Homotopy Type Theory and Hedberg's Theorem

Nicolai Kraus

16/11/12

Reminder: Type Theory

Intensional Type Theory

Reminder: Type Theory

Intensional Type Theory

a formal system

Reminder: Type Theory

Intensional Type Theory

a formal system

…and a possible foundation of (constructive) mathematics

Reminder: Type Theory

Intensional Type Theory

a formal system

...and a possible foundation of (constructive) mathematics

...for proof assistants and (dependently typed) programming

Reminder: Type Theory

Intensional Type Theory

a formal system

. . . and a possible foundation of (constructive) mathematics

. . . for proof assistants and (dependently typed) programming

. . . as used for Coq and Agda

Reminder: Type Theory

Intensional Type Theory

a formal system

. . . and a possible foundation of (constructive) mathematics

. . . for proof assistants and (dependently typed) programming

. . . as used for Coq and Agda

e.g.

$$\lambda f \;\rightarrow\; \lambda a \;\rightarrow\; f\; a\; a \;:\; (A \rightarrow A \rightarrow B) \rightarrow A \rightarrow B$$

Reminder: Equality

Definitional Equality

Decidable equality for typechecking & computation; e. g.

$$(\lambda a.b)x =_\beta b[x/a]$$

Reminder: Equality

Definitional Equality

Decidable equality for typechecking & computation; e. g.

$$(\lambda a.b)x =_\beta b[x/a]$$

Propositional Equality

Equality needing a proof, i. e. a term of the identity type

Reminder: Identity Types

Propositional equality

…is just an inductive type

Reminder: Identity Types

Propositional equality

... is just an inductive type

Formation

$$\frac{a, b \; : \; A}{a \equiv b \; : \; \mathit{type}}$$

Reminder: Identity Types

Propositional equality

... is just an inductive type

Formation

$$\frac{a, b \; : \; A}{a \equiv b \; : \; type}$$

Introduction

$$\frac{a \; : \; A}{refl_a \; : \; a \equiv a}$$

Reminder: Identity Types

Propositional equality

. . . is just an inductive type

Formation

$$\frac{a, b \;:\; A}{a \equiv b \;:\; \mathit{type}}$$

Introduction

$$\frac{a \;:\; A}{\mathit{refl}_a \;:\; a \equiv a}$$

Elimination (J)

$$\frac{\begin{array}{c} P \;:\; (a, b : A) \to a \equiv b \to \mathit{Set} \\ m : \forall a. P(a, a, \mathit{refl}_a) \end{array}}{J_{(a,b,q)} \;:\; P(a, b, q)}$$

Reminder: Identity Types

Propositional equality

... is just an inductive type

Formation

$$\frac{a, b \;:\; A}{a \equiv b \;:\; type}$$

Introduction

$$\frac{a \;:\; A}{refl_a \;:\; a \equiv a}$$

Elimination (J)

$$\frac{\begin{array}{c} P \;:\; (a, b : A) \to a \equiv b \to Set \\ m : \forall a. P(a, a, refl_a) \end{array}}{J_{(a,b,q)} \;:\; P(a, b, q)}$$

Computation (β)

$$J_{(a,a,refl_a)} =_\beta ma$$

Uniqueness of Identity Proofs (UIP)

Given $a : A$ and $p : a \equiv a$, can we prove $p \equiv \mathit{refl}_a$?

Uniqueness of Identity Proofs (UIP)

Given $a : A$ and $p : a \equiv a$, can we prove $p \equiv refl_a$?

Axiom UIP

$$\frac{p,\ q\ :\ a \equiv b}{uip\ :\ \ p \equiv q}$$

Uniqueness of Identity Proofs (UIP)

Given $a : A$ and $p : a \equiv a$, can we prove $p \equiv refl_a$?

Axiom UIP

$$\frac{p,\ q\ :\ a \equiv b}{uip\ :\ p \equiv q}$$

Advantages

Simple,
Good computational properties

Uniqueness of Identity Proofs (UIP)

Given $a : A$ and $p : a \equiv a$, can we prove $p \equiv refl_a$?

