ConstLog: Constructive Logic

Lecture Notes on Harmony

Frank Pfenning André Platzer

Carnegie Mellon University || Karlsruhe Institute of Technology

Lecture 4

1 Introduction

In the verificationist definition of the logical connectives via their introduction rules we have briefly but informally justified the elimination rules. In this lecture, we study the balance between introduction and elimination rules more closely. Clearly, the elimination rules of a connective have to fit exactly, like hand in glove, to the introduction rules of the connective. In classical logic, the meaning of connectives is given by their semantics, which makes it easy to justify the correctness of all proof rules by showing they fit to the semantics. But in the verificationist definition, the introduction rules themselves are used as the *definitions*, which makes them unjustifiable. Fortunately, the elimination rules can still be justified in that they have to fit to the introduction rules.

We elaborate on the verificationist point of view that logical connectives are *defined* by their introduction rules. We show that for intuitionistic logic as presented so far, the elimination rules are in *harmony* with the introduction rules in the sense that they are neither too strong nor too weak. Elimination rules can *regain all information* provided to the introduction rules, *but no more*. We demonstrate this via local reductions and expansions, respectively, which relate to computational reductions from proofs-as-programs. This lecture is a fundamental cornerstone to the verificationist tradition.

2 Local Soundness and Local Completeness

To show that introduction and elimination rules are in harmony we establish *local soundness* and *local completeness*.

Local soundness shows that the elimination rules are not too strong: *no matter how we apply elimination rules to the result of an introduction we cannot gain any new information* (that wasn't originally present at the introduction). We demonstrate this by showing that we can find a more direct proof of the conclusion of an elimination than one that first introduces and then eliminates the connective in question. This is witnessed by a *local reduction* of the given introduction and the subsequent elimination.

Local completeness shows that elimination rules are not too weak: *there is always a way to apply elimination rules to reconstitute a proof of the original proposition from the results of the elimination rules by applying introduction rules*. This is witnessed by a *local expansion* of an arbitrary given derivation into one that reproves the primary connective.

Connectives whose introduction and elimination rules are in *harmony* in the sense that they are locally sound and complete are properly defined from the verificationist perspective. If not, the proposed connective should be viewed with suspicion. Another criterion we would like to apply uniformly is that both introduction and elimination rules do *not* refer to other propositional constants or connectives (besides the one we are trying to define), which could create a dangerous dependency of the various connectives on each other. For well-definedness, it is particularly important that connectives are defined in terms of simpler things (you also would not define a recursive function $f(x)$ as the more complex $f(x+1)$ because that would not terminate). As we present correct definitions we will occasionally also give some counterexamples to illustrate the consequences of violating the principles behind the patterns of harmonious inference.

When discussing each individual connective below we use the notation

$$\begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array} \Longrightarrow_R \begin{array}{c}\mathcal{D}'\\ A\ \mathit{true}\end{array}$$

for the *local reduction* of a deduction $\mathcal{D}$ to another deduction $\mathcal{D}'$ of the same judgment A *true*. In fact, $\Longrightarrow_R$ is a higher-level judgment relating two proofs, $\mathcal{D}$ and $\mathcal{D}'$, although we will not exploit this point of view. Similarly, the *local expansion* notation of $\mathcal{D}$ to $\mathcal{D}'$:

$$\begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array} \Longrightarrow_E \begin{array}{c}\mathcal{D}'\\ A\ \mathit{true}\end{array}$$

Local reductions and local expansions are transformations on constructive proofs.

Conjunction. We start with local soundness, i.e., locally reducing an elimination of a conjunction that was just introduced. Since conjunctions have two elimination rules and one introduction, we have two cases to consider, because there are two different elimination rules $\wedge E_1$ and $\wedge E_2$ that could follow the $\wedge I$ introduction rule. In either case, we can easily reduce.

