

# The HoTT Library

## A Formalization of Homotopy Type Theory in Coq

Andrej Bauer<sup>\*</sup>

University of Ljubljana, Slovenia  
Andrej.Bauer@andrej.com

Jason Gross

MIT, USA  
jgross@mit.edu

Peter LeFanu Lumsdaine<sup>†</sup>

Stockholm University, Sweden  
p.l.lumsdaine@math.su.se

Michael Shulman<sup>‡</sup>

University of San Diego, USA  
shulman@sandiego.edu

Matthieu Sozeau<sup>§</sup>

Inria, France  
mattam@mattam.org

Bas Spitters<sup>¶</sup>

Aarhus University, Denmark  
spitters@cs.au.dk

### Abstract

We report on the development of the *HoTT library*, a formalization of homotopy type theory in the Coq proof assistant. It formalizes most of basic homotopy type theory, including univalence, higher inductive types, and significant amounts of synthetic homotopy theory, as well as category theory and modalities. The library has been used as a basis for several independent developments. We discuss the decisions that led to the design of the library, and we comment on the interaction of homotopy type theory with recently introduced features of Coq, such as universe polymorphism and private inductive types.

**Categories and Subject Descriptors** F.4.1 [Mathematical Logic and Formal Languages]: Mathematical Logic

<sup>\*</sup>This material is based upon work supported by the Air Force Office of Scientific Research, Air Force Materiel Command, USAF under Award No. FA9550-14-1-0096

<sup>†</sup>This material is based upon work supported by the National Science Foundation under Grant No. DMS-1128155.

<sup>‡</sup>This material is based on research sponsored by The United States Air Force Research Laboratory under agreement number FA9550-15-1-0053. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the United States Air Force Research Laboratory, the U.S. Government, or Carnegie Mellon University.

<sup>§</sup>This work has been partly funded by the CoqHoTT ERC Grant 637339.

<sup>¶</sup>This research was partially supported by the Guarded Homotopy Type Theory project, funded by the Villum Foundation, project number 12386.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

Copyright is held by the owner/author(s). Publication rights licensed to ACM.

CPP'17, January 16–17, 2017, Paris, France  
ACM. 978-1-4503-4705-1/17/01...\$15.00  
<http://dx.doi.org/10.1145/3018610.3018615>

**Keywords** Homotopy type theory, Univalent foundations, Coq, Higher inductive types, Universe polymorphism

### 1. Introduction

Homotopy type theory is a novel approach to developing mathematics in Martin-Löf's type theory, based on interpretations of the theory into abstract homotopy-theoretic settings such as certain higher toposes (Kapulkin and Lumsdaine 2012; Shulman 2015a). The connection between type theory and homotopy theory is originally due to (Awodey and Warren 2009) and (Voevodsky 2006).

Identity types are interpreted as path spaces, and type equivalence as homotopy equivalence. Type-theoretic constructions correspond to homotopy-invariant constructions on homotopy types. In addition, homotopical intuition gives rise to entirely new type-theoretic notions, such as higher inductive types and Voevodsky's univalence axiom. One can even develop homotopy theory in the language of type theory in a “synthetic” manner, treating (homotopy) types as a primitive notion.

The first formalization of homotopy type theory in a proof assistant was Voevodsky's *Foundations* library implemented in Coq, now called the *UniMath* project (Voevodsky et al. 2016). Here we present the second major such library, the *HoTT library*, also implemented in Coq, with somewhat different goals from those of UniMath. The library is freely available.<sup>1</sup>

Coq word count reports that the library contains 16800 lines of specifications, 13000 lines of proofs, and 4500 lines of comments. The library is self-sufficient, completely replacing the Coq standard library (which is incompatible with homotopy type theory) with a bare minimum necessary for basic Coq tactics to function properly (see §6).

<sup>1</sup><http://github.com/HoTT/HoTT> or the Coq OPAM package manager

**Contributions** The HoTT library provides a substantive formalization of homotopy type theory. It demonstrates that univalent foundations (cf. §2) provide a workable setup for formalization of mathematics. The library relies on advanced features of Coq (cf. §3), such as automatic handling of universe polymorphism (cf. §3.1) and type classes (cf. §3.2), management of opaque and transparent definitions (cf. §3.3), and automation (cf. §3.4). We used private inductive types to implement higher inductive types (cf. §4), and the Coq module system to formalize modalities (cf. §5). Our development pushed Coq’s abilities, which prompted the developers to extend and modify it for our needs (cf. §6), and to remove several bugs, for which we are most thankful. Overall, the success of the project relies on careful policies and software-engineering approaches that keep the library maintainable and usable (cf. §7). We relate our work to other extensive implementations of homotopy type theory in §8.

**Consistency** A major concern for any piece of formalized mathematics is trust. The HoTT library uses much more than just Martin-Löf type theory, including the univalence axiom, pattern matching, universe polymorphism, type classes, private inductive types, second-class modules, and so on; how do we know these form a consistent system? This is a major concern not just for us, but for every user of complex proof assistants, and has been addressed many times in the past.

In Coq, the typechecker’s kernel is the final gatekeeper. This is fairly large, in part due to the inclusion of the module system. However, other advanced features such as type classes and tactics are outside the kernel and hence do not endanger consistency. So, provided we trust the kernel, the remaining questions are the consistency of our axioms, universe-polymorphic modules, and the implementation of private inductive types.

