Issues in the Semantics of Z

Roger Bishop Jones

ICL Defence Systems
This document consists of the overheads for a presentation at
Data Logic on September 14th 1990.

ISSUES

in

THE SEMANTICS of Z

and their

IMPACT

on

PROOF RULES for Z

UNDEFINED

UNDETERMINED

Undefined predicates

Undefined Terms

Range of Free Variables

Equality

Membership

Set Abstraction

Lambda Abstraction

Definite Description

Weak Equality

FOUR ALTERNATIVE ACCOUNTS of Z

FST

(first order set theory)

BLUE BOOK

(Understanding Z)

RED BOOK

(The Z Reference Manual)

Z STANDARD?

(recommendations for future standard)

UNDEFINED PREDICATES

YES

three valued logic

$\neg(\vdash P \vee \neg P)$

NO

two valued logic

$\vdash P \vee \neg P$

UNDEFINED TERMS

NO
(fst)

$t = t$
for all terms t

YES

all the other systems
(blue, red, Zstan?)

RANGE of FREE VARIABLES

DEF
(fst)

variables range
over defined values only

$\vdash x = x$
for all variables x

only defined terms may be
substituted for free variables

UNDEF
(blue?, red?, Zstan?)

variables range
over undefined as well

$\neg(\vdash x = x)$
if x is a variable

free substitution of terms
for free variables

EQUALITY

CLASSICAL

(fst)

$\vdash t = t$

for all terms t

STRICT

(blue, Zstan)

$\vdash t = t$

only if t is defined

$\vdash \neg (\varnothing\ \varnothing = \varnothing\ \varnothing)$

LOOSE

(red)

$\vdash t = t$

only if t is defined

$\neg (\vdash \varnothing\ \varnothing = \varnothing\ \varnothing)$

$\neg (\vdash \neg (\varnothing\ \varnothing = \varnothing\ \varnothing))$

MEMBERSHIP

CLASSICAL

(fst)

$$\vdash t \in \{t\}$$
$$\vdash t \in X$$

for all terms t of type X

STRICT

(blue, Zstan)

$$\vdash t \in \{t\}$$
$$\vdash t \in X$$

only if t is defined

$$\vdash \neg\ (\varnothing\ \varnothing \in \{\varnothing\ \varnothing\})$$
$$\vdash \neg\ \exists x{:}\mathbb{P}\ X \bullet (\varnothing\ \varnothing \in x)$$

LOOSE

(red)

$$\vdash t \in \{t\}$$

known true only if t is defined

$$\neg\ (\vdash \varnothing\ \varnothing \in \{\varnothing\ \varnothing\})$$
$$\neg\ (\vdash \neg\exists x{:}\mathbb{P}\ X \bullet (\varnothing\ \varnothing \in x))$$

SET ABSTRACTION

CLASSICAL

(fst)

$$\vdash u \in \{S \bullet t\} \Leftrightarrow \exists S \bullet t = u$$

$$\vdash \forall S \bullet t \in \{S \bullet t\}$$

STRICT

(blue)

$$\vdash (\forall S \bullet t = t) \Rightarrow (u \in \{S \bullet t\} \Leftrightarrow \exists S \bullet t = u)$$

$$\vdash t \notin \{S \bullet \varnothing\ \varnothing\}$$

LIBERAL

(red)

$$\vdash u \in \{S \bullet t\} \Leftrightarrow \exists S \bullet t = u$$

$$\neg(\vdash \forall S \bullet t \in \{S \bullet t\})$$

LAMBDA ABSTRACTION

CLASSICAL

(fst)

always defined

$$\vdash (\lambda x{:}X \bullet t) = (\lambda x{:}X \bullet t)$$

domain as specified

$$\vdash \mathrm{dom}\ (\lambda x{:}X \bullet t) = X$$

$$\neg(\vdash \forall f{:}X \nrightarrow Y \bullet (\lambda x{:}X \bullet f\ x) = f)$$

unconditional beta reduction

$$\vdash r = (\lambda x{:}X \bullet t)\ a \Leftrightarrow a \in X \wedge t[a/x] = r$$

STRICT

(blue)

not always defined

$$\vdash (\forall x{:}X \bullet t{=}t) \Leftrightarrow (\lambda x{:}X \bullet t) = (\lambda x{:}X \bullet t)$$

domain as specified, if defined

$$\vdash (\forall x{:}X \bullet t{=}t) \Leftrightarrow \mathrm{dom}\ (\lambda x{:}X \bullet t) = X$$

$$\neg(\vdash \forall f{:}X \nrightarrow Y \bullet (\lambda x{:}X \bullet f\ x) = f)$$

qualified beta reduction

$$\vdash (\forall x:X\bullet\ t=t) \Rightarrow (r = (\lambda x:X \bullet t)\ a \Leftrightarrow a \in X \wedge t[a/x] = r)$$

LIBERAL
(red, Zstan)

always defined
$\vdash (\lambda x:X \bullet t) = (\lambda x:X \bullet t)$

domain not necessarily as specified
$\vdash \mathrm{dom}\ (\lambda x:X \bullet t) = \{x:X \mid t=t\}$
$\vdash \forall f:X \nrightarrow Y\bullet\ (\lambda x:X \bullet f\ x) = f$

unconditional beta reduction
$\vdash r = (\lambda x:X \bullet t)\ a \Leftrightarrow a \in X \wedge t[a/x] = r$

Definitions of the form:

$f = \lambda x:X \bullet t$

where the domain of definition
of f is not known but is to be
derived from the domain of definition
of t are supported by
liberal lambda abstraction
but not by any other form

DEFINITE DESCRIPTION

EXTENSIONAL

(fst, blue)

$$\vdash (\mu\ x{:}X\bullet\ t) = (\mu\ y{:}\{x{:}X\bullet\ t\})$$

NON-EXTENSIONAL

(red, Zstan?)

$$\vdash (\mu\ x{:}\mathbf{N}^1\bullet\ x/x) \neq (\mu\ y{:}\{x{:}\mathbf{N}^1\bullet\ x/x\})$$

STRICT

(blue, red, Zstan?)

$$\vdash (\mu\ x{:}\mathbf{N}\bullet\ x/x) \neq (\mu\ x{:}\mathbf{N}\bullet\ x/x)$$

LIBERAL

()

$$\vdash (\mu\ x{:}\mathbf{N}\bullet\ x/x) = (\mu\ x{:}\mathbf{N}^1\bullet\ x/x)$$

WEAK EQUALITY

YES
(fst, Zstan?)

can reason about terms
without proving them defined

$$\vdash t \cdot t$$

for all terms t

Definitions of the form

$$\forall x{:}X \bullet f\ x \cdot t$$

work,
where the domain of definition
of f may be smaller than X

NO
(blue, red)

can’t reason about terms
without proving them defined

SUMMARY

ISSUE	Fst	Blue	Red	Zstan?
UDP	No	No	No	No
UDT	No	Yes	Yes	Yes
ROFV	D	U?	U?	U
=	C	S	LO	S
∈	C	S	LO	S
{x•t}	C	S	LI	LI
λx•t	C	S	LI	LI
μx•t	EX LO	EX S	NE S	NE S

OTHER ISSUES

CONTEXT CONDITIONS

implicit generic instantiation

schemas/sets of bindings

closure problems

DECORATIONS

decorated top-level sets of bindings

schema composition

PRIMITIVES

are all relations sets?

OTHER

generic predicates

forms of judgement

Δ, Ξ, T