Formal Model of the Contract Automata Runtime Environment

This folder contains different versions of the Uppaal model of CARE (we used the version of Uppal 4.1.26-1, February 2022).

The files `model_exhaustive.xml` and `model_statistical.xml` contain the same model. They contain, respectively, the formulae for exhaustive and statistical model checking (with different set-ups). The other models are variations of this base version. In `model_configurable` the configuration options are also parameters of the templates. In `model_allbuffers` each pair of services has its own buffers for communicating.

Testing

The following models have been employed to generate tests that demonstrate the model's adherence to the actual implementation. Generally, each transition that involves enqueuing or dequeuing messages produces test code for writing to or reading from a socket, respectively. The tests generated by Uppaal have been transformed into concrete tests for the source code. Uppaal provides various methods for test generation, and in this case, we utilized the generation from queries of the form E<>. These queries encode specific simulation traces that are relevant to the specific orchestration employed in the tests. To achieve this, two variables, namely `steps[]` and `step`, are utilized to encode the desired simulation in the query. The generated tests cover all transitions of the model and all interactions between the orchestrator and the services.

The file `model_testing_orc.xml` has been used for testing the RunnableOrchestration. There are three queries used to generate the tests (under the folder `/src/test`) of, respectively,
`DictatorialCentralisedRunnableOrchestrationTest.java`,
`MajoritarianCentralisedRunnableOrchestrationTest.java`,
`MajoritarianDistributedRunnableOrchestrationTest.java`.

The file `model_testing_roc.xml` has been used for testing the RunnableOrchestratedContract. In this case, the tester is only the orchestrator, i.e., the interactions between two services in a distributed match are not tested. There are three queries used to generate the tests (under the folder `/src/test`) of, respectively,
`MajoritarianCentralisedRunnableOrchestratedContractTest.java`,
`DictatorialCentralisedRunnableOrchestratedContract.java`,
`DictatorialDistributedRunnableOrchestratedContract.java`.

The file `model_testing_roc_distributed_offerer` has been used for testing the interactions between two RunnableOrchestratedContract in a distributed match. In this case the tester is represented by the orchestrator and one of the two interactive services, i.e., the requester in the match. The query has been used to generate the test in `DictatorialDistributedRunnableOrchestratedContract_DistributedMatchOfferer_Test.java`.

The file `model_testing_roc_distributed_requester` has been used for testing the interactions between two RunnableOrchestratedContract in a distributed match. In this case the tester is represented by the orchestrator and one of the two interactive services, i.e., the offerer in the match. The query has been used to generate the test in `DictatorialDistributedRunnableOrchestratedContract_DistributedMatchRequester_Test.java`.

