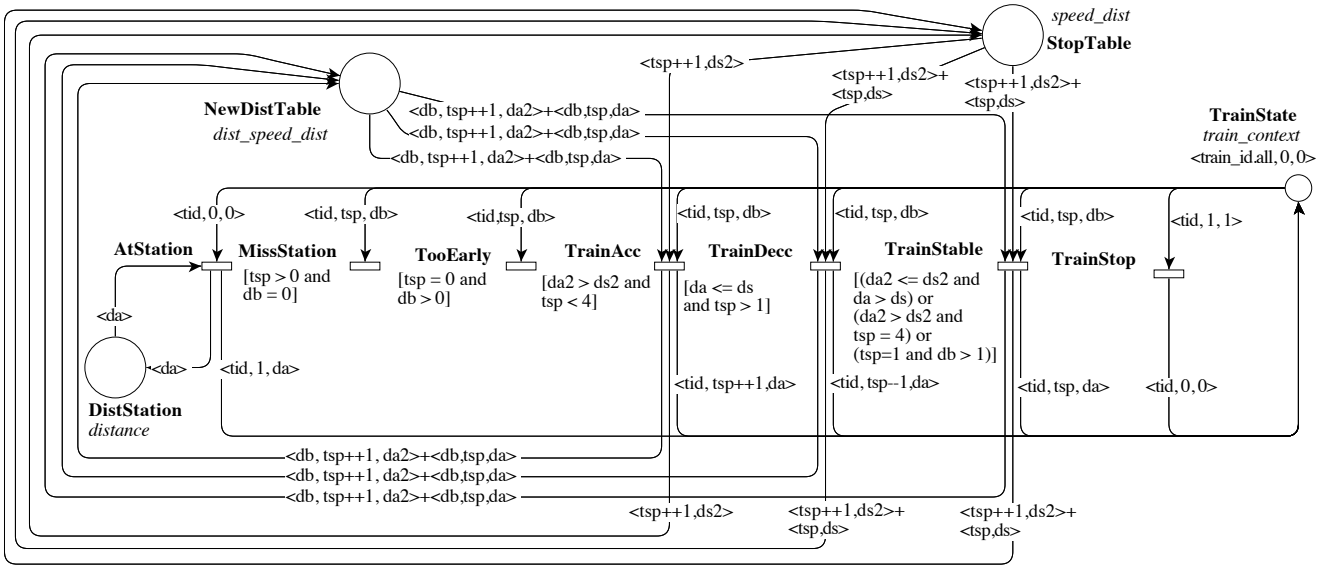
Fabrice Kordon
Fabrice.Kordon@lip6.fr

This form is a summary description of the model entitled "BART" 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 is the model of a speed controller allowing a train (we use the BART description from a case study presented in [**2**]) to reach appropriately a station without missing. To do so, the braking distance according to the current speed of the train is stored in place NewDistTable. This model is parameterized by T, the number of trains running in parallel.



Graphical representation for $T = 2$

References

[1] A. de Groot, J. Hooman, F. Kordon, E. Paviot-Adet, I. Vernier-Mounier, M. Lemoine, G. Gaudiere, V. Winter, and D. Kapur. *A survey: Applying formal methods to a software intensive system.* In 6th IEEE International Symposium on High-Assurance Systems Engineering – HASE, pages 55-64. IEEE Computer Society, 2001.

[2] V. Winter and S. Bhattacharya. *High Integrity Software.* Kluwer Academic Publishers, 2001.

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
T	Number of trains in separate tracks	2, 5, 10, 20, 30, 40, 50, 60

Size of the colored net model

number of places:	4
number of transitions:	7
number of arcs:	26

Fabrice Kordon
Fabrice.Kordon@lip6.fr

Size of the derived P/T model instances

Parameter	Number of places	Number of transitions	Number of arcs
$T = 2$	732	2 282	13 200
$T = 5$	1 427	5 705	33 000
$T = 10$	2 582	11 410	66 000
$T = 20$	4 892	22 820	132 000
$T = 30$	7 202	34 230	198 000
$T = 40$	9 512	45 640	264 000
$T = 50$	11 822	57 050	330 000
$T = 60$	14 132	68 460	396 000

