Lecture Notes on Propositional Theorem Proving

15-317: Constructive Logic

Frank Pfenning*

Lecture 11
March 18, 2021

1 Introduction

The sequent calculus we have introduced so far maintains a close correspondence to natural deductions or, more specifically, to its verifications. One consequence is *persistence of antecedents*: once an assumption has been introduced in the course of a deduction, it will remain available in any sequent above this point. While this is appropriate in a foundational calculus, it is not at all ideal for proof search since rules can be applied over and over again without necessarily making progress (which is a fate this sequent calculus shares with naïve tableau calculi). We therefore develop a second sequent calculus and then a third in order to make the process of bottom-up search for a proof more efficient by reducing unnecessary choices in proof search. By way of the link of the sequent calculus with verification-style natural deductions from previous lectures, this lecture will, thus, give rise to a more efficient way of coming up with natural deduction proofs.

This lecture marks the beginning of a departure from the course of the lectures so far, which, broadly construed, focused on understanding what a constructive proof is and what can be read off or done once one has such a proof. Now we begin to move toward the question of how to find such a proof in the first place.

More ambitiously, we are looking for a *decision procedure* for intuitionistic propositional logic. Specifically, we would like to prove that for every

*With edits by André Platzer

proposition A, either $\Longrightarrow A$ or not $\Longrightarrow A$. Based on experience, we suspect this could be proved by induction on A, but this will fail for various reasons. Since sequent proof rules populate the antecedent, we need to prove that for *every sequent*, either $\Gamma \Longrightarrow A$ or not. That, however, has its own problems because the premises of the rules are more complex than the conclusion so it is not clear how one might apply an induction hypothesis.

First order of business, then, is to find a new, more restrictive system that eliminates redundancy and makes the premises of the rules smaller than the conclusion. This restricted sequent calculus will not quite satisfy our goal yet, but be a useful stepping stone nonetheless.

The second step will be 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. 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 the 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).

2 A More Restrictive Sequent Calculus[1]

Ideally, once we have applied an inference rule during proof search (that is, bottom-up), we should not have to apply the same rule again to the same proposition. Since all rules decompose formulas, if we had such a sequent calculus, we would have a simple and clean decision procedure. As it turns out, there is a fly in the ointment, but let us try to derive such a system.

We write $\Gamma \longrightarrow C$ for a sequent whose deductions try to eliminate principal formulas as much as possible. We keep the names of the rules in this calculus (called G4), since they are largely parallel to the rules of the original sequent calculus, $\Gamma \Longrightarrow C$.

[1] This calculus was mentioned in square brackets in an earlier lecture, without proof. We show it here as a starting point for the contraction-free calculus, as we did in lecture.

Conjunction. The right rule works as before; the left rule extracts *both* conjuncts at once so that the conjunction itself is no longer needed.

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

Observe that for both rules, *all* premises have smaller sequents than the conclusion if one counts the number of connectives in a sequent. So applying either rule obviously made progress toward simplifying the sequent.

It is easy to see that these rules are sound with respect to the ordinary sequent calculus rules. *Soundness* here is the property that if $\Gamma \longrightarrow C$ then $\Gamma \Longrightarrow C$. This is straightforward since $\wedge R$ is the same rule and $\wedge L$ is the same as $\wedge L_1$ followed by $\wedge L_2$ followed by weakening the original $A \wedge B$ away. Thus, the restricted $\wedge L$ and $\wedge R$ rules are derived rules in the original sequent calculus. *Completeness* is generally more difficult. What we want to show is that if $\Gamma \Longrightarrow C$ then also $\Gamma \longrightarrow C$, where the rules for the latter sequents are more restrictive, by design. The proof of this will eventually proceed by induction on the structure of the given deduction $\mathcal{D}$ and appeal to lemmas on the restrictive sequent calculus. For example:

Case: (of completeness proof)

$$\mathcal{D} = \frac{\begin{array}{c}\mathcal{D}_1 \\ \Gamma, A \wedge B, A \Longrightarrow C\end{array}}{\Gamma, A \wedge B \Longrightarrow C}\ \wedge L_1$$

$\Gamma, A \wedge B, A \longrightarrow C$	By i.h. on $\mathcal{D}_1$
$\Gamma, A, B \longrightarrow A$	By identity for $\longrightarrow$
$\Gamma, A \wedge B \longrightarrow A$	By $\wedge L$ on above
$\Gamma, A \wedge B \longrightarrow C$	By cut for $\longrightarrow$

The induction hypothesis is applicable to $\mathcal{D}_1$ because, even if it is a longer sequent, $\mathcal{D}_1$ is a shorter proof than $\mathcal{D}$. We see that identity and cut for the restricted sequent calculus are needed to show completeness in the sense described above. Fortunately, they hold (see further notes at the end of this section). We will not formally justify many of the rules, but give informal justifications or counterexamples.

