A Typed Formulation of the Semantics of Z

R.D. Arthan
rda@lemma-one.com

10 May 2000

Abstract

This document is a companion to Ian Toyn's presentation of the semantics of Z that is now in the draft Z standard. It contains a reformulation of the semantics within the ProofPower-Z dialect of Z that has been type-checked using ProofPower. The purpose of the document is to act as a check on the definition of the semantics. It also highlights certain points of interest in the required structure of the semantic universe $\mathbb{U}$.

Z Standards Document References

Version 1	20th May 1998	D-235
Version 2	10th May 2000	D-256

1 INTRODUCTION

In 1998, Ian Toyn and I developed a definition of the semantics of the kernel sublanguage of Z. With some modifications as a result of review, this work is now captured in the draft Z standard. The definition is written in first-order set theory using a surface syntax borrowed from Z itself.

An advantage of using the Z-like surface syntax is that with only small adjustments, and without having to define a large number of auxiliary functions, the definition can be viewed as a Z specification and so can be analysed using tools that support Z. As a step in this direction, this document presents a reformulation of the semantic definitions in the ProofPower-Z dialect.

Processing the specification with ProofPower reveals that the semantic definitions are now well-typed in some sense. It is, presumably, useful to know this, since preparing this Z version revealed several minor errors and highlighted some issues. The Z formulation also points up the places at which the type constraints of Z kick in to ensure that the semantic equations are well-defined.

This document is subject to the following cautionary remarks:

- No attempt has been made to make the formal material in this document intelligible independently of the narrative in the draft Z standard: please do *not* start here!
- In several places, I have simply said that things are done in the same order as the original. The intention is that you can put the two documents side by side and compare, and you may well need to do that in order to understand what has been done here.
- Meaning has been sacrificed in favour of surface syntax in this document. A reasonably close syntactic correspondence between the original and the Z version has been maintained by trickery that would detract from semantic analysis of the semantics.
- The transcription into Z has not been done by automated means. Errors of transcription that are not detected by Z type-checking may well persist.
- The current version of this document is based on the August 1999 Committee Draft of the Z Standard (the "1999 CD"). Earlier versions of this documented resulted in the detection of several errors. These have been corrected in the August 1999 draft.
- Some corrections or improvements to the 1999 CD have been applied. See sections 4.3, 4.4.3, 4.6.14 and 4.7.6 below.

The remainder of this document is organised as follows:

Section 2 describes our version of the semantic universe. Because we have to obey the Z type discipline, several transfer functions are needed to stand in for the untyped constructions of the original.

Section 3 gives a Z definition of the kernel abstract syntax sufficient for present needs.

Section 4 gives a few preliminaries that enable us to give the equations in a syntax like that of the original and then gives the Z axioms that model the semantic equations.

Section 5 lists the type assignment generated by ProofPower for the specification.

Section 6 gives an index to the global variables declared in the specification. Global variables are generally shown in bold face at the point of their declaration.

2 SEMANTIC UNIVERSE

Our setup for the semantic universe is necessarily slightly different from the untyped original. First we introduce $\mathbb{U}$ as a given set and then introduce its subsets $NAME$ and $\mathbb{W}$:

$[\ \mathbb{U}\ ]$

$$
\begin{array}{|l}
\boldsymbol{NAME}, \mathbb{W} : \mathbb{P}\ \mathbb{U} \\
\hline
NAME \subseteq \mathbb{W}
\end{array}
$$

$\mathbb{W}$ is a model of a world of pure sets — each member of $\mathbb{W}$ itself represents a set of elements of $\mathbb{W}$. To describe this situation in Z, one possibility would be to introduce a binary relation on $\mathbb{W}$ corresponding to the membership relation in the world of sets. In the present context, it is technically more convenient to introduce a function, η, that maps an element $A \in \mathbb{W}$ to the subset of $\mathbb{W}$ that A represents. We call $\eta(A)$ the *extent* of A. Since we expect the world of sets to be extensional, i.e., we expect two sets to be equal if and only if they have the same elements, η will be an injective function. We also expect that, for any $A \in \mathbb{W}$, there will be a unique element of $\mathbb{W}$ representing the power set of A. Accordingly, we introduce a function, $\mathbb{P}_W$, that sends a set $A \in \mathbb{W}$ to the member of $\mathbb{W}$ that represents its power set. The expected interrelationship of the extent and power set functions gives rise to the defining property in the following:

$$
\begin{array}{|l}
\boldsymbol{\eta} : \mathbb{W} \rightarrowtail \mathbb{P}\ \mathbb{W}; \\
\mathbb{P}_{\boldsymbol{W}} : \mathbb{W} \rightarrowtail \mathbb{W} \\
\hline
\forall\ w : \mathbb{W} \bullet\ \eta(\!|\eta(\mathbb{P}_W\ \ w)|\!) = \mathbb{P}(\eta\ \ w)
\end{array}
$$

Z having reserved superscription for something else, instead of A^k, we use the notation $A \uparrow k$ for the k-fold cartesian product of a set A:

fun $\_ \uparrow \_$

$$
\begin{array}{|l}
[X] \\
\hline
\_\uparrow\_ : (\mathbb{P}\ X \times \mathbb{N}) \rightarrow \mathbb{P}\ (seq\ X) \\
\hline
\forall A : \mathbb{P}X;\ k : \mathbb{N} \bullet\ A \uparrow k = (1..k) \rightarrow A
\end{array}
$$

Now we define functions that transfer between various typed constructions on $\mathbb{W}$ and the untyped universe $\mathbb{U}$. There are three such constructions corresponding to the semantic values of bindings (β), finite sets (ϕ), tuples (χ), and generics (γ). All but the last of these constructions can be carried out within $\mathbb{W}$ itself. We give axioms relating the first four to one another and to the extent operator, η. No property is required of γ other than that it be an injection.

$$
\begin{array}{|l}
\boldsymbol{\beta} : (NAME \mathrel{+\!\!\!\twoheadrightarrow} \mathbb{W}) \rightarrowtail \mathbb{W};\\
\boldsymbol{\phi} : \mathbb{F}\ \mathbb{W} \rightarrowtail \mathbb{W};\\
\boldsymbol{\chi} : \bigcup\{k : \mathbb{N}_1 \bullet \mathbb{W} \uparrow k\} \rightarrowtail \mathbb{W};\\
\boldsymbol{\gamma} : \bigcup\{k : \mathbb{N}_1 \bullet (\mathbb{W} \uparrow k) \rightarrow \mathbb{W}\} \rightarrowtail \mathbb{U}\\
\hline
\forall i : NAME;\ w : \mathbb{W};\ t : NAME \mathrel{+\!\!\!\twoheadrightarrow} \mathbb{W} \bullet\\
\qquad i \mapsto w \in t \Leftrightarrow \chi\ \langle i,\ w\rangle \in \eta(\beta\ t);\\
\forall a : \mathbb{F}\ \mathbb{W};\ w : \mathbb{W} \bullet\ w \in a \Leftrightarrow w \in \eta(\phi\ a);\\
\exists\ \nu : \mathbb{N} \rightarrowtail \mathbb{W} \bullet \forall s : \bigcup\{k : \mathbb{N}_1 \bullet \mathbb{W} \uparrow k\};\ i : \mathbb{N};\ w : \mathbb{W} \bullet\\
\qquad i \mapsto w \in s \Leftrightarrow \chi\ \langle \nu\ i,\ w\rangle \in \eta(\chi\ \ s)
\end{array}
$$

Small names (lower-case Greek letters) have been deliberately chosen for the various transfer functions above. All such functions would be represented by the identity function in an untyped universe. So when comparing this document with the original, if you see a lower-case Greek letter or a composite of Greek letters and possibly their inverses, you can simply ignore it. The inverses crop up at precisely those points where the type rules imply that an object will have a certain form (say a binding) and so will be in the domain of the appropriate inverse function ($\beta^{\sim}$).

3 SYNTAX

We need to develop a Z model of the abstract syntax which forms the domain of the semantic bracket functions. The treatment below is completely customised for the task at hand. E.g., type annotations are only inserted where they are actually used.

We make use of fixity declarations and exploit the fact that ProofPower does not require the chevrons in a free type definition. Within each category, the various alternatives are listed in the same order as the corresponding semantic equations are given in the original, q.v. Occasionally, we introduce additional syntactic categories (e.g., for an individual declaration) just to gain a surface syntax effect. Dependencies between the categories mean that the categories are treated in the opposite order to the original (bottom-up rather than top-down).

3.1 Type

fun $\_ :_t \_,$
$[_t \ldots]_t,$
$(_\times \ldots)_\times,$
$\lambda_t \ldots \bullet_t \_$

$$
\begin{array}{lll}
\boldsymbol{TYPE} & ::= & \textbf{\textit{given}}\ NAME \\
 & | & \textbf{\textit{generic}}\ NAME \\
 & | & \mathbb{P}_{\boldsymbol{t}}\ TYPE \\
 & | & (_{\times}\ seq\ TYPE\ )_{\times} \\
 & | & [_{\boldsymbol{t}}\ seq\ DECL\ ]_{\boldsymbol{t}} \\
 & | & \boldsymbol{\lambda}_{\boldsymbol{t}}\ seq\ NAME\ \bullet_{\boldsymbol{t}}\ TYPE \\
\&\ \boldsymbol{DECL} & ::= & NAME\ \boldsymbol{:}_{\boldsymbol{t}}\ TYPE
\end{array}
$$

3.2 Expression and Predicate

$$
\begin{array}{ll}
\mathit{fun} & geninst\ \_\ [_g\ \cdots\ ]_g, \\
 & \{_e\ \cdots\ \}_e, \\
 & \{_c\ \_\ \bullet_c\ \_\ \}_c, \\
 & (_e\ \cdots\ )_e, \\
 & (_t\ \cdots\ )_t, \\
 & (_b\ \cdots\ )_b, \\
 & \mu_d\ \_\ \bullet_d\ \_, \\
 & [_v\ \_\ ]_v, \\
 & [_s\ \_\ |_s\ \_\ ]_s, \\
 & \neg_e\ \_\ \fatsemi_e\ \_, \\
 & \_\ \wedge_e\ \_\ \fatsemi_c\ \_, \\
 & \forall_s\ \_\ \bullet_s\ \_\ \fatsemi_s\ \_, \\
 & \_\ [_r\ \cdots\ ]_r, \\
 & \_\ ==_b\ \_, \\
 & \_\ \fatsemi_d\ \_, \\
 & \_\ /_r\ \_, \\
 & \_\ \in_p\ \_, \\
 & \forall_p\ \_\ \bullet_p\ \_, \\
 & \_\ \wedge_p\ \_
\end{array}
$$