There are several possible ways to tackle these questions. So far, the primary method available for homotopy type theory is semantic: constructing a model of the theory in some other trusted theory (such as ZFC). While this has been done for various fragments of the theory, combining them all to give a unified semantic account of homotopy type theory together with all the features in Coq’s kernel seems a daunting task.

For this reason, UniMath avoids almost all of Coq’s features (even e.g. record types), restricting itself as far as possible to standard Martin-Löf type theory (except for assuming  $\text{Type} : \text{Type}$  throughout, to simulate Voevodsky’s resizing rules). However, this restriction cannot be enforced by the kernel. We feel rather that proof assistants and computerized formalization of mathematics are at such an early stage that it is well worth experimenting, even at the risk of introducing an inconsistency (which is fairly slight, due to the known semantic accounts of fragments of the theory). In any case, the skeptical reader should keep in mind that the standard of rigor in formalized proofs is at least a great deal

higher than the generally accepted level of rigor in traditional written mathematics.

## 2. Basics

We assume basic familiarity with homotopy type theory (The Univalent Foundations Program 2013), and with the Coq proof assistant (The Coq Development Team 2016). There is a large overlap between the contents of the HoTT library and the contents of the book (The Univalent Foundations Program 2013), which we refer to as the “HoTT book”. The library provides an automatically generated file linking the constructions in the book with the corresponding Coq code.<sup>2</sup>

**Basic type formers and their identity types** The core of the library is in the `Basics` and `Types` directories. These files formalize fundamental results about the higher groupoid structure of identity types, and the identity types of basic types and type formers, such as the empty and unit types, universes,  $+$ ,  $\times$ ,  $\Pi$ , and  $\Sigma$ . This covers most of Chapter 2 of the HoTT book, as well as parts of Chapters 3 and 7 (basic definitions and facts about  $n$ -types), Chapter 4 (equivalences; see below), and Chapter 5 (basic facts about  $W$ -types).

The `Basics` directory contains absolutely basic facts applicable to all types; while the `Types` directory is organized with one file for each standard type former, roughly matching the sections in Chapter 2 of the HoTT book. Some other basic facts from the first part of the HoTT book can be found in the root `theories` directory, such as the comparison of different definitions of equivalence (see below) and the proof that univalence implies function extensionality.

**Equivalences** The HoTT book devotes most of Chapter 4 to discussing various notions of equivalence. After showing that a large class of them are equivalent, in a precise way, one can be agnostic on paper about which is meant. However, for a formalization we need to choose a particular definition.

The intuitive notion of isomorphism or homotopy equivalence consists of  $f : A \rightarrow B$  and  $g : B \rightarrow A$  which are inverses of each other, up to homotopy. However, in homotopy type theory the type of pairs  $f, g$  equipped with two such homotopies is ill-behaved, so one needs to refine it somehow.

We have chosen to use the notion called a *half-adjoint equivalence* in the HoTT book, which adds to this type a single coherence condition between the two homotopies. (The condition is one of the triangle identities involved in an “adjoint equivalence” in category theory; the other one is then provable, but should not be assumed as data or the homotopy type would be wrong again.) Since this is “the” notion of equivalence in the library, we call it simply an *equivalence*. Other possible options are Voevodsky’s definition of an equivalence as a map whose homotopy fibers are contractible, or Joyal’s suggestion of a map equipped with sepa-

<sup>2</sup><https://hott.github.io/HoTT/coqdoc-html/HoTTBook.html>

rate left and right homotopy inverses. We do prove the equivalence of all these definitions (in `EquivalenceVarieties`).

However, we believe that half-adjoint equivalences are a better choice for the standard notion of equivalence in a formalization. This is because the most common way to construct an equivalence, and to use an equivalence, is by way of the “incoherent” notion consisting of two functions and two homotopies, called a *quasi-inverse* in the HoTT book, and half-adjoint equivalences record all this data. That is, usually we construct an equivalence by exhibiting its homotopy inverse, and then apply a “coherentification” result. With half-adjoint equivalences represented as a Coq record, all the data of a quasi-inverse (plus the extra coherence) is stored exactly as supplied when an equivalence is defined. This applies in particular to the homotopy inverse, but also to the witnessing homotopies, though the “coherentification” process alters one of these homotopies, so if we want to preserve them both we have to manually prove the extra coherence property.

In addition to the definitions of equivalence appearing in the HoTT Book, we also consider two others. One is a “relational equivalence” (a relation under which each element of either type is related to a unique element of the other) which has the advantage of being judgmentally invertible, though it increases the universe level:

```
Record RelEquiv A B :=
{ equiv_rel : A → B → Type;
  rcf : forall a, Contr { b : B & equiv_rel a b };
  rcg : forall b, Contr { a : A & equiv_rel a b } }.
```

The other involves “ $n$ -path-splitness”, which says that the induced maps on the first  $n$  path spaces are split surjections.

```
Fixpoint PathSplit (n : nat) (f : A → B) : Type
:= match n with
| 0 => Unit
| S n => (forall a, hfiber f a) *
        forall x y, PathSplit n (@ap _ _ f x y)
end.
```

For  $n > 1$ , this is equivalent to being an equivalence. This definition has the advantage that when  $A$  and  $B$  are function-types and  $f$  is a precomposition map, we can reformulate it to use homotopies rather than equalities, yielding a notion of “precomposition equivalence” (called `ExtendableAlong`) that often avoids function extensionality. This is particularly useful for the universal property of modalities (§5).

