P. Müller and D. Basin

Formal Methods and Functional Programming

Session Sheet 14: Modeling and LTL

Installing and Running Spin

To run the Promela models, you will need to install the Spin model-checker as well as a C compiler. There are multiple ways to install Spin on your machine:

- **Windows:** You can download the archive from the following link and follow the readme: `https://polybox.ethz.ch/index.php/s/cQifMKXUW3G2iAI`
- **Ubuntu:** Run `sudo apt-get install spin` in a terminal to install the `spin` package.
- **Mac:** Use Homebrew (`https://brew.sh`) to install Spin by running `brew install spin`.
- **Executables:** Download pre-compiled executables from Spin's GitHub page: `https://github.com/nimble-code/Spin/tree/master/Bin`.
- **Compiling**: You can compile Spin from source from: `https://github.com/nimble-code/Spin`.

Short re-cap for running Spin:

- `spin filename.pml` will carry out a simulation of the model, yielding one random trace. This does *not* perform an exhaustive check the model.
- `spin -a filename.pml` will create a file `pan.c`, that must be compiled and run to exhaustively check a model. In case of failure, a corresponding trail file (`filename.pml.trail`) is typically generated, containing the information about the failing trace.
- `spin -t filename.pml` will replay the trace from the corresponding trail file.

Assignment 1 (Modeling in Promela)

Task 1.1. Consider the statement

```
y := 0;
while x > 0 do
    y := y + x;
    x := x - 2
end
```

and write a model in Promela to check if the statement, starting in a state σ with $\sigma(\mathrm{x}) = 3$ will reach a state σ' with $\sigma'(\mathrm{y}) = 4$.

Task 1.2. Write a model in Promela to verify that executing the statement

$$\texttt{x := 1} \;\square\; \texttt{x := 2; x := x + 2}$$

will result in a state σ where either $\sigma(\mathrm{x}) = 1$ or $\sigma(\mathrm{x}) = 4$.

Task 1.3. Now, consider the statement

$$\texttt{x := 1 par (x := 2; x := x + 2)}$$

and write a model verifying that its execution results in a state σ with $\sigma(\mathrm{x}) \in \{1, 3, 4\}$.

Task 1.4. Consider the following program:

```
x := 5;
y := 1;
(while x > 1 and y < 5 do
   (x := x - y [] y := y + 1)
end
par
while x > 0 do
    y = y + 1;
    x = x - 1
end)
```

Assume that we start the program in some state. Can we reach a final state σ with $\sigma(\mathrm{x}) = -7$? What is the minimal value of the variable x after executing the program?

Task 1.5. Consider the Promela model below and use spin to identify a deadlock.

```
int x

proctype left() {
    do
    :: x > 0 -> x = x - 1
    od
}

proctype right() {
    do
    :: x < 0 -> x = x + 1
    od
}

init {
x = 2
    run left()
    run right()
}
```

Assignment 2 (Modeling Traffic Lights)

Consider a traffic light with a green, a yellow and a red light. We wish to check the safety property "red is always preceded by yellow". Which atomic propositions do you need? State the LTL property.

Assignment 3 (Linear Temporal Logic)

Task 3.1. Consider a transition system with two states s_1, s_2, where s_1 is the initial state, transitions back and forth from s_1 to s_2 and a loop from s_2 to itself. Let p be true in and only in state s_2. Discuss the difference between $\Box\Diamond p$ (holds) and $\Diamond\Box p$ (does not hold – counter example $s_1 s_2 s_1 s_2 s_1 s_2 ...$).

Task 3.2. Now consider a transition system with three states s_1, s_2, s_3, where s_1 is the initial state. There are the following transitions: $s_1 \to s_2$, $s_1 \to s_3$, $s_2 \to s_3$, $s_2 \to s_2$ and $s_3 \to s_3$. Let p be true in and only in s_2. Discuss the LTL formula $\bigcirc p \Rightarrow \Box p$. The formula is false in the model. However, under the wrong interpretation of $\models$ one might think it is true ($\bigcirc p$ is false in the model; therefore $\bigcirc p \Rightarrow \Box p$ appears to be vacuously true). Notice that $\bigcirc\neg p \Rightarrow \Box\neg p$ happens to be true.

Task 3.3. In the same transition system, discuss the formula $\Diamond p \ \vee \ \Box\neg p$, which is true, but may be considered false (neither of the disjuncts is true).

Assignment 4 (Liveness and Safety Properties)

Let p be an atomic proposition.

Task 4.1. Prove that both $\Box\Diamond p$ and $\Diamond\Box p$ express liveness properties.

Task 4.2. Prove that $\Box p$ expresses a safety property.