Constructive Logic (15-317), Spring 2022
Recitation 3: Proofs and Programs & Verifications (2022-02-02)
clogic staff

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:

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

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:

$$\dfrac{\dfrac{\overline{A \supset B \text{ true}}^{f} \quad \overline{A \text{ true}}^{v}}{B \text{ true}} \supset E}{B \vee C \text{ true}} \vee I_1$$

Let Y be:

$$\dfrac{\dfrac{\overline{A \supset C \text{ true}}^{g} \quad \overline{A \text{ true}}^{v}}{C \text{ true}} \supset E}{B \vee C \text{ true}} \vee I_2$$

The overall proof is:

$$\dfrac{\dfrac{\dfrac{\overline{(A \supset B) \text{ true} \vee (A \supset C) \text{ true}}^{u} \quad X \quad Y}{B \vee C \text{ true}} \vee E^{f,g}}{A \supset (B \vee C) \text{ true}} \supset I^{v}}{((A \supset B) \vee (A \supset C)) \supset A \supset (B \vee C) \text{ true}} \supset I^{u}$$

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

$$\dfrac{A \text{ true} \quad \begin{array}{c}\overline{B \text{ true}}^{u} \\ \vdots \\ \bot \text{ true}\end{array}}{A \sqcup B \text{ true}} \sqcup I_1 \qquad \dfrac{\begin{array}{c}\overline{A \text{ true}}^{u} \\ \vdots \\ \bot \text{ true}\end{array} \quad B \text{ true}}{A \sqcup B \text{ true}} \sqcup I_2$$

$$\dfrac{A \sqcup B \text{ true} \quad \begin{array}{c}\overline{A \text{ true}}^{u} \\ \vdots \\ C \text{ true}\end{array} \quad \begin{array}{c}\overline{\neg B \text{ true}}^{v} \\ \vdots \\ C \text{ true}\end{array}}{C \text{ true}} \sqcup E \qquad \dfrac{A \sqcup B \text{ true} \quad \begin{array}{c}\overline{\neg A \text{ true}}^{u} \\ \vdots \\ C \text{ true}\end{array} \quad \begin{array}{c}\overline{B \text{ true}}^{v} \\ \vdots \\ C \text{ true}\end{array}}{C \text{ true}} \sqcup E$$

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

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

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

And the destructor...

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

Now we still need to define a reduction rule for $\sqcup$. 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 Verifications and Uses

"Verifications" are proofs that proceed upwards from conclusions to premises; this is also known as *backward inference* or *refinement-style proof*. On the other hand, "uses" are proofs that proceed from premise to conclusion, also known as *forward inference*. The judgment $A\uparrow$ stands for verifications of A, and the judgment $A\downarrow$ stands for uses of A.
The rules for verifications and uses of the conjunction connective are as follows:

$$\frac{A\uparrow \quad B\uparrow}{A\wedge B\uparrow}\wedge\mathsf{I} \qquad \frac{A\wedge B\downarrow}{A\downarrow}\wedge\mathsf{E}_1 \qquad \frac{A\wedge B\downarrow}{B\downarrow}\wedge\mathsf{E}_2$$

On this basis, you may think that verifications correspond to introduction forms and uses correspond to elimination forms. This is not correct, as can be seen from the case of disjunction:

$$\frac{A\uparrow}{A\vee B\uparrow}\vee\mathsf{I}_1 \qquad \frac{B\uparrow}{A\vee B\uparrow}\vee\mathsf{I}_2 \qquad \frac{A\vee B\downarrow \quad \begin{array}{c}\overline{A\downarrow}^{\,u}\\ \vdots\\ C\uparrow\end{array} \quad \begin{array}{c}\overline{B\downarrow}^{\,v}\\ \vdots\\ C\uparrow\end{array}}{C\uparrow}\vee\mathsf{E}^{u,v}$$

Will the elimination rule for implication result have a verification or a use in its conclusion?

$$\frac{\begin{array}{c}\overline{A\downarrow}^{\,u}\\ \vdots\\ B\uparrow\end{array}}{A\supset B\uparrow}\supset\mathsf{I}^u \qquad \frac{A\supset B\downarrow \quad A\uparrow}{B\downarrow}\supset\mathsf{E}$$

One dimension along which connectives vary is *polarity*: some connectives are positive, and some are negative. We cannot yet make this distinction precise, but some students have already begun to observe it. Later on, we may see that negative connectives have elimination forms as uses, but positive connectives have elimination forms as verifications.

The calculus of verifications and uses has one extra rule which was not visible in the original logic:

$$\frac{A\downarrow}{A\uparrow}\updownarrow$$

Would it be reasonable to add the inverse of the above rule, which concludes $A\downarrow$ from $A\uparrow$? What would be the consequences of this?

Task 4. Give a verification for this proposition $(A\vee B)\supset(A\vee B)$

Solution 4:
$$\dfrac{\dfrac{\overline{A\vee B\downarrow}^{\,u} \quad \dfrac{\dfrac{\overline{A\downarrow}^{\,v}}{A\uparrow}\updownarrow}{A\vee B\uparrow}\vee I_1 \quad \dfrac{\dfrac{\overline{B\downarrow}^{\,w}}{B\uparrow}\updownarrow}{A\vee B\uparrow}\vee I_2}{A\vee B\uparrow}\vee E^{v,w}}{A\vee B\supset A\vee B\uparrow}\supset I^u$$

Task 5. Give a verification for this proposition $(A\supset B\supset C)\supset((A\wedge B)\supset C)$

Solution 5:
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{A\supset B\supset C\downarrow}^{\,u} \quad \dfrac{\dfrac{\overline{A\wedge B\downarrow}^{\,v}}{A\downarrow}\wedge\mathsf{E}_1}{A\uparrow}\updownarrow}{B\supset C\downarrow}\supset\downarrow \quad \dfrac{\dfrac{\overline{A\wedge B\downarrow}^{\,v}}{B\downarrow}\wedge\mathsf{E}_2}{B\uparrow}\updownarrow}{C\downarrow}\supset E}{C\uparrow}\updownarrow}{A\wedge B\supset C\uparrow}\supset I^v}{(A\supset B\supset C)\supset(A\wedge B\supset C)\uparrow}\supset I^u$$