

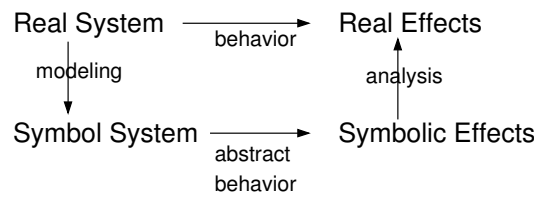
Z and *Vers*

Bart Massey
Portland State University
May 8, 2001

What is Z?

- Formal logic and set theory
- Finite and integer sorts
- Models world
- Specifies constraints

Modeling and Analysis



Z Paragraphs

Z description is natural-language +

- Entities
- Axioms
- Schemata

Z Definitions

Set existence

[*FISH*]

$COIN ::= penny \mid nickle \mid dime \mid quarter$

Functions and constraints

$least_change : 0 .. 99 \rightarrow bag\ COIN$

$\forall n : 0 .. 99 \bullet elems(least_change\ n) \leq 9$

Z Schema

Like records: indicate state change

<i>VendingMachine</i>
<i>change</i> : <i>bag COIN</i>
$\text{elems}(\text{change}) \leq 1000$

Change in Z

Schema can show state change

Sell

Δ *VendingMachine*

payment?, *price?* : \mathbb{N}

change' = *change less*

least_change(payment? – price?)

payment? \geq *price?*

Requirements Inspection

1. Clean up numbering
2. Strengthen vague requirements
3. Add missing requirements
4. Use clear, consistent terminology

Why Z For Vers?

- Consistency
- Completeness
- Precision
- Accuracy
- Terseness
- Verifiability

The Vers Environment

$[USER, DIR, FILE, FILENAME]$

$| fs : DIR \times FILENAME \rightarrow FILE$

$| cwd : USER \rightarrow DIR$

Internals

VERSION ::= \mathbb{N}_1

LOCK_STATE ::= *locked_by*⟨⟨*USER*⟩⟩ | *unlocked*

+ Repository

The Repository

Delta

version : *VERSION*

file : *FILE*

HISTORY == seq *Delta*

Record

lock_state : *LOCK_STATE*

history : *HISTORY*

Repository

repository : *FILENAME* → *Record*

Most Recent Version

$mrv : Record \rightarrow VERSION$

$\forall r : Record \bullet$

$mrvr = (r.history\ 1).version$

Creating A New Record

$new_record : USER \times FILE \rightarrow Record$

$\forall u : USER; f : FILE; r : Record; d : Delta \bullet$
 $r = new_record(u, f) \wedge$
 $r.lock_state = unlocked \wedge$
 $r.history = \langle d \rangle \wedge$
 $d.version = 1 \wedge$
 $d.file = f$

Changing The Repository

InitRepository

Repository'

$repository' = \emptyset$

New

$\Delta Repository$

filename? : FILENAME

user? : USER

$repository' = repository \cup$

$\{ filename? \mapsto$

$new_record(user?,$

$fs(cwd\ user?, filename?)) \}$

$filename? \notin \text{dom}(repository)$

Conclusions

- Important to inspect *Vers* reqs
- Z formalization helps with reqs
- Req's are hard