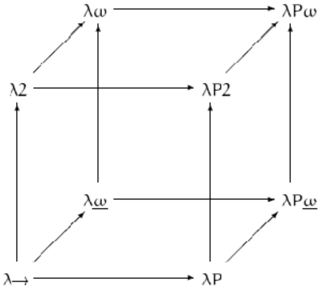
Set-theoretical Intuitionistic Proof-irrelevance Model of CIC^-

Masahiro Sato

May 26, 2014

CIC

- CIC is type system of ‘Coq’
  - Coq is one of the theorem prover
- CIC is a extention of CC($\lambda P\omega$)
  - CC is the strongest type system in λ-Cube
  - CIC $=$ CC $+ \mathrm{Type}_i +$ (Co)Inductive-Type
  - CIC$^-$ $=$ CC $+ \mathrm{Type}_i$



A semantics of type system

	$t : T$	$f : A \to B$	$f : \forall x : A.B$
Set theory	t is a element of Set(Class?) T	f is a function from A to B	f is a function which maps a into some element of $B(a)$
Programming	t is a variable whose type is T	f is a function(method) which returns type B with A type argument	f is a dependent type function(method)
Proof theory	t is a proof of a proposition T	f is a proof of a proposition $A \Rightarrow B$	f is a proof of a Proposition $\forall x \in A, B(x)$

Examples of Model of Type Theory

- Set Theory
- Partial Equivalence Relation
- Topological Space
- Coherence Space
- Presheaf

Definition of Term and Context

Definition (Term)

- Type_i is a term $(i = 0, 1, 2, 3, 4, ...)$.
- Prop is a term.
- x is a term for $x \in V$.
- If t_1 and t_2 is a terms, then $t_1 t_2$ is a term.
- If t and T is a term, and $x \in V$ then, $\lambda x : T.t$ is a term.
- If T_1 and T_2 is a term, and $x \in V$ then $\forall x : T_1.T_2$ is a term.
  - If x dosn't freely appear in B, $\forall x : A.B$ is denoted as $A \to B$.

Definition (Context)

- $[]$ is Context.
- If Γ is Context, T is a term and $x \in V$, then $\Gamma; (x : T)$ is Context.

Typing-Rule1

$$\Gamma \vdash \text{Prop} : \text{Type}_i \qquad \Gamma \vdash \text{Type}_i : \text{Type}_{i+1}$$

$$\frac{\Gamma \vdash A : \text{Prop}}{\Gamma \vdash A : \text{Type}_i} \qquad \frac{\Gamma \vdash A : \text{Type}_i}{\Gamma \vdash A : \text{Type}_{i+1}}$$

$$\frac{\Gamma \vdash A : \text{Type}_i \quad \Gamma ; (x : A) \vdash B : \text{Type}_j}{\Gamma \vdash \forall x : A.B : \text{Type}_{\max(i,j)}} \qquad \frac{\Gamma \vdash A : \text{Prop} \quad \Gamma ; (x : A) \vdash B : \text{Type}_j}{\Gamma \vdash \forall x : A.B.\text{Type}_j}$$

$$\frac{\Gamma \vdash A : \text{Type}_i \quad \Gamma ; (x : A) \vdash Q : \text{Prop}}{\Gamma \vdash \forall x : A.Q : \text{Prop}} \qquad \frac{\Gamma \vdash P : \text{Prop} \quad \Gamma ; (x : A) \vdash Q : \text{Prop}}{\Gamma \vdash \forall x : P.Q : \text{Prop}}$$

Typing-Rule2

$$\frac{\Gamma; (x : A) \vdash t : B \quad \Gamma \vdash \forall x : A.B : \mathrm{Type_i}}{\Gamma \vdash \lambda x : A.t : \forall x : A.B}$$

$$\frac{\Gamma; (x : A) \vdash t : B \quad \Gamma \vdash \forall x : A.B : \mathrm{Prop}}{\Gamma \vdash \lambda x : A.t : \forall x : A.B}$$

$$\frac{\Gamma \vdash u : \forall x : A.B \quad \Gamma \vdash v : A}{\Gamma \vdash (uv) : B[x \backslash v]}$$

$$\frac{(x : A) \in \Gamma \quad \Gamma \vdash A : \mathrm{Type}_i}{\Gamma \vdash x : A}$$

$$\frac{(x : A) \in \Gamma \quad \Gamma \vdash A : \mathrm{Prop}}{\Gamma \vdash x : A}$$

$$\frac{\Gamma \vdash x : A \quad A =_\beta B}{\Gamma \vdash x : B}$$

Merit of “Prop”

