Proof Checker Notes

Yu-Yang Lin

June 24, 2015

1 Syntax Grammar

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

$$
\begin{array}{rcl}
\psi & \vdash & t : \tau \\
\psi & \vdash & A \text{ prop}
\end{array}
$$

2 Rules for terms and hypotheses

Natural Numbers:

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

Booleans:

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

Lists:

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

Variables:

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

Binary Relation Propositions:

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

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

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

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

Quantifier Propositions:

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

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

```
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
```

$$\psi ; \Gamma \ \vdash p : A$$
$$\psi \ \vdash \Gamma$$

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

Conjunction:

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

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

Disjunction:

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

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

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

Implication:

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

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

Using hypotheses:

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

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