15-317 Lecture 16: More proof checking, Prolog internals

- Proof checking recap
- Decidability of proof checking
- Extracting ND proof terms from SC
- cut rule as proof term

- Avoiding variable collision
- Unification
- Reconstructing terms

Checkable terms $M, N ::= \langle M, N \rangle \mid fn\ v \Rightarrow M$

$\mid R \mid \ldots$

Synthesizing terms $R ::= fst\ R \mid snd\ R$

$\mid u \mid R\ M \mid \ldots$

$$\frac{M : A\uparrow}{\mathsf{inl}\ M : A \vee B\uparrow}\vee\mathrm{I}_1 \qquad \frac{M : B\uparrow}{\mathsf{inr}\ M : A \vee B\uparrow}\vee\mathrm{I}_2$$

$$\frac{R : A \vee B\downarrow \qquad \begin{array}{c}[u : A\downarrow]^u \\ \vdots \\ M : C\uparrow\end{array} \qquad \begin{array}{c}[v : B\downarrow]^v \\ \vdots \\ N : C\uparrow\end{array}}{\mathsf{case}\ R\ (\mathsf{inl}\ u \Rightarrow M,\ \mathsf{inr}\ v \Rightarrow N) : C\uparrow}\vee\mathrm{E}$$

$$M, N ::= \langle M, N \rangle \mid \mathsf{fn}\, u \Rightarrow M \mid \mathsf{in}\, l\, M \mid \mathsf{in}\, r\, M \mid \langle\rangle \mid \mathsf{abort}\, R \mid R$$

$$R ::= \mathsf{fst}\, R \mid \mathsf{snd}\, R \mid u \mid R\, M \mid \mathsf{case}\, R\, \mathsf{of} \ldots$$

Theorem/(i) Given Γ, M, A either $\Gamma \vdash M : A\uparrow$ or $\Gamma \not\vdash M : A\uparrow$

(ii) Given Γ, R, either there is a unique A s.t. $\Gamma \vdash R : A\downarrow$ or no such A exists

Proof/ By induction on the structure of M/R^*

* (M/R, part # of theorem statement)

Case $M = (fn\ u \Rightarrow N)$: $\uparrow$

Case $A \neq B \supset C$:

$\Gamma \not\vdash (fn\ u \Rightarrow N) : A\uparrow$

Case $A = B \supset C$:

$$\frac{\Gamma, u : B\downarrow \vdash^{?} N : C\uparrow}{\Gamma \vdash fn\ u \Rightarrow N : A\uparrow}\ \supset I$$

i.h.(i) $N < M$

Case $M = R\ N$ i

by i.h. (ii) on R, either $\exists!\ C$ s.t. $\Gamma \vdash R : C\downarrow$ or no such C exists.

↪ Case $C \neq B \supset A$: ⊬

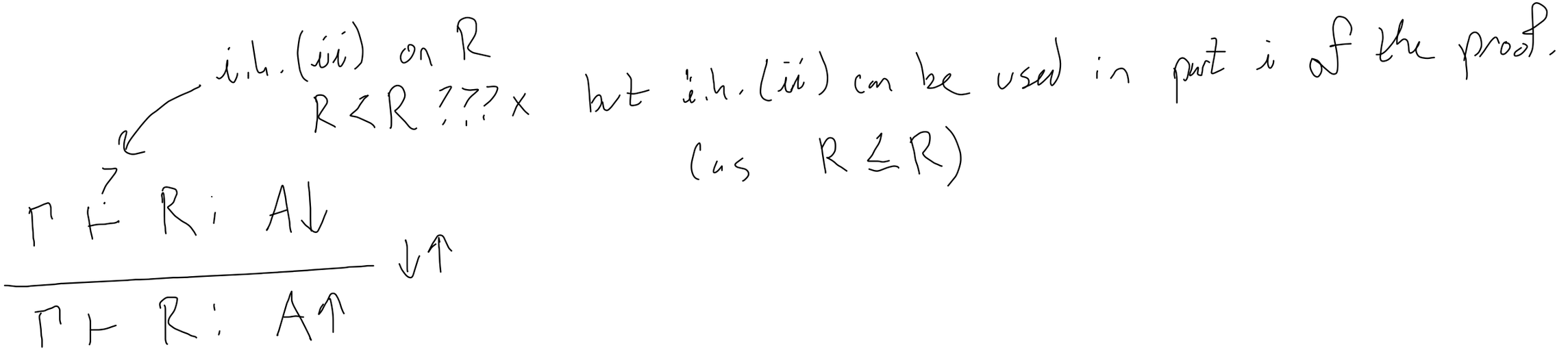
Case $C = B \supset A$:

by i.h. (i) on N, either $\Gamma \vdash N : B\uparrow$ or $\Gamma \not\vdash N : B\uparrow$

$$\frac{\Gamma \stackrel{?}{\vdash} R : B \supset A\downarrow \qquad \Gamma \stackrel{?}{\vdash} N : B\uparrow}{\Gamma \vdash R\ N : A\uparrow}\ \supset E$$

Case $M = R : i$

WTS: given Γ, M, A, $\Gamma \vdash M : A\uparrow$ or $\Gamma \not\vdash M : A\uparrow$



$\Gamma \longrightarrow A \quad \rightleftharpoons \quad \Gamma\downarrow \vdash A\uparrow$

$R_1 : A_1\downarrow, R_2 : A_2\downarrow, \ldots, R_n : A_n\downarrow \longrightarrow N : A\uparrow$

Theorem / If $\overline{A_i} \longrightarrow A$, then for all Δ s.t.