$$
\begin{array}{lll}
\boldsymbol{EXPRESSION} & ::= & \boldsymbol{var}\ NAME \\
& | & \boldsymbol{geninst}\ NAME\ [_{\boldsymbol{g}}\ seq\ EXPRESSION\ ]_{\boldsymbol{g}} \\
& | & \{_{\boldsymbol{e}}\ seq\ EXPRESSION\ \}_{\boldsymbol{e}} \\
& | & \{_{\boldsymbol{c}}\ EXPRESSION\ \bullet_{\boldsymbol{c}}\ EXPRESSION\ \}_{\boldsymbol{c}} \\
& | & \mathbb{P}_{\boldsymbol{p}}\ EXPRESSION \\
& | & (_{\boldsymbol{t}}\ seq\ EXPRESSION\ )_{\boldsymbol{t}} \\
& | & (_{\boldsymbol{b}}\ seq\ BIND\ )_{\boldsymbol{b}} \\
& | & \boldsymbol{\mu_d}\ EXPRESSION\ \bullet_{\boldsymbol{d}}\ EXPRESSION \\
& | & [_{\boldsymbol{v}}\ DEC\ ]_{\boldsymbol{v}} \\
& | & [_{\boldsymbol{s}}\ EXPRESSION\ |_{\boldsymbol{s}}\ PREDICATE\ ]_{\boldsymbol{s}} \\
& | & \neg_{\boldsymbol{e}}\ EXPRESSION\ ⨾_{\boldsymbol{e}}\ TYPE \\
& | & EXPRESSION\ \wedge_{\boldsymbol{e}}\ EXPRESSION\ ⨾_{\boldsymbol{c}}\ TYPE \\
& | & \forall_{\boldsymbol{s}}\ EXPRESSION\ \bullet_{\boldsymbol{s}}\ EXPRESSION\ ⨾_{\boldsymbol{s}}\ TYPE \\
& | & EXPRESSION\ [_{\boldsymbol{r}}\ seq\ RENAME\ ]_{\boldsymbol{r}} \\
\&\ \boldsymbol{BIND} & ::= & NAME\ ==_{\boldsymbol{b}}\ EXPRESSION \\
\&\ \boldsymbol{DEC} & ::= & NAME\ ⨾_{\boldsymbol{d}}\ EXPRESSION \\
\&\ \boldsymbol{RENAME} & ::= & NAME\ /_{\boldsymbol{r}}\ NAME \\
\&\ \boldsymbol{PREDICATE} & ::= & EXPRESSION\ \in_{\boldsymbol{p}}\ EXPRESSION \\
& | & \boldsymbol{true_p} \\
& | & \neg_{\boldsymbol{p}}\ PREDICATE \\
& | & PREDICATE\ \wedge_{\boldsymbol{p}}\ PREDICATE \\
& | & \forall_{\boldsymbol{p}}\ EXPRESSION\ \bullet_{\boldsymbol{p}}\ PREDICATE
\end{array}
$$

3.3 Paragraph

fun $[_d\ \ldots\ ]_d$,
$GENAX\ \ \ldots\ (_g\ \_\ ⨾_g\ \_\ )_g$,
$[_\vdash\ \ldots\ ]_\vdash\ \_$

$$
\begin{array}{lll}
\boldsymbol{PARAGRAPH} & ::= & [_{\boldsymbol{d}}\ seq\ NAME\ ]_{\boldsymbol{d}} \\
& | & \boldsymbol{AX}\ EXPRESSION \\
& | & \boldsymbol{GENAX}\ seq\ NAME\ (_{\boldsymbol{g}}\ EXPRESSION\ ⨾_{\boldsymbol{g}}\ TYPE\ )_{\boldsymbol{g}} \\
& | & \vdash_{\boldsymbol{d}}\ PREDICATE \\
& | & [_\vdash\ seq\ NAME\ ]_\vdash\ PREDICATE
\end{array}
$$

3.4 Section

fun *section* _ *parents* ... *end* ... *END*

$$\boldsymbol{SECTION} ::= \boldsymbol{section}\ NAME\ \boldsymbol{parents}\ seq\ NAME\ \boldsymbol{end}\ seq\ PARAGRAPH\ \boldsymbol{END}$$

3.5 Specification

$$\boldsymbol{SPECIFICATION} ::= \boldsymbol{spec}\ (seq\ SECTION)$$

3.6 Decoration

The semantics use the reserved strokes ♡ and ♠ to distinguish given type names from generic formal parameter names. The function *decor* is used to apply ordinary decorations (strokes) and these special decorations to names. To declare this function we define a given type of strokes (corresponding to the syntactic category `STROKE` in the lexis) and extend it with the two reserved strokes to give a free type, *DECORATOR* representing a set which does not have an official name in the standard.

$$[\ \boldsymbol{STROKE}\ ]$$

$$\boldsymbol{DECORATOR} ::= \boldsymbol{stroke}\ STROKE \mid \heartsuit \mid \spadesuit$$

We can now declare *decor*. Note that both the arrows are injections: each *DECORATOR* determines its own unique injection of the set of names into itself.

$$\boldsymbol{decor} : DECORATOR \rightarrowtail NAME \rightarrowtail NAME$$

4 SEMANTICS

Now after just a few more preliminaries, we can get down to business. Section 4.1 gives the preliminaries and then sections 4.2 to 4.7 give the semantic equations in exactly the same order as the original.

4.1 Preliminaries

We define *Model* and *Theory* just as in the original and introduce the name of the prelude

$$\boldsymbol{Model} \mathrel{\widehat{=}} NAME \mathrel{\twoheadrightarrow\!\!\!\!\!\!\;+} \mathbb{U}$$

$$\boldsymbol{Theory} \mathrel{\widehat{=}} NAME \mathrel{\rightarrow\!\!\!\!\!\!\;+} \mathbb{P} Model$$

$| \; \boldsymbol{prelude} : NAME$

Now we introduce the semantic brackets. In principle, we could give just one or more large axiomatic descriptions containing all the equations. That would be appropriate if one wished to model the semantics of the semantics more accurately than we do. Our goal is to stay near the surface syntax of the original, so we will introduce the semantic equations as individual axioms.

