Fabrice Kordon
Fabrice.Kordon@lip6.fr

This form is a summary description of the model entitled "BridgeAndVehicles" 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.

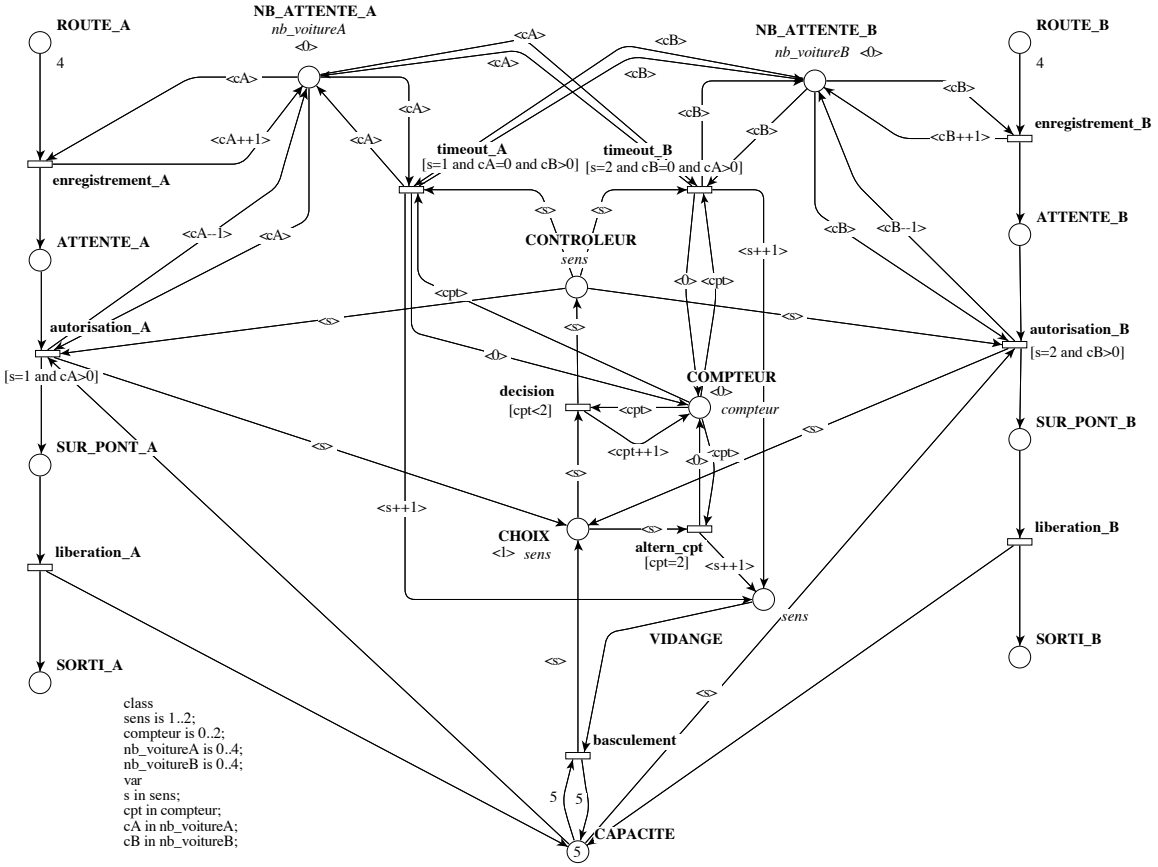
Description

This example is extracted from a formal modeling project that students had to perform at a master (2^{nb}year) at UPMC. The model is in fact the (interesting) answer provided by two students under my supervision (A. Karagiannis and J.-B. Voron in december 2005).

The system is composed of a one-lane automated bridge that automated vehicles must pass. There are two types of automated vehicles: VA_A going in one direction and VA_B going in the other direction.

The bridge has a limited capacity of P vehicles.

The system is supervised by a controller that ensure that at most N vehicles of the same king are passing in a row. Moreover, when the traffic is low, a time out may occurs before N passing vehicles is reached.



Graphical representation for V=4, P=5, N=2

Fabrice Kordon
Fabrice.Kordon@lip6.fr

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
(V, P, N)	V, the number of vehicles in each class (VA_A and VA_B), P, the bridge capacity, and N, the maximum number of vehicles of the same type being allowed to pass the bridge. [(a)].	$(4,5,2)$, $(10,10,10)$, $(20,10,10)$, $(20,10,20)$, $(20,10,50)$, $(20,20,10)$, $(20,20,20)$, $(20,20,50)$, $(50,20,10)$, $(50,20,20)$, $(50,20,50)$, $(50,50,10)$, $(50,50,20)$, $(50,50,50)$, $(80,20,10)$, $(80,20,20)$, $(80,20,50)$, $(80,50,10)$, $(80,50,20)$, $(80,50,50)$

Size of the colored net model

number of places:	15
number of transitions:	11
number of arcs:	57

Size of the derived P/T model instances

Parameter	Number of places	Number of transitions	Number of arcs
V=4, P=5, N=2	28	52	326
V=10, P=10, N=10	48	288	2 090
V=20, P=10, N=10	68	548	4 070
V=20, P=10, N=20	78	968	7 350
V=20, P=10, N=50	108	2228	17 190
V=20, P=20, N=10	68	548	4 070
V=20, P=20, N=20	78	968	7 350
V=20, P=20, N=50	108	2 228	17 190
V=50, P=20, N=10	128	1 328	10 010
V=50, P=20, N=20	138	2 348	18 090
V=50, P=20, N=50	168	5 408	42 330
V=50, P=50, N=10	128	1 328	10 010
V=50, P=50, N=20	138	2 348	18 090
V=50, P=50, N=50	168	5 408	42 330
V=80, P=20, N=10	188	2 108	15 950
V=80, P=20, N=20	198	3 728	28 830
V=80, P=20, N=50	228	8 588	67 470
V=80, P=50, N=10	188	2 108	15 950
V=80, P=50, N=20	198	3 728	28 830
V=80, P=50, N=50	228	8 588	67 470

Structural properties

ordinary — *all arcs have multiplicity one* ..... ✗
simple free choice — *all transitions sharing a common input place have no other input place* ..... ✗ [(b)]
extended free choice — *all transitions sharing a common input place have the same input places* ..... ✗ [(c)]
state machine — *every transition has exactly one input place and exactly one output place* ..... ✗ [(d)]
marked graph — *every place has exactly one input transition and exactly one output transition* ..... ✗ [(e)]
connected — *there is an undirected path between every two nodes (places or transitions)* ..... ✓ [(f)]
strongly connected — *there is a directed path between every two nodes (places or transitions)* ..... ✗ [(g)]

[(a)] These parameters affect some color definition and thus do not impact the size of the model (in the colored version).
[(b)] the net is not ordinary in all its 20 instances (see all aforementioned scaling parameter values).
[(c)] the net is not ordinary in all its 20 instances (see all aforementioned scaling parameter values).
[(d)] the net is not ordinary in all its 20 instances (see all aforementioned scaling parameter values).
[(e)] the net is not ordinary in all its 20 instances (see all aforementioned scaling parameter values).
[(f)] stated by CÆSAR.BDD version 2.3 on all 20 instances (see all aforementioned scaling parameter values).
[(g)] from place "ROUTE_A" one cannot reach place "ROUTE_B".

Fabrice Kordon
Fabrice.Kordon@lip6.fr

source place(s) — *one or more places have no input transitions* ..... ✔ (h)
sink place(s) — *one or more places have no output transitions* ..... ✔ (i)
source transition(s) — *one or more transitions have no input places* ..... ✗ (j)
sink transitions(s) — *one or more transitions have no output places* ..... ✗ (k)
loop-free — *no transition has an input place that is also an output place* ..... ✗ (l)
conservative — *for each transition, the number of input arcs equals the number of output arcs* ..... ✗ (m)
subconservative — *for each transition, the number of input arcs equals or exceeds the number of output arcs* ..... ✗ (n)
nested units — *places are structured into hierarchically nested sequential units* (o) ..... ✗

Behavioural properties

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

(h) there exist 2 source places, e.g., place "ROUTE_A".
(i) there exist 2 sink places, e.g., place "SORTI_A".
(j) stated by CÆSAR.BDD version 2.3 on all 20 instances (see all aforementioned scaling parameter values).
(k) stated by CÆSAR.BDD version 2.3 on all 20 instances (see all aforementioned scaling parameter values).
(l) stated by CÆSAR.BDD version 2.3 on all 20 instances (see all aforementioned scaling parameter values).
(m) stated by PNML2NUPN 3.1.0 on all 20 instances (see all aforementioned scaling parameter values).
(n) stated by PNML2NUPN 3.1.0 on all 20 instances (see all aforementioned scaling parameter values).
(o) the definition of Nested-Unit Petri Nets (NUPN) is available from `http://mcc.lip6.fr/nupn.php`
(p) by construction of the model: the initial marking is not safe; confirmed by CÆSAR.BDD version 2.3 on all 20 instances (see all aforementioned scaling parameter values).
(q) checked by PROD in December 2014. There are several terminal states that correspond to the "end" of the system (all vehicles passed in the other bank).
(r) by construction of the model (see the vehicle modeling).

Fabrice Kordon
Fabrice.Kordon@lip6.fr

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
(V=4, P=5, N=2)	2874 [(s)]	7160 [(t)]	?	$\geq$ 17 [(u)]
(V=10, P=10, N=10)	259 556 [(v)]	821 282 [(w)]	?	$\geq$ 34 [(x)]
(V=20, P=10, N=10)	6 732 570 [(y)]	23 489 216 [(z)]	?	$\geq$ 54 [(aa)]
(V=20, P=10, N=20)	?	?	?	$\geq$ 54 [(ab)]
(V=20, P=10, N=50)	?	?	?	$\geq$ 54 [(ac)]
(V=20, P=20, N=10)	?	?	?	$\geq$ 64 [(ad)]
(V=20, P=20, N=20)	?	?	?	$\geq$ 64 [(ae)]
(V=20, P=20, N=50)	?	?	?	$\geq$ 64 [(af)]
(V=50, P=20, N=10)	?	?	?	$\geq$ 124 [(ag)]
(V=50, P=20, N=20)	?	?	?	$\geq$ 124 [(ah)]
(V=50, P=20, N=50)	?	?	?	$\geq$ 124 [(ai)]
(V=50, P=50, N=10)	?	?	?	$\geq$ 154 [(aj)]
(V=50, P=50, N=20)	?	?	?	$\geq$ 154 [(ak)]
(V=50, P=50, N=50)	?	?	?	$\geq$ 154 [(al)]
(V=80, P=20, N=10)	?	?	?	$\geq$ 184 [(am)]
(V=80, P=20, N=20)	?	?	?	$\geq$ 184 [(an)]
(V=80, P=20, N=50)	?	?	?	$\geq$ 184 [(ao)]
(V=80, P=50, N=10)	?	?	?	$\geq$ 214 [(ap)]
(V=80, P=50, N=20)	?	?	?	$\geq$ 214 [(aq)]
(V=80, P=50, N=50)	?	?	?	$\geq$ 214 [(ar)]

Other properties

On the colored model, we have the following properties ensured:

$$
\begin{array}{lcl}
P_1 & : & \neg\ (|\text{SUR\_PONT\_A}| > 0 \wedge |\text{SUR\_PONT\_B}| > 0) \\
P_2 & : & \text{AG}\ (|\text{ROUTE\_A}| = V \Rightarrow \text{AF}(|\text{SORTIE\_A}| = V) \wedge \\
 & & \quad |\text{ROUTE\_B}| = V \Rightarrow \text{AF}(|\text{SORTIE\_B}| = V))
\end{array}
$$

(s) computed by PROD in December 2014.
(t) computed by PROD in December 2014.
(u) lower bound given by the number of initial tokens.
(v) computed by PROD in December 2014.
(w) computed by PROD in December 2014.
(x) lower bound given by the number of initial tokens.
(y) computed by PROD in December 2014.
(z) computed by PROD in December 2014.
(aa) lower bound given by the number of initial tokens.
(ab) lower bound given by the number of initial tokens.
(ac) lower bound given by the number of initial tokens.
(ad) lower bound given by the number of initial tokens.
(ae) lower bound given by the number of initial tokens.
(af) lower bound given by the number of initial tokens.
(ag) lower bound given by the number of initial tokens.
(ah) lower bound given by the number of initial tokens.
(ai) lower bound given by the number of initial tokens.
(aj) lower bound given by the number of initial tokens.
(ak) lower bound given by the number of initial tokens.
(al) lower bound given by the number of initial tokens.
(am) lower bound given by the number of initial tokens.
(an) lower bound given by the number of initial tokens.
(ao) lower bound given by the number of initial tokens.
(ap) lower bound given by the number of initial tokens.
(aq) lower bound given by the number of initial tokens.
(ar) lower bound given by the number of initial tokens.

Fabrice Kordon
Fabrice.Kordon@lip6.fr

P_1 means that only one type of vehicle can stand on the bridge and P_2 means that all vehicles will eventually reach the other side of the bridge.