Isomorphism is equality

Nils Anders Danielsson
Joint work with Thierry Coquand

IFIP WG 2.1 Meeting #73,
Lökeberg, 2015-08-25

The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013)/ERC grant agreement n° 247219. It has perhaps also received financial support from the Swedish Research Council, but I do not think that I am required to include a corresponding project number here. This presentation does not necessarily reflect the views of the ERC or the EU. The EU is not liable for any use of the presented information.

Introduction

In set theory

Isomorphic monoids can be provably distinct:

$$(\mathbb{N}, \lambda mn.\ m + n, 0)$$

$$(\mathbb{N} \setminus \{ 0 \}, \lambda mn.\ m + n - 1, 1)$$

Introduction

In Martin-Löf type theory

Isomorphic monoids are not provably distinct.

Introduction

In homotopy type theory

Isomorphic monoids are provably equal.

Introduction

In homotopy type theory

Isomorphic monoids are provably equal.

This talk:

- A more general theorem,
  which applies to a large class of
  algebraic structures.
- Two instantiations: monoids, posets.

Proof parameters (1)

A universe:

$$\begin{array}{lcl} U & : & Type \\ El & : & U \rightarrow Type \rightarrow Type \end{array}$$

Examples

For monoids and posets:

$$
\begin{array}{lll}
\textbf{data } U & : & Type \textbf{ where} \\
\quad \mathsf{id} & : & U \\
\quad \mathsf{type} & : & U \\
\quad \_\multimap\_ & : & U \to U \to U \\
\quad \_\otimes\_ & : & U \to U \to U
\end{array}
$$

Examples

For monoids and posets:

$$
\begin{array}{lll}
\textbf{data}\ U & : & \mathit{Type}\ \textbf{where} \\
\quad \mathsf{id} & : & U \\
\quad \mathsf{type} & : & U \\
\quad \_{\multimap}\_ & : & U \to U \to U \\
\quad \_{\otimes}\_ & : & U \to U \to U
\end{array}
$$

$$
\begin{array}{lll}
\mathit{El} : U \to & \mathit{Type} & \to \mathit{Type} \\
\mathit{El}\ \mathsf{id} & C & = C \\
\mathit{El}\ \mathsf{type} & C & = \mathit{Type} \\
\mathit{El}\ (a \multimap b) & C & = \mathit{El}\ a\ C \to \mathit{El}\ b\ C \\
\mathit{El}\ (a \otimes b) & C & = \mathit{El}\ a\ C \times \mathit{El}\ b\ C
\end{array}
$$

Examples

For monoids and posets:

$$
\begin{aligned}
&\textbf{data } U : \mathit{Type} \textbf{ where}\\
&\quad \mathsf{id} : U\\
&\quad \mathsf{type} : U\\
&\quad \_\rightarrowtriangle\_ : U \to U \to U\\
&\quad \_\otimes\_ : U \to U \to U
\end{aligned}
$$

$$
\begin{aligned}
&\mathit{monoid} : U\\
&\mathit{monoid} = (\mathsf{id} \rightarrowtriangle \mathsf{id} \rightarrowtriangle \mathsf{id}) \otimes \mathsf{id}
\end{aligned}
$$

Examples

For monoids and posets:

$$\begin{array}{lcl}
\textbf{data}\ U & : & \mathit{Type}\ \textbf{where} \\
\quad \mathsf{id} & : & U \\
\quad \mathsf{type} & : & U \\
\quad _\!\rightharpoonup\!_ & : & U \to U \to U \\
\quad _\!\otimes\!_ & : & U \to U \to U
\end{array}$$

$$\begin{array}{l}
\mathit{monoid}\ :\ U \\
\mathit{monoid}\ =\ (\mathsf{id} \rightharpoonup \mathsf{id} \rightharpoonup \mathsf{id}) \otimes \mathsf{id} \\
\mathit{El}\ \mathit{monoid}\ C \overset{\mathrm{def}}{=} (C \to C \to C) \times C
\end{array}$$

