BCS2213 – Formal methods

Teaching assignment 4. TLA specification of Asynchronous Interface.

1. Run TLA+ Toolbox.

2. Develop TLA specification of AsynchInterface, as shown below (please use as module name Lab_4_<Your_ID>)

---- MODULE *AsynchInterface* ----

EXTENDS *Naturals*
CONSTANT *Data*
VARIABLES *val*, *rdy*, *ack*

$$TypeInvariant \triangleq \begin{array}{l} \land\ val \in Data \\ \land\ rdy \in \{0,1\} \\ \land\ ack \in \{0,1\} \end{array}$$

$$Init \triangleq \begin{array}{l} \land\ val \in Data \\ \land\ rdy \in \{0,1\} \\ \land\ ack = rdy \end{array}$$

$$Send \triangleq \begin{array}{l} \land\ rdy = ack \\ \land\ val' \in Data \\ \land\ rdy' = 1 - rdy \\ \land\ \text{UNCHANGED}\ ack \end{array}$$

$$Rcv \triangleq \begin{array}{l} \land\ rdy \neq ack \\ \land\ ack' = 1 - ack \\ \land\ \text{UNCHANGED}\ \langle val, rdy \rangle \end{array}$$

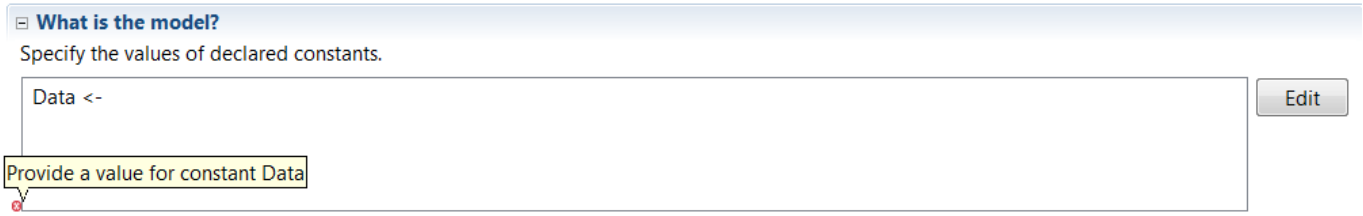
$$Next \triangleq Send \lor Rcv$$

$$Spec \triangleq Init \land \Box[Next]_{\langle val, rdy, ack \rangle}$$

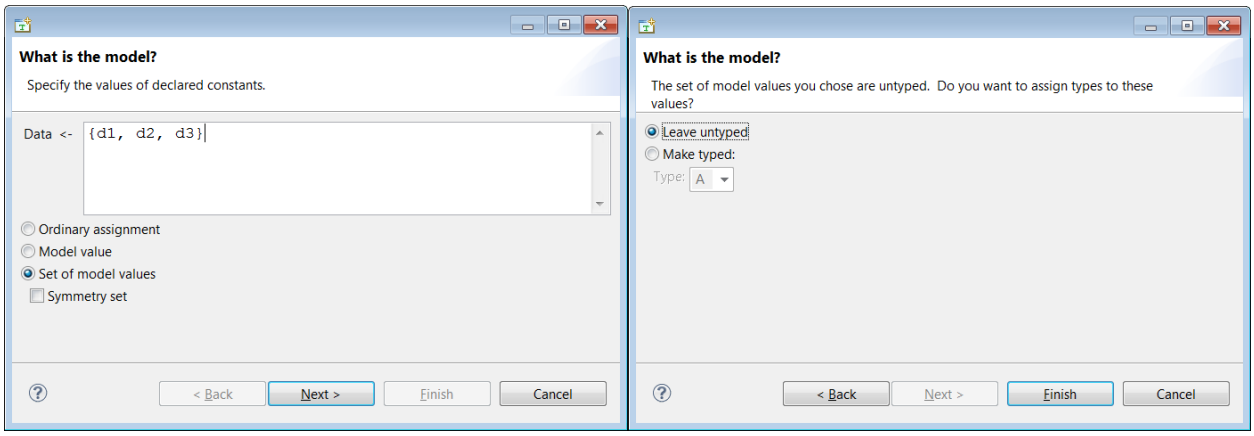
THEOREM $Spec \Rightarrow \Box TypeInvariant$

---

3. To run the model you need provide a value for const Data. Find in the Model Overview page the next window and press "Edit" button.



- Specify the values of declared constants as shown on the next figure and press "Next >"
- Leave values untyped and press "Finish".



As result you will see

4. Analyze the amount of distinct states, generated by TLC.

For it change the size of the Data set (add, delete elements) and see the results.

5. What happens if you will specify ***AND*** operation in the next state predicate, linking ***Send*** and ***Rsv*** actions?

Is such the behavior correct? Check it by TLC. Write corresponding comment in your code.

6. Modify the specification to send the values of data, like we did in HourClock, i.e. variable ***val*** should have values 1, 2, 3 … 12, and next again start from 1, 2, 3 … 12 etc.

7. TLC allows to print values during module checking.

Operator **Print** is defined in the standard module **TLC**, you need include it by the **EXTENDS** keyword.

TLA definition of Print is

Print(exp1, exp2) == exp2

i.e. the return value of Print(exp1, exp2) is the expression exp2

To use Print in formulas as ***true*** *assumption* we can specify

Print(exp, TRUE)

To print more, than one expression we can use tuple

Print(<<id, exp>>, TRUE)

Modify Send and Rsv actions by adding corresponding print statements:

/\ Print(<<"Send ", val>>, TRUE)

/\ Print(<<"Rcv ", val>>, TRUE)

Analyze the printed output.

8. Modify the AsyncInterface protocol in order it has *only one synchronization line* – ***ack*** (you can do it on the base of the initial specification by commenting not needed parts or in a new file).

Conditions:

Sender send a ***val*** and set value of ***ack*** to 0 (“work done”).

Receiver receive a ***val***, and set the ***ack*** to 1 (“new request”).

9. Submit the TLA specification into Kalam for evaluation. Name file Lab_4_<Your ID>.tla

This assignment will be evaluated in maximum 2.5% of the general marks.