Lecture Notes on Proofs and Verifications

15-317: Constructive Logic
Frank Pfenning

Lecture 9
Tuesday, February 14, 2023

1 Introduction

The verificationist approach to the foundation of logic explains the meaning of the individual connectives by their introduction rules, from which we justify the elimination rules. What then is the meaning of a proposition? It is given by its verifications, which essentially composes the meaning of the individual connectives, because a verification is built only by introductions (reading bottom-up) and the justified eliminations (reading top-down). The important aspect of a verification is that it is composed only of subformulas of the proposition we are trying to prove.

General *proofs* do not have this property, because it is entirely legitimate to prove C *true* by proving A *true* and $A \supset C$ *true*, in which case A functions as a kind of lemma in the proof of C.

But does every true proposition have a verification and vice versa? If not, I would say, the verificationist approach has failed, or at least is in jeopardy. We have tested the waters with the local properties and established harmony for each connective, but this does not automatically entail this global property.

Fortunately for the verificationist (including myself), the property does hold and we now have the tools to prove it mathematically. The central technique is induction over the structure of derivations (also known as *rule induction*), and the central property we exploit is the *admissibility of cut*, proved in the last lecture.

In sequence, we prove the following theorems:

1. If A *true* then $\Longrightarrow A$ *succ*
2. If A *succ* then $A\uparrow$
3. If $A\uparrow$ then A *true*

Together these theorems show that, from the point of view of *provability*, the systems of natural deduction, sequent calculus, and verifications all coincide. Of course, the structure of proofs (which we very much care about, because they are related to programs) is very different in these three systems.

The property that we can go from A *true* to $A\uparrow$ is often called *normalization* because we may think of deductions of $A\uparrow$ as a *normal form* of proofs of A *true*. In part, this refers to the observation that a verification cannot be (locally) reduced.

2 From Natural Deduction to Sequent Calculus

We show how to translate an arbitrary natural deduction to the sequent calculus. This is sometimes called *completeness of the sequent calculus with respect to natural deduction*. If we understand natural deduction as defining (intuitionistic!) truth, the we can abbreviate that and just say *completeness of the sequent calculus*.

Just as a reminder, this sequent calculus does not include the rule of cut, and includes the rule of identity only for atomic propositions. To compensate for this, we have proved the admissibility of the following properties:

$$\frac{\Gamma \Longrightarrow A \quad \Gamma, A \Longrightarrow C}{\Gamma \Longrightarrow C}\ \mathsf{cut} \qquad \frac{}{\Gamma, A \Longrightarrow A}\ \mathsf{id}$$

$$\frac{\Gamma \Longrightarrow C}{\Gamma, A \Longrightarrow C}\ \mathsf{weaken} \qquad \frac{\Gamma, A, A \Longrightarrow C}{\Gamma, A \Longrightarrow C}\ \mathsf{contract}$$

Precisely because they are known to be admissible, we can use them freely if we want to construct a sequent derivation.

In both natural deduction and sequent calculus we reason from assumptions: *hypotheses* in natural deduction and *antecedents* in sequents. We need to account for them in the statement of the theorem, from which the unconditional version above follows as a special case. In the statements of the theorems today we abbreviate A_1 *true*, $\ldots$, A_n *true* as Γ *true* and similarly for other judgments. For sequents, we generally omit the explicit "antecedent" and "succedent" judgments.

Theorem 1 (From Natural Deduction to Sequent Calculus)

$$\textit{If} \quad \begin{array}{c} \Gamma \textit{ true} \\ \mathcal{D} \\ A \textit{ true} \end{array} \quad \textit{then} \quad \Gamma \Longrightarrow A$$

Proof: By rule induction on $\mathcal{D}$. We show a few representative cases; the others follow a similar pattern.

