Fabrice Kordon
Fabrice.Kordon@lip6.fr

This form is a summary description of the model entitled "SmallOperatingSystem" 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

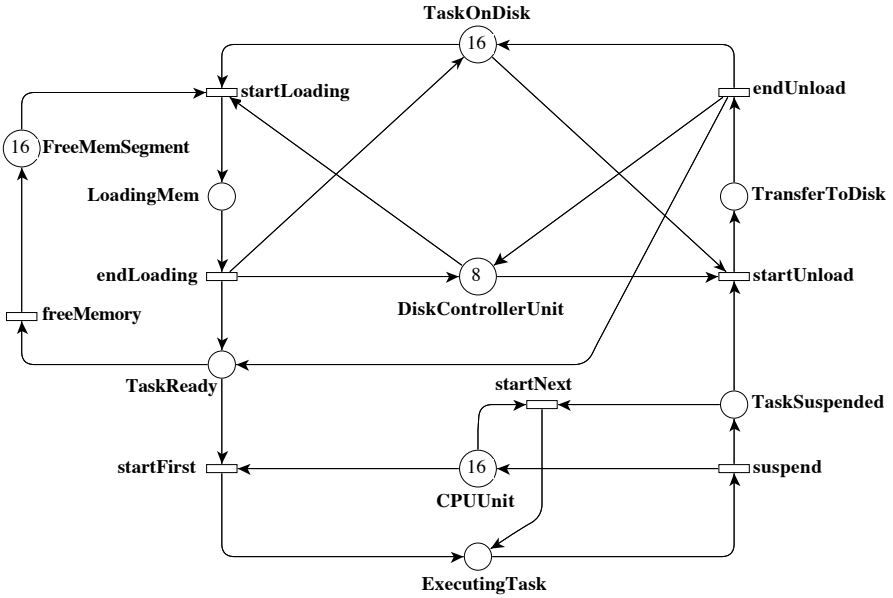
This Petri net models a simplified Operating System handling the execution of tasks on a machine with several so-called "memory segments", Disk controller units, and cores. The typical lifecycle of a task is the following:

1 A ask is loaded from disk to memory (requires a segment and a disk controller),

2 When the task is ready to execute, it can get a core, be suspended and get a core again as long as its execution is not finished. It can also be removed from the memory if some is needed otherwise

3 When the execution finishes, the task is saved back on the disk.

The system has several scaling parameters: M (memory segments), T (tasks), D (Disk controllers) and C (cores). However, to simplify this in the MCC, we reduce it to two parameters, MT and DC with the following correspondence: $M = T = MT$, $D = DC$ and $C = 2 \times DC$.



Graphical representation for $MT16$ and $DC = 8$

Fabrice Kordon
Fabrice.Kordon@lip6.fr

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
MT and *DC*	*MT* to compute available tasks and memory and *DC* to compute available disk controllers and cores	(MT=16, DC=8), (MT=32, DC=8), (MT=32, DC=16), (MT=64, DC=16), (MT=64, DC=32), (MT=128, DC=32), (MT=128, DC=64), (MT=256, DC=64), (MT=256, DC=128), (MT=512, DC=128), (MT=512, DC=256), (MT=1024, DC=256), (MT=1024, DC=512), (MT=2048, DC=512), (MT=2048, DC=1024), (MT=4096, DC=1024), (MT=4096, DC=2048), (MT=8192, DC=2048), (MT=8192, DC=4096)

Size of the model

Although the model is parameterized, its size does not depend on parameter values.