- “Prop” enables to represent of higher order logic
  - The type of “Predicate on Type 'A”' is $A \to \mathrm{Prop}$
  - $\forall P : A \to \mathrm{Prop}, Q(P) : \mathrm{Prop}$
- “Prop” represent other logical symbol as following:
  - $\bot := \forall P : \mathrm{Prop}.P$
  - $\neg A := A \to \bot$
  - $\exists x : A.B := \forall P : \mathrm{Prop}.(\forall x : A, (B(x) \to P)) \to P$
  - $A \land B := \forall P : \mathrm{Prop}.(A \to B \to P) \to P$
  - $A \lor B := \forall P : \mathrm{Prop}.(A \to P) \to (B \to P) \to P$
  - $A \leftrightarrow B := A \to B \land B \to A$
  - $x =_A y := \forall P : \mathrm{Prop}, Px \leftrightarrow Py$

Definition (Propositional Term and Proof Term)

The term P is called Propositional term in Γ iff $\Gamma \vdash P : \mathrm{Prop}$ is derivable. And more, The term t is called Proof term in Γ iff $\Gamma \vdash t : P$ is derivable for some P which is Propositional term in Γ.

Definition (Provable Propositional term)

Let P be Propositional term in Γ. P is called Provable Propositional term if there exists therm t such that $\Gamma \vdash t : P$ is derivable.

Idea of Model

- Soundness of CIC$^-$ is showed by B.Werner.
- He shows following theorem in his paper “Sets in Types, Types in Sets”

Theorem (Soundness)

- *If* $\Gamma \vdash t : T$ *is derivable, then* $[\![\Gamma \vdash t]\!](\gamma) \in [\![\Gamma \vdash T]\!](\gamma)$ *for all* $\gamma \in [\![\Gamma]\!]$
- *If* $\Gamma \vdash t_1 : T$ *and* $t_1 \to_\beta t_2$*, then* $[\![\Gamma \vdash t_1]\!](\gamma) = [\![\Gamma \vdash t_2]\!](\gamma)$ *for all* $\gamma \in [\![\Gamma]\!]$

Where $[\![\Gamma \vdash T]\!]$ *is a function whose domain is* $[\![\Gamma]\!]$

Preparation(Dependent Function)

Definition (Dependent Function)

Let A be a set, and $B(a)$ is a set with parameter $a \in A$.

$$\begin{aligned}
\bigotimes_{a \in A} B(a) &:= \{p \in A \times \bigcup_{a \in A} B(a) \mid \forall a, b, (a, b) \in p \Rightarrow b \in B(a)\} \\
\prod_{a \in A} B(a) &:= \{f \subset \bigotimes_{a \in A} B(a) \mid \forall a \in A, \exists! b \in B(a), (a, b) \in f\}
\end{aligned}$$

Dependent Function is a function with range $B(a)$ with a parameter $a \in A$, i.e.

$$f \in \prod_{a \in A} B(a) \Rightarrow \forall a \in A, f(a) \in B(a)$$

Preparation(Universe)

Definition (Universe)

Let $\mathcal{U}(i)$ be i-th Grothendieck Universe, i.e.

- $\mathcal{U}(i)$ is Grothendieck Universe for each i
- $\mathcal{U}(i) \in \mathcal{U}(i+1)$ for each i

Lemma

$A \in \mathcal{U}(i)$ and $B(a) \in \mathcal{U}(i)$ for each $a \in A$ imply $\prod_{a \in A} B(a) \in \mathcal{U}(i)$.

Interpretation(Context)

Definition (Interpretation of Judgement)

- $[\![[]]\!] := ()$
- $[\![\Gamma; (x : A)]\!] := \{(\gamma, \alpha) | \alpha \in [\![\Gamma \vdash A]\!](\gamma)\}$

Interpretation(Judgement)

Definition (Interpretation of Judgement)

- $[\![\Gamma \vdash t]\!](\gamma) := 0 \quad$ (If t is Proof term in Γ)
- $[\![\Gamma \vdash \mathrm{Type}_i]\!](\gamma) := \mathcal{U}(i)$
- $[\![\Gamma \vdash \mathrm{Prop}]\!](\gamma) := \{0, 1\} = \{\phi, \{\phi\}\}$
- $[\![\Gamma \vdash \lambda x : A.T]\!](\gamma) := \{\big(\alpha, [\![\Gamma; (x : A) \vdash T]\!](\gamma, \alpha)\big) | \alpha \in [\![\Gamma \vdash A]\!](\gamma)\}$
- $[\![\Gamma \vdash t_1 t_2]\!](\gamma) := [\![\Gamma \vdash t_1]\!](\gamma)\big([\![\Gamma \vdash t_2]\!](\gamma)\big)$
- $[\![\Gamma \vdash x_i]\!](\gamma) := \gamma_i$
- $[\![\Gamma \vdash \forall x : A.B]\!](\gamma)$
  - $:= [\![\Gamma; (x : A) \vdash B]\!](\gamma, 0)^{[\![\Gamma \vdash A]\!](\gamma)}$
    (when A, B are both Propositional term)
  - $:= \min\{ \ [\![\Gamma; (x : A) \vdash B]\!](\alpha, \gamma) \mid \alpha \in [\![\Gamma \vdash A]\!](\gamma) \ \}$
    (when B is Propositional term)
  - $:= \prod_{[\![\alpha \in \Gamma \vdash A]\!](\gamma)} [\![\Gamma; (x : A) \vdash B]\!](\gamma, \alpha)$
    (Otherwise)