**Finite sets** We define standard finite types `Fin n` as usual,

```
Fixpoint Fin (n : nat) : Type :=
match n with
| 0 => Empty
| S n => Fin n + Unit
end.
```

and then finite types as those that are merely<sup>3</sup> equivalent to the standard ones:

```
Class Finite (X : Type) :=
{ fcard : nat ;
  merely_equiv_fin : merely (X ≃ Fin fcard) }.
```

Perhaps surprisingly, being finite is still a mere proposition, because a set is isomorphic to at most one canonical finite set. Thus, we could have truncated the dependent sum and gotten an equivalent definition, but it would be less convenient to reason about.

**Pointed types** We provide a general theory of pointed types. The theory is facilitated by a tactic which often allows us to pretend that pointed maps and homotopies preserve basepoints *strictly*. We have carefully defined pointed maps `pMap` and pointed homotopies `pHomotopy` so that when destructed, their second components are paths with right endpoints free, to which we can apply Paulin-Mohring path-induction. The theory of pointed types uses type classes, since the base point can usually be found automatically:

```
Class IsPointed (A : Type) := point : A.
Record pType :=
{ pointed_type : Type ;
  ispointed_type : IsPointed pointed_type }.
Coercion pointed_type : pType → Sortclass.
Record pMap (A B : pType) :=
{ pointed_fun : A → B ;
  point_eq : pointed_fun (point A) = point B }.
Record pHomotopy {A B : pType} (f g : pMap A B) :=
{ pointed_htpy : f == g ;
  point_htpy :
    pointed_htpy (point A) @ point_eq g =
    point_eq f }.
```

Here `@` denotes the concatenation of paths.

**Category theory** The library also includes a large development of category theory, following Chapter 9 of the HoTT book and (Ahrens et al. 2015). This part of the library was presented in detail in (Gross et al. 2014), from which we quote only the following:

We wound up adopting the Coq version under development by homotopy type theorists, making critical use of its stronger universe polymorphism and higher inductive types... [which] can simplify the Coq user experience dramatically...

The category theory library employs a different style of formalization from the core library, using so-called “blast” tactics that automatically try many lemmas to produce a proof by brute force. We avoid this approach in the core

<sup>3</sup> As in the HoTT book, “merely” signifies the use of a propositional truncation, in this instance an existence of an equivalence rather than a concretely given one.

library to make proofs more readable and give better control over proof terms, cf. §3.3.

Timany and Jacobs (2016)<sup>4</sup> provide another extensive library for category theory over the HoTT library.

**Synthetic homotopy theory** The library also contains a variety of other definitions and results, many relevant to synthetic homotopy theory or higher category theory. This includes classifying spaces of automorphism groups, the Cantor space, the theory of idempotents with the results of (Shulman 2015b), and the definition of  $\infty$ -groups with actions. Such non-trivial additions to the core provide strong evidence that the overall design is sustainable and usable.

### 3. Features of Coq

In our library we made use of a number of useful features of Coq, some established and others relatively new. In this section we discuss most of these; two of the most substantial we give their own sections (§4 and §5).

#### 3.1 Universe Polymorphism

Coq’s type theory supports an infinite progression of cumulative universes, and constructions that are polymorphic in the universes (Sozeau and Tabareau 2014). Our library heavily relies on the flexible treatment of universe polymorphism, which allows us to forego universe annotations in specifications. However, one needs to be careful because Coq’s heuristic for minimizing the number of universes and constraints occasionally produces undesirable constraints, or just does not cope with them very well. For instance, the formalization of cumulative hierarchy of sets by Ledent (2014) induced unexpected universe inconsistencies that could only be resolved with explicit universe constraint annotations. These were indeed implemented in response to our troubles, and are now part of the standard Coq distribution.

Timany and Jacobs (2015) propose cumulative inductive types in Coq. It seems this would indeed alleviate most of the issues in our library, too.

**Object classifier** Following Section 4.8 of the HoTT book, we formalized the proof that the universe is an object classifier, a fundamental concept in higher topos theory. From this we can show that the propositions  $\mathbf{hProp}$  form a *large* subobject classifier. In fact, we show more generally that for each  $P : \text{Type} \rightarrow \text{Type}$  taking values in mere propositions, we have a classifier for maps whose fibers satisfy  $P$ ; this also includes all modalities (see §5).

In this part of the library, universe polymorphism works nicely and leads to a satisfactory treatment of subobject classifiers in a predicative setting. As a test, we verified that in  $\mathbf{hSets}$  epimorphisms are surjective. The proof looks like the usual impredicative one, but in fact, is entirely predicative thanks to universe polymorphism.

<sup>4</sup><https://github.com/amintimany/Categories-HoTT>

#### 3.2 Type Classes

Coq’s type class system is a very convenient mechanism for automatic derivation of instances of structures. The instance search follows a logic programming discipline which is sometimes difficult to predict and control, a potential problem for proof-relevant settings such as homotopy type theory. Nevertheless, it is safe to use the type class mechanism as long as it is employed to find only mere propositions, as all their instances are equal. Luckily, being an equivalence, deriving a truncation level, and placing a type into a subuniverse, are all of this kind, and so our library does use type classes in these non-problematic cases. We follow the development style of the math-classes library (Spitters and van der Weegen 2011; Krebbers and Spitters 2013; Castéran and Sozeau 2012), but since we have a better behaved equality and quotients, we can avoid an extensive use of setoids.

