RECITATION 2

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 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

$$\frac{M : A \text{ true} \qquad N : B \text{ true}}{\langle M, N\rangle : A \wedge B \text{ true}} \qquad \frac{M : A \text{ true}}{\mathsf{inl}(M) : A \vee B \text{ true}} \qquad \frac{M : B \text{ true}}{\mathsf{inr}(M) : A \vee B \text{ true}} \qquad \frac{M : A \wedge B \text{ true}}{\mathsf{fst}(M) : A \text{ true}}$$

$$\frac{M : A \wedge B \text{ true}}{\mathsf{snd}(M) : B \text{ true}} \qquad \frac{M : A \vee B \text{ true} \qquad \begin{array}{c} \overline{u : A \text{ true}}^{\,u} \\ \vdots \\ \hline N : C \text{ true} \end{array} \qquad \begin{array}{c} \overline{v : B \text{ true}}^{\,v} \\ \vdots \\ \hline R : C \text{ true} \end{array}}{\mathsf{case}\ M\ \mathsf{of}\ \mathsf{inl}(c) \Rightarrow N \mid \mathsf{inl}(c) \Rightarrow R : C \text{ true}}\ u,v \qquad \frac{\begin{array}{c} \overline{u : A \text{ true}}^{\,u} \\ \vdots \\ \hline M : B \text{ true} \end{array}}{\mathsf{fn}\ u \Rightarrow M : A \supset B \text{ true}}\ u$$

$$\frac{M : A \supset B \text{ true} \qquad N : A \text{ true}}{M(N) : B \text{ true}}$$

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.

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

Date: September 8, 2017.

[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.

Proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{A \supset B \supset C}^{\,u} \qquad \overline{A}^{\,w}}{B \supset C} \qquad \dfrac{\overline{A \supset B}^{\,v} \qquad \overline{A}^{\,w}}{B}}{C}}{A \supset C}\,w}{(A \supset B) \supset A \supset C}\,v}{(A \supset B \supset C) \supset (A \supset B) \supset A \supset C}\,u$$

Program: `fn f => fn g => fn a => f a (g a)`

(2) $(A \supset B \supset C) \supset (B \supset A \supset C)$

Proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{A \supset (B \supset C)}^{\,a} \qquad \overline{A}^{\,c}}{B \supset C} \qquad \overline{B}^{\,b}}{C}}{A \supset C}\,c}{B \supset (A \supset C)}\,b}{(A \supset B \supset C) \supset (B \supset (A \supset C))}\,a$$

Program: `fn f => fn a => fn b => f b a`

(3) $A \wedge (B \vee C) \supset (A \wedge B) \vee (A \wedge C)$

Proof:

$$\dfrac{\dfrac{\dfrac{\overline{A \wedge (B \vee C)}^{\,u}}{B \vee C} \qquad \dfrac{\dfrac{\dfrac{\overline{A \wedge (B \vee C)}^{\,u}}{A} \qquad \overline{B}^{\,w}}{A \wedge B}}{(A \wedge B) \vee (A \wedge C)} \qquad \dfrac{\dfrac{\dfrac{\overline{A \wedge (B \vee C)}^{\,u}}{A} \qquad \overline{C}^{\,w}}{A \wedge C}}{(A \wedge B) \vee (A \wedge C)}}{(A \wedge B) \vee (A \wedge C)}\,w}{A \wedge (B \vee C) \supset (A \wedge B) \vee (A \wedge C)}\,u$$

Program: `fn x => case snd x of inl b => inl (fst x, b) | inr c => inr (fst x, c)`

(4) $(\top \vee \top) \supset (\top \vee \top) \supset (\top \vee \top)$

Proof:

$$\dfrac{\dfrac{\dfrac{\overline{\top \vee \top}^{\,u} \qquad \overline{\top \vee \top}^{\,w} \qquad \dfrac{\overline{\top}}{\top \vee \top}\,\vee\,\mathrm{I2}}{\top \vee \top}\,v}{(\top \vee \top) \supset (\top \vee \top)}\,w}{(\top \vee \top) \supset (\top \vee \top) \supset (\top \vee \top)}\,u$$

Program: `fn a => fn b => case a of inl _ => b | inr _ => inr ()`

(5) $(\top \vee \top) \supset (\top \vee \top) \supset (\top \vee \top)$

Proof:

$$\dfrac{\dfrac{\dfrac{\overline{\top \vee \top}^{\,u} \qquad \dfrac{\overline{\top}}{\top \vee \top}\,\vee\,\mathrm{I1} \qquad \overline{\top \vee \top}^{\,w}}{\top \vee \top}\,v}{(\top \vee \top) \supset (\top \vee \top)}\,w}{(\top \vee \top) \supset (\top \vee \top) \supset (\top \vee \top)}\,u$$

Program: `fn a => fn b => case a of inl _ => inl () | inr _ => b`