Mathematical Structures in Computer Science (2023), **33**, pp. 1–32
doi:10.1017/S0960129523000087

PAPER

An intuitionistic set-theoretical model of fully dependent CC$^\omega$

Masahiro Sato[1] and Jacques Garrigue[2,*]

[1]SIOS Technology, Inc., 2-12-3 Minami-Asabu, Minato-ku, Tokyo 106-0047, Japan
[2]Graduate School of Mathematics, Nagoya University, Chikusa-ku, Nagoya 464-8602, Japan
[*]Corresponding author. Email: garrigue@math.nagoya-u.ac.jp

(Received 19 October 2020; revised 29 September 2022; accepted 18 January 2023; first published online 17 April 2023)

Abstract

Werner's set-theoretical model is one of the simplest models of CIC. 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 $P \vee \neg P$ holds. Following our previous work, we interpret Prop into a topological space (a special case of Heyting algebra) to make the model more intuitionistic without sacrificing simplicity. We improve on that work by providing a full interpretation of dependent product types, using Alexandroff spaces. We also extend our approach to inductive types by adding support for lists.

Keywords: type theory, model, intuitionistic logic

1. Introduction

There are various models of type theory. Werner's set-theoretical model (Werner 1997) provides an intuitive model of CIC. 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 $P \vee \neg P$ holds in it.

In this paper, we construct a set-theoretical model of CC$^\omega$ in which the principle of excluded middle does not hold, making it closer to completeness.

CC (the Calculus of Constructions, Coquand and Huet 1988) is a pure type system (Barendregt 1991) with two sorts, impredicative $*$ and predicative $\Box$. CC$^\omega$ replaces $\Box$ by a cumulative hierarchy of predicative sorts Type$_i$. CIC (the Calculus of Inductive Constructions) adds inductive types to CC$^\omega$.

Werner (1997) provided 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 (Reynolds 1984). Therefore, the model for Prop is two-valued. Hence, the principle of excluded middle is valid in this model, making it classical. Later, Miquel and Werner (2003) have shown that proving the soundness of this model was not as easy as it seems, but this does not change the simplicity of the model itself. This simple approach is to be contrasted with Luo's model of ECC (CC$^\omega$ extended with strong sums $\Sigma x : A.B$) which uses ω-sets (Luo 1991), syntactic models based on combinatory logic (Geuvers 2001; Stefanova and Geuvers 1995), or more recent models such as categorical models (Jacobs 2001; Streicher 1991) or models based on homotopy theory (Univalent

Foundations Program 2013). 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^{ω}.

Our goal has been to recover the intuitionistic part of CC^{ω} without increasing the complexity of the model. Barras (2010) provided a first way to do it, by interpreting CC^{ω} in IZF (intuitionistic Zermelo–Fraenkel set theory, Aczel and Rathjen 2010) 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.

This leaves the question of how to interpret proofs, in a way that makes the whole interpretation coherent. In our previous work (Sato and Garrigue 2016), propositions were already interpreted as open sets, but proofs were interpreted by a fixed value, that had to be included in all true propositions. This choice was too inflexible to accomodate propositions parameterized over proofs, which we had to reject. While this type of parameterization is rare, it is for instance required to express proof-irrelevance as a proposition. In this paper, we are able to lift this restriction by shifting the interpretation to Alexandroff spaces (Arenas 1999), and making the interpretation of proofs a function of the context valuation. Alexandroff spaces act as parameters to the model, their choice making it more or less precise. For instance, if we use the trivial topological space $(X, \mathscr{O}(X))$ where $X = \{\cdot\}$ is a singleton and $\mathscr{O}(X) = \{\varnothing, X\}$, we obtain a model of classical logic, which is the coarsest one.

Our model is still proof irrelevant, as it does not depend on the the proof term itself. As a result, this model does validate some propositions that are not provable, in particular logical proof irrelevance, hence it does not reach completeness. However, this is sufficient to exclude many classical propositions such as the principle of excluded middle $P \vee \neg P$ or the linearity axiom $(P \to Q) \vee (Q \to P)$.

Note that, in this paper, we choose a slightly restricted version of CC^{ω}, which omits subsumption between universes `Prop` and $\texttt{Type}_i$. Subsumption between the predicative universes $\texttt{Type}_i$ poses no problem, but our model of propositions is too different to allow subsumption between `Prop` and $\texttt{Type}_i$. Werner (2008) omitted this same subsumption in his exploration of proof irrelevance.

This model can also be extended to inductive types. To demonstrate it, we define a model of lists, with principles for recursion (in $\texttt{Type}_0$) and induction (in `Prop`), and extend our soundness proof to those. This is one more step in the direction of a model for the full CIC.

In Section 2, we define the language of the type system CC^{ω}. In Section 3, we give our set-theoretical interpretation of CC^{ω} and prove its soundness. In Section 4, we study some properties of this model. For instance, we show that it satisfies proof irrelevance, and that the excluded middle cannot be derived from the linearity axiom in CC^{ω}. In Section 5, we extend our interpretation to inductive types. Finally, we conclude and discuss some future directions.

2. Typing of CC^{ω}

2.1 Definition of CC^{ω}

We define the type system CC^{ω} as follows. The only deviation from the standard presentation is that our version has no subsumption between `Prop` and $\texttt{Type}_i$.

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

$$[\,] \vdash \texttt{Prop} : \texttt{Type}_0 \qquad (\text{Axiom-}\texttt{Prop})$$

$$[\,] \vdash \texttt{Type}_i : \texttt{Type}_{i+1} \qquad (\text{Axiom-}\texttt{Type})$$

$$\frac{\Gamma \vdash t : T \quad \Gamma \vdash A : s \quad x \notin \mathrm{dom}(\Gamma)}{\Gamma; (x : A) \vdash t : T} \qquad (\text{Weakening})$$

$$\frac{\Gamma \vdash A : s_1 \quad \Gamma; (x : A) \vdash B : s_2 \quad (s_1, s_2) \in \{\texttt{Prop}, \texttt{Type}_i\} \times \{\texttt{Prop}, \texttt{Type}_i\}}{\Gamma \vdash \forall x : A.B : s_2} \qquad (\text{PI-Type})$$

$$\frac{\Gamma; (x : A) \vdash t : B \quad \Gamma \vdash \forall x : A.B : s}{\Gamma \vdash \lambda x : A.t : \forall x : A.B} \qquad (\text{Abstraction})$$

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

$$\frac{\Gamma \vdash A : s \quad x \notin \mathrm{dom}(\Gamma)}{\Gamma; (x : A) \vdash x : A} \qquad (\text{Variable})$$

$$\frac{\Gamma \vdash t : A \quad \Gamma \vdash B : s \quad A =_\beta B}{\Gamma \vdash t : B} \qquad (\text{Beta Equality})$$

$$\frac{\Gamma \vdash t : \forall x_1 : A_1, \ldots, \forall x_n : A_n, \texttt{Type}_i \quad i < j}{\Gamma \vdash t : \forall x_1 : A_1, \ldots, \forall x_n : A_n, \texttt{Type}_j} \qquad (\text{Subsumption})$$

Figure 1. Typing rules of CC$^\omega$.

Definition 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* $\mathrm{fv}\,(T_1) \cup (\mathrm{fv}\,(T_2) \setminus \{x\})$.
- *The symbols* $\texttt{Prop}$ *and* $\texttt{Type}_i$ *(for $i = 0, 1, 2, \ldots$) are terms with free variables $\varnothing$.*

$\texttt{Prop}$ and $\texttt{Type}_i$ are called *sorts*. $\texttt{Prop}$ is called the impredicative sort and it represents the type of all propositions.

Definition 2 (Context).

- $[\,]$ *is a context with domain* $\mathrm{dom}\,([\,]) = \varnothing$.
- *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* $\mathrm{dom}\,(\Gamma) \cup \{x\}$.

Figure 1 contains the typing rules of CC$^\omega$. The metavariables s, s_1, s_2 denote sorts. In rule (PI-Type), either $s_1 = s_2$ or one of them is $\texttt{Prop}$. The equality $=_\beta$ denotes *beta equality* and $B[x \backslash v]$ denotes *substitution*. Here are their definitions. We assume that α-conversion occurs when needed.

Definition 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 $y[x\backslash v] = \begin{cases} v & (y = x) \\ y & (\mathit{otherwise}), \end{cases}$

(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) $s[x\backslash v] = s$ *where s is a sort.*

Definition 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* $\forall x : A.B =_\beta \forall x : A' B'$.

Now that we have defined CC$^\omega$'s terms and typing rules, we show the following three lemmas that will be used in proofs. They can be proved by induction over the typing rules above.

Lemma 5 (Uniqueness of Typing). *If $\Gamma \vdash t : A$ and $\Gamma \vdash t : B$ are derivable, then either $A =_\beta B$, or $A =_\beta \forall x_1 : A_1, \ldots, \forall x_n : A_n, \mathtt{Type}_i$ and $B =_\beta \forall x_1 : A_1, \ldots, \forall x_n : A_n, \mathtt{Type}_j$.*

Lemma 6 (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 7 (Extended 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 $\Gamma_1; \Delta; \Gamma_2 \vdash \mathtt{Type}_i : \mathtt{Type}_{i+1}$ is derivable.*

Lemma 8 (Condensing Lemma). *If $\Gamma; (x : A); \Delta \vdash t : T$ is derivable and x does not occurs in Δ, t and T, then $\Gamma; \Delta \vdash t : T$ is derivable.*

Proof. See Jiménez (1999). □

2.2 Propositional terms and proof terms

In CC$^\omega$, propositions are types that belong to the impredicative sort Prop, and proofs are terms of types that represent propositions. Next, we give a definition of propositions and proofs through syntactic derivability. Rather than introducing an explicitly sorted type system like in Miquel and Werner (2003), 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 9.

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

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

(2) Proof Term
A term p is called a proof term for Γ iff $\Gamma \vdash p : P$ is derivable for some P that is a propositional term for Γ. P is then called a provable propositional term for Γ.

Lemma 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.*
(v) *If t is a proof term for Γ, then there does not exist a term T such that $\Gamma \vdash t : T$ and $\Gamma \vdash T : \mathtt{Type}_i$ are both derivable.*

Proof terms and propositional terms are preserved under substitution. The following lemmas express this fact.

Lemma 11. *If $\Gamma \vdash t : T$ is derivable, then $\Gamma \vdash T : s$ for some sort s.*

Lemma 12. *We assume that $\Gamma \vdash u : U$ is derivable and p is well typed under $\Gamma; (x : U); \Delta$.*

(i) *If p is a proof (resp. propositional) term for the context $\Gamma; (x : U); \Delta$, then $p[x\backslash u]$ is a proof (resp. propositional) term for the context $\Gamma;\Delta[x\backslash u]$.*
(ii) *If p is not a proof term for the context $\Gamma; (x : U); \Delta$, then $p[x\backslash u]$ is not a proof term for the context $\Gamma; \Delta[x\backslash u]$.*

Proof. (i) is clear by Lemma 6. We will show (ii). Since p is well typed, there exists a type T such that

$$\Gamma; (x : U); \Delta \vdash p : T$$

and by Lemma 11 there exists a sort s such that

$$\Gamma; (x : U); \Delta \vdash T : s$$

Since p is not a proof term for the context $\Gamma; (x : U); \Delta$, we have that $s \neq \mathtt{Prop}$, and as a result there exists an index i such that $s = \mathtt{Type}_i$. Hence by Lemma 6,

$$\Gamma; \Delta[x\backslash u] \vdash p[x\backslash u] : T[x\backslash u]$$
$$\Gamma; \Delta[x\backslash u] \vdash T[x\backslash u] : \mathtt{Type}_i$$

hold. If there exists a term P such that

$$\Gamma; \Delta[x\backslash u] \vdash p[x\backslash u] : P$$
$$\Gamma; \Delta[x\backslash u] \vdash P : \mathtt{Prop},$$

it implies a contradiction by Lemma 10 (v). □

Note that the fact that P is not a propositional term for $\Gamma; (x : U); \Delta$ does not imply that $P[x\backslash u]$ is not a propositional term for $\Gamma; \Delta[x\backslash u]$ in general. Here is a counterexample.

$$\Gamma; (U : \mathtt{Type}_i); (P : U) \vdash P : U$$
$$\Gamma \vdash \mathtt{Prop} : \mathtt{Type}_i$$

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

In this case, P is not a propositional term. However $P[U\backslash\mathtt{Prop}] = P$ is a propositional term under $\Gamma; (P : \mathtt{Prop})$.