Case:

$$\mathcal{D} = \frac{\begin{array}{cc} \Gamma \textit{ true} & \Gamma \textit{ true} \\ \mathcal{D}_1 & \mathcal{D}_2 \\ A_1 \textit{ true} & A_2 \textit{ true} \end{array}}{A_1 \wedge A_2 \textit{ true}}\ \wedge I$$

where $A = A_1 \wedge A_2$. In this case we just apply the induction hypothesis to both $\mathcal{D}_1$ and $\mathcal{D}_2$ and mimic conjunction introduction with the right rule for conjunction.

$$\frac{\begin{array}{cc} \mathrm{IH}(\mathcal{D}_1) & \mathrm{IH}(\mathcal{D}_2) \\ \Gamma \Longrightarrow A_1 & \Gamma \Longrightarrow A_2 \end{array}}{\Gamma \Longrightarrow A_1 \wedge A_2}\ \wedge R$$

Case:

$$\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}' \\ A \wedge B \ \mathit{true}\end{array}}{A \ \mathit{true}} \wedge E_1$$

Again, we apply the induction hypothesis in order to construct a sequent proof.

$$\begin{array}{c}\mathrm{IH}(\mathcal{D}') \\ \Gamma \Longrightarrow A \wedge B \\ \vdots \\ \Gamma \Longrightarrow A\end{array}$$

We note that we do not have a rule to complete this proof now! This shouldn't come as a surprise, since when we constructed the sequent calculus we translated the elimination rules of natural deduction to left rules in the sequent calculus. But there $A \wedge B$ shows up on the right-hand side of a sequent.

Fortunately, we have some powerful principles, and, in particular, the admissibility of cut, which will make the conjunction appear on the left-hand side of a sequent.

$$\dfrac{\begin{array}{c}\mathrm{IH}(\mathcal{D}') \\ \Gamma \Longrightarrow A \wedge B\end{array} \quad \begin{array}{c}\vdots \\ \Gamma, A \wedge B \Longrightarrow A\end{array}}{\Gamma \Longrightarrow A}\ \mathsf{cut}$$

Now we can complete this construction with the left rule followed by the (admissible) identity.

$$\dfrac{\begin{array}{c}\mathrm{IH}(\mathcal{D}') \\ \Gamma \Longrightarrow A \wedge B\end{array} \quad \dfrac{\dfrac{}{\Gamma, A \wedge B, A \Longrightarrow A}\ \mathsf{id}}{\Gamma, A \wedge B \Longrightarrow A}\ \wedge L_1}{\Gamma \Longrightarrow A}\ \mathsf{cut}$$

Case: $\mathcal{D}$ proceeds with the use of a hypothesis $A \ \mathit{true}$ labelled u. The two-dimensional notation is a bit awkward, but the hypothesis is part of Γ in this case.

$$\mathcal{D} = \dfrac{}{A \ \mathit{true}}\ u$$

where $\Gamma = (\Gamma', \dfrac{}{A \ \mathit{true}}\ u)$. Then we construct

$$\dfrac{}{\Gamma', A \Longrightarrow A}\ \mathsf{id}$$

Case:

$$\mathcal{D} = \dfrac{\begin{array}{c}\Gamma \\ \mathcal{D}' \\ \bot \ \mathit{true}\end{array}}{A \ \mathit{true}} \bot E$$

Then we construct, similar to the case for $\wedge E_1$:

$$\dfrac{\dfrac{\begin{array}{c}\text{IH}(\mathcal{D}')\\ \Gamma \Longrightarrow \bot\end{array} \quad \dfrac{}{\Gamma, \bot \Longrightarrow A}\,\bot L}{\Gamma \Longrightarrow A}\,\textsf{cut}}{}$$

□

3 From Sequent Calculus to Verifications

When we translate from sequent calculus derivations to verifications, we once again have to navigate the fact that left rules are the reverse of elimination rules. Once we understand that, though, the proof cases are not that difficult. The key insight is that we do not have to consider cut or general identity (and also neither weakening nor contraction) since these are all "just" admissible.

Theorem 2 (From Sequent Calculus to Verifications)

$$\textit{If} \quad \begin{array}{c}\mathcal{D}\\ \Gamma \Longrightarrow A\end{array} \quad \textit{then} \quad \begin{array}{c}\Gamma\!\downarrow\\ \mathcal{E}\\ A\!\uparrow\end{array}$$

Proof: By rule induction on $\mathcal{D}$. Again, we show only a few representative cases.