Truth. There is a small surprise here, in that, unlike in natural deduction which had no elimination rule for $\top$, we can have a left rule for $\top$, which

eliminates it from the antecedents to make progress (cleanup). It is analogous to the zero-ary case of conjunction.

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

Atomic propositions. They are straightforward, since the initial sequents do not change and already make the best possible progress: close the proof.

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

Disjunction. The right rules to do not change; in the left rule we can eliminate the principal formula.

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

Intuitively, the assumption $A \vee B$ can be eliminated from both premises of the $\vee L$ rule, because the new assumptions A and B are each stronger than the previous assumption $A \vee B$. More formally:

Case: (of completeness proof)

$$\mathcal{D} = \frac{\begin{array}{c}\mathcal{D}_1\\ \Gamma, A \vee B, A \Longrightarrow C\end{array} \quad \begin{array}{c}\mathcal{D}_2\\ \Gamma, A \vee B, B \Longrightarrow C\end{array}}{\Gamma, A \vee B \Longrightarrow C}\ \vee L$$

$\Gamma, A \vee B, A \longrightarrow C$	By i.h. on $\mathcal{D}_1$
$\Gamma, A \longrightarrow A$	By identity for $\longrightarrow$
$\Gamma, A \longrightarrow A \vee B$	By $\vee R_1$
$\Gamma, A \longrightarrow C$	By cut for $\longrightarrow$
$\Gamma, A \vee B, B \longrightarrow C$	By i.h. on $\mathcal{D}_2$
$\Gamma, B \longrightarrow B$	By identity for $\longrightarrow$
$\Gamma, B \longrightarrow A \vee B$	By $\vee R_2$
$\Gamma, B \longrightarrow C$	By cut for $\longrightarrow$
$\Gamma, A \vee B \longrightarrow C$	By rule $\vee L$

Falsehood. Importantly, there is no right rule, and the left rule has no premise, which means it transfers directly.

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

Implication. In all the rules so far, all premises have fewer connectives than the conclusion. For implication, we will not be able to maintain this desirable property in rule $\supset L$.

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

Here, the assumption $A \supset B$ persists in the first premise of rule $\supset L$ but not in the second. While the assumption B is more informative than $A \supset B$, so only B is kept in the second premise, this is *not* the case in the first premise. Unfortunately, $A \supset B$ may be needed again in that branch of the proof. An example which requires the implication more than once is $\longrightarrow \neg\neg(A \vee \neg A)$, where $\neg A = A \supset \bot$ as usual. Without that additional assumption (marked in red below), the proof would not work:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\color{red}\neg(A \vee \neg A)}, A \longrightarrow A}\ \mathsf{id}}{\color{red}\neg(A \vee \neg A)}, A \longrightarrow A \vee \neg A}\ \vee R_1 \quad \dfrac{}{A, \bot \longrightarrow \bot}\ \bot L}{\color{red}\neg(A \vee \neg A)}, A \longrightarrow \bot}\ \color{red}\supset L}{\color{red}\neg(A \vee \neg A)} \longrightarrow \neg A}\ \supset R}{\color{red}\neg(A \vee \neg A)} \longrightarrow A \vee \neg A}\ \vee R_2 \quad \dfrac{}{\bot \longrightarrow \bot}\ \bot L}{\neg(A \vee \neg A) \longrightarrow \bot}\ \supset L}{\longrightarrow \neg\neg(A \vee \neg A)}\ \supset R$$

Now all rules have smaller premises (if one counts the number of logical constants and connectives in them) except for the $\supset L$ rule. We will address the issue with $\supset L$ in Section 4.

