Constructive Logic (15-317), Spring 2021
Recitation 2: Proofs and Programs (2021-02-10)
André Platzer et al

1 Proofs Are Programs

As discussed previously in lecture, there is a tight correspondence between the structure of a derivation for a constructive proof and a term in some particular programming language. This leads to the slogans "proofs are programs" and "propositions are types". The (Curry-Howard-Lambek) correspondence can be fleshed out for the logic we're studying (intuitionistic propositional logic)[1] by the following table

Propositions	Types
$A \wedge B$	$A * B$
$A \vee B$	$A + B$
$A \supset B$	$A \to B$
$\top$	1 (unit)
$\bot$	0 (void)

Based on this we can produce a version of our rules from the previous recitation that annotate each proposition step in the derivation with the program that it constructs. Those rules are:

$$\frac{M : A \qquad N : B}{\langle M, N \rangle : A \wedge B}\ \wedge I \qquad \frac{M : A \wedge B}{\mathsf{fst}\ M : A}\ \wedge E_1 \qquad \frac{M : A \wedge B}{\mathsf{snd}\ M : B}\ \wedge E_2$$

$$\frac{M : A}{\mathsf{inl}\ M : A \vee B}\ \vee I_1 \qquad \frac{N : B}{\mathsf{inr}\ N : A \vee B}\ \vee I_2 \qquad \frac{M : A \vee B \qquad \begin{array}{c}\overline{u : A}^{\,u} \\ \vdots \\ N : C\end{array} \qquad \begin{array}{c}\overline{w : B}^{\,w} \\ \vdots \\ O : C\end{array}}{\mathsf{case}\ M\ \mathsf{of}\ \mathsf{inl}\ u \Rightarrow N \mid \mathsf{inr}\ w \Rightarrow O : C}\ \vee E^{u,w}$$

$$\frac{\begin{array}{c}\overline{u : A}^{\,u} \\ \vdots \\ M : B\end{array}}{\mathsf{fn}\ u \Rightarrow M : A \supset B}\ \supset I^u \qquad \frac{M : A \supset B \qquad N : A}{M\ N : B}\ \supset E$$

$$\frac{}{\langle\rangle : \top}\ \top I \qquad \frac{M : \bot}{\mathsf{abort}\ M : A}\ \bot E$$

2 Translation

We now turn to the question of translating proofs to programs and back again. In these notes, we present both for the sake of accessibility.

Task 1. $(A \supset B \supset C) \supset (B \supset A \supset C)$

[1] Of course, what makes this correspondence so remarkable is that it extends far beyond this one logic. It is quite robust and extends to almost any well-behaved logic. It also maps between logic and functional programming and lattices which are just closed cartesian categories

Solution 1: Proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{true A \supset B \supset C}\,f \qquad \dfrac{}{true A}\,a}{true B \supset C} \qquad \dfrac{}{true B}\,b}{true C}\supset E}{true A \supset C}\supset I^{a}}{true B \supset A \supset C}\supset I^{b}}{true (A \supset B \supset C) \supset (B \supset A \supset C)}\supset I^{f}$$

Program:

$$\mathsf{fn}\ f \Rightarrow \mathsf{fn}\ b \Rightarrow \mathsf{fn}\ a \Rightarrow (f\ a)\ b$$

Task 2. $((A \supset B) \vee (A \supset C)) \supset A \supset (B \vee C)$

Solution 2: Proof:
Let X be:

$$\dfrac{\dfrac{\dfrac{}{true A \supset B}\,f \qquad \dfrac{}{true A}\,a}{true B}\supset E}{true B \vee C}\vee I_1$$

Let Y be:

$$\dfrac{\dfrac{\dfrac{}{true A \supset C}\,g \qquad \dfrac{}{true A}\,a}{true C}\supset E}{true B \vee C}\vee I_2$$

The overall proof is:

$$\dfrac{\dfrac{\dfrac{}{true (A \supset B\ true) \vee (A \supset C)}\,f\,g \qquad X \qquad Y}{true B \vee C}\vee E^{f,g}}{true A \supset (B \vee C)}\supset I^{a}}{true ((A \supset B) \vee (A \supset C)) \supset A \supset (B \vee C)}\supset I^{f\,g}$$

Program:

$$\mathsf{fn}\ u \Rightarrow \mathsf{fn}\ v \Rightarrow \mathsf{case}\ u\ \mathsf{of}\ \mathsf{inl}\ f \Rightarrow \mathsf{inl}\ (f\ v) \mid \mathsf{inr}\ g \Rightarrow \mathsf{inr}\ (g\ v)$$

