

## Basic temporal formulas

| Property             | Formula pattern  | Meaning  | Example  |
|----------------------|--|--|--|
| Deadlock             | $\text{deadlock} = [\text{true}] \text{false}$   | State without any outgoing transition (sink)   |  |
| Deadlock freedom     | $\text{not } < \text{true}^* > \text{deadlock}$<br>$=$<br>$\text{not } < \text{true}^* > [\text{true}] \text{false}$<br>$=$<br>$[\text{true}^*] < \text{true} > \text{true}$                           | There is no deadlock state reachable from the initial state (every reachable state has at least one outgoing transition)   |  |
| Safety               | $[\text{R}] \text{false}$  | There is no transition sequence matching the regular formula R   | $[\text{true}^* . \text{REQ0} . (\text{not REL0})^* . \text{REQ1}] \text{false}$ |
| Potentiality         | $< \text{R} > \text{true}$   | There exists a transition sequence matching the regular formula R  | $< \text{true}^* . \text{PUT} . \text{true}^* . \text{GET} > \text{true}$        |
| Inevitable execution | $\text{INEV (A)} =$<br>// using macros from actl.mcl<br>$\text{AU\_A\_A (true, true, A, true)} =$<br>// using MCL operators<br>$\mu X . (< \text{true} > \text{true} \text{ and } [\text{not (A)}] X)$ | All transition sequences going out of the initial state contain an A-transition  | $\text{INEV (GET)}$  |
| Fair execution       | $\text{FAIR (A)} =$<br>$[\text{(not (A))}^*] < \text{true}^* . (\text{A}) > \text{true}$   | All transition sequences, after skipping possible cycles, contain an A-transition (as long as an A-transition has not been reached, it is still possible to reach one) | $\text{FAIR (GET)}$  |
| Response             | $[\text{R}] \text{INEV (A)}$   | All sequences matching the regular formula R lead necessarily to states from which A is inevitably executed  | $[\text{true}^* . \text{PUT}] \text{INEV (GET)}$                                 |
| Unfair execution     | $< \text{R} > @$   | There is an infinite (unfair) sequence made by concatenating subsequences satisfying R   | $< \text{true}^* . \text{REQ0} >$<br>$< (\text{not CS0})^* . \text{CS1} > @$     |

## Data-handling temporal formulas

| Property                                      | Formula pattern   | Meaning   | Example   |
|---|---|---|---|
| Wildcard                                      | $\langle \{ A ?any \} \rangle \text{ true}$   | State having an outgoing A-transition carrying some data value  | $\langle \{ PUT ?any \} \rangle \text{ true}$   |
| Value matching                                | $\langle \{ A !v \} \rangle \text{ true}$   | State having an outgoing A-transition carrying value v  | $\langle \{ PUT !0 \} \rangle \text{ true}$   |
| Value extraction                              | $[ \{ A ?x:T \} ] (x = v)$<br>=<br>$[ \{ A ?x:T \text{ where } x \neq v \} ] \text{ false}$     | State whose all outgoing A-transitions carry a value $x=v$ (or there are no outgoing A-transitions carrying a value different from v)   | $[ \{ GET ?m:Nat \} ]$<br>( $m = 1$ )   |
| Value propagation (inside the same modality)  | $[ R1 . \{ A1 ?x:T \} . R2 . \{ A2 !x \} ] \text{ false}$                                       | There is no transition sequence matching the regular formula R1, followed by an A1-transition carrying value v (captured in data variable x), followed by a subsequence matching R2, and ending with an A2-transition carrying value v      | $[ \text{true}^* . \{ CS ?x:Nat \} . (\text{not } \{ REL ?any \})^* . \{ CS !x \} ] \text{ false}$    |
| Value propagation (inside the same modality)  | $\langle R1 . \{ A1 ?x:T \} . R2 . \{ A2 !x \} \rangle @$                                       | There is an infinite sequence made by concatenating subsequences matching R1, followed by an A1-transition carrying value v (captured in data variable x), followed by a subsequence matching R2, then by an A2-transition carrying value v | $\langle \text{true}^* . \{ REQ ?x:T \} . (\text{not } \{ REL !x \})^* . \{ CS !x \} \rangle @$       |
| Value propagation (between nested modalities) | $[ \text{true}^* . \{ A ?x:T \} ]$<br>$\langle \text{true}^* . \{ B !x \} \rangle \text{ true}$ | After each A-transition carrying value v (captured in data variable x) it is possible to reach a B-transition carrying value v  | $[ \text{true}^* . \{ PUT ?m:Nat \} ]$<br>$\langle \text{true}^* . \{ GET !m \} \rangle \text{ true}$ |
| Value propagation (between nested formulas)   | $[ \text{true}^* . \{ A ?x:T \} ]$<br>$INEV (\{ B !x \})$                                       | After each A-transition carrying value v (captured in data variable x) it is inevitable to execute a B-transition carrying value v  | $[ \text{true}^* . \{ REQ ?x:T \} ]$<br>$INEV (\{ CS !x \})$  |