As is well known, one can only push the type class mechanism so far. For instance, we cannot add a rule for automatic instantiation of inverses of equivalence, as it makes Coq look for “the inverse of the inverse of the inverse ...”.

**Transfer from  $\Sigma$ -types to record types** Type classes are (dependently typed) record types, so many of the central concepts in the library are expressed as record types (rather than nested  $\Sigma$ -types). To avoid proving a series of general lemmas over and over, separately for each record type, we implemented a tactic `issig` that allows us to automatically transfer general facts about iterated  $\Sigma$ -types to record types. For example, `Contr` and `IsEquiv` are record types, and the tactic is able to automatically prove that

$$\text{forall } A, \{x : A \ \& \ \text{forall } y:A, x = y\} \simeq \text{Contr } A.$$

and

$$\begin{aligned} &\text{forall } A \ B, \text{forall } f : A \rightarrow B, \\ &\text{IsEquiv } f \simeq \\ &\quad \{g : B \rightarrow A \ \& \\ &\quad \{r : \text{Sect } g \ f \ \& \\ &\quad \{s : \text{Sect } f \ g \ \& \\ &\quad \text{forall } x : A, r \ (f \ x) = \text{ap } f \ (s \ x)\} \} \}. \end{aligned}$$

A fairly substantial use of this tactic arises in the development of factorization systems (e.g. epi-mono factorization), for the proof of uniqueness of factorizations (our `path_factorization`, Theorem 7.6.6 in the HoTT book). The book proof expresses the uniqueness using a threefold nesting of  $\Sigma$ -types followed by a threefold cartesian product. In the formalization this corresponds to a record type with six fields. The formal proof requires delicate transformations between records and  $\Sigma$ -types that would be very laborious to perform without `issig`.

**The  $\eta$ -rule for record types** Recent versions of Coq support an extensionality  $\eta$ -rule for record types, implemented by primitive projections. When we adapted the library to use primitive projections, the compilation time for the entire library dropped by a factor of two. We were also able to re-

place eight different kinds of natural transformations with a single one, remove applications of function extensionality from a number of proofs, and greatly speed up the tactics for transfer between  $\Sigma$ -types are record types.

**Type classes for axioms** We also use type classes to track the use of the univalence and function extensionality axioms. These axioms are defined to depend on an instance of a class that inhabits a dummy type. For instance, here is function extensionality:

```
Monomorphic Axiom dummy_fe : Type0.
Monomorphic Class Funext := { fev : dummy_fe }.
Axiom isequiv_apD10 :
  forall '{Funext} (A : Type) (P : A → Type) f g,
    IsEquiv (@apD10 A P f g).
```

Here, `apD10` is the canonical map from paths in the function type to homotopies between functions.

Any theorem that uses function extensionality must then state this fact explicitly with a `{Funext}` assumption. This makes it easy to tell which parts of the library depend on which axioms, without the need for `Print Assumptions`. We make `Funext` inhabit a dummy type rather than the actual type of `isequiv_apD10` so that the latter can be used at multiple universe levels with only a single assumption of `Funext`.

### 3.3 Transparency and Opacity

Since equality in homotopy type theory is proof-relevant, our lemmas are more often transparent than in most Coq developments. This means that much more care must be taken to construct the right, coherent, proof terms. An example is the proof of the Eckmann-Hilton theorem for identity types (Theorem 2.1.6 of the HoTT book), which is given explicitly using (higher) composites and whiskerings:

```
Definition eckmann_hilton
  {A : Type} {x:A} (p q : 1 = 1 => (x = x)) :
  p @ q = q @ p
:= (whiskerR_p1 p @@ whiskerL_1p q)^
   @ (concat_p1 _ @@ concat_p1 _)
   @ (concat_1p _ @@ concat_1p _)
   @ (concat_whisker _ _ _ p q)
   @ (concat_1p _ @@ concat_1p _)
   @ (concat_p1 _ @@ concat_p1 _)
   @ (whiskerL_1p q @@ whiskerR_p1 p).
```

Here `@` denotes concatenation of paths and `@@` denotes horizontal composition of 2-dimensional paths. It might be easier to find a proof using rewrite-type tactics, but we want this particular one.

We could benefit from good support for construction of explicit proof terms. Sozeau’s dependent pattern matching compiler (Sozeau 2010a) aims to provide such support in Coq. It is similar to how Agda works. Unfortunately, it currently depends on both the equality type being in `Prop` and uniqueness of identity proofs, which is incompatible with univalence. This issue has been solved in Agda (Cockx

et al. 2014) and is currently being adapted to Coq as part of the Equations package (Mangin and Sozeau 2015). The prelude of the HoTT library can already be processed using Equations, and we hope to be able to use it for the entire library in the future.

### 3.4 Automation

Once we collected a large number of lemmas about paths, we organized them in a rewrite database and used it to simplify proofs. Currently, we rewrite terms in a standard fashion, that is with *J*-elimination. However, we are likely to obtain better proof terms by using the technology of generalized rewriting (Sozeau 2010b), which would also know how to rewrite with equivalences, and other suitable general relations. For instance,

```
forall {A B : Type},
  IsHProp A → (A ≃ B) → IsHProp B
```

can be proved by rewriting without invoking the univalence axiom. This is done by first showing that the basic type constructors  $\Pi, \Sigma$  respect equivalence, and that contractibility transfers along equivalence. All concepts built from these will then also respect equivalence. So, surprisingly, even now that we have quotients in our type theory, the technology initially developed for setoid rewriting is still useful.

