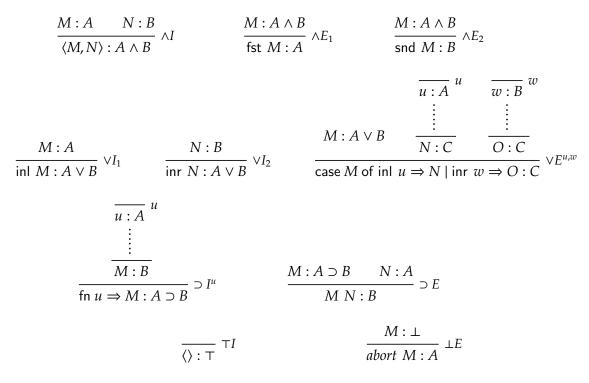
1 Proofs Are Programs

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
$A \lor B$	A + B
$A \supset B$	$A \rightarrow B$
Т	1 (unit)
L	0 (void)
	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:



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

¹Of 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:

$\overline{A \supset B \supset C \text{ true}}^f$	$\overline{A \text{ true}}^a$	h	
$B \supset C$ true		$\frac{\overline{B} \text{ true}^{b}}{\overline{B} \text{ true}} \supset \overline{B}$	
Ct	true	J L	$- \supset I^a$
A	$\supset C$ true		- <u>- 1</u>
$B \supset A \supset C \text{ true} \qquad \qquad \supset I^f$			
$(A \supset B \supset C) \supset (B \supset A \supset C) \text{ true}$			

Program:

$$\operatorname{fn} f \Longrightarrow \operatorname{fn} b \Longrightarrow \operatorname{fn} a \Longrightarrow (f a) b$$

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

Solution 2: Proof:

Let *X* be:

$\overline{A \supset B \text{ true}}^f$	$\frac{\overline{A \text{ true}}^a}{\overline{A \text{ true}}} \supset E$
<i>B</i> true	V I1
$B \lor C t$	

Let Y be:

$$\frac{\overline{A \supset C \text{ true}}^{g} \quad \overline{A \text{ true}}^{a}}{C \text{ true}} \supset E}{B \lor C \text{ true}} \lor I_{2}$$

The overall proof is:

$$\frac{\overline{(A \supset B) \text{ true } \lor (A \supset C) \text{ true}}^{fg} \quad X \quad Y}{B \lor C \text{ true}} \lor E^{f,g}}$$

$$\frac{A \supset (B \lor C) \text{ true}}{((A \supset B) \lor (A \supset C)) \supset A \supset (B \lor C) \text{ true}} \supset I^{fg}$$

Program:

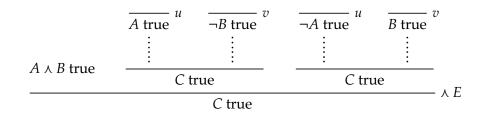
fn
$$u \Rightarrow$$
 fn $v \Rightarrow$ case u of inl $f \Rightarrow$ inl $(f v) |$ inr $g \Rightarrow$ inr $(g v)$

3 Inventing proof terms

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

$$\frac{A \text{ true}}{A \text{ true}} \stackrel{u}{\underbrace{\frac{B \text{ true}}{\bot \text{ true}}}} A = \frac{I_1}{A \land B \text{ true}} \land I_1$$

$$\frac{A \text{ true}}{A \text{ true}} \stackrel{u}{\underbrace{\frac{B \text{ true}}{\bot \text{ true}}}} B \text{ true} \land I_2$$



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

$$\frac{\overline{u:B}^{u}}{M:A} \qquad \frac{\overline{u:B}^{u}}{N:\bot}$$

$$\frac{\overline{M:A}^{u}}{\operatorname{Ift}(M, u.N): A \land B}$$

$$\frac{\overline{u:A}^{u}}{M:\bot} \qquad N:B$$

$$\overline{rght}(u.M, N): A \land B$$

And the destructor...

$$\frac{E:A \land B}{\frac{\bigcup_{i=1}^{w} (a_i - a_i) - B}{M:C}} \xrightarrow{w : \neg A} (a_i - a_i) - A} (a_i - a_i) \xrightarrow{w : \neg A} (a_i - a_i)$$

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

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

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

4 Reductions

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

Task 4.

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

Solution 4:

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

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.

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

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

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

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