Model: AutonomousCar
Type: P/T Net
Origin: Academic

since
MCC 2022

Lucie Muller and Hubert Garavel
lucie.muller@inria.fr

This form is a summary description of the model entitled "AutonomousCar" proposed for the Model Checking Contest @ Petri Nets. Models can be given in several instances parameterized by scaling parameters. Colored nets can be accompanied by one or many equivalent, unfolded P/T nets. Models are given together with property files (possibly, one per model instance) giving a set of properties to be checked on the model.

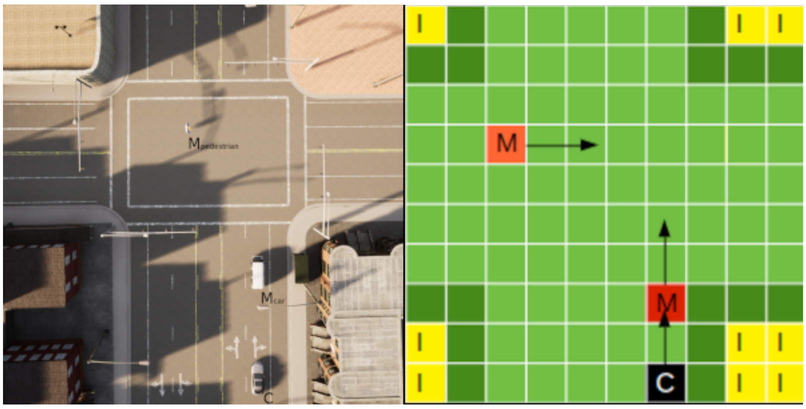
Description

This model was created to simulate realistic scenes involving a car moving towards a destination and trying to avoid collision with obstacles. The car is equipped with sensors (camera, LiDAR, etc.) to perceive its environment. Obstacles represent various hazards. There are immobile obstacles (buildings, trees, parked cars, etc.) and mobile obstacles (cars, cyclists, pedestrians, etc.), the trajectories of which are either predefined or (partially) random. Both kinds of obstacles may be transparent, in which case the car sensors can perceive the environment behind the obstacle, thus making a difference between, e.g., a ball and a truck. The scene map is represented as a two-dimensional grid, the cells of which are either free, occupied by the car, or occupied by an obstacle. The grid is updated every time the car or an obstacle moves. A scene terminates when the car reaches its destination or when a collision occurs.

This system was formally specified using the LNT value-passing process calculus and analyzed using the verification tools available in the CADP toolbox. The collection of P/T nets was obtained from the LNT specifications of the system. Each LNT specification was translated automatically to LOTOS, and then to an interpreted Petri net using the CADP toolbox. Finally, a P/T net was obtained by stripping out all data-related information (variables, types, assignments, guards, etc.) from the interpreted Petri net, leading to a NUPN (Nested-Unit Petri Net) model translated to PNML using the CÆSAR.BDD tool.

Each instance of the model is parameterized by the number N of mobile obstacles.

Each instance is also parameterized by its version V, which specifies how the NUPN has been produced from the LOTOS specification. V is either equal to "*a*" if the NUPN has been generated *after* applying all the structural and data-flow optimizations of the CÆSAR compiler for LOTOS, or to "*b*" if the NUPN has been generated *before* these optimizations.



Representation of a map with one car, four immobile obstacles, and two mobile obstacles.

References

[1] Jean-Baptiste Horel, Christian Laugier, Lina Marsso, Radu Mateescu, Lucie Muller, Anshul Paigwar, Alessandro Renzaglia, and Wendelin Serwe. *Using Formal Conformance Testing to Generate Scenarios for Autonomous Vehicles.* Design, Automation & Test in Europe Conference & Exhibition (DATE 2022), Antwerp, Belgium, March 2022, IEEE, pages 532-537.

[2] Lina Marsso, Radu Mateescu, Lucie Muller, and Wendelin Serwe. *Formally Modeling Autonomous Vehicles in LNT for Simulation and Testing.* Proceedings of the 5th Workshop on Models for Formal Analysis of Real Systems (MARS 2022), Munich, Germany, April 2022. EPTCS vol. 355, pages 60-117, `https://doi.org/10.4204/EPTCS.355.5`.

