λZ: Zermelo's Set Theory as a PTS with 4 Sorts

Alexandre Miquel

PPS & Université Paris 7
175 rue du Chevaleret, 75013 Paris

Abstract. We introduce a pure type system (PTS) λZ with four sorts and show that this PTS captures the proof-theoretic strength of Zermelo's set theory. For that, we show that the embedding of the language of set theory into λZ via the 'sets as pointed graphs' translation makes λZ a conservative extension of IZ + AFA + TC (intuitionistic Zermelo's set theory plus Aczel's antifoundation axiom plus the axiom of transitive closure)—a theory which is equiconsistent to Zermelo's. The proof of conservativity is achieved by defining a retraction from λZ to a (skolemised version of) Zermelo's set theory and by showing that both transformations commute via the axioms AFA and TC.

Introduction

Modern proof assistants based on the Curry Howard correspondence—such as Agda, Coq, Nuprl or Plastic—basically implement a well-known pure type system [7, 3] (PTS) enriched with many extensions such as inductive data-types and recursive definitions of functions. Traditionally, the proof-theoretic strength of the implemented formalisms is estimated via the sets-in-types and types-in-sets encodings [13, 2], that respectively give a lower and an upper bound of the proof-theoretic strength of the system, expressed as a variant of set theory.

Surprisingly, very little is known about the proof-theoretic strength of the underlying PTSs themselves. The main reason is that the framework of PTSs lacks the inductive data-types that are crucial in the definition of the traditional sets-in-types encoding based on Aczel's W-trees. Another reason is that there is currently no simple set-theoretic interpretation of type-theoretic universes that does not rely on the existence of large cardinals—an assumption which is definitely too strong to give a reasonable upper bound of a PTS.

The aim of this paper is to initiate a more systematic study of the proof-theoretic strength of the subsystems of the Calculus of Constructions with universes (CC_ω) following the correspondence with extensions of Zermelo's set theory that was outlined in the author's thesis [11]. In this direction, we present a first result by extracting a sub-PTS of the Calculus of Constructions with universes—the system λZ presented in section 1—that captures the proof-theoretic strength of Zermelo's set theory (without the Foundation Axiom). Moreover, we show that through the sets-as-pointed-graphs encoding (which is recalled in section 3) the PTS λZ appears to be a conservative extension of a

very natural extension of Intuitionistic Zermelo's set theory, namely, the system IZ + AFA + TC whose classical version as been already considered in [5], and which is clearly equiconsistent to Z.

Finally, let us mention that the crucial ingredient of the equiconsistency proof presented in this paper does not come from the type-theoretic side, but from the set-theoretic side. As we shall see in section 2, introducing an explicitly Skolemised version of Zermelo's set theory reveals some unexpected closure properties of this system that are fruitfully exploited in the definition of the types-in-sets interpretation presented in section 4.

1 The PTS λZ

In this section, we assume the reader has some familiarity with the theory of PTS (see [7, 3]).

1.1 The PTS presentation

Definition 1 (λZ). — *λZ is the PTS whose set of sorts $\mathscr{S}$, whose set of axioms $\mathscr{A} \subset \mathscr{S}^2$ and whose set of rules $\mathscr{R} \subset \mathscr{S}^3$ are given by*

$$\begin{aligned}
\mathscr{S} &= \{*;\ \Box_1;\ \Box_2;\ \Box_3\}\,,\\
\mathscr{A} &= \{(* : \Box_1);\ (\Box_1 : \Box_2);\ (\Box_2 : \Box_3)\}\,,\\
\mathscr{R} &= \{(*,*,*);\ (\Box_i,*,*) \mid i \in \{1,2,3\}\}\ \cup\ \{(\Box_i,\Box_j,\Box_{\max(i,j)}) \mid i,j \in \{1,2\}\}\,.
\end{aligned}$$

By construction, the PTS λZ is a sub-system of the calculus of constructions with universes (CC_ω), and actually, a subsystem of system $F\omega$ with universes ($F\omega^2$, the non-dependent fragment of CC_ω) which is the PTS defined by:

$$\begin{aligned}
\mathscr{S}_{F\omega^2} &= \{*;\ \Box_i \mid i \geq 1\}\,,\\
\mathscr{A}_{F\omega^2} &= \{(* : \Box_0);\ (\Box_i : \Box_{i+1}) \mid i \geq 1\}\,,\\
\mathscr{R}_{F\omega^2} &= \{(*,*,*);\ (\Box_i,*,*);\ (\Box_i,\Box_j,\Box_{\max(i,j)}) \mid i,j \geq 1\}\,.
\end{aligned}$$

Moreover, if we write $F\omega.n$ (for $n \geq 1$) the PTS obtained by restricting $F\omega^2$ to the set of sorts $\{*;\ \Box_i \mid 1 \leq i \leq n\}$, then we have the inclusions:

$$F\omega.2\ \subset\ \lambda\mathrm{Z}\ \subset\ F\omega.3\ \subset\ \cdots\ \subset\ F\omega^2\ \subset\ \mathrm{CC}_\omega$$

Intuitively, the PTS λZ extends $F\omega.2$ with a sort $\Box_3$, an axiom $\Box_2 : \Box_3$ and a unique rule $(\Box_3,*,*)$, whereas $F\omega.3$ completes the extension by adding all the 'missing rules' $(\Box_3,\Box_i,\Box_3)$ and $(\Box_i,\Box_3,\Box_3)$ for $i \in \{1;2;3\}$.

As for any PTS, λZ enjoys many good properties, such as substitutivity and subject-reduction [7] as well as the property of uniqueness of types up to β-conversion (since λZ is a functional PTS).

From the inclusions $\lambda\mathrm{Z} \subset F\omega^2 \subset \mathrm{CC}_\omega$ we immediately get [9, 10]:

Fact 1 (Strong normalisation) — *All the well-typed term of λZ are strongly normalisable terms.*

It is important to notice that this result will not be used in the following, for that the conservativity result we will present purely relies on syntactic codings (that involve straightforward conversion steps on the type-theoretic side). On the other hand, using the normalisation result above—which seems to require much more proof-theoretic strength than the consistency of Zermelo's[1]—would dramatically weaken the interest of our relative consistency proof.

1.2 Stratified presentation of $F\omega^2$

As for the systems of Barendregt's cube, the PTS $F\omega^2$ (and its subsystems) can be given a stratified presentation which syntactically distinguishes the terms whose type has type $\Box_i$—that represent mathematical objects—from the terms whose type has type $*$—that represent mathematical proofs.

Formally, we say that in a given context Γ, a term M of type T is an *object term* if $\Gamma \vdash T : \Box_i$ for some $i \geq 1$, and a *proof term* if $\Gamma \vdash T : *$. Notice that *propositions*—that is, terms of type $*$—are a special case of object terms. In the rest of this presentation, we use capital letters M, N, T, U, A, B, etc. to denote object terms (and more specifically: T, U for types and A, B for propositions) whereas lowercase letters t, u, etc. are reserved for proof terms.

Dependent and non-dependent products are stratified according to their formation rule as follows:

- Non-dependent products formed according to the rule $(*, *, *)$, which express logical implication, are written $A \Rightarrow B$. Notice that non-dependent products are the only products that can be formed by this rule, since λZ is a non-dependent logical PTS (following the terminology of [4]).
- Dependent products formed according to the rule $(\Box_i, *, *)$, which express universal quantification, are written $\forall x : T \,.\, A$.
- Dependent products formed according to the rule $(\Box_i, \Box_i, \Box_i)$, which express dependent function spaces, are still written $\Pi x : T \,.\, U$ (or simply $T \to U$ in the non-dependent case, when $x \notin FV(U)$).

The stratified presentation of system $F\omega^2$ is given in table 1, and the corresponding (stratified) typing rules are recalled in table 2.

Proposition 1 (Stratification equivalence). — *The well-typed terms of system $F\omega^2$ are exactly the object terms and proof terms that can be expressed in the syntax given in table 1 and type-checked using the rules of table 2.*

[1] We conjecture that the *(strong) normalisation* of λZ has the same proof-theoretic strength as (the consistency of) IZ plus one Zermelo-universe. This has to be compared to the formalisms CC and $F\omega$, whose strong normalisation properties have exactly the same proof-theoretic strength as higher-order arithmetic (HAω) but whose consistency can be proved within Heyting arithmetic (HA).

