Formalizing category theory in type theory

Benedikt Ahrens

Semantics of proofs and certified mathematics
Institut Henri Poincaré
2014-05-06

Harrison, *Formalized Mathematics* (1996)

> *... category theory [is] notoriously hard to formalize in any kind of system ...*

- I did have a painful experience trying to formalize category theory in `HOL Light`.
- In **dependent** type theory, such a formalization is feasible; witnessed by various libraries created between then and now.

In this talk

- give an overview of category theory in extensional and intensional type theory
- discuss a definition of categories in Univalent Foundations, an intensional type theory with extensional features

What is a category in set theory?

Definition

A **category** is given by

- a set O of **objects**
- a set A of **arrows** (or **morphisms**)
- two maps

$$\mathsf{source}, \mathsf{target} : A \to O$$

...

Say $f : a \to b$ for $f \in A$ with $\mathsf{source}(f) = a$ and $\mathsf{target}(f) = b$.

What is a category in set theory?

Definition (contd.)

...

- composition of **composable** arrows

$$\frac{f : a \to b \qquad g : b \to c}{g \circ f : a \to c}$$

- for any object $a \in O$, an identity arrow

$$\frac{a \in O}{\mathrm{id}(a) : a \to a}$$

- satisfying some axioms similar to monoid axioms

Why formalizing category theory in (ML) type theory?

Dyckhoff: *Category theory as an extension of MLTT* (1985)

- Curry-Howard is conceptually clean
- category theory is inherently typed
- category theory is inherently dependently typed
- dependent functions allow natural implementation of composition, definition of pullbacks etc.
- hierarchy of universes allows for a "category of categories"

Outline

1. Category theory in dependent type theory
   - Categories in extensional type theory
   - Categories in intensional type theory
2. Univalent Foundations
   - Univalent Foundations: an overview
   - Propositions and sets in UF
   - The Univalence Axiom for sets
3. Categories in Univalent Foundations
   - A univalence axiom for categories
   - The Rezk completion

Table of Contents

Table of Contents

A definition of category in `Nuprl`

From Altucher & Panangaden: *A Mechanically Assisted Constructive Proof in Category Theory* (1990)

```
Category ==
   Obj: U2
 # Mor: (Obj # Obj) -> U1
 # Id : (A:Obj -> Mor(A,A))
 # o  : (A:Obj -> B:Obj -> C:Obj -> Mor(A,B)
              -> Mor(B,C) -> Mor(A,C))
```

A definition of category in Nuprl

From Altucher & Panangaden: *A Mechanically Assisted Constructive Proof in Category Theory* (1990)

```
Category ==
   Obj: U2
 # Mor: (Obj # Obj) -> U1
 # Id : (A:Obj -> Mor(A,A))
 # o  : (A:Obj -> B:Obj -> C:Obj -> Mor(A,B)
            -> Mor(B,C) -> Mor(A,C))

 # forall A,B:Obj.forall f:Mor(A,B).
       f o Id(A) {A,A,B} = f in Mor(A,B)
 # forall A,B:Obj.forall g:Mor(B,A).
       Id(A) o g {B,A,A} = g in Mor(B,A)
 # forall A,B,C,D:Obj.forall f:Mor(C,D).
     forall g:Mor(B,C). forall h:Mor(A,B).
       ((f o g {B,C,D}) o h {A,B,D}) =
        (f o (g o h {A,B,C}) {A,C,D}) in Mor(A,D)
```

Sanity check: a category of sets/types

Altucher & Panangaden '90:

> *For instance we have proved the goal "Category" using* ***U1*** *(the universe of small types in Nuprl) to represent the objects and the function space between two types to represent the morphisms. Identity and composition are what you would expect and the axioms were easily proved.*

```
Category ==
   Obj: U2
 # Mor: (Obj # Obj) -> U1
```

Where do morphisms live?

