Proof Checker Notes

Yu-Yang Lin

July 7, 2015

1 Syntax Grammar

(types)	τ ::= bool ∣ $\tau \to \tau$ ∣ nat ∣ list τ
(hypotheses)	A , B ::= $\top$ ∣ $\bot$ ∣ A $\wedge$ B ∣ A $\vee$ B ∣ A $\supset$ B ∣ $\forall\, x : \tau$. A ∣ $\exists\, x : \tau$. A ∣ t = t : τ
(terms)	e , t ::= x ∣ t t ∣ true ∣ false ∣ [ ] ∣ t :: t ∣ zero ∣ suc(t)
(term context)	ψ ::= . ∣ ψ, $x : \tau$

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

2 Specification rules of terms typing and hypotheses

2.1 Terms

Natural Numbers:

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

Booleans:

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

Lists:

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

Variables:

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

Application:

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

2.2 Propositions

Truth and Falsity Propositions:

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

Binary Relation Propositions:

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

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

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

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

Quantifier Propositions:

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

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

3 Implementation rules for type inference and checking

3.1 Syntax grammar

(infer) e ::= x | e v | true | false | zero | suc(e)
(check) v ::= v :: v | nil | e

Type Inferece Rule:

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

Type Checking Rule:

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

3.2 Term type inference

Variables:

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

Application:

$$\frac{\psi \vdash \text{t} \Rightarrow \tau \to \tau' \qquad \psi \vdash \text{t}' \Leftarrow \tau}{\psi \vdash \text{t t}' \Rightarrow \tau'} \quad (\text{app})$$

Natural Numbers:

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

Booleans:

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

3.3 Term type checking

Lists:

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

Inference Case:

$$\frac{\psi \vdash t \Rightarrow \tau' \qquad \tau = \tau'}{\psi \vdash t \Leftarrow \tau} \quad \text{(app)}$$

3.4 Propositions type checking

Truth and Falsity Propositions:

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

Binary Relation Propositions:

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

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

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

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

Quantifier Propositions:

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

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

3.5 Function signatures

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

4 Rules for well-formedness of proofs

4.1 Syntax grammar

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

$$
\begin{array}{rl}
\psi;\Gamma & \vdash \mathrm{p} : \mathrm{A} \\
\psi & \vdash \Gamma
\end{array}
$$

4.2 Rules

Truth and Falsity:

$$\frac{}{\psi;\Gamma \vdash \top : \mathrm{C}}\ (\top\mathrm{R}) \qquad \frac{}{\psi;\Gamma, \mathrm{H} : \bot \vdash \texttt{match}\ \mathrm{H}\ \texttt{with}\ \bot : \mathrm{C}}\ (\bot\mathrm{L})$$

Conjunction:

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

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

Disjunction:

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

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

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

Implication:

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

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

Using hypotheses:

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

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

4.3 Function signature

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