Two other tactics are worth mentioning. First, we have a tactic transparent `assert`, like ordinary `assert` (allowing on-the-fly interactive proof of assertions) except that the term produced remains transparent in the rest of the proof. (Meanwhile, this has been ported for inclusion in standard Coq.) Second, we implemented a custom version of the `apply` tactic which uses a more powerful unification algorithm than the one used by the standard `apply` tactic. This idea is inspired by similar techniques in `ssreflect` (Gonthier et al. 2015).

## 4. Higher Inductive Types

Higher inductive types are one of the main novelties in homotopy type theory. Where usual inductive types allow us to freely generate terms in a type, *higher* inductive types also allow us to *freely* generate equalities. Examples include the interval (two points and a path), the circle (a point and a self loop), suspensions, set quotients, and more complex examples that we shall discuss briefly.

Coq does not implement higher inductive types natively, so we simulate them using Licata’s trick (Licata and Shulman 2013). This method was originally used in Agda; to make it possible in Coq, experimental *private inductive types* had to be added (Bertot 2013). Private inductive types are defined inside a module, within which they behave as usual. Outside the module their induction principles and pattern matching are no longer available; but functions that were defined inside the module using those principles can still be called, and importantly still compute on constructors.

Licata’s trick uses this to implement higher inductive types whose induction principles compute definitionally on



Module Export Interval.

```
Private Inductive interval : Type1 :=
| zero : interval
| one : interval.
```

Axiom seg : zero = one.

```
Definition interval_ind (P : interval → Type)
(a : P zero) (b : P one) (p : seg # a = b)
: forall x:interval, P x
:= fun x => (match x return _ → P x with
| zero => fun _ => a
| one => fun _ => b
end) p.
```

```
Axiom interval_ind_beta_seg :
forall (P : interval → Type)
(a : P zero) (b : P one) (p : seg # a = b),
apD (interval_ind P a b p) seg = p.
```

End Interval.

```
Definition interval_rec (P : Type) (a b : P) (p : a = b)
: interval → P :=
interval_ind (fun _ => P) a b (transport_const _ _ @ p).
```

```
Definition interval_rec_beta_seg
(P : Type) (a b : P) (p : a = b) :
ap (interval_rec P a b p) seg = p.
```

**Figure 1.** The higher inductive interval

point-constructors. For instance, the definition of the interval is shown in Figure 1. Here  $\#$  denotes transport,  $@$  is concatenation of paths, and  $\text{apD}$  is application of a dependent function to a path. Importantly,  $\text{interval.rec } a \ b \ p$  *reduces* to  $a$ , because  $\text{zero}$  is actually a constructor of  $\text{interval}$ . The axiom  $\text{seg}$  could be used to derive a contradiction within the module; but this is not possible outside the module, so all we need to do is check that the code inside the module is safe.

Note that in  $\text{interval.ind}$  rather than simply matching on  $x$ , we apply the match statement to the path hypothesis  $p$  (but then never use it). If the path-hypotheses were not “used” anywhere in the match, Coq would notice this and conclude that two invocations of the induction principle ought to be judgmentally equal as soon as they have the same point-hypotheses, even if their path-hypotheses differ, also leading to inconsistency. (This was noticed by Bordg.)

The library currently includes higher inductive definitions of the interval, the circle, suspensions, truncations, set-quotients, and homotopy colimits such as coequalizers and pushouts, as well as the flattening lemma, all from Chapter 6 of the HoTT book. The library also formalizes some basic

synthetic homotopy theory from Chapter 8, such as using the encode-decode method to prove that the fundamental group of the circle is the integers.

The library contains some of the more experimental higher inductive types from the HoTT book. The cumulative hierarchy of well-founded sets from Chapter 10 was formalized by Ledent (2014) and is now part of the library. Two higher inductive-inductive types from Chapter 11, the Cauchy reals and the surreal numbers are trickier. Even ordinary inductive-inductive types (Nordvall Forsberg and Setzer 2012) are not supported in Coq 8.5, but fortunately it is possible to simulate them using private inductive types. The surreals are thus in the library, while the Cauchy reals have been formalized elsewhere (Gilbert 2016), as has another example of a higher inductive-inductive type, the partiality monad (Altenkirch et al. 2016). The formalization of the Cauchy reals and the partiality monad is based on an experimental Coq implementation of inductive-inductive types.<sup>5</sup> We plan to include these developments into the library as soon as the support for inductive-inductive types is sufficiently mature.

Finally, we note that since private inductive types do not technically use the path constructors, higher inductive types defined in this way sometimes end up in a universe that is too low. This can usually be fixed with explicit universe annotations.

## 5. Modalities and Modules

Type-theoretic modalities, cf. Section 7.7 of the HoTT book and (Rijke et al. 2016), generalize the  $n$ -truncations in homotopy type theory. They were used in *cohesive* homotopy type theory of Schreiber and Shulman (2012). While we were able to formalize proofs and constructions about modalities in a straightforward manner, the overall architecture of the definitions was quite tricky to implement.