- Category theory requires a category of **sets** (or types) where morphisms live.
- **extensional** universe of types behaves like a category (of sets)
- **intensional** universe does **not**, e.g.,
  cannot prove
  $$f \circ \mathsf{id} = f$$
  but only
  $$\forall x : A, (f \circ \mathsf{id})(x) = f(x)$$
  for a function $f : A \to B$

Equality of morphisms in `Constructions`

Coquand & Huet: *Constructions: A higher-order proof system for mechanizing mathematics* (1985)
Equality given by **Leibniz principle**:

$$a = b : A \quad := \quad \forall P : A \to \mathsf{U}, P(a) \to P(b)$$

About an axiomatization of categories using Leibniz equality:

> *This definition is not quite general enough, since it assumes intensional equality for morphisms. A more general definition would replace the equality = by a relation E postulated to be an equivalence relation compatible with composition.*

Table of Contents

Setoids for hom-objects

Definition

A **setoid** is given by

- a type A
- an equivalence relation $R : A \to A \to \mathsf{U}$

In type theory:

$$\mathsf{Setoid} := \sum_{(A:\mathsf{U})} \sum_{(R:A\to A\to \mathsf{U})} \mathsf{isEquivRel}(R)$$

Category theory in **intensional** type theory

```
Category ==
   Obj: U2
 # Mor: (Obj # Obj) -> Setoid
 # Id : (A:Obj -> Mor(A,A))
 # o  : (A:Obj -> B:Obj -> C:Obj -> Mor(A,B)
              -> Mor(B,C) -> Mor(A,C))
 # o_R: <composition is compatible with R>
 # forall A,B:Obj.forall f:Mor(A,B).
       f o Id(A) {A,A,B} R f in Mor(A,B)
 # forall A,B:Obj.forall g:Mor(B,A).
       Id(A) o g {B,A,A} R g in Mor(B,A)
 # forall A,B,C,D:Obj.forall f:Mor(C,D).
     forall g:Mor(B,C). forall h:Mor(A,B).
       ((f o g {B,C,D}) o h {A,B,D}) R
        (f o (g o h {A,B,C}) {A,C,D}) in Mor(A,D)
```

Sanity check: setoids form a category

Category of setoids

The cartesian closed category of setoids is a category for aforementioned definition.

- Aczel '93: *Galois: A Theory Development Project*
- Dybjer & Gaspes '94: *Implementing a category of sets in ALF*
- Huet & Saïbi: working towards *ConCaT* ('98)

Nowadays many libraries of basic category theory in `Coq` and `Agda` use setoids.

How to do category theory in Univalent Foundations?

Univalent Foundations is an intensional type theory with extensional features.

Question

What is a good definition of category in Univalent Foundations?

Table of Contents

Table of Contents

Univalent Foundations

What are the Univalent Foundations?

- Intensional Martin-Löf Type Theory

$\rightsquigarrow$ *Types as Spaces* interpretation

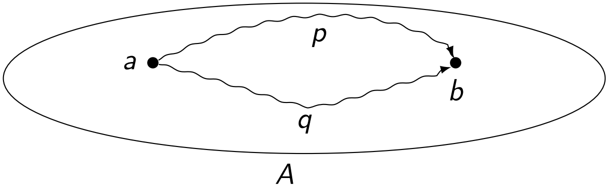
$+$ Voevodsky's **Univalence Axiom**

Martin-Löf TT and its Homotopy Interpretation

Type theory	Notation	Interpretation
Inhabitant	$a : A$	a is a point in space A
Dependent type	$x : A \vdash B(x)$	...
Sigma type	$\sum_{x:A} B(x)$	...
Product type	$\prod_{x:A} B(x)$	...
Identity type	$\mathsf{Id}_A(a, b)$	space of **paths** $p : a \rightsquigarrow b$

Interpretation: identity type as path space

Terms $p, q : \mathsf{Id}_A(a, b)$ are interpreted as paths $p, q : a \rightsquigarrow b$



Mixing syntax and semantics

- Call a term $p : \mathsf{Id}(a, b)$ a "path from a to b", write $p : a \rightsquigarrow b$
- Say a and b are **homotopic** if there is a path $p : a \rightsquigarrow b$.

The homotopy interpretation of identity types

Interpretation of the operations on paths:

Type theory	Interpretation	Notation
"reflexivity"	constant path on a	$\mathsf{refl}(a)$
"symmetry"	path reversal	p^{-1}
"transitivity"	path concatenation	$p \star q$
higher identity type	paths between paths	$p \leadsto q$

Univalence vs. Axiom K

- Univalence is incompatible with the assumption that any two terms of identity type are identical (Axiom K).
- That is, identities between identities matter.
- However, for some types, one can **prove K**.