Examples

For monoids and posets:

$$\begin{aligned}
&\textbf{data}\ U\ :\ Type\ \textbf{where}\\
&\quad \mathsf{id}\quad :\ U\\
&\quad \mathsf{type}\ :\ U\\
&\quad _\multimap_\ :\ U \to U \to U\\
&\quad _\otimes_\ :\ U \to U \to U
\end{aligned}$$

$$\begin{aligned}
&poset\ :\ U\\
&poset\ =\ \mathsf{id} \multimap \mathsf{id} \multimap \mathsf{type}
\end{aligned}$$

Examples

For monoids and posets:

$$\begin{aligned}
&\textbf{data}\ U\ :\ \mathit{Type}\ \textbf{where}\\
&\quad \mathsf{id}\ :\ U\\
&\quad \mathsf{type}\ :\ U\\
&\quad _\!\rightharpoonup\!_\ :\ U \to U \to U\\
&\quad _\!\otimes\!_\ :\ U \to U \to U
\end{aligned}$$

$$\begin{aligned}
&\mathit{poset}\ :\ U\\
&\mathit{poset}\ =\ \mathsf{id} \rightharpoonup \mathsf{id} \rightharpoonup \mathsf{type}\\
&\mathit{El}\,\mathit{poset}\ C \stackrel{\text{def}}{=} C \to C \to \mathit{Type}
\end{aligned}$$

What about the properties?

Extended codes

$$
\begin{aligned}
&Code : Type \\
&Code = \\
&\quad \Sigma\, a : U. \\
&\quad (C : Type) \to El\; a\; C \to \\
&\quad\quad \Sigma\, P : Type.\; Is\text{-}proposition\; P
\end{aligned}
$$

Extended codes

$$
\begin{aligned}
&\mathit{Code} \;:\; \mathit{Type} \\
&\mathit{Code} \;= \\
&\quad \Sigma\, a \;:\; U. \\
&\quad (C \;:\; \mathit{Type}) \;\rightarrow\; \mathit{El}\; a\; C \;\rightarrow \\
&\qquad \Sigma\, P \;:\; \mathit{Type}.\ \mathit{Is\text{-}proposition}\; P
\end{aligned}
$$

$$
\mathit{Is\text{-}proposition}\; A \quad \Leftrightarrow \quad (x\; y \;:\; A) \;\rightarrow\; x \;\equiv\; y
$$

$$
\begin{aligned}
&\mathit{Is\text{-}set}\; A \quad \Leftrightarrow \\
&\quad (x\; y \;:\; A) \;\rightarrow\; \mathit{Is\text{-}proposition}\,(x \;\equiv\; y)
\end{aligned}
$$

Examples

$$
\begin{array}{l}
monoid\ :\ Code \\
monoid\ = \\
\quad ((\mathsf{id} \rightharpoonup \mathsf{id} \rightharpoonup \mathsf{id}) \otimes \mathsf{id} \\
\quad , \lambda\, C\, (\_\bullet\_, e). \\
\qquad (\ (\ (\forall\ x.\ e \bullet x\ \equiv\ x) \times \\
\qquad\qquad (\forall\ x.\ x \bullet e\ \equiv\ x) \times \\
\qquad\qquad (\forall\ x\ y\ z.\ x \bullet (y \bullet z)\ \equiv\ (x \bullet y) \bullet z) \times \\
\qquad\qquad \textit{Is-set}\ C \\
\qquad\quad) \\
\qquad , \ldots \\
\qquad) \\
\quad)
\end{array}
$$

Examples

$$
\begin{array}{l}
poset\ :\ Code \\
poset\ = \\
\quad (\textsf{id} \rightharpoonup \textsf{id} \rightharpoonup \textsf{type} \\
\quad ,\lambda\ C\ \_{\leqslant}\_. \\
\qquad (\ (\ \ (\forall\ x.\ x \leqslant x) \times \\
\qquad\qquad (\forall\ x\ y\ z.\ x \leqslant y\ \rightarrow\ y \leqslant z\ \rightarrow\ x \leqslant z) \times \\
\qquad\qquad (\forall\ x\ y.\ x \leqslant y\ \rightarrow\ y \leqslant x\ \rightarrow\ x\ \equiv\ y) \times \\
\qquad\qquad \textit{Is-set}\ C \times \\
\qquad\qquad (\forall\ x\ y.\ \textit{Is-proposition}\ (x \leqslant y)) \\
\qquad\quad) \\
\qquad ,\ ... \\
\qquad) \\
\quad)
\end{array}
$$

