Regular Paper

An Intuitionistic Set-theoretical Model of $\mathrm{CC}^{\bar{\omega}}$

Masahiro Sato[1,a)] Jacques Garrigue[1,b)]

Received: October 5, 2015, Accepted: January 15, 2016

Abstract: Werner's set-theoretical model is one of the simplest models of $\mathrm{CC}^{\bar{\omega}}$. It combines a functional view of predicative universes with a collapsed view of the impredicative sort Prop. However this model of Prop is so coarse that the principle of excluded middle $P \lor \neg P$ holds. In this paper, we interpret Prop into a topological space (a special case of Heyting algebra) to make it more intuitionistic without sacrificing simplicity. We prove soundness and show some applications of our model.

Keywords: type theory, model, intuitionistic logic

1. Introduction

There are various models of type theory. Werner's Set-theoretical model [14] provides an intuitive model of CC^{ω}. It combines a functional view of predicative universes with a collapsed view of the impredicative sort Prop. However this model of Prop is so coarse that the principle of excluded middle $P \lor \neg P$ holds in it.

In this paper, we construct a set-theoretical model of CC^{ω} in which the principle of excluded middle $P \lor \neg P$ doesn't hold, and thus closer to completeness.

CC (the Calculus of Constructions [5]) is a pure type system [2] with two sorts, impredicative Prop and predicative Type. CC^{ω} extends CC with a hierarchy of predicative sorts Type_i. CIC (the Calculus of Inductive Constructions) adds inductive types to CC^{ω}.

In Ref. [14], Werner provides a remarkably simple model of CIC. In this model, $\lambda x : A.t$ is interpreted by a set-theoretical function for predicative sorts. Yet such a simple approach is known to fail for impredicative sorts as it runs afoul of Reynolds' paradox [11]. Therefore, the model for Prop is two-valued. Hence the principle of excluded middle $P \lor \neg P$ is valid in this model, making it classical. Later, Miquel and Werner [10] have shown that proving the soundness of this model was not so easy, but this doesn't change the simplicity of the model itself. This simple approach is to be contrasted with Luo's model of ECC (CC^{ω} extended with strong sums $\Sigma x : A.B$) which uses ω-sets [8], or more recent models such as categorical models [7] or models based on homotopy theory [12]. This is the drawback of simplicity: while Werner's approach avoids many complications of more precise models, it is at times counter-intuitive, as it completely ignores the intuitionistic aspect of CC.

Our goal has been to recover the intuitionistic part of CC without increasing the complexity of the model. Barras [4] provided a first way to do it, by interpreting CC^{ω} in IZF (intuitionistic Zermelo-Fraenkel set theory [1]) rather than ZF. While this is an interesting result, and the fact it is backed by a fully formalized proof is very impressive, this requires one to work in the radically different world of IZF, where it is difficult to express meta-reasoning about the expressiveness of the language. For this reason we prefer to stay inside classical set theory ZF, but we change the interpretation of Prop to be some topological space. The open sets of a topological space form a Heyting algebra. Heyting algebras are used when constructing models of intuitionistic logic, but usually their elements are not understood as sets. In our model, proofs shall be interpreted as elements of denotations of propositions, hence these denotations must be sets, and the order must be set inclusion. Using topological spaces solves this problem. Despite the fact that the interpretation of Prop is many valued, we avoid Reynolds' paradox by making the interpretation of proofs undistinguished. Due to proof-irrelevance, this model still validates some propositions that are not provable, hence this model does not reach completeness yet. However this is sufficient to exclude many classical propositions such as the principle of excluded middle $P \lor \neg P$ or the linearity axiom $(P \to Q) \lor (Q \to P)$. Note that, to make the model coherent, we had to slightly restrict the type system CC^{ω}, in particular not allowing propositions to be parametrized by proofs, and we named it $\mathrm{CC}^{\bar{\omega}}$ (read CC-omega-minus). We believe the scope is still sufficient to make this model practical, but hope to remove these restrictions in the future.

This model is parametrized by a topological space $(X, \mathcal{O}(X))$ and a point $p \in X$, which is called the *reference point* [*1]. By replacing the parameters of the model, we can make it more or less precise. For instance if its parameters are the topological space $(\{\cdot\}, \{\emptyset, \{\cdot\}\})$ and the reference point '$\cdot$', we obtain a model of classical logic, which is the coarsest one. It suffices to add one more point and shift the reference point to invalidate the principle of excluded middle.

[1] Graduate School of Mathematics, Nagoya University, Nagoya 464–8602, Japan
[a)] sato.masahiro.math@gmail.com
[b)] garrigue@math.nagoya-u.ac.jp

[*1] Our proof of soundness requires this reference point to satisfy a condition, which is called the *point condition*.

In Section 2, we define the language of the type system $\mathrm{CC}^{\bar{\omega}}$. In Section 3, we give our set-theoretical interpretation of $\mathrm{CC}^{\bar{\omega}}$, and prove its soundness. In Section 4, we show some applications of this model. For instance, we show that the excluded middle cannot be derived from the linearity axiom in $\mathrm{CC}^{\bar{\omega}}$. In Section 5, we analyze how we avoid Reynolds' paradox.

2. Definition of $\mathrm{CC}^{\bar{\omega}}$

We define the type system $\mathrm{CC}^{\bar{\omega}}$ as follows.

Definition 2.1 (Term)**.** *Let V be an infinite set of variables.*

- *For all $x \in V$, x is a term with free variables* $\mathrm{fv}(x) = \{x\}$.
- *If t_1 and t_2 are terms, then $t_1\ t_2$ is a term with free variables* $\mathrm{fv}(t_1) \cup \mathrm{fv}(t_2)$.
- *If t and T are terms, and $x \in V$ then, $\lambda x : T.t$ is a term with free variables* $\mathrm{fv}(T) \cup (\mathrm{fv}(t) \setminus \{x\})$.
- *If T_1 and T_2 are terms, and $x \in V$ then $\forall x : T_1.T_2$ is a term with free variables* $\mathrm{fv}(T_1) \cup (\mathrm{fv}(T_2) \setminus \{x\})$.
- Prop, Type_i *are terms ($i = 1, 2, 3, \ldots$) with free variables* $\emptyset$.

Prop and Type_i are called *sorts*. Prop is called the impredicative sort and it represents the type of all propositions.

Definition 2.2 (Context)**.**

- [] *is a context with domain* $\mathrm{dom}([]) = \emptyset$.
- *If Γ is a context, and T is a term and $x \in V \setminus \mathrm{dom}(\Gamma)$, then $\Gamma; (x : T)$ is a context with domain* $\mathrm{dom}(\Gamma) \cup \{x\}$.

We show the typing rules of $\mathrm{CC}^{\bar{\omega}}$ in **Table 1**. They are standard, except that we restricted the PI-Type rule in the case A : Prop and B : Prop, and removed the subtyping rule from Prop to Type. The unrestricted Prop-Prop PI-Type rule creates difficulties when building an intuitionistic model, and if we do not remove the subtyping rule it becomes possible to use the Prop-Type case of the PI-Type rule in place of the restricted Prop-Prop case, which would make the model incoherent. We believe these restrictions are reasonable, as the proof component is seldom used in the PI-Type rule, with the notable exception of the generic statement of proof-irrelevance. Since the Type-Prop case of the PI-Type rule is unfettered, one can still write propositions parametrized over terms, types, or propositions (hence the impredicativity). Removing the subtyping between Prop and Type does not change the expressive power, as it is still possible to explicitly duplicate properties using Type to Prop. We hope to solve these problems in the future, and allow the standard typing rules.

Table 1 Typing rules of $\mathrm{CC}^{\bar{\omega}}$.

$[] \vdash \mathrm{Prop} : \mathrm{Type}_1$	(Axiom)
$[] \vdash \mathrm{Type}_i : \mathrm{Type}_{i+1}$	
$\dfrac{\Gamma \vdash A : s \quad x \notin \mathrm{dom}(\Gamma)}{\Gamma; (x : A) \vdash x : A}$	(Variable)
$\dfrac{\Gamma \vdash t : T \quad \Gamma \vdash A : s \quad x \notin \mathrm{dom}(\Gamma)}{\Gamma; (x : A) \vdash t : T}$	(Weakening)
$\dfrac{\Gamma \vdash A : \mathrm{Type}_i}{\Gamma \vdash A : \mathrm{Type}_{i+1}}$	(Subtyping)
$\dfrac{\Gamma \vdash A : \mathrm{Type}_i \quad \Gamma; (x : A) \vdash B : \mathrm{Type}_j}{\Gamma \vdash \forall x : A.B : \mathrm{Type}_{\max(i,j)}}$	(PI − Type)
$\dfrac{\Gamma \vdash A : \mathrm{Prop} \quad \Gamma; (x : A) \vdash B : \mathrm{Type}_j}{\Gamma \vdash \forall x : A.B : \mathrm{Type}_j}$	
$\dfrac{\Gamma \vdash A : \mathrm{Type}_i \quad \Gamma; (x : A) \vdash B : \mathrm{Prop}}{\Gamma \vdash \forall x : A.B : \mathrm{Prop}}$	
$\dfrac{\Gamma \vdash A : \mathrm{Prop} \quad \Gamma \vdash B : \mathrm{Prop} \quad x \notin \mathrm{fv}(B)}{\Gamma \vdash \forall x : A.B : \mathrm{Prop}}$	
$\dfrac{\Gamma; (x : A) \vdash t : B \quad \Gamma \vdash \forall x : A.B : s}{\Gamma \vdash \lambda x : A.t : \forall x : A.B}$	(Abstract)
$\dfrac{\Gamma \vdash u : \forall x : A.B \quad \Gamma \vdash v : A}{\Gamma \vdash u\ v : B[x \backslash v]}$	(Apply)
$\dfrac{\Gamma \vdash t : A \quad \Gamma \vdash B : s \quad A =_\beta B}{\Gamma \vdash t : B}$	(BetaEquality)

In Table 1, the metavariable s denotes a sort, $=_\beta$ denotes *beta equality* and $B[x \backslash v]$ denotes substitution. Here are their definitions.

