Proof Checker Notes

Yu-Yang Lin

July 9, 2015

1 Syntax Grammar

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

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

2 Specification rules of terms typing and hypotheses

Note: functions are included as term types, but not directly as term constructors. Instead, function terms are added into the term context (ψ) manually. This simplifies the checker since function type inference is not required.

2.1 Terms

Natural Numbers:

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

Booleans:

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

Lists:

$$\frac{}{\psi \vdash [\ ] : \mathrm{list\ t}}\ \text{(list-nil)} \qquad \frac{\psi \vdash \mathrm{t}' : \mathrm{t} \qquad \psi \vdash \mathrm{t}'' : \mathrm{list\ t}}{\psi \vdash \mathrm{t}' :: \mathrm{t}'' : \mathrm{list\ t}}\ \text{(list-cons)}$$

Variables:

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

Application:

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

2.2 Propositions

Truth and Falsity Propositions:

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

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

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

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:

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

Natural Numbers:

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

Booleans:

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

3.3 Term type checking

Lists:

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

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:

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

Binary Relation Propositions:

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

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

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

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

Quantifier Propositions:

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

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

3.5 Function signatures

$$\begin{array}{lcl} \texttt{infer\_term} & : & \psi \rightarrow \texttt{t} \rightarrow \tau \ \texttt{option} \\ \texttt{check\_term} & : & \psi \rightarrow \texttt{t} \rightarrow \tau \rightarrow \texttt{unit option} \\ \texttt{check\_prop} & : & \psi \rightarrow \texttt{A} \rightarrow \texttt{unit option} \end{array}$$

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

4 Well-formedness of proofs

4.1 Syntax grammar

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

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

4.2 Rules

Truth and Falsity:

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

Conjunction:

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

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

Disjunction:

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

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

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

Implication:

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

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

Using hypotheses:

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

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

4.3 Function signature

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

5 Dealing with quantifiers in proofs

5.1 Rules

Existentials:

$$\frac{\psi;\Gamma \vdash \mathrm{t} : \tau \qquad \psi;\Gamma \vdash \mathrm{p} : [\mathrm{x} \mapsto \mathrm{t}]\ \mathrm{A}}{\psi;\Gamma \vdash \mathrm{Choose\ t\ ;\ p} : \exists x : \tau.\mathrm{A}} \quad (\exists\ \mathrm{R})$$

$$\frac{\psi, y : \tau;\Gamma, \mathrm{H} : \exists x : \tau.A, \mathrm{H'}\text{: } [x \mapsto y]A \vdash \mathrm{p} : \mathrm{C}}{\psi;\Gamma, \mathrm{H} : \exists x : \tau.\ \mathrm{A} \vdash \texttt{let}\ (y,\mathrm{H'}) = \mathrm{H}\ \texttt{in}\ \mathrm{p} : \mathrm{C}} \quad (\exists\ \mathrm{L})$$

Universals:

$$\frac{\psi, y : \tau;\Gamma, \vdash \mathrm{p} : [x \mapsto y]\ \mathrm{A}}{\psi;\Gamma \vdash \mathrm{Assume}\ y : \tau\ .\ \mathrm{p} : \forall x : \tau.A} \quad (\forall\ \mathrm{R})$$

$$\frac{\psi;\Gamma \vdash \mathrm{t} : \tau \qquad \psi;\Gamma\ , \mathrm{H} : \forall x : \tau\ .\ \mathrm{A}\ , \mathrm{H'} : [\mathrm{x} \mapsto \mathrm{t}]\ \mathrm{A} \vdash \mathrm{p} : \mathrm{C}}{\psi;\Gamma, \mathrm{H} : \forall x : \tau.\ \mathrm{A} \vdash \texttt{let}\ \mathrm{H'} = \mathrm{H\ with\ t}\ \texttt{in}\ \mathrm{p} : \mathrm{C}} \quad (\forall\ \mathrm{L})$$