Nevertheless, we can interpret the rules as a decision procedure if we make the important observation that in bottom-up proof search we are licensed to fail a branch if along it we have a *repeating sequent*. If there were a deduction, we would be able to find it applying a different choice at an earlier sequent, lower down in the incomplete deduction. If there is a proof

with repeating sequents, there also is a proof without repeating sequents, by applying the proof that was used for the later occurrence of the repeating sequent already to the first occurrence of said sequent. If we also apply contraction (which is admissible in the restricted sequent calculus) to argue that we can remove duplicate formulas from the antecedent, then there are only *finitely* many sequents because antecedents and succedents are composed only of (proper or improper) subformulas of our original proof goal.

One can be much more efficient in loop checking than this [How98, Chapter 4], but just to see that intuitionistic propositional calculus is decidable, this is sufficient. In fact, we could have made this observation on the original sequent calculus, although it would be even further from a realistic implementation.

3 Metatheory of the Restricted Sequent Calculus

We only enumerate the basic properties.

Theorem 1 (Weakening) *If* $\Gamma \longrightarrow C$ *then* $\Gamma, A \longrightarrow C$ *with a structurally identical deduction.*

Theorem 2 (Atomic contraction) *If* $\Gamma, P, P \longrightarrow C$ *then* $\Gamma, P \longrightarrow C$ *with a structurally identical deduction*

Theorem 3 (Identity) $A \longrightarrow A$ *for any proposition* A.

Proof: By induction on the structure of A. □

Theorem 4 (Cut) *If* $\Gamma \longrightarrow A$ *and* $\Gamma, A \longrightarrow C$ *then* $\Gamma \longrightarrow C$

Proof: Analogous to the proof for the ordinary sequent calculus in Lecture 8. In the case where the first deduction is initial, we use atomic contraction. □

Theorem 5 (Contraction) *If* $\Gamma, A, A \longrightarrow C$ *then* $\Gamma, A \longrightarrow C$.

Proof: $\Gamma, A \longrightarrow A$ by identity and weakening. Therefore $\Gamma, A \longrightarrow C$ by cut. □

Theorem 6 (Soundness wrt. $\Longrightarrow$) *If* $\Gamma \longrightarrow A$ *then* $\Gamma \Longrightarrow A$.

Proof: By induction on the structure of the given deduction. □

Theorem 7 (Completeness wrt. $\Longrightarrow$) *If $\Gamma \Longrightarrow A$ then $\Gamma \longrightarrow A$.*

Proof: By induction on the structure of the given deduction, appealing to identity and cut in many cases. See the cases for $\wedge L_1$ and $\vee L$ in the previous section. $\square$

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

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

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

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

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

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

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

4 Refining the Left Rule for Implication

In order to find a more efficient form of the only problematic rule, rule $\supset L$, we consider each possible shape for the implication in the antecedent 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:

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

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

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 the elided antecedent $\bot \supset B$.

Disjunction. Now we consider a sequent

$$\Gamma, (A_1 \vee A_2) \supset B \longrightarrow C$$

Again, we have to ask if there is a simpler equivalent formula we can use instead of $(A_1 \vee A_2) \supset B$. If we consider the $\vee L$ rule, we might consider $(A_1 \supset B) \wedge (A_2 \supset B)$. A little side calculation confirms that, indeed,

$$((A_1 \vee A_2) \supset B) \equiv ((A_1 \supset B) \wedge (A_2 \supset B))$$

The computational intuition is that getting a B out of having either an A_1 or an A_2 is equivalent to separate ways of getting a B out of an A_1 as well as a way of getting a B out of an A_2. We can exploit this, playing through the rules as follows

$$\dfrac{\dfrac{\Gamma, A_1 \supset B, A_2 \supset B \longrightarrow C}{\Gamma, (A_1 \supset B) \wedge (A_2 \supset B) \longrightarrow C}\ \wedge L}{\Gamma, (A_1 \vee A_2) \supset B \longrightarrow C}\ \mathsf{equiv}$$

This suggests the specialized rule

$$\frac{\Gamma, A_1 \supset B, A_2 \supset B \longrightarrow C}{\Gamma, (A_1 \vee A_2) \supset B \longrightarrow C}\ \vee{\supset}L$$

The question is whether the premise is really smaller than the conclusion in some well-founded measure. We note that both of the new premises $A_1 \supset B$ and $A_2 \supset B$ are individually smaller than the original formula $(A_1 \vee A_2) \supset B$. 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. Operationally, the effect of $\vee\supset L$ is to separately consider the smaller implications $A_1 \supset B$ and $A_2 \supset B$.

