Adding boolean extensionality to intensional dependent type theory... a tentative

Kenji Maillard

Inria Nantes, team Gallinette

GdT Scalp
Wednesday the 15th of February, 2023

A question from M. Shulman

Proof Assistants Beta

Home

PUBLIC

Questions

Tags

Users

Unanswered

TEAMS ✕

Strong eta-rules for functions on sum types

Ask Question

Asked 2 months ago Modified 2 months ago Viewed 145 times

8

I am wondering whether a rule like the following is consistent with decidable conversion and type-checking for dependent type theory:

$$\frac{f\ g : (x : \mathsf{bool}) \to C\ x \qquad f\ \mathsf{tt} \equiv g\ \mathsf{tt} \qquad f\ \mathsf{ff} \equiv g\ \mathsf{ff}}{f \equiv g}$$

That is, if two functions with domain bool agree definitionally on tt and ff, then they are convertible. An analogous rule for functions on general inductive types like $\mathbb{N}$ is certainly

Martin-Löf Type Theory and its implementations

Martin-Löf logical framework + type formers $(\square, \Pi, \Sigma, x =_A y, \ldots)$

$$\Gamma \vdash \qquad \Gamma \vdash A \qquad \Gamma \vdash A \equiv B$$

$$\Gamma \vdash t : A \qquad \Gamma \vdash t \equiv u : A$$

Idealized metatheory of various proofs assistants:

Agda Idris LEAN THEOREM PROVER

Practical implementation $\rightsquigarrow$ algorithms deciding each judgements

Extensional principles in intensional type theory

When can we add an extensionality principle for some type former ?

Type formers	Dec. of conv.	Reference
Functions $\Pi(x : A)B$	✓	[Coquand 96]
(Negative) records $\Sigma(x : A)B$	✓	[Norell 07]
Unit $\mathbb{1}$	✓	[Norell 07]
Identity $x =_A y$	×	[Castellan et al. 17]
Natural numbers $\mathbb{N}$	×	
Well-founded trees $\mathbb{W}(x : A)B$	×	
Streams, $\mathbb{M}$-types	×	[McBride]
Empty $\mathbb{0}$	×	[McBride]
Booleans $\mathbb{B}$	???	

Booleans 101

Introductions

$$\frac{}{\Gamma \vdash \mathbb{B}} \qquad \frac{}{\Gamma \vdash \texttt{tt} : \mathbb{B}} \qquad \frac{}{\Gamma \vdash \texttt{ff} : \mathbb{B}}$$

Simple elimination

$$\frac{\Gamma \vdash b : \mathbb{B} \qquad \Gamma \vdash t : C \qquad \Gamma \vdash u : C}{\Gamma \vdash \texttt{if}\ b\ \texttt{then}\ t\ \texttt{else}\ u : C}$$

Booleans 101

Introductions

$$\frac{}{\Gamma \vdash \mathbb{B}} \qquad \frac{}{\Gamma \vdash \texttt{tt} : \mathbb{B}} \qquad \frac{}{\Gamma \vdash \texttt{ff} : \mathbb{B}}$$

Simple elimination

$$\frac{\Gamma \vdash b : \mathbb{B} \qquad \Gamma \vdash t : C \qquad \Gamma \vdash u : C}{\Gamma \vdash \texttt{if}\ b\ \texttt{then}\ t\ \texttt{else}\ u : C}$$

$$\texttt{if}\ \texttt{tt}\ \texttt{then}\ t\ \texttt{else}\ u \longrightarrow t \qquad \texttt{if}\ \texttt{ff}\ \texttt{then}\ t\ \texttt{else}\ u \longrightarrow u$$

Booleans 101

Introductions

$$\frac{}{\Gamma \vdash \mathbb{B}} \qquad \frac{}{\Gamma \vdash \texttt{tt} : \mathbb{B}} \qquad \frac{}{\Gamma \vdash \texttt{ff} : \mathbb{B}}$$

Simple elimination

$$\frac{\Gamma \vdash b : \mathbb{B} \qquad \Gamma \vdash t : C \qquad \Gamma \vdash u : C}{\Gamma \vdash \texttt{if}\ b\ \texttt{then}\ t\ \texttt{else}\ u : C}$$