Axiom UIP

$$\frac{p,\ q\ :\ a \equiv b}{uip\ :\ p \equiv q}$$

Advantages

Simple,
Good computational properties

Disadvantages

Intuitively wrong,
impossible to express statements about equality,
isomorphic sets cannot be equal

Homotopic Model - technical details

Voevodsky (and Awodey, independently, and others):

Without UIP: new model of Type Theory

(types as weak ω-groupoids)

Homotopic Model - technical details

Voevodsky (and Awodey, independently, and others):

Without UIP: new model of Type Theory

(types as weak ω-groupoids)

- best expressible in Simplicial Sets *SSets* (the topos $Sets^{\Delta^{op}}$)

Homotopic Model - technical details

Voevodsky (and Awodey, independently, and others):

Without UIP: new model of Type Theory

(types as weak ω-groupoids)

- best expressible in Simplicial Sets *SSets* (the topos $Sets^{\Delta^{op}}$)
- realization functor $R: SSets \to Top$

Homotopic Model - technical details

Voevodsky (and Awodey, independently, and others):

Without UIP: new model of Type Theory

(types as weak ω-groupoids)

- best expressible in Simplicial Sets *SSets* (the topos $Sets^{\Delta^{op}}$)
- realization functor $R : SSets \to Top$
- R is a *Quillen equivalence* of model categories

Homotopic Model - technical details

Voevodsky (and Awodey, independently, and others):

Without UIP: new model of Type Theory

(types as weak ω-groupoids)

- best expressible in Simplicial Sets *SSets* (the topos $Sets^{\Delta^{op}}$)
- realization functor $R : SSets \to Top$
- R is a *Quillen equivalence* of model categories
- $\Rightarrow$ (more or less) a model that uses topological spaces as types

Hedberg's theorem

Fix a type A.

Decidable Equality

$$\mathit{DecidableEquality} \; := \; \forall\, a\, b \; \rightarrow (a \equiv b \; + \; \neg\, a \equiv b)$$

Hedberg's theorem

$$\mathit{DecidableEquality} \; \longrightarrow \; \mathit{UIP}$$

Hedberg's theorem

Constant Function

$$const(f) \;:=\; \forall\, a\, b \;\rightarrow\; f\, a \equiv f\, b$$

Constant Endofunction on Path Spaces

$$g \;:\; \forall\, a\, b \;\rightarrow\; a \equiv b \;\rightarrow\; a \equiv b$$
$$path\text{-}const(g) \;:=\; \forall\, a\, b \;\rightarrow\; const\, g_{ab}$$

Hedberg's theorem

Lemma 1

$$\mathit{DecidableEquality} \longrightarrow \Sigma_g \,.\, \mathit{path\text{-}const}(g)$$

Hedberg's theorem

Lemma 1

$DecidableEquality \longrightarrow \Sigma_g\,.\,path\text{-}const(g)$

Proof.

- Given $dec : \forall\, a\, b \rightarrow (a \equiv b\ +\ \neg\, a \equiv b)$.

Hedberg's theorem

Lemma 1

$$\mathit{DecidableEquality} \longrightarrow \Sigma_g \,.\, \mathit{path\text{-}const}(g)$$

Proof.

- Given $dec : \forall\, a\, b \to (a \equiv b + \neg\, a \equiv b)$.
- Given a, b, we want: $g_{ab} : a \equiv b \to a \equiv b$.

Hedberg's theorem

Lemma 1

$$DecidableEquality \longrightarrow \Sigma_g \,.\, path\text{-}const(g)$$

Proof.

- Given $dec : \forall\, a\, b \rightarrow (a \equiv b + \neg\, a \equiv b)$.
- Given a, b, we want: $g_{ab} : a \equiv b \rightarrow a \equiv b$.
- If $dec\, a\, b = inr\ \_$, then nothing to do

Hedberg's theorem

Lemma 1

$$\mathit{DecidableEquality} \longrightarrow \Sigma_g \,.\, \mathit{path\text{-}const}(g)$$

Proof.

- Given $dec : \forall\, a\, b \to (a \equiv b + \neg\, a \equiv b)$.
- Given a, b, we want: $g_{ab} : a \equiv b \to a \equiv b$.
- If $dec\, a\, b = inr\ \_$, then nothing to do
- If $dec\, a\, b = inl\, p$, then $g_{ab}(\_) = p$ $\square$

Hedberg's theorem

Lemma 2

$$\Sigma_g \,.\, \textit{path-const}(g) \;\longrightarrow\; \textit{UIP}$$

Hedberg's theorem

Lemma 2

$$\Sigma_g \,.\, \mathit{path\text{-}const}(g) \;\longrightarrow\; \mathit{UIP}$$

Proof.

- Given $g \;:\; \forall\, a\, b \;\rightarrow\; a \equiv b \;\rightarrow\; a \equiv b$ which is constant

Hedberg's theorem

Lemma 2

$$\Sigma_g \,.\, \mathit{path\text{-}const}(g) \longrightarrow \mathit{UIP}$$

Proof.

- Given $g : \forall\, a\, b \to a \equiv b \to a \equiv b$ which is constant
- Given any $a, b : A$ and $p, q : a \equiv b$.

Hedberg's theorem

Lemma 2

$$\Sigma_g \, . \, path\text{-}const(g) \;\longrightarrow\; UIP$$

Proof.