Definition 2.3 (Substitution)**.** *Let t and v be terms and x be a variable. The substitution $t[x \backslash v]$, which means v replaces x in t, is defined inductively as follows:*

(i) *If y is a variable, then* $y[x \backslash v] = \begin{cases} v & (y = x) \\ y & (\textit{otherwise}), \end{cases}$

(ii) $(t_1 t_2)[x \backslash v] = (t_1[x \backslash v])(t_2[x \backslash v])$,

(iii) $(\lambda x' : T.t')[x \backslash v] = \lambda x' : (T[x \backslash v]).t'[x \backslash v]$ *when* $x' \notin \mathrm{fv}(v) \cup \{x\}$,

(iv) $(\forall x' : T_1.T_2)[x \backslash v] = \forall x' : (T_1[x \backslash v]).(T_2[x \backslash v])$ *when* $x' \notin \mathrm{fv}(v) \cup \{x\}$,

(v) $(\mathrm{Prop})[x \backslash v] = \mathrm{Prop}$,

(vi) $(\mathrm{Type}_i)[x \backslash v] = \mathrm{Type}_i \quad (i = 1, 2, 3, \ldots)$.

Definition 2.4 (Beta Equality)**.** *Let $=_\beta$ be the smallest equivalence relation such that the following conditions hold.*

(i) $(\lambda x : A.t)\ a =_\beta t[x \backslash a]$.

(ii) *If $t_1 =_\beta t_1'$ and $t_2 =_\beta t_2'$, then $t_1 t_2 =_\beta t_1' t_2'$.*

(iii) *If $t =_\beta t'$ and $A =_\beta A'$, then $\lambda x : A.t =_\beta \lambda x : A't'$.*

(iv) *If $A =_\beta A'$ and $B =_\beta B'$, then $\forall x : A.B =_\beta \forall x : A'B'$.*

Definition 2.5 (Relaxed Beta Equality)**.** *Let $\simeq_\beta$ be the smallest equivalence relation such that the following conditions hold.*

(i) *∼ (iv) as in Definition 2.4.*

(v) $\mathrm{Type}_i \simeq_\beta \mathrm{Type}_j$ *for any i, j.*

Lemma 2.6 (Uniqueness of Typing)**.** *If $\Gamma \vdash t : A$ and $\Gamma \vdash t : B$ are derivable, then $A \simeq_\beta B$.*

Lemma 2.7 (Substitution)**.** *If $\Gamma \vdash u : U$ and $\Gamma; (x : U); \Delta \vdash t : T$ are derivable then $\Gamma; \Delta[x \backslash u] \vdash t[x \backslash u] : T[x \backslash u]$ is also derivable.*

Lemma 2.8 (Weakening)**.** *If $\Gamma_1; \Gamma_2 \vdash t : T$ is derivable, then $\Gamma_1; \Delta; \Gamma_2 \vdash t : T$ is also derivable when $\Gamma_1; \Delta; \Gamma_2$ is well-formed, i.e., when $\Gamma_1; \Delta; \Gamma_2 \vdash \mathrm{Prop} : \mathrm{Type}_1$ is derivable.*

In $\mathrm{CC}^{\bar{\omega}}$, propositions are types which belong to the impredicative sort Prop, and proofs are terms of types which represent propositions. Next, we give a definition of propositions and proofs as follows. Rather than introducing an explicitly sorted type system like in Ref. [10], we will prove that these definitions are stable under substitution, weakening, and reduction, so that we can safely use them when defining our interpretation.

Definition 2.9.

(1) *Propositional Term*
The term P is called a propositional term for Γ iff $\Gamma \vdash P : \mathrm{Prop}$ is derivable.

(2) *Proof Term*
The term p is called a proof term for Γ iff $\Gamma \vdash p : P$ is derivable for some P which is a propositional term for Γ. P is then called a Provable Propositional Term for Γ.

Lemma 2.10 (Proof and propositional terms)**.**

(i) *We assume that P_1 and P_2 are well typed under the same context Γ. If P_1 is a propositional term for Γ and $P_1 =_\beta P_2$, then P_2 is also a propositional term for Γ.*

(ii) *We assume that p_1 and p_2 are well typed under the same context Γ. If p_1 is a proof term for Γ and $p_1 =_\beta p_2$, then p_2 is also a proof term for Γ.*

(iii) *We assume that $\Gamma \vdash u : \forall x : A.B$ and $\Gamma \vdash v : A$ are derivable. If u is a proof term for Γ, then $u\ v$ is also a proof term for Γ.*

(iv) *If t is a proof term for $\Gamma; (x : A)$ and $\lambda x : A.t$ is well typed under Γ, then $\lambda x : A.t$ is also a proof term for Γ.*

Thanks to our restriction on the subtyping rule, Lemma 2.10 (i) holds. If we were to assume the following rule

$$\frac{\Gamma \vdash A : \mathrm{Prop}}{\Gamma \vdash A : \mathrm{Type}_i}$$

the above lemma would not hold. Specifically, for A a propositional term for Γ, $(\lambda T : \mathrm{Type}_i.T)\ A$ would be typable, but not a propositional term for Γ despite $(\lambda T : \mathrm{Type}_i.T)\ A =_\beta A$. Since the interpretation of a term is going to depend on whether it is propositional or not, this would make our model incoherent.

Proof terms and propositional terms are preserved under substitution. The following lemma expresses this fact.

Lemma 2.11. *If p is a proof (resp. propositional) term for the context $\Gamma; (x : U); \Delta$ and $\Gamma \vdash u : U$ is derivable, then $p[x\backslash u]$ is a proof (resp. propositional) term for the context $\Gamma; \Delta[x\backslash u]$.*

Lemma 2.12. *If p is a proof (resp. propositional) term for the context $\Gamma_1; \Gamma_2$, then p is a proof (resp. propositional) term for the context $\Gamma_1; \Delta; \Gamma_2$ when $\Gamma_1; \Delta; \Gamma_2$ is well formed* [*2].

The function $\mathbf{PT}_{\Gamma,x}(A, B)$ maps two types into the string symbols $\{\mathsf{PP}, \mathsf{TP}, \mathsf{T}\}$. Its goal is to discriminate cases of $\forall x : A.B$ to give them different interpretations.

Definition 2.13 (Product Type)**.** *We assume that $\Gamma \vdash A : s_1$ and $\Gamma; (x : A) \vdash B : s_2$ are derivable where s_1, s_2 are sorts.*

$$\mathbf{PT}_{\Gamma,x}(A, B) := \begin{cases} \mathsf{PP} & (s_1, s_2) = (\mathrm{Prop}, \mathrm{Prop}) \\ \mathsf{TP} & (s_1, s_2) = (\mathrm{Type}_i, \mathrm{Prop}) \\ \mathsf{T} & s_2 = \mathrm{Type}_i \end{cases}$$

Thanks to uniqueness of typing in Lemma 2.6, the function $\mathbf{PT}_{\Gamma,x}(A, B)$ is well defined. Again, $\mathbf{PT}_{\Gamma,x}(A, B)$ is stable under substitution and weakening.

Lemma 2.14.

(i) *If A and B are typable under $\Gamma; (x{:}U); \Delta$, and $\Gamma \vdash u : U$, then $\mathbf{PT}_{(\Gamma;(x:U);\Delta),a}(A, B) = \mathbf{PT}_{(\Gamma;\Delta[x\backslash u]),a}(A[x\backslash u], B[x\backslash u])$ holds.*

(ii) *If A and B are typable under $\Gamma_1; \Gamma_2$ and $\Gamma_1; \Delta; \Gamma_2$, then $\mathbf{PT}_{(\Gamma_1;\Delta;\Gamma_2),a}(A, B) = \mathbf{PT}_{(\Gamma_1;\Gamma_2),a}(A, B)$ holds.*

Proof. (i) When $\mathbf{PT}_{\Gamma;(x:U);\Delta,a}(A, B) = \mathsf{PP}$, A is a proposition for $(\Gamma; (x : U); \Delta)$ and B is a proposition for $(\Gamma; (x : U); \Delta)$. By Lemma 2.11, $A[x\backslash u]$ is a proposition for $(\Gamma; \Delta[x\backslash u])$ and $B[x\backslash u]$ is also a proposition for $(\Gamma; \Delta[x\backslash u])$. Hence the statement holds in this case. When $\mathbf{PT}_{\Gamma;(x:U);\Delta,a}(A, B) = \mathsf{TP}$, $\Gamma; \Delta[x\backslash u] \vdash A[x\backslash u] : \mathrm{Type}_i$ is derivable for some i. By Lemma 2.6 and the fact $\mathrm{Prop} \neq_\beta \mathrm{Type}_i$, the statement holds in this case. The remaining case is similar.

