

SOEN 331 - S: Formal Methods
for Software Engineering

Assignment 1

Nathan Grenier, Nirav Patel

March 21, 2024

1. Here is some code in Prolog:

```
member(X, [X|_]).  
member(X, [_|T]) :- member(X, T).
```

2. LTL formulas:

(a) $\Box\phi \rightarrow \Diamond\psi$

If ϕ is an invariant, then ψ becomes true eventually.

(b) $\Box\phi \rightarrow \bigcirc\Box\Diamond\psi$

If ϕ is an invariant, the ψ will be true infinitely often, starting from the next moment.

(c) $(\phi \wedge \bigcirc\psi) \rightarrow \Diamond\Box\tau$

If ϕ is true at time $= i$ and ψ is true at time $= i + 1$, then eventually τ becomes true and stays true.

(d) $\Box((\psi \wedge \bigcirc\chi) \rightarrow \bigcirc\tau)$

It is always the case that if ψ is true at time $= i$ and if χ is true at time $= i + 1$, then τ is true at time $= i + 1$.

(e) $(\chi \wedge \bigcirc\omega) \rightarrow \bigcirc^2(\phi\mathcal{U}\psi)$

If χ is true at time $= i$ and if ω is true at time $= i + 1$, then at time $= i + 2$ ϕ becomes true and stays true until ψ becomes true.

(f) $(\phi \oplus \psi) \rightarrow \Box\omega$

If one of ϕ or ψ are true at time $= i$, then ω becomes an invariant at time $= i$.

3. The behavior of a program is expressed by the following temporal formula:

$$\square \left[\begin{array}{c} 1. \text{start} \rightarrow \neg a \vee \neg b \\ \\ 2. \text{start} \rightarrow c \\ \\ 3. b \wedge c \rightarrow \bigcirc^2(d \oplus e) \\ \\ 4. a \vee c \rightarrow \bigcirc(k \mathcal{R} g) \\ \\ 5. (d \vee e) \rightarrow \bigcirc^2 k \\ \\ 6. c \rightarrow (h \mathcal{W}(e \wedge g)) \\ \\ 7. (d \wedge g \wedge h) \rightarrow \bigcirc^3 m \\ \\ 8. d \rightarrow m \mathcal{R} h \\ \\ 9. e \wedge \bigcirc^2(k \wedge g) \rightarrow \bigcirc^2 m \\ \\ 10. (e \wedge g) \rightarrow \bigcirc^3 c \\ \\ 11. k \wedge m \rightarrow \bigcirc h \\ \\ 12. (e \wedge \bigcirc^2 k) \rightarrow \bigcirc^3 b \end{array} \right]$$

4. Let $B(x)$ denote the subject “x is a bird” and $W(x)$ denote the predicate “x is white.” Translate the following formal statements into English sentences and attach the corresponding categorical form to each:

(a) $\forall x (B(x) \rightarrow W(x))$

(b) $\forall x (B(x) \rightarrow \neg W(x))$

$$(c) \exists x (B(x) \wedge W(x))$$

$$(d) \exists x (B(x) \wedge \neg W(x))$$

Solution:

$$(a) \forall x (B(x) \rightarrow W(x)) : \text{“All birds are white.”: (A)}$$

$$(b) \forall x (B(x) \rightarrow \neg W(x)) : \text{“All birds are non-white.”: (E)}$$

$$(c) \exists x (B(x) \wedge W(x)) : \text{“Some birds are white.”: (I)}$$

$$(d) \exists x (B(x) \wedge \neg W(x)) : \text{“There is an non-white bird.”: (O)}$$

5. Describe when the following predicate can be false: $\forall x \exists y P(x, y)$.

Solution: The statement can be false when there is an x such that $P(x, y)$ is false for every y .

6. Let $P(x, y)$ be the statement “ x asked y out to lunch” where the domain is all students in class. Express each of the following quantifications in English:

$$(a) \exists y \forall x P(x, y).$$

Solution: Recall that this reads **”There in an y that makes $P(x, y)$ true for every x .”** There is a student in class who has been asked out to lunch by every student in class.

$$(b) \forall x \exists y P(x, y).$$

Solution: Recall that this reads **“For every x there is a y for which $P(x, y)$ is true.”** Every student in class has asked out to lunch some (at least one) student in class.

An important observation on functions is that we can view them as relations, and as such we can model a function as a set of pairs (tuples).

1. Consider the following relation:

$$phone : Model \leftrightarrow Brand$$

where

$$\begin{aligned} phone = & \\ \{ & \\ & iPhone7 \mapsto apple, \\ & iPhoneX \mapsto apple, \\ & galaxyS \mapsto samsung, \\ & galaxyA \mapsto samsung, \\ & galaxyJ \mapsto samsung, \\ & mate20 \mapsto huawei, \\ & p20 \mapsto huawei \\ & \} \end{aligned}$$

- (a) What is the domain of the relation?

$$\text{dom } phone = \{iPhone7, iPhoneX, galaxyS, galaxyA, galaxyJ, mate20, p20\}.$$

(b) What is the range of the relation?

$$\text{ran } phone = \{apple, samsung, huawei\}.$$

(c) What is the result of the expression $\{iPhone7, galaxyA\} \triangleleft phone$?