Object terms	M, N, T, U, A, B	$::=$	$x \mid \lambda x{:}T\,.\,M \mid MN$
		$\mid$	$\Pi x{:}T\,.\,U \mid * \mid \Box_i \quad (i \geq 1)$
		$\mid$	$A \Rightarrow B \mid \forall x{:}T\,.\,A$
Proof terms	t, u	$::=$	ξ
		$\mid$	$\lambda \xi^A\,.\,t \mid tu$
		$\mid$	$\lambda x{:}T\,.\,t \mid tM$

Table 1. The stratified presentation of $F\omega^2$

Context formation

$$\frac{}{[] \vdash} \qquad \frac{\Gamma \vdash T : \Box_i}{\Gamma,\ x : T \vdash} \qquad \frac{\Gamma \vdash A : *}{\Gamma,\ \xi : A \vdash}$$

Object terms

$$\frac{\Gamma \vdash}{\Gamma \vdash x : T}\ {\scriptstyle (x:T)\in\Gamma} \qquad \frac{\Gamma \vdash}{\Gamma \vdash * : \Box_1} \qquad \frac{\Gamma \vdash}{\Gamma \vdash \Box_i : \Box_{i+1}}$$

$$\frac{\Gamma \vdash \Pi x{:}T\,.\,U : \Box_i \qquad \Gamma,\ x : T \vdash M : U}{\Gamma \vdash \lambda x{:}T\,.\,M : \Pi x{:}T\,.\,U} \qquad \frac{\Gamma \vdash M : \Pi x{:}T\,.\,U \qquad \Gamma \vdash N : T}{\Gamma \vdash MN : U\{x := N\}}$$

$$\frac{\Gamma \vdash A : * \qquad \Gamma \vdash B : *}{\Gamma \vdash A \Rightarrow B : *} \qquad \frac{\Gamma,\ x : T \vdash A : *}{\Gamma \vdash \forall x{:}T\,.\,A : *}$$

$$\frac{\Gamma \vdash T : \Box_i \qquad \Gamma,\ x : T \vdash U : \Box_j}{\Gamma \vdash \Pi x{:}T\,.\,U : \Box_{\max(i,j)}} \qquad \frac{\Gamma \vdash M : T \qquad \Gamma \vdash T' : \Box_i}{\Gamma \vdash M : T'}\ {\scriptstyle T' =_\beta T}$$

Proof terms

$$\frac{\Gamma \vdash}{\Gamma \vdash \xi : A}\ {\scriptstyle (\xi:T)\in\Gamma} \qquad \frac{\Gamma \vdash t : A \qquad \Gamma \vdash A' : *}{\Gamma \vdash t : A'}\ {\scriptstyle A' =_\beta A}$$

$$\frac{\Gamma,\ \xi : A \vdash t : B}{\Gamma \vdash \lambda \xi : A\,.\,t : A \Rightarrow B} \qquad \frac{\Gamma \vdash t : A \Rightarrow B \qquad \Gamma \vdash u : A}{\Gamma \vdash tu : B}$$

$$\frac{\Gamma,\ x : T \vdash t : A}{\Gamma \vdash \lambda x{:}T\,.\,t : \forall x{:}T\,.\,A} \qquad \frac{\Gamma \vdash t : \forall x{:}T\,.\,A \qquad \Gamma \vdash N : T}{\Gamma \vdash tN : A\{x := N\}}$$

Table 2. Typing rules of $F\omega^2$

1.3 The stratified presentation of λZ

In the stratified setting, system λZ naturally appears as the subsystem of $F\omega^2$ which is obtained:

- By restricting the set of sorts to the initial segment $\mathscr{S} = \{*;\ \Box_1;\ \Box_2;\ \Box_3\}$ of $\mathscr{S}_{F\omega^2}$ and the set $\mathscr{A}$ of axioms accordingly.
- By restricting the formation rule of dependent function spaces to the rules of the form $(\Box_i, \Box_j, \Box_{\max(i,j)})$ for $i, j \in \{1; 2\}$.

On the other hand, system λZ does not further restrict the rules $(\Box_i, *, *)$ that are responsible for the formation of universal quantification $\forall x : T\,.\,A$, and that can be used at any index $i \in \{1; 2; 3\}$.

To understand the structure of λZ, let us explain the meaning of each universe $\Box_i$ (for $i \in \{1; 2; 3\}$) and of each formation rule $(\Box_i, *, *)$ in terms of the notions they will correspond to via our translation to set theory:

1. The first universe $\Box_1$—that contains no provably infinite data-type[2]—has to be thought as the universe of *finite data-types*. Technically, the presence of a first universe below the universe $\Box_2$ of sets (see below) is needed to justify the existence of a provably infinite data-type in $\Box_2$, and plays the very same role as the axiom of infinity in set theory. In particular, universal quantifications $\forall x : T\,.\,A(x)$ formed by the rule $(\Box_1, *, *)$ roughly correspond to finite quantifications $\forall x < t\ A(x)$ (where $t \in \omega$) in set theory.
2. The universe $\Box_2$ has to be thought as the universe of sets, or, more precisely, as the universe of the *carriers* of the pointed graphs that we will use to represent sets. Thus, universal quantifications $\forall x : T\,.\,A(x)$ formed by the rule $(\Box_2, *, *)$ correspond to bounded quantifications $\forall x{\in}t\ A(x)$ in set theory.
3. The sort $\Box_3$ is a top sort whose only inhabitant is the universe $\Box_2$—which is due to the absence of formation rules of the form $(s_1, s_2, \Box_3)$. Technically this sort is needed to type-check the construction $\forall x : \Box_2\,.\,A(x)$—the only form of universal quantification induced by the rule $(\Box_3, *, *)$—that corresponds to the unbounded quantification $\forall x\ A(x)$ in set theory.

The aim of this paper is to formalise the correspondence depicted above to turn it into a result of proof-theoretic equivalence.

2 Zermelo's set theory

2.1 The core language

Zermelo's set theory (Z) is the classical first-order theory whose language is built from the two binary relations $x = y$ (*equality*) and $x \in y$ (*membership*)

$$\textbf{Formulæ}\qquad \phi, \psi \quad ::= \quad \top \ \mid\ \bot \ \mid\ x = y \ \mid\ x \in y \\ \mid\ \phi \wedge \psi \ \mid\ \phi \vee \psi \ \mid\ \phi \Rightarrow \psi \ \mid\ \forall x\ \psi \ \mid\ \exists x\ \psi$$

[2] This will be a consequence of the soundness of the translation $(\_)^\dagger$ defined in section 4.

and whose axioms are given in table 3, using the following shorthands:

$$\begin{array}{lcllcl}
\neg\phi & \equiv & \phi \Rightarrow \bot & \phi \Leftrightarrow \psi & \equiv & (\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \phi) \\
x \notin y & \equiv & \neg(x \in y) & x \subset y & \equiv & \forall z\ (z \in x \Rightarrow z \in y) \\
\mathrm{Zero}(x) & \equiv & \forall z\ (z \notin x) & \mathrm{Succ}(x,y) & \equiv & \forall z\ [z \in y \Leftrightarrow z \in x \vee z = x] \\
\mathrm{Nat}(n) & \equiv & \forall a\ [\forall x\ (\mathrm{Zero}(x)\ \Rightarrow\ x \in a)\ \ \wedge & & & \\
 & & \quad \forall x\ \forall y\ (x \in a \wedge \mathrm{Succ}(x,y)\ \Rightarrow\ y \in a)\ \Rightarrow\ n \in a] & & &
\end{array}$$

(Notice that in this presentation of Z, there is no Axiom of Foundation.)

	Equality axioms
(Reflexivity)	$\forall x\ (x = x)$
(Symmetry)	$\forall x\ \forall y\ (x = y\ \Rightarrow\ y = x)$
(Transitivity)	$\forall x\ \forall y\ \forall z\ (x = y\ \wedge\ y = z\ \Rightarrow\ x = z)$
(Mem-Compat-L)	$\forall x\ \forall y\ \forall z\ (x = y\ \wedge\ y \in z\ \Rightarrow\ x \in z)$
(Mem-Compat-R)	$\forall x\ \forall y\ \forall z\ (x \in y\ \wedge\ y = z\ \Rightarrow\ x \in z)$
	Zermelo's axioms
(Extensionality)	$\forall a\ \forall b\ [\forall x\ (x \in a \Leftrightarrow x \in b)\ \Rightarrow\ a = b]$
(Pairing)	$\forall a_1\ \forall a_2\ \exists b\ \forall x\ [x \in b\ \Leftrightarrow\ x = a_1\ \vee\ x = a_2]$
(Comprehension)	$\forall x_1 \cdots \forall x_n\ \forall a\ \exists b\ \forall x\ [x \in b\ \Leftrightarrow\ x \in a\ \wedge\ \phi]$ for any formula ϕ such that $FV(\phi) \subset \{x_1; \ldots; x_n; x\}$.
(Powerset)	$\forall a\ \exists b\ \forall x\ [x \in b\ \Leftrightarrow\ x \subset a]$
(Union)	$\forall a\ \exists b\ \forall x\ [x \in b\ \Leftrightarrow\ \exists y\ (y \in a\ \wedge\ x \in y)]$
(Infinity)	$\exists a\ \forall x\ [x \in a\ \Leftrightarrow\ \mathrm{Nat}(x)]$

Table 3. Axioms of Zermelo's set theory

Intuitionistic Zermelo's set theory (IZ) is the theory based on the same language and axioms as Z, but in which reasoning is done in intuitionistic logic. As shown by [6], there is a double negation translation which maps (classically) provable formulæ of Z to (intuitionistically) provable formulæ of IZ, so that both theories IZ and Z are actually equiconsistent.

In what follows, we will mainly work in IZ.

2.2 Skolemising Z

The main drawback of the traditional presentation of set theory is the lack of notations to express objects (i.e. sets). To define the 'retraction' of section 4, we first need to enrich—in a conservative way—the term algebra of set theory (that only contains variables) with notations to express the unordered pairs, the powersets, the unions, the set of natural numbers and all the sets defined by using the comprehension scheme.

Formally, we introduce a system called Z^{sk}, whose terms and formulæ are mutually defined by:

$$\begin{array}{lrcl} \textbf{Terms} & t, u & ::= & x \mid \omega \mid \{t_1; t_2\} \mid \mathfrak{P}(t) \mid \bigcup t \mid \{x \in t \mid \phi\} \\ \textbf{Formulæ} & \phi, \psi & ::= & t = u \mid t \in u \mid \top \mid \bot \\ & & & \mid \phi \wedge \psi \mid \phi \vee \psi \mid \phi \Rightarrow \psi \mid \forall x\ \phi \mid \exists x\ \phi \end{array}$$

(Free and bound occurrences of variables are defined as expected, keeping in mind that the construction $\{x \in t \mid \phi\}$ binds all the free occurrences of the variable x in ϕ, but none of the free occurrences of x in t. The notions of substitutions $t\{x := u\}$ and $A\{x := u\}$ are defined accordingly.)