Table of Contents

Propositions as some types

Definition (Proposition in UF)

A type A is a **proposition** if all its inhabitants are homotopic, ie. if one can construct a function of type

$$\mathsf{isProp}(A) := \prod_{x:A} \prod_{y:A} x \rightsquigarrow y \quad .$$

Propositions as some types

Definition (Proposition in UF)

A type A is a **proposition** if all its inhabitants are homotopic, ie. if one can construct a function of type

$$\mathsf{isProp}(A) := \prod_{x:A} \prod_{y:A} x \rightsquigarrow y \quad .$$

- "Being a proposition" is an internal notion.
- "Being a proposition" is a proposition, ie. one can prove

$$\mathsf{isProp}(\mathsf{isProp}(A))$$

- Intuitively, a proposition is either empty or a singleton.

Sets in Univalent Foundations

Definition (Sets in UF)

The type A is a **set** if for any $x, y : A$ the type $x \rightsquigarrow y$ is a proposition,

$$\mathsf{isSet}(A) := \prod_{x,y:A} \mathsf{isProp}(x \rightsquigarrow y)$$

Define

$$\mathsf{Set} := \sum_{A:\mathsf{U}} \mathsf{isSet}(A)$$

Sets in Univalent Foundations

Definition (Sets in UF)

The type A is a **set** if for any $x, y : A$ the type $x \rightsquigarrow y$ is a proposition,

$$\mathsf{isSet}(A) := \prod_{x,y:A} \mathsf{isProp}(x \rightsquigarrow y)$$

Define

$$\mathsf{Set} := \sum_{A:\mathsf{U}} \mathsf{isSet}(A)$$

- Points of a set are identical in a unique way, if they are.
- Sets are precisely those types which satisfy UIP / Axiom K.
- Sets correspond to **discrete spaces**.

About the use of the word “unique”

Definition

We call the point $a : A$ **unique** if any point $x : A$ is **homotopic** to a, ie. if we can construct a function of type

$$\prod_{x:A} x \rightsquigarrow a$$

About the use of the word "unique"

Definition

We call the point $a : A$ **unique** if any point $x : A$ is **homotopic** to a, ie. if we can construct a function of type

$$\prod_{x:A} x \rightsquigarrow a$$

A type A with a unique point $a : A$ is called "contractible":

Definition

We call A **contractible** if we can construct a term of type

$$\mathsf{isContr}(A) := \sum_{(a:A)} \prod_{(x:A)} x \rightsquigarrow a$$

Table of Contents

Isomorphism of sets. . .

Definition

Let $A, B : \mathsf{Set}$ be sets. The map $f : A \to B$ is an **isomorphism** if there are

- $$g : B \to A$$
- $$\eta : \prod_{a:A} g\big(f(a)\big) \rightsquigarrow a \qquad \epsilon : \prod_{b:B} f\big(g(b)\big) \rightsquigarrow b$$

Isomorphism of sets...

Definition

Let $A, B : \mathsf{Set}$ be sets. The map $f : A \to B$ is an **isomorphism** if there are

- $$g : B \to A$$
- $$\eta : \prod_{a:A} g\big(f(a)\big) \rightsquigarrow a \qquad \epsilon : \prod_{b:B} f\big(g(b)\big) \rightsquigarrow b$$

That is

$$\mathsf{isIso}(f) := \sum_{g:B\to A} \left(\prod_{a:A} g\big(f(a)\big) \rightsquigarrow a \right) \times \left(\prod_{b:B} \dots \right)$$

Isomorphism of sets

Lemma

$\mathsf{isIso}(f)$ *is a proposition; in particular, an inverse of* f *is unique.*

Definition (Type of isomorphisms from A to B)

$$\mathsf{Iso}(A, B) := \sum_{f:A\to B} \mathsf{isIso}(f)$$

The Univalence Axiom for sets

Definition (From paths to isomorphisms)

$$\mathsf{idtoiso} : \prod_{A,B:\mathsf{Set}} (A \rightsquigarrow B) \to \mathsf{Iso}(A, B)$$

$$\mathsf{idtoiso}_{A,A}(\mathsf{refl}(A)) :\equiv (\lambda x^A.x, \_)$$

The Univalence Axiom for sets

Definition (From paths to isomorphisms)

$$\mathsf{idtoiso} : \prod_{A,B:\mathsf{Set}} (A \rightsquigarrow B) \to \mathsf{Iso}(A, B)$$

$$\mathsf{idtoiso}_{A,A}(\mathsf{refl}(A)) :\equiv (\lambda x^A.x, \_)$$

Univalence Axiom for sets

$$\mathsf{univalence} : \prod_{A,B:\mathsf{Set}} \mathsf{isIso}(\mathsf{idtoiso}_{A,B})$$