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]
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]
deadlock — *there exists a reachable marking from which no transition can be fired* ..... ✔ [p]
reversible — *from every reachable marking, there is a transition path going back to the initial marking* ..... ✘ [q]
quasi-live — *for every transition t, there exists a reachable marking in which t can fire* ..... ✔ [r]

[a] stated by CÆSAR.BDD version 2.7 on all 8 instances (see all aforementioned parameter values).
[b] stated by CÆSAR.BDD version 2.7 on all 8 instances (see all aforementioned parameter values).
[c] stated by CÆSAR.BDD version 2.7 on all 8 instances (see all aforementioned parameter values).
[d] stated by CÆSAR.BDD version 2.7 on all 8 instances (see all aforementioned parameter values).
[e] 6 places are not connected to place "TrainState_1_0_0", e.g., place "NewDistTable_38_4_34"; notice that the colored nets are connected and disconnected places have been introduced by the unfolding tool, the optimizations of which have been disabled.
[f] the net is not connected and, thus, not strongly connected; notice that the colored nets are strongly connected.
[g] there exist 6 source places, e.g., place "NewDistTable_38_4_34"; notice that the colored nets have no source places.
[h] there exist 6 sink places, e.g., place "NewDistTable_38_4_34"; notice that the colored nets have no sink places.
[i] stated by CÆSAR.BDD version 2.7 on all 8 instances (see all aforementioned parameter values).
[j] stated by CÆSAR.BDD version 2.7 on all 8 instances (see all aforementioned parameter values).
[k] stated by CÆSAR.BDD version 2.7 on all 8 instances (see all aforementioned parameter values).
[l] stated by CÆSAR.BDD version 2.7 on all 8 instances (see all aforementioned parameter values).
[m] stated by CÆSAR.BDD version 2.7 on all 8 instances (see all aforementioned parameter values).
[n] the definition of Nested-Unit Petri Nets (NUPN) is available from http://mcc.lip6.fr/nupn.php
[o] on the P/T equivalent version, there should not be more than one token per place; stated by CÆSAR.BDD version 2.7 to be true on 1 instance(s) out of 8, and unknown on the remaining 7 instance(s).
[p] for some initial markings, transition TooEarly may be fired; stated by CÆSAR.BDD version 2.7 to be true on 1 instance(s) out of 8, and unknown on the remaining 7 instance(s).
[q] stated by CÆSAR.BDD version 2.7 to be false on 1 instance(s) out of 8, and unknown on the remaining 7 instance(s).
[r] stated by CÆSAR.BDD version 2.7 to be true on 1 instance(s) out of 8, and unknown on the remaining 7 instance(s).

Fabrice Kordon
Fabrice.Kordon@lip6.fr

live — *for every transition t, from every reachable marking, one can reach a marking in which t can fire* ..... ✗ [(s)]

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
$T = 2$	53 824 [(t)]	?	1	274 [(u)]
$T = 5$	672 109 330 432 [(v)]	?	?	277 [(w)]
$T = 10$	?	?	?	282 [(x)]
$T = 20$	?	?	?	292 [(y)]
$T = 30$	?	?	?	302 [(z)]
$T = 40$	?	?	?	312 [(aa)]
$T = 50$	?	?	?	322 [(ab)]
$T = 60$	?	?	?	332 [(ac)]

(s) For some initial marking, transition MissStation can be fired; stated by CÆSAR.BDD version 2.7 to be false on 1 instance(s) out of 8, and unknown on the remaining 7 instance(s).
(t) stated by prod in May 2017; confirmed by CÆSAR.BDD version 2.7.
(u) number of initial tokens, because the net is sub-conservative.
(v) stated by ITS-Tools in May 2017.
(w) number of initial tokens, because the net is sub-conservative.
(x) number of initial tokens, because the net is sub-conservative.
(y) number of initial tokens, because the net is sub-conservative.
(z) number of initial tokens, because the net is sub-conservative.
(aa) number of initial tokens, because the net is sub-conservative.
(ab) number of initial tokens, because the net is sub-conservative.
(ac) number of initial tokens, because the net is sub-conservative.