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array} \quad \begin{array}{c}\mathcal{E}\\ B\ \mathit{true}\end{array}}{A \wedge B\ \mathit{true}}\wedge I}{A\ \mathit{true}}\wedge E_1 \quad \Longrightarrow_R \quad \begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array} \qquad\qquad \dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array} \quad \begin{array}{c}\mathcal{E}\\ B\ \mathit{true}\end{array}}{A \wedge B\ \mathit{true}}\wedge I}{B\ \mathit{true}}\wedge E_2 \quad \Longrightarrow_R \quad \begin{array}{c}\mathcal{E}\\ B\ \mathit{true}\end{array}$$

These two reductions justify that, after we proved a conjunction $A \wedge B$ to be true by the introduction rule $\wedge I$ from a proof $\mathcal{D}$ of A *true* and a proof $\mathcal{E}$ of B *true*, the only thing we can get back out by any of its elimination rules is something that we have originally put into the proof of $A \wedge B$ *true*. This makes $\wedge E_1$ and $\wedge E_2$ locally sound, because the only thing we get out is A *true* which already has the direct proof $\mathcal{D}$ as well as B *true* which has a direct proof $\mathcal{E}$. The above two reductions make $\wedge E_1$ and $\wedge E_2$ locally sound.

Local completeness establishes that we are not losing information from the elimination rules. Local completeness requires us to apply eliminations to an arbitrary proof $\mathcal{D}$ of $A \wedge B$ *true* in such a way that we can reconstitute a proof of $A \wedge B$ solely from the results obtained by the eliminations.

$$\begin{array}{c}\mathcal{D}\\ A \wedge B\ \mathit{true}\end{array} \quad \Longrightarrow_E \quad \dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ A \wedge B\ \mathit{true}\end{array}}{A\ \mathit{true}}\wedge E_1 \quad \dfrac{\begin{array}{c}\mathcal{D}\\ A \wedge B\ \mathit{true}\end{array}}{B\ \mathit{true}}\wedge E_2}{A \wedge B\ \mathit{true}}\wedge I$$

This local expansion shows that, collectively, the elimination rules $\wedge E_1$ and $\wedge E_2$ extract *all* information from the judgment $A \wedge B$ *true* that is needed to reprove $A \wedge B$ *true* with the introduction rule $\wedge I$. Remember that the hypothesis $A \wedge B$ *true*, once available, can be used multiple times, which is apparent in the local expansion, because the expansion simply repeats the same proof $\mathcal{D}$ of $A \wedge B$ *true* on the left and on the right premise.

As an example where local completeness fails, consider the case where we "forget" the second/right elimination rule $\wedge E_2$ for conjunction. The remaining rule is still locally sound, because it proves something that was put into the proof of $A \wedge B$ *true*, but not locally complete because we can no longer extract a proof of B from the assumption $A \wedge B$. Now, for example, we cannot prove $(A \wedge B) \supset (B \wedge A)$ even though this should clearly be true.

Substitution Principle. We need the defining property for hypothetical judgments before we can discuss implication. Intuitively, we can always substitute a deduction of A *true* for any use of a hypothesis A *true*, because every deduction of A *true* justifies the hypothesis A *true*. In order to avoid ambiguity, we make sure assumptions are labelled and we substitute simultaneously for *all* uses of an assumption with a given label. We can only substitute for assumptions that are not already discharged (e.g., by $\supset I^u$) in the subproof we are considering. The substitution principle then reads as follows:

If

$$\begin{array}{c}\overline{A\ \mathit{true}}\ u\\ \mathcal{E}\\ B\ \mathit{true}\end{array}$$

is a hypothetical proof of B *true* under the *undischarged* hypothesis A *true* labelled u (especially, no $\supset I^u$ appears in $\mathcal{E}$), and

$$\begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array}$$

is a proof of A *true* then

$$\begin{array}{c} \mathcal{D} \\ \hline A\ \mathit{true} \end{array} u \\ \begin{array}{c} \mathcal{E} \\ B\ \mathit{true} \end{array}$$

is our notation for substituting deduction $\mathcal{D}$ for *all* uses of the hypothesis labelled u in the deduction $\mathcal{E}$. This deduction, also written in linear notation as $[\mathcal{D}/u]\mathcal{E}$ no longer depends on assumption u.

