15-317 Lecture 4: Proofs as Programs

- HW1 Due today, 23:59 (Eastern time)
- HW2 out today, due next Thursday
- In-person starting next lecture, Posner A35

- Propositions as types
- Proofs as programs (or expressions)
- Reduction of programs
- Expansions?

Proof Terms

- A simpler, linear representation of proofs
- New judgement $M : A$
  - "M is a proof term for proposition A"
  - "M is a program with type A"
- If A true, then $M : A$ for some M
- If $M : A$, then A true
- Beyond that:
  - "Proofs of $M : A$ are in bijective correspondence with Proofs of A true".

$$\frac{A \text{ true} \qquad B \text{ true}}{A \wedge B \text{ true}} \wedge I$$

$$\Downarrow$$

$$\frac{M : A \qquad N : B}{\langle M, N \rangle : A \wedge B} \wedge I$$

Equally valid
Less useful as a program

$$\frac{\ldots \qquad \ldots}{\wedge I(M, N) : A \wedge B} \wedge I$$

$$\frac{M : A \wedge B}{\text{fst } M : A} \wedge E_1 \qquad \frac{M : A \wedge B}{\text{snd } M : B} \wedge E_2$$

$$A \wedge B \sim A * B$$

$$\frac{}{\langle\rangle : \top}\ \top I \qquad \top \sim \text{unit} \quad \langle\rangle \sim ()$$

Implication

$$\frac{\dfrac{}{A\ \text{true}}\,u \quad \vdots \quad B\ \text{true}}{A \supset B\ \text{true}}\ \supset I^{u}$$

$$\Downarrow$$

$$\frac{\dfrac{}{u : A}\,u \quad \vdots \quad M : B}{fn\ u : A \Rightarrow M : A \supset B}\ \supset I^{u}$$

$\lambda u.M$ or $\lambda u{:}A.M$

$fn\ u \Rightarrow u : A \supset A$

$fn\ u \Rightarrow \langle u, u\rangle : A \supset (A \wedge A)$

$fn\ u \Rightarrow \langle\rangle : A \supset \top$

$$\frac{M : A \supset B \qquad N : A}{M\ N : B}\ \supset E$$

$M\ (N)$

$$\dfrac{\dfrac{\dfrac{}{u : A \wedge B}\,u}{\mathrm{snd}\ u : B}\wedge E_2 \qquad \dfrac{\dfrac{}{u : A \wedge B}\,u}{\mathrm{fst}\ u : A}\wedge E_1}{\langle \mathrm{snd}\ u, \mathrm{fst}\ u\rangle : B \wedge A}\wedge I}{\mathrm{fn}\ u : A \wedge B \Rightarrow \langle \mathrm{snd}\ u, \mathrm{fst}\ u\rangle : (A \wedge B) \supset (B \wedge A)}\supset I^u$$

$$\dfrac{\dfrac{\dfrac{}{A \wedge B\ \mathrm{true}}\,u}{B\ \mathrm{true}}\wedge E_2 \qquad \dfrac{\dfrac{}{A \wedge B\ \mathrm{true}}\,u}{A\ \mathrm{true}}\wedge E_1}{B \wedge A\ \mathrm{true}}\wedge I}{(A \wedge B) \supset (B \wedge A)\ \mathrm{true}}\supset I^u$$

$$f_n\ \underbrace{u : A \wedge B}_{\text{pattern}} \Rightarrow \langle \mathrm{snd}\ u, \mathrm{fst}\ u\rangle \quad \Big] \ f$$

$u : A \wedge B$

$\left.\begin{array}{l} \mathrm{fst}\ u : A \\ \mathrm{snd}\ u : B \end{array}\right]$

$\langle \mathrm{snd}\ u, \mathrm{fst}\ u\rangle : B \wedge A$

so $f : (A \wedge B) \supset (B \wedge A)$

(or $f : (A * B) \to (B * A)$

- We can have different proofs of the same proposition

$$\dfrac{\dfrac{\dfrac{}{u : A}\,u \qquad \dfrac{}{v : B}\,v}{\vdots}}{\dfrac{v : B}{\mathrm{fn}\ v : B \Rightarrow v : B \supset B}\,\supset I^{v}}\,\supset I^{u}$$

$$\mathrm{fn}\ u : A \Rightarrow (\mathrm{fn}\ v : B \Rightarrow v) : A \supset (B \supset B)$$

$$\dfrac{\dfrac{\dfrac{}{u : A}\,u \qquad \dfrac{}{v : A}\,v}{\vdots}}{\dfrac{\dfrac{u : A}{\mathrm{fn}\ v : A \Rightarrow u : A \supset A}\,\supset I^{v}}{\mathrm{fn}\ u : A \Rightarrow (\mathrm{fn}\ v : A \Rightarrow u) : A \supset (A \supset A)}\,\supset I^{u}}$$

$$\dfrac{\dfrac{\dfrac{}{u : A}\,u \qquad \dfrac{}{v : A}\,v}{\vdots}}{\dfrac{\dfrac{v : A}{\mathrm{fn}\ v : A \Rightarrow v : A \supset A}\,\supset I^{v}}{\mathrm{fn}\ u : A \Rightarrow (\mathrm{fn}\ v : A \Rightarrow v) : A \supset (A \supset A)}\,\supset I^{u}}$$

$$\frac{M : A}{\text{inl}_{A \vee B}\ M : A \vee B}\ \vee I_1 \qquad \frac{M : B}{\text{inr}_{A \vee B}\ M : A \vee B}\ \vee I_2$$

- In principle inl $M : A \vee$???
  if $M : A$.
- Not enough information to give
  inl M a precise type, so we annotate
  as $\text{inl}_{A \vee B}\ M$.

'a 'b Either =
  inl of 'a
| inr of 'b

$$\frac{M : A \vee B \qquad \begin{array}{c}[v : A]^{v} \\ \vdots \\ N : C\end{array} \qquad \begin{array}{c}[w : B]^{w} \\ \vdots \\ O : C\end{array}}{\text{case } M \text{ of inl } v \Rightarrow N \mid \text{inr } w \Rightarrow O : C}\ \vee E^{v,w}$$

$$\frac{M : F}{\text{abort}_C\ M : C}\ F E$$

Summary

- For every proof of A true
  there is a unique M and proof of M : A
  with the same structure (uses same rules,
  in same order, on the same propositions)
- Also the other way around.

Reduction / Computation

$$\dfrac{\dfrac{\mathcal{D} \quad \mathcal{E}}{A\ true \quad B\ true}\wedge I}{A \wedge B\ true}\wedge E_1 \quad \Longrightarrow_R \quad \mathcal{D}\ A\ true$$

$$\dfrac{\dfrac{\mathcal{D} \quad \mathcal{E}}{M : A \quad N : B}\wedge I}{\langle M, N\rangle : A \wedge B}\wedge E_1 \quad \Longrightarrow_R \quad \mathcal{D}\ M : A$$

- Proof reduction is computation

---

fn $(x, y) \Rightarrow x$

- $\mathrm{snd}\langle M, N\rangle \Longrightarrow_R N$

T: Has no reductions

- Intuitively, $\langle\rangle$ is already a value, so can't step.

- $(\mathrm{fn}(u:A) \Rightarrow M)\ N \Longrightarrow_R [N/u]M$
- $\mathrm{case}(\mathrm{inl}\ M)\ \mathrm{of}\ \mathrm{inl}\ u \Rightarrow N \mid \mathrm{inr}\ v \Rightarrow O$
  $\Longrightarrow_R [M/u]N.$
- $\mathrm{case}(\mathrm{inr}\ M)\ \mathrm{of}\ \mathrm{inl}\ u \Rightarrow N \mid \mathrm{inr}\ v \Rightarrow O$
  $\Longrightarrow_R [M/v]O$

- F: Has no reductions