Although Z^{sk} is not based on a first-order language, the underlying notions of sequent, inference rule and derivation are defined as in first-order theories. The axioms of Z^{sk} are the same as in Z, except that the existential axioms of Zermelo's system (table 3) are replaced by their Skolemized forms (table 4).

The intuitionistic fragment of Z^{sk} is written $\mathrm{IZ}^{\mathrm{sk}}$.

($\textsc{Pairing}^{\mathrm{sk}}$)	$\forall a_1\ \forall a_2\ \forall x\ [x \in \{a_1; a_2\} \ \Leftrightarrow\ x = a_1 \ \vee\ x = a_2]$
($\textsc{Comprehension}^{\mathrm{sk}}$)	$\forall x_1 \cdots \forall x_n\ \forall a\ \forall x\ [x \in \{z \in a \mid \phi\} \ \Leftrightarrow\ x \in a \ \wedge\ \phi\{z := x\}]$ for any formula ϕ such that $FV(\phi) \subset \{x_1; \ldots; x_n; z\}$.
($\textsc{Powerset}^{\mathrm{sk}}$)	$\forall a\ \forall x\ [x \in \mathfrak{P}(a) \ \Leftrightarrow\ x \subset a]$
($\textsc{Union}^{\mathrm{sk}}$)	$\forall a\ \forall x\ [x \in \bigcup a \ \Leftrightarrow\ \exists y\ (y \in a \ \wedge\ x \in y)]$
($\textsc{Infinity}^{\mathrm{sk}}$)	$\forall x\ [x \in \omega \ \Leftrightarrow\ \mathrm{Nat}(x)]$

Table 4. Skolemised axioms of Z^{sk}

The theory $(\mathrm{I})\mathrm{Z}^{\mathrm{sk}}$ is clearly an extension of (I)Z,[3] in the sense that for any formula ϕ of set theory, $(\mathrm{I})\mathrm{Z} \vdash \phi$ entails $(\mathrm{I})\mathrm{Z}^{\mathrm{sk}} \vdash \phi$.

From the axioms of table 4, we easily check that the function symbols $\{\_;\_\}$, $\mathfrak{P}(\_)$ and $\bigcup\_$ are compatible with equality (in $\mathrm{IZ}^{\mathrm{sk}}$) as well as the construction

[3] The shorthand (I)Z reads: "Z (resp. IZ)". And similarly for $(\mathrm{I})\mathrm{Z}^{\mathrm{sk}}$.

$\{x \in t \mid \phi\}$ in the sense that:

$$\begin{array}{lll} \mathrm{IZ}^{\mathrm{sk}} & \vdash & \forall x_1 \cdots \forall x_n\ \forall a\ \forall a'\ [a = a'\ \Rightarrow\ \{x \in a \mid \phi\} = \{x \in a' \mid \phi\}] \\ \mathrm{IZ}^{\mathrm{sk}} & \vdash & \forall x_1 \cdots \forall x_n\ \forall a\ [\forall x\ (\phi \Leftrightarrow \phi')\ \Rightarrow\ \{x \in a \mid \phi\} = \{x \in a \mid \phi'\}] \end{array}$$

(for all formulæ ϕ, ϕ' of Z^{sk} such that $FV(\phi) \cup FV(\phi') \subset \{x_1; \ldots; x_n; x\}$), from which we deduce that Leibniz principle holds, both for terms and formulæ:

Proposition 2 (Leibniz principle). — *For any term t and for any formula ϕ of the language of Z^{sk}:*

$$\begin{array}{lllll} \mathrm{IZ}^{\mathrm{sk}} & \vdash & x_1 = x_2 & \Rightarrow & t\{x := x_1\} = t\{x := x_2\} \\ \mathrm{IZ}^{\mathrm{sk}} & \vdash & x_1 = x_2 & \Rightarrow & \phi\{x := x_1\} \Leftrightarrow \phi\{x := x_2\} \end{array}$$

Proof. This result is proved by mutual induction on t and ϕ. □

In Z^{sk} (and, actually, in $\mathrm{IZ}^{\mathrm{sk}}$), most standard mathematical notations such as $\varnothing$ (empty set), $x \cup y$ (union), $x \cap y$ (intersection), $x \setminus y$ (difference), $f(x)$ (function application), $\langle x, y \rangle$ (ordered pair), B^A (function space), etc. are easily definable as macros in the enriched term algebra.

We now have to ensure that $(\mathrm{I})\mathrm{Z}^{\mathrm{sk}}$ is a conservative extension of (I)Z.

2.3 The deskolemisation procedure

The proof of conservativity of $(\mathrm{I})\mathrm{Z}^{\mathrm{sk}}$ w.r.t. (I)Z relies on a deskolemisation procedure that is achieved by two transformations:

- A transformation on *terms*, which maps each pair (t, z) formed by a term t of Z^{sk} and a variable z to a formula of set theory written $z \in^\circ t$;[4]
- A transformation on *formulæ*, which maps each formula ϕ of Z^{sk} to a formula of set theory written ϕ°.

Both transformations are defined by mutual induction on t and ϕ from the deskolemisation equations given in table 5.

This process of deskolemisation preserves the meaning of terms and formulæ in $\mathrm{IZ}^{\mathrm{sk}}$ in the sense that:

Proposition 3 (Translation equivalence). — *For all terms t and formulæ ϕ of the language of Z^{sk}, one has:*

$$\mathrm{IZ}^{\mathrm{sk}} \vdash (z \in^\circ t) \Leftrightarrow z \in t \qquad \textit{and} \qquad \mathrm{IZ}^{\mathrm{sk}} \vdash \phi^\circ \Leftrightarrow \phi$$

Moreover, if ϕ is expressed in the core language $(=, \in)$ of set theory, then:

$$\mathrm{IZ} \vdash \phi^\circ \Leftrightarrow \phi\,.$$

[4] Notice the conceptual similarity between the design of the deskolemisation procedure for terms $(z \in^\circ t)$ and the notions of realisability and forcing $(t \Vdash \phi)$.

$$
\begin{array}{lcl}
z \in^\circ x & \equiv & z \in x \\
z \in^\circ \omega & \equiv & \mathrm{Nat}(z) \\
z \in^\circ \{t_1; t_2\} & \equiv & (z = t_1)^\circ \ \vee \ (z = t_2)^\circ \\
z \in^\circ \mathfrak{P}(t) & \equiv & \forall x \ (x \in z \ \Rightarrow \ x \in^\circ t) \\
z \in^\circ \bigcup t & \equiv & \exists y \ (y \in^\circ t \wedge z \in y) \\
z \in^\circ \{x \in t \mid \phi\} & \equiv & z \in^\circ t \ \wedge \ \phi^\circ\{x := z\}
\end{array}
$$

$$
\begin{array}{lcl@{\qquad}lcl}
(t = u)^\circ & \equiv & \forall z \ (z \in^\circ t \Leftrightarrow z \in^\circ u) & (\phi \wedge \psi)^\circ & \equiv & \phi^\circ \wedge \psi^\circ \\
(t \in u)^\circ & \equiv & \exists z \ ((z = t)^\circ \wedge z \in^\circ u) & (\phi \vee \psi)^\circ & \equiv & \phi^\circ \vee \psi^\circ \\
 & & & (\phi \Rightarrow \psi)^\circ & \equiv & \phi^\circ \Rightarrow \psi^\circ \\
\top^\circ & \equiv & \top & (\forall x \ \phi)^\circ & \equiv & \forall x \ \phi^\circ \\
\bot^\circ & \equiv & \bot & (\exists x \ \phi)^\circ & \equiv & \exists x \ \phi^\circ
\end{array}
$$

Table 5. Deskolemisation equations for terms and formulæ of Z^{sk}

Proof. The first two items are proved by mutual induction on t and ϕ. Last item is proved by induction on ϕ. □

Furthermore, we can show:

Proposition 4 (Soundness of deskolemisation). — *If a closed formula ϕ is a theorem of* (I)Z^{sk}*, then ϕ° is a theorem of* (I)Z.

From Prop. 3 (last equivalence) and Prop. 4 we easily deduce:

Proposition 5 (Conservativity). — *The theory* (I)Z^{sk} *is a conservative extension of* (I)Z.

Proof. See appendix A.

2.4 A weak form of replacement in Zermelo's system

Historically, one of the motivations of Fraenkel and Skolem to introduce the replacement scheme in set theory

$$\text{(Replacement)} \qquad \forall a \ [\forall x{\in}a \ \exists! y \ \phi(x,y) \ \Rightarrow \ \exists b \ \forall x{\in}a \ \exists y{\in}b \ \phi(x,y)]$$

(which fills the gap between Z and ZF) was to justify the notation $\{t(x) \mid x \in u\}$ which expresses the image of the set u by the functional relation $x \mapsto t(x)$.

Surprisingly, the study of Z^{sk} reveals that the justification of the notation $\{t(x) \mid x \in u\}$ does not need any extension of Zermelo's system *when the term $t(x)$ is expressed in the term language of* Z^{sk}.