(ii) It is clearly proved by applying the result of (i) in this lemma, since variables in Δ do not appear in Γ_2 and terms A and B.

□

Lastly, here are some notations allowing to use other logical symbols [3].

Definition 2.15.

$$\begin{aligned}
&A \to B := \forall x : A.B && (\text{when } x \notin fv(B)),\\
&\bot := \forall P : \mathrm{Prop}.P,\\
&\neg A := A \to \bot,\\
&A \wedge B := \forall P : \mathrm{Prop}.(A \to B \to P) \to P,\\
&A \vee B := \forall P : \mathrm{Prop}.(A \to P) \to (B \to P) \to P,\\
&\exists x : A.Q := \forall P : \mathrm{Prop}.(\forall x : A.(Q \to P)) \to P,\\
&A \leftrightarrow B := (A \to B) \wedge (B \to A),\\
&x =_A y := \forall Q : (A \to \mathrm{Prop}).Q\ x \leftrightarrow Q\ y.
\end{aligned}$$

3. Interpretation

3.1 Lattice

Several interpretations of type theory have been proposed such as using ω-sets [8] or coherent spaces [6]. In this paper, we use *Heyting algebras* [9], [13] for propositions. Heyting algebras provide models of intuitionistic logic. The open sets of a topological space can be given the structure of a Heyting algebra (see Lemma 3.2), and as such provide models of intuitionistic logic too [13]. We give a definition of lattice and Heyting algebra as follows.

Definition 3.1 (Lattice)**.** *Let $(A, \leq)$ be a partially ordered set (i.e., reflexive, antisymmetric, and transitive). $(A, \leq)$ is called a Lattice when any two elements a and b of A have a supremum '$a \sqcup b$' and an infimum '$a \sqcap b$', which are called join and meet* [*3]*. A lattice is also called a complete lattice if every subset S of A has a supremum '$\bigsqcup S$' and an infimun '$\bigsqcap S$'. We write a minimum element $\mathbb{O} := \bigsqcup \varnothing$ and a maximum element $\mathbb{I} := \bigsqcap \varnothing$. If a lattice has an exponential operator a^b such that*

$$x \leq z^y \Leftrightarrow x \sqcap y \leq z$$

holds, then we call it a Heyting Algebra.

The following lemma shows that topological spaces are complete Heyting algebras.

[*2] A context Γ is called well formed iff $\Gamma \vdash \mathrm{Prop} : \mathrm{Type}_1$ is derivable.

[*3] We use the lattice operation symbols join '$\sqcup$' and meet '$\sqcap$' instead of '$\vee$' and '$\wedge$', since we use the latter as logical symbols.

Lemma 3.2. *Any topological space $(X, O(X))$ is a Heyting algebra, moreover it is a complete lattice.*

Proof. Let $a \leq b$ be $a \subset b$, and define each operation as follows:

$$\begin{aligned}
&\mathbb{I} := X,\\
&\mathbb{O} := \emptyset,\\
&\bigsqcup S := \bigcup S,\\
&\bigsqcap S := \bigsqcup\{t \mid \forall s \in S, t \leq s\} = \left(\bigcap S\right)^{\circ}\\
&\qquad (where\ A^{\circ}\ is\ the\ interior\ of\ A),\\
&b^{a} := \bigsqcup\{t \mid t \sqcap a \leq b\}.
\end{aligned}$$

□

The following lemma states well known properties of complete Heyting algebras.

Lemma 3.3. *Let $(A, \leq)$ be a complete Heyting algebra. Then the following conditions hold.*

$$(x^{b})^{a} = x^{a \sqcap b}, \tag{1}$$

$$\bigsqcap\{t^{t^{a}} \mid t \in A\} = a, \tag{2}$$

$$x^{a} \sqcap x^{b} = x^{a \sqcup b}, \tag{3}$$

$$\bigsqcap\{a^{t} \mid t \in S\} = a^{\bigsqcup S}, \tag{4}$$

$$\bigsqcap \emptyset = 1, \tag{5}$$

$$x \leq x^{y}, \tag{6}$$

$$x^{y} \sqcap y^{x} = 1 \Rightarrow x = y, \tag{7}$$

$$\bigsqcap S = 1 \Rightarrow \forall a \in S, a = 1. \tag{8}$$

3.2 Preparation of the Interpretation

Let p, which is called the *reference point*, be some point of the topological space $(X, O(X))$ such that the following condition

$$\bigcap \mathcal{U}(p)\ is\ an\ open\ set$$

holds where $\mathcal{U}(p)$ is the set of all open sets which contain p. We will parametrize our model with $O(X)$ and p. Let us call this condition the *point condition*. It becomes necessary when proving soundness.

Definition 3.4 (Dependent Function)**.** *Let A be a set, and $B(a)$ be a set with parameter $a \in A$. We define the set of dependent functions as follows*

$$\prod_{a \in A} B(a) := \{f \subset \coprod_{a \in A} B(a) \mid \forall a \in A, \exists! b \in B(a), (a, b) \in f\}$$

that is the set of functions whose graphs are included in

$$\coprod_{a \in A} B(a) := \{(x, y) \in A \times \bigcup_{a \in A} B(a) \mid y \in B(x)\}.$$

Next, we introduce Grothendieck universes, which are closed under dependent-function construction, and which we will use to interprete Type_{i}.

Definition 3.5. *Let α be an ordinal. We define V_{α} as follows*

$$V_{0} = \emptyset,$$

$$V_{\alpha+1} = \mathcal{P}(V_{\alpha}),$$

$$V_{\alpha} = \bigcup_{\beta < \alpha} V_{\beta} \quad (when\ \alpha\ is\ a\ limit\ ordinal).$$

We define a universe $\mathcal{U}(i)$ as follows

$$\mathcal{U}(i) = V_{\lambda_{i}},$$

where λ_{i} is the i-th inaccessible cardinal.

The following lemma is necessary when proving soundness.

Lemma 3.6.

(i) $A \in \mathcal{U}(i)$ *implies* $\mathcal{P}(A) \in \mathcal{U}(i)$

(ii) $A \in \mathcal{U}(i)$ *implies* $A \subset \mathcal{U}(i)$

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

(iv) $\mathcal{U}(i) \in \mathcal{U}(i+1)$

(v) $\mathcal{U}(i) \subset \mathcal{U}(i+1)$

(vi) $x \in \mathcal{U}(i)$ *and* $y \in x$ *imply* $y \in \mathcal{U}(i)$

(vii) $x \in \mathcal{U}(i)$ *and* $y \subset x$ *imply* $y \in \mathcal{U}(i)$

3.3 Interpretation of the Judgments

In this model, a type T is interpreted into a set $[\![T]\!]$, and a context $x_{1} : T_{1}; x_{2} : T_{2}; \cdots ; x_{n} : T_{n}$ is interpreted into a dependent tuple; in particular, when there are no dependent types in the context, it is a tuple in $[\![T_{1}]\!] \times [\![T_{2}]\!] \times \cdots \times [\![T_{n}]\!]$.

First, we define the (partial) interpretation of contexts $[\![-]\!]$, judgments $[\![- \vdash -]\!]$ and strict judgments $[\![- \vdash -]\!]'$ by mutual recursion as follows.

Definition 3.7 (interpretation)**.** *Let $(X, O(X))$ be a topological space such that $X \in \mathcal{U}(1)$, and p be a reference point of X satisfying the point condition.*

(i) Definition of the strict-interpretation of a judgment $[\![\Gamma \vdash A]\!]'$

$$[\![\Gamma \vdash A]\!]'(\gamma) = \begin{cases} [\![\Gamma \vdash A]\!](\gamma) \cap \{p\} \\ \quad (A\ is\ a\ propositional\ term\ for\ \Gamma) \\ [\![\Gamma \vdash A]\!](\gamma) \qquad\qquad (otherwise) \end{cases}$$

(ii) Definition of the interpretation of a context $[\![\Gamma]\!]$

$$\begin{aligned}
[\![[]]\!] &:= \{()\}\\
[\![\Gamma; (x : A)]\!] &:= \{(\gamma, \alpha) \mid \gamma \in [\![\Gamma]\!] \text{ and } \alpha \in [\![\Gamma \vdash A]\!]'(\gamma)\}\\
&= \coprod_{\gamma \in [\![\Gamma]\!]} [\![\Gamma \vdash A]\!]'(\gamma)
\end{aligned}$$

where $()$ represents the empty sequence.

