SOEN 331 - S: Formal Methods for Software Engineering

Assignment 1

Nathan Grenier, Nirav Patel

February 15, 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 *phi* 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 at invariant at time $= i$.

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

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

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) $\forall\, x\,(B(x) \to W(x))$

   (b) $\forall\, x\,(B(x) \to \neg W(x))$

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

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

Solution:

(a) $\forall\, x\, (B(x) \rightarrow W(x))$: "All birds are white.": (A)

(b) $\forall\, x\, (B(x) \rightarrow \neg W(x))$: "All birds are non-white.": (E)

(c) $\exists\, x\, (B(x) \wedge W(x))$: "Some birds are white.": (I)

(d) $\exists\, x\, (B(x) \wedge \neg W(x))$: "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

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

   (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?

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

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

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

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

Restriction operators are deployed to model database *queries*.

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

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

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

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 $\{iPhone7, iPhoneX, galaxyA, mate20\} \lhd phone$?

Domain subtraction removes elements from the domain of the relation:

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

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

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

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 $phone \rhd \{huawei\}$?

Range subtraction removes elements from the codomain of the relation:

$$phone \rhd \{huawei\} =$$
$$\{$$
$$galaxyS \mapsto samsung,$$
$$galaxyJ \mapsto samsung$$
$$\}$$

Assume now that we did

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

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

$$phone =$$
$$\{$$
$$galaxyS \mapsto samsung,$$
$$galaxyJ \mapsto samsung$$
$$\}$$

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

Relational overriding can model database updates.

$$phone \oplus \{iPhoneXSMax \mapsto apple\} =$$
$$\{$$
$$iPhoneXSMax \mapsto apple,$$
$$galaxyS \mapsto samsung,$$
$$galaxyJ \mapsto samsung$$
$$\}$$

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

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

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

Answer:

- The domain is defined as:

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

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

(b) What is the result of the expression

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

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

Answer:

The result is

$$\{xps15, xps13, swift3, envyx360\} \lhd laptops =$$
$$\{$$
$$xps15 \mapsto dell,$$
$$xps13 \mapsto dell,$$
$$swift3 \mapsto acer,$$
$$envyx360 \mapsto hp$$
$$\}$$

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

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

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

Answer:

The result is

$$laptops \rhd \{lenovo, hp\} =$$
$$\{$$
$$legion5 \mapsto lenovo,$$
$$spectre \mapsto hp,$$
$$dragonfly \mapsto hp,$$
$$envyx360 \mapsto hp$$
$$\}$$

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

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

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

Answer:

The result is

$$\{legion5, xps15, xps13, dragonfly\} \lhd laptops =$$
$$\{$$
$$macbookair \mapsto apple,$$
$$spectre \mapsto hp,$$
$$swift3 \mapsto acer,$$
$$macbookpro \mapsto apple,$$
$$envyx360 \mapsto hp$$
$$\}$$

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

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

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

Answer:

The result is

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

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

$$
\begin{aligned}
&\mathit{laptops} \oplus \{\mathit{ideapad} \mapsto \mathit{lenovo}\} = \\
&\quad \{ \\
&\qquad \mathit{ideapad} \mapsto \mathit{lenovo}, \\
&\qquad \mathit{legion}5 \mapsto \mathit{lenovo}, \\
&\qquad \mathit{macbookair} \mapsto \mathit{apple}, \\
&\qquad \mathit{xps}15 \mapsto \mathit{dell}, \\
&\qquad \mathit{spectre} \mapsto \mathit{hp}, \\
&\qquad \mathit{xps}13 \mapsto \mathit{dell}, \\
&\qquad \mathit{swift}3 \mapsto \mathit{acer}, \\
&\qquad \mathit{macbookpro} \mapsto \mathit{apple}, \\
&\qquad \mathit{dragonfly} \mapsto \mathit{hp}, \\
&\qquad \mathit{envyx}360 \mapsto \mathit{hp} \\
&\quad \}
\end{aligned}
$$

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

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

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: