

15-317 Lecture 15: Proof checking and Prolog

- Certifying verifications
- Bidirectional proof/type checking (only for λ , λ for now)

-
- Prolog demos
 - Binary numbers
 - Proof checking

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

$$\frac{R: A \wedge B \downarrow}{\text{fst } R: A \downarrow} \wedge E_1$$

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

Thm /

- Given N and A , either $N: A \uparrow$ or not. ← Normal
- Given R , either there exists A s.t. $R: A \downarrow$ or no such A exists. ↗ Neutral

$$\frac{}{u : A \downarrow}$$

$$\vdots$$

$$\frac{M : B \uparrow}{(f \text{ and } M) : A \supset B \uparrow} \supset I^u$$

$$\frac{R : A \supset B \downarrow \quad M : A \uparrow}{R \ M : B \downarrow} \supset E$$

$$\frac{R : A \downarrow}{R : A \uparrow} \downarrow \uparrow$$

Thm

- Given Γ, M, A , either $\Gamma \vdash M : A \uparrow$ or $\Gamma \not\vdash M : A \uparrow$
- Given Γ, R , either there is a unique A s.t. $\Gamma \vdash R : A \downarrow$ or no such A exists.

$$\overline{\text{inc}(e, \text{bl}(e))}^{\text{inc}_e}$$

$$\overline{\text{inc}(\text{b0}(M), \text{bl}(M))}^{\text{inc}_0}$$

$$\text{inc}(M, N)$$

$$\overline{\text{inc}(\text{bl}(M), \text{b0}(N))}^{\text{inc}_1}$$

$$\begin{array}{c} \text{bl}(M) \\ M \end{array} \left\{ \begin{array}{l} 2k+1 \\ k \end{array} \right\} \left\| \begin{array}{l} 2k+2 \\ k+1 \end{array} \right\} \left| \begin{array}{l} \text{b0}(N) \\ N \end{array} \right.$$