Domain restriction selects pairs based on their first element. As a result,

$$\{iPhone7, galaxyA\} \triangleleft phone = \{iPhone7 \mapsto apple, galaxyA \mapsto samsung\}$$

Restriction operators are deployed to model database *queries*.

(d) What is the result of the expression $phone \triangleright \{apple, samsung\}$?

Range restriction selects pairs based on their second element. As a result,

$$\begin{aligned} phone \triangleright \{apple, samsung\} = \\ \{ \\ & iPhone7 \mapsto apple, \\ & iPhoneX \mapsto apple, \\ & galaxyS \mapsto samsung, \\ & galaxyA \mapsto samsung, \\ & galaxyJ \mapsto samsung \\ \} \end{aligned}$$

Consider the following Questions to be done in one sequence where we will make permanent modifications to the contents of *phone*:

- (e) What is the result of the expression $\{iPhone7, iPhoneX, galaxyA, mate20\} \triangleleft phone$?

Domain subtraction removes elements from the domain of the relation:

$$\begin{aligned} \{iPhone7, iPhoneX, galaxyA, mate20\} \triangleleft phone = \\ \{ \\ & galaxyS \mapsto samsung, \\ & galaxyJ \mapsto samsung, \\ & p20 \mapsto huawei \\ \} \end{aligned}$$

Note that for a modification to phone, we need to write

$$phone' = \{iPhone7, iPhoneX, galaxyA, mate20\} \triangleleft phone$$

which reads as: “The new value of phone is assigned the value of the evaluation of the expression on the right-hand-side.”

- (f) What is the result of the expression $phone \triangleright \{huawei\}$?

Range subtraction removes elements from the codomain of the relation:

$$\begin{aligned}
& phone \triangleright \{huawei\} = \\
& \{ \\
& \quad galaxyS \mapsto samsung, \\
& \quad galaxyJ \mapsto samsung \\
& \}
\end{aligned}$$

Assume now that we did

$$phone' = phone \triangleright \{huawei\}$$

and as a result, the new value of *phone* will be

$$\begin{aligned}
& phone = \\
& \{ \\
& \quad galaxyS \mapsto samsung, \\
& \quad galaxyJ \mapsto samsung \\
& \}
\end{aligned}$$

(g) What is the result of $phone \oplus \{iPhoneXSMax \mapsto apple\}$?

Relational overriding can model database updates.

$$\begin{aligned}
& phone \oplus \{iPhoneXSMax \mapsto apple\} = \\
& \{ \\
& \quad iPhoneXSMax \mapsto apple, \\
& \quad galaxyS \mapsto samsung, \\
& \quad galaxyJ \mapsto samsung \\
& \}
\end{aligned}$$

Note that for a modification to *phone*, we need to write

$$phone' = phone \oplus \{iPhoneXSMax \mapsto apple\}$$

2. Consider the sets

- $Phone = \{Samsung, Huawei, Apple, Sony, Motorola, HTC\}$, and
- $Favorite = \{Sony, HTC\}$.

Answer the following questions:

- (a) How do we interpret the expression $Favorite : \mathbb{P}Phone$?
- (b) Is $\mathbb{P}Phone$ a legitimate type?
- (c) What is the nature of the variable in $Favorite : \mathbb{P}Phone$? (i.e. atomic or composite?)
- (d) Is $Apple \in \mathbb{P}Phone$?
- (e) Is $\{Apple\} \in \mathbb{P}Phone$?
- (f) Is $\{\{\}\} \in \mathbb{P}Phone$?
- (g) Is $\{\} \in \mathbb{P}Phone$?
- (h) If we define variable $Favorite : \mathbb{P}Phone$, is $\{\}$ a legitimate value for variable $Favorite$?
- (i) Is $Favorite \in \mathbb{P}Phone$?
- (j) Is $Favorite \subset \mathbb{P}Phone$?

Solution:

- (a) How do we interpret the expression $Favorite : \mathbb{P}Phone$? Answer: This is interpreted as “The variable *Favorite* can assume any value supported by the powerset of *Phone*.”
- (b) Is $\mathbb{P}Phone$ a legitimate type? **Yes.**

- (c) What is the nature of the variable in $Favorite : \mathbb{P}Phone$? Answer: Variable $Favorite$ is a **set**.
- (d) Is $Apple \in \mathbb{P}Phone$? **No**.
- (e) Is $\{Apple\} \in \mathbb{P}Phone$? **Yes**.
- (f) Is $\{\{\}\} \in \mathbb{P}Phone$? **No**.
- (g) Is $\{\} \in \mathbb{P}Phone$? **Yes**.
- (h) If we define variable $favorite : \mathbb{P}Phone$, is $\{\}$ a legitimate value for variable $Favorite$? **Yes**.
- (i) Is $Favorite \in \mathbb{P}Phone$? **Yes**.
- (j) Is $Favorite \subset \mathbb{P}Phone$? **No**.

3. Consider the following relation:

$$laptops : Model \leftrightarrow Brand$$

where

$$\begin{aligned}
 laptops = & \\
 & \{ \\
 & \quad legion5 \mapsto lenovo, \\
 & \quad macbookair \mapsto apple, \\
 & \quad xps15 \mapsto dell, \\
 & \quad spectre \mapsto hp, \\
 & \quad xps13 \mapsto dell, \\
 & \quad swift3 \mapsto acer, \\
 & \quad macbookpro \mapsto apple, \\
 & \quad dragonfly \mapsto hp, \\
 & \quad envyx360 \mapsto hp \\
 & \}
 \end{aligned}$$

(a) What is the domain and the range of the relation?

Answer:

- The domain is defined as:

$$\begin{aligned} \text{dom } laptops = \\ & \{ \\ & \quad legion5, \\ & \quad macbookair, \\ & \quad xps15, \\ & \quad spectre, \\ & \quad xps13, \\ & \quad swift3, \\ & \quad macbookpro, \\ & \quad dragonfly, \\ & \quad envyx360 \\ & \} \end{aligned}$$

- The range is defined as: $\text{ran } laptops = \{lenovo, apple, dell, hp, acer\}$.

(b) What is the result of the expression

$$\{xps15, xps13, swift3, envyx360\} \triangleleft laptops$$

What is the meaning of operator \triangleleft and where would you deploy such operator in the context of a database management system?

Answer:

The result is

$$\begin{aligned} \{xps15, xps13, swift3, envyx360\} \triangleleft laptops = \\ \{ \\ \quad xps15 \mapsto dell, \\ \quad xps13 \mapsto dell, \\ \quad swift3 \mapsto acer, \\ \quad envyx360 \mapsto hp \\ \} \end{aligned}$$

Domain restriction selects pairs based on their first element. We deploy such operators to model database queries.

(c) What is the result of the expression

$$laptops \triangleright \{lenovo, hp\}$$

What is the meaning of operator \triangleright and where would you deploy such operator in the context of a database management system?

Answer:

The result is

$$\begin{aligned} laptops \triangleright \{lenovo, hp\} = \\ \{ \\ \quad legion5 \mapsto lenovo, \\ \quad spectre \mapsto hp, \\ \quad dragonfly \mapsto hp, \\ \quad envyx360 \mapsto hp \\ \} \end{aligned}$$

Range restriction selects pairs based on their second element. We deploy such operators to model database queries.

(d) What is the result of the expression

$$\{legion5, xps15, xps13, dragonfly\} \triangleleft laptops$$

What is the meaning of operator \triangleleft and where would you deploy such operator in the context of a database management system?

Answer:

The result is

$$\begin{aligned} &\{legion5, xps15, xps13, dragonfly\} \triangleleft laptops = \\ &\{ \\ &\quad macbookair \mapsto apple, \\ &\quad spectre \mapsto hp, \\ &\quad swift3 \mapsto acer, \\ &\quad macbookpro \mapsto apple, \\ &\quad envyx360 \mapsto hp \\ &\} \end{aligned}$$

Domain subtraction removes elements from the domain of the relation. We deploy such operation to model deletion of records.

(e) What is the result of the expression

$$laptops \triangleright \{apple, dell, hp\}$$

What is the meaning of operator \triangleright and where would you deploy such operator in the context of a database management system?

Answer:

The result is

$$\begin{aligned} laptops \rhd \{apple, dell, hp\} = \\ \{ \\ \quad legion5 \mapsto lenovo, \\ \quad swift3 \mapsto acer \\ \} \end{aligned}$$

Range subtraction removes elements from the codomain of the relation. We deploy such operation to model database updates (deletion of records).

(f) Consider the following expression

$$laptops \oplus \{ideapad \mapsto lenovo\}$$

- i. What is the result of the expression?
- ii. What is the meaning of operator \oplus and where would you deploy such operator in the context of a database management system?
- iii. Does the result of the expression have a permanent effect on the database (relation)? If not, describe in detail how would you ensure a permanent effect.

Answer:

- i. The result is

$$\begin{aligned} laptops \oplus \{ideapad \mapsto lenovo\} = \\ \{ \\ ideapad \mapsto lenovo, \\ legion5 \mapsto lenovo, \\ macbookair \mapsto apple, \\ xps15 \mapsto dell, \\ spectre \mapsto hp, \\ xps13 \mapsto dell, \\ swift3 \mapsto acer, \\ macbookpro \mapsto apple, \\ dragonfly \mapsto hp, \\ envyx360 \mapsto hp \\ \} \end{aligned}$$

- ii. Relational overriding can model database updates (addition of records).
- iii. The expression does not have a permanent effect on the database (relation).
To ensure a permanent effect on the relation, we need to define an assignment statement

$$laptops' = laptops \oplus \{ideapad \mapsto lenovo\}$$

which reads “The value of variable (relation) *laptops* is assigned the result of the expression on the right-hand-side of the assignment statement.”

4. You can produce a figure using any drawing package and save it as an image e.g. `.png`.

The image file can then be embedded in your `.tex` document as follows:

