T-79.232 Safety Critical Systems

Home Assignment 2005

Teemu Tynjälä

April 13, 2005

Ilkka’s questions

Ilkka’s two questions are as follows. Please choose either Question Set 1 or Question Set 2, (Storey’s or Leveson’s book)

Question Set 1 (Neil Storey, Chapter 15.2 An explosive chemical plant)

1. List potential hazards of the basic nitrator process
2. Explain functions of safety components and their relation to hazards

Question Set 2 (Nancy Leveson, Appendix A, Medical Devies: The Therac-25 story - A3.6 Yakima Valley)

1. Describe the critical path which led to Yakima II accident.
2. Explain the effects of new modifications to the Therac-25 system after final CAP

Teemu Tynjälä

Teemu's questions - 1

1. If $TENNIS = \{alice, bob, cath\}$, $GOLF = \{cath, diana, elvis\}$, and $COURSE = \{augusta, wentworth\}$, which of the following assertions are true, and which are false?

1. $(elvis, wentworth) \in GOLF \times COURSE$
2. $\{bob, cath\} \subseteq TENNIS$
3. $\{bob, cath\} \in \mathbb{P}\, TENNIS$
4. $\{bob, cath\} \subseteq \mathbb{P}\, TENNIS$
5. $\{\} \in \mathbb{P}\,(GOLF \times COURSE)$
6. $\{\} \subseteq \mathbb{P}\,(GOLF \times COURSE)$
7. $TENNIS \in \mathbb{P}\,(TENNIS \cup GOLF)$

Teemu Tynjälä

Teemu's questions - 2

2. Which of the following assertions are true and which are false? (Notice that the sets in the clauses can be instantiated arbitrarily..)

1. $(member \subseteq list \ \wedge \ new \in list) \ \Rightarrow \ new \in member$

2. $new \in list \ \Rightarrow \ \{new\} \in list$

3. $\forall\, n.\, (n \in member \ \Rightarrow \ \exists s.\, (s \in \mathbb{P}(member) \ \wedge \ n \in s))$

4. $\forall\, n.\, (n \in member \ \Rightarrow \ \exists s.\, (s \in \mathbb{P}(member) \ \wedge \ s \neq \{\} \ \wedge \ n \notin s))$

Teemu’s questions - 3

3. Calculate the following weakest preconditions: (In the following $x..y$ refers to the range of naturals from x to y inclusive)

1. $[serve\ :=\ serve + new](serve \leq next)$

2. $[serve, next\ :=\ serve + new,\ next + 1](serve \leq next)$

3. $[x, y\ :=\ 3, 11](\forall\, x.\ (x \in \mathbb{N}\ \Rightarrow\ x^2 + 4))$

4. $[x, y, house\_set\ :=\ x - 1, y + 1, house\_set\ \cup\ \{x, y\}](houset\_set \subseteq x..y)$

Teemus's questions - 4

4. What, if anything, is wrong with the following machine context ?

MACHINE $Inventory(space)$

CONSTRAINTS $space \in \mathbb{N}_1 \wedge maximum \leq space$

CONSTANTS $maximum$

PROPERTIES $maximum \in \mathbb{N}_1$

Teemu’s questions - 5

5. The Relation $eats$ is defined as follows:

$$eats = \{\ ian \mapsto eggs,\ ian \mapsto cheese,\ ian \mapsto pizza,\ jim \mapsto eggs,$$
$$jim \mapsto salad,\ ken \mapsto pizza,\ lisa \mapsto cheese,\ lisa \mapsto salad,\ lisa \mapsto pizza\ \}$$

1. What is $\{ian\} \lhd eats$?
2. What is the relation $\{jim\} \blacktriangleleft eats$?
3. What is the relation $eats \rhd \{cheese, pizza\}$?
4. What is $dom(eats \rhd \{eggs\})$?

Teemu Tynjälä

Teemu’s questions - 6

6. Remember the $Results$ machine I showed you as part of the B sequences? Now, your task is to augment the machine with two operations as follows:

- $pp \longleftarrow$ **position**(rr) which takes a runner rr who is in the list and gives his/her position pp as output
- **remove**(rr) which takes a runner rr who appears in the list $finish$, and removes him/her from it

Teemu’s questions - 7

7. A helper may be chose from the set *here* using the following SELECT statement:

```
SELECT $albert \in here$ THEN $hh := albert$
        WHEN $betty \in here$ THEN $hh := betty$
        WHEN $clarissa \in here$ THEN $hh := clarissa$
        ELSE $hh := fido$
END
```

1. What is the weakest precondition which guarantees postcondition $hh = clarissa$?

2. In which initial state is the postcondition $hh \neq albert$ guaranteed ?

3. What guarantees the postcondition $hh \neq fido$?

Teemu Tynjälä

Teemu’s questions - 8

8. Give a machine which captures the following description:

A $Deliveries$ machine keeps track of the items on a delivery van, and the addresses to which they should be delivered. It also keeps track of a special set of addresses $nogo$ for which there might be problems making deliveries.

Initially, the van is empty, and the set $nogo$ can be initialised with any arbitrary set of addresses.

The machine provides four operations:

- **load** takes an address aa and an item ii as input, and adds ii (to be delivered to aa) to the contents of the van

Teemu’s questions - 8 continued

- **drop** should only be invoked when the van is not empty. In such a case, it chooses an arbitrary item *ii* on the van, and delivers it to the address *aa*; these two values are provided as outputs to the operation. (Note, giving two outputs is possible...)

- **endofday** can always be invoked. It nondeterministically chooses either to empty the van, or to leave it as it is. It has no inputs or outputs.

- **warning** takes an address *aa* as input. If the address is in *nogo* then it might remove all the items associated with that address from the van; or alternatively it might remove the address from *nogo*. If the address is not in *nogo* and there are no deliveries to that address, then it will be inserted into *nogo*. In all other cases, the operation has no effect.

Due Dates + Submission format

- You have until midnight on May 12 to return the assignments.
- Make an electronic submission (*.doc, *.ps or *.pdf) and mail it to Ilkka and myself to addresses teemu.tynjala@nokia.com and herttua@eurolock.org