In particular, Univalence gives a map backwards:

$$\mathsf{isotoid}_{A,B} : \mathsf{Iso}(A, B) \to (A \rightsquigarrow B)$$

Consequences of Univalence

- Propositional extensionality

$$(P \leftrightarrow Q) \to (P \rightsquigarrow Q)$$

- Function extensionality:

$$\left(\prod_{x:A} f(x) \rightsquigarrow g(x)\right) \to (f \rightsquigarrow g)$$

  and its dependent variant

- Quotient types exist

Table of Contents

Table of Contents

Categories in Univalent Foundations — Take I

A naïve definition of categories

A **category** $\mathcal{C}$ is given by

- a type $\mathcal{C}_0$ of objects
- for any $a, b : \mathcal{C}_0$, a type $\mathcal{C}(a, b)$ of morphisms
- operations: identity id & composition $(\circ)$
- axioms: unitality & associativity

$$\text{unital} : \prod_{a,b:\mathcal{C}_0, f:\mathcal{C}(a,b)} (\mathsf{id}_b \circ f \rightsquigarrow f) \times (f \circ \mathsf{id}_a \rightsquigarrow f)$$

Categories in Univalent Foundations — Take I

A naïve definition of categories

A **category** $\mathcal{C}$ is given by

- a type $\mathcal{C}_0$ of objects
- for any $a, b : \mathcal{C}_0$, a **type** $\mathcal{C}(a, b)$ of morphisms
- operations: identity id & composition $(\circ)$
- axioms: unitality & associativity

$$\text{unital} : \prod_{a,b:\mathcal{C}_0, f:\mathcal{C}(a,b)} (\mathsf{id}_b \circ f \rightsquigarrow f) \times (f \circ \mathsf{id}_a \rightsquigarrow f)$$

Where should morphisms live?

- Types (of a fixed universe) and functions between them form a category.
- But the definition is wrong for other reasons:

  categorical **axioms** should be **properties**
- Categorical axioms speak about identities of morphisms.
- If morphisms form a **set**, then identities between them are propositions.

Categories in Univalent Foundations — Take II

Definition (Category in UF)

A **category** $\mathcal{C}$ is given by

- a type $\mathcal{C}_0$ of objects
- for any $a, b : \mathcal{C}_0$, a set $\mathcal{C}(a, b)$ of morphisms
- operations: identity & composition
- axioms

Categories in Univalent Foundations — Take II

Definition (Category in UF)

A **category** $\mathcal{C}$ is given by

- a type $\mathcal{C}_0$ of objects
- for any $a, b : \mathcal{C}_0$, a **set** $\mathcal{C}(a, b)$ of morphisms
- operations: identity & composition
- axioms

- Functions between sets form a set

$\rightsquigarrow$ we can define a category of sets

A closer look at the category of sets

The Univalence Axiom for sets A and B says:

$$\mathsf{idtoiso}_{A,B} : (A \rightsquigarrow B) \to \mathsf{Iso}(A, B)$$

is an isomorphism, i.e.

In the category of sets

$$\text{identities of objects} \quad \cong \quad \text{isomorphisms of objects}$$

Motivates adding this as additional axiom to the definition of category. . .

Isomorphism in a category

Definition (Isomorphism in a category)

A morphism $f : \mathcal{C}(a, b)$ is an **isomorphism** if there are

- $$g : \mathcal{C}(b, a)$$
- $$\eta : g \circ f \rightsquigarrow \mathsf{id}_a \qquad \epsilon : f \circ g \rightsquigarrow \mathsf{id}_b$$

i.e.

$$\mathsf{isIso}(f) := \sum_{g : \mathcal{C}(b,a)} \Big((g \circ f \rightsquigarrow \mathsf{id}_a) \times (f \circ g \rightsquigarrow \mathsf{id}_b) \Big)$$

Isomorphism in a category

Definition (Isomorphism in a category)

A morphism $f : \mathcal{C}(a, b)$ is an **isomorphism** if there are

- $$g : \mathcal{C}(b, a)$$
- $$\eta : g \circ f \rightsquigarrow \mathsf{id}_a \qquad \epsilon : f \circ g \rightsquigarrow \mathsf{id}_b$$

i.e.

$$\mathsf{isIso}(f) :\equiv \sum_{g : \mathcal{C}(b,a)} \Big((g \circ f \rightsquigarrow \mathsf{id}_a) \times (f \circ g \rightsquigarrow \mathsf{id}_b) \Big)$$

For the category of sets, this definition of isomorphism is equivalent to the one given above (using FE).

