

# Why so much fuss over equality?

Cyril Cohen

Programming Logic  
cyrilc@chalmers.se

September 10, 2013

# Equalities on natural numbers

$$2 + 2 = 4$$

$$\forall n, n + n = 2n$$

$$\forall n, \exists m, \exists (p_i)_{i < m} \text{ primes, } n = \prod_i p_i$$

# Equalities on natural numbers

$$2 + 2 = 4$$

$$\forall n, n + n = 2n$$

$$\forall n, \exists m, \exists (p_i)_{i < m} \text{ primes, } n = \prod_i p_i$$

Everyone should agree at least on these.

# Equalities on higher order objects?

- equality of functions

quicksort = bubble sort?

- equality of sets

$$\left\{ \prod_i p_i^{k_i} \mid k \in \text{list } \mathbb{N} \right\} = \mathbb{N}$$

$\{0, 1\} = \{a, b\}$  when  $a \neq b$ ?

- equality of groups

$$\mathbb{Z}/n\mathbb{Z} = \{\omega^k \mid \omega \text{ primitive } n^{\text{th}} \text{ root of unity}\}?$$

## What is equality?

Axiom I (Axiom of extensionality) from Zermelo's 1908 *Investigations in the foundation of set theory*:

“If every element of a set  $M$  is also an element of  $N$  and vice versa, [...] then always  $M = N$ ”.

Everything is defined from sets, in particular, equality of functions is equality of their graphs.

# Equalities on higher order objects?

- equality of functions

quicksort = bubble sort? Yes

- equality of sets

$$\left\{ \prod_i p_i^{k_i} \mid k \in \text{list } \mathbb{N} \right\} = \mathbb{N} \quad \text{Yes}$$

$\{0, 1\} = \{a, b\}$  when  $a \neq b$ ? No

- equality of groups

$\mathbb{Z}/n\mathbb{Z} = \{\omega^k \mid \omega \text{ primitive } n^{\text{th}} \text{ root of unity}\}$ ? No

What is equality?

# In Type Theory

What is equality?

Leibniz equality:

$$\text{Id } A \ x \ y \quad = \quad \forall P : A \rightarrow *, P \ x \rightarrow P \ y$$

We also write  $x = y$  for  $\text{Id } A \ x \ y$ .



# Type Theory motto

Propositions are Types, Proofs are Programs

$x = y$  is an identity **type**, any element of this type is a proof that  $x$  is equal to  $y$ .

# Equalities on higher order objects?

- equality of functions

quicksort = bubble sort?

- equality of sets

$$\left\{ \prod_i p_i^{k_i} \mid k \in \text{list } \mathbb{N} \right\} = \mathbb{N}$$

$\{0, 1\} = \{a, b\}$  when  $a \neq b$ ?

- equality of groups

$$\mathbb{Z}/n\mathbb{Z} = \{\omega^k \mid \omega \text{ primitive } n^{\text{th}} \text{ root of unity}\}?$$

# Functional extensionality

Equality of functions?

quicksort = bubble sort?

Functional extensionality *axiom*:

$$(\forall x, f\ x = g\ x) \rightarrow f = g$$

Not provable in Type Theory  $\Rightarrow$  no explicit inhabitant of the above proposition.

# Equalities on higher order objects?

- equality of functions

quicksort = bubble sort? FunExt

- equality of sets

$$\left\{ \prod_i p_i^{k_i} \mid k \in \text{list } \mathbb{N} \right\} = \mathbb{N} \quad \text{FunExt?}$$

$\{0, 1\} = \{a, b\}$  when  $a \neq b$ ? No

- equality of groups

$\mathbb{Z}/n\mathbb{Z} = \{\omega^k \mid \omega \text{ primitive } n^{\text{th}} \text{ root of unity}\}$ ? No

# Even numbers

Sum type of natural numbers with proofs they are even:

$$E := \Sigma(n : \mathbb{N})(n \bmod 2 = 0).$$

Equality on even numbers:

let  $x = (m, p_m)$  and  $y = (n, p_n)$  be elements of  $E$ , then  $x = y$  if:

- $m = n$
- $p_m = p_n$

# Even numbers

Sum type of natural numbers with proofs they are even:

$$E := \Sigma(n : \mathbb{N})(n \bmod 2 = 0).$$

Equality on even numbers:

let  $x = (m, p_m)$  and  $y = (n, p_n)$  be elements of  $E$ , then  $x = y$  if:

- $m = n$
- $p_m = p_n$

Problems!