Conjunction. Next we consider

$$\Gamma, (A_1 \wedge A_2) \supset B \longrightarrow C$$

In this case we can create an equivalent formula by currying using that $(A_1 \wedge A_2) \supset B \equiv A_1 \supset (A_2 \supset B)$.

$$\frac{\Gamma, A_1 \supset (A_2 \supset B) \longrightarrow C}{\Gamma, (A_1 \wedge A_2) \supset B \longrightarrow C} \wedge\supset L$$

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 and quite importantly, 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 A_1 by the other rules and then subsequently consider the second conjunct A_2, which has the computational effect of currying.

Atomic propositions. How do we use an assumption $P \supset B$? We can conclude B if we also know P, so we restrict the rule to the case where the atomic proposition 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 B from a P. But if we have such an atomic proposition P, the above rule already establishes B once and for all. Note that, unlike a premise $\Gamma \longrightarrow P$, the premise $P \in \Gamma$ will 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

$$\Gamma, (A_1 \supset A_2) \supset B \longrightarrow C$$

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.

$$\dfrac{\dfrac{\Gamma, (A_1 \supset A_2) \supset B, A_1 \longrightarrow A_2}{\Gamma, (A_1 \supset A_2) \supset B \longrightarrow A_1 \supset A_2}\,\supset R \qquad \Gamma, B \longrightarrow C}{\Gamma, (A_1 \supset A_2) \supset B \longrightarrow C}\,\supset L$$

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 $((A_1 \supset A_2) \supset B) \wedge A_1$, which represents the two distinguished formulas in the antecedent context by a conjunction. Fortunately, we find

$$((A_1 \supset A_2) \supset B) \wedge A_1 \equiv (A_2 \supset B) \wedge A_1$$

which can be checked easily since $A_1 \supset A_2$ is equivalent to A_2 if we already have A_1. This leads to the specialized rule

$$\dfrac{\Gamma, A_2 \supset B, A_1 \longrightarrow A_2 \quad \Gamma, B \longrightarrow C}{\Gamma, (A_1 \supset A_2) \supset B \longrightarrow C}\,\supset\supset L$$

Indeed, *all* premises of $\supset\supset L$ are simpler now, because $A_2 \supset B$ has strictly less operators than $(A_1 \supset A_2) \supset B$ and its operators are of the same weight.

There is a minor variation of this rule, which is also both sound and complete, and the premises are all smaller (by the multiset ordering) than the conclusion:

$$\dfrac{\Gamma, A_2 \supset B \longrightarrow A_1 \supset A_2 \quad \Gamma, B \longrightarrow C}{\Gamma, (A_1 \supset A_2) \supset B \longrightarrow C}\,\supset\supset L$$

They are equivalent because, in general, $\Gamma \longrightarrow A_1 \supset A_2$ iff $\Gamma, A_1 \longrightarrow A_2$.

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 in intuitionistic propositional logic are covered. The complete set of rule is summarized in Figure 1.

Even though these rules can be interpreted as defining a decision procedure, such a procedure would still not be practical except for small examples because there is too much nondeterminism in choosing which rule to apply when. We will discuss such nondeterminism in the next lecture.

$$\frac{P \in \Gamma}{\Gamma \longrightarrow P}\ \mathsf{id}$$

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

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

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

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

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

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

$$\frac{\Gamma, A_1 \supset (A_2 \supset B) \longrightarrow C}{\Gamma, (A_1 \wedge A_2) \supset B \longrightarrow C}\ \wedge{\supset}L \qquad \frac{\Gamma, B \longrightarrow C}{\Gamma, \top \supset B \longrightarrow C}\ \top{\supset}L$$

$$\frac{\Gamma, A_1 \supset B, A_2 \supset B \longrightarrow C}{\Gamma, (A_1 \vee A_2) \supset B \longrightarrow C}\ \vee{\supset}L \qquad \frac{\Gamma \longrightarrow C}{\Gamma, \bot \supset B \longrightarrow C}\ \bot{\supset}L$$

$$\frac{\Gamma, A_2 \supset B, A_1 \longrightarrow A_2 \quad \Gamma, B \longrightarrow C}{\Gamma, (A_1 \supset A_2) \supset B \longrightarrow C}\ {\supset}{\supset}L$$

Figure 1: Contraction-free sequent calculus

References

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

[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.