Proof Checker Notes

Yu-Yang Lin

July 30, 2015

1 Syntax Grammar

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

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

2 Specification rules for terms and propositional 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:

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

Booleans:

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

Lists:

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

Variables:

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

Application:

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

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:

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

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

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

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

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:

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

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:

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

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

```
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 Well-formedness of proofs

4.1 Syntax grammar

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

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

4.2 Rules

Truth and Falsity:

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

Conjunction:

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

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

Disjunction:

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

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

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

Implication:

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

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

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

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

5 Quantifiers in proofs

5.1 Rules

Existentials:

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

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

Universals:

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

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

5.2 Substituting terms into variables

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

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

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

6 α-equivalence

6.1 Terms

Variables:

$$\frac{}{x \overset{\alpha}{=} x} \quad (\mathrm{var}\overset{\alpha}{=})$$

Booleans:

$$\frac{}{\mathrm{true} \overset{\alpha}{=} \mathrm{true}} \quad (\text{bool-true}\overset{\alpha}{=}) \qquad \frac{}{\mathrm{false} \overset{\alpha}{=} \mathrm{false}} \quad (\text{bool-false}\overset{\alpha}{=})$$

Natural Numbers:

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

Lists:

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

Application:

$$\frac{\text{e} \overset{\alpha}{=} \text{e}' \qquad \text{v} \overset{\alpha}{=} \text{v}'}{\text{e v} \overset{\alpha}{=} \text{e}' \text{ v}'} \quad (\text{var}\overset{\alpha}{=})$$

6.2 Propositions

Truth and Falsity:

$$\frac{}{\top \overset{\alpha}{=} \top} \quad (\top \overset{\alpha}{=}) \qquad \frac{}{\bot \overset{\alpha}{=} \bot} \quad (\bot \overset{\alpha}{=})$$

Binary Relations:

$$\frac{\text{A} \overset{\alpha}{=} \text{A}' \qquad \text{B} \overset{\alpha}{=} \text{B}'}{\text{A} \wedge \text{B} \overset{\alpha}{=} \text{A}' \wedge \text{B}'} \quad (\wedge \overset{\alpha}{=})$$

$$\frac{\text{A} \overset{\alpha}{=} \text{A}' \qquad \text{B} \overset{\alpha}{=} \text{B}'}{\text{A} \vee \text{B} \overset{\alpha}{=} \text{A}' \vee \text{B}'} \quad (\vee \overset{\alpha}{=})$$