(iii) Definition of the interpretation of a judgment $[\![\Gamma \vdash t]\!]$
If t is a proof term for Γ, then its interpretation is the reference point.

$$[\![\Gamma \vdash t]\!](\gamma) := p$$

*Otherwise, if $\Gamma \vdash t : T$ is derivable and T is not a proposition for Γ, we follow the definition in **Table 2**.*

For simplicity, we write $[\![T]\!]$ for $[\![[] \vdash T]\!]()$, when the context is empty.

When defined, the interpretation of a context $[\![\Gamma]\!]$ is a set of sequences γ whose length is the length of Γ, and $[\![\Gamma \vdash t]\!]$ is a function whose domain is $[\![\Gamma]\!]$, and which returns some set

Table 2 Interpretation of judgments.

$$
\begin{aligned}
\llbracket \Gamma \vdash \mathrm{Type}_i \rrbracket(\gamma) &:= \mathcal{U}(i)\\
\llbracket \Gamma \vdash \mathrm{Prop} \rrbracket(\gamma) &:= \mathcal{O}(X)\\
\llbracket \Gamma \vdash \forall x : A.B \rrbracket(\gamma) &:=
\end{aligned}
$$

$$
\begin{cases}
\Big(\llbracket \Gamma \vdash B \rrbracket(\gamma)\Big)^{\llbracket \Gamma \vdash A \rrbracket(\gamma)} \\
\qquad (\text{when } \mathbf{PT}_{\Gamma,x}(A,B) = \mathsf{PP}) \\[2ex]
\bigsqcap\{\llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, \alpha) \mid \alpha \in \llbracket \Gamma \vdash A \rrbracket(\gamma)\} \\
\qquad (\text{when } \mathbf{PT}_{\Gamma,x}(A,B) = \mathsf{TP}) \\[2ex]
\prod_{\alpha \in \llbracket \Gamma \vdash A \rrbracket'(\gamma)} \llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, \alpha) \\
\qquad (\text{when } \mathbf{PT}_{\Gamma,x}(A,B) = \mathsf{T})
\end{cases}
$$

$$
\begin{aligned}
\llbracket \Gamma \vdash \lambda x : A.t \rrbracket(\gamma) &:= \\
&\Big\{(\alpha, \llbracket \Gamma; (x : A) \vdash t \rrbracket(\gamma, \alpha)) \mid \alpha \in \llbracket \Gamma \vdash A \rrbracket'(\gamma)\Big\}\\
\llbracket \Gamma \vdash u\ v \rrbracket(\gamma) &:= \llbracket \Gamma \vdash u \rrbracket(\gamma)\Big(\llbracket \Gamma \vdash v \rrbracket(\gamma)\Big)\\
\llbracket (x_1 : T_1); \cdots ; (x_n : T_n) \vdash x_i \rrbracket(\gamma_1, \cdots, \gamma_n) &:= \gamma_i
\end{aligned}
$$

$\llbracket \Gamma \vdash t \rrbracket(\gamma)$ — soundness will tell us that if $\Gamma \vdash t : T$, then $\llbracket \Gamma \vdash t \rrbracket(\gamma) \in \llbracket \Gamma \vdash T \rrbracket(\gamma)$. We choose to interprete all proof terms by the reference point p, which represents (absolute) truth. However, for this to make sense from a Heyting algebra point of view, we need all proofs in the valuation γ to be also true, *i.e.*, to be p. Hence we use the strict-interpretation to define contexts, which ensures exactly that property. Concerning Table 2, most cases are similar to Werner's interpretation, so we only explain the interpretation of $\forall x : A.B$. There are three cases, according to the result of $\mathbf{PT}_{\Gamma,x}(A,B)$. When $\mathbf{PT}_{\Gamma,x}(A,B) = \mathsf{PP}$, the interpretation of $\llbracket \Gamma \vdash \forall x : A.B \rrbracket$ represents the logical implication $A \Rightarrow B$. We use the Heyting algebra representation of this implication. Here we assume that x does not appear in B, thanks to our restriction. Otherwise we would need to build the interpretation of $\llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, p)$, but this requires that $p \in \llbracket \Gamma \vdash A \rrbracket(\gamma)$, which is not always true. When $\mathbf{PT}_{\Gamma,x}(A,B) = \mathsf{TP}$ the interpretation of $\llbracket \Gamma \vdash \forall x : A.B \rrbracket$ represents universal quantification, and again we use the infinite meet operator of the complete Heyting algebra to express it. In the last case only the representation becomes a set theoretical dependent function. Note that while we intend our interpretation to be total on well-typed terms, until soundness is proved we must assume that the intepretation of application is partial, since the interpretation of u might not be a function graph, and the interpretation of v could be outside of its domain.

We start with the weakening and substitution lemmas. They show that our interpretation is well behaved.

Lemma 3.8 (interpretation of weakening)**.** *The following equation holds*

$$\llbracket \Gamma \vdash t \rrbracket(\gamma) = \llbracket \Gamma; \Delta \vdash t \rrbracket(\gamma, \delta)$$

when both sides are well defined.

Proof. If t is a proof term, it is clear by Lemma 2.12. If t is not a proof term, it is proved by induction on the term t. The subtle point is the case of PI-Type. However the value of $\mathbf{PT}_{\Gamma,x}(A,B)$ is invariant by Lemma 2.14 (ii). □

Our substitution lemma is similar to those in Refs. [14] and [10].

Lemma 3.9 (interpretation of substitution)**.** *We assume* $\Gamma \vdash u : U$ *is derivable. If* $\Gamma; (x : U); \Delta$ *is well formed and*

$$(\gamma, \llbracket \Gamma \vdash u \rrbracket(\gamma), \delta) \in \llbracket \Gamma; (x : U); \Delta \rrbracket$$

holds (with all interpretations defined), then

$$(\gamma, \delta) \in \llbracket \Gamma; \Delta[x \backslash u] \rrbracket$$

holds. Moreover, in

$$
\begin{aligned}
&\llbracket \Gamma; (x : U); \Delta \vdash t \rrbracket(\gamma, \llbracket \Gamma \vdash u \rrbracket(\gamma), \delta)\\
&\qquad\qquad = \llbracket \Gamma; \Delta[x \backslash u] \vdash t[x \backslash u] \rrbracket(\gamma, \delta)
\end{aligned}
$$

the right hand side is defined whenever the left hand side is, and the equation holds for all t *and* T *such that* $\Gamma; (x : U); \Delta \vdash t : T$ *is derivable.*

Proof. If t is a proof term, it is clear by Lemma 2.11. It t is not a proof term, it is provable by induction on term t by using Lemmas 3.8 and 2.14 (i) in the same way as Ref. [10]. □

Finally we prove the following theorem about the interpretation of logical symbols in Definition 2.15. It demonstrates the validity of the interpretation.

Theorem 3.10 (interpretation of logical symbols)**.**

(i) $\llbracket \Gamma \vdash \bot \rrbracket = \varnothing$

(ii) $\llbracket \Gamma \vdash A \wedge B \rrbracket(\gamma) = (\llbracket \Gamma \vdash A \rrbracket(\gamma)) \sqcap (\llbracket \Gamma \vdash B \rrbracket(\gamma))$

(iii) $\llbracket \Gamma \vdash A \vee B \rrbracket(\gamma) = (\llbracket \Gamma \vdash A \rrbracket(\gamma)) \sqcup (\llbracket \Gamma \vdash B \rrbracket(\gamma))$

(iv) $\llbracket \Gamma \vdash \exists x : A.Q \rrbracket(\gamma)$
$$= \bigsqcup_{\alpha \in \llbracket \Gamma \vdash A \rrbracket(\gamma)} \llbracket \Gamma; (x : A) \vdash Q \rrbracket(\gamma, \alpha)$$

(v) $\llbracket \Gamma \vdash A \leftrightarrow B \rrbracket(\gamma) = X \Rightarrow \llbracket \Gamma \vdash A \rrbracket(\gamma) = \llbracket \Gamma \vdash B \rrbracket(\gamma)$

(vi) $\llbracket \Gamma \vdash x =_A y \rrbracket(\gamma) = X \Rightarrow \llbracket \Gamma \vdash x \rrbracket(\gamma) = \llbracket \Gamma \vdash y \rrbracket(\gamma)$

Proof. Let $a, b, q(\alpha)$ be

$$
\begin{aligned}
&a := \llbracket \Gamma \vdash A \rrbracket(\gamma)\\
&b := \llbracket \Gamma \vdash B \rrbracket(\gamma)\\
&q(\alpha) := \llbracket \Gamma; (x : A) \vdash Q \rrbracket(\gamma, \alpha).
\end{aligned}
$$

By using Lemma 3.3 and Lemma 3.8 we have the followings:

(i) For $\llbracket \Gamma \vdash \bot \rrbracket = \varnothing$.

$$
\begin{aligned}
&\llbracket \Gamma \vdash \bot \rrbracket(\gamma)\\
&\quad = \llbracket \Gamma \vdash \forall P : \mathrm{Prop}.P \rrbracket(\gamma)\\
&\quad = \bigsqcap\{\llbracket \Gamma; (P : \mathrm{Prop}) \vdash P \rrbracket(\gamma, x) \mid x \in \llbracket \Gamma \vdash \mathrm{Prop} \rrbracket(\gamma)\}\\
&\quad = \bigsqcap\{x | x \in \mathcal{O}(X)\}\\
&\quad = \varnothing
\end{aligned}
$$