Lemma 13. *We assume that p is well typed under* $\Gamma_1; \Gamma_2$ *and* $\Gamma_1; \Delta; \Gamma_2$. *p is a proof (resp. propositional) term for the context* $\Gamma_1; \Gamma_2$ *if and only if p is a proof (resp. propositional) term for the context* $\Gamma_1;\Delta; \Gamma_2$.

The function $\mathbf{PT}_{\Gamma,x}(A, B)$ maps two types A and B into the string symbols $\{\mathsf{PP}, \mathsf{TP}, \mathsf{PT}, \mathsf{TT}\}$ according to their sorts. Its goal is to give different interpretations to $\forall x : A.B$.

Definition 14 (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. We define:*

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

Again, $\mathbf{PT}_{\Gamma,x}(A, B)$ is stable under substitution and weakening.

Lemma 15.

(i) If A and B are typable under $\Gamma; (x : U); \Delta$ *and* $\Gamma \vdash u : U$ *is derivable, 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 $(\Gamma; (x : U); \Delta; (a : A))$. By Lemma 12, $A[x\backslash u]$ is a proposition for $(\Gamma; \Delta[x\backslash u])$ and $B[x\backslash u]$ is also a proposition for $(\Gamma; \Delta[x\backslash u]; (a : A[x\backslash u]))$. Hence, the statement holds in this case. When $\mathbf{PT}_{\Gamma;\,(x:U);\, \Delta,a}(A, B) = \mathsf{TP}$, $\Gamma; \Delta[x\backslash u] \vdash A[x\backslash u] : \mathtt{Type}_i$ is derivable. 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.

□

2.3 Logical symbols

Lastly, here are some notations allowing to use other logical symbols (Barendregt 1992). We shall use them to prove the adequacy of our model with respect to intuitionistic logic.

Definition 16.

$$\begin{aligned} A \to B &:= \forall x : A.B \qquad (\textit{when } x \notin fv(B)), \\ \bot &:= \forall P : \mathtt{Prop}.P, \\ \neg A &:= A \to \bot, \\ A \wedge B &:= \forall P : \mathtt{Prop}.(A \to B \to P) \to P, \\ A \vee B &:= \forall P : \mathtt{Prop}.(A \to P) \to (B \to P) \to P, \\ \exists x : A.Q &:= \forall P : \mathtt{Prop}.(\forall x : A.(Q \to P)) \to P, \end{aligned}$$

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

$$A \leftrightarrow B := (A \to B) \wedge (B \to A),$$
$$x =_A y := \forall Q : (A \to \mathtt{Prop}).Q\,x \to Q\,y.$$

3. Interpretation

3.1 Preparation of the interpretation

3.1.1 Heyting algebras

Several interpretations of type theory have been proposed such as using ω-sets (Luo 1991) or coherent spaces (Girard 1989). In this paper, we use *Heyting algebras* (MacLane and Moerdijk 1992; van Dalen 1984) 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 18), and as such provide models of intuitionistic logic too (van Dalen 1984). We give a definition of lattice and Heyting algebra as follows.

Definition 17 (Lattices and Heyting algebras)**.** *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.*[1] *A lattice is also called a* complete lattice *if every subset S of A has a supremum "$\bigsqcup S$" and an infimun '$\bigsqcap S$'. A complete lattice has a minimum element $\mathbb{O} := \bigsqcup \varnothing$ and a maximum element $\mathbb{I} := \bigsqcap \varnothing$. If a (complete) 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 (complete) Heyting Algebra.

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

Lemma 18. *Any topological space $(X, \mathcal{O}(X))$ is a complete Heyting algebra.*

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

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

□

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

Lemma 19. *Let $(A, \leq)$ be a complete Heyting algebra. Then the following conditions hold.*

$$(x^b)^a = x^{a \sqcap b}, \tag{1}$$
$$\bigsqcap\{t \mid t \in A\} = \varnothing, \tag{2}$$
$$\bigsqcap\{t^{t^a} \mid t \in A\} = a, \tag{3}$$

$$x^a \sqcap x^b = x^{a \sqcup b}, \tag{4}$$

$$\bigsqcap\{a^t \mid t \in S\} = a^{\bigsqcup S}, \tag{5}$$

$$x^1 = x, \tag{6}$$

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

$$x \sqcap y^x \leq y, \tag{8}$$

$$x \neq \varnothing \Rightarrow \varnothing^x = \varnothing \tag{9}$$

$$x^y \sqcap y^x = 1 \Rightarrow x = y, \tag{10}$$

3.1.2 Alexandroff spaces

Following in the steps of our previous work (Sato and Garrigue 2016), our interpretation avoids the Reynolds' Paradox by not looking inside proof terms. In that previous work, this was done by interpreting all proof terms as a single point, the *reference point*. Soundness then required this reference point to be included in the interpretation of all propositions in the context, which forced us to restrict the type system.

In this paper, a proof term is again interpreted into an element of an open set. However, we make the interpretation of proofs a function of the context, which allows us to overcome this restriction. For soundness to stand, we must then assume that the proof we interpret uses all proofs in the context, which means that its interpretation should be smaller, in some "dependency order," than their interpretations. For this we need to introduce an order on the elements of our topological space and ensure that there is always an infimum. Alexandroff spaces (Arenas 1999) allow us to define such an order on points, so that we just need to require the existence of the infimum.

Definition 20 (Alexandroff Space)**.** *A topological space $(X, \mathcal{O}(X))$ is an Alexandroff space iff the intersection of any tribe of open set is also an open set, i.e.*

$$\bigcap S \in \mathcal{O}(X) \quad \textit{for any } S \subset \mathcal{O}(X)$$

The definition of Alexandroff space can also be given by the following equivalent statement.

Lemma 21 (Minimal Neighborhood)**.** *A topological space $(X, \mathcal{O}(X))$ is an Alexandroff space iff any point has a minimal neighborhood. The minimal neighborhood of the point x is denoted by $\downarrow x$.*

These are the basic definitions for Alexandroff spaces. However, to prove our soundness theorem later, we need more conditions. We state those as *well behaved* Alexandroff spaces.

Definition 22 (Well Behaved Alexandroff Space)**.** *An Alexandroff space $(X, \mathcal{O}(X))$ is well behaved if the following conditions hold.*

- *For any finite subset $\{t_1, t_2, \cdots, t_n\}$ of X, we can choose a point $t \in X$ such that*

$$\downarrow t_1 \cap \downarrow t_2 \cap \cdots \cap \downarrow t_n = \downarrow t$$

  holds. We write such a point t as $\inf\{t_1, t_2, \cdots, t_n\}$.
- *There exists an element $\bot_X \in X$ such that any inhabited open set contains it, i.e.*

$$\forall O \in \mathcal{O}(X), O \textit{ is inhabited} \Rightarrow \bot_X \in O.$$

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

To clarify the use of the notation of the minimal neighborhood $\downarrow x$ and $\bot_X$, let us discuss a preordered (i.e. reflexivity and transitivity hold) set generated from an Alexandroff space. Let $\leq$ be the relation on X defined as follows.

$$a \leq b \quad \overset{\text{def}}{=} \quad \forall O \in \mathscr{O}(X), b \in O \Rightarrow a \in O$$

The relation $\leq$ is a preorder. Moreover, if this Alexandroff space is a T_0 space (i.e. it fulfills the T_0 separation axiom), then the generated preorder $(X, \leq)$ becomes an order (the antisymmetry condition holds). If the relation $(X, \leq)$ generated from an Alexandroff space forms an ordered set, then the followings hold.

$$\begin{aligned} \downarrow x &= \{t \in X \mid t \leq x\} \\ \bot_X &= \min X \end{aligned}$$

Using an ordered Alexandroff space for X allows us to give multiple interpretations of proofs in the typing context, whereas in our previous work (Sato and Garrigue 2016) we used a fixed point $p \in X$. This fixed point was required to satisfy a *point condition*, which was no other than the existence of a minimal neighborhood, satisfied by every point in an Alexandroff space.

3.1.3 Dependent function and universes

Definition 23 (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*

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

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 the sort $\mathtt{Type}_i$.

Definition 24 (Grothendieck Universe). *We define a ith Grothendieck Universe $\mathscr{U}_i$ (for i any natural number) as*

$$\mathscr{U}_i := V_{\lambda_i},$$

where a set V_α, with an ordinal number α, is recursively defined as follows

$$\begin{aligned} V_0 &= \varnothing, \\ V_{\alpha+1} &= \mathscr{P}(V_\alpha), \\ V_\alpha &= \bigcup_{\beta<\alpha} V_\beta \quad \text{(when } \alpha \text{ is a limit ordinal)}, \end{aligned}$$

and λ_i is the ith inaccessible cardinal.

The class of all universes is well founded for the relation $\in$. We write $\mathscr{U}_i$ as the ith universe. Note that $\mathscr{U}_i$ is so large that it cannot be constructed in ZFC without assuming an inaccessible cardinal. Our interpretation uses $\mathscr{U}_i$ for all $i \in \mathbf{N}$. The following lemma is necessary when proving soundness.

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

Lemma 25. *The followings hold for any i.*

(i) $A \in \mathscr{U}_i$ *implies* $A \subset \mathscr{U}_i$.
(ii) $A \in \mathscr{U}_i$ *and* $B_\alpha \in \mathscr{U}_i$ *for all* $\alpha \in A$ *imply* $\prod\limits_{\alpha \in A} B_\alpha \in \mathscr{U}_i$.
(iii) $x \in \mathscr{U}_i$ *and* $y \subset x$ *imply* $y \in \mathscr{U}_i$.
(iv) $\mathscr{U}_i \subset \mathscr{U}_{i+1}$.

3.2 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 interpretation of application and product types. The interpretation of application depends on whether the argument is a proof term or not, and may be undefined. We shall later prove that every time we use it, we actually have $\mathsf{app}_{\Gamma,v}(f, a) = f(a)$.

Definition 26.

$$\mathsf{app}_{\Gamma,v}(f,a) := \begin{cases} f(\bot_X) \\ \quad (v \textit{ is a proof term for } \Gamma \\ \qquad \textit{and } f \textit{ is a function whose domain contains } a \textit{ and } \bot_X) \\ f(a) \\ \quad (v \textit{ is not a proof term for } \Gamma \\ \qquad \textit{and } f \textit{ is a function whose domain contains } a) \\ \mathsf{undefined} \\ \quad (\textit{otherwise}) \end{cases}$$

$$\mathsf{prod}_{\mathsf{X}}(\mathscr{A}, \{\mathscr{B}(\alpha)\}_{\alpha\in\mathscr{A}}) := \begin{cases} \left(\prod\{\mathscr{B}(\alpha) \mid \alpha \in \mathscr{A}\}\right)^{\mathscr{A}} \\ \quad (\textit{when } \mathsf{X} = \mathsf{PP}) \\ \prod\{\mathscr{B}(\alpha) \mid \alpha \in \mathscr{A}\} \\ \quad (\textit{when } \mathsf{X} = \mathsf{TP}) \\ \{f \in \prod_{\alpha\in\mathscr{A}} \mathscr{B}(\alpha) \mid f \textit{ is a constant function}\} \\ \quad (\textit{when } \mathsf{X} = \mathsf{PT}) \\ \prod_{\alpha\in\mathscr{A}} \mathscr{B}(\alpha) \\ \quad (\textit{when } \mathsf{X} = \mathsf{TT}) \end{cases}$$

Now, we define the (partial) interpretations of contexts $[\![-]\!]$ and judgments $[\![- \vdash -]\!]$. The former is by induction on the length of the context and the latter by induction on the structure of terms. Note that the interpretation of judgments does not rely on the interpretation of contexts.

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

Definition 27 (interpretation). *Let $(X, \mathscr{O}(X)) \in \mathscr{U}_0$ be a well-behaved Alexandroff space.*

(i) 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.

