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:

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

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

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

$$\dfrac{}{\langle\rangle : \top}\ \top I \qquad \dfrac{M : \bot}{\mathit{abort}\ M : A}\ \bot E$$

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:

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

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:

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

Let Y be:

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

The overall proof is:

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

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 $\curlywedge$. We'll give the intro and elim rules and try to come up with constructors, destructors and reduction rules that make sense.

$$\dfrac{A \text{ true} \qquad \begin{array}{c} \overline{B \text{ true}}\ u \\ \vdots \\ \hline \bot \text{ true} \end{array}}{A \curlywedge B \text{ true}}\curlywedge I_1$$

$$\dfrac{\begin{array}{c} \overline{A \text{ true}}\ u \\ \vdots \\ \hline \bot \text{ true} \end{array} \qquad B \text{ true}}{A \curlywedge B \text{ true}}\curlywedge I_2$$

$$\dfrac{A \wedge B\ \text{true} \qquad \dfrac{\begin{array}{cc}\dfrac{}{A\ \text{true}}\,u & \dfrac{}{\neg B\ \text{true}}\,v \\ \vdots & \vdots\end{array}}{C\ \text{true}} \qquad \dfrac{\begin{array}{cc}\dfrac{}{\neg A\ \text{true}}\,u & \dfrac{}{B\ \text{true}}\,v \\ \vdots & \vdots\end{array}}{C\ \text{true}}}{C\ \text{true}}\ \wedge E$$

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

$$\dfrac{M : A \qquad \dfrac{\begin{array}{c}\dfrac{}{u : B}\,u \\ \vdots\end{array}}{N : \bot}}{\mathsf{lft}(M, u.N) : A \wedge B}$$

$$\dfrac{\dfrac{\begin{array}{c}\dfrac{}{u : A}\,u \\ \vdots\end{array}}{M : \bot} \qquad N : B}{\mathsf{rght}(u.M, N) : A \wedge B}$$

And the destructor...

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

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.

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

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

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

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