Instances

$$
\begin{aligned}
&\mathit{Code} \ : \ \mathit{Type} \\
&\mathit{Code} \ = \\
&\quad \Sigma\, a \ : \ U. \\
&\quad (C \ : \ \mathit{Type}) \ \to \ \mathit{El}\ a\ C \ \to \\
&\qquad \Sigma\, P \ : \ \mathit{Type}.\ \mathit{Is\text{-}proposition}\ P
\end{aligned}
$$

$$
\begin{aligned}
&\mathit{Instance} \ : \ \mathit{Code} \ \to \ \mathit{Type} \\
&\mathit{Instance}\,(a, P) \ = \\
&\quad \Sigma\, C \ : \ \mathit{Type}. \\
&\quad \Sigma\, x \ : \ \mathit{El}\ a\ C. \\
&\quad \mathit{fst}\,(P\ C\ x)
\end{aligned}
$$

Examples

$$
\begin{aligned}
&\mathit{Instance\ monoid} \stackrel{\text{def}}{=} \\
&\quad \Sigma\, C \ :\ \mathit{Type}. \\
&\quad \Sigma\, (\_\bullet\_, e) \ :\ (C \ \rightarrow\ C \ \rightarrow\ C) \times C. \\
&\quad (\forall\ x.\ e \bullet x \ \equiv\ x) \times \\
&\quad (\forall\ x.\ x \bullet e \ \equiv\ x) \times \\
&\quad (\forall\ x\ y\ z.\ x \bullet (y \bullet z) \ \equiv\ (x \bullet y) \bullet z) \times \\
&\quad \mathit{Is\text{-}set}\ C
\end{aligned}
$$

Examples

$$
\begin{aligned}
&\mathit{Instance\ poset} \stackrel{\text{def}}{=} \\
&\quad \Sigma\, C \;:\; \mathit{Type}. \\
&\quad \Sigma\, \_\leqslant\_ \;:\; C \;\rightarrow\; C \;\rightarrow\; \mathit{Type}. \\
&\quad (\forall\, x.\; x \leqslant x) \times \\
&\quad (\forall\, x\; y\; z.\; x \leqslant y \;\rightarrow\; y \leqslant z \;\rightarrow\; x \leqslant z) \times \\
&\quad (\forall\, x\; y.\; x \leqslant y \;\rightarrow\; y \leqslant x \;\rightarrow\; x \;\equiv\; y) \times \\
&\quad \mathit{Is\text{-}set}\; C \times \\
&\quad (\forall\, x\; y.\; \mathit{Is\text{-}proposition}\; (x \leqslant y))
\end{aligned}
$$

How is “isomorphism” defined?

Equivalence

Equivalence:

$$\_\simeq\_ \ : \ Type \ \to \ Type \ \to \ Type$$

$A \ \simeq \ B$ is logically equivalent to
"A is in bijective correspondence with B".

$$id \ : \ A \ \simeq \ A$$

Proof parameters (2)

$$\begin{aligned} resp \quad &: \forall\, a.\; B \;\simeq\; C \;\rightarrow\; El\; a\; B \;\rightarrow\; El\; a\; C \\ resp\text{-}id \;&: \forall\, a.\; (x \;:\; El\; a\; B) \;\rightarrow\; resp\; a\; id\; x \;\equiv\; x \end{aligned}$$

Examples

$$cast\ :\forall\ a.\ B\ \Leftrightarrow\ C\ \rightarrow\ El\ a\ B\ \Leftrightarrow\ El\ a\ C$$

Isomorphisms

$$
\begin{aligned}
&Isomorphic\ :\\
&\quad \forall\ c.\ Instance\ c\ \rightarrow\ Instance\ c\ \rightarrow\ Type\\
&Isomorphic\,(a, \_)\ (C, x, \_)\ (D, y, \_)\ =\\
&\quad \Sigma\ eq\ :\ C\ \simeq\ D.\ resp\ a\ eq\ x\ \equiv\ y
\end{aligned}
$$

