Type Soundness in an Intensional Dependent Type Theory with Type-in-Type and Recursion

February 27, 2021

1 Type Soundness

1.1 Contexts

1.1.1 Sub-Contexts are well formed

The following rules are admissible:

$$\frac{\Gamma, \Gamma' \vdash}{\Gamma \vdash}$$

$$\frac{\Gamma, \Gamma' \vdash m : M}{\Gamma \vdash}$$

$$\frac{\Gamma, \Gamma' \vdash m \Rrightarrow m' : M}{\Gamma \vdash}$$

$$\frac{\Gamma, \Gamma' \vdash m \Rrightarrow_* m' : M}{\Gamma \vdash}$$

$$\frac{\Gamma, \Gamma' \vdash m \equiv m' : M}{\Gamma \vdash}$$

by mutual induction on the derivations.

1.1.2 Context weakening

For any derivation of $\Gamma \vdash M : \star$, the following rules are admissible:

$$\frac{\Gamma, \Gamma' \vdash}{\Gamma, x : M, \Gamma' \vdash}$$

$$\frac{\Gamma, \Gamma' \vdash n : N}{\Gamma, x : M, \Gamma' \vdash n : N}$$

$$\frac{\Gamma, \Gamma' \vdash n \Rrightarrow n' : N}{\Gamma, x : M, \Gamma' \vdash n \Rrightarrow n' : N}$$

$$\frac{\Gamma, \Gamma' \vdash n \Rrightarrow_* n' : N}{\Gamma, x : M, \Gamma' \vdash n \Rrightarrow_* n' : N}$$

$$\frac{\Gamma, \Gamma' \vdash n \equiv n' : N}{\Gamma, x : M, \Gamma' \vdash n \equiv n' : N}$$

by mutual induction on the derivations.

1.1.3 $\Rrightarrow$ is reflexive

The following rule is admissible:

$$\frac{\Gamma \vdash m : M}{\Gamma \vdash m \Rrightarrow\ m : M} \Rrightarrow\text{-refl}$$

by induction

1.1.4 $\equiv$ is reflexive

The following rule is admissible:

$$\frac{\Gamma \vdash m : M}{\Gamma \vdash m \equiv m : M} \equiv\text{-refl}$$

by $\Rrightarrow *$-refl

1.1.5 Context substitution

For any derivation of $\Gamma \vdash m : M$ the following rules are admissible:

$$\frac{\Gamma, x : M, \Gamma' \vdash}{\Gamma, \Gamma' [x \coloneqq m] \vdash}$$

$$\frac{\Gamma, x : M, \Gamma' \vdash n : N}{\Gamma, \Gamma' [x \coloneqq m] \vdash n [x \coloneqq m]\ :\ N [x \coloneqq m]}$$

$$\frac{\Gamma, x : M, \Gamma' \vdash n \Rrightarrow n' : N}{\Gamma, \Gamma' [x \coloneqq m] \vdash n [x \coloneqq m] \Rrightarrow n' [x \coloneqq m] : N [x \coloneqq m]}$$

$$\frac{\Gamma, x : M, \Gamma' \vdash n \Rrightarrow_* n' : N}{\Gamma, \Gamma' [x \coloneqq m] \vdash n [x \coloneqq m] \Rrightarrow_* n' [x \coloneqq m] : N}$$

$$\frac{\Gamma, x : M, \Gamma' \vdash n \equiv n' : N}{\Gamma, \Gamma' [x \coloneqq m] \vdash n [x \coloneqq m]\ \equiv\ n' [x \coloneqq m] : N [x \coloneqq m]}$$

by mutual induction on the derivations. Specifically, at every usage of x from the var rule in the original derivation, replace the usage of the var rule with the derivation of $\Gamma \vdash m : M$ weakened to the context of $\Gamma, \Gamma' [x \coloneqq m]$, and apply $\Rrightarrow$-refl , $\Rrightarrow_*$-refl or $\equiv$-refl when needed.