Chapter 7 of the HoTT book contains a number of facts about truncations and connectedness which actually hold (as remarked therein) for any modality, with exactly the same proofs. In the library we therefore formalized general facts about modalities, following Chapter 7, and then instantiated them to truncations, which we defined as particular instances of modalities.

A modality is an operator  $\bigcirc$  which acts on types and satisfies a universal property that quantifies over all types. One might expect the formalization of  $\bigcirc$  to be a universe-polymorphic record type whose fields are the operator and its universal property. This does not work however, because the fields would share a common universally quantified universe index  $i$ , and would thus express the wrong universal property. That is, we need to express that  $\bigcirc$  at level  $i$  has the universal property with respect to every level  $j$ , not only  $i$ . We needed a construct like record types, but allowing each field to be individually universe-polymorphic.

<sup>5</sup> Sozeau, <https://github.com/mattam82/coq/tree/IR>

The solution was an undocumented feature of the Coq module system, which we briefly review. Coq provides ML-style modules similar to those of OCaml, the programming language used to implement Coq. Modules and type classes are similar, but the former are not first-class objects and therefore cannot be used for formalization of structures. Instead, modules serve a software-engineering purpose: they are used to organize source code into units, and to control visibility of implementation details. By a fortunate design choice, each entry in a module carries its own universal quantification over the universe levels.

The library formalizes a modality as a module type so that it can have the correct universal property. However, we lose many of the benefits of record types and type classes, as well as notational conveniences.

First, to pass a simple argument to a parametrized module (a functor in the ML-terminology), we need to wrap it into a module, which considerably increases the complexity of the code. Even worse, it prevents us from defining families of modalities, such as  $n$ -truncations indexed by a truncation index  $n$ . We used the standard trick of passing from families to display maps, and included in the definition of modality an additional field `Modality : Type`, to be used as the domain of a display map which encodes a family of modalities. For instance, truncations are implemented as a single module which sets `Modality` to `trunc_index`.

Second, Coq is very strict about matching modules against module types: it insists that the universe parameters and constraints match the specified ones exactly. Thus, in the formalization we had to battle Coq's universe heuristics and tightly control universes with explicit annotations in both definitions and proofs. We persevered with frequent use of `Set Printing Universes` and `Show Universes`, but we cannot recommend manual treatment of universe levels.

Third, Coq insists that every field in a module be fully polymorphic, while in several places we wanted to express additional constraints on the universe levels. We found a way around it which is far from ideal. It would be helpful if we could control universe indices and constraints in modules more precisely, although we fear having to do even more manual bookkeeping of universes. It would be interesting to attempt to formalize modalities in Agda or Lean, although it is not clear how this could be accomplished, since neither seem to support the kind of polymorphism that we needed.

Despite all these problems, the modalities code in the library is quite usable; from the outside one rarely needs to worry about the universe issues. In particular, the  $n$ -truncation is defined as a modality, and most of the basic theorems about truncation are obtained by specialization from general theorems about modalities. This seems to work quite smoothly in the rest of the library, although the user looking for a theorem about truncations has to know to check the general theorems about modalities.

## 6. Technical Changes to Coq

From the beginning, the development of the library has involved close collaboration with Coq developers, most notably Sozeau. A number of changes to the Coq system were needed when we started, but today the library compiles with standard Coq 8.5.1 and later. Our library has served as a testing platform for a number of new Coq features. Inefficiencies and bugs were reported by us and quickly addressed by the Coq developers. We mention several noteworthy changes to Coq:

- The inductive definition of the identity type has a single constructor, and so Coq puts it in `Prop`, contrary to what is needed in homotopy type theory. The `indices-matter` option of Coq, which was implemented already by Herbelin for the purposes of the Foundations library (Voevodsky 2015), changes this behavior to the desired one.
- We avoid the impredicative `Prop` altogether and only use `hProp`. An element of `hProp` consists of a type together with a proof that the type has at most one element. This small change makes the whole standard library unusable, and many tactics stop working, too. The solution was rather drastic: we ripped out the standard library and replaced it with a minimal core that is sufficient for the basic tactics to work. There is experimental work that aims to disentangle the tactics and the standard library,<sup>6</sup> which we hope to use in the future.
- The private inductive types are another experimental addition to Coq which allowed us to implement higher inductive types. This was already discussed in §4.

## 7. Software Engineering

The collaborative development of the library was made possible by using modern software engineering tools:

- We use GitHub as a platform for version control and discussion of the code. We have a strict “two pairs of eyes” policy according to which a code change may be accepted only after it has been reviewed by two other developers. This encourages good collaboration and the use of standardized naming schemes.
- An extensive style guide facilitates collaboration and allows others to contribute and build on the library. We use the GitHub wiki to keep track of documentation, and we automatically generate browsable and replayable literate code with `Coqdoc` and `Proviola`<sup>7</sup> tools. Our library is also one of the test cases for the JavaScript interface for Coq.<sup>8</sup>

<sup>6</sup>Gallego Arias, <http://github.com/ejgallego/coq/tree/coqlib-cleanup-master>

<sup>7</sup><http://mws.cs.ru.nl/proviola/>

<sup>8</sup><https://x80.org/rhino-hott/>

- We use Travis<sup>9</sup> for continuous integration. It checks whether a proposed code change compiles, which serves as a very useful sanity check. Travis also allowed us to keep track of compilation time, which may be an issue with such a large library. We built tools that help identify causes of performance degradation. When the culprit was a Coq change, we reported it to Coq developers who quickly fixed the issue.
- The installation procedure for the HoTT library is fairly complicated, as it requires a customized Coq installation. We provide automated scripts that help users with the installation. We also made the library available through the very successful OCaml Package Manager (OPAM).
- The use of Proof General together with Emacs TAGS allows us to easily navigate the library and find definitions of terms; Company-coq<sup>10</sup> provides even better facilities.