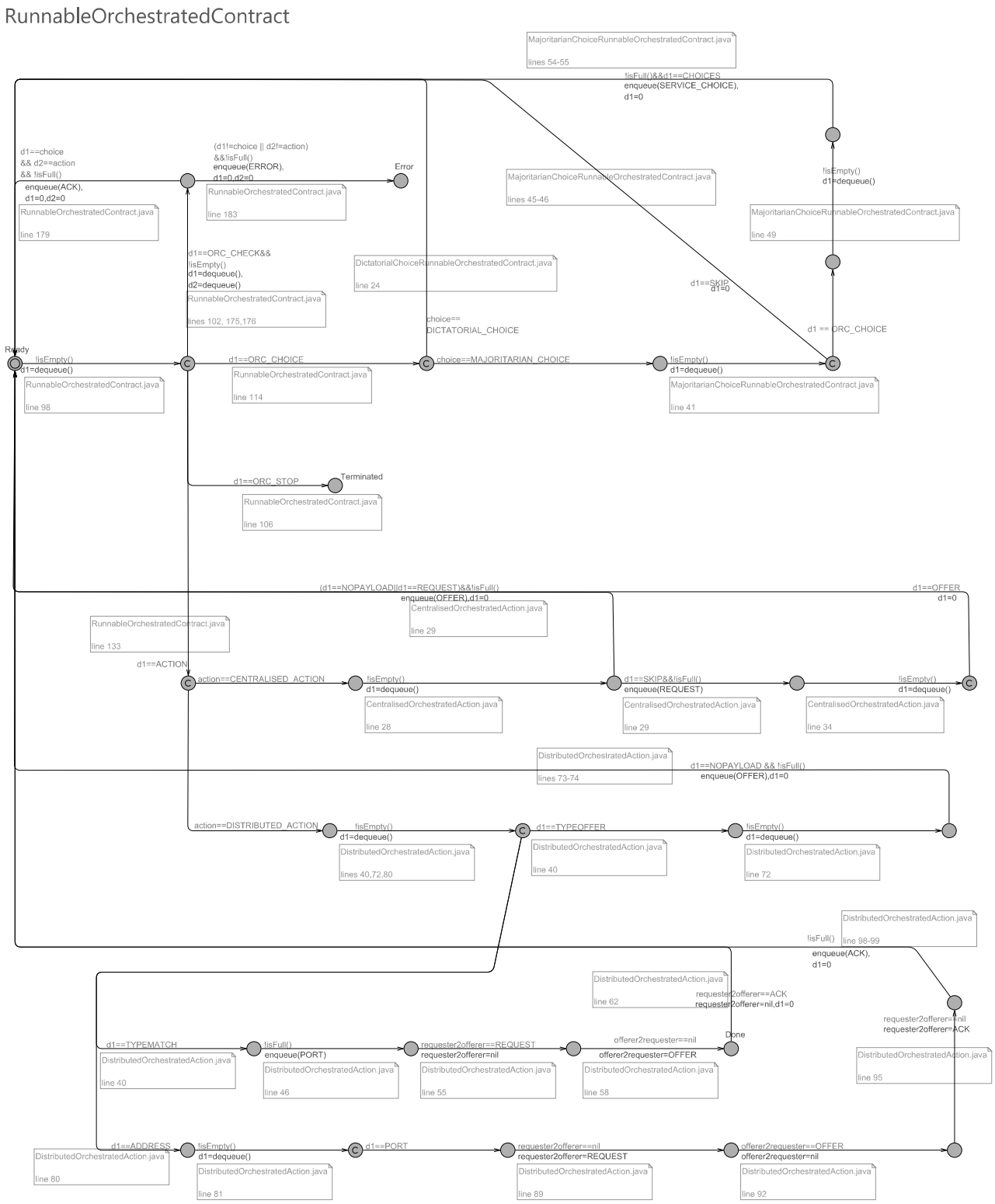
Here is the coverage information generated by IntelliJ. The code coverage indicates that the tests derived from the model cover a significant portion of the source code. This suggests that the model is not excessively abstract compared to the actual implementation.

Element	Class, %	Method, %	Line, %
io.github.contractautomata.care.runnable	100% (12/12)	84% (39/46)	83% (292/351)
actions	100% (4/4)	100% (8/8)	92% (91/98)
CentralisedOrchestratedAction	100% (1/1)	100% (2/2)	100% (8/8)
CentralisedOrchestratorAction	100% (1/1)	100% (2/2)	95% (22/23)
DistributedOrchestratedAction	100% (1/1)	100% (2/2)	88% (39/44)
DistributedOrchestratorAction	100% (1/1)	100% (2/2)	95% (22/23)
OrchestratedAction	100% (0/0)	100% (0/0)	100% (0/0)
OrchestratorAction	100% (0/0)	100% (0/0)	100% (0/0)
choice	100% (4/4)	81% (13/16)	90% (57/63)
DictatorialChoiceRunnableOrchest	100% (1/1)	100% (3/3)	100% (3/3)
DictatorialChoiceRunnableOrchest	100% (1/1)	75% (3/4)	83% (10/12)
MajoritarianChoiceRunnableOrche	100% (1/1)	100% (4/4)	94% (16/17)
MajoritarianChoiceRunnableOrche	100% (1/1)	60% (3/5)	90% (28/31)
AutoCloseableList	100% (1/1)	100% (2/2)	71% (5/7)
RunnableOrchestratedContract	100% (2/2)	80% (8/10)	80% (69/86)
RunnableOrchestration	100% (1/1)	80% (8/10)	72% (70/97)