Implication. To witness local soundness, we reduce an implication introduction followed by an elimination using the substitution operation.

$$\dfrac{\dfrac{\begin{array}{c}\overline{A\ \mathit{true}}\ u \\ \mathcal{E} \\ B\ \mathit{true}\end{array}}{A \supset B\ \mathit{true}}\supset I^u \qquad \begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array}}{B\ \mathit{true}}\supset E \quad \Longrightarrow_R \quad \begin{array}{c}\dfrac{\mathcal{D}}{A\ \mathit{true}}\ u \\ \mathcal{E} \\ B\ \mathit{true}\end{array}$$

This reduction plugs in the deduction $\mathcal{D}$ of A *true* in for the assumption A *true* labelled u in the deduction $\mathcal{E}$ that proved B *true*. The conditions on the substitution operation are satisfied, because label u was just introduced at the $\supset I^u$ inference and therefore cannot be discharged in $\mathcal{E}$ itself, since labels introduced during a proof are always fresh.

Local completeness is witnessed by the following expansion.

$$\begin{array}{c}\mathcal{D}\\ A \supset B\ \mathit{true}\end{array} \quad \Longrightarrow_E \quad \dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ A \supset B\ \mathit{true}\end{array} \quad \overline{A\ \mathit{true}}\ u}{B\ \mathit{true}}\supset E}{A \supset B\ \mathit{true}}\supset I^u$$

Here label u must be chosen fresh: it only labels the new hypothesis A *true* which is used only once. This local expansion reconstitutes a proof of $A \supset B$ *true* (using the hypothesis u introduced by $\supset I^u$) from the conclusion B *true* obtained from the deduction $\mathcal{D}$ of $A \supset B$ *true* by elimination $\supset E$.

Disjunction. For disjunctions we also employ the substitution principle because the two cases we consider in the elimination rule introduce hypotheses. In order to show local soundness we have two possibilities for the introduction rule, in both situations followed by the only elimination rule.

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array}}{A \lor B\ \mathit{true}}\lor I_L \quad \begin{array}{c}\overline{A\ \mathit{true}}^{\,u}\\ \mathcal{E}\\ C\ \mathit{true}\end{array} \quad \begin{array}{c}\overline{B\ \mathit{true}}^{\,w}\\ \mathcal{F}\\ C\ \mathit{true}\end{array}}{C\ \mathit{true}}\lor E^{u,w} \quad \Longrightarrow_R \quad \begin{array}{c}\dfrac{\mathcal{D}}{A\ \mathit{true}}u\\ \mathcal{E}\\ C\ \mathit{true}\end{array}$$

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ B\ \mathit{true}\end{array}}{A \lor B\ \mathit{true}}\lor I_R \quad \begin{array}{c}\overline{A\ \mathit{true}}^{\,u}\\ \mathcal{E}\\ C\ \mathit{true}\end{array} \quad \begin{array}{c}\overline{B\ \mathit{true}}^{\,w}\\ \mathcal{F}\\ C\ \mathit{true}\end{array}}{C\ \mathit{true}}\lor E^{u,w} \quad \Longrightarrow_R \quad \begin{array}{c}\dfrac{\mathcal{D}}{B\ \mathit{true}}w\\ \mathcal{F}\\ C\ \mathit{true}\end{array}$$

An example of a rule that would not be locally sound is

$$\dfrac{A \lor B\ \mathit{true}}{A\ \mathit{true}}\lor E_1?$$

and, indeed, we would not be able to reduce

$$\dfrac{\dfrac{B\ \mathit{true}}{A \lor B\ \mathit{true}}\lor I_R}{A\ \mathit{true}}\lor E_1?$$