1.2 Computation

1.2.1 $\Rrightarrow$ preserves type of source

The following rule is admissible:

$$\frac{\Gamma \vdash m \Rrightarrow m' : M}{\Gamma \vdash m : M}$$

by induction

1.2.2 $\Rrightarrow$-substitution

The following rule is admissible:

$$\frac{\Gamma, x : M, \Gamma' \vdash n \Rrightarrow n' : N \quad \Gamma \vdash m \Rrightarrow m' : M}{\Gamma, \Gamma' [x \coloneqq m] \vdash n [x \coloneqq m] \Rrightarrow n' [x \coloneqq m'] : N [x \coloneqq m]}$$

by induction on the $\Rrightarrow$ derivations

1.2.3 $\Rrightarrow$ is confluent

if $\Gamma \vdash m \Rrightarrow n : M$ and $\Gamma \vdash m \Rrightarrow n' : M$ then there exists m' such that
$\Gamma \vdash n \Rrightarrow m' : M$ and $\Gamma \vdash n' \Rrightarrow m' : M$
by standard techniques

1.3 $\Rrightarrow_*$

1.3.1 $\Rrightarrow_*$ is transitive

The following rule is admissible:

$$\frac{\Gamma \vdash m \Rrightarrow_* m' : M \quad \Gamma \vdash m' \Rrightarrow_* m'' : M}{\Gamma \vdash m \Rrightarrow_* m'' : M} \Rrightarrow *\text{-trans}$$

by induction

1.3.2 $\Rrightarrow$ preserves type in destination

$$\frac{\Gamma \vdash m \Rrightarrow m' : M}{\Gamma \vdash m' : M}$$

By induction on the $\Rrightarrow$ derivation with the help of the substitution lemma.

- Π-$\Rrightarrow$
  - $m' [x \coloneqq n', f \coloneqq (\mathsf{fun}\, f.\, x.m')] : M' [x \coloneqq n']$ by the substitution lemma used on the inductive hypotheses
  - $M [x \coloneqq n] \Rrightarrow M' [x \coloneqq n']$ by $\Rrightarrow$-substitution , so $M [x \coloneqq n] \equiv M' [x \coloneqq n']$
  - by the conversion rule $m' [x \coloneqq n', f \coloneqq (\mathsf{fun}\, f.\, x.m')] : M [x \coloneqq m]$
- Π-E-$\Rrightarrow$

  - $m' \, n' \ : \ \tau \, [x \coloneqq n']$, by $\Rrightarrow$-substitution and reflexivity, $M \, [x \coloneqq n] \Rrightarrow M \, [x \coloneqq n']$, so $M \, [x \coloneqq n] \equiv M \, [x \coloneqq n']$
  - by the conversion rule $m' \, n' \ : \ M \, [x \coloneqq n]$

- Π-I-$\Rrightarrow$
  - $\mathsf{fun} \, f. \, x.m' \ : \ \Pi x : M'.N'$, $\Pi x : M.N \Rrightarrow \Pi x : M'.N'$, so $\Pi x : M.N \equiv \Pi x : M'.N'$
  - by the conversion rule $\mathsf{fun} \, f. \, x.m' \ : \ \Pi x : M.N$

- all other cases are trivial

1.3.3 $\Rrightarrow_*$ preserves type

The following rule is admissible:

$$\frac{\Gamma \vdash m \Rrightarrow_* \ m' : M}{\Gamma \vdash m : M}$$

by induction

$$\frac{\Gamma \vdash m \Rrightarrow_* \ m' : M}{\Gamma \vdash m' : M}$$

by induction

1.3.4 $\Rrightarrow_*$ is confluent

if $\Gamma \vdash m \Rrightarrow_* \ n : M$ and $\Gamma \vdash m \Rrightarrow_* \ n' : M$ then there exists m' such that $\Gamma \vdash n \Rrightarrow_* m' : M$ and $\Gamma \vdash n' \Rrightarrow_* m' : M$

Follows from $\Rrightarrow *$-trans and the confluence of $\Rrightarrow$ using standard techniques

1.3.5 $\equiv$ is symmetric

The following rule is admissible:

$$\frac{\Gamma \vdash m \equiv m' : M}{\Gamma \vdash m' \equiv m : M} \equiv\text{-sym}$$

trivial

1.3.6 $\equiv$ is transitive

$$\frac{\Gamma \vdash m \equiv m' : M \qquad \Gamma \vdash m' \equiv m'' : M}{\Gamma \vdash m \equiv m'' : M} \equiv\text{-trans}$$

by the confluence of $\Rrightarrow_*$

1.3.7 $\equiv$ preserves type

The following rules are admissible:

$$\frac{\Gamma \vdash m \equiv m' : M}{\Gamma \vdash m : M}$$

$$\frac{\Gamma \vdash m \equiv m' : M}{\Gamma \vdash m' : M}$$

by the def of $\Rrightarrow_*$

1.3.8 Regularity

The following rule is admissible:

$$\frac{\Gamma \vdash m : M}{\Gamma \vdash M : \star}$$

by induction with $\equiv$-preservation for the Conv case

1.3.9 $\rightsquigarrow$ implies $\Rrightarrow$

For any derivations of $\Gamma \vdash m : M$, $m \rightsquigarrow m'$

$$\Gamma \vdash m \Rrightarrow m' : M$$

by induction on $\rightsquigarrow$

1.3.10 $\rightsquigarrow$ preserves type

For any derivations of $\Gamma \vdash m : M$, $m \rightsquigarrow m'$,

$$\Gamma \vdash m' : M$$

since $\rightsquigarrow$ implies $\Rrightarrow$ and $\Rrightarrow$ preserves types

