

# 2IW05 – Software Specification

## Functionality Specification in Z: Part II - Schema Calculus

Mohammad Mousavi

Design and Analysis of Systems (OAS) Group  
Department of Computer Science  
TU/Eindhoven

November 28, 2011

## A Library System

- From some **books**, there are a number of **copies**;
- Each **person**, can **borrow** (at most) *maxLoan* books
- List of **loans** can be reported;
- Borrowed book can (should) be **returned**;
- New **books** may be added to the library
- ...

Ack. The exercise and its solution are due to B. Potter, et. al. "An Introduction to Formal Specification and Z", Prentice Hall, 1996.

## A Library System

[*Book, Copy, Person*]

| *maxLoan* :  $\mathbb{N}$

## Solution (cont'd)

*Library*

$stock : Copy \rightarrow Book$

$borrowed : Copy \rightarrow Person$

$shelved : \mathbb{P} Copy$

$shelved \cup \text{dom } borrowed = \text{dom } stock$

$shelved \cap \text{dom } borrowed = \emptyset$

$\forall p : Person \cdot \#(borrowed \triangleright \{p\}) \leq maxLoan$

## Solution (cont'd)

*Borrow*

$\Delta$ *Library*

$b? : \text{Book}$

$p? : \text{Person}$

$\text{stock}' = \text{stock}$

$\#(\text{borrowed} \triangleright \{p?\}) < \text{maxLoan}$

$\exists c : \text{Copy} \bullet \text{stock}(c) = b? \wedge c \in \text{shelved}$

$\text{shelved}' = \text{shelved} \setminus \{c\} \wedge$

$\text{borrowed}' = \text{borrowed} \oplus \{c \mapsto p?\}$

## Solution (cont'd)

*Return*

$\Delta$ *Library*

$c? : \text{Copy}$

$\text{stock}' = \text{stock}$

$c? \in \text{dom } \text{borrowed}$

$\text{borrowed}' = \text{borrowed} \setminus \{c? \mapsto \text{borrowed}(c?)\}$

$\text{shelved}' = \text{shelved} \cup \{c?\}$

## Solution (cont'd)

*AddCopy*

$\Delta$ *Library*

$b? : \textit{Book}$

$c? : \textit{Copy}$

$\textit{borrowed}' = \textit{borrowed}$

$c? \notin \text{dom } \textit{stock}$

$\textit{stock}' = \textit{stock} \oplus \{c? \mapsto b?\}$

$\textit{shelved}' = \textit{shelved} \cup \{c?\}$

## Solution (cont'd)

*MyLoans* \_\_\_\_\_

$\exists$  *Library*

*person?* : *Person*

*copies!* :  $\mathbb{P}$  *Copy*

*copies!* =  $\text{dom}(\textit{borrowed} \triangleright \{\textit{person?}\})$

## Solution (cont'd)

*Init*

*Library'*

*stock'* =  $\emptyset$

*borrowed'* =  $\emptyset$

*shelved'* =  $\emptyset$

# Outline

- 1 Schema Calculus

## Operation Schemas

*Borrow* \_\_\_\_\_

$\Delta$ *Library*

*copy?* : *Copy*

*person?* : *Person*

$stock = stock'$

$copy? \in shelved$

$shelved' = shelved \setminus \{copy?\}$

$borrowed' = borrowed \oplus \{person? \mapsto copy?\}$

What if  $copy? \notin shelved$ ?

## Definitions

Given **normalized**  $Schema_0$  and  $Schema_1$ :

$$Schema_0 = [Decl_0 \mid Pred_0]$$

$$Schema_1 = [Decl_1 \mid Pred_1]$$

for **consistent**  $Decl_0$  and  $Decl_1$ ,

$$Schema_0 \text{ Op } Schema_1 = [Decl_0 \cup Decl_1 \mid Pred_0 \text{ Op } Pred_1]$$

where  $Op \in \{\vee, \wedge, \Rightarrow\}$

## Operation Schemas

*Borrow*

$\Delta$ *Library*

*copy?* : *Copy*

*person?* : *Person*

---

*stock* = *stock'*

*copy?*  $\in$  *shelved*

*shelved'* = *shelved*  $\setminus$  {*copy?*}

*borrowed'* = *borrowed*  $\oplus$  {*person?*  $\mapsto$  *copy?*}

---

## Operation Schemas

*NotAvailable*

---

$\exists$ *Library*

*copy?* : *Copy*

*report!* : *Report*

---

*copy?*  $\notin$  *shelved*

*report!* = *CopyNotAvailable*

---

### Operation Schemas

$NewBorrow \hat{=} Borrow \vee NotAvailable$

## Operation Schemas

*NewBorrow*

$stock : Copy \leftrightarrow Book \dots$

$copy? : Copy; \quad person? : Person$

$report! : Report$

$(shelved \cup \text{dom } borrowed = \text{dom } stock \dots$

$stock = stock' \wedge copy? \in shelved \wedge shelved' = shelved \setminus \{copy?\}$