The reason is that for any term u of Z^{sk} and for any term $t(x)$ of Z^{sk} that possibly depends on a variable x, we can define a term written $\mathsf{B}(t(x), \ x \in u)$

which uniformly bounds $t(x)$ when x ranges over u. Formally, such a term can be defined by structural induction on $t(x)$ as follows:

$$\begin{array}{lcl}
\mathsf{B}(x,\ x \in u) & = & u \\
\mathsf{B}(y,\ x \in u) & = & \mathfrak{P}(y) \qquad (\text{if } y \not\equiv x) \\
\mathsf{B}(\omega,\ x \in u) & = & \mathfrak{P}(\omega) \\
\mathsf{B}(\{t_1;t_2\},\ x \in u) & = & \mathfrak{P}\big(\mathsf{B}(t_1,\ x \in u) \cup \mathsf{B}(t_2,\ x \in u)\big) \\
\mathsf{B}(\mathfrak{P}(t),\ x \in u) & = & \mathfrak{P}(\mathfrak{P}(\bigcup \mathsf{B}(t,\ x \in u))) \\
\mathsf{B}(\bigcup t,\ x \in u) & = & \mathfrak{P}(\bigcup\bigcup \mathsf{B}(t,\ x \in u)) \\
\mathsf{B}(\{y \in t \mid \phi\},\ x \in u) & = & \mathfrak{P}(\bigcup \mathsf{B}(t,\ x \in u))
\end{array}$$

Lemma 1. — *For all terms $t(x)$ and u of Z^{sk} such that $x \notin FV(u)$:*

$$\mathrm{IZ}^{\mathrm{sk}} \ \vdash\ \forall x\ [x \in u \Rightarrow t(x) \in \mathsf{B}(t(x),\ x \in u)]\,.$$

Proof. By induction on $t(x)$. □

Setting $\{t(x) \mid x \in u\} \ \equiv\ \{y \in \mathsf{B}(t(x),\ x \in u) \mid \exists x\ (x \in u \wedge y = t(x))\}$ we easily check that:

Proposition 6. — *For all terms t and u such that $x \notin FV(u)$ and $y \notin FV(t)$:*

$$\mathrm{IZ}^{\mathrm{sk}} \ \vdash\ \forall y\ [y \in \{t \mid x \in u\} \ \Leftrightarrow\ \exists x\ (x \in u \wedge y = t)]\,.$$

An important consequence of this result is that we can now define in the language of Z^{sk} both the notation for function abstraction and the notation for generalised Cartesian product that are crucial ingredients for any translation of type theory in set theory:

$$\begin{array}{rcl}
\lambda x \in t\,.\,u(x) & \equiv & \big\{\langle x, u(x)\rangle \mid x \in t\big\} \\
\prod_{x \in t} u(x) & \equiv & \Big\{f \in \big(\bigcup\{u(x) \mid x \in t\}\big)^t \mid \forall x\ (x \in t \Rightarrow f(x) \in u(x))\Big\}
\end{array}$$

(Remember that these notations are not macros, but that they denote the result of complex transformations in the term language of Z^{sk}.)

3 Sets as pointed graphs

In this section, we present the translation $(\_)^*$ of IZ into λZ using the representation of sets as pointed graphs [1]. This translation is basically the one presented by the author in [11, 12], except that:

- The target formalism λZ is slightly weaker than the formalism (i.e. $F\omega.3$) in which this translation was originally presented.
- We also prove the soundness of two additional axioms that are crucial to achieve the conservativity result (theorem 2) of section 4, namely: the anti-foundation axiom (AFA) and the axiom of the transitive closure (TC).

Before defining the translation, let us first recall the basic notions of the theory of pointed graphs (presented in set theory) that are needed to introduce the axiom of anti-foundation.

3.1 Pointed graphs and anti-foundation

In set theory, a *pointed graph* is a triple $\langle X, R, r\rangle$ formed by an arbitrary set X (the *carrier*) equipped with a binary relation $R \subset (X \times X)$ (the *edge relation*) and a distinguished element $r \in X$ (the *root*).

Given a binary relation R (on any set), we say that a function ϕ (whose domain is written D_ϕ) *decorates* R if for all $x \in D_\phi$ and for any set z, the relation $z \in \phi(x)$ holds iff there exists $x' \in D_\phi$ such that $z = \phi(x')$ and $\langle x', x\rangle \in R$. Finally, we say that a pointed graph $\langle X, R, r\rangle$ *pictures* a set x when there exists a decoration ϕ of R such that $r \in D_\phi$ and $\phi(r) = x$.

Formally, the relations $\mathrm{PGraph}(G)$ ('G is a pointed graph'), $\mathrm{Decor}(\phi, R)$ ('the function ϕ decorates R') and $\mathrm{Pict}(G, x)$ ('G pictures x') are defined by:[5]

$$\begin{aligned}
\mathrm{PGraph}(G) &\equiv \exists X\ \exists R\ \exists r\ [G = \langle X, R, r\rangle\ \wedge\ R \subset (X \times X)\ \wedge\ r \in X] \\
\mathrm{Decor}(\phi, R) &\equiv \forall x{\in}D_\phi\ \forall z\ [z \in \phi(x)\ \Leftrightarrow\ \exists x'{\in}D_\phi\ (z = \phi(x') \wedge \langle x', x\rangle \in R)] \\
\mathrm{Pict}(G, x) &\equiv \exists X\ \exists R\ \exists r\ \exists \phi\ [G = \langle X, R, r\rangle\ \wedge\ \mathrm{function}(\phi)\ \wedge \\
&\qquad\qquad \mathrm{Decor}(\phi, R)\ \wedge\ r \in D_\phi\ \wedge\ x = \phi(r)]
\end{aligned}$$

In ZF, it is easy to show that any pointed graph $G = \langle X, R, r\rangle$ whose root r is accessible[6] w.r.t. the relation R pictures a unique set.[7]

In presence of the axiom of foundation [8], this result cannot be extended further, for the relation $\mathrm{Pict}(\langle X, R, r\rangle, x)$ automatically implies the accessibility of the root r w.r.t. the relation R.

The axiom of anti-foundation (AFA) refutes the axiom of foundation by extending the latter result of existence and uniqueness to all the pointed graphs:

$$\text{(AFA)} \qquad \forall G\ [\mathrm{PGraph}(G)\ \Rightarrow\ \exists! x\ \mathrm{Pict}(G, x)]$$

Notice that this axiom has two parts: the existence part that allows to build arbitrarily non well-founded sets (for instance, a set x such that $x = \{x\}$), and the uniqueness part that allows to prove equalities between non-wellfounded sets (for instance, that any two sets x and y such that $x = \{x\}$ and $y = \{y\}$ are equal).

3.2 The axiom of transitive closure

In ZF it is easy to associate to each set x a pointed graph $\langle X, R, r\rangle$ that pictures x—a *representation* of x—simply by taking $X = \mathrm{Cl}(\{x\})$ the transitive closure of the singleton $\{x\}$, $R = \{(y', y) \in X \mid y' \in y\}$ and $r = x$.

---

[5] Formally, these definitions are expressed in the language of Z^{sk}, but in what follows we will consider them as definitions expressed in the ordinary language of set theory, implicitly using the deskolemisation procedure presented in section 2.

[6] The accessibility predicate $\mathrm{Acc}_R(x)$ is inductively defined on X by the unique clause: if $\mathrm{Acc}_R(y)$ for all $y \in X$ such that $\langle y, x\rangle \in R$, then $\mathrm{Acc}_R(x)$.

[7] Actually, the proof does not rely on classical principles and can be done in IZF_R (intuitionistic ZF with replacement). In IZ, only the uniqueness is provable.

Unfortunately, the latter construction relies on the existence of a transitive closure, which is not provable in Z [5]. For this reason, we consider the extension of Zermelo's system with the following axiom

$$\text{(TC)} \qquad \forall a\ \exists b\ [a \subset b\ \wedge\ \forall x\ (x \in b \Rightarrow x \subset b)]\,.$$

that expresses that any set is included in a transitive set. From this axiom it is easy to derive the expected representation property

$$\text{(Repr)} \qquad \forall x\ \exists G\ (\mathrm{PGraph}(G) \wedge \mathrm{Pict}(G, x))$$

using the construction described above.[8]

3.3 The translation of IZ into λZ

To each variable x of set theory we associate in λZ three object term variables written $\bar{x}$ (the carrier), $\tilde{x}$ (the relation) and $\dot{x}$ (the root), with types

$$\bar{x} : \Box_2, \qquad \tilde{x} : \bar{x} \to \bar{x} \to *, \qquad \dot{x} : \bar{x}\,,$$

that are intended to represent the set x as a pointed graph $(\bar{x}, \tilde{x}, \dot{x})$ in λZ. We also assume that for any pair x and y of distinct variables of set theory, the variables $\bar{x}$, $\tilde{x}$, $\dot{x}$, $\bar{y}$, $\tilde{y}$ and $\dot{y}$ are pairwise distinct.

Given a finite set X of variables of set theory, we denote by Γ_X the well-formed context of λZ given by

$$\Gamma_X \quad = \quad \bigcup_{x \in X} [\bar{x} : \Box_2;\ \tilde{x} : \bar{x} \to \bar{x} \to *,\ \dot{x} : \bar{x}]$$

(here, the union refers to a concatenation of contexts whose order is irrelevant).