3 Inventing proof terms

Task 3. Let's consider a new connective $\wedge$. We'll give the intro and elim rules and try to come up with constructors, destructors and reduction rules that make sense.

$$\dfrac{true A \qquad \begin{array}{c}\dfrac{}{true B}\,u\\ \vdots \\ \dfrac{}{true \bot}\end{array}}{true A \wedge B}\wedge I_1$$

$$\dfrac{\begin{array}{c}\dfrac{}{true A}\,u\\ \vdots \\ \dfrac{}{true \bot}\end{array} \qquad true B}{true A \wedge B}\wedge I_2$$

$$\dfrac{trueA \wedge B \qquad \dfrac{\overset{\overset{u}{\overline{trueA}}}{\vdots}}{trueC} \qquad \dfrac{\overset{\overset{v}{\overline{true\neg B}}}{\vdots}}{trueC}}{trueC}\wedge E \qquad \dfrac{\overset{\overset{u}{\overline{true\neg A}}}{\vdots}}{trueC} \qquad \dfrac{\overset{\overset{v}{\overline{trueB}}}{\vdots}}{trueC}$$

Solution 3: Let's come up with constructors that make sense for $\wedge$

$$\dfrac{M : A \qquad \dfrac{\overset{\overset{u}{\overline{u : B}}}{\vdots}}{N : \bot}}{\mathsf{lft}(M, u.N) : A \wedge B}$$

$$\dfrac{\dfrac{\overset{\overset{u}{\overline{u : A}}}{\vdots}}{M : \bot} \qquad N : B}{\mathsf{rght}(u.M, N) : A \wedge B}$$

And the destructor...

$$\dfrac{E : A \wedge B \qquad \dfrac{\overset{\overset{u}{\overline{u : A}}}{\vdots}}{M : C} \qquad \dfrac{\overset{\overset{v}{\overline{v : \neg B}}}{\vdots}}{M : C} \qquad \dfrac{\overset{\overset{w}{\overline{w : \neg A}}}{\vdots}}{N : C} \qquad \dfrac{\overset{\overset{x}{\overline{x : B}}}{\vdots}}{N : C}}{\mathsf{case}\, E\, \mathsf{of}\, \mathsf{lft}(u, v) \Rightarrow M \mid \mathsf{rght}(w, x) \Rightarrow N : C}$$

Now we still need to define a reduction rule for $\wedge$. Reduction rules are applied when the destructor is applied to a constructor.

$$\mathsf{case}\, \mathsf{lft}(N', u'.M')\, \mathsf{of}\, \mathsf{lft}(u, v) \Rightarrow M \mid \mathsf{rght}(w, x) \Rightarrow N \Longrightarrow^r [N'/u, \mathsf{fn}\, u' \Rightarrow M'/v]M$$

$$\mathsf{case}\, \mathsf{rght}(u'.N', M')\, \mathsf{of}\, \mathsf{lft}(u, v) \Rightarrow M \mid \mathsf{rght}(w, x) \Rightarrow N \Longrightarrow^r [\mathsf{fn}\, u' \Rightarrow N'/w, M'/x]N$$

4 Reductions

Let's try reducing a term until we can no longer apply reduction rules.

Task 4.

$$\mathsf{fn}\, a \Rightarrow \mathsf{fn}\, b \Rightarrow (\mathsf{fn}\, f \Rightarrow \mathsf{fn}\, p \Rightarrow \langle (\mathsf{fst}\ f)\ (\mathsf{fst}\ p), (\mathsf{snd}\ f)\ (\mathsf{snd}\ p)\rangle)\ \langle \mathsf{fn}\, u \Rightarrow a, \mathsf{fn}\, u \Rightarrow b\rangle\ \langle b, a\rangle$$

Solution 4:

$$\mathsf{fn}\, a \Rightarrow \mathsf{fn}\, b \Rightarrow (\mathsf{fn}\, p \Rightarrow \langle (\mathsf{fst}\ \langle \mathsf{fn}\, u \Rightarrow a, \mathsf{fn}\, u \Rightarrow b\rangle)\ (\mathsf{fst}\ p), \mathsf{snd}\ \langle \mathsf{fn}\, u \Rightarrow a, \mathsf{fn}\, u \Rightarrow b\rangle\ (\mathsf{snd}\ p)\rangle)\ \langle b, a\rangle$$

Notice at this point we have a few options on how to proceed. It's actually the case that there is a term that we will reach no matter which order we apply reduction rules. It's generally know as the Church Rosser theorem that if a term finishes reducing in two ways, then they arrive at the same place. With our system we'll always react a "normal" form, so we can apply rules in such a way that save us the trouble of writing a lot.