In fact we can now derive a contradiction from no assumption, which means the whole system is incorrect, violating the fundamental principle that $\perp$ *true* has no proof.

$$\dfrac{\dfrac{\dfrac{}{\top\ \mathit{true}}\top I}{\perp \lor \top\ \mathit{true}}\lor I_R}{\perp\ \mathit{true}}\lor E_1?$$

Local completeness of disjunction distinguishes cases on the known judgment $A \lor B$ *true*, using the common $A \lor B$ *true* as the conclusion of the elimination $\lor E^{u,w}$.

$$\begin{array}{c}\mathcal{D}\\ A \lor B\ \mathit{true}\end{array} \quad \Longrightarrow_E \quad \dfrac{\begin{array}{c}\mathcal{D}\\ A \lor B\ \mathit{true}\end{array} \quad \dfrac{\overline{A\ \mathit{true}}^{\,u}}{A \lor B\ \mathit{true}}\lor I_L \quad \dfrac{\overline{B\ \mathit{true}}^{\,w}}{A \lor B\ \mathit{true}}\lor I_R}{A \lor B\ \mathit{true}}\lor E^{u,w}$$

Visually, this looks somewhat different from the local expansions for conjunction or implication. It looks like the elimination rule is applied last, rather than first. Mostly, this is due to the two-dimensional notation of natural deduction: the above represents the step from using the knowledge of $A \lor B$ *true* and eliminating it to obtain the hypotheses A *true* and B *true* in the two cases.

Truth. The constant $\top$ only has an introduction rule, but no elimination rule. Consequently, there are no cases to check for local soundness: any introduction followed by any elimination can be reduced, simply because $\top$ has no elimination rules at all.

However, local completeness still yields a local expansion: Any proof $\mathcal{D}$ of $\top$ *true* can be trivially converted to one by the introduction rule $\top I$ without even using $\mathcal{D}$.

$$\begin{array}{c}\mathcal{D}\\ \top\ \mathit{true}\end{array} \quad \Longrightarrow_E \quad \dfrac{}{\top\ \mathit{true}}\ \top I$$

Falsehood. As for truth, there is no local reduction for $\bot$, because local soundness is trivially satisfied since we have no introduction rule.

Local completeness is slightly tricky. Literally, we have to show that there is a way to apply an elimination rule to any proof of $\bot$ *true* so that we can reintroduce a proof of $\bot$ *true* from the result. However, there will be zero cases to consider, so we apply no introductions. Nevertheless, the following is the right local expansion.

$$\begin{array}{c}\mathcal{D}\\ \bot\ \mathit{true}\end{array} \quad \Longrightarrow_E \quad \dfrac{\begin{array}{c}\mathcal{D}\\ \bot\ \mathit{true}\end{array}}{\bot\ \mathit{true}}\ \bot E$$

Reasoning about situations where falsehood is true may seem vacuous, but is common in practice because it corresponds to reaching a contradiction. In intuitionistic reasoning, this occurs when we prove $A \supset \bot$ which is often abbreviated as $\neg A$, as a construction turning a (hypothetical) proof of A into a proof of $\bot$, which, after all, cannot have a proof except from counterfactual assumptions. In *classical logic reasoning* it is even more frequent, due to the rule of proof by contradiction that classically concludes A from having led the extra assumption $\neg A$ to a contradiction.

3 Revisiting Proof Terms

Now that all the proof rules of intuitionistic propositional logic for the truth judgment are shown harmonious, the next question would be to show that all the proof rules for the proof term rules are also harmonious. Notice how the pattern of elimination rules applied to the result of an introduction rule is like the pattern of a destructor applied to a constructor, as pursued in the proof term reductions of the Proofs-as-Programs lecture. Specifically, in that lecture, eliminations (destructors) applied to the result of introductions (constructor) give rise to computation in the form of a reduction. We invite you to go back and verify that these computational reductions are *exactly* the witnesses of the local reductions on proofs shown in this lecture! In other words, *computational reductions on proof terms witness local soundness of the rules!* Proof term reductions are the computational interpretation of local soundness proofs.