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
(N, V)	N is the number of mobile obstacles and V is the version defined above	$\{1, ..., 10\} \times \{a, b\}$

Size of the model

Parameter	Number of places	Number of transitions	Number of arcs	Number of units	HWB code
$N = 1, V = a$	25	35	143	7	2–6–15
$N = 1, V = b$	119	132	339	11	4–6–31
$N = 2, V = a$	33	69	368	8	2–7–19
$N = 2, V = b$	155	194	620	13	5–7–36
$N = 3, V = a$	41	121	745	9	2–8–22
$N = 3, V = b$	190	273	1051	15	6–8–42
$N = 4, V = a$	49	193	1306	10	2–9–25
$N = 4, V = b$	221	368	1658	17	7–9–49
$N = 5, V = a$	57	289	2123	11	2–10–28
$N = 5, V = b$	255	490	2527	19	8–10–55
$N = 6, V = a$	65	417	3356	12	2–11–32
$N = 6, V = b$	289	644	3812	21	9–11–61
$N = 7, V = a$	73	593	5357	13	2–12–35
$N = 7, V = b$	323	846	5865	23	10–12–67
$N = 8, V = a$	81	849	8894	14	2–13–38
$N = 8, V = b$	357	1128	9454	25	11–13–73
$N = 9, V = a$	89	1249	15631	15	2–14–41
$N = 9, V = b$	391	1554	16243	27	12–14–79
$N = 10, V = a$	97	1921	29152	16	2–15–44
$N = 10, V = b$	425	2252	29816	29	13–15–85

Structural properties

ordinary — *all arcs have multiplicity one* .... ✓

simple free choice — *all transitions sharing a common input place have no other input place* .... ✗ [a]

extended free choice — *all transitions sharing a common input place have the same input places* .... ✗ [b]

state machine — *every transition has exactly one input place and exactly one output place* .... ✗ [c]

marked graph — *every place has exactly one input transition and exactly one output transition* .... ✗ [d]

connected — *there is an undirected path between every two nodes (places or transitions)* .... ✓ [e]

strongly connected — *there is a directed path between every two nodes (places or transitions)* .... ✗ [f]

source place(s) — *one or more places have no input transitions* .... ✓ [g]

sink place(s) — *one or more places have no output transitions* .... ✗ [h]

source transition(s) — *one or more transitions have no input places* .... ✗ [i]

sink transitions(s) — *one or more transitions have no output places* .... ✗ [j]

loop-free — *no transition has an input place that is also an output place* .... ? [k]

[a] stated by CÆSAR.BDD version 3.7 on all 20 instances (10 values of N × 2 values of V).

[b] stated by CÆSAR.BDD version 3.7 on all 20 instances (10 values of N × 2 values of V).

[c] stated by CÆSAR.BDD version 3.7 on all 20 instances (10 values of N × 2 values of V).

[d] stated by CÆSAR.BDD version 3.7 on all 20 instances (10 values of N × 2 values of V).

[e] stated by CÆSAR.BDD version 3.7 on all 20 instances (10 values of N × 2 values of V).

[f] from place 1 one cannot reach place 0.

[g] place 0 is a source place.

[h] stated by CÆSAR.BDD version 3.7 on all 20 instances (10 values of N × 2 values of V).

[i] stated by CÆSAR.BDD version 3.7 on all 20 instances (10 values of N × 2 values of V).

[j] stated by CÆSAR.BDD version 3.7 on all 20 instances (10 values of N × 2 values of V).

[k] stated by CÆSAR.BDD version 3.7 to be true on 10 instance(s) out of 20, and false on the remaining 10 instance(s).

conservative — *for each transition, the number of input arcs equals the number of output arcs* .... ✗ [l]
subconservative — *for each transition, the number of input arcs equals or exceeds the number of output arcs* ...... ✗ [m]
nested units — *places are structured into hierarchically nested sequential units* [n] .... ✓

Behavioural properties

safe — *in every reachable marking, there is no more than one token on a place* .... ✓ [o]
dead place(s) — *one or more places have no token in any reachable marking* .... ? [p]
dead transition(s) — *one or more transitions cannot fire from any reachable marking* .... ? [q]
deadlock — *there exists a reachable marking from which no transition can be fired* .... ✓ [r]
reversible — *from every reachable marking, there is a transition path going back to the initial marking* .... ✗ [s]
live — *for every transition t, from every reachable marking, one can reach a marking in which t can fire* .... ✗ [t]

Size of the marking graphs

Parameter	Number of reachable markings	Number of transition firings	Max. number of tokens per place	Max. number of tokens per marking
$N = 1, V = a$	227 [u]	?	1	6
$N = 1, V = b$	117338 [v]	?	1	6
$N = 2, V = a$	2314 [w]	?	1	7
$N = 2, V = b$	4.05173e+06 [x]	?	1	7
$N = 3, V = a$	22521 [y]	?	1	8
$N = 3, V = b$	1.44453e+08 [z]	?	1	8
$N = 4, V = a$	206492 [aa]	?	1	9
$N = 4, V = b$	4.90617e+09 [ab]	?	1	9
$N = 5, V = a$	1.80307e+06 [ac]	?	1	10
$N = 5, V = b$	1.58e+11 [ad]	?	1	10
$N = 6, V = a$	1.51682e+07 [ae]	?	1	11
$N = 6, V = b$	4.86429e+12 [af]	?	1	11
$N = 7, V = a$	1.24045e+08 [ag]	?	1	12
$N = 7, V = b$	1.44416e+14 [ah]	?	1	12
$N = 8, V = a$	9.92718e+08 [ai]	?	1	13
$N = 8, V = b$	4.16431e+15 [aj]	?	1	13
$N = 9, V = a$	7.81208e+09 [ak]	?	1	14
$N = 9, V = b$	1.17275e+17 [al]	?	1	14
$N = 10, V = a$	6.06653e+10 [am]	?	1	15
$N = 10, V = b$	3.23927e+18 [an]	?	1	15

[l] stated by CÆSAR.BDD version 3.7 on all 20 instances (10 values of N × 2 values of V).
[m] stated by CÆSAR.BDD version 3.7 on all 20 instances (10 values of N × 2 values of V).
[n] the definition of Nested-Unit Petri Nets (NUPN) is available from `http://mcc.lip6.fr/nupn.php`
[o] safe by construction – stated by the CÆSAR compiler.
[p] stated by CÆSAR.BDD version 3.7 to be true on 10 instance(s) out of 20, and false on the remaining 10 instance(s).
[q] stated by CÆSAR.BDD version 3.7 to be true on 10 instance(s) out of 20, and false on the remaining 10 instance(s).
[r] stated by CÆSAR.BDD version 3.7 on all 20 instances (10 values of N × 2 values of V).
[s] the marking graph has deadlocks and contains more than one reachable marking.
[t] stated by CÆSAR.BDD version 3.7 on all 20 instances (10 values of N × 2 values of V).
[u] stated by CÆSAR.BDD version 3.7.
[v] stated by CÆSAR.BDD version 3.7.
[w] stated by CÆSAR.BDD version 3.7.
[x] stated by CÆSAR.BDD version 3.7.
[y] stated by CÆSAR.BDD version 3.7.
[z] stated by CÆSAR.BDD version 3.7.
[aa] stated by CÆSAR.BDD version 3.7.
[ab] stated by CÆSAR.BDD version 3.7.
[ac] stated by CÆSAR.BDD version 3.7.

[ad] stated by CÆSAR.BDD version 3.7.

[ae] stated by CÆSAR.BDD version 3.7.

[af] stated by CÆSAR.BDD version 3.7.

[ag] stated by CÆSAR.BDD version 3.7.

[ah] stated by CÆSAR.BDD version 3.7.

[ai] stated by CÆSAR.BDD version 3.7.

[aj] stated by CÆSAR.BDD version 3.7.

[ak] stated by CÆSAR.BDD version 3.7.

[al] stated by CÆSAR.BDD version 3.7.

[am] stated by CÆSAR.BDD version 3.7.

[an] stated by CÆSAR.BDD version 3.7.