$$\frac{\text{A} \overset{\alpha}{=} \text{A}' \qquad \text{B} \overset{\alpha}{=} \text{B}'}{\text{A} \supset \text{B} \overset{\alpha}{=} \text{A}' \supset \text{B}'} \quad (\supset \overset{\alpha}{=})$$

Equality:

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

Quantifiers:

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

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

6.3 Swapping variable names

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

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

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

7 Induction in proofs

7.1 Rules through predicates

Natural Numbers:

$$\frac{\psi;\Gamma \vdash \mathrm{p} : \mathrm{P(zero)} \qquad \psi\ , n : \mathrm{nat}\ ; \Gamma\ , \mathrm{H} : \mathrm{P}(n) \vdash \mathrm{q} : \mathrm{P(suc}(n))}{\psi;\Gamma \vdash \text{(Induction on nat: case zero : p ; case suc}(n)\text{ : [H] , q)} : (\forall\ m : \mathrm{nat}\ .\ \mathrm{P}(m))} \quad \text{(induction-nat)}$$

Lists:

$$\frac{\psi;\Gamma \vdash \mathrm{p} : \mathrm{P(\,[\,]\,)} \qquad \psi\ , x : \tau\ , xs : \mathrm{list}\ \tau\ ; \Gamma\ , \mathrm{H} : \mathrm{P}(xs) \vdash \mathrm{q} : \mathrm{P}(x :: xs)}{\psi;\Gamma \vdash \text{(Induction on list: case [] : p ; case }(x :: xs)\text{ : [H] , q)} : (\forall\ ys : \mathrm{list}\ \tau\ .\ \mathrm{P}(ys))} \quad \text{(induction-list)}$$

Booleans:

$$\frac{\psi;\Gamma \vdash \mathrm{p} : \mathrm{P(\ true\ )} \qquad \psi;\Gamma \vdash \mathrm{q} : \mathrm{P(\ false\ )}}{\psi;\Gamma \vdash \text{(Induction on bool: case true : p ; case false : q)} : (\forall\ b : \mathrm{bool}\ .\ \mathrm{P(}\ b\ \mathrm{)})} \quad \text{(induction-bool)}$$

7.2 Rules through substitution

Natural Numbers:

$$\frac{\psi;\Gamma \vdash \mathrm{p} : [m \mapsto \mathrm{zero}]\ \mathrm{C} \qquad \psi\ , n : \mathrm{nat}\ ; \Gamma\ , \mathrm{H} : [m \mapsto \mathrm{zero}]\ \mathrm{C} \vdash \mathrm{q} : [\mathrm{m} \mapsto \mathrm{suc}(n)]\ \mathrm{C}}{\psi;\Gamma \vdash \text{(Ind-Nat: zero : p ; suc}(n)\text{ : [H] , q)} : (\forall\ m : \mathrm{nat}\ .\ \mathrm{C})} \quad \text{(induction-nat)}$$

Lists:

$$\frac{\psi;\Gamma \vdash \mathrm{p} : [ys \mapsto [\,]\,]\ \mathrm{C} \qquad \psi\ , x : \tau\ , xs : \mathrm{list}\ \tau\ ; \Gamma\ , \mathrm{H} : [ys \mapsto xs\ ]\ \mathrm{C} \vdash \mathrm{q} : [ys \mapsto x :: xs\ ]\ \mathrm{C}}{\psi;\Gamma \vdash \text{(Ind-List: [] : p ; }(x :: xs)\text{ : [H] , q)} : (\forall\ ys : \mathrm{list}\ \tau\ .\ \mathrm{C})} \quad \text{(induction-list)}$$

Booleans:

$$\frac{\psi;\Gamma \vdash \mathrm{p} : [b \mapsto \mathrm{true}\ ]\ \mathrm{C} \qquad \psi;\Gamma \vdash \mathrm{q} : [b \mapsto \mathrm{false}\ ]\ \mathrm{C}}{\psi;\Gamma \vdash \text{(Ind-Bool: true : p ; false : q)} : (\forall\ b : \mathrm{bool}\ .\ \mathrm{C})} \quad \text{(induction-bool)}$$

8 Equality in proofs

8.1 Abstract congruence closure [1, p. 4–7]

8.1.1 Definition

Rewrite-Rules:

$$\begin{array}{rrl} \textit{D-rule} : & f(c_0, ...c_k) \rightarrow c & \textit{where } f \textit{ is a term constructor and } c_i \textit{ are constants in } K \\ \textit{C-rule} : & c \rightarrow d & \textit{where } c \textit{ and } d \textit{ are constants in } K \end{array}$$

Sets:

$$D : \{\textit{D-rule}\}$$
$$C : \{\textit{C-rule}\}$$

$$E : \{(t = t) : \tau\}$$
$$K : \{x \mid x \notin E\}$$
$$R : D \cup C$$

Closure Construction:

$$state : (K, E, R)$$

$$\texttt{build\_acc}: \quad \frac{(\emptyset, E, \emptyset)}{(K, \emptyset, R)} \quad \textit{where } R \textit{ is the abstract congruence closure (ACC) of } E$$

8.1.2 Sate transition rules

$$\text{Extension:} \quad \frac{(K, E[t], R) \qquad t = f(c_0, ..., c_k) \qquad c_i \in K \wedge c \notin K}{(K \cup \{c\}, E[c], R \cup \{t \to c \ : D\})} \quad \text{(Ext)}$$