Examples

Monoids are isomorphic if there is a homomorphic equivalence between their carrier types:

$$
\begin{aligned}
&\mathit{Isomorphic\ monoid}\ (C_1, (\_\bullet_1\_, e_1), \mathit{laws}_1) \\
&\qquad\qquad\qquad\qquad\qquad (C_2, (\_\bullet_2\_, e_2), \mathit{laws}_2) \ \stackrel{\text{def}}{=} \\
&\quad \Sigma\ eq\ :\ C_1\ \simeq\ C_2. \\
&\qquad (\ \ (\lambda\ (x\ y\ :\ C_2).\ \mathit{to}\ eq\ (\mathit{from}\ eq\ x \bullet_1 \mathit{from}\ eq\ y)) \\
&\qquad ,\ \ \mathit{to}\ eq\ e_1 \\
&\qquad) \\
&\qquad\quad \equiv \\
&\qquad (\_\bullet_2\_, e_2)
\end{aligned}
$$

Examples

For posets we get something which is provably equivalent to order isomorphism:

$$
\begin{array}{l}
\textit{Isomorphic poset}\,(C_1, \_\leqslant_1\_, \textit{laws}_1) \\
\qquad\qquad\qquad\qquad (C_2, \_\leqslant_2\_, \textit{laws}_2) \stackrel{\text{def}}{=} \\
\quad \Sigma\, eq : C_1 \simeq C_2. \\
\qquad (\lambda\, (a\; b : C_2).\ \textit{from eq}\ a \leqslant_1 \textit{from eq}\ b) \\
\qquad\quad \equiv \\
\qquad \_\leqslant_2\_
\end{array}
$$

The main theorem

The main theorem

- Parameters: U, El, $resp$, $resp\text{-}id$.
- The theorem:

$$\begin{aligned}&\forall\ c.\ (X\ Y\ :\ Instance\ c)\ \rightarrow\\&\quad Isomorphic\ c\ X\ Y\ \equiv\ (X\ \equiv\ Y)\end{aligned}$$

- Provable using univalence and "equivalence reasoning".

Substitutivity

Equality is substitutive:

$$\_*\_ : x \equiv y \to P\,x \to P\,y$$

Lemma

$$\forall\ c.\ ((C, x, p)\ (D, y, q)\ :\ Instance\ c)\ \to$$
$$((C, x, p)\ \equiv\ (D, y, q))$$
$$\simeq$$
$$\Sigma\ eq\ :\ C\ \equiv\ D.\ eq\ _*\ x\ \equiv\ y$$

Lemma

$$\forall\ c.\ ((C, x, p)\ (D, y, q)\ :\ Instance\ c)\ \rightarrow$$

$$((C, x, p)\ \equiv\ (D, y, q))$$

$$\simeq$$

$$\Sigma\ eq\ :\ C\ \equiv\ D.\ eq\ {}_{*}\ x\ \equiv\ y$$

$$(C, x, p)\quad \equiv\ (D, y, q)\qquad\qquad \simeq$$

Lemma

$$\forall\ c.\ (((C, x, p)\ (D, y, q)\ :\ Instance\ c)\ \rightarrow$$

$$((C, x, p)\ \equiv\ (D, y, q))$$

$$\simeq$$

$$\Sigma\ eq\ :\ C\ \equiv\ D.\ eq\ _{*}\ x\ \equiv\ y$$

$$(C, x, p)\quad \equiv\ (D, y, q)\qquad \simeq$$

$$((C, x), p)\ \equiv\ ((D, y), q)\qquad \simeq$$

Lemma

$$\forall\ c.\ ((C, x, p)\ (D, y, q)\ :\ \mathit{Instance}\ c)\ \rightarrow$$
$$((C, x, p)\ \equiv\ (D, y, q))$$
$$\simeq$$
$$\Sigma\ eq\ :\ C\ \equiv\ D.\ eq\ _*\ x\ \equiv\ y$$

$$\begin{array}{lcll}
(C, x, p) & \equiv & (D, y, q) & \simeq \\
((C, x), p) & \equiv & ((D, y), q) & \simeq \\
(C, x) & \equiv & (D, y) & \simeq
\end{array}$$