$borrowed' = borrowed \oplus \{person? \mapsto copy?\}) \vee$

$(shelved \cup \text{dom } borrowed = \text{dom } stock \dots$

$stock = stock' \wedge borrowed' = borrowed \wedge shelved' = shelved$

$report! = CopyNotAvailable)$

# Library (cont'd): Normalization

## Operation Schemas

*NewBorrow*

$stock : Copy \leftrightarrow Book \dots$

$copy? : Copy; \quad person? : Person$

$report! : Report$

$(shelved \cup \text{dom } borrowed = \text{dom } stock \dots$

$stock = stock' \wedge copy? \in shelved \wedge shelved' = shelved \setminus \{copy?\}$

$borrowed' = borrowed \oplus \{person? \mapsto copy?\}) \vee$

$(shelved \cup \text{dom } borrowed = \text{dom } stock \dots$

$stock = stock' \wedge borrowed' = borrowed \wedge shelved' = shelved$

$report! = CopyNotAvailable)$

What about  $report!$  when  $copy? \in shelved$  ?

## Operation Schemas

*Available* \_\_\_\_\_

*report!* : *Report*

*report!* = *CopyAvailable*

$CompleteBorrow \hat{=} (Borrow \wedge Available) \vee NotAvailable$

## Definitions: Quantification

Given **normalized** *Schema*:

$$\textit{Schema} \hat{=} [\textit{Decl} \mid \textit{Pred}]$$

for **consistent**  $\textit{Decl}' \subset \textit{Decl}$ ,

$$\exists \textit{Decl}' \bullet \textit{Schema} = [\textit{Decl} \setminus \textit{Decl}' \mid \exists \textit{Decl}' \bullet \textit{Pred}]$$

$$\forall \textit{Decl}' \bullet \textit{Schema} = [\textit{Decl} \setminus \textit{Decl}' \mid \forall \textit{Decl}' \bullet \textit{Pred}]$$

## Definitions: Negation

Given **normalized** *Schema*:

$$\textit{Schema} \hat{=} [\textit{Decl} \mid \textit{Pred}]$$

$$\neg \textit{Schema} = [\textit{Decl} \mid \neg \textit{Pred}]$$

# Negation

$Available_1 \hat{=} \neg NotAvailable$

*NotAvailable*

$\exists Library$

*copy?* : *Copy*

*report!* : *Report*

*copy?*  $\notin$  *shelved*

*report!* = *CopyNotAvailable*

# Negation

*Available*<sub>1</sub>

*stock* : *Copy*  $\leftrightarrow$  *Book* ...

*copy?* : *Copy*

*report!* : *Report*

$(\neg \text{shelved} \cup \text{dom borrowed} = \text{dom stock} \vee \dots) \vee$

$(\neg \text{stock}' = \text{stock} \vee \dots) \vee \text{copy?} \in \text{shelved} \vee$

$\neg \text{report!} = \text{CopyNotAvailable}$

# Negation

$\text{SomeOtherVar} \hat{=} \neg \text{SomeVar}$

$\text{SomeVar}$

$x : 1 .. 10$

# Negation

$\text{SomeOtherVar} \hat{=} \neg \text{SomeVar}$

$\text{SomeVar}$

$x : \mathbb{Z}$

$1 \leq x \wedge x \leq 10$

# Negation

$\text{SomeOtherVar} \hat{=} \neg \text{SomeVar}$

$\text{SomeVar}$

$x : \mathbb{Z}$

$1 \leq x \wedge x \leq 10$

$\text{SomeOtherVar}$

$x : \mathbb{Z}$

$x < 1 \vee x > 10$

## Definitions: Composition

Given **normalized**  $Schema_0$  and  $Schema_1$ :

$$Schema_0 = [Decl_0 \mid Pred_0]$$

$$Schema_1 = [Decl_1 \mid Pred_1]$$

for **consistent**  $Decl_0$  and  $Decl_1$ ,

$$Schema_0 \circledast Schema_1 = \exists State'' \bullet Schema_0[''/'] \wedge Schema_1[''/']$$

# (Sequential) Composition

$\text{borrowReturn} \hat{=} \exists \text{stock}'' : \text{Copy} \leftrightarrow \text{Book};$   
 $\text{borrowed}'' : \text{Copy} \leftrightarrow \text{Person}; \text{shelved}'' : \mathbb{P} \text{Copy} \bullet$

$\text{Borrow} \frac{}{\text{Library}; \text{Library}''}$ $\text{copy?} : \text{Copy}$ $\text{person?} : \text{Person}$ <hr/> $\text{stock} = \text{stock}''$ $\text{copy?} \in \text{shelved}$ $\text{shelved}'' = \text{shelved} \setminus \{\text{copy?}\}$ $\text{borrowed}'' = \text{borrowed} \cup \{(\text{copy?}, \text{person?})\}$ <hr/>	$\wedge$	$\text{Return} \frac{}{\text{Library}''; \text{Library}'}$ $\text{copy?} : \text{Copy}$ <hr/> $\text{stock}'' = \text{stock}'$ $\text{copy?} \in \text{dom } \text{borrowed}''$ $\text{borrowed}' = \text{borrowed}'' \setminus$ $\quad \{(\text{copy?}, \text{borrowed}''(\text{copy?}))\}$ <hr/>
---	----------	--