Given two variables x and y of set theory, the relation $x = y$ that expresses the extensional equality of the sets x and y is interpreted in λZ as the *bisimilarity* of the pointed graphs $\langle \bar{x}, \tilde{x}, \dot{x} \rangle$ and $\langle \bar{y}, \tilde{y}, \dot{y} \rangle$, namely, as the proposition written $\langle \bar{x}, \tilde{x}, \dot{x} \rangle \approx \langle \bar{y}, \tilde{y}, \dot{y} \rangle$ and defined by

$$\begin{array}{l}
(\bar{x}, \tilde{x}, \dot{x}) \approx (\bar{y}, \tilde{y}, \dot{y}) \quad \equiv \\
\quad \exists r : (\bar{x} \to \bar{y} \to *)\,. \\
\quad\quad [\ R\ \dot{x}\ \dot{y} \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \wedge \\
\quad\quad\ \forall \alpha, \alpha' : \bar{x}\,.\, \forall \beta : \bar{y}\,.\, \big(\tilde{x}\ \alpha'\ \alpha\ \wedge\ r\ \alpha\ \beta\ \Rightarrow\ \exists \beta' : \bar{y}\,.\, (\tilde{y}\ \beta'\ \beta\ \wedge\ r\ \alpha'\ \beta')\big) \wedge \\
\quad\quad\ \forall \beta, \beta' : \bar{y}\,.\, \forall \alpha : \bar{x}\,.\, \big(\tilde{y}\ \beta'\ \beta\ \wedge\ r\ \alpha\ \beta\ \Rightarrow\ \exists \alpha' : \bar{x}\,.\, (\tilde{x}\ \alpha'\ \alpha\ \wedge\ r\ \alpha'\ \beta')\big)\ ]
\end{array}$$

To each formula ϕ of set theory we associate a proposition ϕ^* of λZ by setting

$$\begin{array}{rcll}
(x = y)^* & \equiv & (\bar{x}, \tilde{x}, \dot{x}) \approx (\bar{y}, \tilde{y}, \dot{y}) & \\
(x \in y)^* & \equiv & \exists z : \bar{y}\,.\, (\tilde{y}\ z\ \dot{y}\ \wedge\ (\bar{x}, \tilde{x}, \dot{x}) \approx (\bar{y}, \tilde{y}, z)) & \\
(\phi \wedge \psi)^* & \equiv & \phi^* \wedge \psi^* \qquad\qquad (\top)^* & \equiv\ \top \\
(\phi \vee \psi)^* & \equiv & \phi^* \vee \psi^* \qquad\qquad (\bot)^* & \equiv\ \bot \\
(\phi \Rightarrow \psi)^* & \equiv & \phi^* \Rightarrow \psi^* & \\
(\forall x\ \phi)^* & \equiv & \forall \bar{x} : \Box_2\,.\ \forall \tilde{x} : (\bar{x} \to \bar{x} \to *)\,.\ \forall \dot{x} : \bar{x}\,.\ \phi^* & \\
(\exists x\ \phi)^* & \equiv & \exists \bar{x} : \Box_2\,.\ \exists \tilde{x} : (\bar{x} \to \bar{x} \to *)\,.\ \exists \dot{x} : \bar{x}\,.\ \phi^* &
\end{array}$$

[8] The proposition (Repr) is actually equivalent to (TC) in IZ + AFA.

It is easy to check that $FV(\phi^*) = \bigcup_{x \in FV(x)} \{\bar{x}; \tilde{x}; \dot{x}\}$ and that $\Gamma_{FV(\phi)} \vdash \phi^* : *$.

Theorem 1 (Soundness). — *For all formulæ ϕ of set theory such that* IZ + AFA + TC $\vdash \phi$*, there is a proof-term t such that $\Gamma_{FV(\phi)} \vdash t : \phi^*$.*

Proof. See appendix B.

4 Retracting λZ in Z^{sk} + AFA

We now define a converse translation $(\_)^\dagger$ from λZ to IZ^{sk} + AFA, using the standard types-in-sets interpretation [13, 2]. Notice that here, we only need anti-foundation (AFA) to justify the existence of the set HF of hereditarily finite sets (a.k.a. V_ω) [8], which is used to interpret the sort $\Box_1$. [9]

4.1 The translation $M \mapsto M^\dagger$

Raw object terms of λZ (cf table 1) are translated into terms of Z^{sk} as follows:

$$\begin{array}{rcl}
x^\dagger & \equiv & x \\
*^\dagger & \equiv & \mathfrak{P}(\{\bullet\}) \\
\Box_1^\dagger & \equiv & \mathsf{HF} \\
\Box_2,\ \Box_3 & & \text{no translation} \\
(\Pi x : T\,.\,U)^\dagger & \equiv & \prod_{x \in T^\dagger} U^\dagger \\
(\lambda x : T\,.\,M)^\dagger & \equiv & \lambda x \in T^\dagger\,.\,M^\dagger \\
(MN)^\dagger & \equiv & M^\dagger(N^\dagger) \\
(A \Rightarrow B)^\dagger & \equiv & \{\pi \in \{\bullet\} \mid \bullet \in A^\dagger \Rightarrow \bullet \in B^\dagger\} \\
\forall x : \Box_2\,.\,A & \equiv & \{\pi \in \{\bullet\} \mid \forall x\ (\bullet \in A^\dagger)\} \\
\forall x : T\,.\,A & \equiv & \{\pi \in \{\bullet\} \mid \forall x\ (x \in T^\dagger \Rightarrow \bullet \in A^\dagger)\}
\end{array}$$

This translation is partial, and associates no term to the sorts $\Box_2$ and $\Box_3$. (Notice that $FV(M^\dagger) = FV(M)$ whenever $M^\dagger$ is defined.)

Propositions are interpreted in a proof-irrelevant way, as subsets of a singleton $\{\bullet\}$, where $\bullet$ is any closed term of Z^{sk}. We use here the standard trick by which any (intuitionistic) formula ϕ of Z^{sk} can be encoded as a subset $\hat{\phi} \subset \{\bullet\}$ by setting $\hat{\phi} = \{\pi \in \{\bullet\} \mid \phi\}$ whereas any subset $p \subset \{\bullet\}$ naturally decodes to the formula $\bullet \in p$. This correspondence between propositions and subsets of $\{\bullet\}$ is one-to-one,[10] in this sense that the equivalence $\phi \Leftrightarrow (\bullet \in \hat{\phi})$ is provable in IZ^{sk} (for all formulæ ϕ), as well as the implication $p \subset \{\bullet\} \Rightarrow (p = \widehat{\bullet \in p})$.

Up to this coding trick, the different kinds of universal quantifications are interpreted exactly as outlined in subsection 1.3. In particular, universal quantifications of the form $\forall x : \Box_2 \ldots$ are treated in a separate case, using unbounded quantification of set theory.

[9] Remember that the existence of the set HF of all hereditarily finite sets cannot be justified in IZ ([8], p. 238, exercise 10). This is no more the case if we extend the system with AFA, in which case HF can be reconstructed as the reification of a universal (and denumerable) pointed graph whose root points to all the finite trees.

[10] Classically, this is even more obvious since $\mathfrak{P}(\{\bullet\}) = \{\varnothing; \{\bullet\}\}$.

Contexts of λZ are translated as formulæ of Z^{sk} as follows:

$$\begin{array}{lcll}
([])^\dagger & \equiv & \top & \\
(\Gamma;\ x:\Box_2)^\dagger & \equiv & \Gamma^\dagger & \\
(\Gamma;\ x:T)^\dagger & \equiv & \Gamma^\dagger \wedge (x \in T^\dagger) & (\text{if } T \not\equiv \Box_2) \\
(\Gamma,\ \xi:A)^\dagger & \equiv & \Gamma^\dagger \wedge (\bullet \in A^\dagger) &
\end{array}$$

Notice that $FV(\Gamma^*) \subset FV(\Gamma)$. In particular, proof-term variables are systematically erased (as well as object term variables declared with type $\Box_2$.)

Proposition 7 (Soundness). — *For any derivable judgment of λZ of the form $\Gamma \vdash M : T$ where M and T are object terms such that T is neither $\Box_2$ nor $\Box_3$, one has:*

$$\mathrm{IZ}^{\mathrm{sk}} \ \vdash\ \Gamma^\dagger \ \Rightarrow\ M^\dagger \in T^\dagger$$

Proof. By induction on the derivation of $\Gamma \vdash M : T$.

Proposition 8 (Soundness). — *For any derivable judgment of λZ of the form $\Gamma \vdash t : A$ where t is a proof-term and A and object term, one has:*

$$\mathrm{IZ}^{\mathrm{sk}} \ \vdash\ \Gamma^\dagger \ \Rightarrow\ \bullet \in A^\dagger$$

Proof. By induction on the derivation of $\Gamma \vdash t : A$.

Since the equality $(\Pi x : * \,.\, x)^\dagger = \varnothing$ is easily provable in IZ, the latter proposition implies that the translation $M \mapsto M^\dagger$ transforms any inconsistency of λZ (given as a closed proof-term of $\Pi x : * \,.\, x$) into an inconsistency of IZ + AFA (expressed as a proof of $\bullet \in \varnothing$). Combining this with theorem 1 we get:

Proposition 9 (Equiconsistency). — *The theories* IZ + AFA + TC *and* λZ *are equiconsistent.*

However, this result of equiconsistency can be refined as a result of conservativity by studying the composition of the translations $(\_)^*$ and $(\_)^\dagger$.

4.2 Composing both translations

The translation $(\_)^*$ from IZ to λZ rephrases each formula of set theory in graph-theoretic terms by replacing each variable x (of set theory) by three variables $\bar{x} : \Box_2$, $\tilde{x} : \bar{x} \to \bar{x} \to *$ and $\dot{x} : \bar{x}$ that denote a pointed graph representing x.