(ii) Definition of the interpretation of a judgment $[\![\Gamma \vdash t]\!]$
If t is a proof term for $\Gamma = (x_1 : T_1); \cdots ; (x_n : T_n)$, then

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

where

$$\lfloor \gamma_1, \gamma_2, \cdots, \gamma_n \rfloor := \inf\{\gamma_i \mid x_i \text{ is a proof under } \Gamma\}.$$

Otherwise, if $\Gamma \vdash t : T$ is derivable and T is not a proposition for Γ, then

$$\begin{aligned} [\![\Gamma \vdash \mathtt{Type}_i]\!](\gamma) &:= \mathscr{U}_i \\ [\![\Gamma \vdash \mathtt{Prop}]\!](\gamma) &:= \mathscr{O}(X) \\ [\![(x_1 : T_1); \cdots ; (x_n : T_n) \vdash x_i]\!](\gamma_1, \cdots, \gamma_n) &:= \gamma_i \\ [\![\Gamma \vdash \forall x : A.B]\!](\gamma) &:= \mathsf{prod}_{\mathsf{X}}\left(\mathscr{A}, \{\mathscr{B}(\alpha)\}_{\alpha \in \mathscr{A}}\right) \\ & \quad \text{where} \\ & \quad \begin{cases} \mathsf{X} := \mathbf{PT}_{\Gamma,x}(A, B) \\ \mathscr{A} := [\![\Gamma \vdash A]\!](\gamma) \\ \mathscr{B}(\alpha) := [\![\Gamma; (x:A) \vdash B]\!](\gamma, \alpha) \end{cases} \\ [\![\Gamma \vdash \lambda x : A.t]\!](\gamma) &:= \left\{\left(\alpha, [\![\Gamma; (x:A) \vdash t]\!](\gamma, \alpha)\right) \mid \alpha \in [\![\Gamma \vdash A]\!](\gamma)\right\} \\ [\![\Gamma \vdash u\, v]\!](\gamma) &:= \mathsf{app}_{\Gamma,v}([\![\Gamma \vdash u]\!](\gamma), [\![\Gamma \vdash v]\!](\gamma)) \end{aligned}$$

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 $[\![\Gamma \vdash t]\!](\gamma)$ – soundness will tell us that if $\Gamma \vdash t : T$, then $[\![\Gamma \vdash t]\!](\gamma) \in [\![\Gamma \vdash T]\!](\gamma)$.

Concerning Definitions 26 and 27, most cases are similar to Werner's interpretation, and we explained $\mathsf{app}_{\Gamma,v}$ above, so we only explain the interpretations of proof terms and PI-Types $\forall x : A.B$.

The interpretation of a proof term $[\![\Gamma \vdash p]\!](\gamma)$ is the minimum element of the set of proof values in γ. Since each of these values belong to the interpretations of propositions in the context, which are open sets in our Alexandroff space, this minimum element belongs to all of them. This will allow us to prove that any proof variable belongs to the interpretation of its type, which is key to the soundness theorem.

$\mathsf{prod}_{\mathsf{X}}$ has four cases, according to $\mathsf{X} = \mathbf{PT}_{\Gamma,x}(A, B)$. When $\mathsf{X} = \mathsf{PP}$, we use the Heyting algebra representation of this implication. If x does not appear in B, the interpretation of $[\![\Gamma \vdash \forall x : A.B]\!]$ is $\mathscr{B}^{\mathscr{A}}$, which represents the logical implication $A \Rightarrow B$, as will be proved in Corollary 28. If x appears in B, we still have the same meaning, since $\mathscr{B}(\alpha)$ does not depend on α, as will be proved in

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

Lemma 31. This definition also works if $\mathscr{A}$ is empty, as the empty meet is X, and $X^{\emptyset}$ is X again (the top element of the lattice). In our previous work, α was required to be the (fixed) interpretation of a proof term, meaning that we could not interpret the case where $\mathscr{A}$ was not empty, but did not contain the reference point used for proof terms. Here we do not have such a problem, as the interpretation of proof terms is a function of the context; thanks to the interpretation with well behaved Alexandroff spaces, there is always a value small enough to serve as proof term.

When $\mathsf{X} = \mathsf{TP}$, the interpretation of $[\![\Gamma \vdash \forall x : A.B]\!]$ represents universal quantification, and again we use the infinite meet operator of the complete Heyting algebra to express it.

When $\mathsf{X} = \mathsf{PT}$, the interpretation of $[\![\Gamma \vdash \forall x : A.B]\!]$ becomes a set theoretical constant function. Functions whose argument are proofs should be constant functions since our model is proof-irrelevant. Note that here again, it follows from Lemma 31 that $\mathscr{B}(\alpha)$ shall not depend on α.

In the last case, when $\mathsf{X} = \mathsf{TT}$, the representation becomes a set theoretical dependent function.

As soon as one component is $\mathsf{undefined}$ the whole interpretation is $\mathsf{undefined}$. Thanks to Corollary 28 which is a consequence of the Soundness Theorem 33, $\mathsf{undefined}$ never appears, and implication and application can be defined in a straightforward way.

Corollary 28.

- *If $\Gamma \vdash t$ is well typed, then $[\![\Gamma \vdash t]\!]$ is a total function whose domain is $[\![\Gamma]\!]$.*
- *If $\mathbf{PT}_{\Gamma,x}(A, B) = \mathsf{PP}$ and $[\![\Gamma \vdash A]\!](\gamma) \neq \varnothing$, then*

$$[\![\Gamma \vdash \forall x : A.B]\!](\gamma) = \Big([\![\Gamma; (x : A) \vdash B]\!](\gamma, \alpha)\Big)^{[\![\Gamma \vdash A]\!](\gamma)}$$

  holds for any $\alpha \in [\![\Gamma \vdash A]\!](\gamma)$.
- *If $\mathbf{PT}_{\Gamma,x}(A, B) = \mathsf{PP}$ and $[\![\Gamma \vdash A]\!](\gamma) = \varnothing$, then*

$$[\![\Gamma \vdash \forall x : A.B]\!](\gamma) = X$$

  holds.
- *If $\Gamma \vdash t_1\ t_2$ is well typed and t_1 is not a proof term for Γ, then $[\![\Gamma \vdash t_1]\!](\gamma)$ is a function whose domain contains $[\![\Gamma \vdash t_2]\!](\gamma)$ and*

$$[\![\Gamma \vdash t_1\ t_2]\!](\gamma) = [\![\Gamma \vdash t_1]\!](\gamma)\Big([\![\Gamma \vdash t_2]\!](\gamma)\Big)$$

  holds.

3.3 Soundness

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

Lemma 29 (interpretation of weakening). *If t is not a proof term, then the following equation holds*

$$[\![\Gamma_1; \Gamma_2 \vdash t]\!](\gamma_1, \gamma_2) = [\![\Gamma_1; (x' : A'); \Gamma_2 \vdash t]\!](\gamma_1, \alpha', \gamma_2)$$

when both sides are well defined.

Proof. See Appendix A. □

Our substitution lemma is similar to those in Werner (1997) and Miquel and Werner (2003).

Lemma 30 (interpretation of substitution)**.** *We assume $\Gamma \vdash u : U$ is derivable. If $\Gamma; (x : U); \Delta$ is well formed and*

$$(\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta) \in [\![\Gamma; (x : U); \Delta]\!]$$

holds (with all interpretations defined), then

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

holds. Moreover, in

$$[\![\Gamma; (x : U); \Delta \vdash t]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta) = [\![\Gamma; \Delta[x\backslash u] \vdash t[x\backslash u]]\!](\gamma, \delta)$$

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. See Appendix B. □

While propositions can be interpreted by sets with multiple values, our interpretation is still proof-irrelevant, as the interpretation of terms of sort `Type` does not depend on the parameters of sort `Prop`. This simplifies the proof of the next lemma.

Lemma 31 (semantic proof irrelevance)**.** *We assume that A' is a propositional term for Γ and t is not a proof term under $\Gamma; (x' : A'); \Delta$. If*

$$(\gamma, p_1, \delta) \in [\![\Gamma; (x' : A'); \Delta]\!]$$
$$(\gamma, p_2, \delta) \in [\![\Gamma; (x' : A'); \Delta]\!]$$

hold, then

$$[\![\Gamma; (x' : A'); \Delta \vdash t : T]\!](\gamma, p_1, \delta) = [\![\Gamma; (x' : A'); \Delta \vdash t : T]\!](\gamma, p_2, \delta)$$

holds.

Proof. See Appendix C. □

Theorem 32 (soundness of beta equality)**.** *If $t_1 =_\beta t_2$, and $\Gamma \vdash t_1 : T$, $\Gamma \vdash t_2 : T$ are derivable, then $[\![\Gamma \vdash t_1]\!](\gamma) = [\![\Gamma \vdash t_2]\!](\gamma)$ when both sides are well defined.*

Proof. If t_1 is a proof term, then t_2 is also a proof term by Lemma 10, hence the statement holds. If not, it is sufficient to only prove that $[\![\Gamma \vdash (\lambda x : U.t)\, u]\!](\gamma) = [\![\Gamma \vdash t[x\backslash u]]\!](\gamma)$ holds. If $(\lambda x : U.t)u$ is well typed under Γ, then $\Gamma \vdash u : U$ is derivable. If u is not a proof term, then

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

holds by Lemma 30. If u is a proof term, then $[\![\Gamma \vdash \lambda x : U.t]\!](\gamma)$ is a function whose domain contains $[\![\Gamma \vdash u]\!](\gamma)$ by definition of the interpretation. Therefore, $[\![\Gamma; (x : U) \vdash t]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma))$ is also well defined. Hence,

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

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

$$= [\![\Gamma; (x : U) \vdash t]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma))$$
$$= [\![\Gamma \vdash t[x\backslash u]]\!](\gamma)$$

holds by Lemmas 30 and 31. Hence, the statement holds. □

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

Theorem 33 (soundness). *We assume $\gamma \in [\![\Gamma]\!]$. If $\Gamma \vdash t : T$ is derivable, then $[\![\Gamma \vdash t]\!](\gamma) \in [\![\Gamma \vdash T]\!](\gamma)$.*

Proof. See Appendix D. □

4. Properties of the Model

4.1 Interpretation of logical symbols

The following theorem explicits the interpretation of logical symbols from Definition 16. It demonstrates the logical adequacy of the interpretation.

Theorem 34 (interpretation of logical symbols). *Here, let A and B be propositional terms and T be any (propositional or non propositional) term.*

(i) $[\![\Gamma \vdash A \to B]\!](\gamma) = [\![\Gamma \vdash B]\!](\gamma)^{[\![\Gamma \vdash A]\!](\gamma)}$
(ii) $[\![\Gamma \vdash \bot]\!](\gamma) = \varnothing$
(iii) $[\![\Gamma \vdash A \wedge B]\!](\gamma) = ([\![\Gamma \vdash A]\!](\gamma)) \sqcap ([\![\Gamma \vdash B]\!](\gamma))$
(iv) $[\![\Gamma \vdash A \vee B]\!](\gamma) = ([\![\Gamma \vdash A]\!](\gamma)) \sqcup ([\![\Gamma \vdash B]\!](\gamma))$
(v) $[\![\Gamma \vdash \exists x : A.B]\!](\gamma) = \begin{cases} [\![\Gamma \vdash A]\!](\gamma) \sqcap [\![\Gamma; x : A \vdash B]\!](\gamma, \alpha) & (\alpha \in [\![\Gamma \vdash A]\!](\gamma)) \\ \varnothing & ([\![\Gamma \vdash A]\!](\gamma) = \varnothing) \end{cases}$
(vi) *When T is not a propositional term:*
$[\![\Gamma \vdash \exists x : T.B]\!](\gamma) = \bigsqcup_{\alpha \in [\![\Gamma \vdash T]\!](\gamma)} [\![\Gamma; (x : T) \vdash B]\!](\gamma, \alpha)$
(vii) a. $[\![\Gamma \vdash x =_T y]\!](\gamma) = X$ *iff* $[\![\Gamma \vdash x]\!](\gamma) = [\![\Gamma \vdash y]\!](\gamma)$
b. $[\![\Gamma \vdash x =_T y]\!](\gamma) = \varnothing$ *iff* $[\![\Gamma \vdash x]\!](\gamma) \neq [\![\Gamma \vdash y]\!](\gamma)$
(viii) a. $[\![\Gamma \vdash A =_{\mathtt{Prop}} B]\!](\gamma) \subset [\![\Gamma \vdash A \leftrightarrow B]\!](\gamma)$
b. $[\![\Gamma \vdash A \leftrightarrow B]\!](\gamma) = X$ *implies* $[\![\Gamma \vdash A =_{\mathtt{Prop}} B]\!](\gamma) = X$

Proof. See Appendix E □

Here some consequences of Theorem 34.

Corollary 35.