(ii) For $\llbracket \Gamma \vdash A \wedge B \rrbracket(\gamma) = (\llbracket \Gamma \vdash A \rrbracket(\gamma)) \sqcap (\llbracket \Gamma \vdash B \rrbracket(\gamma))$.

$$
\begin{aligned}
&\llbracket \Gamma \vdash A \wedge B \rrbracket(\gamma)\\
&\quad = \llbracket \Gamma \vdash \forall P : \mathrm{Prop}.(A \to (B \to P)) \to P \rrbracket(\gamma)\\
&\quad = \bigsqcap\{x^{(x^b)^a} \mid x \in \mathcal{O}(X)\}\\
&\quad = \bigsqcap\{x^{x^{a \sqcap b}} \mid x \in \mathcal{O}(X)\} \quad \text{(by Lemma 3.3 (1))}\\
&\quad = a \sqcap b \quad \text{(by Lemma 3.3 (2))}\\
&\quad = \llbracket \Gamma \vdash A \rrbracket(\gamma) \sqcap \llbracket \Gamma \vdash B \rrbracket(\gamma)
\end{aligned}
$$

(iii) For $\llbracket \Gamma \vdash A \vee B \rrbracket(\gamma) = (\llbracket \Gamma \vdash A \rrbracket(\gamma)) \sqcup (\llbracket \Gamma \vdash B \rrbracket(\gamma))$.

$$\begin{aligned}
&\llbracket \Gamma \vdash A \vee B \rrbracket(\gamma)\\
&\quad = \llbracket \Gamma \vdash \forall P : \mathrm{Prop}.(A \to P) \to ((B \to P) \to P) \rrbracket(\gamma)\\
&\quad = \bigsqcap \{(x^{x^b})^{x^a} \mid x \in \mathcal{O}(X)\}\\
&\quad = \bigsqcap \{x^{x^a \sqcap x^b} \mid x \in \mathcal{O}(X)\} \quad \text{(by Lemma 3.3 (1))}\\
&\quad = \bigsqcap \{x^{x^{a \sqcup b}} \mid x \in \mathcal{O}(X)\} \quad \text{(by Lemma 3.3 (3))}\\
&\quad = a \sqcup b \quad \text{(by Lemma 3.3 (2))}\\
&\quad = \llbracket \Gamma \vdash A \rrbracket(\gamma) \sqcup \llbracket \Gamma \vdash B \rrbracket(\gamma)
\end{aligned}$$

(iv) For $\llbracket \Gamma \vdash \exists x : A.Q \rrbracket(\gamma) = \bigsqcup_{\alpha \in \llbracket \Gamma \vdash A \rrbracket(\gamma)} \llbracket \Gamma ; (x : A) \vdash Q \rrbracket(\gamma, \alpha)$.

$$\begin{aligned}
&\llbracket \Gamma \vdash \exists a : A.Q \rrbracket(\gamma)\\
&\quad = \llbracket \Gamma \vdash \forall P : \mathrm{Prop}.(\forall a : A.(Q \to P) \to P \rrbracket(\gamma)\\
&\quad = \bigsqcap \{x^{\bigsqcap \{x^{q(\alpha)} \mid \alpha \in a\}} \mid x \in \mathcal{O}(X)\}\\
&\quad = \bigsqcap \{x^{x^{\bigsqcup \{q(\alpha) \mid \alpha \in a\}}} \mid x \in \mathcal{O}(X)\}\\
&\qquad\qquad\qquad \text{(by Lemma 3.3 (4))}\\
&\quad = \bigsqcup \{q(\alpha) \mid \alpha \in a\} \quad \text{(by Lemma 3.3 (2))}\\
&\quad = \bigsqcup_{\alpha \in \llbracket \Gamma \vdash A \rrbracket(\gamma)} \llbracket \Gamma ; (a : A) \vdash Q \rrbracket(\gamma, \alpha)
\end{aligned}$$

(v) For $\llbracket \Gamma \vdash A \leftrightarrow B \rrbracket(\gamma) = X \Rightarrow \llbracket \Gamma \vdash A \rrbracket(\gamma) = \llbracket \Gamma \vdash B \rrbracket(\gamma)$.

$$\begin{aligned}
&\llbracket \Gamma \vdash A \leftrightarrow B \rrbracket(\gamma)\\
&\quad = \llbracket \Gamma \vdash A \to B \rrbracket(\gamma) \sqcap \llbracket \Gamma \vdash B \to A \rrbracket(\gamma)\\
&\quad = a^b \sqcap b^a
\end{aligned}$$

Hence we have $a = b$ by Lemma 3.3 (7) since $a^b \sqcap b^a = X$.

(vi) For $\llbracket \Gamma \vdash x =_A y \rrbracket(\gamma) = X \Rightarrow \llbracket \Gamma \vdash x \rrbracket(\gamma) = \llbracket \Gamma \vdash y \rrbracket(\gamma)$.

$$\begin{aligned}
&\llbracket \Gamma \vdash x =_A y \rrbracket(\gamma)\\
&\quad = \llbracket \Gamma \vdash \forall Q : (A \to \mathrm{Prop}).Q\ x \leftrightarrow Q\ y \rrbracket(\gamma)\\
&\quad = \bigsqcap_{f : a \to \mathcal{O}(X)} \llbracket \Gamma ; (Q : A \to \mathrm{Prop}) \vdash Q\ x \leftrightarrow Q\ y \rrbracket(\gamma, f)
\end{aligned}$$

Since $\llbracket \Gamma \vdash x =_A y \rrbracket(\gamma) = X$ and Lemma 3.3 (8), we have the following fact:

$$\begin{aligned}
&\forall f : a \to \mathcal{O}(X),\\
&\quad \llbracket \Gamma ; (Q : A \to \mathrm{Prop}) \vdash Q\ x \leftrightarrow Q\ y \rrbracket(\gamma, f) = X
\end{aligned}$$

Therefore we have $f(\llbracket \Gamma \vdash x \rrbracket(\gamma)) = f(\llbracket \Gamma \vdash y \rrbracket(\gamma))$ for any function $f : a \to \mathcal{O}(X)$. Hence, the statement holds.

□

3.4 Soundness

We are now ready to prove the soundness of this type system.

Theorem 3.11 (soundness)**.** *We assume $\gamma \in \llbracket \Gamma \rrbracket$.*

(1) If $t_1 =_\beta t_2$, and $\Gamma \vdash t_1 : T, \Gamma \vdash t_2 : T$ are derivable, then $\llbracket \Gamma \vdash t_1 \rrbracket(\gamma) = \llbracket \Gamma \vdash t_2 \rrbracket(\gamma)$ when both sides are well defined.

(2) If $\Gamma \vdash t : T$ is derivable, then $\llbracket \Gamma \vdash t \rrbracket(\gamma) \in \llbracket \Gamma \vdash T \rrbracket(\gamma)$.

Proof.

(1) If t_1 is a proof term, then t_2 is also a proof term by Lemma 2.10, hence the statement holds. If not, it is sufficient that $\llbracket \Gamma \vdash (\lambda x : U.t)\ u \rrbracket(\gamma) = \llbracket \Gamma \vdash t[x \backslash u] \rrbracket(\gamma)$. By using Lemma 3.9,

$$\begin{aligned}
&\llbracket \Gamma \vdash (\lambda x : U.t)\ u \rrbracket(\gamma)\\
&\quad = \llbracket \Gamma \vdash \lambda x : U.t \rrbracket(\gamma)(\llbracket \Gamma \vdash u \rrbracket(\gamma))\\
&\quad = \llbracket \Gamma ; (x : U) \vdash t \rrbracket(\gamma, \llbracket \Gamma \vdash u \rrbracket(\gamma))\\
&\quad = \llbracket \Gamma \vdash t[x \backslash u] \rrbracket(\gamma)
\end{aligned}$$

Hence, the statement holds.

(2) This is proved by induction on the Typing Rules in Table 1. For details, see Appendix A.1. We must be careful in the case of Abstraction, i.e., $T = \forall x : A.B$ and $\mathbf{PT}_{\Gamma,x}(A, B) = \mathsf{TP}$. To prove the soundness, we need the following equation

$$\begin{aligned}
&\llbracket \Gamma \vdash \forall x : A.B \rrbracket(\gamma)\\
&\quad = \bigcap \{\llbracket \Gamma ; (x : A) \vdash B \rrbracket(\gamma, \alpha) | \alpha \in \llbracket \Gamma \vdash A \rrbracket(\gamma)\}.
\end{aligned}$$

This equation does not hold in general, however we can obtain it by assuming the point condition at p.

□

Corollary 3.12. *If P is a provable propositional term for Γ, then*

$$\forall \gamma \in \llbracket \Gamma \rrbracket, p \in \llbracket \Gamma \vdash P \rrbracket(\gamma)$$

holds.

4. Application

Let us compare Werner's classical model with our intuitionistic model on some simple cases.