Via the translation $(\_)^\dagger$, each type-theoretic pointed graph (X, R, r) becomes in turn a set-theoretic pointed graph $\langle X^\dagger, R^\dagger, r^\dagger \rangle$, up to this (minor) difference that the edge relation $R^\dagger$ is not given as a subset of $X^\dagger \times X^\dagger$, but as an element of the function space $X^\dagger \to X^\dagger \to \mathfrak{P}(\{\bullet\})$ which is clearly isomorphic to the set $\mathfrak{P}(X^\dagger \times X^\dagger)$ using the same coding trick as before. (For the sake of clarity, both sets $X \to X \to \mathfrak{P}(\{\bullet\})$ and $\mathfrak{P}(X \times X)$ will be identified in what follows.)

Consequently, the composition $(\_)^{*\dagger}$ of both translations is nothing but the graph-theoretic rephrasing of non-well founded set theory into set theory itself. Using the anti-foundation axiom AFA together with TC we easily close the diagram as follows:

Proposition 10 (Composition). — *Let ϕ be a formula of* IZ *with free variables $x_1, \dots, x_n$. If $y_1, \dots, y_n$ are variables such that the variables $x_1, \dots, x_n$, $\bar{y}_1, \dots, \bar{y}_n$, $\tilde{y}_1, \dots, \tilde{y}_n$ and $\dot{y}_1, \dots, \dot{y}_n$ are pairwise distinct, then:*

$$\mathrm{IZ} + \mathrm{AFA} + \mathrm{TC} \;\vdash\; \Big(\bigwedge_{i=1}^{n} \mathrm{Pict}\big((\bar{y}_i, \tilde{y}_i, \dot{y}_i),\ x_i\big)\Big) \;\Rightarrow\; (\phi \;\Leftrightarrow\; \bullet \in \phi\{\vec{x} := \vec{y}\}^{*\dagger})$$

Proof. By induction on the formula ϕ. AFA and TC are used to treat the case of atomic formulæ $x = y$ and $x \in y$ as well as quantifiers $\forall x\ \psi$ and $\exists x\ \psi$. □

When ϕ is a closed formula, the equivalence $\phi \Leftrightarrow \bullet \in \phi^{*\dagger}$ is thus provable in IZ + AFA + TC. Consequently:

Theorem 2 (Conservativity). — *Via the embedding $\phi \mapsto \phi^*$, λZ is a conservative extension of* IZ + AFA + TC.

References

1. P. Aczel. Non well-founded sets. *Center for the Study of Language and Information*, 1988.
2. Peter Aczel. On relating type theories and set theories. In Thorsten Altenkirch, Wolfgang Naraschewski, and Bernhard Reus, editors, *TYPES*, volume 1657 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 1998.
3. Henk Barendregt and Herman Geuvers. Proof-assistants using dependent type systems. In John Alan Robinson and Andrei Voronkov, editors, *Handbook of Automated Reasoning*, pages 1149–1238. Elsevier and MIT Press, 2001.
4. Thierry Coquand and Hugo Herbelin. A-translation and looping combinators in pure type systems. *Journal of Functional Programming*, 4(1):77–88, 1994.
5. Olivier Esser and Roland Hinnion. Antifoundation and transitive closure in the system of Zermelo. *Notre Dame Journal of Formal Logic*, 40(2):197–205, 1999.
6. H. Friedman. Some applications of Kleene's methods for intuitionistic systems. In *Cambridge Summer School in Mathematical Logic*, volume 337 of *Springer Lecture Notes in Mathematics*, pages 113–170. Springer-Verlag, 1973.
7. J.H. Geuvers and M.J. Nederhof. A modular proof of strong normalization for the calculus of constructions. In *Journal of Functional Programming*, volume 1,2(1991), pages 155–189, 1991.
8. J.-L. Krivine. *Théorie des ensembles.* Cassini, 1998.
9. Z. Luo. *Computation and Reasoning: A Type Theory for Computer Science.* Oxford University Press, 1994.
10. Paul-André Melliès and Benjamin Werner. A generic normalisation proof for pure type systems. In Eduardo Giménez and Christine Paulin-Mohring, editors, *TYPES*, volume 1512 of *Lecture Notes in Computer Science*, pages 254–276. Springer, 1996.
11. A. Miquel. *Le calcul des constructions implicite: syntaxe et sémantique.* PhD thesis, Université Paris 7, 2001.
12. Alexandre Miquel. A strongly normalising Curry-Howard correspondence for IZF set theory. In Matthias Baaz and Johann A. Makowsky, editors, *CSL'03*, volume 2803 of *Lecture Notes in Computer Science*, pages 441–454. Springer, 2003.
13. Benjamin Werner. Sets in types, types in sets. In Martín Abadi and Takayasu Ito, editors, *TACS*, volume 1281 of *Lecture Notes in Computer Science*, pages 530–346. Springer, 1997.

A Soundness of deskolemisation (from IZ$^{\mathrm{sk}}$ to IZ)

The proof of the soundness of the deskolemisation procedure (Prop. 4) actually involves several intermediate steps that we briefly sketch here.

Fact 2 — *For all terms t and formulæ ϕ of the language of* Z$^{\mathrm{sk}}$*, one has* $FV(z \in^\circ t) = FV(t) \cup \{z\}$ *and* $FV(\phi^\circ) = FV(\phi)$.

Proof. By mutual induction on t and ϕ. □

To prove that the deskolemisation procedure transforms each theorem ϕ of (I)Z$^{\mathrm{sk}}$ into a theorem ϕ° of (I)Z, we first check that each term of the extended language Z$^{\mathrm{sk}}$ corresponds to a set whose existence can be proved in Z:

Lemma 2 (Collection). — *For each term t of* Z$^{\mathrm{sk}}$*, one has:*

$$\mathrm{IZ} \;\vdash\; \exists x\, \forall z\, [z \in x \Leftrightarrow z \in^\circ t] \qquad (x \text{ and } z \text{ fresh})$$

Proof. By structural induction on t, using the corresponding existential axiom of Zermelo's system for each syntactic construct of the term algebra of Z$^{\mathrm{sk}}$. □

Lemma 3. — *For each axiom ϕ of* Z$^{\mathrm{sk}}$*, one has:* $\mathrm{IZ} \vdash \phi^\circ$.

Notice that for all axioms ϕ of Z$^{\mathrm{sk}}$, the proof of ϕ° only relies on the equality axioms and the axiom of extensionality. In the deskolemisation process, Zermelo's existential axioms actually play their role in the deduction rules that involve a substitution, and whose translation relies on the following lemma:

Lemma 4 (Substitutivity). — *For all formulæ ϕ and for all terms t and u of* Z$^{\mathrm{sk}}$ *one has the equivalences:*

1. $\mathrm{IZ} \;\vdash\; y \in^\circ t\{x := u\} \;\Leftrightarrow\; \exists x\, [y \in^\circ t \;\wedge\; \forall z\, (z \in x \Leftrightarrow z \in^\circ u)] \quad (y \not\equiv x)$
2. $\mathrm{IZ} \;\vdash\; (\phi\{x := u\})^\circ \;\Leftrightarrow\; \exists x\, [\phi^\circ \;\wedge\; \forall z\, (z \in x \Leftrightarrow z \in^\circ u)]$

Proof. We first prove by mutual induction on t and ϕ that:

1. $\mathrm{IZ} \;\vdash\; \forall x\, [\forall z\, (z \in x \Leftrightarrow z \in^\circ u) \;\Rightarrow\; \forall z\, (z \in^\circ t\{x := u\} \Leftrightarrow z \in^\circ t)]$
2. $\mathrm{IZ} \;\vdash\; \forall x\, [\forall z\, (z \in x \Leftrightarrow z \in^\circ u) \;\Rightarrow\; (\phi\{x := u\}^\circ \Leftrightarrow \phi)]$

We then conclude that the desired equivalences hold by using lemma 2, whose proof relies on Zermelo's existential axioms. □

Lemma 5 (Deskolemisation of a derivation). — *Let A be a formula and Γ a list of formulæ both expressed in the language of* Z$^{\mathrm{sk}}$*. If $\Gamma \vdash A$ is classically (resp. intuitionistically) derivable, then there exists a list Δ of axioms of* Z *such that $\Delta, \Gamma^\circ \vdash A^\circ$ is classically (resp. intuitionistically) derivable.*

Proof. By induction on the derivation of $\Gamma \vdash A$. The only interesting cases correspond to the rules ∀-elim and ∃-intro, whose translation rely on lemma 4. □

From lemmas 3 and 5 it is then clear that:

Proposition 11 (Soundness of deskolemisation). — *If a closed formula ϕ is a theorem of* (I)Z$^{\mathrm{sk}}$*, then ϕ° is a theorem of* (I)Z.

B Soundness of the translation $\phi \mapsto \phi^*$

The translation $(\_)^*$ from IZ $(+\,\mathrm{AFA} + \mathrm{TC})$ into λZ depicted in section 3 is actually a fragment of a translation of $\mathrm{IZ}^{\mathrm{sk}}$ $(+\,\mathrm{AFA} + \mathrm{TC})$ into λZ, in which the pointed graphs associated to sets are explicitly built from the terms of Z^{sk}.