Traceability

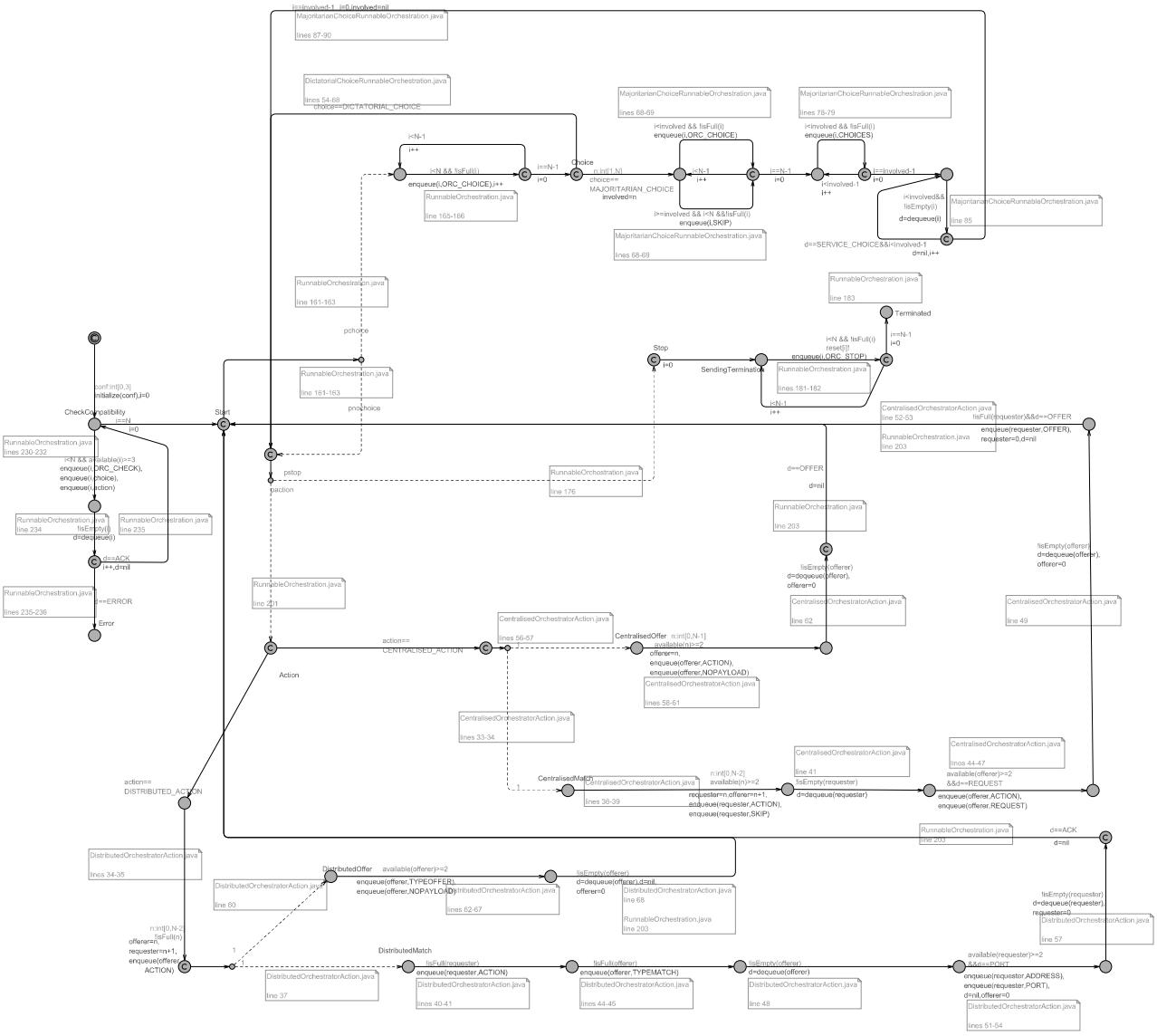
In the file `model_traceability.xml` each transition is traced back to the corresponding source code instructions using comments. The model is slightly polished to improve readability. Traceability information is related to the source code version b1a6954, navigable here https://github.com/contractautomataproject/CARE/tree/b1a695469fbb5a4d212a96dd95bffa0ed39b71b8.