4.1 Classical Model

We start with the simplest case. Let the topological space be the simplest one, which is the trivial topological space with its base set the singleton $\{a\}$.

$$\begin{aligned}
&X := \{a\}\\
&\mathcal{O}(X) := \{\varnothing, \{a\}\} \equiv \{0, 1\}\\
&p := a
\end{aligned}$$

This coincides with Werner's Model [14]. However this model is so coarse that it represents classical logic, since the principle of excluded middle holds.

$$a \in \llbracket \forall P : \mathrm{Prop}.P \vee \neg P \rrbracket = \bigsqcap_{o \in \mathcal{O}(X)} o \vee \neg o = 1.$$

If we want to be more discriminating, we need more open sets in $\mathcal{O}(X)$.

4.2 Models Disproving Excluded Middle

Now, let us consider the next simplest topological space. To do this, we add a new point 'b' and a new open set $\{a, b\}$ into the topological space.

$$\begin{aligned}
&X := \{a, b\},\\
&\mathcal{O}(X) := \{\varnothing, \{a\}, \{a, b\}\} \equiv \{0, 1, 2\},\\
&p := b.
\end{aligned}$$

Although this model stays simple, its topological space is fine enough to avoid the principle of excluded middle, since the following statement holds.

$$b \notin \llbracket \forall P : \mathrm{Prop}.P \vee \neg P \rrbracket = 1.$$

Table 3 Value of x^y for $X = \{a, b\}$.

x^y	0	1	2
0	2	0	0
1	2	2	1
2	2	2	2

Table 4 Value of x^y for $X = \{a, b, x\}$.

x^y	$\varnothing$	α	β	γ	X
$\varnothing$	X	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
α	X	X	α	α	α
β	X	β	X	β	β
γ	X	X	X	X	γ
X	X	X	X	X	X

This statement is derived by using the following equations.

$$\neg 0 = 2 \qquad \neg 1 = 0 \qquad \neg 2 = 0$$

By our soundness theorem, this proves that the principle of excluded middle cannot be deduced in $\mathrm{CC}^{\bar{\omega}}$.

Yet this model is not fully intutionistic as the linearity axiom $(P \to Q) \vee (Q \to P)$ holds, since we have the following fact by **Table 3**.

$$\begin{aligned}&[\![\forall P : \mathrm{Prop}.\forall Q : \mathrm{Prop}.(P \to Q) \vee (Q \to P)]\!]\\ &= \bigsqcap_{o_1, o_2 \in O(X)} o_1^{o_2} \vee o_2^{o_1}\\ &= 2.\end{aligned}$$

This is actually interesting because it shows that we can use this model to prove non trivial facts, for instance that the excluded middle cannot be deduced from the linearity axiom in $\mathrm{CC}^{\bar{\omega}}$. Indeed,

$$\begin{aligned}&[\![(\forall P : \mathrm{Prop}.\forall Q : \mathrm{Prop}.(P \to Q) \vee (Q \to P))\\ &\qquad \to \quad (\forall P : \mathrm{Prop}.P \vee \neg P)]\!] = 1.\end{aligned}$$

By our soundness theorem, this equation means that there is no term proving the above implication in $\mathrm{CC}^{\bar{\omega}}$.

By adding more elements we can refine the model further. Let

$$\begin{aligned}X &:= \{a, b, x\}\\ O(X) &:= \{\varnothing, \{a\}, \{b\}, \{a, b\}, \{a, b, x\}\}\\ &\equiv \{\varnothing, \alpha, \beta, \gamma, X\},\\ p &:= x.\end{aligned}$$

In this model, $(P \to Q) \vee (Q \to P)$ does not hold, since we have the following fact by **Table 4**.

$$x \notin [\![\forall P : \mathrm{Prop}.\forall Q : \mathrm{Prop}.(P \to Q) \vee (Q \to P)]\!] = \gamma$$

5. Reynolds' Paradox

There is a problem when expanding the set theoretical model, which is called Reynolds' paradox [11]. Basically Reynolds' paradox says that if the interpretation of an impredicative sort has more than one element, it causes a cardinality paradox in the set theoretical model. This seems to be in contradiction with our model, so in this section we will analyze its assumptions.

5.1 Outline of the Paradox

Let $\mathbb{J}$ be an impredicative sort, i.e., if $\Gamma \vdash A : s$ and $\Gamma; (x : A) \vdash B : \mathbb{J}$ are derivable for any sort s then $\Gamma \vdash \forall x : A.B : \mathbb{J}$ is derivable. We assume that there exists a type B whose sort is $\mathbb{J}$ such that $[\![B]\!]$ has at least two elements, i.e.,

$$\vdash B : \mathbb{J} \quad \mathit{and} \quad \sharp[\![B]\!] \geq 2.$$

In Ref. [11] Reynolds says that the existence of such a term B causes a paradox in set-theoretical models. First, we define the category $\mathbf{Sets}_{\mathbb{J}}$ and the endofunctor T of $\mathbf{Sets}_{\mathbb{J}}$.

Definition 5.1.

- *Let* $\mathbf{Sets}_{\mathbb{J}}$ *be a category with:*
  - $\mathrm{Obj}(\mathbf{Sets}_{\mathbb{J}}) := \{[\![P]\!] \mid \vdash P : \mathbb{J}$ *is derivable* $\}$
  - $\mathrm{Hom}([\![P_1]\!], [\![P_2]\!]) := [\![P_1]\!] \to [\![P_2]\!]$ $= \{f \mid f$ is a function from $[\![P_1]\!]$ to $[\![P_2]\!]\}$
- *Let* T *be a endofunctor of* $\mathbf{Sets}_{\mathbb{J}}$ *with*
  - $T([\![P]\!]) := ([\![P]\!] \to [\![B]\!]) \to [\![B]\!]$
  - $T(\rho) := h \in T([\![P_1]\!]) \mapsto \{(g, h(g \circ \rho)) | g \in [\![P_2]\!] \to [\![B]\!]\}$ *where* $\rho \in [\![P_1]\!] \to [\![P_2]\!]$

The paper [11] claims the following lemma:

Lemma 5.2.

- $\exists u \in \mathrm{Obj}(\mathbf{Sets}_{\mathbb{J}}), \exists H \in \mathrm{Hom}(Tu, u)$ *s.t.* $\forall s \in \mathrm{Obj}(\mathbf{Sets}_{\mathbb{J}}), \forall f \in \mathrm{Hom}(Ts, s), \exists! \rho \in \mathrm{Hom}(u, s)$ *s.t. following diagram commutes.*

$$\begin{tikzcd} Tu \arrow[r, "T\rho"] \arrow[d, "H"'] & Ts \arrow[d, "f"] \\ u \arrow[r, "\rho"] & s \end{tikzcd}$$

- *Tu and u are equivalent, i.e., $Tu \cong u$.*

By definition of endofunctor T, $\sharp[\![B]\!] \geq 2$ implies Tu and u have different cardinalities in spite of Tu and u being isomorphic. Therefore, the existence of a type B of impredicative sort such that $\sharp[\![B]\!] \geq 2$ causes a paradox.

5.2 Avoiding the Paradox

In $\mathrm{CC}^{\bar{\omega}}$, we have an impredicative sort Prop, and there is a type B of Prop such that $\sharp[\![B]\!] \geq 2$. However, this doesn't cause a paradox. In fact, to prove the existence of a function $H \in Tu \to u$, Reynolds constructs a term t of type $((P \to B) \to B) \to P$ in the proof of lemma 2 in Ref. [11], where P is a type such that $[\![P]\!] = u$. If $[\![(P \to B) \to B]\!]$ were interpreted as a set theoretical function space, it would cause a paradox in cardinality since $(P \to B) \to B \;\cong\; P$ by Lemma 5.2 and $\sharp[\![B]\!] \geq 2$. However in our model $[\![(P \to B) \to B]\!]$ is not a function space, i.e., it is not $([\![P]\!] \to [\![B]\!]) \to [\![B]\!]$, but just some open set of $(X, O(X))$:

$$[\![(P \to B) \to B]\!] = [\![B]\!]^{[\![B]\!]^{[\![P]\!]}} \in O(X)$$

since both P and B are propositional terms. Thus this discussion moves to the Heyting algebra part of the model where we need not fear such paradox.

6. Future Work

There are still three remaining questions we would like to answer in the future: whether the *point condition* is really needed to prove soundness; whether we can handle full CC^{ω}, without our restrictions on the type system, or even CIC, including inductive types; and how close to completeness is our model.

The point condition is very restrictive. It seems to require p to be an isolated point. Hence we would like to remove it to allow a wider variety of models. In fact we have not found any counterexample when removing the *point condition*, up to now.

We would also like to lift the restrictions on the PI-Type rule, which prohibits statements about proofs, and on the subtyping rule. They come from the fact that, in the interpretation of contexts, we use the strict interpretation, which restricts all propositional terms to either $\emptyset$ or the singleton $\{p\}$, so that we cannot build an element when the non-strict interpretation, while being non-empty, does not contain p. We have been considering several approaches to overcome this problem, with some success. While we are confident that this can be achieved, this seems to require more restrictions on the topological spaces one could use as model of propositions. We shall then consider adding inductive types (and their elimination schemes) to that more expressive interpretation.