What about local completeness? It turns out that the local expansions are less relevant to computation. What they tell us, however, is that if we need to return a pair from a function, we can always construct it explicitly as a pair $\langle M, N\rangle$ for some M and N. Indeed, any proof term O for which $O : A \wedge B$ holds can be explicitly turned into the pair $\langle \mathbf{fst}\, O, \mathbf{snd}\, O\rangle$. Another example would be that whenever we need to return a function, we can always construct it as a function abstraction $\mathsf{fn}\, u \Rightarrow M$ for some M.

We can derive what the local expansion must be by annotating the deductions witnessing local expansions *on proofs* from this lecture with proof terms. We leave this as an exercise to the reader. The left-hand side of each expansion has the form $M : A$, where M is an arbitrary term and A is a logical connective or constant applied to arbitrary propositions. On the right hand side we have to apply a destructor to M and then reconstruct a term of the original type. The resulting expansion rules are in Figure 1.

$$
\begin{array}{lll}
M : A \wedge B & \Longrightarrow_E & \langle \mathbf{fst}\, M, \mathbf{snd}\, M\rangle \\
M : A \supset B & \Longrightarrow_E & \mathsf{fn}\, u{:}A \Rightarrow M\, u \quad \text{for } u \text{ not free in } M \\
M : \top & \Longrightarrow_E & \langle\,\rangle \\
M : A \vee B & \Longrightarrow_E & \mathbf{case}\, M\, \mathbf{of}\, \mathbf{inl}\, u \Rightarrow \mathbf{inl}_B\, u \mid \mathbf{inr}\, w \Rightarrow \mathbf{inr}_A\, w \\
M : \bot & \Longrightarrow_E & \mathbf{abort}_\bot\, M
\end{array}
$$

Figure 1: Proof term expansions

4 Logical Equivalence as a Connective

As another example we would now like to define a new connective, develop introduction and elimination rules, and check their local soundness and completeness (if they hold). First, the proposed introduction rule to define the connective:

$$
\dfrac{\begin{array}{cc} \dfrac{}{A\ \mathit{true}}\,u & \dfrac{}{B\ \mathit{true}}\,w \\ \vdots & \vdots \\ B\ \mathit{true} & A\ \mathit{true} \end{array}}{A \equiv B\ \mathit{true}}\,{\equiv}I^{u,w}
$$

This suggests the two eliminations rules below. If we omitted one of them, we would expect the eliminations *not* to be locally complete.

$$
\dfrac{A \equiv B\ \mathit{true} \quad A\ \mathit{true}}{B\ \mathit{true}}\,{\equiv}E_1 \qquad \dfrac{A \equiv B\ \mathit{true} \quad B\ \mathit{true}}{A\ \mathit{true}}\,{\equiv}E_2
$$

There is one introduction and two eliminations, so we have to check two cases for local soundness. The first case:

$$\dfrac{\dfrac{\begin{array}{c}\overline{A\ \mathit{true}}\ u\\ \mathcal{D}\\ B\ \mathit{true}\end{array}\quad\begin{array}{c}\overline{B\ \mathit{true}}\ w\\ \mathcal{E}\\ A\ \mathit{true}\end{array}}{A \equiv B\ \mathit{true}}\equiv I^{u,w}\quad\begin{array}{c}\mathcal{F}\\ A\ \mathit{true}\end{array}}{B\ \mathit{true}}\equiv E_1 \quad\Longrightarrow_R\quad \begin{array}{c}\mathcal{F}\\ \overline{A\ \mathit{true}}\ u\\ \mathcal{D}\\ B\ \mathit{true}\end{array}$$

