

Concordia University
Department of Computer Science and Software
Engineering
SOEN 331:
Formal Methods for Software Engineering

Exercises in Z and Object-Z

Nathan Grenier, Nirav Patel

March 25, 2024

PROBLEM 1 (40 pts)

Consider a system called 'TempMonitor' that keeps a number of sensors, where each sensor is deployed in a separate location in order to read the location's temperature. Before the system is deployed, all locations are marked on a map, and each location will be addressed by a sensor. The formal specification of the system introduces the following three types:

SENSOR_TYPE, LOCATION_TYPE, TEMPERATURE_TYPE

We also introduce an enumerated type *MESSAGE* which will assume values that correspond to success and error messages.

Provide a formal specification in Z, with the following operations:

- **DeploySensorOK**: Places a new sensor to a unique location. You may assume that some (default) temperature is also passed as an argument.
- **ReadTemperatureOK**: Obtain the temperature reading from a sensor, given the sensor's location.

Provide appropriate success and error schemata to be combined with the definitions above to produce robust specifications for the following interface:

- **DeploySensor**,
- **ReadTemperature**.

Solution:

TempMonitor

$deployed' : \mathbb{P} \text{ SENSOR_TYPE}$ $map : \text{SENSOR_TYPE} \rightarrow \text{LOCATION_TYPE} \quad \text{--partial bijective}$ $read : \text{SENSOR_TYPE} \rightarrow \text{TEMPERATURE_TYPE}$
$deployed = \text{dom } map$ $deployed = \text{dom } read$

DeploySensorOK

$\Delta \text{TempMonitor}$ $sensor? : \text{SENSOR_TYPE}$ $location? : \text{LOCATION_TYPE}$ $temperature? : \text{TEMPERATURE_TYPE}$
$sensor? \notin deployed$ $location? \notin \text{ran } map$ $deployed' = deployed \cup \{sensor?\}$ $map' = map \cup \{sensor? \mapsto location?\}$ $read' = read \cup \{sensor? \mapsto temperature?\}$

ReadTemperatureOK

$\exists \text{TempMonitor}$ $location? : \text{LOCATION_TYPE}$ $temperature! : \text{TEMPERATURE_TYPE}$
$location? \in \text{ran } map$ $temperature! = read(map^{-1}(location?))$

Success

$\exists \text{TempMonitor}$ $response! : \text{MESSAGE}$
$response! = 'ok'$

<i>SensorAlreadyDeployed</i>
$\exists \text{TempMonitor}$
$\text{sensor?} : \text{SENSOR_TYPE}$
$\text{response!} : \text{Message}$
$\text{sensor?} \in \text{deployed}$
$\text{response!} = \text{'Sensor deployed'}$

<i>LocationAlreadyCovered</i>
$\exists \text{TempMonitor}$
$\text{location?} : \text{LOCATION_TYPE}$
$\text{response!} : \text{Message}$
$\text{location?} \in \text{ran map}$
$\text{response!} = \text{'Location already covered'}$

<i>LocationUnknown</i>
$\exists \text{TempMonitor}$
$\text{location?} : \text{LOCATION_TYPE}$
$\text{response!} : \text{Message}$
$\text{location?} \notin \text{ran map}$
$\text{response!} = \text{'Location not covered'}$

$$\text{DeploySensor} \hat{=} (\text{DeploySensorOK} \wedge \text{Success}) \oplus (\text{SensorAlreadyDeployed} \vee \text{LocationAlreadyCovered})$$

$$\text{ReadTemperature} \hat{=} (\text{ReadTemperatureOK} \wedge \text{Success}) \oplus \text{LocationUnknown}$$

Part 2: A booking system with the Object Z specification

We introduce the basic types $[Person, SeatType]$. We also introduce an enumerated type *Message* which will assume values (feel free to define your own) that correspond to success and error messages. Consider a system to book seats for a theater play. A customer can book a single seat, and a seat can only accommodate a single customer. The booking system keeps a log of the customers that have booked a seat. The system publishes a plan of the theater and it allows customers to access it online and make a booking or cancel a booking.

Class Booking

Define a formal specification in Object-Z for class *Bookingt* to support the following operations:

- **BookOK**: Reserves a seat for a given customer.
- **CancelOK**: Frees a seat for a given customer.

You will also need to provide appropriate success and error schemata to be combined with the definitions above to produce *robust specifications* for the following interface:

- **Book**, and
- **Cancel**.

Class Booking2

Subclassify *Booking* to introduce class **Booking2** that behaves exactly like *Booking*, while introducing the following operations:

- **GetNumberOfCustomers** returns the total number of customers who have made a booking.

- `ModifyBookingOK` assigns an existing customer to a different seat. Provide any additional schema(ta) in order to extend the interface to include a robust operation `ModifyBooking`.

The extended interface will now include operations

- `GetNumberOfCustomers`, and
- `ModifyBooking`.

Solution:

The main functionality for class **Booking** together with the success and error schemata are given below:

<i>Booking</i>
$\uparrow (Book, Cancel)$
$booked : \mathbb{P} Person$ $booking : Person \leftrightarrow SeatType$ $capacity : \mathbb{N}$ $count : \mathbb{N}$
$booked = dom\ booking$ $capacity > 0$ $count \geq 0$
<i>INIT</i>
$booked = \emptyset$ $capacity = 100$ $count = 0$
<i>BookOK</i>
$\Delta(booking, count)$ $customer? : Person$ $seat? : SeatType$
$customer? \notin booked$ $seat? \notin ran\ SeatType$ $count < capacity$ $booking' = booking \cup \{customer? \mapsto seat?\}$ $count' = count + 1$
<i>CancelOK</i>
$\Delta(booking, count)$ $customer? : Person$
$customer? \in booked$ $count > 0$ $booking' = \{customer?\} \triangleleft booking$ $count' = count - 1$
...

Booking/cont.

...

Success

$response! : Message$

$response! = 'ok'$

CustomerExists

$customer? : Person$

$response! : Message$

$customer? \in booked$

$response! = 'Customer\ already\ exists'$

CustomerUnknown

$customer? : Person$

$response! : Message$

$customer? \notin booked$

$response! = 'Customer\ unknown'$

SeatTaken

$seat? : SeatType$

$response! : Message$

$seat? \in ran\ booking$

$response! = 'Seat\ taken'$

TheaterFull

$response! : Message$

$count = capacity$

$response! = 'Theater\ full'$

TheaterEmpty

$response! : Message$

$count = 0$

$response! = 'Theater\ empty'$

$Book \triangleq (BookOK \wedge Success) \oplus CustomerExists \oplus (SeatTaken \vee TheaterFull)$

$Cancel \triangleq (CancelOK \wedge Success) \oplus (CustomerUnknown \vee TheaterEmpty)$

Booking2

$\uparrow (Book, Cancel, GetNumberOfCustomers)$

Booking

GetNumberOfCustomers

$result! : \mathbb{N}$

$result! = count$

ModifyBookingOK

$\Delta(booking)$

$customer? : Person$

$seat? : SeatType$

$customer? \in booked$

$seat? \notin ran\ booking$

$booking' = booking \oplus \{customer? \mapsto seat?\}$

$ModifyBooking \hat{=} (ModifyBookingOK \wedge Success) \oplus (CustomerUnknown \vee SeatTaken)$