$$\mathsf{fn}\, a \Rightarrow \mathsf{fn}\, b \Rightarrow (\mathsf{fn}\, p \Rightarrow \langle (\mathsf{fn}\, u \Rightarrow a)\ (\mathsf{fst}\, p), (\mathsf{snd}\ \langle \mathsf{fn}\, u \Rightarrow a, \mathsf{fn}\, u \Rightarrow b\rangle)\ (\mathsf{snd}\, p)\rangle)\ \langle b, a\rangle$$

$$\mathsf{fn}\, a \Rightarrow \mathsf{fn}\, b \Rightarrow (\mathsf{fn}\, p \Rightarrow \langle (\mathsf{fn}\, u \Rightarrow a)\, (\mathsf{fst}\, p), (\mathsf{fn}\, u \Rightarrow b)\, (\mathsf{snd}\, p) \rangle)\, \langle b, a \rangle$$

$$\mathsf{fn}\, a \Rightarrow \mathsf{fn}\, b \Rightarrow (\mathsf{fn}\, p \Rightarrow \langle a, (\mathsf{fn}\, u \Rightarrow b)\, (\mathsf{snd}\, p) \rangle)\, \langle b, a \rangle$$

$$\mathsf{fn}\, a \Rightarrow \mathsf{fn}\, b \Rightarrow (\mathsf{fn}\, p \Rightarrow \langle a, b \rangle)\, \langle b, a \rangle$$

$$\mathsf{fn}\, a \Rightarrow \mathsf{fn}\, b \Rightarrow \langle a, b \rangle$$

Constructive Logic (15-317), Spring 2021
Recitation 3: Harmonic proofs and verifications (2021-02-17)
André Platzer et al

1 Harmony

Proof-theoretic harmony is a necessary, but not sufficient, condition for the well-behavedness of a logic; harmony ensures that the connectives are *locally* well-behaved, and is closely related to the critical cases of cut and identity elimination which we may discuss later on. Therefore, when designing or extending a logic, checking harmony is a first step.

From the verificationist standpoint, a connective is *harmonious* if its elimination rules are neither too strong nor too weak in relation to its introduction rules. The first condition is called *local soundness* and the second condition is called *local completeness*. The content of the soundness condition is a method to reduce or simplify proofs, and the content of completeness is a method to expand any arbitrary proof into a canonical proof (i.e. one that ends in an introduction rule).

1.1 Conjunction

Local soundness for conjunction is witnessed by the following two reduction rules:

$$\dfrac{\dfrac{\mathcal{D}}{A\ true} \quad \dfrac{\mathcal{E}}{B\ true}\ \wedge\mathsf{I}}{\dfrac{A \wedge B\ true}{A\ true}\ \wedge\mathsf{E}_1} \longrightarrow_{\mathsf{R}} \dfrac{\mathcal{D}}{A\ true}$$

$$\dfrac{\dfrac{\mathcal{D}}{A\ true} \quad \dfrac{\mathcal{E}}{B\ true}\ \wedge\mathsf{I}}{\dfrac{A \wedge B\ true}{B\ true}\ \wedge\mathsf{E}_2} \longrightarrow_{\mathsf{R}} \dfrac{\mathcal{E}}{B\ true}$$

Local completeness is witnessed by the following expansion rule:

$$\dfrac{\mathcal{D}}{A \wedge B\ true} \longrightarrow_{\mathsf{E}} \dfrac{\dfrac{\dfrac{\mathcal{D}}{A \wedge B\ true}\ \wedge\mathsf{E}_1 \quad \dfrac{\mathcal{D}}{A \wedge B\ true}\ \wedge\mathsf{E}_2}{A \wedge B\ true}\ \wedge\mathsf{I}}{}$$

When regarded as generating relations on *programs* rather than proofs, the reduction and expansion rules can be recast into another familiar format:

$$\mathsf{fst}\,\langle M, N\rangle \longrightarrow_{\mathsf{R}} M$$
$$\mathsf{snd}\,\langle M, N\rangle \longrightarrow_{\mathsf{R}} N$$
$$M \longrightarrow_{\mathsf{E}} \langle \mathsf{fst}\,M, \mathsf{snd}\,M\rangle$$