(1) $[\![\Gamma \vdash x =_T y \vee x \neq_T y]\!](\gamma) = X$
(2) $[\![\Gamma \vdash A \leftrightarrow B]\!](\gamma) = X$ *iff* $[\![\Gamma \vdash A =_{\mathtt{Prop}} B]\!](\gamma) = X$.
(3) $[\![\Gamma \vdash A \leftrightarrow B]\!](\gamma) = \varnothing$ *implies* $[\![\Gamma \vdash A =_{\mathtt{Prop}} B]\!](\gamma) = \varnothing$

Note that the reverse of (3) in Corollary 35 is not true in general, i.e. there are cases such that $[\![\Gamma \vdash A \leftrightarrow B]\!](\gamma) \neq \varnothing$ holds while $[\![\Gamma \vdash A =_{\mathtt{Prop}} B]\!](\gamma) = \varnothing$ holds. This fact means that the propositional extensionality axiom does not always hold in this model, as detailed later.

Table 1. Value of y^x for $X = \{\varnothing, \{\varnothing\}\}$

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

4.2 Interpretation of excluded middle and linearity

Our original goal was to provide intuitionistic models of CC$^\omega$. We will see here that by changing the topological space used by the interpretation, one can change the validity of axioms.

4.2.1 Classical model

We start with the simplest case. Let us consider the trivial topological space, whose base set is the singleton $\{\varnothing\}$.

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

This topological space is a well-behaved Alexandroff space and coincides with Werner's model (Werner 1997). However, this model is so coarse that it represents classical logic, since the principle of excluded middle holds.

$$\varnothing \in [\![\forall P : \mathtt{Prop}.P \vee \neg P]\!] = \bigsqcap_{o \in \mathcal{O}(X)} o \vee \neg o = 1.$$

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

4.2.2 Models disproving excluded middle

Now, let us consider the next simplest topological space, which contains another element.

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

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

$$2 \notin [\![\forall P : \mathtt{Prop}.P \vee \neg P]\!] = 1.$$

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 CC$^\omega$.

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 1.

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

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

Table 2. Value of y^x for $X = \{b, l, r, t\}$

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

The above remark 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 CC^ω. Indeed,

$$[\![(\forall P : \texttt{Prop}.\forall Q : \texttt{Prop}.(P \to Q) \vee (Q \to P)) \to (\forall P : \texttt{Prop}.P \vee \neg P)]\!] = 1.$$

By our soundness theorem, this equation means that there is no term proving the above implication in CC^ω.

4.2.3 Models disproving linearity

By adding more elements we can refine the model further. Let $(X, \mathscr{O}(X))$ be the Alexandroff space

$$\begin{aligned} X &:= \{b, l, r, t\} \\ \mathscr{O}(X) &= \{\varnothing, \{b\}, \{b, l\}, \{b, r\}, \{b, l, r\}, X\} \\ &\equiv \{\varnothing, \alpha, \beta, \gamma, \delta, X\} \end{aligned}$$

In this model, $(P \to Q) \vee (Q \to P)$ does not hold, since we have the following fact by Table 2.

$$t \notin [\![\forall P : \texttt{Prop}.\forall Q : \texttt{Prop}.(P \to Q) \vee (Q \to P)]\!] = \alpha$$

4.3 Interpretation of logical proof irrelevance

A general form of proof irrelevance, which does not depend on the type of the result, can be expressed as a logical formula, using the propositional encoding for equality:

$$\vdash \forall P : \texttt{Prop}.\forall p_1, p_2 : P.\ p_1 =_P p_2.$$

Proposition 36 (interpretation of proof irrelevance). *The logical formula for proof irrelevance is valid for any Alexandroff space.*

Proof. We shall prove that for any topological space $(X, \mathscr{O}(X))$, the interpretation of this formula is X. First note that, for any valuation γ,

$$[\![P : \texttt{Prop}; p_1 : P; p_2 : P \vdash p_1]\!](\gamma) = \lfloor \gamma \rfloor = [\![P : \texttt{Prop}; p_1 : P; p_2 : P \vdash p_2]\!](\gamma).$$

By using (vii) from Theorem 34, we have

$$[\![P : \texttt{Prop}; p_1 : P; p_2 : P \vdash p_1 =_P p_2]\!](\gamma) = X.$$

As a result,

$$\begin{aligned}&[\![\forall P:\mathtt{Prop}.\forall p_1,p_2:P.p_1=_P p_2]\!]\\&=\prod_{o\in\mathscr{O}(X)}\ \prod_{x_1,x_2\in o}[\![P:\mathtt{Prop};p_1:P;p_2:P\vdash p_1=_P p_2]\!](o,x_1,x_2)\\&=\prod_{o\in\mathscr{O}(X)}\ \prod_{x_1,x_2\in o}X\\&=X.\end{aligned}$$

□

Note that semantic proof irrelevance (Lemma 31) and logical proof irrelevance (Proposition 36) are quite different. The former is about equality of interpretations of non-proof terms under different valuations, while the latter uses the equality of interpretations of proof terms under the same valuation. As a result, their proofs are independent.

4.4 Interpretation of propositional extensionality

As a notable property, propositional extensionality does not hold in general in our model.

The classical model, which was presented in Section 4.2.1, validates propositional extensionality, but any model disproving the excluded middle invalidates it.

Let us recall the model of Section 4.2.2. We assume that $\Gamma\vdash A:\mathtt{Prop}$ and $\Gamma\vdash B:\mathtt{Prop}$ are derivable and

$$\begin{aligned}[\![\Gamma\vdash A]\!](\gamma)&=1\\ [\![\Gamma\vdash B]\!](\gamma)&=2\end{aligned}$$

hold. In this case,

$$\begin{aligned}[\![\Gamma\vdash A\leftrightarrow B]\!](\gamma)&=[\![\Gamma\vdash B]\!](\gamma)^{[\![\Gamma\vdash A]\!](\gamma)}\sqcap[\![\Gamma\vdash A]\!](\gamma)^{[\![\Gamma\vdash B]\!](\gamma)}\\&=1\end{aligned}$$

holds. Since $[\![\Gamma\vdash A]\!](\gamma)\neq[\![\Gamma\vdash B]\!](\gamma)$, then we have $[\![\Gamma\vdash A=_{\mathtt{Prop}}B]\!](\gamma)=0$. Therefore,

$$\begin{aligned}[\![\Gamma\vdash(A\leftrightarrow B)\to A=_{\mathtt{Prop}}B]\!](\gamma)&=0^1\\&=0\end{aligned}$$

holds by (9) in Lemma 19. Hence, propositional extensionality does not hold in this model.

More generally, the followings holds.

Proposition 37. *In any nonclassical model, i.e. any model which has more than 2 open sets, the following holds.*

$$[\![\vdash\forall P_1P_2:\mathtt{Prop}.(P_1\leftrightarrow P_2)\to P_1=_{\mathtt{Prop}}P_2]\!]=\varnothing$$

Proof.

$$\begin{aligned}&[\![\vdash\forall P_1P_2:\mathtt{Prop}.(P_1\leftrightarrow P_2)\to P_1=_{\mathtt{Prop}}P_2]\!]\\&=\prod_{S_1,S_2\in\mathscr{O}(X)}[\![P_1:\mathtt{Prop},P_2:\mathtt{Prop}\vdash(P_1\leftrightarrow P_2)\to P_1=_{\mathtt{Prop}}P_2]\!](S_1,S_2)\\&=\prod_{S_1,S_2\in\mathscr{O}(X)}\left([\![P_1:\mathtt{Prop};P_2:\mathtt{Prop}\vdash P_1=_{\mathtt{Prop}}P_2]\!](S_1,S_2)\right)^{{S_2}^{S_1}\sqcap{S_1}^{S_2}}\end{aligned}$$

$$
\begin{aligned}
&= \bigsqcap_{\substack{S_1,S_2\in\mathscr{O}(X)\\ S_1\neq S_2}} \left([\![P_1 : \texttt{Prop}; P_2 : \texttt{Prop} \vdash P_1 =_{\texttt{Prop}} P_2]\!](S_1, S_2)\right)^{{S_2}^{S_1}\sqcap {S_1}^{S_2}}\\
&= \bigsqcap_{\substack{S_1,S_2\in\mathscr{O}(X)\\ S_1\neq S_2}} \varnothing^{{S_2}^{S_1}\sqcap {S_1}^{S_2}}
\end{aligned}
$$

Here, we can choose $S_1 = \downarrow\perp$ and $S_2 = X$. Since S_1 is then the smallest nonempty open set and S_2 the biggest, they cannot be equal as it would contradict the existence of at least 3 open sets. Since $X^{(\downarrow\perp)} \sqcap (\downarrow\perp)^X \neq \varnothing$, the interpretation equals to $\varnothing$. □

4.5 Interpretation of the axiom of choice

If we choose ZFC as ambient logic for our interpretation, then it validates the Axiom of Choice for any topological space $(X, \mathscr{O}(X))$. That is, if $\Gamma \vdash A : \texttt{Type}_i$, $\Gamma \vdash B : \texttt{Type}_j$, and $\Gamma \vdash R : A \to B \to \texttt{Prop}$ are derivable, then

$$[\![\Gamma \vdash \forall x : A.\exists y : B.R\,x\,y \to \exists f : A \to B.\forall x : A.R\,x\,(f\,x)]\!](\gamma) = X$$

holds. Now, let us consider the interpretation of the Axiom of Choice. We pose:

$$
\begin{aligned}
S &:= [\![\Gamma \vdash A]\!](\gamma)\\
T &:= [\![\Gamma \vdash B]\!](\gamma)\\
\Theta &:= [\![\Gamma \vdash R]\!](\gamma).
\end{aligned}
$$

Then we have:

$$
\begin{aligned}
[\![\Gamma \vdash \forall x : A.\exists y : B.R\,x\,y]\!] &= \bigsqcap_{s\in S}\bigsqcup_{t\in T}\Theta(s,t)\\
[\![\Gamma \vdash \exists f : A \to B.\forall x : A.R\,x\,(f\,x)]\!] &= \bigsqcup_{\psi\in S\to T}\bigsqcap_{s\in S}\Theta(s,\psi(s)).
\end{aligned}
$$

Under ZFC set theory,

$$\bigsqcap_{s\in S}\bigsqcup_{t\in T}\Theta(s,t) \subset \bigsqcup_{\psi\in S\to T}\bigsqcap_{s\in S}\Theta(s,\psi(s))$$

is true. Therefore, the Axiom of Choice is valid by Lemma 19 (7).

This may look surprising as Diaconescu's Theorem states that, in set theory, the Axiom of Choice implies the excluded middle.

However, it has been observed that to prove the excluded middle, one needs in general more properties: propositional extensionality and functional extentionality (Forster 2021; van den Berg 2007). In our model, functional extensionality is still valid, but propositional extensionality is not valid, as mentioned in Section 4.4. Hence, we obtain a model in which the Axiom of Choice is valid without necessarily implying the excluded middle.

5. Interpretation of Inductive Types

Until now, we have discussed the interpretation of CC^ω. However, Coq's type system is not CC^ω but CIC, which is CC^ω extended with (co)inductive types. In this paper, we do not give a general definition of inductive types, but we present some examples of inductive definitions. Here, we introduce a new type system $CC^\omega_{\mathsf{list}}$, which is CC^ω with the list type.

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

$$[\,] \vdash \mathsf{list} : \mathtt{Type}_0 \to \mathtt{Type}_0 \qquad (\mathsf{list}\text{-intro})$$

$$[\,] \vdash \mathsf{nil} : \forall A : \mathtt{Type}_0 . \mathsf{list}\, A \qquad (\mathsf{nil}\text{-intro})$$

$$[\,] \vdash \mathsf{cons} : \forall A : \mathtt{Type}_0 . A \to \mathsf{list}\, A \to \mathsf{list}\, A \qquad (\mathsf{cons}\text{-intro})$$

$$\begin{array}{l} [\,] \vdash \mathsf{list\_rec} : \forall A : \mathtt{Type}_0 . \forall F : \mathsf{list}\, A \to \mathtt{Type}_0 . \\ \qquad F\ (\mathsf{nil}\, A) \to (\forall a : A. \forall l : \mathsf{list}\, A. F\ l \to F\ (\mathsf{cons}\, A\ a\ l)) \to \forall l : \mathsf{list}\, A. F\ l \end{array} \qquad (\mathsf{list\_rec}\text{-intro})$$

$$\begin{array}{l} [\,] \vdash \mathsf{list\_ind} : \forall A : \mathtt{Type}_0 . \forall P : \mathsf{list}\, A \to \mathtt{Prop} . \\ \qquad P\ (\mathsf{nil}\, A) \to (\forall a : A. \forall l : \mathsf{list}\, A. P\ l \to P\ (\mathsf{cons}\, A\ a\ l)) \to \forall l : \mathsf{list}\, A. P\ l \end{array} \qquad (\mathsf{list\_ind}\text{-intro})$$

Figure 2. New typing rules of $\mathrm{CC}^{\omega}_{\mathsf{list}}$.