$$\text{Simplification:} \quad \frac{(K, E[t], R \cup \{t \to c : D\})}{(K, E[c], R \cup \{t \to c : D\})} \quad \text{(Sim)}$$

$$\text{Orientation1:} \quad \frac{(K \cup \{c\}, E \cup \{t = c\}, R\})}{(K \cup \{c\}, E, R \cup \{t \to c : D\})} \quad \text{(Ori1)}$$

$$\text{Orientation2:} \quad \frac{(K \cup \{c, d\}, E \cup \{c = d\}, R\}) \qquad c < d}{(K \cup \{c, d\}, E, R \cup \{c \to d : C\})} \quad \text{(Ori2)}$$

$$\text{Orientation3:} \quad \frac{(K \cup \{c, d\}, E \cup \{c = d\}, R\}) \qquad d < c}{(K \cup \{c, d\}, E, R \cup \{d \to c : C\})} \quad \text{(Ori2)}$$

$$\text{Deletion:} \quad \frac{(K, E \cup \{t = t\}, R\})}{(K, E, R\})} \quad \text{(Del)}$$

$$\text{Deduction1:} \quad \frac{(K, E, R \cup \{t \to c : D, t \to d : D\})}{(K, E \cup \{c = d\}, R \cup \{t \to d : D\})} \quad \text{(Ded1)}$$

$$\text{Deduction2:} \quad \frac{(K, E, R \cup \{c \to c' : C, c \to d : C\})}{(K, E \cup \{c' = d\}, R \cup \{c \to d : C\})} \quad \text{(Ded2)}$$

$$\text{Collapse:} \quad \frac{(K, E, R \cup \{s[c] \to c' : D, c \to d : C\})}{(K, E, R \cup \{s[d] \to c' : D, c \to d : C\})} \quad \text{(Col)}$$

$$\text{Composition:} \quad \frac{(K, E, R \cup \{t \to c : D, c \to d : C\})}{(K, E, R \cup \{t \to d : D, c \to d : C\})} \quad \text{(Com)}$$

8.2 Equality through congruence

$$\frac{\psi\, ;\, \Gamma \ \vdash \ \mathrm{H}_i : (t_i = t'_i) : \tau_i \qquad \forall i \in \{1...n\}\, .\, \overrightarrow{t_i = t'_i} \ \models \ t = t'}{\psi\, ;\, \Gamma \ \vdash \ \text{By Equality}\ (\ \mathrm{H}_0\ , ...\ , \mathrm{H}_n\ ) : (t = t' : \tau)} \quad \text{(eq)}$$

9 Spine application and hypotheses labelling

9.1 Rules for proofs

$$
\begin{array}{rrl}
\text{(simple-proofs)} & \mathrm{spf} ::= & \text{[H] with s} \mid \text{[H]} \mid \text{Left spf} \mid \text{Right spf} \mid \text{(spf , spf)} \\
\text{(proofs)} & \mathrm{p} ::= & \text{...} \mid \text{[H] with s} \mid \text{We know [H] : A because spf , p} \\
\text{(spines)} & \mathrm{s} ::= & . \mid \text{[H] , s} \mid \text{t , s}
\end{array}
$$

$$\texttt{check\_simple\_pf} \;::\; \texttt{spf} \rightarrow \texttt{unit option}$$

Labelling:
$$\frac{\psi;\Gamma \vdash \mathrm{spf} : \mathrm{A} \qquad \psi;\Gamma, \mathrm{H} : \mathrm{A} \vdash \mathrm{p} : \mathrm{C}}{\psi;\Gamma \vdash \text{We know [H] : A because spf , p} : \mathrm{C}} \quad \text{(hyp-label)}$$

Spine application:
$$\frac{\overset{-}{\psi};\overset{-}{\Gamma}, \mathrm{H} : \mathrm{A} \vdash \overset{-}{\mathrm{s}} : \overset{-}{\mathrm{A}} \gg \overset{+}{\mathrm{B}} \qquad \mathrm{B} \overset{\alpha}{=} \mathrm{C}}{\psi;\Gamma, \mathrm{H} : \mathrm{A} \vdash \text{[H] with s} : \mathrm{C}} \quad \text{(spine-app)}$$

9.2 Rules for spline application

Rules:

$$\frac{}{\psi;\Gamma \vdash . : \mathrm{A} \gg \mathrm{A}} \quad \text{(id-spine-app)}$$

$$\frac{\psi;\Gamma, [\mathrm{H}] : \mathrm{A} \vdash \mathrm{s} : \mathrm{B} \gg \mathrm{C}}{\psi;\Gamma \vdash [\mathrm{H}] , \mathrm{s} : \mathrm{A} \supset \mathrm{B} \gg \mathrm{C}} \quad (\supset\text{-spine-app})$$

$$\frac{\psi \vdash \mathrm{t} : \tau \qquad \psi;\Gamma \vdash \mathrm{s} : [\mathrm{t} \mapsto \mathrm{x}]\, \mathrm{A} \gg \mathrm{C}}{\psi;\Gamma \vdash \mathrm{t} , \mathrm{s} : \forall x : \tau \,.\, \mathrm{A} \gg \mathrm{C}} \quad (\forall\text{-spine-app})$$

Function signatures:

$$
\begin{array}{lcl}
\texttt{apply\_spine} & :: & \psi \rightarrow \Gamma \rightarrow \mathrm{s} \rightarrow \mathrm{A} \rightarrow \mathrm{B}\ \texttt{option} \\
\texttt{apply\_spine} & :: & \texttt{ctx} \rightarrow \texttt{hyps} \rightarrow \texttt{spine} \rightarrow \texttt{prop} \rightarrow \texttt{prop option}
\end{array}
$$

References

[1] Leo Bachmair, Ashish Tiwari, and Laurent Vigneron. Abstract congruence closure. *J. Autom. Reasoning*, 31(2):129–168, 2003.