Lemma

$$\forall\ c.\ ((C, x, p)\ (D, y, q)\ :\ Instance\ c)\ \rightarrow$$

$$((C, x, p)\ \equiv\ (D, y, q))$$

$$\simeq$$

$$\Sigma\ eq\ :\ C\ \equiv\ D.\ eq\ {}_{*}\ x\ \equiv\ y$$

$$\begin{array}{lcll}
(C, x, p) & \equiv & (D, y, q) & \simeq \\
((C, x), p) & \equiv & ((D, y), q) & \simeq \\
(C, x) & \equiv & (D, y) & \simeq \\
\multicolumn{4}{l}{\Sigma\ eq\ :\ C\ \equiv\ D.\ eq\ {}_{*}\ x\ \equiv\ y}
\end{array}$$

The univalence axiom

The function

$$\lambda\, eq.\ eq_*\, id : A \equiv B \to A \simeq B$$

is the forward component of an equivalence.

The inverse:

$$eq\text{-}to\text{-}eq : A \simeq B \to A \equiv B$$

The transport theorem

Follows from the univalence axiom:

$$(\mathit{resp} : \forall\ A\ B.\ A \simeq B \to P\ A \to P\ B) \to$$
$$(\mathit{resp}\text{-}\mathit{id} : \forall\ A\ p.\ \mathit{resp}\ A\ A\ \mathit{id}\ p \equiv p) \to$$
$$\forall\ \mathit{eq}\ p.\ \mathit{resp}\ A\ B\ \mathit{eq}\ p \equiv \mathit{eq}\text{-}\mathit{to}\text{-}\mathit{eq}\ \mathit{eq}\ {}_*\ p$$

Proof of the main theorem

$$Isomorphic\ c\ (C, x, p)\ (D, y, q) \qquad \equiv$$

$$(C, x, p)\ \equiv\ (D, y, q)$$

Proof of the main theorem

$$Isomorphic\ c\ (C, x, p)\ (D, y, q) \qquad \simeq$$

$$(C, x, p) \equiv (D, y, q)$$

Proof of the main theorem

$$
\begin{aligned}
&\mathit{Isomorphic}\ c\ (C, x, p)\ (D, y, q) && \simeq \\
&\Sigma\, eq\ :\ C\ \simeq\ D.\ \mathit{resp}\ a\ eq\ x\ \equiv\ y && \simeq
\end{aligned}
$$

$$(C, x, p)\ \equiv\ (D, y, q)$$

Proof of the main theorem

$$
\begin{aligned}
&Isomorphic\ c\ (C, x, p)\ (D, y, q) && \simeq \\
&\Sigma\, eq\ :\ C\ \simeq\ D.\ resp\ a\ eq\ x\ \equiv\ y && \simeq \\
\\
&\Sigma\, eq\ :\ C\ \equiv\ D.\ eq\ _{*}\ x\ \equiv\ y && \simeq \\
&(C, x, p)\ \equiv\ (D, y, q)
\end{aligned}
$$

Proof of the main theorem

$$
\begin{aligned}
&\mathit{Isomorphic}\ c\ (C, x, p)\ (D, y, q) && \simeq \\
&\Sigma\, eq : C \simeq D.\ \mathit{resp}\ a\ eq\ x \equiv y && \simeq \\
&\Sigma\, eq : C \simeq D.\ (\mathit{eq\text{-}to\text{-}eq}\ eq_{\ast}\ x) \equiv y && \simeq \\
&\Sigma\, eq : C \equiv D.\ eq_{\ast}\ x \equiv y && \simeq \\
&(C, x, p) \equiv (D, y, q)
\end{aligned}
$$

Discussion

- Related ideas were published already in the 1930s (Lindenbaum and Tarski).
- Isomorphism is equality,
  for a large class of structures,
  in homotopy type theory.
- More abstract:
  Aczel's structure identity principle.