5.1 Typing rule of $\mathrm{CC}^{\omega}_{\mathsf{list}}$

To construct the new type system $\mathrm{CC}^{\omega}_{\mathsf{list}}$, we add new terms and typing rules to CC^{ω}. Here, we give five new terms, list, nil, cons, list_rec, and list_ind, and also give new typing rules for the list type in Figure 2.

Now, we define the beta equality for $\mathrm{CC}^{\omega}_{\mathsf{list}}$.

Definition 38 (Beta Equality for $\mathrm{CC}^{\omega}_{\mathsf{list}}$). *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* $\forall x : A.B =_{\beta'} \forall x : A'B'$.
(v) $\mathsf{list\_rec}\ A\ F\ t_1\ t_2\ (\mathsf{nil}\ A) =_{\beta'} t_1$
(vi) $\mathsf{list\_rec}\ A\ F\ t_1\ t_2\ (\mathsf{cons}\ A\ a\ l) =_{\beta'} t_2\ a\ l\ (\mathsf{list\_rec}\ A\ F\ t_1\ t_2\ l)$
(vii) $\mathsf{list\_ind}\ A\ F\ t_1\ t_2\ (\mathsf{nil}\ A) =_{\beta'} t_1$
(viii) $\mathsf{list\_ind}\ A\ F\ t_1\ t_2\ (\mathsf{cons}\ A\ a\ l) =_{\beta'} t_2\ a\ l\ (\mathsf{list\_ind}\ A\ F\ t_1\ t_2\ l)$

Now that we defined $\mathrm{CC}^{\omega}_{\mathsf{list}}$'s terms and typing rules, we can define some familiar operators over list type, such as membership operator 'in' for instance.

$$\begin{array}{l} \mathsf{in} : \forall A : \mathtt{Type}_0 . A \to \mathsf{list}\, A \to \mathtt{Prop} := \\ \quad \lambda A : \mathtt{Type}_0 .\ \lambda a : A.\ \lambda l : \mathsf{list} A. \\ \qquad (\mathsf{list\_rec}\ A\ (\lambda\_ : \mathsf{list}\, A.\ \mathtt{Prop}) \\ \qquad\quad \mathrm{False} \\ \qquad\quad (\ \lambda x : A.\ \lambda\_ : \mathsf{list}\, A.\ \lambda \mathsf{ind} : \mathtt{Prop}.\ x = a \vee \mathsf{ind}\ ) \\ \qquad\quad l) \end{array}$$

We can then derive the following equalities from Definition 38.

- $\mathsf{in}\ A\ a\ (\mathsf{nil}\ A) =_{\beta'} \mathrm{False}$
- $\mathsf{in}\ A\ a\ (\mathsf{cons}\ A\ x\ l) =_{\beta'} x = a \vee \mathsf{in}\ A\ a\ l$

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

5.2 Interpretation

Here, we define an interpretation of $\mathrm{CC}^{\omega}_{\mathsf{list}}$. The interpretation of lists is obtained through an initial algebra construction. We fix an arbitrary element denoted by the dot symbol "$\cdot$" to interpret the unit type. We can then define the interpretations of list, nil, cons, $\mathsf{list\_rec}$ and $\mathsf{list\_ind}$ as follows.

(I) Interpretation of list.
First, we define the Kleene closure S^* of a set S as follows.

$$S^* := \bigcup_{n\in\omega} S^n$$

where S^n is an n-tuple of S, i.e.

$$\begin{aligned} S^0 &:= \{(0,\cdot)\} \\ S^{n+1} &:= \{(1,(a,l)) \mid a\in S \text{ and } l \in S^n\}. \end{aligned}$$

Then list is interpreted as a function building the Kleene closure of a set.

$$[\![\Gamma \vdash \mathsf{list}]\!](\gamma) := \{(S, S^*) \mid S \in \mathscr{U}_0\}$$

We can easily check that

$$[\![\Gamma \vdash \mathsf{list}]\!](\gamma) \in [\![\Gamma \vdash \mathtt{Type}_0 \to \mathtt{Type}_0]\!](\gamma)$$

holds for any $\gamma \in [\![\Gamma]\!]$.

(II) Interpretation of nil.
nil is interpreted by the constant function returning "$(0,\cdot)$".

$$[\![\Gamma \vdash \mathsf{nil}]\!](\gamma) := \{(S, (0,\cdot)) \mid S \in \mathscr{U}_0\},$$

We can again easily check that

$$[\![\Gamma \vdash \mathsf{nil}]\!](\gamma) \in [\![\Gamma \vdash \forall A : \mathtt{Type}_0, \mathsf{list} A]\!](\gamma)$$

holds since $(0,\cdot)\in S^*$ for any set S.

(III) Interpretation of cons.
First, we define cons_S as follows

$$\mathsf{cons}_S := \{(s,(l,(1,s,l))) \mid s \in S \text{ and } l \in S^*\}$$

for any set S. We can easily check that

$$\mathsf{cons}_S \in S \to S^* \to S^*$$

holds. Now, we can define the interpretation of cons as follows.

$$[\![\Gamma \vdash \mathsf{cons}]\!](\gamma) := \{(S, \mathsf{cons}_S) \mid S \in \mathscr{U}_0\}$$

We can again easily check that

$$[\![\Gamma \vdash \mathsf{cons}]\!](\gamma) \in [\![\Gamma \vdash \forall A : \mathtt{Type}_0, A \to \mathsf{list}\, A \to \mathsf{list}\, A]\!](\gamma)$$

holds.

(IV) Interpretation of $\mathsf{list\_rec}$.
Given a function $T : S^* \to \mathscr{U}_0$, we define the dependent function $\mathrm{rec}^{(n)}_{t,f} \in \prod_{l\in S^n} T(l)$ by recursion on natural numbers.

$$\begin{aligned} \mathrm{rec}^{(0)}_{t,f} &:= \{((0,\cdot),t)\} \\ \mathrm{rec}^{(n+1)}_{t,f} &:= \{((1,(a,l)), f(a)(l)(\mathrm{rec}^{(n)}_{t,f}(l))) \mid a \in S \text{ and } l \in S^n\} \end{aligned}$$

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

where t is an element of $T((0, \cdot))$ and f is a dependent function

$$f \in \prod_{a \in S} \prod_{l \in S^*} \Big(T(l) \to T((1, (a, l)))\Big).$$

Next, we define $\mathrm{rec}_{t,f} \in \prod_{l \in S^*} T(l)$ as follows.

$$\mathrm{rec}_{t,f} := \bigcup_{n \in \omega} \mathrm{rec}^{(n)}_{t,f}$$

Finally, we define $\mathsf{list\_rec}$ as follows.

$$\begin{aligned}[\![\Gamma \vdash \mathsf{list\_rec}]\!](\gamma) := \{(S, (T, (t, (f, \mathrm{rec}_{t,f})))) \mid\ & \\ & S \in \mathscr{U}_0 \\ & T \in S^* \to \mathscr{U}_0 \\ & t \in T((0, \cdot)) \\ & f \in \prod_{a \in S} \prod_{l \in S^*} \Big(T(l) \to T((1, (a, l)))\Big)\}\end{aligned}$$

We can again easily check that

$$\begin{aligned}&[\![\Gamma \vdash \mathsf{list\_rec}]\!](\gamma) \in [\![\Gamma \vdash \\ &\quad \forall A : \mathsf{Type}_0 . \forall F : \mathsf{list} A \to \mathsf{Type}_0 . \\ &\qquad F(\mathsf{nil}\ A) \to (\forall a : A . \forall l : \mathsf{list} A . F\, l \to F\,(\mathsf{cons}\ A\ a\ l)) \to \forall l : \mathsf{list}\ A . F\, l \\ &]\!](\gamma)\end{aligned}$$

holds.

(V) Interpretation of $\mathsf{list\_ind}$.
The interpretation of $\mathsf{list\_ind}$ is much simpler. Since $\mathsf{list\_ind}$ is a proof term, its interpretation must be

$$[\![\Gamma \vdash \mathsf{list\_ind}]\!](\gamma) := \lfloor \gamma \rfloor.$$

For the soundness theorem, we shall prove that

$$\begin{aligned}&[\![\Gamma \vdash \mathsf{list\_ind}]\!](\gamma) \in [\![\Gamma \vdash \\ &\quad \forall A : \mathsf{Type}_0 . \forall P : \mathsf{list} A \to \mathtt{Prop}. \\ &\qquad P(\mathsf{nil}\ A) \to (\forall a : A . \forall l : \mathsf{list} A . P\, l \to P\,(\mathsf{cons}\ A\ a\ l)) \to \forall l : \mathsf{list}\ A . P\, l \\ &]\!](\gamma)\end{aligned}$$

holds. This is a corollary of Lemma 40.

It remains to prove the soundness of $\mathrm{CC}^{\omega}_{\mathsf{list}}$.

Theorem 39 (soundness for $\mathrm{CC}^{\omega}_{\mathsf{list}}$). *(1) If $t_1 =_{\beta'} t_2$ holds and $\Gamma \vdash t_1 : T$ and $\Gamma \vdash t_2 : T$ are derivable, then $[\![\Gamma \vdash t_1]\!](\gamma) = [\![\Gamma \vdash t_2]\!](\gamma)$ holds.*
(2) If $\Gamma \vdash t : T$ is derivable in $\mathrm{CC}^{\omega}_{\mathsf{list}}$, then $[\![\Gamma \vdash t]\!](\gamma) \in [\![\Gamma \vdash T]\!](\gamma)$ holds.

To prove (1), we need a $\mathrm{CC}^{\omega}_{\mathsf{list}}$version of Lemmas 10 and 30. They can be proved similary as for CC^{ω}. To prove (2), we need the following lemma that states the soundness of induction on lists.

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

Lemma 40.

$$
\begin{aligned}
&[\![\Gamma \vdash \forall A : \mathtt{Type}_0 . \forall P : \mathsf{list}\, A \to \mathtt{Prop}.\\
&\qquad P(\mathsf{nil}\, A) \to (\forall a : A. \forall l : \mathsf{list}\, A . P\, l \to P\,(\mathsf{cons}\, A\, a\, l)) \to \forall l : \mathsf{list}\, A . P\, l\\
&]\!](\gamma) = X
\end{aligned}
$$

where X is the whole topological space $(X, \mathscr{O}(X))$.

Proof. Let S be a set and $\psi \in S^* \to \mathscr{O}(X)$ be a function. We define the set of open sets T_n^ψ as

$$
\begin{aligned}
T_0^\psi &:= \{\psi(0, \cdot)\}\\
T_{n+1}^\psi &:= T_n^\psi \cup \{\psi(1, (a, l))^{\psi(l)} \mid a \in S \text{ and } l \in S^n\}.
\end{aligned}
$$

For any $n \in \omega$ and $l \in S^n$, $\bigsqcap T_n^\psi \leq \psi(l)$ holds by induction on natural numbers. Let T^ψ be their union

$$T^\psi := \bigcup_{n \in \omega} T_n^\psi .$$

Since $T_n^\psi \subset T^\psi$, therefore $\bigsqcap T^\psi \leq \bigsqcap T_n^\psi$ holds, hence we have $\bigsqcap T^\psi \leq \psi(l)$ for any $l \in S^*$. Therefore, we also have $\bigsqcap T^\psi \leq \bigsqcap \{\psi(l) \mid l \in S^*\}$.

Now, let us calculate the first equation:

$$
\begin{aligned}
&[\![\forall A : \mathtt{Type}_0 . \forall P : \mathsf{list}\, A \to \mathtt{Prop}.\\
&\qquad P(\mathsf{nil}\, A) \to (\forall a : A. \forall l : \mathsf{list}\, A . P\, l \to P\,(\mathsf{cons}\, A\, a\, l)) \to \forall l : \mathsf{list}\, A . P\, l\\
&]\!](\gamma)\\
&= \bigsqcap_{S \in \mathscr{U}_0} \left(\bigsqcap_{\psi \in S^* \to \mathscr{O}(X)} (\bigsqcap_{l \in S^*} \psi(l))^{(\bigsqcap T^\psi)} \right)\\
&= \bigsqcap_{S \in \mathscr{U}_0} \left(\bigsqcap_{\psi \in S^* \to \mathscr{O}(X)} X \right)\\
&= X
\end{aligned}
$$

To calculate it, we use (1) and (7) from Lemma 19.

□

6. Conclusion and Future Work

We could construct an intuitionistic set-theoretical model of CC^ω, which allowed us to prove that PEM and the linearity axiom do not hold in CC^ω. This model is not complete with respect to plain CC^ω, since it is proof-irrelevant.

This model combines an impredicative interpretation of propositional terms and a predicative interpretation of nonpropositional terms as in Miquel and Werner (2003).

Since one of our goals is to provide a model for Coq, we need to extend our model to all of CIC. This requires working on several extensions:

- CIC adds subsumption between $\mathtt{Prop}$ and $\mathtt{Type}_i$.

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

In fact, this rule breaks Lemmas 12 and 15. As a result, Theorem 32, soundness of beta equality, does not hold, as we show here.

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

Let $\mathscr{I}$ be $\lambda T : \texttt{Type}_i . T \to T$. In a set-theoretical interpretation, $[\![\mathscr{I}]\!]$ must be a function $A \mapsto \{f \mid f : A \to A\}$. However, for any propositional term P, the term $\mathscr{I} P$ is a tautology, and its interpretation is X, which leads to conflicting interpretations as $[\![\mathscr{I}]\!]([\![P]\!]) = [\![P]\!] \to [\![P]\!] \neq X$. Using an idea from Aczel (1998), Lee and Werner (2011), and Timany and Sozeau (2017) avoided this problem in an elegant way, by giving a uniform interpretation of propositional and non-propositional terms. They define the encoding functions app and lam as follows.

$$\mathsf{app}(u, x) := \{z \mid (x, z) \in u\}$$
$$\mathsf{lam}(f) := \bigcup_{(x,y) \in f} \{(x, z) \mid z \in y\}$$

These satisfy the expected property $\mathsf{app}(\mathsf{lam}(f), x) = f(x)$. Using the classical interpretation $[\![\texttt{Prop}]\!] = \{\varnothing, \{\varnothing\}\}$, the interpretation of the product type $\forall x : A.B$ becomes $\{\mathsf{lam}(f) \mid f \in \prod_{x \in A} B(x)\} \in [\![\texttt{Prop}]\!]$. It evaluates to $\{\varnothing\}$ iff $B(x) = \{\varnothing\}$ for all $x \in A$.
Unfortunately, this solution does not apply to intuitionistic settings, since $[\![\texttt{Prop}]\!]$ should contain more elements, making such a simple encoding impossible. We believe that searching for a non uniform encoding is a more resonable direction.

- Finally, CIC adds inductive and co-inductive type definitions, and they both can live in the impredicative universe $\texttt{Prop}$. The model in Lee and Werner (2011) supports generic inductive definitions through their set theoretical interpretation in a predicative universe as it was defined by Dybjer (2000), using Aczel's Φ-closed set approach (Aczel and Rathjen 2010). However, they do not extend this interpretation to the impredicative case. We have not yet investigated how to handle generic inductive definitions, co-inductive defintions, and impredicative inductive definitions in our model.

Notes

[1] We use the lattice operation symbols join '$\sqcup$' and meet '$\sqcap$' instead of '$\vee$' and '$\wedge$', since we use the latter as logical symbols.
[2] If $[\![\Gamma \vdash A]\!](\gamma)$ is the empty set, then $[\![\Gamma \vdash \forall x : A.B]\!](\gamma) = \{\varnothing\}$ and $[\![\Gamma \vdash \lambda x : A.t]\!](\gamma) = \varnothing$ hold.
[3] The remaining propositions yield by contrapositions of this fact.

References

Aczel, P. (1998). On relating type theories and set theories. In: *Proceedings of Types*, Springer LNCS, vol. 1657, 1–18.

Aczel, P. and Rathjen, M. (2010). CST Book draft. https://www1.maths.leeds.ac.uk/~rathjen/book.pdf

Arenas, F. G. (1999). Alexandroff spaces. *Acta Mathematica Universitatis Comenianae* **68** (1) 17–25.

Barendregt, H. (1991). Introduction to generalized type systems. *Journal of Functional Programming* **1** (2) 125–154.

Barendregt, H. (1992). Lambda calculus with types. In: *Handbook of Logic in Computer Science*, Chapter 2, vol. 2, Oxford University Press.

Barras, B. (2010). Sets in coq, coq in sets. *Journal of Formalized Reasoning* **3** (1) 29–48.

Coquand, T. and Huet, G. (1988). The calculus of constructions. *Information and Computation* **76** (2) 95–120.

Dybjer, P. (2000). A general formulation of simultaneous inductive-recursive definitions in type theory. *Journal of Symbolic Logic* **65** (2) 525–549.

Forster, Y. (2021). Church's thesis and related axioms in Coq's type theory. In: *29th EACSL Annual Conference on Computer Science Logic (CSL 2021)*, LIPIcs, vol. 183, 21:1–21:19.

Geuvers, H. (2001). Induction is not derivable in second order dependent type theory. In: *Types for Proofs and Programs*.

Girard, J.-Y. (1989). *Proofs and Types*, Cambridge University Press.

Jacobs, B. (2001). *Categorical Logic and Type Theory*, Studies in Logic and the Foundations of Mathematics, vol. 141, Elsevier.

Jiménez, B. C. R. (1999). Condensing lemmas for pure type systems with universes. In: *Algebraic Methodology and Software Technology*, Springer LNCS, vol. 1548, 422–437.

Lee, G. and Werner, B. (2011). Proof-irrelevant model of CC with predicative induction and judgemental equality. *Logical Methods in Computer Science* **7** (4:5). https://doi.org/10.2168/LMCS-7(4:5)2011

Luo, Z. (1991). A higher-order calculus and theory abstraction. *Information and Computation* **90** (1) 107–137.

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

MacLane, S. and Moerdijk, I. (1992). *Sheaves in Geometry and Logic: A First Introduction to Topos Theory*, New York, Springer.

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

Reynolds, J. (1984). Polymorphism is not set-theoretic. In: *Semantics of Data Types*, Springer LNCS, vol. 173, 145–156.

Sato, M. and Garrigue, J. (2016). An intuitionistic set-theoretical model of $\mathrm{CC}^{\bar{\omega}}$. *Journal of Information Processing* **24** (4) 711–720.

Stefanova, M. and Geuvers, H. (1995). A simple model construction for the calculus of constructions. In: *International Workshop on Types for Proofs and Programs.*

Streicher, T. (1991). *Semantics of Type Theory: Correctness, Completeness and Independence Results*, Boston, MA, Birkäuser.

Timany, A. and Sozeau, M. (2017). Consistency of the predicative calculus of cumulative inductive constructions (pCuIC). coRR. arXiv preprint arXiv:1710.03912.

Univalent Foundations Program (2013). *Homotopy Type Theory: Univalent Foundations of Mathematics*. http://homotopytypetheory.org/book, Institute for Advanced Study.

van Dalen, D. (1984). Intuitionistic logic. In: *Handbook of Philosophical Logic, Volume III*, Springer, 225–339.

van den Berg, B. (2007). Diaconescu's theorem and the principle of propositional extensionality (Unpublished).

Werner, B. (1997). Sets in types, types in sets. In: *Theoretical Aspects of Computer Software*, Springer LNCS, vol. 1281, 530–546.

Werner, B. (2008). On the strength of proof-irrelevant type theories. *Logical Methods in Computer Science* **4** (3:13) 1–20.

Appendix A. Proof of Weakening

Lemma 29. The proof is by induction on t, using Lemma 13.

- $t = x$ (case of variable)
  It is clear since t is not a proof term.
- $t = \lambda x : A.t'$
  By Lemma 10, t' is also not a proof term for $\Gamma_1; (x' : A'); \Gamma_2; (x : A)$. Therefore,

$$\begin{aligned}
&[\![\Gamma_1; \Gamma_2 \vdash \lambda x : A.t']\!](\gamma_1, \gamma_2) \\
&= \{(\alpha, [\![\Gamma_1; \Gamma_2; (x : A) \vdash t']\!](\gamma_1, \gamma_2, \alpha) \mid \\
&\qquad \alpha \in [\![\Gamma_1; \Gamma_2 \vdash A]\!](\gamma_1, \gamma_2)\} \\
&= \{(\alpha, [\![\Gamma_1; (x' : A'); \Gamma_2; (x : A) \vdash t']\!](\gamma_1, \alpha', \gamma_2, \alpha) \mid \\
&\qquad \alpha \in [\![\Gamma_1; (x' : A'); \Gamma_2 \vdash A]\!](\gamma_1, \alpha', \gamma_2)\} \\
&= [\![\Gamma_1; (x' : A'); \Gamma_2 \vdash \lambda x : A.t']\!](\gamma_1, \alpha', \gamma_2)
\end{aligned}$$

  holds.
- $t = t_1\ t_2$
  By Lemma 10, t_1 is also not a proof term for $\Gamma_1; (x' : A'); \Gamma_2$. If t_2 is a proof term for $\Gamma_1; (x' : A'); \Gamma_2$, then

$$\begin{aligned}
&[\![\Gamma_1; \Gamma_2 \vdash t_1\ t_2]\!](\gamma_1, \gamma_2) \\
&= [\![\Gamma_1; \Gamma_2 \vdash t_1]\!](\gamma_1, \gamma_2)\ (\bot_X) \\
&= [\![\Gamma_1; (x' : A'); \Gamma_2 \vdash t_1]\!](\gamma_1, \alpha', \gamma_2)\ (\bot_X) \\
&= [\![\Gamma_1; (x' : A'); \Gamma_2 \vdash t_1\ t_2]\!](\gamma_1, \alpha', \gamma_2)
\end{aligned}$$

  holds. If t_2 is not a proof term, then it is proved similarly.
- $t = \forall x : A.B$
  By Lemma 15

$$\mathbf{PT}_{\Gamma_1; \Gamma_2, x}(A, B) = \mathbf{PT}_{\Gamma_1; (x' : A'); \Gamma_2, x}(A, B)$$

  holds. Hence, we can only prove in the case of $\mathbf{PT}_{\Gamma_1 : \Gamma_2, x}(A, B)$.
- $t = \texttt{Prop}$ or $\texttt{Type}_i$
  Clear.

□

Appendix B. Proof of Substitution

Lemma 30. We define the predicates $P(\Delta)$ and $Q(\Delta, t)$ as follows.

$$\begin{aligned}
P(\Delta) \equiv{}& \forall\delta, (\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta) \in [\![\Gamma; (x : u); \Delta)]\!] \\
&\Rightarrow \quad (\gamma, \delta) \in [\![\Gamma;\Delta[x\backslash u]]\!], \\
Q(\Delta, t) \equiv{}& \forall\delta, [\![\Gamma; (x : U); \Delta \vdash t]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta) \text{ is well defined} \\
&\Rightarrow \quad \Big([\![\Gamma; \Delta[x\backslash u] \vdash t[x\backslash u]]\!](\gamma, \delta) \text{ is well-defined} \\
&\quad \text{and} \quad [\![\Gamma; x : U; \Delta \vdash t]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta) \\
&\qquad = [\![\Gamma; \Delta[x\backslash u] \vdash t[x\backslash u]]\!](\gamma, \delta)\Big).
\end{aligned}$$

We prove this lemma in three steps (i)$P([])$, (ii)$P(\Delta) \Rightarrow \forall t, Q(\Delta, t)$, (iii)$(\forall t, Q(\Delta, t)) \Rightarrow \forall T, P(\Delta; y : T)$.

(i) $P([])$
Clear

(ii) $P(\Delta) \Rightarrow \forall t, Q(\Delta, t)$
If t is a proof term for $\Gamma; (x : U); \Delta$, then $t[x\backslash u]$ is also a proof term for $\Gamma; \Delta[x\backslash u]$ by Lemma 12. Therefore

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

hold. Hence, we must prove that

$$\lfloor \gamma, [\![\Gamma \vdash u]\!](\gamma), \delta \rfloor = \lfloor \gamma, \delta \rfloor.$$

If u is not a proof term for Γ, it is clear. If u is a proof term then $[\![\Gamma \vdash u]\!](\gamma) = \lfloor \gamma \rfloor$ holds, therefore it also hold.