$$\begin{array}{ll} fun & [\![_Z \ \_ \ ]\!]_Z, \\ & [\![_S \ \_ \ ]\!]_S, \\ & [\![_D \ \_ \ ]\!]_D, \\ & [\![_P \ \_ \ ]\!]_P, \\ & [\![_E \ \_ \ ]\!]_E, \\ & [\![_T \ \_ \ ]\!]_T \end{array}$$

$$\begin{array}{|l} [\![_{\boldsymbol{Z}} \ \_ \ ]\!]_{\boldsymbol{Z}} : SPECIFICATION \rightarrow Theory; \\ [\![_{\boldsymbol{S}} \ \_ \ ]\!]_{\boldsymbol{S}} : SECTION \rightarrow Theory \rightarrow Theory; \\ [\![_{\boldsymbol{D}} \ \_ \ ]\!]_{\boldsymbol{D}} : PARAGRAPH \rightarrow Model \leftrightarrow Model; \\ [\![_{\boldsymbol{P}} \ \_ \ ]\!]_{\boldsymbol{P}} : PREDICATE \rightarrow \mathbb{P}\ Model; \\ [\![_{\boldsymbol{E}} \ \_ \ ]\!]_{\boldsymbol{E}} : EXPRESSION \rightarrow Model \rightarrow \mathbb{W}; \\ [\![_{\boldsymbol{T}} \ \_ \ ]\!]_{\boldsymbol{T}} : TYPE \rightarrow Model \rightarrow \mathbb{PU} \end{array}$$

In principle, in Z, which doesn't allow free variables in axioms, each equation should be individually universally quantified over its free variables. This would clutter our presentation. Instead we declare all the syntactic jokers as global variables. This makes our description logically too weak, but suffices for type-checking purposes.

$$\begin{array}{|l} \boldsymbol{m}, \boldsymbol{n} : \mathbb{N}; \\ \boldsymbol{i}, \boldsymbol{i_1}, \boldsymbol{i_m}, \boldsymbol{i_n}, \boldsymbol{j_1}, \boldsymbol{j_m}, \boldsymbol{j_n} : NAME; \\ \boldsymbol{\tau}, \boldsymbol{\tau_1}, \boldsymbol{\tau_m}, \boldsymbol{\tau_n} : TYPE; \\ \boldsymbol{s_1}, \boldsymbol{s_n} : SECTION; \\ \boldsymbol{d_1}, \boldsymbol{d_n} : PARAGRAPH; \\ \boldsymbol{e}, \boldsymbol{e_1}, \boldsymbol{e_2}, \boldsymbol{e_n} : EXPRESSION; \\ \boldsymbol{p}, \boldsymbol{p_1}, \boldsymbol{p_2} : PREDICATE \end{array}$$

Finally, we need some help with the equations that involve sequences of syntactic constructs. Z does not support the elliptical notation that is used in the original. However, we can pretend that it does. To do this, we will weaken the specification but preserve the surface syntax by taking $n = m = 3$. We then use the notations "...", "$\cdots$" and "$\cdots$", which by a little sleight of hand we have made into ProofPower-Z names, in place of the ellipses of the original.

“$\cdots$” and “$^{\cdots}$” are declared below as a generic value and a generic schema respectively. “...” is used as a bound variable and so needs no declaration here (although, for want of a better name, we use it for the single component of “$^{\cdots}$”). Given these declarations, we can use “$\cdots$” to represent an ellipsis used in a syntactic phrase inside semantic brackets, “$^{\cdots}$” to represent an ellipsis standing for zero or more declarations, and “...” as a local variable for all the other uses of ellipses.

$$
\begin{array}{|l}
\hline
[X] \\
\hline
\cdots : X \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
{}^{\cdots}[X] \\
\hline
\ldots : X \\
\hline
\end{array}
$$

4.2 Specification

$$[\![_Z\ spec\ \langle s_1,\ \cdots,\ s_n\rangle\ ]\!]_Z$$
$$=$$
$$([\![_S\ section\ prelude\ parents\ \cdots\ end\ \cdots\ END\ ]\!]_S\ ⨾\ [\![_S\ s_1\ ]\!]_S\ ⨾\ \cdots\ ⨾\ [\![_S\ s_n\ ]\!]_S)\ \varnothing$$

4.3 Section

$$[\![_S\ section\ prelude\ parents\ \ end\ d_1,\ \cdots,\ d_n\ END\ ]\!]_S$$
$$=$$
$$(\lambda T : Theory \bullet \{prelude \mapsto$$
$$([\![_D\ d_1\ ]\!]_D\ ⨾ \cdots ⨾\ [\![_D\ d_n\ ]\!]_D)(\!|\ \varnothing\ |\!)\}\ )$$

Correction: Mark Saaltink has pointed out that the formulation of the following in the 1999 CD is incorrect: it attempts to form a model as the union of a family of models which need not be compatible as functions. This has been corrected below (by asserting that the union, M, is a member of the set of models).

$$[\![_S\ section\ i\ parents\ i_1,\ \cdots,\ i_m\ end\ d_1,\ \cdots,\ d_n\ END\ ]\!]_S$$
$$=$$
$$(\lambda T : Theory \bullet T \cup \{i \mapsto$$
$$([\![_D\ d_1\ ]\!]_D\ ⨾ \cdots ⨾\ [\![_D\ d_n\ ]\!]_D)$$
$$(\!|\ \{M_0 : T\ prelude;\ M_1 \colon T\ i_1;\ \cdots;\ M_m : T\ i_m;\ M : Model$$
$$\mid M = M_0 \cup \cdots \cup M_m\ \bullet\ M\}|\!)\})$$

4.4 Paragraph

4.4.1 Given types paragraph

$$[\![_D\ [_d\ i_1,\ \cdots,\ i_n\ ]_d\ ]\!]_D =$$
$$\{M : Model;\ w_1,\ \ldots,\ w_n : \mathbb{W} \bullet$$
$$(M,\ M \cup \{i_1 \mapsto w_1,\ \cdots,\ i_n \mapsto w_n\} \cup$$
$$\{decor \heartsuit i_1 \mapsto w_1,\ \cdots,\ decor \heartsuit i_n \mapsto w_n\})\}$$

4.4.2 Axiomatic description paragraph

$$[\![_D\ AX\ e\ ]\!]_D = \{M : Model;\ t : \mathbb{W} \mid t \in \eta([\![_E\ e\ ]\!]_E\ M) \bullet\ (M,\ M \cup (\beta^\sim)\ t)\}$$