1.4 Type constructors

1.4.1 Type constructors are stable

- if $\Gamma \vdash * \Rrightarrow m : M$ then m is $*$
- if $\Gamma \vdash * \Rrightarrow_* m : M$ then m is $*$
- if $\Gamma \vdash \Pi x : N.P \Rrightarrow m : M$ then m is $\Pi x : N'.P'$ for some N', P'
- if $\Gamma \vdash \Pi x : N.P \Rrightarrow_* m : M$ then m is $\Pi x : N'.P'$ for some N', P'

by induction on the respective relations

1.4.2 Type constructors definitionaly unique

There is no derivation of $\Gamma \vdash * \equiv \Pi x : M.N \ : P$ for any Γ, M, N, P
from $\equiv$ -Def and constructor stability

1.5 Canonical forms

If $\lozenge \vdash v : P$ then

- if P is $\star$ then v is $\star$ or $\Pi x : M.N$
- if P is $\Pi x : M.N$ for some M, N then v is $\mathsf{fun}\, f.\, x.m$ for some m

By induction on the typing derivation

- Conv,
  - if P is $\star$ then eventually, it was typed with type-in-type, or Π-F. it could not have been typed by Π-I since constructors are definitionaly unique
  - if P is $\Pi x : M.N$ then eventually, it was typed with Π-I. it could not have been typed by type-in-type, or Π-F since constructors are definitionaly unique
- type-in-type, $\lozenge \vdash v : P$ is $\lozenge \vdash \star : \star$
- Π-F, $\lozenge \vdash v : P$ is $\lozenge \vdash \Pi x : M.N \ : \star$
- Π-I, $\lozenge \vdash v : P$ is $\lozenge \vdash \mathsf{fun}\, f.\, x.m \ : \ \mathit{\Pi} x : M.N$
- no other typing rules are applicable

1.6 Progress

$\lozenge \vdash m : M$ implies that m is a value or there exists m' such that $m \rightsquigarrow m'$.

By direct induction on the typing derivation with the help of the canonical forms lemma

Explicitly:

- m is typed by the conversion rule, then by **induction**, m is a value or there exists m' such that $m \rightsquigarrow m'$.
- m cannot be typed by the variable rule in the empty context
- m is typed by type-in-type. m is $\star$, a value
- m is typed by Π-F. M is $\Pi x : N.P$, a value
- m is typed by Π-I. m is $\mathsf{fun}\, f.\, x.n$, a value

- m is typed by Π-E. M is $p\,n$ then exist some σ, τ for $\Diamond \vdash P : \Pi x : \sigma.\tau$ and $\Diamond \vdash N : \sigma$. By **induction** (on the P branch of the derivation) P is a value or there exists P' such that $P \rightsquigarrow P'$. By **induction** (on the N branch of the derivation) N is a value or there exists N' such that $N \rightsquigarrow N'$
  - if P is a value then by **canonical forms**, P is$\mathsf{fun}\, f : (x.\tau) \,.\, x : \sigma.P'$ and
    - if N is a value then the one step reduction is $(\mathsf{fun}\, f : (x.\tau) \,.\, x : \sigma.P')\ N \rightsquigarrow P'\,[x \coloneqq N, f \coloneqq \mathsf{fun}\, f : (x.\tau) \,.\, x : \sigma.M]$
    - otherwise there exists N' such that $N \rightsquigarrow N'$, and the one step reduction is $(\mathsf{fun}\, f : (x.\tau) \,.\, x : \sigma.P')\ N \rightsquigarrow (\mathsf{fun}\, f : (x.\tau) \,.\, x : \sigma.P')\ N'$
  - otherwise, there exists P' such that $P \rightsquigarrow P'$ and the one step reduction is $P\,N \rightsquigarrow P'\,N$
- m is typed by ::, m is $n :: N$ by induction
  - n is a value, $n :: N \rightsquigarrow n$
  - or there exists n' such that $n \rightsquigarrow n'$., $n :: N \rightsquigarrow n' :: N$

1.7 Type Soundness

For any well typed term in an empty context, no sequence of small step reductions will cause result in a computation to “get stuck”. Either a final value will be reached or further reductions can be taken. This follows by iterating the progress and preservation lemmas.