Formally, this translation maps

- Each variable x of set theory to three variables $\bar{x}$, $\tilde{x}$ and $\dot{x}$ of λZ, declared (in this order) as follows: $\bar{x} : \Box_2$, $\tilde{x} : \bar{x} \to \bar{x} \to *$, $\dot{x} : \bar{x}$.
- Each formula ϕ of the language of Z^{sk} to a term ϕ of λZ of type $*$ in the typing context associated to the free variables of ϕ.
- Each term t of the language of Z^{sk} to three terms $t^{\bar{*}} : \Box_2$, $t^{\tilde{*}} : t^{\bar{*}} \to t^{\bar{*}} \to *$ and $t^* : t^{\bar{*}}$ of λZ (in the typing context associated to the free variables of t) that respectively represent the carrier, the edge relation and the root of the pointed graph that represents the set denoted by t in λZ.

B.1 Logic and data types

The formal definition of the translation relies on the usual second-order encodings of connectives, existential quantifier and Leibniz equality in λZ:

$$\begin{array}{rcl@{\qquad}rcl}
\bot & \equiv & \forall \gamma : * \,.\, \gamma & \top & \equiv & \forall \gamma : * \,.\, (\gamma \Rightarrow \gamma) \\
A \wedge B & \equiv & \forall \gamma : * \,.\, ((A \Rightarrow B \Rightarrow \gamma) \;\Rightarrow\; \gamma) & & & \\
A \vee B & \equiv & \forall \gamma : * \,.\, ((A \Rightarrow \gamma) \;\Rightarrow\; (B \Rightarrow \gamma) \;\Rightarrow\; \gamma) & & & \\
\exists x : T \,.\, A(x) & \equiv & \forall \gamma : * \,.\, (\forall x : T \,.\, (A(x) \Rightarrow \gamma) \;\Rightarrow\; \gamma) & & & \\
x =_T y & \equiv & \forall \gamma : (T \to *) \,.\, (\gamma\ x \Rightarrow \gamma\ y) & & &
\end{array}$$

Given two types $X, Y : \Box_2$ we define two data-types $\mathsf{opt}(X) : \Box_2$ ('pseudo option type') and $\mathsf{sum}(X, Y) : \Box_2$ ('pseudo union type') as follows:

$$\begin{array}{lcll@{\qquad}l}
\mathsf{opt}(X) & : & \Box_2 & \equiv & (X \to *) \to * & \\
\mathsf{some}(X, x) & : & \mathsf{opt}(X) & \equiv & \lambda f : (X \to *) \,.\, f\ x & (x : X) \\
\mathsf{none}(X) & : & \mathsf{opt}(X) & \equiv & \lambda f : (X \to *) \,.\, \bot & \\
\mathsf{sum}(X, Y) & : & \Box_2 & \equiv & (X \to *) \to (Y \to *) \to * & \\
\mathsf{inl}(X, Y, x) & : & \mathsf{sum}(X, Y) & \equiv & \lambda f : (X \to *) \,.\, \lambda g : (Y \to *) \,.\, f\ x & (x : X) \\
\mathsf{inr}(X, Y, y) & : & \mathsf{sum}(X, Y) & \equiv & \lambda f : (X \to *) \,.\, \lambda g : (Y \to *) \,.\, g\ y & (y : Y) \\
\mathsf{out}(X, Y) & : & \mathsf{sum}(X, Y) & \equiv & \lambda f : (X \to *) \,.\, \lambda g : (Y \to *) \,.\, \bot &
\end{array}$$

It can be shown [11] that the constructions $\mathsf{some}(X, x)$ and $\mathsf{none}(X)$ (for the data type $\mathsf{opt}(X)$) and the constructions $\mathsf{inl}(X, Y, x)$, $\mathsf{inr}(X, Y, y)$ and $\mathsf{out}(X, Y)$ (for the data type $\mathsf{sum}(X, Y)$) behave as constructors in the sense that they enjoy the expected properties of injectivity and non-confusion. On the other hand, these data types (that actually contain much more values than the ones introduced by the constructors) have no associated elimination principle.

The type nat of Church numerals is easily constructed in $\Box_2$ as shown below. As usual, this definition is accompanied with a relativisation predicate $\mathsf{wf\_nat}(n)$

which captures the induction strength. We also introduce the definition of large and strict ordering on natural numbers:

$$\begin{array}{lcl}
\mathsf{nat} & \equiv & \Pi Z : \Box_1 \,.\, (Z \to (Z \to Z) \to Z) \\
\mathsf{0} & \equiv & \lambda Z : \Box_1 \,.\, \lambda z : Z \,.\, \lambda f : (Z \to Z) \,.\, z \\
\mathsf{S}(n) & \equiv & \lambda Z : \Box_1 \,.\, \lambda z : Z \,.\, \lambda f : (Z \to Z) \,.\, f\ (n\ Z\ z\ f)
\end{array}$$

$$\begin{array}{lcl}
n \leq m & \equiv & \forall P : (\mathsf{nat} \to *) \,.\, (P\ n\ \Rightarrow\ \forall z : \mathsf{nat} \,.\, (P\ z \Rightarrow\ P\ \mathsf{S}(z))\ \Rightarrow\ P\ m) \\
n < m & \equiv & \mathsf{S}(n) \leq m \qquad\qquad \mathsf{wf_nat}(n)\ =\ \mathsf{0} \leq n
\end{array}$$

(assuming n, m : nat). This encoding is sound w.r.t. all principles of Heyting arithmetic provided all quantifications on the type nat are relativised to the class defined by the predicate $\mathsf{wf\_nat}$.

B.2 Translation of terms and formulæ

The four transformations $\phi \mapsto \phi^*$ (proposition), $t \mapsto t^{\bar{*}}$ (carrier), $t \mapsto t^{\tilde{*}}$ (edge relation) and $t \mapsto t^{\dot{*}}$ (root) are defined by mutual induction on ϕ and t.

Translation of formulæ The translation $\phi \mapsto \phi^*$ is defined by:

$$\begin{array}{lcll}
(t = u)^* & \equiv & (t^{\bar{*}}, t^{\tilde{*}}, t^{\dot{*}}) \approx (u^{\bar{*}}, u^{\tilde{*}}, u^{\dot{*}}) & \\
(t \in u)^* & \equiv & \exists \beta : u^{\tilde{*}} \,.\, (u^{\tilde{*}}\ \beta\ u^*\ \wedge\ (t^{\bar{*}}, t^{\tilde{*}}, t^{\dot{*}}) \approx (u^{\bar{*}}, u^{\tilde{*}}, \beta) & \\
(\phi \diamond \psi)^* & \equiv & \phi^* \diamond \psi^* \qquad U^*\ \equiv\ U & (\diamond = \wedge, \vee, \Rightarrow \quad U = \top, \bot) \\
(Q x\ \phi)^* & \equiv & Q \bar{x} : \Box_2 \,.\ Q \tilde{x} : (\bar{x} \to \bar{x} \to *) \,.\ Q \dot{x} : \bar{x} \,.\ \phi^* & (Q = \forall, \exists)
\end{array}$$

(where $\approx$ denotes the type-theoretic expression of the bisimilarity relation, that has been already given in subsection 3.3).

Translation of terms The translations $t \mapsto t^{\bar{*}}$, $t \mapsto t^{\tilde{*}}$ and $t \mapsto t^{\dot{*}}$ are defined in table 6. For the sake of clarity, we omit type parameters X and Y in the constructors some, none, inl, inr, out and Leibniz equality '='.

B.3 Soundness of the axioms of IZ$^{\mathrm{sk}}$

Lemma 6. — *For each axiom ϕ of* IZ$^{\mathrm{sk}}$*, the proposition $\phi^* : *$ has a closed proof-term in* λZ*.*

The proof essentially proceeds as in [11], except that the target formalism λZ is slightly weaker than $F\omega.3$, in which the translation was originally presented. Technically, the difference appears with the comprehension scheme, whose translation in $F\omega.3$ benefits from the possibility of encoding class abstraction (using the rule $(\Box_3, \Box_1, \Box_3)$) and class quantification (using rule $(\Box_3, *, *)$) so that comprehension can be expressed as a single proposition.[11] In λZ however, class abstraction is not possible anymore, and each instance of the comprehension scheme has to be translated separately.

[11] The main reason is that $F\omega.3$ ($\supsetneq \lambda$Z) actually captures the strength of IZω (intuitionistic higher-order Zermelo's set theory.

