Proof Checker Notes

Yu-Yang Lin

July 2, 2015

1 Syntax Grammar

$$
\begin{array}{rl}
\text{(types)} & \tau ::= \mathrm{bool} \mid \tau \to \tau \mid \mathrm{nat} \mid \mathrm{list}\ \tau \\
\text{(hypotheses)} & \mathrm{A}\ ,\mathrm{B} ::= \top \mid \bot \mid \mathrm{A} \wedge \mathrm{B} \mid \mathrm{A} \vee \mathrm{B} \mid \mathrm{A} \supset \mathrm{B} \mid \forall\, x : \tau\ .\ \mathrm{A} \mid \exists\, x : \tau\ .\ \mathrm{A} \mid \mathrm{t} = \mathrm{t} : \tau \\
\text{(terms)} & \mathrm{e}\ ,\mathrm{t} ::= x \mid \mathrm{t}\ \mathrm{t} \mid \mathrm{true} \mid \mathrm{false} \mid [\ ] \mid \mathrm{t} :: \mathrm{t} \mid \mathrm{zero} \mid \mathrm{suc}(\ \mathrm{t}\ ) \\
\text{(term context)} & \psi ::= .\ \mid \psi, x : \tau
\end{array}
$$

$$
\begin{array}{lcl}
\psi & \vdash & \mathrm{t} : \tau \\
\psi & \vdash & \mathrm{A\ prop}
\end{array}
$$

2 Rules for terms and hypotheses

Natural Numbers:

$$\frac{}{\psi \vdash \mathrm{zero} : \mathrm{nat}}\ \text{(nat-zero)} \qquad \frac{\psi \vdash \mathrm{t} : \mathrm{nat}}{\psi \vdash \mathrm{suc}(\ \mathrm{t}\ ) : \mathrm{nat}}\ \text{(nat-suc-n)}$$

Booleans:

$$\frac{}{\psi \vdash \mathrm{true} : \mathrm{bool}}\ \text{(bool-true)} \qquad \frac{}{\psi \vdash \mathrm{false} : \mathrm{bool}}\ \text{(bool-false)}$$

Lists:

$$\frac{}{\psi \vdash [\ ] : \mathrm{list\ t}}\ \text{(list-empty)} \qquad \frac{\psi \vdash \mathrm{t}' : \mathrm{t} \qquad \psi \vdash \mathrm{t}'' : \mathrm{list\ t}}{\psi \vdash \mathrm{t}' :: \mathrm{t}'' : \mathrm{list\ t}}\ \text{(list-hd::tl)}$$

Variables:

$$\frac{x : \tau \in \psi}{\psi \vdash x : \tau}\ \text{(var)}$$

Application:

$$\frac{\psi \vdash \mathrm{t} : \tau \to \tau' \qquad \psi \vdash \mathrm{t}' : \tau}{\psi \vdash \mathrm{t}\ \mathrm{t}' : \tau'}\ \text{(app)}$$

Truth and Falsity Propositions:

$$\frac{}{\psi \vdash \top\ \mathrm{prop}}\ (\top\text{-prop}) \qquad \frac{}{\psi \vdash \bot\ \mathrm{prop}}\ (\bot\text{-prop})$$

Binary Relation Propositions:

$$\frac{\psi \vdash \mathrm{A\ prop} \qquad \psi \vdash \mathrm{B\ prop}}{\psi \vdash \mathrm{A} \wedge \mathrm{B\ prop}}\ (\wedge\text{-prop})$$

$$\frac{\psi \vdash \mathrm{A\ prop} \qquad \psi \vdash \mathrm{B\ prop}}{\psi \vdash \mathrm{A} \vee \mathrm{B\ prop}}\ (\vee\text{-prop})$$

$$\frac{\psi \vdash \text{A prop} \qquad \psi \vdash \text{B prop}}{\psi \vdash \text{A} \supset \text{B prop}} \;(\supset\text{-prop})$$

$$\frac{\psi \vdash \text{t}:\tau \qquad \psi \vdash \text{t}':\tau}{\psi \vdash (\text{t} = \text{t}' : \tau)\ \text{prop}} \;(\text{eq-prop})$$

Quantifier Propositions:

$$\frac{\psi, x:\tau \vdash \text{A prop}}{\psi \vdash \forall x:\tau.\ \text{A prop}} \;(\forall\text{-prop})$$

$$\frac{\psi, x:\tau \vdash \text{A prop}}{\psi \vdash \exists x:\tau.\ \text{A prop}} \;(\exists\text{-prop})$$