While this model rejects the excluded middle, it still admits proof-irrelevance

$$\forall t_1, t_2, (t_1, t_2 \textit{ is proof term for } \Gamma)$$
$$\Rightarrow [\![\Gamma \vdash t_1]\!](\gamma) = [\![\Gamma \vdash t_2]\!](\gamma).$$

Since the existence of t such that following condition

$$\Gamma; (p_1 : P); (p_2 : P) \vdash t : p_1 =_P p_2$$
$$\text{(where } \Gamma \vdash P : \text{Prop is derivable)}$$

holds is not provable in general, this means that our model is not complete with respect to $\mathrm{CC}^{\bar{\omega}}$. We are now investigating whether completeness can be stated with respect to $\mathrm{CC}^{\bar{\omega}}$ extended with some axioms.

References

[1] Aczel, P. and Rathjen, M.: Notes on constructive set theory (2008).

[2] Barendregt, H.: Introduction to generalized type systems, *Journal of Functional Programming*, Vol.1, No.2, pp.125–154 (1991).

[3] Barendregt, H.: *Handbook of Logic in Computer Science* (*Vol.2*), chapter 2: Lambda calculus with types, Oxford University Press, Inc. (1992).

[4] Barras, B.: Sets in Coq, Coq in Sets, *Journal of Formalized Reasoning*, Vol.3, No.1, pp.29–48 (2010).

[5] Coquand, T. and Huet, G.: The calculus of constructions, *Information and Computation*, Vol.76, No.2, pp.95–120 (1988).

[6] Girard, J.-Y.: Proofs and types, Cambridge University Press (1989).

[7] Jacobs, B.: *Categorical Logic and Type Theory*, Studies in Logic and the Foundations of Mathematics, Vol.141, Elsevier (2001).

[8] Luo, Z.: A higher-order calculus and theory abstraction, *Information and Computation*, Vol.90, No.1, pp.107–137 (1991).

[9] MacLane, S. and Moerdijk, I.: *Sheaves in geometry and logic: A first introduction to topos theory*, Springer (1992).

[10] Miquel, A. and Werner, B.: The not so simple proof-irrelevant model of CC, *Types for Proof and Programs*, Springer LNCS, Vol.2426, pp.240–258 (2003).

[11] Reynolds, J.: Polymorphism is not set-theoretic, *Semantics of Data Types*, Springer LNCS, Vol.173, pp.145–156 (1984).

[12] Univalent Foundations Program: *Homotopy Type Theory: Univalent Foundations of Mathematics*, available from ⟨http://homotopytypetheory.org/book⟩, Institute for Advanced Study (2013).

[13] van Dalen, D.: Intuitionistic logic, *Handbook of Philosophical Logic*, Vol.III, pp.225–339 (1984).

[14] Werner, B.: Sets in types, types in sets, *Theoretical aspects of computer software*, Springer LNCS, Vol.1281, pp.530–546 (1997).

Appendix

A.1 Proof of Soundness

Theorem 3.11 (2). We assume that p is a reference point.

(1) Case of Axiom
$[\![\Gamma \vdash \text{Prop}]\!](\gamma) \in [\![\Gamma \vdash \text{Type}_i]\!](\gamma)$ is clear. Similarly, $[\![\Gamma \vdash \text{Type}_i]\!](\gamma) \in [\![\Gamma \vdash \text{Type}_{i+1}]\!](\gamma)$ is also clear.

(2) Case of Weakening
It is clear by Lemma 3.8.

(3) Case of Subtyping
The fact that $[\![\Gamma \vdash A]\!](\gamma) \in [\![\Gamma \vdash \text{Type}_i]\!](\gamma)$ implies $[\![\Gamma \vdash A]\!](\gamma) \in [\![\Gamma \vdash \text{Type}_{i+1}]\!](\gamma)$ is clear.

(4) Case of PI-Type
We will show the fact that

$$\begin{aligned}&(\forall \gamma, \alpha,\ [\![\Gamma \vdash A]\!](\gamma) \in [\![\Gamma \vdash s_1]\!](\gamma)\\ &\quad \land \quad [\![\Gamma; (x : A) \vdash B]\!](\gamma, \alpha) \in [\![\Gamma; (x : A) \vdash s_2]\!](\gamma, \alpha))\\ &\quad \Rightarrow \quad (\forall \gamma, [\![\Gamma \vdash \forall x : A.B]\!](\gamma) \in [\![\Gamma \vdash s_3]\!](\gamma)).\end{aligned}$$

There are three cases as follows.

- $\mathbf{PT}_{\Gamma,x}(A, B) = \mathsf{T}$
  By definition of the interpretation of judgment, the following equation
  $$[\![\Gamma \vdash \forall x : A.B]\!](\gamma) = \prod_{\alpha \in [\![\Gamma \vdash A]\!]'(\gamma)} [\![\Gamma; (x : A) \vdash B]\!](\gamma, \alpha)$$
  holds. There are the following two cases:
  - A is not a propositional term for Γ
    Since $[\![\Gamma \vdash A]\!](\gamma) \in \mathcal{U}(i)$, $[\![\Gamma; (x : A) \vdash B]\!](\gamma, \alpha) \in \mathcal{U}(j)$ for any γ, α and Lemma 3.6 (iii), we have
    $$\prod_{\alpha \in [\![\Gamma \vdash A]\!](\gamma)} [\![\Gamma; (x : A) \vdash B]\!](\gamma, \alpha) \in \mathcal{U}(\max(i, j)).$$
  - A is a propositional term for Γ
    Since $[\![\Gamma \vdash A]\!]'(\gamma) \in \mathcal{U}(j)$, $[\![\Gamma; (x : A) \vdash B]\!](\gamma, \alpha) \in \mathcal{U}(j)$ for any γ, α and Lemma 3.6 (iii), we have
    $$\prod_{\alpha \in [\![\Gamma \vdash A]\!]'(\gamma)} [\![\Gamma; (x : A) \vdash B]\!](\gamma, \alpha) \in \mathcal{U}(j).$$

  Hence, the statement holds.
- $\mathbf{PT}_{\Gamma,x}(A, B) = \mathsf{TP}$
  It is clear since $[\![\Gamma \vdash \forall x : A.B]\!](\gamma)$ is an open set by definition of the interpretation of judgment.
- $\mathbf{PT}_{\Gamma,x}(A, B) = \mathsf{PP}$
  It is clear since $[\![\Gamma \vdash \forall x : A.B]\!](\gamma)$ is an open set by definition of the interpretation of judgment.

(5) Case of Abstraction
We will show the fact that

$$\begin{aligned}&(\forall \gamma, \alpha,\ [\![\Gamma; (x : A) \vdash t]\!](\gamma, \alpha) \in [\![\Gamma; (x : A) \vdash B]\!](\gamma, \alpha)\\ &\quad \land \quad [\![\Gamma \vdash \forall x : A.B]\!](\gamma) \in [\![\Gamma \vdash s]\!](\gamma))\\ &\quad \Rightarrow \quad (\forall \gamma, [\![\Gamma \vdash \lambda x : A.t]\!](\gamma) \in [\![\Gamma \vdash \forall x : A.B]\!](\gamma)).\end{aligned}$$

There are three cases as follows.

- $\mathbf{PT}_{\Gamma,x}(A, B) = \mathsf{T}$
  By definition of the interpretation, we have the following equations:

$$\begin{aligned}&\llbracket \Gamma \vdash \lambda x : A.t \rrbracket(\gamma)\\ &\quad = \Big\{(\alpha, \llbracket \Gamma; (x : A) \vdash t \rrbracket(\gamma, \alpha)) \mid \alpha \in \llbracket \Gamma \vdash A \rrbracket'(\gamma)\Big\},\\ &\llbracket \Gamma \vdash \forall x : A.B \rrbracket(\gamma)\\ &\quad = \prod_{\alpha \in \llbracket \Gamma \vdash A \rrbracket'(\gamma)} \llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, \alpha).\end{aligned}$$

Then, we must prove the following equation:

$$\begin{aligned}&\Big\{(\alpha, \llbracket \Gamma; (x : A) \vdash t \rrbracket(\gamma, \alpha)) \mid \alpha \in \llbracket \Gamma \vdash A \rrbracket'(\gamma)\Big\}\\ &\qquad \in \prod_{\alpha \in \llbracket \Gamma \vdash A \rrbracket'(\gamma)} \llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, \alpha).\end{aligned}$$

But it is clear [*4] by induction of hypothesis.