Isomorphism in a category II

Lemma

For any $\mathsf{f} : \mathcal{C}(a, b)$*, the type* $\mathsf{isIso}(f)$ *is a proposition.*

Definition (The type of isomorphisms)

$$\mathsf{Iso}(a, b) := \sum_{f : \mathcal{C}(a,b)} \mathsf{isIso}(f)$$

From paths to isomorphisms

Definition (Univalent category, Hofmann & Streicher '98)

For objects $a, b : \mathcal{C}_0$ define

$$\begin{aligned} \mathsf{idtoiso}_{a,b} : (a \rightsquigarrow b) &\to \mathsf{Iso}(a,b) \\ \mathsf{refl}(a) &\mapsto \mathsf{id}_a \end{aligned}$$

Call the category $\mathcal{C}$ **univalent** if, for any objects $a, b : \mathcal{C}_0$,

$$\mathsf{idtoiso}_{a,b} : (a \rightsquigarrow b) \to \mathsf{Iso}(a,b)$$

is an isomorphism of sets.

From paths to isomorphisms

Definition (Univalent category, Hofmann & Streicher '98)

For objects $a, b : \mathcal{C}_0$ define

$$\begin{aligned} \mathsf{idtoiso}_{a,b} : (a \rightsquigarrow b) &\to \mathsf{Iso}(a, b) \\ \mathsf{refl}(a) &\mapsto \mathsf{id}_a \end{aligned}$$

Call the category $\mathcal{C}$ **univalent** if, for any objects $a, b : \mathcal{C}_0$,

$$\mathsf{idtoiso}_{a,b} : (a \rightsquigarrow b) \to \mathsf{Iso}(a, b)$$

is an isomorphism of sets.

- In a univalent category, isomorphic objects are equal.
- *"$\mathcal{C}$ is univalent"* is a proposition.

Further definitions

- Functors between (univalent) categories are defined as usual.
- Same for natural transformations.
- "Equivalence" means "adjoint equivalence" in the following.

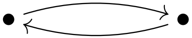
Examples of univalent categories

- <u>Set</u> (follows from the Univalence Axiom)
- categories of algebraic structures (groups, rings,...)
  - $\rightsquigarrow$ made precise by the **Structure Identity Principle** (Aczel, Coquand, Danielsson)
- full subcategories of univalent categories
- functor category $\mathcal{D}^{\mathcal{C}}$, if $\mathcal{D}$ is univalent

Some more examples of univalent categories

- A preorder, considered as a category, is univalent iff it is antisymmetric.
- Suppose X with $\mathsf{isSet}(x \rightsquigarrow y)$ for any $x, y : X$, then there is a univalent category with X as objects and $\mathsf{hom}(x, y) := (x \rightsquigarrow y)$.
- If $\mathcal{C}$ is univalent, then the category of cones of shape $F : \mathcal{J} \to \mathcal{C}$ is.

Non-univalent categories

- 
- more generally, any **chaotic** category $\mathcal{C}$ with $\mathcal{C}(x, y) := \mathbf{1}$ unless $\mathcal{C}_0$ is contractible
- any chaotic category $\mathcal{C}$ with an object $c : \mathcal{C}_0$ is **equivalent** to the terminal category $\mathbf{1} := \bullet$
  - $\rightsquigarrow$ a category can be equivalent to a univalent one without being univalent itself

Extensionality for univalent categories

Theorem (A., Kapulkin, Shulman; conjectured by Hofmann & Streicher '98)

For ***univalent*** *categories $\mathcal{C}$ and $\mathcal{D}$, the following are equivalent (as types in UF).*

Identity	$\mathcal{C} \rightsquigarrow \mathcal{D}$
Isomorphism	$\mathcal{C} \cong \mathcal{D}$
Equivalence	$\mathcal{C} \simeq \mathcal{D}$

Extensionality for univalent categories

Theorem (A., Kapulkin, Shulman; conjectured by Hofmann & Streicher '98)

*For **univalent** categories $\mathcal{C}$ and $\mathcal{D}$, the following are equivalent (as types in UF).*

Identity	$\mathcal{C} \rightsquigarrow \mathcal{D}$
Isomorphism	$\mathcal{C} \cong \mathcal{D}$
Equivalence	$\mathcal{C} \simeq \mathcal{D}$

Consequence

Every property of univalent categories definable in UF is invariant under equivalence.