number of places:	9
number of transitions:	8
number of arcs:	27

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] 9 arcs are not simple free choice, e.g., the arc from place "TaskOnDisk" (which has 2 outgoing transitions) to transition "startLoading" (which has 3 input places).
[b] transitions "startLoading" and "startUnload" share a common input place "TaskOnDisk", but only the former transition has input place "FreeMemSegment".
[c] 7 transitions are not of a state machine, e.g., transition "startLoading".
[d] 6 places are not of a marked graph, e.g., place "TaskOnDisk".
[e] stated by CÆSAR.BDD version 2.6 on all 19 instances ((MT=16, DC=8), (MT=32, DC=8), etc.).
[f] stated by CÆSAR.BDD version 2.6 on all 19 instances ((MT=16, DC=8), (MT=32, DC=8), etc.).
[g] stated by CÆSAR.BDD version 2.6 on all 19 instances ((MT=16, DC=8), (MT=32, DC=8), etc.).
[h] stated by CÆSAR.BDD version 2.6 on all 19 instances ((MT=16, DC=8), (MT=32, DC=8), etc.).
[i] stated by CÆSAR.BDD version 2.6 on all 19 instances ((MT=16, DC=8), (MT=32, DC=8), etc.).
[j] stated by CÆSAR.BDD version 2.6 on all 19 instances ((MT=16, DC=8), (MT=32, DC=8), etc.).
[k] stated by CÆSAR.BDD version 2.6 on all 19 instances ((MT=16, DC=8), (MT=32, DC=8), etc.).
[l] 7 transitions are not conservative, e.g., transition "startLoading".
[m] 3 transitions are not subconservative, e.g., transition "endLoading".
[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]
deadlock — *there exists a reachable marking from which no transition can be fired* ..... ✗
reversible — *from every reachable marking, there is a transition path going back to the initial marking* ..... ✓
quasi-live — *for every transition t, there exists a reachable marking in which t can fire* ..... ✓ [p]
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
MT=16, DC=8	16 587 [q]	100 896 [r]	?	≥ 56 [s]
MT=32, DC=8	166 515 [t]	1 112 454 [u]	?	≥ 88 [v]
MT=32, DC=16	354 501 [w]	2 451 264 [x]	?	≥ 112 [y]
MT=64, DC=16	7 245 654 [z]	29 675 132 [aa]	?	≥ 176 [ab]
MT=64, DC=32	9 133 641 [ac]	67 762 816 [ad]	?	≥ 224 [ae]
MT=128, DC=32	?	?	?	≥ 352 [af]
MT=128, DC=64	?	?	?	≥ 448 [ag]
MT=256, DC=64	?	?	?	≥ 704 [ah]
MT=256, DC=128	?	?	?	≥ 896 [ai]
MT=512, DC=128	?	?	?	≥ 1408 [aj]
MT=512, DC=256	?	?	?	≥ 1792 [ak]
MT=1024, DC=256	?	?	?	≥ 2816 [al]
MT=1024, DC=512	?	?	?	≥ 3584 [am]
MT=2048, DC=512	?	?	?	≥ 5632 [an]
MT=2048, DC=1024	?	?	?	≥ 7168 [ao]
MT=4096, DC=1024	?	?	?	≥ 11264 [ap]
MT=4096, DC=2048	?	?	?	≥ 14336 [aq]
MT=8192, DC=2048	?	?	?	≥ 22528 [ar]
MT=8192, DC=4096	?	?	?	≥ 28672 [as]

[o] by construction of the model (the initial marking is not safe); confirmed by CÆSAR.BDD version 2.6 on all 19 instances ((MT=16, DC=8), (MT=32, DC=8), etc.).
[p] stated by CÆSAR.BDD version 2.6 on all 19 instances ((MT=16, DC=8), (MT=32, DC=8), etc.).
[q] computed by PROD in March 2015.
[r] computed by PROD in March 2015.
[s] lower bound given by the number of initial tokens.
[t] computed by PROD in March 2015.
[u] computed by PROD in March 2015.
[v] lower bound given by the number of initial tokens.
[w] computed by PROD in March 2015.
[x] computed by PROD in March 2015.
[y] lower bound given by the number of initial tokens.
[z] computed by PROD in March 2015.
[aa] computed by PROD in March 2015.
[ab] lower bound given by the number of initial tokens.
[ac] computed by PROD in March 2015.
[ad] computed by PROD in March 2015.
[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.

Fabrice Kordon
Fabrice.Kordon@lip6.fr

(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.
(as) lower bound given by the number of initial tokens.