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.

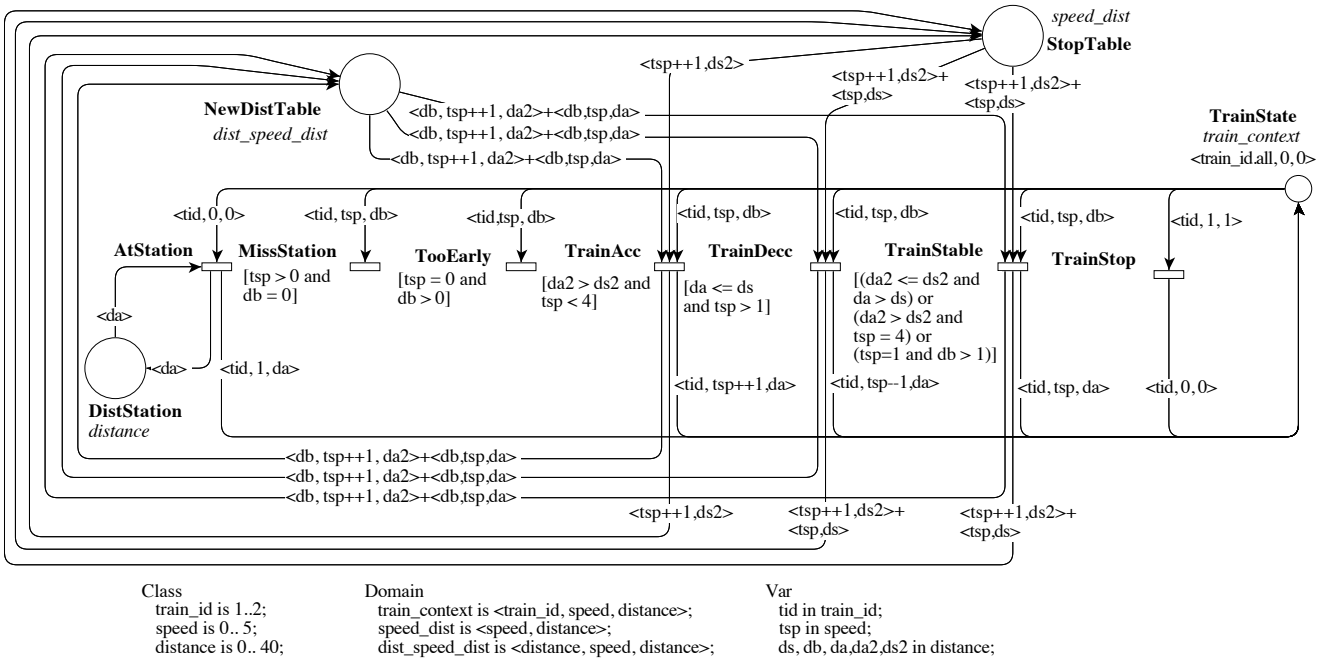
Description

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.

This model is given in two forms: a colored net and a P/T net. Both forms are not necessarily equivalent for the following reason: the P/T net was produced by unfolding the colored BART model; unfortunately, this P/T was far too large (due to the discretization of acceleration and braking functions); so, the P/T was simplified aggressively by deleting places and transitions, many of which were dead (i.e., 0-bounded or unfirable).

The P/T instances of this model have been modified for the 2018 edition of the MCC and are no longer equivalent to the corresponding colored instances.

In March 2020, Pierre Bouvier and Hubert Garavel provided a decomposition of all instances of this model into networks of communicating automata. Each network is expressed as a Nested-Unit Petri Net (NUPN) that can be found, for each instance, in the "toolspecific" section of the corresponding PNML file.



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.