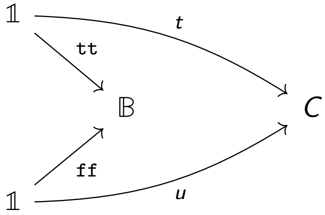
$$\texttt{if}\ \texttt{tt}\ \texttt{then}\ t\ \texttt{else}\ u \longrightarrow t \qquad \texttt{if}\ \texttt{ff}\ \texttt{then}\ t\ \texttt{else}\ u \longrightarrow u$$

Dependent elimination

$$\frac{\begin{array}{cc}\Gamma \vdash b : \mathbb{B} & \Gamma, x : \mathbb{B} \vdash P \\ \Gamma \vdash t : P[\texttt{tt}/x] & \Gamma \vdash u : P[\texttt{ff}/x]\end{array}}{\Gamma \vdash \texttt{match}\ b\ \texttt{as}\ x\ \texttt{return}\ P\ \texttt{with}\ \texttt{tt} \Rightarrow t \mid \texttt{ff} \Rightarrow u\ \texttt{end} : P[b/x]}$$

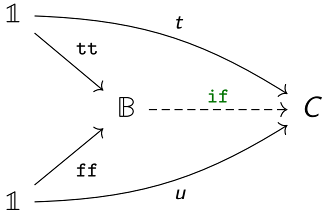
What's boolean extensionality ?

Returning to the categorical universal property of $\mathbb{B} \cong \mathbb{1} + \mathbb{1}$



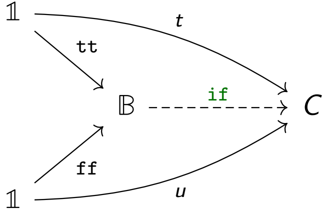
What's boolean extensionality ?

Returning to the categorical universal property of $\mathbb{B} \cong \mathbb{1} + \mathbb{1}$



What's boolean extensionality ?

Returning to the categorical universal property of $\mathbb{B} \cong \mathbb{1} + \mathbb{1}$

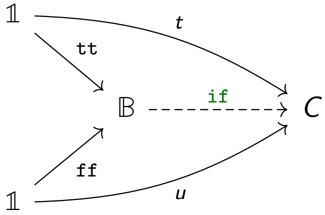


Unicity part:

$$\frac{}{\Gamma \vdash p \equiv q : C}$$

What's boolean extensionality ?

Returning to the categorical universal property of $\mathbb{B} \cong \mathbb{1} + \mathbb{1}$

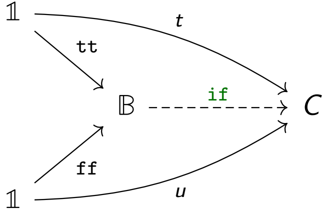


Unicity part:

$$\frac{\Gamma \vdash b : \mathbb{B}}{\Gamma \vdash p \equiv q : C}$$

What's boolean extensionality ?

Returning to the categorical universal property of $\mathbb{B} \cong \mathbb{1} + \mathbb{1}$

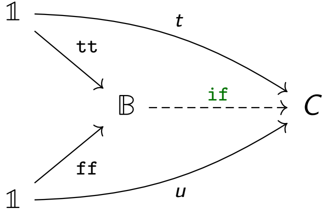


Unicity part:

$$\frac{\Gamma \vdash b : \mathbb{B} \qquad \Gamma \vdash p[\mathtt{tt}/b] \equiv q[\mathtt{tt}/b] : C[\mathtt{tt}/b]}{\Gamma \vdash p \equiv q : C}$$

What's boolean extensionality ?