4.4.3 Generic axiomatic description paragraph

Correction: it is intuitively much better to have u below range over functions on $\mathbb{W} \uparrow n$ rather than $\mathbb{W}$. Also, as u ranges over a set of total functions it is misleading to write $dom\ u$, since we know that that is equal to $\mathbb{W} \uparrow n$.

$$
\begin{array}{l}
[\![_D\ GENAX\ i_1,\ \cdots,\ i_n \\
\quad (_g\ e\ \S_g\ \mathbb{P}_t\ [_t\ j_1\ :_t\ \tau_1,\ \cdots,\ j_m\ :_t\ \tau_m\ ]_t)_g\ ]\!]_D = \\
\quad \{M : Model;\ u : \mathbb{W} \uparrow n \rightarrow \mathbb{W} \\
\qquad \mid \forall\ w_1,\ ...,\ w_n : \mathbb{W} \bullet \exists\ w : \mathbb{W} \bullet \\
\qquad\qquad u\langle w_1,\ ...,\ w_n\rangle \in \eta\ w \\
\qquad\qquad \wedge\ ((M \oplus \{i_1 \mapsto w_1,\ \cdots,\ i_n \mapsto w_n\} \cup \\
\qquad\qquad\qquad \{decor\spadesuit i_1 \mapsto w_1,\ \cdots,\ decor\spadesuit i_n \mapsto w_n\}) \mapsto w) \in [\![_E e]\!]_E \\
\quad \bullet\ (M,\ M \cup (\lambda\ y : \{j_1,\ \cdots,\ j_m\} \bullet\ \gamma(\lambda x : \mathbb{W} \uparrow n \bullet\ (\beta^\sim)(u\ x)\ y)))\}
\end{array}
$$

4.4.4 Conjecture paragraph

$$[\![_D \vdash_d\ p\ ]\!]_D = id\ Model$$

4.4.5 Generic conjecture paragraph

$$[\![_D\ [_\vdash\ i_1,\ \cdots,\ i_n\ ]_\vdash\ p\ ]\!]_D = id\ Model$$

4.5 Predicate

4.5.1 Membership predicate

$$[\![_P\ e_1 \in_p e_2\ ]\!]_P = \{M : Model \mid [\![_E\ e_1\ ]\!]_E\ M \in \eta([\![_E\ e_2\ ]\!]_E\ M) \bullet M\}$$

4.5.2 Truth predicate

$$[\![_P\ true_p\ ]\!]_P = Model$$

4.5.3 Negation predicate

$$[\![_P\ \neg_p\ p\ ]\!]_P = Model \setminus [\![_P\ p\ ]\!]_P$$

4.5.4 Conjunction predicate

$$[\![_P\ p_1 \wedge_p p_2\ ]\!]_P = [\![_P\ p_1\ ]\!]_P \cap [\![_P\ p_2\ ]\!]_P$$

4.5.5 Universal quantification predicate

$$[\![_P\ \forall_p\ e\ \bullet_p\ p\ ]\!]_P = \{M : Model \mid \forall\ t : \eta([\![_E\ e\ ]\!]_E\ M)\bullet\ M \oplus (\beta^{\sim})t \in [\![_P\ p\ ]\!]_P \bullet M\}$$

4.6 Expression

4.6.1 Reference expression

$$[\![_E\ var\ i\ ]\!]_E = (\lambda M : Model\bullet\ M\ i)$$

4.6.2 Generic instantiation expression

$$\begin{aligned}&[\![_E\ geninst\ i\ [_g\ e_1, \cdots, e_n\ ]_g\ ]\!]_E = \\ &\qquad (\lambda M : Model\ \bullet(\gamma^{\sim})(M\ i)\ \langle [\![_E\ e_1]\!]_E\ M, \cdots, [\![_E\ e_n]\!]_E\ M\rangle)\end{aligned}$$

4.6.3 Set extension expression

$$\begin{aligned}&[\![_E\ \{_e\ e_1, \cdots, e_n\ \}_e\ ]\!]_E = \\ &\qquad (\lambda M : Model\ \bullet\ \phi\{[\![_E\ e_1]\!]_E\ M, \cdots, [\![_E\ e_n]\!]_E\ M\})\end{aligned}$$

4.6.4 Set comprehension expression

$$\begin{aligned}&[\![_E\ \{_c\ e_1\ \bullet_c\ e_2\ \}_c\ ]\!]_E = \\ &\qquad (\lambda M : Model \mid \forall\ t : \eta([\![_E\ e_1\ ]\!]_E\ M)\bullet\ (M \oplus (\beta^{\sim})\ t) \in dom[\![_E\ e_2]\!]_E \\ &\qquad\qquad \bullet(\eta^{\sim})\{t_1 : \eta([\![_E\ e_1\ ]\!]_E\ M)\bullet\ [\![_E\ e_2]\!]_E\ (M \oplus (\beta^{\sim})\ t_1)\})\end{aligned}$$

4.6.5 Powerset expression

$$[\![_E\ \mathbb{P}_p\ e\ ]\!]_E = (\lambda M : Model\bullet\ \mathbb{P}_W([\![_E\ e]\!]_E\ M))$$

4.6.6 Tuple extension expression

$$\llbracket_E\ (_t\ e_1,\ \cdots,\ e_n\ )_t\ \rrbracket_E = \\ \quad (\lambda M : Model \bullet \chi\langle\llbracket_E\ e_1\rrbracket_E\ M,\ \cdots,\ \llbracket_E\ e_n\rrbracket_E\ M\rangle)$$

4.6.7 Binding extension expression

$$\llbracket_E\ (_b\ i_1 ==_b e_1,\ \cdots,\ i_n ==_b e_n\ )_b\ \rrbracket_E = \\ \quad (\lambda M : Model \bullet \beta\{i_1 \mapsto \llbracket_E\ e_1\rrbracket_E\ M,\ \cdots,\ i_n \mapsto \llbracket_E\ e_n\rrbracket_E\ M\})$$

4.6.8 Definite description expression

$$\{M : Model;\ t_1 : \mathbb{W} \\ \quad \mid t_1 \in \eta(\llbracket_E\ e_1\ \rrbracket_E\ M) \\ \quad \land (\forall t_3 : \eta(\llbracket_E\ e_1\ \rrbracket_E\ M) \\ \qquad \bullet \llbracket_E\ e_2\ \rrbracket_E\ (M \oplus (\beta^\sim)\ t_3) = \llbracket_E\ e_2\ \rrbracket_E\ (M \oplus (\beta^\sim)\ t_1)) \\ \quad \bullet (M,\ \llbracket_E\ e_2\ \rrbracket_E\ (M \oplus (\beta^\sim)\ t_1))\} \qquad \subseteq \llbracket_E\ \mu_d\ e_1 \bullet_d e_2\ \rrbracket_E$$

4.6.9 Variable construction expression

$$\llbracket_E\ [_v\ i\ ⨾_d\ e\ ]_v\ \rrbracket_E = (\lambda M : Model \bullet (\eta^\sim)\{w : \eta(\llbracket_E\ e\ \rrbracket_E\ M) \bullet\ \beta\{i \mapsto w\}\})$$

4.6.10 Schema construction expression

$$\llbracket_E\ [_s\ e\ |_s\ p\ ]_s\ \rrbracket_E = (\lambda M : Model \bullet \\ \quad (\eta^\sim)\{t : \eta(\llbracket_E\ e\ \rrbracket_E\ M) \mid M \oplus (\beta^\sim)\ t \in \llbracket_P\ p\ \rrbracket_P \bullet\ t\})$$

4.6.11 Schema negation expression

$$\llbracket_E\ \neg_e\ e\ ⨾_e\ \mathbb{P}_t\ \tau\ \rrbracket_E = (\lambda M : Model \bullet \\ \quad (\eta^\sim)\{t : \llbracket_T\ \tau\ \rrbracket_T\ M \mid \neg t \in \eta(\llbracket_E\ e\ \rrbracket_E\ M) \bullet\ t\})$$

4.6.12 Schema conjunction expression

$$\llbracket_E\ e_1 \land_e e_2\ ⨾_c\ \mathbb{P}_t\ \tau\ \rrbracket_E = \\ \quad (\lambda M : Model \\ \qquad \bullet (\eta^\sim)(\{t : \llbracket_T\ \tau\ \rrbracket_T\ M;\ t_1 : \eta(\llbracket_E\ e_1\rrbracket_E\ M);\ t_2 : \eta(\llbracket_E\ e_2\rrbracket_E\ M) \\ \qquad\quad \mid \eta\ t_1 \cup \eta\ t_2 = \eta\ t \bullet t\}))$$

4.6.13 Schema universal quantification expression

$$
\begin{array}{l}
[\![_E\ \forall_s\ e_1 \bullet_s e_2\ {}_{9}^{\circ}{}_s\ \mathbb{P}_t\ \tau\ ]\!]_E = \\
\quad (\lambda M : Model \\
\quad\quad \bullet(\eta^{\sim})\{t_2 : [\![_T\ \tau\ ]\!]_T\ M\ | \\
\quad\quad\ \ \forall\ t_1 : \eta([\![_E\ e_1]\!]_E\ M)\bullet \\
\quad\quad\quad\quad \beta((\beta^{\sim})t_1 \cup (\beta^{\sim})t_2) \in \eta([\![_E\ e_2]\!]_E\ (M \oplus (\beta^{\sim})t_1))\bullet\ t_2\})
\end{array}
$$

4.6.14 Schema renaming expression

Correction: the 1999 CD has a misprint in this equation (t_1 on the last line rather than t_2). The formulation below also incorporates an improvement suggested by comment UK83 on the 1999 CD.

$$
\begin{array}{l}
[\![_E\ e\ [_r\ j_1\ /_r\ i_1, \cdots, j_n\ /_r\ i_n\ ]_r\ ]\!]_E = \\
\quad (\lambda M : Model \\
\quad\quad \bullet(\eta^{\sim})\{t_1 : \eta([\![_E\ e\ ]\!]_E\ M);\ t_2 : \mathbb{W}\ | \\
\quad\quad\quad\quad (\beta^{\sim})t_2 = \{j_1 \mapsto i_1, \cdots, j_n \mapsto i_n\}{}_{9}^{\circ}\ (\beta^{\sim})t_1 \cup \{i_1, \cdots, i_n\} \lhd (\beta^{\sim})t_1 \\
\quad\quad\quad\quad \wedge\ (\beta^{\sim})\ t_2 \in (\_ \nrightarrow \_) \\
\quad\quad\quad\quad \bullet\ t_2\})
\end{array}
$$

4.7 Type

4.7.1 Given type

$$[\![_T\ given\ i\ ]\!]_T = (\lambda M : Model\bullet\ \eta(M\ i))$$

4.7.2 Generic parameter type

$$[\![_T\ generic\ i\ ]\!]_T = (\lambda M : Model\bullet\ \eta(M\ (decor\ \spadesuit\ i)))$$

4.7.3 Set type

$$[\![_T\ \mathbb{P}_t\ \tau\ ]\!]_T = (\lambda M : Model\bullet\ (\eta^{\sim})(\!|\mathbb{P}([\![_T\ \tau\ ]\!]_T\ M)|\!))$$

4.7.4 Cartesian product type

There seems to be no particularly good way of preserving the syntax used in the original for the cartesian product operator in $\mathbb{W}$. Consequently we have changed the right-hand side of the next equation to use a description of the cartesian product along the lines of that used below for schema types.

$$
\begin{array}{l}
[\![_T\ (_\times\ \tau_1,\ \cdots,\ \tau_n\ )_\times\ ]\!]_T = (\lambda M : Model \bullet \\
\qquad \{\ f\colon \{1,\ \cdots,\ n\} \rightarrow \mathbb{W} \\
\qquad\qquad |\ f\ 1 \in ([\![_T\ \tau_1\ ]\!]_T\ M) \wedge \cdots \wedge f\ n \in ([\![_T\ \tau_n\ ]\!]_T\ M) \bullet \chi\ f\})
\end{array}
$$

4.7.5 Schema type

$$
\begin{array}{l}
[\![_T\ [_t\ i_1 :_t \tau_1,\ \cdots,\ i_n :_t \tau_n\ ]_t\ ]\!]_T = (\lambda M : Model \bullet \\
\qquad \{\ t\colon \{i_1,\ \cdots,\ i_n\} \rightarrow \mathbb{W} \\
\qquad\qquad |\ t\ i_1 \in ([\![_T\ \tau_1\ ]\!]_T\ M) \wedge \cdots \wedge t\ i_n \in ([\![_T\ \tau_n\ ]\!]_T\ M) \bullet \beta\ t\})
\end{array}
$$

4.7.6 Generic type

Correction: As in section 4.4.3, it is better to use $\mathbb{W} \uparrow n$ here for the domain of g. In fact, it is now proposed to remove the equation altogether, since it is no longer used anywhere.

$$
\begin{array}{l}
[\![_T\ \lambda_t\ i_1,\ \cdots,\ i_n \bullet_t \tau\ ]\!]_T = (\lambda M : Model \bullet \\
\qquad \{g : \mathbb{W} \uparrow n \rightarrow \mathbb{W} \\
\qquad\qquad |\ \forall w_1,\ \ldots,\ w_n\colon\mathbb{W} \\
\qquad\qquad \bullet \qquad g\langle w_1,\ \ldots,\ w_n\rangle \in \\
\qquad\qquad\qquad\qquad [\![_T\ \tau\ ]\!]_T\ (M \oplus \{i_1 \mapsto w_1,\ \cdots,\ i_n \mapsto w_n\}) \bullet \gamma\ g\})
\end{array}
$$

5 TYPES INFERRED

The following table shows the types inferred by ProofPower for the global variables of the specification:

AX	$EXPRESSION \leftrightarrow PARAGRAPH$
$BIND$	$\mathbb{P}\ BIND$
DEC	$\mathbb{P}\ DEC$
$DECL$	$\mathbb{P}\ DECL$
$decor$	$DECORATOR \leftrightarrow \mathbb{U} \leftrightarrow \mathbb{U}$
$DECORATOR$	$\mathbb{P}\ DECORATOR$
d_n	$PARAGRAPH$
d_1	$PARAGRAPH$
e	$EXPRESSION$
$EXPRESSION$	$\mathbb{P}\ EXPRESSION$
e_n	$EXPRESSION$
e_1	$EXPRESSION$
e_2	$EXPRESSION$
$generic$	$\mathbb{U} \leftrightarrow TYPE$
$given$	$\mathbb{U} \leftrightarrow TYPE$
i	$\mathbb{U}$
i_m	$\mathbb{U}$
i_n	$\mathbb{U}$
i_1	$\mathbb{U}$
j_m	$\mathbb{U}$
j_n	$\mathbb{U}$
j_1	$\mathbb{U}$
m	$\mathbb{Z}$
$Model$	$\mathbb{P}\ (\mathbb{U} \leftrightarrow \mathbb{U})$
n	$\mathbb{Z}$
$NAME$	$\mathbb{P}\ \mathbb{U}$
p	$PREDICATE$
$PARAGRAPH$	$\mathbb{P}\ PARAGRAPH$
$PREDICATE$	$\mathbb{P}\ PREDICATE$
$prelude$	$\mathbb{U}$
p_1	$PREDICATE$
p_2	$PREDICATE$
$RENAME$	$\mathbb{P}\ RENAME$
$SECTION$	$\mathbb{P}\ SECTION$
$spec$	$(\mathbb{Z} \leftrightarrow SECTION) \leftrightarrow SPECIFICATION$
$SPECIFICATION$	$\mathbb{P}\ SPECIFICATION$
$STROKE$	$\mathbb{P}\ STROKE$
$stroke$	$STROKE \leftrightarrow DECORATOR$
s_n	$SECTION$
s_1	$SECTION$
$Theory$	$\mathbb{P}\ (\mathbb{U} \leftrightarrow \mathbb{P}\ (\mathbb{U} \leftrightarrow \mathbb{U}))$
$true_p$	$PREDICATE$