Table of Contents

Rezk completion

- *"Being univalent"* is a proposition

$\rightsquigarrow$ Inclusion from univalent categories to categories

Theorem (A., Kapulkin, Shulman)

The inclusion of univalent categories into categories has a left adjoint (in bicategorical sense),

$$\mathcal{C} \mapsto \widehat{\mathcal{C}}, \qquad \textit{the } \textbf{\textit{Rezk completion}} \textit{ of } \mathcal{C}\ .$$

Rezk completion

- *"Being univalent"* is a proposition

$\rightsquigarrow$ Inclusion from univalent categories to categories

Theorem (A., Kapulkin, Shulman)

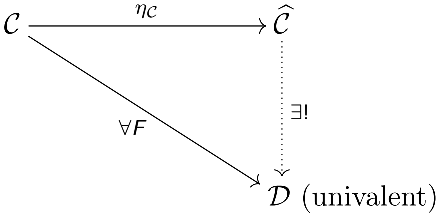
The inclusion of univalent categories into categories has a left adjoint (in bicategorical sense),

$$\mathcal{C} \mapsto \widehat{\mathcal{C}}, \qquad \textit{the } \textbf{\textit{Rezk completion}} \textit{ of } \mathcal{C} \;.$$

Named after C. Rezk (*A model for the homotopy theory of homotopy theory* (2001))

Rezk completion II

Any functor $F : \mathcal{C} \to \mathcal{D}$ with $\mathcal{D}$ univalent factors uniquely:



The functor $\eta_{\mathcal{C}}$ is the unit of the adjunction; it is

- fully faithful and
- essentially surjective.

Construction of the Rezk completion

- $\widehat{\mathcal{C}}$:= full image subcat. of $\underline{\mathsf{Set}}^{\mathcal{C}^{\mathrm{op}}}$ of Yoneda embedding
  - $\widehat{\mathcal{C}}$ is univalent
- $\eta_{\mathcal{C}} : \mathcal{C} \to \widehat{\mathcal{C}}$:= the Yoneda embedding (into $\widehat{\mathcal{C}}$):
  - fully faithful
  - essentially surjective (by definition)
- precomposition $\_ \circ H : \mathcal{C}^{\mathcal{B}} \to \mathcal{C}^{\mathcal{A}}$ is an equivalence—and hence an isomorphism—of categories if
  - H is essentially surjective and fully faithful
  - $\mathcal{C}$ is univalent
- the object function thus is an isomorphism of types

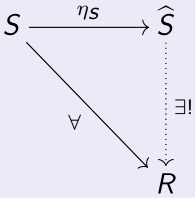
$$\_ \circ H : (\mathcal{C}^{\mathcal{B}})_0 \to (\mathcal{C}^{\mathcal{A}})_0$$

Special case of Rezk completion: Quotienting

Consider a setoid as a category:

Theorem (Univalent Foundations admits quotients)

Any map $f : S \to R$ such that $s \sim s' \implies f(s) \rightsquigarrow f(s')$ factors uniquely via $\widehat{S}$:



More direct construction of set-level quotients by Voevodsky: "type of equivalence classes"

Another example: the classifying space of a group

- Consider group G as category with one object
- $\mathcal{B}(G) :=$ classifying space, ie. the space such that

$$\Omega(\mathcal{B}(G)) = G$$

- Construction of $\mathcal{B}(G)$ as space of **torsors** is the Rezk completion
- Directly formalized in UF by Dan Grayson

Implementation in Coq

Rezk completion checked in Coq+UA+Type:Type

- approx. 4000 lines of code
- based on Voevodsky's library "*Foundations*"

Wishlist for proof assistant

- Tactics for "relevant rewriting"
- Facilities for handling of (iterated) Sigma types and identities between dependent pairs

Future work

- (univalent) enriched categories
- higher categories via enrichment

Thanks to

- Peter Aczel
- Thierry Coquand
- Peter Dybjer
- Roy Dyckhoff
- Gérard Huet
- Christoph Kreitz
- Tim Richter

for answering questions about the beginnings of category theory in type theory.