\Gamma, \top \longrightarrow C}\ \top L$$

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

$$\text{no } \bot R \text{ rule} \qquad \frac{}{\Gamma, \bot \longrightarrow C}\ \bot L$$

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

2 Refining the Left Rule for Implication

We consider each possibility for the antecedent of the implication in turn.

Truth. Consider a sequent

$$\Gamma, \top \supset B \longrightarrow C.$$

Can we find a simpler proposition expressing the same as $\top \supset B$? Yes, namely just B, since $(\top \supset B) \equiv B$. So we can propose the following specialized rule:

$$\frac{\Gamma, B \longrightarrow C}{\Gamma, \top \supset B \longrightarrow C}\ \top{\supset}L$$

Falsehood. Consider a sequent

$$\Gamma, \bot \supset B \longrightarrow C.$$

Can we find a simpler proposition expressing the same contents? Yes, namely $\top$, since $(\bot \supset B) \equiv \top$. But $\top$ on the left-hand side can be eliminated by $\top L$, so we can specialize the general rule as follows:

$$\frac{\Gamma \longrightarrow C}{\Gamma, \bot \supset B \longrightarrow C} \; \bot{\supset}L$$

Disjunction. Now we consider a sequent

$$\Gamma, (D \vee E) \supset B \longrightarrow C.$$

Again, we have to ask if there is a simpler equivalent formula we can use instead of $(C \vee D) \supset B$. If we consider the $\vee L$ rule, we might consider $(D \supset B) \wedge (E \supset B)$. A little side calculation confirms that, indeed,

$$((D \vee E) \supset B) \equiv ((D \supset B) \wedge (E \supset B))$$

We can exploit this, playing through the rules as follows

$$\frac{\dfrac{\Gamma, D \supset B, E \supset B \longrightarrow C}{\Gamma, (D \supset B) \wedge (E \supset B) \longrightarrow C} \; \wedge L}{\Gamma, (D \vee E) \supset B \longrightarrow C} \; \mathsf{equiv}$$

This suggests the specialized rule

$$\frac{\Gamma, D \supset B, E \supset B \longrightarrow}{\Gamma, (D \vee E) \supset B \longrightarrow C} \; \vee{\supset}L$$

The question is whether the premise is really smaller than the conclusion in some well-founded measure. We note that both $D \supset B$ and $E \supset B$ are smaller than the original formula $(D \vee E) \supset B$. Replacing one element in a multiset by several, each of which is strictly smaller according to some well-founded ordering, induces another well-founded ordering on multisets. So, the premise is indeed smaller in the multiset ordering.

Conjunction. Next we consider

$$\Gamma, (D \wedge E) \supset B \longrightarrow C.$$

In this case we can create an equivalent formula by currying.

$$\frac{\Gamma, D \supset (E \supset B) \longrightarrow C}{\Gamma, (D \wedge E) \supset B \longrightarrow C} \; \wedge{\supset}L$$

This formula is not strictly smaller, but we can make it so by giving conjunction a weight of 2 while counting implications as 1. Fortunately, this weighting does not conflict with any of the other rules we have.

Atomic propositions. How do we use an assumption $P \supset B$? We can conclude if we also know P, so we restrict the rule to the case where P is already among the assumption.

$$\frac{P \in \Gamma \quad \Gamma, B \longrightarrow C}{\Gamma, P \supset B \longrightarrow C}\ P{\supset}L$$

Clearly, the premise is smaller than the conclusion.

Implication. Last, but not least, we consider the case

$$\Gamma, (D \supset E) \supset B \longrightarrow C.$$

We start by playing through the left rule for this particular case because, as we have already seen, implication on the left does not simplify when interacting with another implication.

$$\frac{\dfrac{\Gamma, (D \supset E) \supset B, D \longrightarrow E}{\Gamma, (D \supset E) \supset B \longrightarrow D \supset E}\ {\supset}R \qquad \Gamma, B \longrightarrow C}{\Gamma, (D \supset E) \supset B \longrightarrow C}\ {\supset}L$$

The second premise is smaller and does not require any further attention. For the first premise, we need to find a smaller formula that is equivalent to $((D \supset E) \supset B) \wedge D$. The conjunction here is a representation of two distinguished formulas in the context. Fortunately, we find

$$((D \supset E) \supset B) \wedge D \equiv (E \supset B) \wedge D$$

which can be checked easily. This leads to the specialized rule

$$\frac{\Gamma, E \supset B, D \longrightarrow E \quad \Gamma, B \longrightarrow C}{\Gamma, (D \supset E) \supset B \longrightarrow C}\ {\supset}{\supset}L$$

This concludes the presentation of the specialized rules. The complete set of rule is summarized in Figure 1.

$$\frac{}{\Gamma, P \longrightarrow P}\ \mathsf{init}$$

$$\frac{\Gamma \longrightarrow A \quad \Gamma \longrightarrow B}{\Gamma \longrightarrow A \wedge B}\ {\wedge}R \qquad \frac{\Gamma, A, B \longrightarrow C}{\Gamma, A \wedge B \longrightarrow C}\ {\wedge}L$$

$$\frac{}{\Gamma \longrightarrow \top}\ {\top}R \qquad \frac{\Gamma \longrightarrow C}{\Gamma, \top \longrightarrow C}\ {\top}L$$