$TYPE$	$\mathbb{P}\ TYPE$
var	$\mathbb{U} \leftrightarrow EXPRESSION$
$\mathbb{U}$	$\mathbb{P}\ \mathbb{U}$
$\mathbb{W}$	$\mathbb{P}\ \mathbb{U}$
$\heartsuit$	$DECORATOR$
$\spadesuit$	$DECORATOR$
$(GENAX\ ...\ (_g\ \_\ \fatsemi_g\ \_\ )_g)$	$(\mathbb{Z} \leftrightarrow \mathbb{U}) \times EXPRESSION \times TYPE \leftrightarrow PARAGRAPH$
$(geninst\ \_\ [_g\ ...\ ]_g)$	$\mathbb{U} \times (\mathbb{Z} \leftrightarrow EXPRESSION) \leftrightarrow EXPRESSION$
$(section\ \_\ parents\ ...\ end\ ...\ END)$	$\mathbb{U} \times (\mathbb{Z} \leftrightarrow \mathbb{U}) \times (\mathbb{Z} \leftrightarrow PARAGRAPH) \leftrightarrow SECTION$
$((_b\ ...\ )_b)$	$(\mathbb{Z} \leftrightarrow BIND) \leftrightarrow EXPRESSION$
$((_t\ ...\ )_t)$	$(\mathbb{Z} \leftrightarrow EXPRESSION) \leftrightarrow EXPRESSION$
$((_\times\ ...\ )_\times)$	$(\mathbb{Z} \leftrightarrow TYPE) \leftrightarrow TYPE$
$([_d\ ...\ ]_d)$	$(\mathbb{Z} \leftrightarrow \mathbb{U}) \leftrightarrow PARAGRAPH$
$([_s\ \_\ \|_s\ \_\ ]_s)$	$EXPRESSION \times PREDICATE \leftrightarrow EXPRESSION$
$([_t\ ...\ ]_t)$	$(\mathbb{Z} \leftrightarrow DECL) \leftrightarrow TYPE$
$([_v\ \_\ ]_v)$	$DEC \leftrightarrow EXPRESSION$
$([_\vdash\ ...\ ]_\vdash\ \_)$	$(\mathbb{Z} \leftrightarrow \mathbb{U}) \times PREDICATE \leftrightarrow PARAGRAPH$
$(\_ \uparrow \_)[X]$	$\mathbb{P}\ X \times \mathbb{Z} \leftrightarrow \mathbb{P}\ (\mathbb{Z} \leftrightarrow X)$
$(\_\ /_r\ \_)$	$\mathbb{U} \times \mathbb{U} \leftrightarrow RENAME$
$(\_\ :_t\ \_)$	$\mathbb{U} \times TYPE \leftrightarrow DECL$
$(\_\ ==_b\ \_)$	$\mathbb{U} \times EXPRESSION \leftrightarrow BIND$
$(\_\ [_r\ ...\ ]_r)$	$EXPRESSION \times (\mathbb{Z} \leftrightarrow RENAME) \leftrightarrow EXPRESSION$
$(\_\ \in_p\ \_)$	$EXPRESSION \times EXPRESSION \leftrightarrow PREDICATE$
$(\_\ \wedge_e\ \_\ \fatsemi_c\ \_)$	$EXPRESSION \times EXPRESSION \times TYPE \leftrightarrow EXPRESSION$
$(\_\ \wedge_p\ \_)$	$PREDICATE \times PREDICATE \leftrightarrow PREDICATE$
$(\_\ \fatsemi_d\ \_)$	$\mathbb{U} \times EXPRESSION \leftrightarrow DEC$
$(\{_c\ \_\ \bullet_c\ \_\ \}_c)$	$EXPRESSION \times EXPRESSION \leftrightarrow EXPRESSION$
$(\{_e\ ...\ \}_e)$	$(\mathbb{Z} \leftrightarrow EXPRESSION) \leftrightarrow EXPRESSION$
$(\neg_e\ \_\ \fatsemi_e\ \_)$	$EXPRESSION \times TYPE \leftrightarrow EXPRESSION$

$(\forall_p\ \_\ \bullet_p\ \_)$	$EXPRESSION \times PREDICATE \leftrightarrow PREDICATE$
$(\forall_s\ \_\ \bullet_s\ \_\ {}^{o}_{o}{}_s\ \_)$	$EXPRESSION \times EXPRESSION \times TYPE \leftrightarrow EXPRESSION$
$(\lambda_t\ \ldots\ \bullet_t\ \_)$	$(\mathbb{Z} \leftrightarrow \mathbb{U}) \times TYPE \leftrightarrow TYPE$
$(\mu_d\ \_\ \bullet_d\ \_)$	$EXPRESSION \times EXPRESSION \leftrightarrow EXPRESSION$
$([\![_D\ \_\ ]\!]_D)$	$PARAGRAPH \leftrightarrow (\mathbb{U} \leftrightarrow \mathbb{U}) \leftrightarrow \mathbb{U} \leftrightarrow \mathbb{U}$
$([\![_E\ \_\ ]\!]_E)$	$EXPRESSION \leftrightarrow (\mathbb{U} \leftrightarrow \mathbb{U}) \leftrightarrow \mathbb{U}$
$([\![_P\ \_\ ]\!]_P)$	$PREDICATE \leftrightarrow \mathbb{P}\ (\mathbb{U} \leftrightarrow \mathbb{U})$
$([\![_S\ \_\ ]\!]_S)$	$SECTION$ $\leftrightarrow (\mathbb{U} \leftrightarrow \mathbb{P}\ (\mathbb{U} \leftrightarrow \mathbb{U}))$ $\leftrightarrow \mathbb{U} \leftrightarrow \mathbb{P}\ (\mathbb{U} \leftrightarrow \mathbb{U})$
$([\![_T\ \_\ ]\!]_T)$	$TYPE \leftrightarrow (\mathbb{U} \leftrightarrow \mathbb{U}) \leftrightarrow \mathbb{P}\ \mathbb{U}$
$([\![_Z\ \_\ ]\!]_Z)$	$SPECIFICATION \leftrightarrow \mathbb{U} \leftrightarrow \mathbb{P}\ (\mathbb{U} \leftrightarrow \mathbb{U})$
$\cdots[X]$	X
$\cdots[X]$	$\mathbb{P}\ [\ldots : X]$
$\neg_p$	$PREDICATE \leftrightarrow PREDICATE$
β	$(\mathbb{U} \leftrightarrow \mathbb{U}) \leftrightarrow \mathbb{U}$
ϕ	$\mathbb{P}\ \mathbb{U} \leftrightarrow \mathbb{U}$
γ	$((\mathbb{Z} \leftrightarrow \mathbb{U}) \leftrightarrow \mathbb{U}) \leftrightarrow \mathbb{U}$
η	$\mathbb{U} \leftrightarrow \mathbb{P}\ \mathbb{U}$
χ	$(\mathbb{Z} \leftrightarrow \mathbb{U}) \leftrightarrow \mathbb{U}$
τ	$TYPE$
τ_m	$TYPE$
τ_n	$TYPE$
τ_1	$TYPE$
$\mathbb{P}_p$	$EXPRESSION \leftrightarrow EXPRESSION$
$\mathbb{P}_t$	$TYPE \leftrightarrow TYPE$
$\mathbb{P}_W$	$\mathbb{U} \leftrightarrow \mathbb{U}$
$\vdash_d$	$PREDICATE \leftrightarrow PARAGRAPH$

6 INDEX