Next, if t is not a proof term for $\Gamma; (x : U); \Delta$, then $t[x\backslash u]$ is also not a proof term for $\Gamma; \Delta[x\backslash u]$ by Lemma 12. We prove by induction on the term t.

- $t = \mathtt{Prop}$ or $\mathtt{Type}_i$
  It is clear.
- $t = \forall a : A.B$
  We assume that
  $$[\![\Gamma; (x : U); \Delta \vdash \forall a : A.B]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta)$$
  is well defined, therefore
  $$\begin{aligned}
  [\![\Gamma; (x : U); \Delta \vdash A]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta), \\
  [\![\Gamma; (x : U); \Delta; (a : A) \vdash B]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta, \alpha)
  \end{aligned}$$
  are also well defined. By induction hypothesis, $Q(\Delta, A)$ and $Q(\Delta; (a : A), B)$ are assumed. By Lemma 15, the value of PT is invariant. Hence, the statement holds in this case.
- $t = \lambda a : A.t$
  We assume that
  $$[\![\Gamma; (x : U); \Delta \vdash \lambda a : A.t]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta)$$
  is well defined, therefore
  $$\begin{aligned}
  [\![\Gamma; (x : U); \Delta; (a : A) \vdash t]\!](\gamma, [\![\Gamma \vdash t]\!](\gamma), \delta, \alpha) \\
  [\![\Gamma; (x : U); \Delta \vdash A]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta)
  \end{aligned}$$

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

are also well defined. By induction hypothesis, $Q(\Delta; (a:A), t)$ and $Q(\Delta, A)$ are assumed. Hence, the statement holds in this case.

- $t = a\,b$
  We assume that
  $$[\![\Gamma; (x:U); \Delta \vdash a\,b]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta)$$
  is well defined, therefore
  $$[\![\Gamma; (x:U); \Delta \vdash a]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta)$$
  is well defined and a function whose domain contains
  $$[\![\Gamma; (x:U); \Delta \vdash b]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta).$$
  By induction hypothesis, $Q(\Delta, a)$ and $Q(\Delta, b)$ are assumed. By Lemma 12, if b is a (resp. not) proof term for $\Gamma; (x:U); \Delta$, then $b[x\backslash u]$ is also a (resp. not) proof term for $\Gamma; \Delta[x\backslash u]$. Hence, the statement holds in this case.
- $t = y$ (case of variable)
  We prove in three cases as follows.
  - The variable y occur in Γ.
    In this case, we have
    $$\begin{aligned}[\![\Gamma; (x:U); \Delta \vdash y]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta) &= \gamma_i,\\ [\![\Gamma; \Delta[x\backslash u] \vdash y[x\backslash u]]\!](\gamma, \delta) &= \gamma_i.\end{aligned}$$
    for some i. Hence, the statement holds in this case.
  - The case $y = x$.
    We have
    $$\begin{aligned}[\![\Gamma; (x:U); \Delta \vdash x]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta) &= [\![\Gamma \vdash u]\!](\gamma),\\ [\![\Gamma; \Delta[x\backslash u] \vdash x[x\backslash u]]\!](\gamma, \delta) &= [\![\Gamma; \Delta[x\backslash u] \vdash u]\!](\gamma).\end{aligned}$$
    By Lemma 29, the statement holds in this case.
  - The variable y occur in Δ.
    In this case, we have
    $$[\![\Gamma; (x:U); \Delta \vdash y]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta) = \delta_i$$
    for some i. Since $(\gamma, \delta) \in [\![\Gamma; \Delta[x\backslash u]]\!]$ by hypothesis $P(\Delta)$, hence following equation is well defined.
    $$[\![\Gamma; \Delta[x\backslash u] \vdash y]\!](\gamma, \delta) = \delta_i$$
    Hence, the statement holds in this case.

(iii) $(\forall t, Q(\Delta, t)) \Rightarrow \forall T, P(\Delta; y:T)$
We assume that
$$(\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta, \epsilon) \in [\![\Gamma; (x:U); \Delta; (y:T)]\!].$$
By definition of the interpretation of contexts, we have
$$\begin{aligned}(\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta) &\in [\![\Gamma; (x:U); \Delta]\!]\\ \epsilon &\in [\![\Gamma; (x:U); \Delta \vdash T]\!](\gamma, [\![\Gamma \vdash u]\!](\gamma), \delta)\end{aligned}$$
Since $Q(\Delta, T)$ holds, hence following equations hold.
$$\begin{aligned}(\gamma, \delta) &\in [\![\Gamma; \Delta[x\backslash u]]\!],\\ \epsilon &\in [\![\Gamma; \Delta[x\backslash u] \vdash T[x\backslash u]]\!](\gamma, \delta).\end{aligned}$$

Therefore, we have

$$(\gamma, \delta, \epsilon) \in [\![\Gamma; \Delta[x\backslash u] \vdash T[x\backslash u]]\!](\gamma, \delta).$$

□

Appendix C. Proof of Semantic Proof Irrelevance

Lemma 31. The proof is by induction on t.

- $t = x$ (case of variable)
  Since t is not a proof term for $\Gamma; (x' : A'); \Delta$, therefore we have $t \neq x'$, hence the statement holds in this case.
- $t = \lambda x : A.t'$
  By Lemma 10, t is also not a proof term for $\Gamma; (x' : A'); \Delta; (x : A)$. Therefore,

$$\begin{aligned} & [\![\Gamma; (x' : A'); \Delta \vdash \lambda x : A.t']\!](\gamma, p_1, \delta) \\ = & \{(\alpha, [\![\Gamma; (x' : A'); \Delta; (x : A) \vdash t']\!](\gamma, p_1, \delta, \alpha)) \mid \\ & \qquad \alpha \in [\![\Gamma; (x' : A'); \Delta \vdash A]\!](\gamma, p_1, \delta)\} \\ = & \{(\alpha, [\![\Gamma; (x' : A'); \Delta; (x : A) \vdash t']\!](\gamma, p_2, \delta, \alpha)) \mid \\ & \qquad \alpha \in [\![\Gamma; (x' : A'); \Delta \vdash A]\!](\gamma, p_2, \delta)\} \\ = & [\![\Gamma; (x' : A'); \Delta \vdash \lambda x : A.t']\!](\gamma, p_2, \delta) \end{aligned}$$

  holds.
- $t = t_1\ t_2$
  By Lemma 10, t_1 is also not a proof term for $\Gamma; (x' : A'); \Delta$. If t_2 is a proof term for $\Gamma; (x' : A'); \Delta$, then

$$\begin{aligned} & [\![\Gamma; (x' : A'); \Delta \vdash t_1\ t_2]\!](\gamma, p_1, \delta) \\ = & [\![\Gamma; (x' : A'); \Delta \vdash t_1]\!](\gamma, p_1, \delta)(\bot_X) \\ = & [\![\Gamma; (x' : A'); \Delta \vdash t_1]\!](\gamma, p_2, \delta)(\bot_X) \\ = & [\![\Gamma; (x' : A'); \Delta \vdash t_1\ t_2]\!](\gamma, p_2, \delta) \end{aligned}$$

  holds. If t_2 is not a proof term for $\Gamma; (x' : A'); \Delta$, then similarly.
- $t = \forall x : A.B$
  Similarly.

□

Appendix D. Proof of Soundness

Theorem 33. The proof is by induction on the typing derivation.

1. Case of Axiom
   $[\![\texttt{Prop}]\!] \in [\![\texttt{Type}_i]\!]$ is holds by the condition of $(X, \mathscr{O}(X))$.
2. Case of Weakening
   It holds by Lemma 29.
3. Case of Subsumption
   It holds by (iv) of Lemma 25.

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

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

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

There are four cases as follows.

- $\mathbf{PT}_{\Gamma,x}(A,B)=\mathsf{TT}$
  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. Since $[\![\Gamma\vdash A]\!](\gamma)\in\mathscr{U}_i$, $[\![\Gamma;(x:A)\vdash B]\!](\gamma,\alpha)\in\mathscr{U}_i$ for any γ,α and Lemma 25 (ii), we have

$$\prod_{\alpha\in[\![\Gamma\vdash A]\!](\gamma)}[\![\Gamma;(x:A)\vdash B]\!](\gamma,\alpha)\in\mathscr{U}_i.$$

- $\mathbf{PT}_{\Gamma,x}(A,B)=\mathsf{PT}$
  By definition of the interpretation of judgment, the following equation

$$\begin{aligned}&[\![\Gamma\vdash\forall x:A.B]\!](\gamma)=\\ &\quad\left\{f\in\prod_{\alpha\in[\![\Gamma\vdash A]\!](\gamma)}[\![\Gamma;(x:A)\vdash B]\!](\gamma,\alpha)\mid f\text{ is a constant function}\right\}\end{aligned}$$

  holds. Since $[\![\Gamma\vdash A]\!](\gamma)\in\mathscr{U}_i$, $[\![\Gamma;(x:A)\vdash B]\!](\gamma,\alpha)\in\mathscr{U}_i$ for any γ,α and Lemma 25 (ii), 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

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

There are four cases as follows.

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

$$\begin{aligned}&[\![\Gamma\vdash\lambda x:A.t]\!](\gamma)=\\ &\quad\left\{\big(\alpha,[\![\Gamma;(x:A)\vdash t]\!](\gamma,\alpha)\big)\mid\alpha\in[\![\Gamma\vdash A]\!](\gamma)\right\},\\ &[\![\Gamma\vdash\forall x:A.B]\!](\gamma)=\\ &\quad\prod_{\alpha\in[\![\Gamma\vdash A]\!](\gamma)}[\![\Gamma;(x:A)\vdash B]\!](\gamma,\alpha).\end{aligned}$$

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

Then, we must prove the following equation:

$$\Big\{\big(\alpha, [\![\Gamma; (x:A) \vdash t]\!](\gamma,\alpha)\big) \mid \alpha \in [\![\Gamma \vdash A]\!](\gamma)\Big\} \\ \in \prod_{\alpha\in[\![\Gamma\vdash A]\!](\gamma)} [\![\Gamma; (x:A) \vdash B]\!](\gamma,\alpha).$$

But it is clear[2] by induction hypothesis.

- $\mathbf{PT}_{\Gamma,x}(A,B) = \mathsf{PT}$
  It is similar the case of $\mathbf{PT}_{\Gamma,x}(A,B) = \mathsf{TT}$. We must prove that

  $$[\![\Gamma \vdash \lambda x : A.t]\!](\gamma) = \\ \Big\{\big(\alpha, [\![\Gamma; (x:A) \vdash t]\!](\gamma,\alpha)\big) \mid \alpha \in [\![\Gamma \vdash A]\!](\gamma)\Big\}$$

  is a constant function. Since A is a propositional term for Γ, this is a consequence of Lemma 31.
- $\mathbf{PT}_{\Gamma,x}(A,B) = \mathsf{TP}$
  Since $\lambda x : A.t$ is a proof term, we have following equations

  $$[\![\Gamma \vdash \lambda x : A.t]\!](\gamma) = \lfloor\gamma\rfloor.$$

  Hence, the fact we must prove that

  $$\lfloor\gamma\rfloor \in [\![\Gamma \vdash \forall x : A.B]\!](\gamma).$$

  By definition we have the following equation.

  $$[\![\Gamma \vdash \forall x : A.B]\!](\gamma) = \\ \bigsqcap\{[\![\Gamma; (x:A) \vdash B]\!](\gamma,\alpha) \mid \alpha \in [\![\Gamma \vdash A]\!](\gamma)\}.$$

  If $[\![\Gamma \vdash A]\!](\gamma)$ is the empty set, then the statement holds since $[\![\Gamma \vdash \forall x : A.B]\!](\gamma) = X$. We assume that $[\![\Gamma \vdash A]\!](\gamma)$ is a nonempty set. We have

  $$\forall\alpha \in [\![\Gamma \vdash A]\!](\gamma),\ \lfloor\gamma\rfloor \in [\![\Gamma; (x:A) \vdash B]\!](\gamma,\alpha)$$

  by induction hypothesis and $[\![\Gamma; (x:A) \vdash t]\!](\gamma,\alpha) = \lfloor\gamma,\alpha\rfloor = \lfloor\gamma\rfloor$. Therefore, we have the following equation

  $$\lfloor\gamma\rfloor \in \bigsqcap\{[\![\Gamma; (x:A) \vdash B]\!](\gamma,\alpha) \mid \alpha \in [\![\Gamma \vdash A]\!](\gamma)\}.$$