Case:

$$\mathcal{D} = \dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2\\ \Gamma \Longrightarrow A_1 & \Gamma \Longrightarrow A_2\end{array}}{\Gamma \Longrightarrow A_1 \wedge A_2}\,\wedge R$$

where $A = A_1 \wedge A_2$. Then we appeal to the induction hypothesis twice and construct a verification with $\wedge I$.

$$\dfrac{\begin{array}{cc}\Gamma\!\downarrow & \Gamma\!\downarrow\\ \text{IH}(\mathcal{D}_1) & \text{IH}(\mathcal{D}_2)\\ A_1\!\uparrow & A_2\!\uparrow\end{array}}{A_1 \wedge A_2\!\uparrow}\,\wedge I$$

Case:

$$\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma', B_1 \wedge B_2, B_1 \Longrightarrow A\end{array}}{\Gamma', B_1 \wedge B_2 \Longrightarrow A}\,\wedge L_1$$

where $\Gamma = (\Gamma', B_1 \wedge B_2)$. The induction hypothesis gives us a derivation of $A\!\uparrow$ from one additional hypothesis, $B_1\!\downarrow$.

$$\begin{array}{c}\Gamma'\!\downarrow, B_1 \wedge B_2\!\downarrow, B_1\!\downarrow\\ \text{IH}(\mathcal{D}_1)\\ A\!\uparrow\end{array}$$

What we need is a derivation *without* the additional hypothesis $B_1\downarrow$. Fortunately we can justify it by $\wedge E_1$ applied to the conjunction:

$$\dfrac{\Gamma'\downarrow, B_1 \wedge B_2\downarrow, \quad \dfrac{B_1 \wedge B_2\downarrow}{B_1\downarrow}\wedge E_1}{\begin{array}{c}\mathrm{IH}(\mathcal{D}_1)\\ A\uparrow\end{array}}$$

The hypothesis $B_1 \wedge B_2\downarrow$ now appears more than once, but that's permissible for verifications (and natural deduction in general). The important observation is that the deduction no longer depends on $B_1\downarrow$, because this has now been justified.

□

4 From Verifications to Proofs

We constructed the system of verifications by restricting the free application of inference rules, keeping the rules and even reusing their names. As such, it should be quite straightforward that we can translate verifications to proofs. Nevertheless, the proof illustrates a general principle. Looking back at our definition, we see that $A\uparrow$ refers to $A\downarrow$ and vice versa. Most of the time this means we cannot prove a property of $A\uparrow$ in isolation, but need to generalize our induction hypothesis to include both judgments. Sometimes, that's very tricky. Here, it's easy.

Theorem 3 (From Verifications to Proofs)

1.

$$\textit{If} \quad \begin{array}{c}\Gamma\downarrow\\ \mathcal{D}\\ A\uparrow\end{array} \quad \textit{then} \quad \begin{array}{c}\Gamma\ \textit{true}\\ \mathcal{E}\\ A\ \textit{true}\end{array}$$

2.

$$\textit{If} \quad \begin{array}{c}\Gamma\downarrow\\ \mathcal{D}\\ A\downarrow\end{array} \quad \textit{then} \quad \begin{array}{c}\Gamma\ \textit{true}\\ \mathcal{E}\\ A\ \textit{true}\end{array}$$

Proof: By simultaneous rule induction on the given derivation. "Simultaneous" here means that induction hypothesis (1) can apply induction hypothesis (2) on a smaller derivation and vice versa. Because the $\Gamma\downarrow$ and Γ *true* aren't relevant in most cases and just carry over, we reduce syntactic overhead by not writing them down.

Case:

$$\mathcal{D} = \dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2\\ A_1\uparrow & A_2\uparrow\end{array}}{A_1 \wedge A_2\uparrow}\wedge I$$

The we just apply the first induction hypothesis on both subderivations and reapply the $\wedge I$ rule.

$$\dfrac{\begin{array}{cc}\mathrm{IH}_1(\mathcal{D}_1) & \mathrm{IH}_1(\mathcal{D}_2) \\ A_1\ \mathit{true} & A_2\ \mathit{true}\end{array}}{A_1 \wedge A_2\ \mathit{true}}\ \wedge I$$

Case:

$$\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}' \\ A \wedge B \downarrow\end{array}}{A \downarrow}\ \wedge E_1$$

This time we are in the induction part (2), and we only need the second induction hypothesis.