5.2 Substituting terms into variables

$$\texttt{subs} \ = \ [x \mapsto z]$$

$$\begin{array}{lll} \texttt{subs\_term} & : & x \to \texttt{t} \to \texttt{t} \to \texttt{t} \\ \texttt{subs\_prop} & : & x \to \texttt{t} \to \texttt{A} \to [x] \to \texttt{A} \end{array}$$

```
val subs_term  :  var -> term -> term -> term
val subs_prop  :  var -> term -> prop -> var list -> prop
```

6 α-equivalence

6.1 Terms

Variables:

$$\frac{}{x \equiv x} \quad (\text{var}\equiv)$$

Booleans:

$$\frac{}{\mathrm{true} \equiv \mathrm{true}} \quad (\text{bool-true}\equiv) \qquad \frac{}{\mathrm{false} \equiv \mathrm{false}} \quad (\text{bool-false}\equiv)$$

Natural Numbers:

$$\frac{}{\text{zero} \equiv \text{zero}} \quad (\text{nat-zero}\equiv) \qquad \frac{\text{t} \equiv \text{t}'}{\text{suc(t)} \equiv \text{suc(t}' \text{)}} \quad (\text{nat-suc-n}\equiv)$$

Lists:

$$\frac{}{[] \equiv []} \quad (\text{list-nil}\equiv) \qquad \frac{\text{e} \equiv \text{e}' \qquad \text{v} \equiv \text{v}'}{\text{e::v} \equiv \text{e}'\text{::v}'} \quad (\text{list-cons}\equiv)$$

Application:

$$\frac{\text{e} \equiv \text{e}' \qquad \text{v} \equiv \text{v}'}{\text{e v} \equiv \text{e}' \text{ v}'} \quad (\text{var}\equiv)$$

6.2 Propositions

Truth and Falsity:

$$\frac{}{\top \equiv \top} \quad (\top \equiv) \qquad \frac{}{\bot \equiv \bot} \quad (\bot \equiv)$$

Binary Relations:

$$\frac{\text{A} \equiv \text{A}' \qquad \text{B} \equiv \text{B}'}{\text{A} \wedge \text{B} \equiv \text{A}' \wedge \text{B}'} \quad (\wedge \equiv)$$

$$\frac{\text{A} \equiv \text{A}' \qquad \text{B} \equiv \text{B}'}{\text{A} \vee \text{B} \equiv \text{A}' \vee \text{B}'} \quad (\vee \equiv)$$

$$\frac{\text{A} \equiv \text{A}' \qquad \text{B} \equiv \text{B}'}{\text{A} \supset \text{B} \equiv \text{A}' \supset \text{B}'} \quad (\supset\equiv)$$

Equality:

$$\frac{\text{t}_1 \equiv \text{t}_1' \qquad \text{t}_2 \equiv \text{t}_2' \qquad \tau \equiv \tau'}{(\text{t}_1 = \text{t}_2 : \tau) \equiv (\text{t}_1{}' = \text{t}_2{}' : \tau')} \quad (=\equiv)$$

Quantifiers:

$$\frac{\text{И}\, z\,.\ (x\ z)\ \text{B} \equiv (x\ z)\ \text{B}' \qquad \tau \equiv \tau'}{\exists x : \tau.\ \text{B} \equiv \exists y : \tau'.\ \text{B}'} \quad (\exists \equiv)$$

$$\frac{\text{И}\, z\,.\ (x\ z)\ \text{B} \equiv (x\ z)\ \text{B}' \qquad \tau \equiv \tau'}{\forall x : \tau.\ \text{B} \equiv \forall y : \tau'.\ \text{B}'} \quad (\forall \equiv)$$

6.3 Swapping variable names

$$\texttt{swap} = (x\ \ z)$$

$$\begin{array}{lcl} \texttt{swap\_term} & : & x \to z \to \texttt{t} \to \texttt{t} \\ \texttt{swap\_prop} & : & x \to z \to \texttt{A} \to \texttt{A} \end{array}$$

```
val swap_term  :  var -> var -> term -> term
val swap_prop  :  var -> var -> prop -> prop
```