Returning to the categorical universal property of $\mathbb{B} \cong \mathbb{1} + \mathbb{1}$



Unicity part:

$$\frac{\Gamma \vdash b : \mathbb{B} \quad \Gamma \vdash p[\texttt{tt}/b] \equiv q[\texttt{tt}/b] : C[\texttt{tt}/b] \quad \Gamma \vdash p[\texttt{ff}/b] \equiv q[\texttt{ff}/b] : C[\texttt{ff}/b]}{\Gamma \vdash p \equiv q : C}$$

With type dependency, substitution is not enough

Assuming $\alpha : \mathbb{N} \to \mathbb{B}$, consider

$$\texttt{match}\ \alpha\ 42\ \texttt{as b return}\ \forall\ \texttt{n},\ \alpha\ \texttt{n} = \texttt{b} \to \mathbb{N}\ \texttt{with}$$
$$\mid \texttt{tt} \Rightarrow \lambda\ \texttt{n eq} \Rightarrow 0$$
$$\mid \texttt{ff} \Rightarrow \lambda\ \texttt{n eq} \Rightarrow 0$$
$$\texttt{end}\ 42\ (\texttt{refl} : \alpha\ 42 = \alpha\ 42)$$

With type dependency, substitution is not enough

Assuming $\alpha : \mathbb{N} \to \mathbb{B}$, consider

```
match α 42 as b return ∀ n, α n = b → ℕ with
| tt ⇒ λ n eq ⇒ 0
| ff ⇒ λ n eq ⇒ 0
end 42 (refl : α 42 = α 42)
```

Morally convertible to 0 by boolean extensionality.

With type dependency, substitution is not enough

Assuming $\alpha : \mathbb{N} \to \mathbb{B}$, consider

```
match α 42 as b return ∀ n, α n = b → ℕ with
| tt ⇒ λ n eq ⇒ 0
| ff ⇒ λ n eq ⇒ 0
end 42 (refl : α 42 = α 42)
```

Morally convertible to 0 by boolean extensionality.

But substituting α 42 by tt is ill-typed:

```
match tt as b return ∀ n, α n = b → ℕ with
| tt ⇒ λ n eq ⇒ 0
| ff ⇒ λ n eq ⇒ 0
end 42 (refl : α 42 = tt)
```

Need to keep track of convertibility relations at $\mathbb{B}$!

Reflecting conversion at $\mathbb{B}$

Add boolean constraints (cf. Altenkirch 2011 Shonan talk)

$$\frac{\Gamma \vdash \qquad \Gamma \vdash e : \mathbb{B} \qquad b \in \{\mathtt{tt}, \mathtt{ff}\}}{\Gamma, e \equiv b \vdash} \qquad e \text{ atomic neutral}$$

Reflecting conversion at $\mathbb{B}$

Add boolean constraints (cf. Altenkirch 2011 Shonan talk)

$$\frac{\Gamma \vdash \qquad \Gamma \vdash e : \mathbb{B} \qquad b \in \{\texttt{tt}, \texttt{ff}\}}{\Gamma, e \equiv b \vdash} \qquad e \text{ atomic neutral}$$

Extend conversion

$$\textsc{Reflection}\ \frac{(e \equiv b) \in \Gamma}{\Gamma \vdash e \equiv b : \mathbb{B}} \qquad \textsc{Explosion}\ \frac{(e \equiv \texttt{tt}), (e \equiv \texttt{ff}) \in \Gamma \qquad \Gamma \vdash t, u : C}{\Gamma \vdash t \equiv u : C}$$

$$\textsc{Cover}\ \frac{\Gamma \vdash e : \mathbb{B} \qquad \Gamma, e \equiv \texttt{tt} \vdash t \equiv u : C \qquad \Gamma, e \equiv \texttt{ff} \vdash t \equiv u : C}{\Gamma \vdash t \equiv u : C}$$

With BoolExt, `If` is enough !

`if b then t else u` vs.

```
match b as x return P with
| tt ⇒ t
| ff ⇒ u
end
```

With BoolExt, `If` is enough !

`if b then t else u` vs.

```
match b as x return P with
| tt ⇒ t
| ff ⇒ u
end
```

In general, we cannot synthetize $x : \mathbb{B} \vdash P$ from $t : P_t$ and $u : P_u$.

With BoolExt, `If` is enough !

`if b then t else u` vs.

```
match b as x return P with
| tt ⇒ t
| ff ⇒ u
end
```

In general, we cannot synthetize $x : \mathbb{B} \vdash P$ from $t : P_t$ and $u : P_u$.

However with boolean extensionality, for an arbitrary $\mathtt{P} : \mathbb{B} \to \square$

$$\texttt{if b then P tt else P ff} \equiv \texttt{P b}$$

With BoolExt, `If` is enough !

`if b then t else u` vs.

```
match b as x return P with
| tt ⇒ t
| ff ⇒ u
end
```

In general, we cannot synthetize $x : \mathbb{B} \vdash P$ from $t : P_t$ and $u : P_u$.

However with boolean extensionality, for an arbitrary `P` $: \mathbb{B} \to \square$

$$\texttt{if b then P tt else P ff} \equiv \texttt{P b}$$

$\rightsquigarrow$ no need for a motive `P` !

$$P(x) := \texttt{if}\ x\ \texttt{then}\ P_t\ \texttt{else}\ P_u$$

What's the trouble with $\mathbb{0}$?

$$\frac{\Gamma \vdash e : \mathbb{0} \qquad \Gamma \vdash t, u : C}{\Gamma \vdash t \equiv u : C}\ \mathbb{0}\text{-}\textsc{Ext}$$

What's the trouble with $\mathbb{0}$?

$$\frac{\Gamma \vdash e : \mathbb{0} \qquad \Gamma \vdash t, u : C}{\Gamma \vdash t \equiv u : C}\ \mathbb{0}\text{-}\textsc{Ext}$$

Let F_n be the type of triples $\Sigma(x, y, z : \mathbb{N}^3) x^n + y^n = z^n$, then $x : F_{42} \vdash_{\mathbb{0}\text{-}\textsc{Ext}} 7 : \mathbb{B}$.

What's the trouble with $\mathbb{0}$?

$$\frac{\Gamma \vdash e : \mathbb{0} \qquad \Gamma \vdash t, u : C}{\Gamma \vdash t \equiv u : C}\ \mathbb{0}\text{-}\textsc{Ext}$$

Let F_n be the type of triples $\Sigma(x, y, z : \mathbb{N}^3) x^n + y^n = z^n$, then $x : F_{42} \vdash_{\mathbb{0}\text{-}\textsc{Ext}} 7 : \mathbb{B}$.

Indeed, by Fermat's last theorem F_{42} is empty, so using $\mathbb{0}$-ext $x : F_{42} \vdash_{\mathbb{0}\text{-}\textsc{Ext}} \mathbb{N} \equiv \mathbb{B} : \square$, and $\vdash_{\mathbb{0}\text{-}\textsc{Ext}} 7 : \mathbb{N}$

What's the trouble with $\mathbb{0}$?

$$\frac{\Gamma \vdash e : \mathbb{0} \qquad \Gamma \vdash t, u : C}{\Gamma \vdash t \equiv u : C}\ \mathbb{0}\text{-}\textsc{Ext}$$

Let F_n be the type of triples $\Sigma(x, y, z : \mathbb{N}^3) x^n + y^n = z^n$, then $x : F_{42} \vdash_{\mathbb{0}\text{-}\textsc{Ext}} 7 : \mathbb{B}$.

Indeed, by Fermat's last theorem F_{42} is empty, so using $\mathbb{0}$-ext $x : F_{42} \vdash_{\mathbb{0}\text{-}\textsc{Ext}} \mathbb{N} \equiv \mathbb{B} : \square$, and $\vdash_{\mathbb{0}\text{-}\textsc{Ext}} 7 : \mathbb{N}$

$\mathbb{0}$-extensionality can impact typing without leaving a trace !

Algorithmic aspects of conversion

How do we decide $\Gamma \vdash t \overset{?}{\equiv} u : A$ in general ?

Step 1: Weak-head reduce

$$t \longrightarrow^{*}_{wh} t' \overset{?}{\equiv} u' \ {}^{*}_{wh}\!\longleftarrow u$$

Step 2: Apply congruences for canonical introduction forms.

Step 3: Once we get to neutrals, use extensionality rules potentially directed by the (weak-head reduced) type A, e.g.

$$\Gamma, x : \mathbb{1}, y : \mathbb{1} \vdash x \equiv y : \mathbb{1}$$

Step 4: Recurse on arbitrary subterms.

Towards an implementation of boolean extensionality

Atomic neutral: A boolean neutral in deep normal-form with no proper boolean sub-neutral.

Idea: Hoist-away all atomic neutrals, and split them.