  Hence, the statement 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

  $$[\![\Gamma \vdash \lambda x : A.t]\!](\gamma) = \lfloor\gamma\rfloor.$$

  Hence, the fact we must prove that

  $$\lfloor\gamma\rfloor \in [\![\Gamma \vdash \forall x : A.B]\!](\gamma).$$

  To prove it, we show that

  $$\downarrow\lfloor\gamma\rfloor \subset [\![\Gamma \vdash \forall x : A.B]\!](\gamma).$$

  This fact is equivalent to the following equation

  $$\downarrow\lfloor\gamma\rfloor \cap [\![\Gamma \vdash A]\!](\gamma) \subset \bigsqcap_{\alpha\in[\![\Gamma\vdash A]\!](\gamma)} [\![\Gamma; (x:A) \vdash B]\!](\gamma,\alpha)$$

since definition of interpretation and Heyting Algebra. We assume $\varepsilon \in\downarrow \lfloor\gamma\rfloor \cap [\![\Gamma \vdash A]\!](\gamma)$. By Lemma 31, we have

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

holds; since $\varepsilon \in [\![\Gamma \vdash A]\!](\gamma)$ holds, right side of this equation is well defined. Here, we also have

$$\lfloor\gamma,\varepsilon\rfloor \in [\![\Gamma; (x:A)\vdash B]\!](\gamma,\varepsilon)$$

by induction hypothesis. Now, we prove that $\lfloor\gamma,\varepsilon\rfloor = \varepsilon$ holds. Since $\varepsilon \in\downarrow \lfloor\gamma\rfloor$ holds, therefore we have $\varepsilon \le \lfloor\gamma\rfloor$. Hence, we have $\varepsilon = \lfloor\gamma,\varepsilon\rfloor$, and the statement holds in this case.

(6) Case of Apply
We will show the fact that

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

There are four cases as follows.

- $\mathbf{PT}_{\Gamma,x}(A,B) = \mathsf{TT}$
  By definition of the interpretation of judgment and induction hypothesis, the following equation

$$\begin{aligned}[\![\Gamma\vdash u\,v]\!](\gamma) &= [\![\Gamma\vdash u]\!](\gamma)\big([\![\Gamma\vdash v]\!](\gamma)\big)\\ [\![\Gamma\vdash u]\!](\gamma) &\in \prod_{\alpha\in[\![\Gamma\vdash A]\!](\gamma)} [\![\Gamma; (x:A)\vdash B]\!](\gamma,\alpha)\\ [\![\Gamma\vdash v]\!](\gamma) &\in [\![\Gamma\vdash A]\!](\gamma)\end{aligned}$$

  hold. Therefore, we have

$$[\![\Gamma\vdash u\,v]\!](\gamma) \in [\![\Gamma; (x:A)\vdash B]\!](\gamma, [\![\Gamma\vdash v]\!](\gamma)).$$

  By Lemma 30, we have

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

  Hence, the statement holds in this case.
- $\mathbf{PT}_{\Gamma,x}(A,B) = \mathsf{PT}$
  By definition of the interpretation of judgment and induction hypothesis, the following equation

$$\begin{aligned}[\![\Gamma\vdash u\,v]\!](\gamma) &= [\![\Gamma\vdash u]\!](\gamma)\big(\bot_X\big)\\ [\![\Gamma\vdash u]\!](\gamma) &\in \Bigg\{f\in \prod_{\alpha\in[\![\Gamma\vdash A]\!](\gamma)} [\![\Gamma; (x:A)\vdash B]\!](\gamma,\alpha) \mid \\ &\qquad\qquad f \text{ is a constant function}\Bigg\}\\ [\![\Gamma\vdash v]\!](\gamma) &\in [\![\Gamma\vdash A]\!](\gamma)\end{aligned}$$

  hold. Therefore, we have

$$\begin{aligned}[\![\Gamma\vdash u\,v]\!](\gamma) &\in [\![\Gamma; (x:A)\vdash B]\!](\gamma, \bot_X)\\ &= [\![\Gamma; (x:A)\vdash B]\!](\gamma, [\![\Gamma\vdash v]\!](\gamma))\end{aligned}$$

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

by Lemma 31. Moreover, the following equation

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

holds by Lemma 30. Hence, the statement holds in this case.

- $\mathbf{PT}_{\Gamma,x}(A, B) = \mathsf{TP}$
  It suffices to show that $\lfloor\gamma\rfloor \in [\![\Gamma \vdash B[x\backslash v]]\!](\gamma)$, since $[\![\Gamma \vdash u]\!](\gamma) = [\![\Gamma \vdash u\, v]\!](\gamma) = \lfloor\gamma\rfloor$ holds. By induction hypothesis, we have the following equation

  $$\lfloor\gamma\rfloor \in \bigsqcap\{[\![\Gamma; (x : A) \vdash B]\!](\gamma, \alpha) \mid \alpha \in [\![\Gamma \vdash A]\!](\gamma)\}.$$

  This equation implies the fact that

  $$\forall\alpha \in [\![\Gamma \vdash A]\!](\gamma),\ \lfloor\gamma\rfloor \in [\![\Gamma; (x : A) \vdash B]\!](\gamma, \alpha).$$

  By Lemma 30 and the fact $[\![\Gamma \vdash v]\!](\gamma) \in [\![\Gamma \vdash A]\!](\gamma)$, we have

  $$\lfloor\gamma\rfloor \in [\![\Gamma \vdash B[x\backslash v]]\!](\gamma).$$

  Hence, the statement holds in this case.
- $\mathbf{PT}_{\Gamma,x}(A, B) = \mathsf{PP}$
  By induction hypothesis, we have

  $$\lfloor\gamma\rfloor \in [\![\Gamma \vdash \forall x : A.B]\!](\gamma),$$
  $$\lfloor\gamma\rfloor \in [\![\Gamma \vdash A]\!](\gamma)$$

  since $[\![\Gamma \vdash u]\!](\gamma) = [\![\Gamma \vdash v]\!](\gamma)$ holds. The following equation holds.

  $$[\![\Gamma \vdash \forall x : A.B]\!](\gamma) = \left(\bigsqcap_{\alpha\in[\![\Gamma\vdash A]\!](\gamma)} [\![\Gamma; (x : A) \vdash B]\!](\gamma, \alpha)\right)^{[\![\Gamma\vdash A]\!](\gamma)}$$

  By (8) in Lemma 19, we have

  $$[\![\Gamma \vdash \forall x : A.B]\!](\gamma) \cap [\![\Gamma \vdash A]\!](\gamma) \subset \bigsqcap_{\alpha\in[\![\Gamma\vdash A]\!](\gamma)} [\![\Gamma; (x : A) \vdash B]\!](\gamma, \alpha).$$

  Then we also have

  $$\lfloor\gamma\rfloor \in \bigsqcap_{\alpha\in[\![\Gamma\vdash A]\!](\gamma)} [\![\Gamma; (x : A) \vdash B]\!](\gamma, \alpha).$$

  Hence,

  $$\lfloor\gamma\rfloor \in [\![\Gamma; (x : A) \vdash B]\!](\gamma, [\![\Gamma \vdash v]\!](\gamma))$$

  holds. By Lemma 30 and $[\![\Gamma \vdash u\, v]\!](\gamma) = \lfloor\gamma\rfloor$, the statement holds in this case.

(7) Case of Variable
We show that

$$\forall\alpha \in [\![\Gamma \vdash A]\!](\gamma), [\![\Gamma; (x : A) \vdash x]\!](\gamma, \alpha) \in [\![\Gamma; (x : A) \vdash A]\!](\gamma, \alpha).$$

By Lemma 29, we must prove that

$$\forall\alpha \in [\![\Gamma \vdash A]\!](\gamma), [\![\Gamma; (x : A) \vdash x]\!](\gamma, \alpha) \in [\![\Gamma \vdash A]\!](\gamma).$$

If A is not a propositional term for Γ, the statement holds since $[\![\Gamma; (x : A) \vdash x]\!](\gamma, \alpha) = \alpha$. If A is a propositional term for Γ, then

$$[\![\Gamma; (x : A) \vdash x]\!](\gamma, \alpha) = \lfloor\gamma, \alpha\rfloor$$

holds. Since $\lfloor\gamma, \alpha\rfloor \in \downarrow\alpha \subset [\![\Gamma \vdash A]\!](\gamma)$,

$$[\![\Gamma; (x : A) \vdash x]\!](\gamma, \alpha) \in [\![\Gamma \vdash A]\!](\gamma)$$

holds. Hence, the statement holds in this case.

https://doi.org/10.1017/S0960129523000087 Published online by Cambridge University Press

(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 33 (1).

□

Appendix E. Proof of Interpretation of Logical Symbols

Theorem 34.

(i) Use Lemmas 8 and 29.
(ii) Use (2) in Lemma 19.
(iii) Use (1) and (3) in Lemma 19.
(iv) Use (1), (3) and (4) in Lemma 19.
(v) Use (i) in Theorem 34 and (1), (2), (3) and (6) in Lemma 19.
(vi) Use (i) in Theorem 34 and (3) and (5) in Lemma 19.
(vii) What we prove is the following.[3]

$$[\![\Gamma\vdash x=_A y]\!](\gamma)=\begin{cases}X & ([\![\Gamma\vdash x]\!](\gamma)=[\![\Gamma\vdash y]\!](\gamma))\\ \varnothing & ([\![\Gamma\vdash x]\!](\gamma)\neq[\![\Gamma\vdash y]\!](\gamma))\end{cases}$$

By using (i) in Theorem 34, we have

$$[\![\Gamma\vdash x=_A y]\!](\gamma)=\bigsqcap\{\pi([\![\Gamma\vdash y]\!](\gamma))^{\pi([\![\Gamma\vdash x]\!](\gamma))}\mid\pi\in[\![\Gamma\vdash A\to\texttt{Prop}]\!](\gamma)\}.$$

If $[\![\Gamma\vdash x]\!](\gamma)\neq[\![\Gamma\vdash y]\!](\gamma)$, we can choose π as the followings

$$\pi([\![\Gamma\vdash x]\!](\gamma))\neq\varnothing$$
$$\pi([\![\Gamma\vdash y]\!](\gamma))=\varnothing$$

hold. By (9) in Lemma 19, we have $[\![\Gamma\vdash x=_A y]\!](\gamma)=\varnothing$. Hence, the statement holds in this case.
Next, we assume $[\![\Gamma\vdash x]\!](\gamma)=[\![\Gamma\vdash y]\!](\gamma)$. In this case,

$$\pi([\![\Gamma\vdash y]\!](\gamma))^{\pi([\![\Gamma\vdash x]\!](\gamma))}=X$$

holds for any π by (7) in Lemma 19. Hence, the statement also holds in this case.

(viii) a. The following equation

$$[\![\Gamma\vdash A\leftrightarrow B]\!](\gamma)=[\![\Gamma\vdash B]\!](\gamma)^{[\![\Gamma\vdash A]\!](\gamma)}\sqcap[\![\Gamma\vdash A]\!](\gamma)^{[\![\Gamma\vdash B]\!](\gamma)}$$

holds. If $[\![\Gamma\vdash A]\!](\gamma)=[\![\Gamma\vdash B]\!](\gamma)$ holds, then

$$[\![\Gamma\vdash A\leftrightarrow B]\!](\gamma)=X$$
$$[\![\Gamma\vdash A=_{\texttt{Prop}} B]\!](\gamma)=X \qquad \text{(by (vii) in Theorem 34)}$$

holds. Hence, the statement holds in this case. If $[\![\Gamma\vdash A]\!](\gamma)\neq[\![\Gamma\vdash B]\!](\gamma)$, then $[\![\Gamma\vdash A=_{\texttt{Prop}} B]\!](\gamma)=\varnothing$ holds by. Hence, the statement also holds in this case.

b. Use (10) in Lemma 19 and (vii) in Theorem 34.

□

Cite this article: Sato M and Garrigue J (2023). An intuitionistic set-theoretical model of fully dependent CC$^\omega$. *Mathematical Structures in Computer Science* **33**, 1–32. https://doi.org/10.1017/S0960129523000087