## 8. Related Work

The HoTT library was initiated as an attempt to understand the contents of Voevodsky’s Foundations library (Voevodsky 2015). In the beginning we closely followed the order of development of concepts in the Foundations library, but usually with our own proofs.

Nowadays the Foundations library has been incorporated into UniMath (Voevodsky et al. 2016). UniMath and HoTT still share many ideas about how to formalize homotopy type theory, with a few differences: UniMath uses the inconsistent assumption `Type : Type` as a simplifying device, whereas we deal with all the complexities of universe polymorphism; UniMath takes a conservative approach with respect to advanced Coq technology, whereas our library actually inspired a number of Coq features and serves as a testbed for new ones; finally, the HoTT library uses higher inductive types, which are generally avoided by UniMath.

Various external developments have also used the HoTT library as a base, including libraries for the interpretation of the database query language SQL in homotopy theory (Chu et al. 2016), and for monadic semantics of probabilistic computation with continuous data types (Faissole and Spitters 2016).

There are implementations of homotopy type theory in other proof assistants. The HoTT-Agda library<sup>11</sup> was initially started as a parallel development in Agda, but quickly took a different direction and experienced extensive development of synthetic homotopy theory. The private inductive types were inspired by Licata’s trick, which was originally implemented in Agda.

A new formalization of homotopy type theory in the proof assistant Lean (de Moura et al. 2015) is growing at

an impressive rate. Lean’s type class system is a particularly useful feature.

A related development is the prototype implementation of cubical type theory (Cohen et al. 2016), which includes a computational interpretation of univalence and (some) higher inductive types. This improves on one of the limitations of our setting, the use of axioms for univalence and function extensionality, which block computation in some proofs. We look forward to the integration of this technology in proof assistants.

## 9. Conclusion

We have developed a large, well-designed, and well-documented library for homotopy type theory, which formalizes a large portion of the HoTT book, including higher inductive types, and employs universe polymorphism. The library has successfully been used as a basis for several more specific formalizations. It serves as a testing ground for new Coq features, as well as a foundation on which to experiment with formalizing new ideas and applications of homotopy type theory.

## References

- B. Ahrens, K. Kapulkin, and M. Shulman. Univalent categories and the Rezk completion. *Mathematical Structures in Computer Science*, 25(05):1010–1039, 2015. [arXiv:1303.0584](https://arxiv.org/abs/1303.0584).
- T. Altenkirch, N. A. Danielsson, and N. Kraus. Partiality, revisited: The partiality monad as a quotient inductive-inductive type. Preprint, [arXiv:1610.09254](https://arxiv.org/abs/1610.09254), 2016.
- S. Awodey and M. A. Warren. Homotopy theoretic models of identity types. *Mathematical Proceedings of the Cambridge Philosophical Society*, 146:45–55, 2009.
- Y. Bertot. Private inductive types: Proposing a language extension. 2013. URL [https://coq.inria.fr/files/coq5\\_submission\\_3.pdf](https://coq.inria.fr/files/coq5_submission_3.pdf).
- P. Castéran and M. Sozeau. A gentle introduction to type classes and relations in Coq, 2012. URL <https://hal.archives-ouvertes.fr/hal-00702455>.
- S. Chu, K. Weitz, A. Cheung, and D. Suciuc. HoTTSQL: Proving query rewrites with univalent SQL semantics. Preprint, [arXiv:1607.04822](https://arxiv.org/abs/1607.04822), 2016.
- J. Cockx, D. Devriese, and F. Piessens. Pattern matching without K. In J. Jeuring and M. M. T. Chakravarty, editors, *Proc. International Conference on Functional Programming (ICFP 2014)*, volume 49 of *SIGPLAN Notices*, pages 257–268. ACM, 2014.
- C. Cohen, T. Coquand, S. Huber, and A. Mörtberg. Cubical type theory: a constructive interpretation of the univalence axiom. To appear, *Proc. Types for Proofs and Programs (TYPES 2015)*, 2016. URL <https://www.math.ias.edu/~amortberg/papers/cubicaltt.pdf>.
- The Coq Development Team. The Coq proof assistant. 2016. URL <http://coq.inria.fr/>.
- L. de Moura, S. Kong, J. Avigad, F. van Doorn, and J. von Raumer. The Lean theorem prover (system description). In A. P. Felty