The `RunnableOrchestratedContract` automaton with traceability is displayed below.



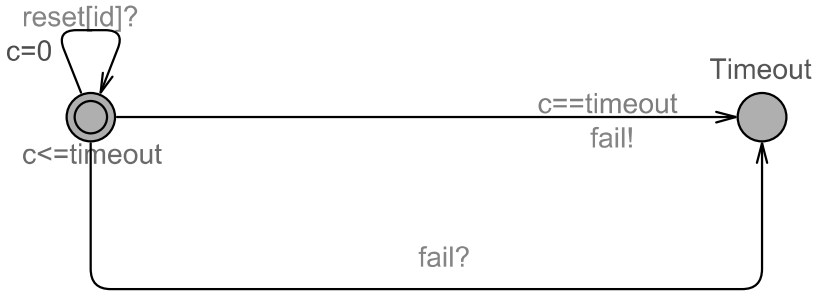
The `RunnableOrchestration` automaton with traceability is displayed below.

RunnableOrchestration



The `SocketTimeout` automaton with traceability is displayed below.

```
java.net.ServerSocket, java.net.Socket, java.net.SocketTimeoutException
RunnableOrchestration.java              lines 44,140,206-210
RunnableOrchestratedContract.java lines 37,82,146-150
```



SocketTimeout

Logs of the Verification

The verification has been performed on a machine with Intel(R) Core(TM) i9-9900K CPU @ 3.60 GHz equipped with 32 GB of RAM.

model_statistical.xml

./verifyta -u --alpha 0.0005 --epsilon 0.0005 model_statistical.xml Options for the verification: Generating no trace Search order is breadth first Using conservative space optimisation Seed is 1685907555 State space representation uses minimal constraint systems

Verifying formula 1 at /nta/queries/query[1]/formula -- Formula is satisfied. (10000 runs) E(max) = 4.5129 Values in [3,9] mean=4.5129 steps=1: 1360 3809 3472 1090 242 24 3 -- States explored : 5242112 states -- CPU user time used : 20020 ms -- Virtual memory used : 50120 KiB -- Resident memory used : 13232 KiB

Verifying formula 2 at /nta/queries/query[2]/formula -- Formula is satisfied. (7598 runs) Pr(<> ...) in [0,0.000999882] with confidence 0.9995. -- States explored : 3947466 states -- CPU user time used : 14570 ms -- Virtual memory used : 50120 KiB -- Resident memory used : 13628 KiB

Verifying formula 3 at /nta/queries/query[3]/formula -- Formula is satisfied. (14670 runs) Pr(<> ...) in [8.0363e-06,0.00100802] with confidence 0.9995. Values in [15,15.4314] mean=15.1438 steps=0.0043138: 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 -- States explored : 7708303 states -- CPU user time used : 21510 ms -- Virtual memory used : 50120 KiB -- Resident memory used : 13696 KiB

Verifying formula 4 at /nta/queries/query[4]/formula -- Formula is satisfied. (21656 runs) Pr(<> ...) in [0.998927,0.999927] with confidence 0.9995. Values in [8.93272,306.729] mean=35.1171 steps=2.97796: 158 1589 2562 2762 1868 1631 1520 1139 1035 930 806 680 599 529 424 370 355 282 252 245 200 192 176 138 132 107 104 102 66 77 56 59 59 48 37 42 32 33 24 15 23 14 17 14 20 13 11 16 11 9 7 4 4 4 8 3 4 3 2 1 3 2 3 0 3 1 1 2 0 2 0 1 0 0 0 0 1 1 1 1 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 -- States explored : 11326049 states -- CPU user time used : 32500 ms -- Virtual memory used : 50512 KiB -- Resident memory used : 13776 KiB