We see that $B\ \mathit{true}$ is justified, because the proof $\mathcal{D}$ ends in $B\ \mathit{true}$ and its hypothesis is proved by $\mathcal{F}$. The other reduction is entirely symmetric.

$$\dfrac{\dfrac{\begin{array}{c}\overline{A\ \mathit{true}}\ u\\ \mathcal{D}\\ B\ \mathit{true}\end{array}\quad\begin{array}{c}\overline{B\ \mathit{true}}\ w\\ \mathcal{E}\\ A\ \mathit{true}\end{array}}{A \equiv B\ \mathit{true}}\equiv I^{u,w}\quad\begin{array}{c}\mathcal{F}\\ B\ \mathit{true}\end{array}}{A\ \mathit{true}}\equiv E_2 \quad\Longrightarrow_R\quad \begin{array}{c}\mathcal{F}\\ \overline{B\ \mathit{true}}\ w\\ \mathcal{D}\\ A\ \mathit{true}\end{array}$$

The local expansion will exhibit the necessity of both elimination rules. You should go through this and construct it in stages—the final result of expansion may otherwise be a bit hard to understand.

$$\begin{array}{c}\mathcal{D}\\ A \equiv B\ \mathit{true}\end{array} \quad\Longrightarrow_E\quad \dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ A \equiv B\ \mathit{true}\end{array}\quad \overline{A\ \mathit{true}}\ u}{B\ \mathit{true}}\equiv E_1 \quad \dfrac{\begin{array}{c}\mathcal{D}\\ A \equiv B\ \mathit{true}\end{array}\quad \overline{B\ \mathit{true}}\ w}{A\ \mathit{true}}\equiv E_2}{A \equiv B\ \mathit{true}}\equiv I^{u,w}$$

At this point we know that, logically, the equivalence connective makes sense: it is both locally sound and complete.

Next, we should carry out a proof term assignment and re-express local reduction and expansions on proof terms. The local reduction should give us a rule of computation; the local expansion an extensional equality principle. The mnemonic for the proof terms for the elimination rules are congruence rules from left to right ($\overrightarrow{\mathbf{C}}$) or from right to left ($\overleftarrow{\mathbf{C}}$), respectively.

$$\dfrac{\begin{array}{c}\overline{u : A}\ u\\ \vdots\\ N : B\end{array}\quad\begin{array}{c}\overline{w : B}\ w\\ \vdots\\ M : A\end{array}}{(\!|u \Rightarrow N, w \Rightarrow M|\!) : A \equiv B}\equiv I^{u,w}$$

$$\dfrac{M : A \equiv B \quad N : A}{\overrightarrow{\mathbf{C}}\ M\ N : B}\equiv E_1 \qquad \dfrac{M : A \equiv B \quad N : B}{\overleftarrow{\mathbf{C}}\ M\ N : A}\equiv E_2$$

We can now annotate the local reductions and expansion with proof terms and read off:

$$\overrightarrow{\mathbf{C}}\ (\!|u \Rightarrow N, w \Rightarrow M|\!)\ P \Longrightarrow_R [P/u]N$$
$$\overleftarrow{\mathbf{C}}\ (\!|u \Rightarrow N, w \Rightarrow M|\!)\ P \Longrightarrow_R [P/w]M$$
$$M : A \equiv B \Longrightarrow_E (\!|u \Rightarrow \overrightarrow{\mathbf{C}}\ M\ u, w \Rightarrow \overleftarrow{\mathbf{C}}\ N\ w|\!)$$

Introducing new syntax for new connectives and programs can be tedious and difficult to use. Therefore, in practice, we probably wouldn't define logical equivalence as a new primitive, but instead use *notational definition*:

$$A \equiv B \quad \triangleq \quad (A \supset B) \wedge (B \supset A)$$

whose meaning as a type is a pair of functions between the types A and B.

5 Summary of Judgments

$M : A \Longrightarrow_E M'$ proof term M for proposition A expands to M', see Figure 1