Proof Checker Notes

Yu-Yang Lin

June 20, 2015

1 Syntax Grammar

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

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

2 Rules for terms and hypotheses

Natural Numbers:

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

Booleans:

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

Lists:

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

Variables:

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

Binary Relation Propositions:

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

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

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

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

Quantifier Propositions:

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

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

```
check_term  :  ctx -> term -> tp option
check_prop  :  ctx -> prop -> unit option

i.e.
      check_term  :  ψ → t → τ option
      check_prop  :  ψ → A → unit option
```

3 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

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

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

Conjunction:

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

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

Disjunction:

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

$$\frac{\psi; \Gamma \vdash \text{A}}{\psi; \Gamma \vdash \text{A} \wedge \text{B}} \quad (\vee R_1)$$

$$\frac{\psi; \Gamma \vdash \text{B}}{\psi; \Gamma \vdash \text{A} \wedge \text{B}} \quad (\vee R_2)$$

Implication:

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

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

Using hypotheses:

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

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