Proof Checker Notes

Yu-Yang Lin

June 16, 2015

1 Syntax Grammar

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

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

2 Rules for terms and hypotheses

Natural Numbers:

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

Booleans:

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

Lists:

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

Variables:

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

Binary Relation Propositions:

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

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

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

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

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

$$\begin{array}{rcll}
\text{(proofs)} & \text{p , q} & ::= & \text{by H} \\
 & & | & \text{(p , q)} \\
 & & | & \texttt{let}\ \text{(H',H'') = H}\ \texttt{in}\ \text{p} \\
 & & | & \text{(p , q)}\ \texttt{either} \\
 & & | & \texttt{match [H] : (}A \vee B\texttt{) with (} \\
 & & & \qquad \texttt{|}\ \text{A [H'] : p -> C} \\
 & & & \qquad \texttt{|}\ \text{B [H''] : q -> C)} \\
\text{(hypotheses context)} & \Gamma & ::= & \cdot \\
 & & | & \Gamma\text{ , H : A} \\
 & & | & \text{Assume A [H] , p}
\end{array}$$

$$\begin{array}{ll}
\psi;\Gamma & \vdash \text{p : A} \\
\psi & \vdash \Gamma
\end{array}$$

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

Conjunction:

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

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

Disjunction:

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

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

Implication:

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

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

Using hypotheses:

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

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