# Proof Checker Notes

Yu-Yang Lin

July 4, 2015

## 1 Syntax Grammar

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

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

## 2 Specification rules of terms typing and hypotheses

### 2.1 Terms

Natural Numbers:

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

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:

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

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

$$\begin{array}{rl} \text{(infer)} & \text{e ::= x} \mid \text{e v} \mid \text{true} \mid \text{false} \mid \text{zero} \mid \text{suc( e )} \\ \text{(check)} & \text{v ::= v :: v} \mid \text{nil} \mid \text{e} \end{array}$$

Type Inferece Rule:

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

Type Checking Rule:

$$\overset{-}{\psi} \vdash \overset{-}{t} \Leftarrow \overset{-}{\tau}$$

## 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:

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

Inference Case:

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

## 3.4 Propositions type checking

Truth and Falsity Propositions:

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

Binary Relation Propositions:

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

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

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

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

Quantifier Propositions:

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

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

## 3.5 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

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

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

## 4.2 Rules

Conjunction:

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

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

Disjunction:

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

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

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

Implication:

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

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

Using hypotheses:

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

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

### 4.3 Function signature

$$\texttt{check\_proof} : \psi \rightarrow \Gamma \rightarrow \texttt{P} \rightarrow \texttt{A} \rightarrow \texttt{unit option}$$