Verifying formula 5 at /nta/queries/query[5]/formula -- Formula is satisfied. (7598 runs) Pr(<> ...) in [0,0.000999882] with confidence 0.9995. -- States explored : 3979140 states -- CPU user time used : 26310 ms -- Virtual memory used : 50512 KiB -- Resident memory used : 14012 KiB

Verifying formula 6 at /nta/queries/query[6]/formula -- Formula is satisfied. (7598 runs) Pr(<> ...) in [0,0.000999882] with confidence 0.9995. -- States explored : 4043243 states -- CPU user time used : 14920 ms -- Virtual memory used : 50512 KiB -- Resident memory used : 13836 KiB

model_exhaustive.xml

N=4 buffer size=5 ./verifyta -T -S 2 -u model.xml Options for the verification: Generating no trace Search order is breadth first Using aggressive space optimisation Using reuse optimisation Seed is 1685897160 State space representation uses minimal constraint systems

Verifying formula 1 at /nta/queries/query[1]/formula -- Formula is satisfied. -- States stored : 14751623 states -- States explored : 51999065 states -- CPU user time used : 148290 ms -- Virtual memory used : 1762344 KiB -- Resident memory used : 1725932 KiB

Verifying formula 2 at /nta/queries/query[2]/formula -- Formula is satisfied. -- States stored : 14751623 states -- States explored : 25584278 states -- CPU user time used : 178960 ms -- Virtual memory used : 1762344 KiB -- Resident memory used : 1725932 KiB

Verifying formula 3 at /nta/queries/query[3]/formula -- Formula is satisfied. -- States stored : 14751623 states -- States explored : 25584278 states -- CPU user time used : 114210 ms -- Virtual memory used : 1500180 KiB -- Resident memory used : 1496252 KiB

Verifying formula 4 at /nta/queries/query[4]/formula -- Formula is NOT satisfied. -- States explored : 24 states -- CPU user time used : 2710 ms -- Virtual memory used : 1394984 KiB -- Resident memory used : 1390828 KiB

N=5 buffer size=3

./verifyta -T -S 2 -u model.xml Options for the verification: Generating no trace Search order is breadth first Using aggressive space optimisation Using reuse optimisation Seed is 1685898109 State space representation uses minimal constraint systems

Verifying formula 1 at /nta/queries/query[1]/formula -- Formula is satisfied. -- States stored : 118680005 states -- States explored : 426454001 states -- CPU user time used : 1842200 ms -- Virtual memory used : 12999600 KiB -- Resident memory used : 12967008 KiB

Verifying formula 2 at /nta/queries/query[2]/formula -- Formula is satisfied. -- States stored : 118680005 states -- States explored : 189186495 states -- CPU user time used : 2338670 ms -- Virtual memory used : 12999600 KiB -- Resident memory used : 12967600 KiB

Verifying formula 3 at /nta/queries/query[3]/formula -- Formula is satisfied. -- States stored : 118680005 states -- States explored : 189186495 states -- CPU user time used : 1588060 ms -- Virtual memory used : 11656076 KiB -- Resident memory used : 10192724 KiB

Verifying formula 4 at /nta/queries/query[4]/formula -- Formula is NOT satisfied. -- States explored : 28 states -- CPU user time used : 23880 ms -- Virtual memory used : 10375828 KiB -- Resident memory used : 10228416 KiB

model_configurable.xml

./verifyta -T -S 2 -u model_configurable.xml Options for the verification: Generating no trace Search order is breadth first Using aggressive space optimisation Using reuse optimisation Seed is 1685907156 State space representation uses minimal constraint systems

Verifying formula 1 at /nta/queries/query[1]/formula -- Formula is satisfied. -- States stored : 19 states -- States explored : 41 states -- CPU user time used : 0 ms -- Virtual memory used : 47984 KiB -- Resident memory used : 10540 KiB