# Even numbers

Sum type of natural numbers with proofs they are even:

$$E := \Sigma(n : \mathbb{N})(n \bmod 2 = 0).$$

Equality on even numbers:

let  $x = (m, p_m)$  and  $y = (n, p_n)$  be elements of  $E$ , then  $x = y$  if:

- $m = n$
- $p_m = p_n$

## Problems!

- $p_m : (m \bmod 2 = 0)$  and  $p_n : (n \bmod 2 = 0)$  don't have the same type!

# Even numbers

Sum type of natural numbers with proofs they are even:

$$E := \Sigma(n : \mathbb{N})(n \bmod 2 = 0).$$

Equality on even numbers:

let  $x = (m, p_m)$  and  $y = (n, p_n)$  be elements of  $E$ , then  $x = y$  if:

- $m = n$
- $p_m = p_n$

## Problems!

- $p_m : (m \bmod 2 = 0)$  and  $p_n : (n \bmod 2 = 0)$  don't have the same type!
- Are  $p_m$  and  $p_n$  equal?



# Even numbers

Sum type of natural numbers with proofs they are even:

$$E := \Sigma(n : \mathbb{N})(n \bmod 2 = 0).$$

Equality on even numbers:

let  $x = (m, p_m)$  and  $y = (n, p_n)$  be elements of  $E$ , then  $x = y$  if:

- $m = n$
- $p_m = p_n$

## Problems!

- $p_m : (m \bmod 2 = 0)$  and  $p_n : (n \bmod 2 = 0)$  don't have the same type!
- Are  $p_m$  and  $p_n$  equal?

# UIP and Proof Irrelevance

Uniqueness of Identify Proofs axiom:

$$\forall (X : *) (a b : X) (p q : a = b), p = q$$

Proof Irrelevance axiom:

$$\forall (A : \text{Prop}) (p q : A), p = q$$

- What is Prop?
- Is the identity type in Prop?

# Axioms we have seen so far

- Functional extentionality

$$(\forall x, f\ x = g\ x) \rightarrow f = g$$

- Proof Irrelevance

$$\forall (A : \text{Prop})(p\ q : A), p = q$$

- Uniqueness of Identity Proofs

$$\forall (X : *) (a\ b : X)(p\ q : a = b), p = q$$

# Homotopy Type Theory

## Types as Spaces, Equalities as Paths.

- $HContr$  is the type of types that have exactly one element.
- types in  $HProp$  satisfy proof irrelevance

$$HProp := \Sigma(P : *) (\forall (p q : P), isHContr(p = q))$$

- types in  $HSet$  have uniqueness of identity proofs.

$$HSet := \Sigma(X : *) (\forall (a b : X), isHProp(a = b))$$

# The Univalence Axiom

The Univalence Axiom (V. Voevodsky) makes Type Theory behave well with regard to these new notions. In particular,

- Functional extensionality is derivable,
- $\mathbf{HProp}$  and  $\mathbf{HSet}$  are stable by product ( $A \rightarrow B$ ),
- equalities **are not** always propositions,
- equality is isomorphism (T. Coquand and N. A. Danielsson). E.g.:

$$\{0, 1\} = \{a, b\} \quad \text{when } a \neq b?$$

$$\mathbb{Z}/n\mathbb{Z} = \{\omega^k \mid \omega \text{ primitive } n^{\text{th}} \text{ root of unity}\},$$

• ...

Active research topic:

find a system in which univalence is not an axiom but a *program*.

# Other problems

If  $a : A$  and  $A = B$ , is  $a : B$ ?

True in Extensional Type Theory  
(don't confuse with functional extensionality),

but strange in Homotopy Type Theory:  
no unique way to see elements of  $A$  as elements of  $B$ .

# Other problems

If  $a : A$  and  $A = B$ , is  $a : B$ ?

If  $a : A$   $m$  and  $m = n$ , is  $a : A$   $n$ ?

True in Extensional Type Theory  
(don't confuse with functional extensionality),

but strange in Homotopy Type Theory:  
no unique way to see elements of  $A$  as elements of  $B$ .



Thank you for your attention.