Towards an implementation of boolean extensionality

Atomic neutral: A boolean neutral in deep normal-form with no proper boolean sub-neutral.

Idea: Hoist-away all atomic neutrals, and split them.

$$f : \mathbb{B} \to \mathbb{B}, x : \mathbb{B} \vdash f\,(f\,(f\,x)) \stackrel{?}{\equiv} f\,x : \mathbb{B}$$

Towards an implementation of boolean extensionality

Atomic neutral: A boolean neutral in deep normal-form with no proper boolean sub-neutral.

Idea: Hoist-away all atomic neutrals, and split them.

$$f : \mathbb{B} \to \mathbb{B}, x : \mathbb{B}, x \equiv \texttt{tt} \vdash f\,(f\,(f\,\texttt{tt})) \stackrel{?}{\equiv} f\,\texttt{tt} : \mathbb{B}$$

$$f : \mathbb{B} \to \mathbb{B}, x : \mathbb{B}, x \equiv \texttt{ff} \vdash f\,(f\,(f\,\texttt{ff})) \stackrel{?}{\equiv} f\,\texttt{ff} : \mathbb{B}$$

Split on the unique atomic neutral x.

Towards an implementation of boolean extensionality

Atomic neutral: A boolean neutral in deep normal-form with no proper boolean sub-neutral.

Idea: Hoist-away all atomic neutrals, and split them.

$$f : \mathbb{B} \to \mathbb{B}, x : \mathbb{B}, x \equiv \texttt{tt} \vdash f\,(f\,(f\,\texttt{tt})) \stackrel{?}{\equiv} f\,\texttt{tt} : \mathbb{B}$$

$$f : \mathbb{B} \to \mathbb{B}, x : \mathbb{B}, x \equiv \texttt{ff} \vdash f\,(f\,(f\,\texttt{ff})) \stackrel{?}{\equiv} f\,\texttt{ff} : \mathbb{B}$$

Remark: Some atomic neutral ($f\,\texttt{tt}, f\,\texttt{ff}$) may appear when splitting another neutral (x).

Towards an implementation of boolean extensionality

Atomic neutral: A boolean neutral in deep normal-form with no proper boolean sub-neutral.

Idea: Hoist-away all atomic neutrals, and split them.

$$f : \mathbb{B} \to \mathbb{B}, f\,\texttt{tt} \equiv \texttt{ff}, x : \mathbb{B}, x \equiv \texttt{tt} \vdash f\,(f\,\texttt{ff}) \overset{?}{\equiv} \texttt{ff} : \mathbb{B}$$

(Keeping only one case)

Split on the atomic neutral $f\,\texttt{tt}$.

Remark: There is a canonical location to split atomic neutrals.

Towards an implementation of boolean extensionality

Atomic neutral: A boolean neutral in deep normal-form with no proper boolean sub-neutral.

Idea: Hoist-away all atomic neutrals, and split them.

$$f : \mathbb{B} \to \mathbb{B}, f\ \mathtt{tt} \equiv \mathtt{ff}, f\ \mathtt{ff} \equiv \mathtt{tt}, x : \mathbb{B}, x \equiv \mathtt{tt} \vdash f\ \mathtt{tt} \stackrel{?}{\equiv} \mathtt{ff} : \mathbb{B}$$

(Keeping only one case)

Split on the atomic neutral $f\ \mathtt{ff}$.

Remark: There is a canonical location to split atomic neutrals up to some permutations.

Outline of the roadmap

Goal: Implement a correct and complete decision procedure for MLTT + boolean extensionality.

Following [Abel et al. 18], build a logical relation based on reducibility inside a proof-assistant.

Concretely, develop on top of Meven Bertrand and Loic Pujet's version in Coq.

Categorically, a variation of the sheaf model of simply typed theory from [Altenkirch et al. 01]: context-indexed families stable by renamings and satisfying the Cover rule.

Main obstacle: How to deal constructively with the universe ?

Conclusion

Future steps

- Finish the proof of normalization for MLTTin Coq
- Implement the conversion algorithm on top of it

Further directions

- Martin Baillon: application to (external) continuity of functions $(\mathbb{N} \to \mathbb{B}) \to \mathbb{N}$