Verifying formula 2 at /nta/queries/query[2]/formula -- Formula is satisfied. -- States explored : 79 states -- CPU user time used : 0 ms -- Virtual memory used : 49092 KiB -- Resident memory used : 11964 KiB

model_allbuffers.xml

./verifyta -T -S 2 -u model_allbuffers.xml Options for the verification: Generating no trace Search order is breadth first Using aggressive space optimisation Using reuse optimisation Seed is 1685906976 State space representation uses minimal constraint systems

Verifying formula 1 at /nta/queries/query[1]/formula -- Formula is satisfied. (29 runs) Pr(<> ...) in [0.901855,1] with confidence 0.95. Values in [3.29874,46.2886] mean=14.6587 steps=0.429898: 2 0 1 4 1 0 1 1 2 3 0 1 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 -- States explored : 5377 states -- CPU user time used : 10 ms -- Virtual memory used : 48152 KiB -- Resident memory used : 11108 KiB

Verifying formula 2 at /nta/queries/query[2]/formula -- Formula is satisfied. (29 runs) Pr(<> ...) in [0,0.0981446] with confidence 0.95. -- States explored : 8198 states -- CPU user time used : 20 ms -- Virtual memory used : 48152 KiB -- Resident memory used : 11108 KiB

Verifying formula 3 at /nta/queries/query[3]/formula -- Formula is satisfied. (10000 runs) E(max) = 3.7594 Values in [3,8] mean=3.7594 steps=1: 4751 3365 1484 342 55 3 -- States explored : 2104778 states -- CPU user time used : 2750 ms -- Virtual memory used : 48400 KiB -- Resident memory used : 11440 KiB

Verifying formula 4 at /nta/queries/query[4]/formula -- Formula is satisfied. (29 runs) Pr(<> ...) in [0,0.0981446] with confidence 0.95. -- States explored : 6321 states -- CPU user time used : 10 ms -- Virtual memory used : 48400 KiB -- Resident memory used : 11440 KiB

Verifying formula 5 at /nta/queries/query[5]/formula -- Formula is satisfied. (29 runs) Pr(<> ...) in [0,0.0981446] with confidence 0.95. -- States explored : 4482 states -- CPU user time used : 0 ms -- Virtual memory used : 48152 KiB -- Resident memory used : 11192 KiB

Verifying formula 6 at /nta/queries/query[6]/formula -- Formula is satisfied. (29 runs) Pr(<> ...) in [0.901855,1] with confidence 0.95. Values in [0.00620472,1.40342] mean=0.284262 steps=0.0139721: 3 0 2 0 0 3 0 3 1 1 1 2 0 0 1 0 2 1 0 0 0 1 0 0 1 0 0 0 0 0 0 2 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 -- States explored : 58 states -- CPU user time used : 10 ms -- Virtual memory used : 48152 KiB -- Resident memory used : 11192 KiB

Verifying formula 7 at /nta/queries/query[7]/formula -- Formula is satisfied. -- States stored : 260327 states -- States explored : 538250 states -- CPU user time used : 2240 ms -- Virtual memory used : 70804 KiB -- Resident memory used : 38388 KiB

Verifying formula 8 at /nta/queries/query[8]/formula -- Formula is satisfied. -- States stored : 260327 states -- States explored : 538250 states -- CPU user time used : 1340 ms -- Virtual memory used : 70860 KiB -- Resident memory used : 38508 KiB

Verifying formula 9 at /nta/queries/query[9]/formula -- Formula is satisfied. -- States stored : 260327 states -- States explored : 866811 states -- CPU user time used : 1810 ms -- Virtual memory used : 77004 KiB -- Resident memory used : 44596 KiB

Verifying formula 10 at /nta/queries/query[10]/formula -- Formula is NOT satisfied. -- States explored : 20 states -- CPU user time used : 30 ms -- Virtual memory used : 77004 KiB -- Resident memory used : 44596 KiB