$$\dfrac{\begin{array}{c}\mathrm{IH}_2(\mathcal{D}') \\ A \wedge B\ \mathit{true}\end{array}}{A\ \mathit{true}}\ \wedge E_1$$

Case: Finally, one case where the two judgments interact. We leave others (like $\vee E$ or $\supset E$ to the reader).

$$\dfrac{\begin{array}{c}\mathcal{D}' \\ P \downarrow\end{array}}{P \uparrow}\ \downarrow\uparrow^*$$

Then just appealing to the induction hypothesis (2) already yields the correct derivation.

$$\begin{array}{c}\mathrm{IH}_2(\mathcal{D}') \\ P\ \mathit{true}\end{array}$$

□

5 Classical Sequent Calculus

One of Gentzen's [1935] remarkable discoveries was the encoding of *classical logic* in the sequent calculus. We already know in natural deduction it can be incorporated by the law of excluded middle, by double negation elimination, or by the rule of indirect proof. All of these are clearly outside the simple beauty of the natural deduction rules as defined by introductions and eliminations.

How do we obtain classical logic? Simply by allowing a sequent to have multiple conclusions! A sequent then has the form $\Gamma \overset{\mathsf{CL}}{\Longrightarrow} \Delta$, where Δ is also a collection of propositions. Now succedents as well as antecedents in the rules are persistent in all the rules. Remarkably, this is all we need to do!

We can then prove the law of excluded middle as follows, remembering that $\neg A \triangleq A \supset \bot$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dots\ \mathsf{id}}{A \overset{\mathsf{CL}}{\Longrightarrow} A \vee \neg A, A, \neg A}\supset R}{\overset{\mathsf{CL}}{\Longrightarrow} A \vee \neg A, A, \neg A}\vee R_2}{\overset{\mathsf{CL}}{\Longrightarrow} A \vee \neg A, A}\vee R_1}{\overset{\mathsf{CL}}{\Longrightarrow} A \vee \neg A}$$

Somehow, by allowing us to "hedge our bets" about which disjunct is true (first we say "A", send we say "$\neg A$") and then using the second possibility to establish the first we have circumvented the usual constructive nature of the disjunction.

I don't know how Gentzen discovered this, but I know why: because it allowed him to prove cut elimination for both intuitionistic and classical logic at the same time. One just needs to inspect every case in the proof and verify that if the two given derivations are intuitionistic (that is, have a single succedent), so is the resulting derivation.

Let's try another classical proof, which is also a neat application of cut. We do not construct it step-by-step, bottom-up, although this is certainly the way you should read it.

$$\dfrac{\dfrac{\dfrac{\dots\ \mathsf{id}}{A \overset{\mathsf{CL}}{\Longrightarrow} A} \quad \dfrac{\dfrac{\dfrac{\dots\ \mathsf{id}}{\neg A \overset{\mathsf{CL}}{\Longrightarrow} \neg A} \quad \dfrac{}{\bot \overset{\mathsf{CL}}{\Longrightarrow} A}\bot L}{\neg A, \neg\neg A \overset{\mathsf{CL}}{\Longrightarrow} A}\supset L}{A \vee \neg A, \neg\neg A \overset{\mathsf{CL}}{\Longrightarrow} A}\vee L}{\overset{\mathsf{CL}}{\Longrightarrow} A \vee \neg A \qquad A \vee \neg A \overset{\mathsf{CL}}{\Longrightarrow} \neg\neg A \supset A}\supset R}{\overset{\mathsf{CL}}{\Longrightarrow} \neg\neg A \supset A}\ \mathsf{cut}$$

We have omitted redundant antecedents and succedents. For example, in the only application of $\supset R$, we may keep a copy of $\neg\neg A \supset A$ in the succedent if we wish.

6 Conclusion

There are other ways to prove the overall connections we established. Here, the central step uses the admissibility of cut and identity. We can instead directly reason on natural deduction, for example, using the powerful technique of *logical relations*. This is often applied in programming languages because it has a more direct connection to proof reduction, which in our approach is hidden in the proof of the admissibility of cut.

References

Gerhard Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210, 405–431, 1935. English translation in M. E. Szabo, editor, *The Collected Papers of Gerhard Gentzen*, pages 68–131, North-Holland, 1969.