SOEN331: Introduction to Formal Methods for Software Engineering

for Software Engineering

Assignment 2 on Object-Z specification

Tarek Ait Hamouda (40044119), Abhijit Gupta (40066502),

Ethel Narra Pangan (40061530)

February 24, 2019

1 Map

───── *Map* ───

$[Description, Coordinate]$
$Point == Coordinate \times Coordinate$
$Message ::== ok \mid location\_already\_known \mid no\_location\_found$

┌───
│ $locations : Description \nrightarrow Point$
├───
│ $\forall\, l1, l2 : locations \bullet (l1.description \neq l2.description)$
└───

┌── *INIT* ────────────────────────────────────
│ $locations = \{\}$
└───

┌── *AddLocationOK* ───────────────────────────
│ $\Delta(locations)$
│ $newDescription? : Description$
│ $newPoint? : Point$
├───
│ $newDescription? \notin dom\ locations$
│ $locations' = locations \cup \{newDescription? \rightarrow newPoint?\}$
└───

┌── *DeleteLocationOK* ────────────────────────
│ $\Delta(locations)$
│ $location? : locations$
├───
│ $location? \in\ locations$
│ $locations' = locations \setminus \{location\}$
└───

┌── *ModifyLocationOK* ────────────────────────
│ $\Delta(locations)$
│ $desc? : Description$
│ $newPoint? : Point$
├───
│ $desc? \in dom\ locations$
│ $locations' = locations \oplus \{desc? \rightarrow newPoint?\}$
└───

┌── *FindLocationOK* ──────────────────────────
│ $desc? : Description$
│ $point! : Point$
├───
│ $desc? \in\ dom locations$
│ $point! = locations(desc?)$
└───

```
┌─ Success ──────────────────────────────────────────────
│ result! : Message
├────────────────────────────────────────────────────────
│ result! = ok
└────────────────────────────────────────────────────────
```

```
┌─ LocationAlreadyKnown ─────────────────────────────────
│ Ξ(locations)
│ description? : Descriptionresult! : Message
├────────────────────────────────────────────────────────
│ description? ∈ domlocations
│ result! = location_already_known
└────────────────────────────────────────────────────────
```

```
┌─ noLocationFound ──────────────────────────────────────
│ Ξ(locations)
│ description? : Descriptionresult! : Message
├────────────────────────────────────────────────────────
│ description? ∉ domlocations
│ result! = no_location_found
└────────────────────────────────────────────────────────
```

$AddLocation = (AddLocationOk \wedge Sucess) \vee locationAlreadyKnown$

$deleteLocation = (DeleteLocationOK \wedge Sucess) \vee NoLocationFound$

$modifyLocation = (ModifyLocationOK \wedge Sucess) \vee NoLocationFound$

$findLocation = (FindLocationOKSucess)NoLocationFound$ ⌐—

Map2

$[Description, Coordinate]$
$Point == Coordinate \times Coordinate$
$Message ::== ok \mid location\_already\_known \mid no\_location\_found$

$locations : Description \nrightarrow Point$
$count : \mathbb{R}$

$\forall\, l1, l2 : \; locations \bullet (l1.description \neq l2.description)$
$count >= 0$

INIT

$locations = \{\}$
$count = 0$

AddLocationOK

$\Delta(locations, count)$
$newDescription? : Description$
$newPoint? : Point$

$newDescription? \notin dom\; locations$
$locations' = locations \cup \{newDescription? \rightarrow newPoint?\}$
$count' = count + 1$

DeleteLocationOK

$\Delta(locations, count)$
$location? : locations$

$location? \in\; locations$
$locations' = locations \setminus \{location\}$
$count' = count - 1$

ModifyLocationOK

$\Delta(locations)$
$desc? : Description$
$newPoint? : Point$

$desc? \in dom\; locations$
$locations' = locations \oplus \{desc? \rightarrow newPoint?\}$
$count' = count$

FindLocationOK

$desc? : Description$
$point! : Point$

$desc? \in\; dom\, locations$
$point! = locations(desc?)$
$count' = count$

```
┌─ Success ─────────────────────────────────────────────
│ result! : Message
│───────────────────────────────────────────────────────
│ result! = ok
└───────────────────────────────────────────────────────
```

```
┌─ LocationAlreadyKnown ────────────────────────────────
│ Ξ(locations)
│ description? : Descriptionresult! : Message
│───────────────────────────────────────────────────────
│ description? ∈ domlocations
│ result! = location_a lready_k nown
└───────────────────────────────────────────────────────
```

```
┌─ noLocationFound ─────────────────────────────────────
│ Ξ(locations)
│ description? : Descriptionresult! : Message
│───────────────────────────────────────────────────────
│ description? ∉ domlocations
│ result! = no_l ocation_f ound
└───────────────────────────────────────────────────────
```

AddLocation = (AddLocationOk ∧ Sucess) ∨ locationAlreadyKnown
deleteLocation = (DeleteLocationOK ∧ Sucess) ∨ NoLocationFound
modifyLocation = (ModifyLocationOK ∧ Sucess) ∨ NoLocationFound
findLocation = (FindLocationOKSucess)NoLocationFound—╷—