- Given $g \,:\, \forall\, a\, b \,\to\, a \equiv b \,\to\, a \equiv b$ which is constant
- Given any $a, b \,:\, A$ and $p, q : \, a \equiv b$.
- Claim: $p \equiv (g_{aa} refl_a)^{-1} \circ g_{ab}(p)$

Hedberg's theorem

Lemma 2

$$\Sigma_g \,.\, \mathit{path\text{-}const}(g) \longrightarrow \mathit{UIP}$$

Proof.

- Given $g : \forall\, a\, b \to a \equiv b \to a \equiv b$ which is constant
- Given any $a, b : A$ and $p, q : a \equiv b$.
- Claim: $p \equiv (g_{aa} \mathit{refl}_a)^{-1} \circ g_{ab}(p)$
- Proof with J: Just do it for (a, a, refl_a). That's true!

Hedberg's theorem

Lemma 2

$$\Sigma_g\,.\,path\text{-}const(g) \longrightarrow UIP$$

Proof.

- Given $g : \forall\, a\, b \to a \equiv b \to a \equiv b$ which is constant
- Given any $a, b : A$ and $p, q : a \equiv b$.
- Claim: $p \equiv (g_{aa} refl_a)^{-1} \circ g_{ab}(p)$
- Proof with J: Just do it for $(a, a, refl_a)$. That's true!
- Same for q. But g_{aa} and g_{ab} are constant. $\square$

Generalizations of Hedberg's theorem

We have seen

Lemma 1

$$\mathit{DecidableEquality} \longrightarrow \Sigma_g\,.\,\mathit{path\text{-}const}(g)$$

DecidableEquality is a very strong property. How about something weaker?

Generalizations of Hedberg's theorem

We have seen

Lemma 1

$$\mathit{DecidableEquality} \longrightarrow \Sigma_g \,.\, \mathit{path\text{-}const}(g)$$

DecidableEquality is a very strong property. How about something weaker? For example:

Separated

$$\forall\, a\, b \;\rightarrow\; \neg\neg(a \equiv b) \;\rightarrow\; a \equiv b$$

"general"

$$\forall\, a\, b \;\rightarrow\; \textit{[propositional evidence for } a \equiv b\textit{]} \;\rightarrow\; a \equiv b$$

Propositions

So, what is “propositional evidence”?

Propositions

So, what is "propositional evidence"?

Type A is a Proposition if

$$prop_A = \forall\, a\, b \to a \equiv b$$

"at most one inhabitant"

Propositions

So, what is "propositional evidence"?

Type A is a Proposition if

$$prop_A = \forall\, a\, b \rightarrow\; a \equiv b$$

"at most one inhabitant"

Write **Prop** for this "subset" of **Type**

H-Propositional Reflection

A some type. We want a way to say that A is inhabited without giving away a specific inhabitant.

H-Propositional Reflection

A some type. We want a way to say that A is inhabited without giving away a specific inhabitant.

H-propositional reflection

$$* \ : \ \mathbf{Type} \to \mathbf{Prop}$$

is defined to be the left adjoint of *emb:* $\mathbf{Prop} \hookrightarrow \mathbf{Type}$

H-Propositional Reflection

A some type. We want a way to say that A is inhabited without giving away a specific inhabitant.

H-propositional reflection

$$^* \;:\; \mathbf{Type} \to \mathbf{Prop}$$

is defined to be the left adjoint of *emb:* $\mathbf{Prop} \hookrightarrow \mathbf{Type}$

This means:

- A^* is in **Prop**
- $\eta : A \to A^*$
- if P is a proposition and $A \to P$, then $A^* \to P$

Generalizations of Hedberg's Theorem

"Propositional evidence for $a \equiv b$" is now just [an inhabitant of] $(a \equiv b)^*$.

H-Separated

$$\forall\, a\, b \;\rightarrow\; (a \equiv b)^* \;\rightarrow\; a \equiv b$$

Generalizations of Hedberg's Theorem

"Propositional evidence for $a \equiv b$" is now just [an inhabitant of] $(a \equiv b)^*$.

H-Separated

$$\forall\, a\, b \;\rightarrow\; (a \equiv b)^* \;\rightarrow\; a \equiv b$$

Theorem

$$\textit{h-separated}_A \longleftrightarrow \Sigma_g \,.\, \textit{path-const}(g) \longleftrightarrow \textit{UIP}_A$$

Nearly uncountable many things to be done . . .

- Higher Inductive Types (see Mike Shulman's work)
- Model construction with modern abstract (not point-set) homotopy theory
- Constructive Simplicial Sets (the combinatorial version of what I have shown; see Thierry Coquand's / Simon Huber's work)
- Univalent foundations / Univalence ("alternative" to K) in general (see Voevodsky)
- . . . and possible computational properties (Thorsten?)

THANK YOU!