3 Terms type checking and inference

Type Inference:

$$\bar{\psi} \vdash \bar{t} \Rightarrow \overset{+}{\tau}$$

Type Checking:

$$\bar{\psi} \vdash \bar{t} \Leftarrow \bar{\tau}$$

Function Signatures:

```
check_term  :  ψ → t → τ option
check_term  :  ψ → t → τ → unit option
check_prop  :  ψ → A → unit option

val infer_term  :  ctx -> term -> tp option
val infer_term  :  ctx -> term -> tp -> unit option
val check_prop  :  ctx -> prop -> unit option
```

4 Rules for well-formedness of proofs

(proofs)	p , q	::=	by H
		|	(p , q)
		|	`let` (H′,H″) = H `in` p
		|	(p , q) `either`
		|	`match [`H`]` : (A ∨ B) `with (`
			| A [H′] : p -> C
			| B [H″] : q -> C)
(hypotheses context)	Γ	::=	·
		|	Γ , H : A
		|	Assume A [H] , p

$$\psi;\Gamma \vdash \text{p} : \text{A}$$
$$\psi \vdash \Gamma$$

```
check_proof :  ψ → Γ → P → A → unit option
```

Conjunction:

$$\frac{\psi;\Gamma, \text{H} : \text{A} \wedge \text{B} , \text{H}' : \text{A} , \text{H}'' : \text{B} \vdash \text{p} : \text{C}}{\psi;\Gamma, \text{H} : \text{A} \wedge \text{B} \vdash \texttt{let}\ (\text{H}', \text{H}'')\ =\ \text{H}\ \texttt{in}\ \text{p}} \;(\wedge\text{L})$$

$$\frac{\psi;\Gamma \vdash \mathrm{p} : \mathrm{A} \qquad \psi;\Gamma \vdash \mathrm{q} : \mathrm{B}}{\psi;\Gamma \vdash (\mathrm{p}\ ,\ \mathrm{q}) : \mathrm{A} \wedge \mathrm{B}}\ (\wedge\mathrm{R})$$

Disjunction:

$$\frac{\psi;\Gamma\ ,\ \mathrm{H} : \mathrm{A} \vee \mathrm{B}\ ,\ \mathrm{H}' : \mathrm{A} \vdash \mathrm{p} : \mathrm{C} \qquad \psi;\Gamma\ ,\ \mathrm{H} : \mathrm{A} \vee \mathrm{B}\ ,\ \mathrm{H}'' : \mathrm{B} \vdash \mathrm{q} : \mathrm{C}}{\psi;\Gamma, \mathrm{H} : \mathrm{A} \vee \mathrm{B} \vdash \texttt{match [H] with(} \mathrm{A}\ \texttt{[H']} : \mathrm{p} \mid \mathrm{B}\ \texttt{[H'']} : \mathrm{q}\ \texttt{)} : \mathrm{C}}\ (\vee\mathrm{L})$$

$$\frac{\psi;\Gamma \vdash \mathrm{A}}{\psi;\Gamma \vdash \mathrm{A} \vee \mathrm{B}}\ (\vee R_1)$$

$$\frac{\psi;\Gamma \vdash \mathrm{B}}{\psi;\Gamma \vdash \mathrm{A} \vee \mathrm{B}}\ (\vee R_2)$$

Implication:

$$\frac{\psi;\Gamma, \mathrm{H} : \mathrm{A} \supset \mathrm{B} \vdash \mathrm{p} : \mathrm{A} \qquad \psi;\Gamma, \mathrm{H} : \mathrm{A} \supset \mathrm{B}\ ,\ \mathrm{H}' : \mathrm{B} \vdash \mathrm{q} : \mathrm{C}}{\psi;\Gamma, \mathrm{H} : \mathrm{A} \supset \mathrm{B} \vdash (\mathrm{p}, \mathrm{B}\ [\ \mathrm{H}'\ ]\ \text{via}\ \mathrm{H}, \mathrm{q}) : \mathrm{C}}\ (\supset\mathrm{L})$$

$$\frac{\psi;\Gamma\ ,\ \mathrm{H} : \mathrm{A} \vdash \mathrm{p} : \mathrm{B}}{\psi;\Gamma \vdash (\ \text{Assume A}\ [\ \mathrm{H}\ ]\ ,\ \mathrm{p}\ ) : \mathrm{A} \supset \mathrm{B}}\ (\supset\mathrm{R})$$

Using hypotheses:

$$\frac{}{\psi;\Gamma, [\ \mathrm{H}\ ] : \mathrm{A} \vdash \text{by}\ \mathrm{H} : \mathrm{A}}\ (\text{by})$$

$$\frac{\psi;\Gamma \vdash \mathrm{p} : \mathrm{A}}{\psi;\Gamma \vdash \mathrm{p}\ \text{Therefore}\ \mathrm{A} : \mathrm{A}}\ (\text{therefore})$$