idea

- Above model is 'Classical Model'
  - In this model, PEM is true
    - $[\![\Gamma \vdash \forall P : \mathrm{Prop}, P \vee P]\!](\gamma) = 1$
  - Can we create the model which is PEM is NOT true?
- Expand the interpretation of Prop from $\{0, 1\}$ into general topological space.

Notation of topological space

Let $(X, \mathcal{O}(X))$ be a topological space.

- $\mathbb{I} := X$
- $\mathbb{O} := \phi$
- $\bigsqcup S := \bigcup S$
- $\bigsqcap S := \bigsqcup \{t \mid \forall s \in S, t \subset s\} = \left(\bigcap S\right)^\circ$
- $b^a := \bigsqcup \{t \mid t \sqcap a \leq b\}$

Point condition

Let p be a point of X such that following condition holds.

$$\bigcap \mathcal{N}(p) \ is\ open\ set. \tag{1}$$

where $\mathcal{N}(p)$ is open neighborhood, i.e.

$$\mathcal{N}(p) := \{O \in \mathcal{O}(X) | p \in O\}$$

We will consider the model with parameter $p(\in X)$ satisfying above condition.

Interpretation(Context)

Definition (Strict Interpretation of Judgement)

$$[\![\Gamma \vdash A]\!]'(\gamma) := \begin{cases} [\![\Gamma \vdash A]\!](\gamma) \cap \{p\} & (A\ is\ Propositional\ Term) \\ [\![\Gamma \vdash A]\!](\gamma) & (otherwise) \end{cases}$$

Definition (Interpretation of Context)

- $[\![[]]\!] := ()$
- $[\![\Gamma; (x : A)]\!] := \{(\gamma, \alpha) | \alpha \in [\![\Gamma \vdash A]\!]'(\gamma)\}$

Interpretation(Judgement)

Definition (Interpretation of Judgement)

- $[\![\Gamma \vdash t]\!](\gamma) := p$ (If t is Proof term in Γ)
- $[\![\Gamma \vdash \mathrm{Type}_i]\!](\gamma) := \mathcal{U}(i)$
- $[\![\Gamma \vdash \mathrm{Prop}]\!](\gamma) := \mathcal{O}(X)$
- $[\![\Gamma \vdash \lambda x : A.T]\!](\gamma) := \{\big(\alpha, [\![\Gamma; (x : A) \vdash T]\!](\gamma, \alpha)\big) | \alpha \in [\![\Gamma \vdash A]\!](\gamma)\}$
- $[\![\Gamma \vdash t_1 t_2]\!](\gamma) := [\![\Gamma \vdash t_1]\!](\gamma)\big([\![\Gamma \vdash t_2]\!](\gamma)\big)$
- $[\![\Gamma \vdash x_i]\!](\gamma) := \gamma_i$
- $[\![\Gamma \vdash \forall x : A.B]\!](\gamma)$
  - $:= [\![\Gamma; (x : A) \vdash B]\!](\gamma, p)^{[\![\Gamma \vdash A]\!](\gamma)}$
    (when A, B are both Propositional term)
  - $:= \min\{[\![\Gamma; (x : A) \vdash B]\!](\alpha, \gamma) | \alpha \in [\![\Gamma \vdash A]\!](\gamma)\}$
    (when B is Propositional term)
  - $:= \prod_{\alpha \in [\![\Gamma \vdash A]\!]'(\gamma)} [\![\Gamma; (x : A) \vdash B]\!](\gamma, \alpha)$
    (Otherwise)

Soundness

Theorem

Following conditions hold:

- $[\![\Gamma \vdash \bot]\!] = \phi$
- $[\![\Gamma \vdash A \wedge B]\!](\gamma) = ([\![\Gamma \vdash A]\!](\gamma)) \sqcap ([\![\Gamma \vdash B]\!](\gamma))$
- $[\![\Gamma \vdash A \vee B]\!](\gamma) = ([\![\Gamma \vdash A]\!](\gamma)) \sqcup ([\![\Gamma \vdash B]\!](\gamma))$
- $[\![\Gamma \vdash \exists x : A.Q]\!](\gamma) = \bigsqcup_{\alpha \in [\![\Gamma \vdash A]\!](\gamma)} [\![\Gamma; (x : A) \vdash Q]\!](\gamma, \alpha)$