# (Sequential) Composition

## Existential Quantifier

$$\exists Decl' \bullet Schema = [Decl \setminus Decl' \mid \exists Decl' \bullet Pred]$$

## Conjunction

$$Schema_0 \text{ Op } Schema_1 = [Decl_0 \cup Dec_1 \mid Pred_0 \text{ Op } Pred_1]$$

## (Sequential) Composition

*BorrowReturn*

*Library; Library'*

*copy? : Copy*

*person? : Person*

$\exists \text{stock}'' : \text{Copy} \leftrightarrow \text{Book}; \text{borrowed}'' : \text{Copy} \leftrightarrow \text{Person};$

$\text{shelved}'' : \mathbb{P} \text{Copy} \bullet$

$\text{stock}'' = \text{stock}$

$\text{copy?} \in \text{shelved}$

$\text{shelved}'' = \text{shelved} \setminus \{\text{copy?}\}$

$\text{borrowed}'' = \text{borrowed} \cup \{(\text{copy?}, \text{person?})\}$

$\text{stock}'' = \text{stock}'$

$\text{copy?} \in \text{dom } \text{borrowed}''$

$\text{borrowed}' = \text{borrowed}'' \setminus \{(\text{copy?}, \text{borrowed}''(\text{copy?}))\}$

# (Sequential) Composition

## One Point Rule

$$\exists x : A \bullet (p \wedge x = t) = t \in A \wedge p[t/x],$$

## (Sequential) Composition

*BorrowReturn*

*Library; Library'*

*copy? : Copy*

*person? : Person*

$\exists$  *stock''* : *Copy*  $\leftrightarrow$  *Book*; *borrowed''* : *Copy*  $\leftrightarrow$  *Person*;

*shelved''* :  $\mathbb{P}$  *Copy* •

*stock'' = stock*

*copy?*  $\in$  *shelved*

*shelved'' = shelved*  $\setminus$   $\{copy?\}$

*borrowed'' = borrowed*  $\cup$   $\{(copy?, person?)\}$

*stock'' = stock'*

*copy?*  $\in$   $\text{dom } borrowed''$

*borrowed' = borrowed''*  $\setminus$   $\{(copy?, borrowed''(copy?))\}$

## (Sequential) Composition

*BorrowReturn*

*Library; Library'*

*copy? : Copy*

*person? : Person*

$\exists$  *borrowed'' : Copy  $\leftrightarrow$  Person;*

*shelved'' :  $\mathbb{P}$  Copy •*

*copy?  $\in$  shelved*

*shelved'' = shelved  $\setminus$  {copy?}*

*borrowed'' = borrowed  $\cup$  {(copy?, person?)}*

*stock = stock'*

*copy?  $\in$  dom borrowed''*

*borrowed' = borrowed''  $\setminus$  {(copy?, borrowed''(copy?))}*

## (Sequential) Composition

*BorrowReturn*

*Library; Library'*

*copy? : Copy*

*person? : Person*

$\exists$  *borrowed''* : *Copy*  $\leftrightarrow$  *Person*; *shelved''* :  $\mathbb{P}$  *Copy* •

*copy?*  $\in$  *shelved*

*shelved''* = *shelved*  $\setminus$  {*copy?*}

*borrowed''* = *borrowed*  $\cup$  {(*copy?*, *person?*)}

*stock* = *stock'*

*copy?*  $\in$  dom *borrowed''*

*borrowed'* = *borrowed''*  $\setminus$  {(*copy?*, *borrowed''*(*copy?*))}

# (Sequential) Composition

*BorrowReturn*

*Library; Library'*

*copy? : Copy*

*person? : Person*

$\exists$

*shelved'' : P Copy •*

*copy? ∈ shelved*

*shelved'' = shelved \ {copy?}*

*borrowed'' = borrowed ∪ {(copy?, person?)}*

*stock = stock'*

*copy? ∈ dom borrowed ∪ {copy?}*

*borrowed' = borrowed ∪ {(copy?, person?)}* \ {(copy?, person?)}

## (Sequential) Composition

*BorrowReturn*

*Library; Library'*

*copy? : Copy*

*person? : Person*

$\exists shelled'' : \mathbb{P} Copy \bullet$

$copy? \in shelled$

$shelled'' = shelled \setminus \{copy?\}$

$stock = stock'$

$borrowed' = borrowed$

# (Sequential) Composition

*BorrowReturn*

*Library; Library'*

*copy? : Copy*

*person? : Person*

$\exists$  *shelved''* :  $\mathbb{P}$  Copy •

*copy?*  $\in$  *shelved*

*shelved''* = *shelved* \ {*copy?*}

*stock* = *stock'*

*borrowed'* = *borrowed*

## (Sequential) Composition

*BorrowReturn*

*Library; Library'*

*copy? : Copy*

*person? : Person*

*copy? ∈ shelved*

*stock = stock'*

*borrowed' = borrowed*

## (Sequential) Composition

*BorrowReturn*

$\exists$  *Library*

*copy?* : *Copy*

*person?* : *Person*

*copy?*  $\in$  *shelved*