Fabrice Kordon
Fabrice.Kordon@lip6.fr

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

Size of the derived P/T model instances

Parameter	Number of places	Number of transitions	Number of arcs	Number of units	HWB code
$T = 2$	474	404	3240	213	1–212–16
$T = 5$	870	1010	8100	216	1–215–40
$T = 10$	1530	2020	16200	222	1–221–81
$T = 20$	2850	4040	32400	423	1–422–468
$T = 30$	4170	6060	48600	624	1–623–855
$T = 40$	5490	8080	64800	825	1–824–1242
$T = 50$	6810	10100	81000	1026	1–1025–1629
$T = 60$	8130	12120	97200	1227	1–1226–2016

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] ..... ✔

[a] stated by CÆSAR.BDD version 3.3 on all 8 instances (see all aforementioned parameter values).
[b] transitions "AtStation_1_5" and "AtStation_1_6" share a common input place "TrainState_1_0_0", but only the former transition has input place "DistStation_5".
[c] stated by CÆSAR.BDD version 3.3 on all 8 instances (see all aforementioned parameter values).
[d] stated by CÆSAR.BDD version 3.3 on all 8 instances (see all aforementioned parameter values).
[e] stated by CÆSAR.BDD version 3.3 on all 8 instances (see all aforementioned parameter values).
[f] stated by CÆSAR.BDD version 3.3 on all 8 instances (see all aforementioned parameter values).
[g] stated by CÆSAR.BDD version 3.3 on all 8 instances (see all aforementioned parameter values).
[h] stated by CÆSAR.BDD version 3.3 on all 8 instances (see all aforementioned parameter values).
[i] stated by CÆSAR.BDD version 3.3 on all 8 instances (see all aforementioned parameter values).
[j] stated by CÆSAR.BDD version 3.3 on all 8 instances (see all aforementioned parameter values).
[k] stated by CÆSAR.BDD version 3.3 on all 8 instances (see all aforementioned parameter values).
[l] stated by CÆSAR.BDD version 3.3 on all 8 instances (see all aforementioned parameter values).
[m] stated by CÆSAR.BDD version 3.3 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

Fabrice Kordon
Fabrice.Kordon@lip6.fr

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* ..... ?
live — *for every transition t, from every reachable marking, one can reach a marking in which t can fire* ..... ?

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
$T = 2$	17 424 [s]	53 328 [t]	1	212 [u]
$T = 5$	40 074 642 432 [v]	?	1 [w]	215 [x]
$T = 10$	1.60598e+21 [y]	?	1	220 [z]
$T = 20$	2.57916e+42 [aa]	?	1	230 [ab]
$T = 30$	$\geq$ 4.14207e+63 [ac]	?	1 [ad]	240 [ae]
$T = 40$	$\geq$ 4.9074e+84 [af]	?	1 [ag]	250 [ah]
$T = 50$	1.06831e+106 [ai]	?	1 [aj]	260 [ak]
$T = 60$	?	?	1 [al]	270 [am]

[o] on the P/T equivalent version, there should not be more than one token per place; stated by CÆSAR.BDD version 3.3 to be true on all 8 instances (see all aforementioned parameter values).
[p] stated by CÆSAR.BDD version 3.3 to be false on 5 instance(s) out of 8, and unknown on the remaining 3 instance(s).
[q] stated by CÆSAR.BDD version 3.3 to be false on 5 instance(s) out of 8, and unknown on the remaining 3 instance(s).
[r] computed by PROD on April 2018; stated by CÆSAR.BDD version 3.3 to be false on 4 instance(s) out of 8, and unknown on the remaining 4 instance(s).
[s] stated by CÆSAR.BDD version 3.3 and by PROD in April 2018.
[t] stated by PROD in April 2018.
[u] number of initial tokens, because the net is sub-conservative.
[v] stated by ITS-Tools in April 2018.
[w] stated by ITS-Tools in April 2018.
[x] number of initial tokens, because the net is sub-conservative.
[y] stated by CÆSAR.BDD version 3.3.
[z] number of initial tokens, because the net is conservative.
[aa] stated by CÆSAR.BDD version 3.3.
[ab] number of initial tokens, because the net is conservative.
[ac] stated by CÆSAR.BDD version 3.3.
[ad] stated by CÆSAR.BDD version 3.3.
[ae] number of initial tokens, because the net is conservative.
[af] stated by CÆSAR.BDD version 3.3.
[ag] stated by CÆSAR.BDD version 3.3.
[ah] number of initial tokens, because the net is conservative.
[ai] stated by CÆSAR.BDD version 3.3.
[aj] stated by CÆSAR.BDD version 3.3.
[ak] number of initial tokens, because the net is conservative.
[al] stated by CÆSAR.BDD version 3.3.
[am] number of initial tokens, because the net is conservative.