<sup>9</sup><https://travis-ci.org/>

<sup>10</sup><https://github.com/cpitclaudel/company-coq>

<sup>11</sup><https://github.com/HoTT/HoTT-Agda>



- and A. Middeldorp, editors, *Automated Deduction – CADE-25*, volume 9195 of *LNCS*, pages 378–388, 2015. doi: 10.1007/978-3-319-21401-6\_26.
- F. Faissole and B. Spitters. Synthetic topology in homotopy type theory for probabilistic programming, 2016. URL <https://www.cs.au.dk/~spitters/ProbProg.pdf>.
- G. Gilbert. Formalising real numbers in homotopy type theory. To appear in *Proc. Certified Programs and Proofs 2017*, arXiv: 1610.05072, 2016.
- G. Gonthier, A. Mahboubi, and E. Tassi. A Small Scale Reflection Extension for the Coq system. Research Report RR-6455, Inria Saclay Île de France, 2015. URL <https://hal.inria.fr/inria-00258384>.
- J. Gross, A. Chlipala, and D. I. Spivak. Experience implementing a performant category-theory library in Coq. In G. Klein and R. Gamboa, editors, *Proc. Interactive Theorem Proving 2014*, volume 8558 of *LNCS*, pages 275–291. Springer, 2014. doi: 10.1007/978-3-319-08970-6\_18.
- C. Kapulkin and P. L. Lumsdaine. The simplicial model of univalent foundations (after Voevodsky). arXiv:1211.2851, 2012.
- R. Krebbers and B. Spitters. Type classes for efficient exact real arithmetic in Coq. *LMCS*, 9(1:1):1–27, 2013. doi: 10.2168/LMCS-9(1:01)2013. arXiv:1106.3448.
- J. Ledent. Modeling set theory in homotopy type theory, 2014. URL [http://perso.ens-lyon.fr/jeremy.ledent/internship\\_report.pdf](http://perso.ens-lyon.fr/jeremy.ledent/internship_report.pdf).
- D. R. Licata and M. Shulman. Calculating the fundamental group of the circle in homotopy type theory. In *Proc. ACM/IEEE Symposium on Logic in Computer Science, 2013*, pages 223–232. IEEE Computer Society, 2013.
- C. Mangin and M. Sozeau. Equations for hereditary substitution in Leivant’s predicative System F: A case study. In I. Cervesato and K. Chaudhuri, editors, *Proc. Logical Frameworks and Meta Languages: Theory and Practice, 2015*, volume 185 of *EPTCS*, pages 71–86. Open Publishing Association, 2015. doi: 10.4204/EPTCS.185.5.
- F. Nordvall Forsberg and A. Setzer. A finite axiomatisation of inductive-inductive definitions. In U. Berger, H. Diener, P. Schuster, and M. Seisenberger, editors, *Logic, Construction, Computation*, volume 3 of *Ontos mathematical logic*, pages 259–287. De Gruyter, 2012.
- E. Rijke, M. Shulman, and B. Spitters. Modalities in homotopy type theory. In preparation, 2016.
- U. Schreiber and M. Shulman. Quantum gauge field theory in cohesive homotopy type theory. In R. Duncan and P. Panangaden, editors, *Proc. 9th Workshop on Quantum Physics and Logic, QPL 2012*, 2012. arXiv:1408.0054.
- M. Shulman. Univalence for inverse diagrams and homotopy canonicity. *Mathematical Structures in Computer Science*, 25(5):1203–1277, 2015a. ISSN 0960-1295. doi: 10.1017/S0960129514000565. arXiv:1203.3253.
- M. Shulman. Idempotents in intensional type theory. arXiv: 1507.03634; to appear in *Logical Methods in Computer Science*, 2015b.
- M. Sozeau. Equations: A dependent pattern-matching compiler. In M. Kaufmann and L. C. Paulson, editors, *Proc. Interactive Theorem Proving 2010*, volume 6172 of *LNCS*, pages 419–434. Springer, 2010a.
- M. Sozeau. A new look at generalized rewriting in type theory. *Journal of Formalized Reasoning*, 2(1):41–62, 2010b.
- M. Sozeau and N. Tabareau. Universe polymorphism in Coq. In G. Klein and R. Gamboa, editors, *Proc. Interactive Theorem Proving 2010*, volume 8558 of *LNCS*, pages 499–514. Springer, 2014.
- B. Spitters and E. van der Weegen. Type classes for mathematics in type theory. *Mathematical Structures in Computer Science*, 21: 1–31, 2011. doi: 10.1017/S0960129511000119.
- A. Timany and B. Jacobs. First steps towards cumulative inductive types in CIC. In *Proc. Theoretical Aspects of Computing – ICTAC 2015*, volume 9399 of *LNCS*, pages 608–617, 2015. doi: 10.1007/978-3-319-25150-9\_36.
- A. Timany and B. Jacobs. Category theory in Coq 8.5: Extended version. CW Reports CW697, Department of Computer Science, KU Leuven, April 2016. URL <https://lirias.kuleuven.be/handle/123456789/540270>.
- The Univalent Foundations Program. *Homotopy Type Theory: Univalent Foundations for Mathematics*. <http://homotopytypetheory.org/book>, Institute for Advanced Study, 2013.
- V. Voevodsky. A very short note on the homotopy  $\lambda$ -calculus. [http://www.math.ias.edu/~vladimir/Site3/Univalent\\_Foundations\\_files/Hlambda\\_short\\_current.pdf](http://www.math.ias.edu/~vladimir/Site3/Univalent_Foundations_files/Hlambda_short_current.pdf), 2006.
- V. Voevodsky. Experimental library of univalent formalization of mathematics. *Mathematical Structures in Computer Science*, 25: 1278–1294, 2015. arXiv:1401.0053.
- V. Voevodsky, B. Ahrens, D. Grayson, et al. *UniMath: Univalent Mathematics*. <https://github.com/UniMath>, 2016.