$\Delta \vdash R_j : A_j\downarrow$ for each j, there exists N s.t.

$\Delta \vdash N : A\uparrow$ and $\underline{\overline{R_i : A_i} \longrightarrow N : A}$

$$\frac{}{\Gamma, R : P \longrightarrow R : P}\ id$$

$$\frac{\Gamma \longrightarrow M : A \qquad \Gamma \longrightarrow N : B}{\Gamma \longrightarrow \langle M, N \rangle\ A \wedge B}\ \wedge R$$

$$\frac{\Gamma, \mathrm{fst}\ R : A, \mathrm{snd}\ R : B \longrightarrow N : C}{\Gamma, R : A \wedge B \longrightarrow N : C}\ \wedge L$$

$$\frac{\Gamma, v : A \longrightarrow M : B}{\Gamma \longrightarrow \mathrm{fn}\ v \Rightarrow M : A \supset B}\ \supset R$$

$$\frac{\Gamma, R : A \supset B \longrightarrow M : A \qquad \Gamma, R\ M : B \longrightarrow N : C}{\Gamma, R : A \supset B \longrightarrow N : C}\ \supset L$$

$$\frac{\Gamma \longrightarrow A \qquad \Gamma, A \longrightarrow C}{\Gamma \longrightarrow C}\ \text{cut}$$

$$\frac{\Gamma \longrightarrow M : A\uparrow \qquad \Gamma, u : A\downarrow \longrightarrow N : C\uparrow}{\Gamma \longrightarrow \underbrace{\text{let } u : A = M \text{ in } N}_{[M/u]N} : C\uparrow}\ \text{cut}$$

$$\frac{}{inc(e, b1(e))} \qquad \frac{}{inc(b0\ b0\ N,\ b1\ b0\ N)}$$

$$\frac{}{inc(b0\ b1\ N,\ b1\ b1\ N)} \qquad \frac{inc(N, M)}{inc(b1\ N,\ b0\ M)}$$

$$\frac{N = e \quad M = b1\ b1\ N}{inc(b0\ b1\ e,\ M)} \qquad \frac{inc(N, M) \quad X_1 = b0\ M \quad N = b0\ b1\ e}{inc(b1\ b0\ b1\ e,\ X_1)}$$

$$\frac{inc(X_2, X_3)}{inc(b1\ X_2, b0\ X_3)} \leftarrow \frac{inc(M, N)}{inc(b1\ M, b0\ N)}$$

$$\frac{}{inc(b0\,b1\ X_4, b1\,b1\ X_4)} \leftarrow \frac{}{inc(b0\ b1\ N, b1\ b1\ N)}$$

$$\frac{}{inc(b0\ b1\ e, X_3)} \qquad \frac{X_4 = e \quad X_3 = b1\ b1\ X_4}{X_4 = e \quad X_3 = b1\ b1\ e}$$

$$\frac{inc(X_2, X_3)}{inc(b1\ b0\ b1\ e, X_1)} \qquad X_2 = b0\ b1\ e \quad X_1 = b0\ X_3$$

$$\begin{cases} X_1 = b0\ b1\ b1\ e \end{cases}$$

Unification

- Input is a list of constraints $t_1 \stackrel{?}{=} t_2$
- Output is a mapping σ from variables to terms satisfying the constraints

  i.e. $\sigma(t_1) = \sigma(t_2)$.

---

terms t : $X \mid f(t_1, \ldots, t_n)$

$C()$

Consider a single constraint

Case $X \stackrel{?}{=} Y$:

- $\sigma(X) = Y$
- $\sigma(Y) = X$
- $\sigma(X) = \sigma(Y) = \_316$

Case $f(t_1, \ldots, t_n) \stackrel{?}{=} g(u_1, \ldots, u_k)$

If $f \neq g$ return no

If $n \neq k$ return no

Otherwise, recurse on $t_1 \stackrel{?}{=} u_1, \ldots, t_n \stackrel{?}{=} u_n$

Case: $X = f(t_1, \ldots t_n)$

- $\sigma(X) = f(t_1, \ldots, t_n)$? ✗ cyclic terms
- $\sigma(X) = f(t_1, \ldots, t_n)$: if X does not occur in $t_1, \ldots, t_n$

Apply σ to remaining constraints

Apply σ to σ?