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

no $\bot R$ rule $\qquad \dfrac{}{\Gamma, \bot \longrightarrow C}\ {\bot}L$

$$\frac{\Gamma, A \longrightarrow B}{\Gamma \longrightarrow A \supset B}\ {\supset}R$$

$$\frac{P \in \Gamma \quad \Gamma, B \longrightarrow C}{\Gamma, P \supset B \longrightarrow C}\ P{\supset}L$$

$$\frac{\Gamma, D \supset (E \supset B) \longrightarrow C}{\Gamma, (D \wedge E) \supset B \longrightarrow C}\ {\wedge}{\supset}L \qquad \frac{\Gamma, B \longrightarrow C}{\Gamma, \top \supset B \longrightarrow C}\ {\top}{\supset}L$$

$$\frac{\Gamma, D \supset B, E \supset B \longrightarrow}{\Gamma, (D \vee E) \supset B \longrightarrow C}\ {\vee}{\supset}L \qquad \frac{\Gamma \longrightarrow C}{\Gamma, \bot \supset B \longrightarrow C}\ {\bot}{\supset}L$$

$$\frac{\Gamma, E \supset B, D \longrightarrow E \quad \Gamma, B \longrightarrow C}{\Gamma, (D \supset E) \supset B \longrightarrow C}\ {\supset}{\supset}L$$

Figure 1: Contraction-free sequent calculus

3 Asynchronous Decomposition

At this point we need to reexamine the question from last lecture: where do we really need to make choices in this sequent calculus? We ask the question slight differently this time, although the primary tool will still be the invertibility of rules. The question we want to ask this time: if we consider a formula on the right or on the left, can we always apply the corresponding rule without considering other choices? The difference between the two question becomes clear, for example, in the $P{\supset}L$ rule.

$$\frac{P \in \Gamma \quad \Gamma, B \longrightarrow C}{\Gamma, P \supset B \longrightarrow C}\ P{\supset}L$$

This rule is clearly invertible, because $P \wedge (P \supset B) \equiv P \wedge B$. Nevertheless, when we consider $P \supset B$ we cannot necessarily apply this rule because P may not be in the remaining context Γ.

Formulas whose left or right rules can always be applied are called left or right *asynchronous*, respectively. We can see by examining the rules and considering the equivalences above and the methods from the last lecture, that the following formulas are asynchrounous:

Right asynchronous	$A \wedge B$, $\top$, $A \supset B$
Left asynchronous	$A \wedge B$, $\top$, $A \vee B$, $\bot$,
	$(D \wedge E) \supset B$, $\top \supset B$, $(D \vee E) \supset B$, $\bot \supset B$

This leaves

Right synchronous	P, $A \vee B$, $\bot$
Left synchronous	P, $P \supset B$, $(D \supset E) \supset B$

Proof search now begins by breaking down all asynchronous formulas, leaving us with a situation where we have a synchronous formula on the right and only synchronous formulas on the left. We now check if init or $P{\supset}L$ can be applied and use them if possible. Since these rules are invertible, this does not require a choice. When no more of these rules are applicable, we have to choose between $\vee R_1$, $\vee R_2$ or ${\supset}{\supset}L$, if the opportunity exists; if not we fail and backtrack to the most recent choice point.

This strategy is complete and efficient for many typical examples, although in the end we cannot overcome the polynomial-space completeness of the intuitionistic propositional logic [Sta79].

The metatheory of the contraction-free sequent calculus has been investigated separately from its use as a decision procedure by Dyckhoff and

Negri [DN00]. The properties there could pave the way for further efficiency improvements by logical considerations, specifically in the treatment of atoms.

An entirely different approach to theorem proving in intuitionistic propositional logic is to use the *inverse method* [MP08] which is, generally speaking, more efficient on difficult problems, but not as direct on easier problems. We will discuss this technique in a later lecture.

References

[DN00] Roy Dyckhoff and Sara Negri. Admissibility of structural rules for contraction-free systems of intuitionistic logic. *Journal of Symoblic Logic*, 65:1499–1518, 2000.

[Dyc92] Roy Dyckhoff. Contraction-free sequent calculi for intuitionistic logic. *Journal of Symbolic Logic*, 57:795–807, 1992.

[How98] Jacob M. Howe. *Proof Search Issues in Some Non-Classical Logics*. PhD thesis, University of St. Andrews, Scotland, 1998.

[MP08] Sean McLaughlin and Frank Pfenning. Imogen: Focusing the polarized inverse method for intuitionistic propositional logic. In I.Cervesato, H.Veith, and A.Voronkov, editors, *Proceedings of the 15th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'08)*, pages 174–181, Doha, Qatar, November 2008. Springer LNCS 5330. System Description.

[Sta79] Richard Statman. Intuitionistic propositional logic is polynomial-space complete. *Theoretical Computer Science*, 9:67–72, 1979.