1.2 Disjunction

Local soundness:

$$\dfrac{\dfrac{\mathcal{D}}{A\ true}}{A \vee B\ true}\ \vee\mathsf{I}_1 \quad \dfrac{\overline{A\ true}^{\,u} \quad \mathcal{E} \quad C\ true}{C\ true} \quad \dfrac{\overline{B\ true}^{\,v} \quad \mathcal{F} \quad C\ true}{C\ true}\ \vee\mathsf{E}^{u,v} \longrightarrow_{\mathsf{R}} \dfrac{\dfrac{\mathcal{D}}{A\ true}}{}\,u \quad \mathcal{E} \quad C\ true$$

$$\dfrac{\dfrac{\mathcal{D}}{B\ true}}{A \vee B\ true}\ \vee\mathsf{I}_2 \quad \dfrac{\overline{A\ true}^{\,u} \quad \mathcal{E} \quad C\ true}{C\ true} \quad \dfrac{\overline{B\ true}^{\,v} \quad \mathcal{F} \quad C\ true}{C\ true}\ \vee\mathsf{E}^{u,v} \longrightarrow_{\mathsf{R}} \dfrac{\dfrac{\mathcal{D}}{B\ true}}{}\,v \quad \mathcal{F} \quad C\ true$$

$$\mathsf{case}\ \mathsf{inl}\,M\ \mathsf{of}\ \mathsf{inl}\,u \Rightarrow L \mid \mathsf{inr}\,v \Rightarrow R \longrightarrow_{\mathsf{R}} [M/u]L$$
$$\mathsf{case}\ \mathsf{inr}\,M\ \mathsf{of}\ \mathsf{inl}\,u \Rightarrow L \mid \mathsf{inr}\,v \Rightarrow R \longrightarrow_{\mathsf{R}} [M/v]R$$

Local completeness:

$$\dfrac{\mathcal{D}}{A \vee B\ true} \longrightarrow_{\mathsf{E}} \dfrac{\dfrac{\mathcal{D}}{A \vee B\ true} \quad \dfrac{\dfrac{}{A\ true}\,u}{A \vee B\ true}\vee\mathsf{I}_1 \quad \dfrac{\dfrac{}{B\ true}\,v}{A \vee B\ true}\vee\mathsf{I}_2}{A \vee B\ true}\vee\mathsf{E}^{u,v}$$

$$M \longrightarrow_{\mathsf{E}} \mathsf{case}\ M\ \mathsf{of}\ \mathsf{inl}\,u \Rightarrow \mathsf{inl}\,u \mid \mathsf{inr}\,v \Rightarrow \mathsf{inr}\,v$$

1.3 Implication

Local soundness:

$$\dfrac{\dfrac{\begin{array}{c}\dfrac{}{A\ true}\,u\\ \mathcal{D}\\ B\ true\end{array}}{A \supset B\ true}\supset\mathsf{I}^u \quad \begin{array}{c}\mathcal{E}\\ A\ true\end{array}}{B}\supset\mathsf{E} \longrightarrow_{\mathsf{R}} \begin{array}{c}\mathcal{E}\\ \dfrac{}{A\ true}\,u\\ \mathcal{D}\\ B\ true\end{array}$$

$$(\mathsf{fn}\,u \Rightarrow M)\ N \longrightarrow_{\mathsf{R}} [N/u]M$$

Local completeness:

$$\dfrac{\mathcal{D}}{A \supset B\ true} \longrightarrow_{\mathsf{E}} \dfrac{\dfrac{\mathcal{D}}{A \supset B\ true} \quad \dfrac{}{A\ true}\,u}{B\ true}\supset\mathsf{E}}{A \supset B\ true}\supset\mathsf{I}^u$$

$$M \longrightarrow_{\mathsf{E}} \mathsf{fn}\,u \Rightarrow M\,u$$

1.4 Experiment: Alternative Implication

What if we replaced the $\supset\mathsf{E}$ rule with the following elimination rule:

$$\dfrac{A \supset B\ true \quad A\ true \quad \begin{array}{c}\dfrac{}{B\ true}\,u\\ \vdots\\ C\ true\end{array}}{C\ true}\supset\mathsf{E}^u$$

The program/proof term assignment is as follows:

$$\dfrac{L : A \supset B \quad M : A \quad \begin{array}{c}\dfrac{}{u : B}\,u\\ \vdots\\ N : C\end{array}}{\mathsf{let}\ u = L\,M\ \mathsf{in}\ N : C}\supset\mathsf{E}^u$$

Task 1. Can we show local soundness and completeness for this version of the implication connective?