Theorem (Soundness)

- *If* $\Gamma \vdash t : T$ *is derivable, then* $[\![\Gamma \vdash t]\!](\gamma) \in [\![\Gamma \vdash T]\!](\gamma)$ *for all* $\gamma \in [\![\Gamma]\!]$
- *If* $\Gamma \vdash t_1 : T$ *and* $t_1 \rightarrow_\beta t_2$, *then* $[\![\Gamma \vdash t_1]\!](\gamma) = [\![\Gamma \vdash t_2]\!](\gamma)$ *for all* $\gamma \in [\![\Gamma]\!]$
  - *If* P *is provable propositional term in* Γ, *then* $p \in [\![\Gamma \vdash P]\!](\gamma)$.

Example

- Let $(X, \mathcal{O}(X)) = (1, \{0, 1\}), p = 0$.
  - This is jsut Classicaly Model.
- Let $(X, \mathcal{O}(X)) = (2, \{0, 1, 2\}), p = 1$
  - If P is true, then $1 \in [\![\vdash P]\!]$ since $[\![\vdash P]\!] = 2$
  - $1 \notin [\![\vdash \forall P : \mathrm{Prop}, P \vee \neg P]\!]$ since $[\![\vdash \forall P : \mathrm{Prop}, p \vee \neg P]\!] = 1$

The reason of point condition

The reason of the condition "$\bigcap \mathcal{N}(p)$ is open set" is ...

- This condition is needed in proof of soundness
- Let P be Propositional term
  - If P is true, then $p \in [\![\Gamma \vdash P]\!](\gamma)$ should hold.
  - The condition that $p \in [\![\Gamma; (x : A) \vdash P]\!](\gamma, \alpha)$ iff $p \in [\![\Gamma \vdash \forall x : A.P]\!](\alpha)$ is needed.
  - But...
  - $[\![\Gamma \vdash \forall x : A.P]\!](\gamma) = (\bigcap\{[\![\Gamma; (x : A) \vdash P]\!](\gamma, \alpha) | \alpha \in [\![\Gamma \vdash A]\!](\gamma)\})^\circ$
  - $p \in [\![\Gamma; (x : A) \vdash P]\!](\gamma, \alpha)$ dose NOT imply $p \in [\![\Gamma \vdash \forall x : A.P]\!](\gamma)$

Paradox

J.Reynolds showed following theorem in his paper "Polymorphism is not set-theoretical"

Theorem

If P is Propositional term, $2 \leqq \sharp\{ [\![\Gamma \vdash t]\!](\gamma) \mid \Gamma \vdash t : P\}$ *causes paradox.*

But I create the model which is any proof term is interpreted to JUST ONE element. Hence, this model is interpreted as if $[\![\Gamma \vdash P]\!]$ has only one element.

Definition of CIC^-

Interpretation

Extended Interpretation

Future Works

Future Work

- Remove the point condition.
  - Is the point condition really needed in proof of soundness?
  - Is there any counterexample?
- Prove the completeness of this model.
  - For any topological space $(X, \mathcal{O}(X))$, $p(\in X)$ with point condition, if P is propositional term, $p \in [\![\Gamma \vdash P]\!](\gamma)$ implies P is provable propositional term?
    - If $\Gamma \vdash p_1 : P$ and $\Gamma \vdash p_2 : P$ where P is Propositional term, then $[\![\Gamma \vdash p_1]\!](\gamma) = [\![\Gamma \vdash p_2]\!](\gamma)$
    - $\Gamma \vdash P_1 \leftrightarrow P_2$ implies $[\![\Gamma \vdash P_1]\!](\gamma) = [\![\Gamma \vdash P_2]\!](\gamma)$.
  - Find "how much this model is complete?"

Reference

[1] Werner, Benjamin. “Sets in types, types in sets.” Theoretical aspects of computer software. Springer Berlin Heidelberg, 1997.

[2] Miquel, Alexandre, and Benjamin Werner. “The not so simple proof-irrelevant model of CC.” Types for proofs and programs. Springer Berlin Heidelberg, 2003. 240-258.

[3] Reynolds, John C. “Polymorphism is not set-theoretic.” Springer Berlin Heidelberg, 1984.

[4] Pierce, Benjamin C. “Types and programming languages.” MIT press, 2002.

[5] Barendregt, Henk, W. Dekkers, and RICHARD Statman. “Lambda calculus with types.” Handbook of logic in computer science 2 (1992): 118-310.

[6] MacLane, Saunders, and Ieke Moerdijk. “Sheaves in geometry and logic: A first introduction to topos theory.” Springer, 1992.

[7] Gierz, Gerhard, ed. “Continuous lattices and domains.” Vol. 93. Cambridge University Press, 2003.