Variables

$$x^{\bar{*}} \;\equiv\; \bar{x}, \qquad x^{\tilde{*}} \;\equiv\; \tilde{x} \qquad \text{and} \qquad x^{\dot{*}} \;\equiv\; \dot{x}$$

Set of von Neumann numerals

$$\omega^{\bar{*}} \;\equiv\; \mathsf{opt}(\mathsf{nat}), \qquad\qquad \omega^{\dot{*}} \;\equiv\; \mathsf{none}$$

$$\begin{aligned}\omega^{\tilde{*}} \;\equiv\;& \lambda\beta', \beta : \mathsf{opt}(\mathsf{nat})\,.\\ & \quad \exists n', n : \mathsf{nat}\,.\,\big(\mathsf{wf\_nat}(n') \;\wedge\; \beta' = \mathsf{some}(n') \;\wedge\\ & \qquad\qquad \mathsf{wf\_nat}(n) \;\wedge\; \beta = \mathsf{some}(n) \;\wedge\; n' < n\big)\\ & \vee\; \exists n' : \mathsf{nat}\,.\,\big(\mathsf{wf\_nat}(n') \;\wedge\; \beta' = \mathsf{some}(n') \;\wedge\; \beta = \mathsf{none}\big)\end{aligned}$$

Unordered pair

$$\{t_1; t_2\}^{\bar{*}} \;\equiv\; \mathsf{sum}(t_1^{\bar{*}}, t_2^{\bar{*}}), \qquad\qquad \{t_1; t_2\}^{\dot{*}} \;\equiv\; \mathsf{out}$$

$$\begin{aligned}\{t_1; t_2\}^{\tilde{*}} \;\equiv\;& \lambda\beta', \beta : \mathsf{sum}(t_1^{\bar{*}}, t_2^{\bar{*}})\,.\\ & \quad \exists\alpha', \alpha : t_1^{\bar{*}}\,.\,\big(\beta' = \mathsf{inl}(\alpha') \;\wedge\; \beta = \mathsf{inl}(\alpha) \;\wedge\; t_1^{\tilde{*}}\;\alpha'\;\alpha\big)\\ & \vee\; \exists\alpha', \alpha : t_2^{\bar{*}}\,.\,\big(\beta' = \mathsf{inr}(\alpha') \;\wedge\; \beta = \mathsf{inr}(\alpha) \;\wedge\; t_2^{\tilde{*}}\;\alpha'\;\alpha\big)\\ & \vee\; \big(\beta' = \mathsf{inl}(t_1^{*}) \;\wedge\; \beta = \mathsf{out}\big)\\ & \vee\; \big(\beta' = \mathsf{inr}(t_2^{\dot{*}}) \;\wedge\; \beta = \mathsf{out}\big)\big)\end{aligned}$$

Powerset

$$(\mathfrak{P}(t))^{\bar{*}} \;\equiv\; \mathsf{sum}(t^{\bar{*}}, t^{\bar{*}}{\to}*), \qquad\qquad (\mathfrak{P}(t))^{\dot{*}} \;\equiv\; \mathsf{out}$$

$$\begin{aligned}(\mathfrak{P}(t))^{\tilde{*}} \;\equiv\;& \lambda\beta', \beta : \mathsf{sum}(t^{\bar{*}}, t^{\bar{*}}{\to}*)\,.\\ & \quad \exists\alpha', \alpha : t^{\bar{*}}\,.\,\big(\beta' = \mathsf{inl}(\alpha') \;\wedge\; \beta = \mathsf{inl}(\alpha) \;\wedge\; t_1^{\tilde{*}}\;\alpha'\;\alpha\big)\\ & \vee\; \exists\alpha : t^{\bar{*}}\,.\,\exists p : (t^{\bar{*}}{\to}*)\,.\,\big(\beta' = \mathsf{inl}(\alpha) \;\wedge\; \beta = \mathsf{inr}(p) \;\wedge\; t^{\tilde{*}}\;\alpha\;t^{\dot{*}} \;\wedge\; p\;\alpha\big)\\ & \vee\; \exists p : (t^{\bar{*}}{\to}*)\,.\,\big(\beta' = \mathsf{inr}(p) \;\wedge\; \beta = \mathsf{out}\big)\end{aligned}$$

Union

$$(\bigcup t)^{\bar{*}} \;\equiv\; \mathsf{opt}(t^{\bar{*}}), \qquad\qquad (\bigcup t)^{\dot{*}} \;\equiv\; \mathsf{none}$$

$$\begin{aligned}(\bigcup t)^{\tilde{*}} \;\equiv\;& \lambda\beta', \beta : \mathsf{opt}(t^{\bar{*}})\,.\\ & \quad \exists\alpha', \alpha : t^{\bar{*}}\,.\,\big(\beta' = \mathsf{some}(\alpha') \;\wedge\; \beta = \mathsf{some}(\alpha) \;\wedge\; t^{\tilde{*}}\;\alpha'\;\alpha\big)\\ & \vee\; \exists\alpha', \alpha : t^{\bar{*}}\,.\,\big(\beta' = \mathsf{some}(\alpha') \;\wedge\; \beta = \mathsf{none} \;\wedge\; t^{\tilde{*}}\;\alpha'\;\alpha \;\wedge\; t^{\tilde{*}}\;\alpha\;t^{\dot{*}}\big)\end{aligned}$$

Comprehension

$$(\{x \in t \mid \phi\})^{\bar{*}} \;\equiv\; \mathsf{opt}(t^{\bar{*}}), \qquad\qquad (\{x \in t \mid \phi\})^{\dot{*}} \;\equiv\; \mathsf{none}$$

$$\begin{aligned}(\{x \in t \mid \phi\})^{\tilde{*}} \;\equiv\;& \lambda\beta', \beta : \mathsf{opt}(t^{\bar{*}})\,.\\ & \quad \exists\alpha', \alpha : t^{\bar{*}}\,.\,\big(\beta' = \mathsf{some}(\alpha') \;\wedge\; \beta = \mathsf{some}(\alpha) \;\wedge\; t^{\tilde{*}}\;\alpha'\;\alpha\big)\\ & \vee\; \exists\alpha : t^{\bar{*}}\,.\,\big(\beta' = \mathsf{some}(\alpha) \;\wedge\; \beta = \mathsf{none} \;\wedge\\ & \qquad\qquad t^{\tilde{*}}\;\alpha\;t^{*} \;\wedge\; \phi^{*}\{\bar{x} := t^{\bar{*}}; \tilde{x} := t^{\tilde{*}}; \dot{x} := \alpha\}\big)\end{aligned}$$

Table 6. Translation of the terms of Z^{sk} in $\lambda\mathrm{Z}$

B.4 Soundness of anti-foundation

The soundness of AFA in λZ is an exercise of decoding a pointed graph structure from the type-theoretic representation of a set-theoretic pointed graph.

Let us assume that (X, R, r) is a type-theoretic pointed graph that represents a set-theoretic pointed graph, that is, three terms

$$X : \Box_2, \qquad R : X \to X \to * \qquad \text{and} \qquad r : X$$

of λZ such that the proposition $\mathrm{PGraph}^*(X, R, r)$ is provable in λZ, where PGraph is the set-theoretic predicate defined by

$$\mathrm{PGraph}(x) \;\equiv\; \exists x_1\, \exists x_2\, \exists x_3\, [G = \langle x_1, x_2, x_3\rangle \;\wedge\; x_2 \subset (x_1 \times x_1) \;\wedge\; x_3 \in x_1]$$

From the assumption $\mathrm{PGraph}^*(X, R, r)$, we can easily extract three pointed graphs (X_1, R_1, r_1), (X_2, R_2, r_2) and (X_3, R_3, r_3) representing the three components x_1, x_2 and x_3 of the set-theoretic triple represented by (X, R, r). In particular, we know that $x_3 \in x_1$ so that there is a vertex $\alpha_0 : X_1$ such that the pointed graphs (X_3, R_3, r_3) and (X_1, R_1, α_0) are bisimilar.

We now have to build in λZ a pointed graph (Y, S, s) that represents the set pictured by the set-theoretic pointed graph whose carrier, edge relation and root are represented by the pointed graphs (X_1, R_1, r_1), (X_2, R_2, r_2) and (X_3, R_3, r_3). This pointed graph (Y, S, s) is constructed from the pointed graph (X_1, R_1, r_1) by changing the edge relation and root as follows:

$$\begin{array}{lcll} Y & \equiv & X_1 & \qquad s \;\equiv\; \alpha \\ S & \equiv & \lambda\alpha', \alpha : X_1\,. & R_1\ \alpha'\ r_1 \;\wedge\; R_1\ \alpha\ r_1 \;\wedge \\ & & & \mathrm{Rel}^*((X_1, R_1, \alpha'), (X_1, R_1, \alpha), (X_2, R_2, r_2)) \end{array}$$

where $\mathrm{Rel}(x, y, z)$ is the set-theoretic formlula $\langle x, y\rangle \in z$. We then check that $\mathrm{Pict}^*((X, R, r), (Y, S, s))$ holds in λZ, and that any pointed graph (Y', S', s') such that $\mathrm{Pict}^*((X, R, r), (Y', S', s'))$ is bisimilar to (Y, S, s). (The proof is the type-theoretic transposition of the validity proof of AFA presented in [1].)

B.5 Soundness of transitive closure

The transitive closure of a pointed graph (X, R, r) is represented in λZ as the pointed graph (Y, S, s) whose components are given by:

$$\begin{array}{lcll} Y & \equiv & \mathsf{opt}(X) & \qquad s \;\equiv\; \mathsf{none} \\ S & \equiv & \lambda\beta', \beta : Y\,. & \\ & & \quad \exists\alpha', \alpha : X\,. \big(\beta' = \mathsf{some}(\alpha') \;\wedge\; \beta = \mathsf{some}(\alpha) \;\wedge\; R\ \alpha'\ \alpha\big) & \\ & & \quad \vee\, \exists\alpha : X\,. \big(\beta' = \mathsf{some}(\alpha) \;\wedge\; \beta = \mathsf{none} \;\wedge\; R^+\ \alpha\ r & \end{array}$$

where R^+ denotes the transitive closure of R (expressed in λZ), namely, the binary relation on X defined by

$$\begin{array}{lcl} R^+ & \equiv & \lambda\alpha_1, \alpha_2 : X\,.\ \forall r : (X \to X \to *)\,. \\ & & \quad [\forall\alpha', \alpha : X\,. (R\ \alpha'\ \alpha \Rightarrow r\ \alpha'\ \alpha) \quad \wedge \\ & & \quad\ \forall\alpha'', \alpha', \alpha : X\,. (r\ \alpha''\ \alpha' \;\Rightarrow\; r\ \alpha'\ \alpha \;\Rightarrow\; r\ \alpha''\ \alpha) \\ & & \quad\ \Rightarrow\ \ r\ \alpha_1\ \alpha_2]\,. \end{array}$$