NuSMV-ARCTL-TLACE – User manual

Simon Busard

December 7, 2011

This document is a short user manual about the generation of TLACEs (tree-like annotated counter-examples) using NuSMV-ARCTL-TLACE.

Three options have been added to NuSMV to manage the generation of TLACEs:

```
-tlaces tl      sets tlaces explanation level to "tl",
                value is used as bitmask
                (1: ex; 2: eu; 4: eg, 0: activate)
-otlaces file   Prints counter-example to file "file"
-dtlaces dl     sets tlaces explanation depth to "dl"
```

The `tlaces` option activates the generation of TLACEs. When this option is provided, the check of a CTL specification on a model leads to the execution of a new algorithm generating and displaying a TLACE if the specification is not satisfied. The value of the `tlaces` option works as a bitmask. If `tlace` $\wedge 1 \neq 0$, `tlace` $\wedge 2 \neq 0$ or `tlace` $\wedge 4 \neq 0$, the **EX**, **EU** or **EG** operators (respectively) will be explained: when a state satisfies a formula $\mathbf{EX}\phi$ (resp. $\mathbf{E}[\phi_1 \mathbf{U} \phi_2]$ or $\mathbf{EG}\phi$), a branch explaining why it satisfies the formula is generated; otherwise, no branch is generated and the annotation of the resulting TLACE node is labelled as unexplained. Finally, if `tlaces` $= 0$, a TLACE will be generated, but no branch will be explained; if the option is not provided, the standard behavior of NuSMV is used. This option can also be activated in the interactive mode of NuSMV by changing the value of the `tlaces_explain_level` variable using appropriate commands.

The second option, `otlaces`, defines the output file. When this option is used, its value is the path to the output file in which the generated TLACE will be printed. If the `tlaces` option is not specified, the `otlaces` option has no effect. This option can also be modified in the interactive mode of NuSMV by changing the value of the `output_tlaces_file` variable using appropriate commands.

The third option, `dtlaces`, defines the depth of temporal operators that the generating algorithm will explain. Every temporal sub-formula with (temporal) depth higher than the given number is not explained and the annotation remains unexplained. For example, a witness for $\mathbf{E}[(\mathbf{EX}\phi)\mathbf{U}(\mathbf{EG}\psi \wedge \mathbf{EFEG}\chi)]$ generated with a maximum depth of 1 will explain the **EU**, **EX**, **EF** and $\mathbf{EG}\psi$ operators, but not the $\mathbf{EG}\chi$ formula because its temporal depth is 2. This option can also be modified in the interactive mode of NuSMV by changing the value of the `tlaces_depth` variable using appropriate commands.

Finally, the XML output of NuSMV is described by the grammar below.

```
XML          ::= <?xml version="1.0" encoding="UTF-8"?>
                     CNTEX
CNTEX        ::= <counterexample specification="SPEC">
                     NODE
                 </counterexample>
NODE         ::= <node id="ID">
                     STATE
                     ATOMIC*
                     EXISTENTIAL*
                     UNIVERSAL*
                 </node>
STATE        ::= <state>
                     VALUE+
                 </state>
VALUE        ::= <value variable="NAME">VAL</value>
ATOMIC       ::= <atomic specification="SPEC" />
EXISTENTIAL ::= <existential specification="SPEC" explained="true">
                     PATH
                 </existential>
                 | <existential specification="SPEC" explained="false" />
UNIVERSAL    ::= <universal specification="SPEC" />
PATH         ::=NODE (INPUT NODE)+ LOOP?
INPUT        ::=<combinatorial>
                     VALUES*
                 </combinatorial>
                 <input>
                     VALUES*
                 </input>
LOOP         ::= INPUT
                 <loop to="ID" />
```