- $\mathbf{PT}_{\Gamma,x}(A, B) = \mathsf{TP}$

  Since $\lambda x : A.t$ is a proof term, we have following equations

  $$\llbracket \Gamma \vdash \lambda x : A.t \rrbracket(\gamma) = p.$$

  Hence, the fact we must prove is

  $$p \in \llbracket \Gamma \vdash \forall x : A.B \rrbracket(\gamma).$$

  By definition we have the following equation.

  $$\begin{aligned}&\llbracket \Gamma \vdash \forall x : A.B \rrbracket(\gamma)\\ &\quad = \bigsqcap \{\llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, \alpha) \mid \alpha \in \llbracket \Gamma \vdash A \rrbracket(\gamma)\}.\end{aligned}$$

  If $\llbracket \Gamma \vdash A \rrbracket(\gamma)$ is the empty set, then the statement holds since $\llbracket \Gamma \vdash \forall x : A.B \rrbracket(\gamma) = X$ by Lemma 3.3 (5). We assume that $\llbracket \Gamma \vdash A \rrbracket(\gamma)$ is a non-empty set. We have

  $$\forall \alpha \in \llbracket \Gamma \vdash A \rrbracket(\gamma), p \in \llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, \alpha).$$

  since $\llbracket \Gamma; (x : A) \vdash t \rrbracket(\gamma, \alpha) = p$. Therefore, we have the following equation:

  $$p \in \bigcap \{\llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, \alpha) \mid \alpha \in \llbracket \Gamma \vdash A \rrbracket(\gamma)\}.$$

  However $\bigsqcap S \neq \bigcap S$ hold in general, since $\bigsqcap S$ is the interior of $\bigcap S$ when S is non empty subset of X. Now, we apply the point condition here [*5]. We have

  $$\begin{aligned}&\llbracket \Gamma \vdash \forall x : A.B \rrbracket(\gamma)\\ &\quad = \bigsqcap \{\llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, \alpha) \mid \alpha \in \llbracket \Gamma \vdash A \rrbracket(\gamma)\}\\ &\quad = \bigcap \{\llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, \alpha) \mid \alpha \in \llbracket \Gamma \vdash A \rrbracket(\gamma)\}\end{aligned}$$

  since $\bigcap \{\llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, \alpha) \mid \alpha \in \llbracket \Gamma \vdash A \rrbracket(\gamma)\}$ is an open set by the point condition. Hence, the condition holds in this case.

- $\mathbf{PT}_{\Gamma,x}(A, B) = \mathsf{PP}$

  Since $\lambda x : A.B$ is a proof term, we have the following equation

  $$\llbracket \Gamma \vdash \lambda x : A.t \rrbracket(\gamma) = p.$$

  Hence, the fact we must prove is

  $$p \in \llbracket \Gamma \vdash \forall x : A.B \rrbracket(\gamma)$$

  By definition of the interpretation of judgment, we have

  $$\llbracket \Gamma \vdash \forall x : A.B \rrbracket(\gamma) = \Big(\llbracket \Gamma \vdash B \rrbracket(\gamma)\Big)^{\llbracket \Gamma \vdash A \rrbracket(\gamma)}.$$

  By characteristic of Heyting algebra,

  $$\llbracket \Gamma \vdash B \rrbracket(\gamma) \subset \llbracket \Gamma \vdash \forall x : A.B \rrbracket(\gamma).$$

  By induction hypothesis $p \in \llbracket \Gamma \vdash B \rrbracket(\gamma)$, so that the condition holds in this case.

(6) Case of Apply

We will show the fact that

$$\begin{aligned}&(\forall \gamma,\ \llbracket \Gamma \vdash u \rrbracket(\gamma) \in \llbracket \Gamma \vdash \forall x : A.B \rrbracket(\gamma)\\ &\quad \wedge\ \ \llbracket \Gamma \vdash v \rrbracket(\gamma) \in \llbracket \Gamma \vdash A \rrbracket(\gamma))\\ &\quad \Rightarrow\ \ (\forall \gamma, \llbracket \Gamma \vdash u\ v \rrbracket(\gamma) \in \llbracket \Gamma \vdash B[x \backslash v] \rrbracket(\gamma)).\end{aligned}$$

There are three cases as follows.

- $\mathbf{PT}_{\Gamma,x}(A, B) = \mathsf{T}$

  By definition of the interpretation of judgment, the following equation

  $$\begin{aligned}&\llbracket \Gamma \vdash u\ v \rrbracket(\gamma) = \llbracket \Gamma \vdash u \rrbracket(\gamma)(\llbracket \Gamma \vdash v \rrbracket(\gamma))\\ &\llbracket \Gamma \vdash u \rrbracket(\gamma) \in \prod_{\alpha \in \llbracket \Gamma \vdash A \rrbracket'(\gamma)} \llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, \alpha)\end{aligned}$$

  holds. Therefore, we have

  $$\llbracket \Gamma \vdash u\ v \rrbracket(\gamma) \in \llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, \llbracket \Gamma \vdash v \rrbracket(\gamma)).$$

  By Lemma 3.9, we have

  $$\llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, \llbracket \Gamma \vdash v \rrbracket(\gamma)) = \llbracket \Gamma \vdash B[x \backslash v] \rrbracket(\gamma).$$

  Hence, the statement holds in this case.

- $\mathbf{PT}_{\Gamma,x}(A, B) = \mathsf{TP}$

  It suffices to show that $p \in \llbracket \Gamma \vdash B[x \backslash v] \rrbracket(\gamma)$, since $\llbracket \Gamma \vdash u \rrbracket(\gamma) = \llbracket \Gamma \vdash u\ v \rrbracket(\gamma) = p$ holds. By induction hypothesis, we have the following equation

  $$p \in \bigsqcap \{\llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, \alpha) \mid \alpha \in \llbracket \Gamma \vdash A \rrbracket(\gamma)\}.$$

  This equation implies the fact that

  $$\forall \alpha \in \llbracket \Gamma \vdash A \rrbracket(\gamma), p \in \llbracket \Gamma; (x : A) \vdash B \rrbracket(\gamma, \alpha).$$

  By Lemma 3.9 and the fact $\llbracket \Gamma \vdash v \rrbracket(\gamma) \in \llbracket \Gamma \vdash A \rrbracket(\gamma)$, we have

  $$p \in \llbracket \Gamma \vdash B[x \backslash v] \rrbracket(\gamma).$$

  Hence, the statement holds in this case.

- $\mathbf{PT}_{\Gamma,x}(A, B) = \mathsf{PP}$

  It suffices to show that $p \in \llbracket \Gamma \vdash B \rrbracket(\gamma)$, since $\llbracket \Gamma \vdash u \rrbracket(\gamma) = \llbracket \Gamma \vdash v \rrbracket(\gamma) = \llbracket \Gamma \vdash u\ v \rrbracket(\gamma) = p$ holds and the variable x does not appear freely in B. The following equation holds.

  $$\llbracket \Gamma \vdash \forall x : A.B \rrbracket(\gamma) = \Big(\llbracket \Gamma \vdash B \rrbracket(\gamma)\Big)^{\llbracket \Gamma \vdash A \rrbracket(\gamma)}$$

  By definition of Heyting algebra, we have

  $$\llbracket \Gamma \vdash \forall x : A.B \rrbracket(\gamma) \cap \llbracket \Gamma \vdash A \rrbracket(\gamma) \subset \llbracket \Gamma \vdash B \rrbracket(\gamma).$$

  Then we have

[*4] If $\llbracket \Gamma \vdash A \rrbracket'(\gamma)$ is the empty set, then $\llbracket \Gamma \vdash \forall x : A.B \rrbracket(\gamma) = \{\emptyset\}$ and $\llbracket \Gamma \vdash \lambda x : A.t \rrbracket(\gamma) = \emptyset$ hold.

[*5] This is the only place we need it in the proof.

$$p \in [\![\Gamma \vdash B]\!](\gamma).$$

by Lemma 3.9. Hence, the statement holds in this case.

(7) Case of Variable

We must show that

$$\begin{aligned}&(\forall\gamma, [\![\Gamma \vdash A]\!](\gamma) \in [\![\Gamma \vdash s]\!](\gamma))\\ &\Rightarrow \forall\gamma,\alpha, [\![\Gamma; (x : A) \vdash x]\!](\gamma,\alpha) \in [\![\Gamma; (x : A) \vdash A]\!](\gamma,\alpha).\end{aligned}$$

It is clear by definition of $[\![\Gamma]\!]$.

(8) Case of Beta Equality

We must show that

$$\begin{aligned}&\forall\gamma,\ [\![\Gamma \vdash t]\!](\gamma) \in [\![\Gamma \vdash A]\!](\gamma),\ [\![\Gamma \vdash B]\!](\gamma) \in [\![\Gamma \vdash s]\!](\gamma)\\ &\wedge\ A =_\beta B\\ &\Rightarrow\ \forall\gamma, [\![\Gamma \vdash t]\!](\gamma) \in [\![\Gamma \vdash B]\!](\gamma).\end{aligned}$$

It is clear by Theorem 3.11 (1).

□

Masahiro Sato received his M.Sc. and D.Sc. degree from the Graduate School of Mathematics, Nagoya University in 2011 and 2015. His research interests include type theory and intuitionistic logic. He is a member of the Mathematical Society of Japan.

Jacques Garrigue received his M.Sc. degree from University Paris 7 in 1992, and D.Sc. degree from the University of Tokyo in 1995. He is alumnus of École Normale Supérieure in Paris. He was Research Associate at Kyoto University from 1995 to 2004, and has been Associate Professor at Nagoya University since October 2004. His interests are in the theory of programming languages, particularly type systems and proof of programs. He is a member of IPSJ, JSSST and ACM.