Solution 1:

$$\dfrac{\dfrac{\begin{array}{c}\dfrac{}{A\ true}\,v\\ \mathcal{D}\\ B\ true\end{array}}{A \supset B\ true}\supset\mathsf{I}^v \quad \begin{array}{c}\mathcal{E}\\ A\ true\end{array} \quad \begin{array}{c}\dfrac{}{B\ true}\,u\\ \mathcal{F}\\ C\ true\end{array}}{C\ true}\supset\mathsf{E}^u \longrightarrow_{\mathsf{R}} \begin{array}{c}\mathcal{E}\\ \dfrac{}{A\ true}\,v\\ \mathcal{D}\\ B\ true\end{array} \quad \begin{array}{c}\dfrac{}{B\ true}\,u\\ \mathcal{F}\\ C\ true\end{array}$$

$$\mathsf{let}\ u = (\mathsf{fn}\,v \Rightarrow L)\ M\ \mathsf{in}\ N \longrightarrow_{\mathsf{R}} [[M/v]L/u]N$$

$$\dfrac{\dfrac{\mathcal{D}}{A \supset B\ true} \quad \dfrac{}{A\ true}\,u \quad \dfrac{}{B\ true}\,v}{\dfrac{B\ true}{A \supset B\ true}\,\supset \mathsf{I}^u}\,\supset \mathsf{E}^v \qquad \dfrac{\mathcal{D}}{A \supset B\ true} \longrightarrow_{\mathsf{E}}$$

$$M \longrightarrow_{\mathsf{E}} \mathsf{fn}\ u \Rightarrow \mathsf{let}\ v = M\ u\ \mathsf{in}\ v$$

Task 2. Last week in recitation we made up introduction and elimination rules to go with a new connective $\wedge$. They are listed again below. Show local soundness and completeness of this connective's rules.

$$\dfrac{A\ true \qquad \dfrac{\dfrac{}{B\ true}\,u}{\vdots}}{\dfrac{}{\bot\ true}}{A \wedge B\ true}\,\wedge I_1$$

$$\dfrac{\dfrac{\dfrac{}{A\ true}\,u}{\vdots}}{\dfrac{}{\bot\ true}} \quad B\ true}{A \wedge B\ true}\,\wedge I_2$$

$$\dfrac{A \wedge B\ true \qquad \dfrac{\dfrac{}{A\ true}\,u \quad \dfrac{}{\neg B\ true}\,v}{\vdots} \qquad \dfrac{\dfrac{}{\neg A\ true}\,w \quad \dfrac{}{B\ true}\,x}{\vdots}}{\dfrac{C\ true}{C\ true}}{C\ true}\,\wedge E$$

Solution 2: Local soundness:

$$\dfrac{\dfrac{\mathcal{D}}{A\ true} \quad \dfrac{\mathcal{E}}{\bot\ true}}{A \wedge B\ true}\,\wedge \mathsf{I}_1^u \qquad \dfrac{\dfrac{}{A\ true}\,w \quad \mathcal{F} \quad \dfrac{}{\neg B\ true}\,v}{C\ true} \qquad \dfrac{\dfrac{}{\neg A\ true}\,y \quad \mathcal{G} \quad \dfrac{}{B\ true}\,z}{C\ true}}{C\ true}\,\wedge \mathsf{E} \longrightarrow_{\mathsf{R}} \dfrac{\dfrac{\mathcal{D}}{A\ true}\,w \quad \mathcal{F} \quad \dfrac{\mathcal{E}}{\neg B\ true}\,v}{C\ true}$$

The proof for the second introduction rule is analogous to the above.

Local completeness:

$$\dfrac{\mathcal{D}}{A \wedge B\ true} \longrightarrow_{\mathsf{E}} \dfrac{\dfrac{\mathcal{D}}{A \wedge B\ true} \qquad \dfrac{\dfrac{}{A\ true}\,u \quad \dfrac{}{\neg B\ true}\,v}{A \wedge B\ true}\,\wedge \mathsf{I}_1^v \qquad \dfrac{\dfrac{}{\neg A\ true}\,w \quad \dfrac{}{B\ true}\,x}{A \wedge B\ true}\,\wedge \mathsf{I}_2^w}{A \wedge B\ true}\,\wedge \mathsf{E}$$

"Proof search" is not a mere matter of practice: it is *praxis*. The dialectic of proof search is to discover ways to pare down the state space of a logic, and then synthesize this into a new logic which is exactly as expressive as the old one. This new restricted logic not only has better search complexity, but also exposes critical semantic content which tends to have been obscured in the original logic.

Perhaps the most famous example of this process is Andreoli's *focalization*; in recent lectures, we have begun to study a simpler instance of this process, namely the decomposition of truth into *verification* and *use*. The passage to verifications constitutes a collation of upward and downward deductions respectively.