Concordia University

Department of Computer Science and Software Engineering

SOEN 331:

Formal Methods for Software Engineering

Exercise in Z

Dr. Constantinos Constantinides, P.Eng.

October 16, 2022

Temperature monitoring system with the Z specification

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

$deployed' : \mathbb{P}\ SENSOR\_TYPE$
$map : SENSOR\_TYPE \pfun LOCATION\_TYPE$ `--partial bijective`
$read : SENSOR\_TYPE \pfun TEMPERATURE\_TYPE$

$deployed = \mathrm{dom}\ map$
$deployed = \mathrm{dom}\ read$

DeploySensorOK

$\Delta TempMonitor$
$sensor? : SENSOR\_TYPE$
$location? : LOCATION\_TYPE$
$temperature? : TEMPERATURE\_TYPE$

$sensor? \notin deployed$
$location? \notin \mathrm{ran}\ map$
$deployed' = deployed \cup \{sensor?\}$
$map' = map \cup \{sensor? \mapsto location?\}$
$read' = read \cup \{sensor? \mapsto temperature?\}$

ReadTemperatureOK

$\Xi TempMonitor$
$location? : LOCATION\_TYPE$
$temperature! : TEMPERATURE\_TYPE$

$location? \in \mathrm{ran}\ map$
$temperature! = read(map^{-1}(location?))$

Success

$\Xi TempMonitor$
$response! : MESSAGE$

$response! = 'ok'$

SensorAlreadyDeployed

$\Xi TempMonitor$
$sensor? : SENSOR\_TYPE$
$response! : Message$

$sensor? \in deployed$
$response! = 'Sensor\ deployed'$

LocationAlreadyCovered

$\Xi TempMonitor$
$location? : LOCATION\_TYPE$
$response! : Message$

$location? \in \operatorname{ran} map$
$response! = 'Location\ already\ covered'$

LocationUnknown

$\Xi TempMonitor$
$location? : LOCATION\_TYPE$
$response! : Message$

$location? \notin \operatorname{ran} map$
$response! = 'Location\ not\ covered'$

$$DeploySensor \mathrel{\hat=} (DeploySensorOK \land Success) \oplus (SensorAlreadyDeployed \lor LocationAlreadyCovered)$$

$$ReadTemperature \mathrel{\hat=} (ReadTemperatureOK \land Success) \oplus LocationUnknown$$