Lecture Notes on Propositional Theorem Proving

15-317: Constructive Logic
Frank Pfenning*

Lecture 12
October 11, 2016

1 Introduction

The inversion calculus from the last lecture constitutes a significant step forward in making proof search for intuitionistic propositional logic systematic. But it still has the problem that in the $\supset L$ rule, the principal formula has to be copied to the first premise to remain usable. 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 to ensure that implications will be expanded but not repeatedly in the same way. 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 for sequents $\Gamma \longrightarrow C$ 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, so we never duplicate reasoning (which we could if there were a contraction rule).

*With edits by André Platzer

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

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

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

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

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

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

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

2 Refining the Left Rule for Implication

In order to find a more efficient form of the problematic rule $\supset L$, we consider each possibility for the antecedent of the implication in turn. We will start with more obvious cases to find out the principles behind the design of the rules.

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 (which, in fact, derives from $\supset L$ and $\top R$):

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

This rule derives from $\supset L$ and $\top R$, which are both sound.

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:

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

Soundness of this rule also follows from weakening. Are we losing information compared to applying $\supset L$ here? No because that would require a proof of $\Gamma, \bot \supset B \longrightarrow \bot$ which will succeed if $\bot$ can be proved from Γ, but then there also is a direct proof without using $\bot \supset B$.

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,

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

The computational intuition is that getting a B out of having either a D or an E is equivalent to separate ways of getting a B out of a D as well as a way of getting a B out of an E. We can exploit this, playing through the rules as follows

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

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 [DM79]. So, the premises are indeed smaller in the multiset ordering, since the arose by replacing the original formula $(D \vee E) \supset B$ with either $D \supset B$ or with $E \supset B$, each of which are smaller. Operationally, the effect of $\vee\supset L$ is to separately consider the smaller implications $D \supset B$ and $E \supset B$.

Conjunction. Next we consider

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

In this case we can create an equivalent formula by currying using that $(D \wedge E) \supset B \equiv D \supset (E \supset B)$.

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

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. Operationally, the effect of $\wedge\supset L$ is to first consider what to make of the first assumed conjunct D by the other rules and then subsequently consider the second conjunct E.

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. If we were to use $\supset L$ instead, $P \supset B$ would remain in the first premise. The intuitive reason why we do not have to keep it is because the only way to make use of $P \supset B$ is to produce a P. But if we have such an atomic P, the above rule already establishes B. Note that, unlike a premise $\Gamma \longrightarrow P$, the premise $P \in \Gamma$ will obviously never search for possible proof rule applications within Γ. Indeed, those would not be useful, because we might as well apply them first before splitting into two premises.

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 $\supset L$ for this particular case because, as we have already seen, an implication on the left does not directly 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 since $D \supset E$ is equivalent to E if we already have D. This leads to the specialized rule

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

Indeed, all premises of $\supset\supset L$ are simpler now, because $E \supset B$ has strictly less operators than $(D \supset E) \supset B$ and its operators are of the same weight.

This concludes the presentation of the specialized rules so that the only rule that kept its principal formula around, $\supset L$, is no longer needed since all forms of implications are covered. The complete set of rule is summarized in Figure 1.

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

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

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

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

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

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

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

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

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

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

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

Figure 1: Contraction-free sequent calculus

questions 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. It might become available in the context later, though, after decomposing Γ. So we may have to wait with applying $P{\supset}L$ until $P \in \Gamma$.

Formulas whose left or right rules can always be applied are called left or right *asynchronous*, respectively, otherwise *synchronous*, because we may have to wait until they can be applied. 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, $P \supset B$, $(D \supset E) \supset B$

Atomic propositions are synchronous, because we may have to wait until it shows up in the antecedent and succedent. Disjunction is right synchronous because of the honest choice that $\vee R_1$ versus $\vee R_2$ imposes. Falsum is right synchronous because it needs to wait for $\bot$ to appear in the antecedent (no $\bot R$ rule). Atomic implication $P \supset B$ is left synchronous, because its rule $P{\supset}L$ waits for a $P \in \Gamma$. Nested implication $(D \supset E) \supset B$ could be considered left synchronous in the sense of waiting, because it is useful to handle the remaining context Γ before applying ${\supset}{\supset}L$, because any rules on Γ would otherwise have to be repeated in the first and second premise. But that is not actual reason! Nested implication $(D \supset E) \supset B$ is left synchronous, because ${\supset}{\supset}L$ is not invertible. In its first premise, rule ${\supset}{\supset}L$ sets out to prove E from some assumptions, which may be unsuccessful, e.g., if C is a disjunction $P \vee Q$ for which the other synchronous cases $\vee R_1$ or $\vee R_2$ succeed without expanding $(D \supset E) \supset B$ in the antecedent.

Similar to the idea behind the inversion calculus from the previous lecture, proof search proceeds in phases. Proof search 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, fortunately, does not require a choice. But, of course, if they do not apply, we have to check again later as more facts became available in Γ. 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 makes intuitive sense. If we have a disjunction on the right and an implication with an implicational assumption on the left, there is a tradeoff of whether proof search should try proving the assumption via $\supset\supset L$ or try proving one of the two disjuncts by $\vee R_1$ or $\vee R_2$.

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]. Indeed, the search will only ever keep strictly smaller subformulas of the input (in the well-founded order) in the sequents. But we need to search through different choices to find the right combination of $\vee R_1$, $\vee R_2$ or $\supset\supset L$ that yield a proof.

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.

Finally observe a computational interpretation of the identity theorem that $A \longrightarrow A$. In particular, in combination with the weakening theorem, $\Gamma, A \longrightarrow A$, which is in direct competition with the init rule which is of the same form but only applicable if A is an atomic formula. The pragmatics for proof search is that a check for applicability of the identity theorem would lead to frequent formula comparisons of complexity linear in the size of the formulas. In comparison, init is simpler because it is a direct comparison of atoms, so can essentially be made in constant time for a finite number of atoms. The identity theorem shows that it is sufficient to wait for only atomic formulas to be compared for init.

References

[DM79] Nachum Dershowitz and Zohar Manna. Proving termination with multiset orderings. *Commun. ACM*, 22(8):465–476, 1979.

[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.