Fabrice Kordon
Fabrice.Kordon@lip6.fr

*This form is a summary description of the model entitled "PolyORBLF" 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

**PolyORB** is a middleware that was jointly developped at Telecom ParisTech and Université P. & M. Curie (LIP6) between 2000 and 2006. Its main characteristics is to be "schyzophrenic", that means it is able to support various protocols simultaneously. **PolyORB** was a research tool to investigate interoperability between several distribution models (message oriented, distributed objetcs, etc.). It was also experimented to elaborate high-critical dexecution infrastructure for distributed systems. Thus, to ensure reliability, some aspects of this middelware where architectured together with a formal modeling for verification purpose (see reference). This model describes one of the **PolyORB** implementation that was proved to be deadlock-free as well as starvation-free.

This model implements the multitasking implementation of **PolyORB** following a *Leader/Followers* policy (see reference 18 in the paper referenced below). Unfortunately, due to some loss of data during a disk crash, this model is not the final version of the work.

*The colored-net instances of this model have been patched in March 2015 because they contained mistakes that have been detected and reported by Yann Thierry-Mieg; in particular, these mistakes led to diverging sizes for the state space (and thus for any formula). The P/T-net instances have been kept unchanged.*

## References

The first reference presents the formal modeling of **PolyORB** while se second one is a link to its current distribution (this middelware is now supported by AdaCore).


- J. Hugues, Y. Thierry-Mieg, F. Kordon, L. Pautet, S. Baarir, and T. Vergnaud. On the Formal Verification of Middleware Behavioral Properties. *9th International Workshop on Formal Methods for Industrial Critical Systems (FMICS)*, Electornic Notes in Theoretical Computer Science (vol 133), pages 139-157, Elsevier, September 2004,
- http://www.adacore.com/polyorb.


## Scaling parameter

| Parameter name | Parameter description | Chosen parameter values |
|---|---|---|
| $(S, J, T)$ | $S$, the maximum number of sources, $J$, the maximum number of simultaneous jobs, and $T$, the number of threads allocated to the $\mu$Broker [(a)]. | $(S = 2, J = 4, T = 6)$, $(S = 2, J = 4, T = 8)$, $(S = 2, J = 4, T = 10)$, $(S = 2, J = 6, T = 6)$, $(S = 2, J = 6, T = 8)$, $(S = 2, J = 6, T = 10)$, $(S = 4, J = 4, T = 6)$, $(S = 4, J = 4, T = 8)$, $(S = 4, J = 4, T = 10)$, $(S = 4, J = 6, T = 6)$, $(S = 4, J = 6, T = 8)$, $(S = 4, J = 6, T = 10)$, $(S = 6, J = 4, T = 4)$, $(S = 6, J = 4, T = 6)$, $(S = 6, J = 4, T = 8)$, $(S = 6, J = 6, T = 4)$, $(S = 6, J = 6, T = 6)$, $(S = 6, J = 6, T = 8)$ |

## Size of the colored net model

| | |
|---|---|
| number of places: | 81 |
| number of transitions: | 65 |
| number of arcs: | 258 |

[(a)] These parameters affect some color definition and thus do not impact the size of the model (in the colored version).

Fabrice Kordon
Fabrice.Kordon@lip6.fr

## Size of the derived P/T model instances

| Parameter | Number of places | Number of transitions | Number of arcs |
|---|---|---|---|
| $(S = 2, J = 4, T = 6)$ | 476 | 920 | 4242 |
| $(S = 2, J = 4, T = 8)$ | 614 | 1242 | 5732 |
| $(S = 2, J = 4, T = 10)$ | 752 | 1572 | 7262 |
| $(S = 2, J = 6, T = 6)$ | 536 | 1064 | 4866 |
| $(S = 2, J = 6, T = 8)$ | 690 | 1434 | 6564 |
| $(S = 2, J = 6, T = 10)$ | 844 | 1812 | 8302 |
| $(S = 4, J = 4, T = 6)$ | 554 | 2998 | 20754 |
| $(S = 4, J = 4, T = 8)$ | 712 | 4012 | 27744 |
| $(S = 4, J = 4, T = 10)$ | 870 | 5034 | 34774 |
| $(S = 4, J = 6, T = 6)$ | 618 | 3190 | 21570 |
| $(S = 4, J = 6, T = 8)$ | 792 | 4268 | 28832 |
| $(S = 4, J = 6, T = 10)$ | 966 | 5354 | 36134 |
| $(S = 6, J = 4, T = 4)$ | 454 | 6994 | 59152 |
| $(S = 6, J = 4, T = 6)$ | 632 | 10500 | 88770 |
| $(S = 6, J = 4, T = 8)$ | 810 | 14014 | 118428 |
| $(S = 6, J = 6, T = 4)$ | 506 | 7154 | 59824 |
| $(S = 6, J = 6, T = 6)$ | 700 | 10740 | 89778 |
| $(S = 6, J = 6, T = 8)$ | 894 | 14334 | 119772 |

## Structural properties

**ordinary** — *all arcs have multiplicity one* ..... ✗
**simple free choice** — *all (different) transitions with a shared input place have no other input place* ..... ✗ (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) ..... ✗

(b) stated by CÆSAR.BDD version 2.0 on all 18 instances (see all aforementioned scaling parameter values).
(c) stated by CÆSAR.BDD version 2.0 on all 18 instances (see all aforementioned scaling parameter values).
(d) stated by CÆSAR.BDD version 2.0 on all 18 instances (see all aforementioned scaling parameter values).
(e) stated by CÆSAR.BDD version 2.0 on all 18 instances (see all aforementioned scaling parameter values).
(f) stated by CÆSAR.BDD version 2.0 on all 18 instances (see all aforementioned scaling parameter values).
(g) stated by CÆSAR.BDD version 2.0 on all 18 instances (see all aforementioned scaling parameter values).
(h) stated by CÆSAR.BDD version 2.0 on all 18 instances (see all aforementioned scaling parameter values).
(i) stated by CÆSAR.BDD version 2.0 on all 18 instances (see all aforementioned scaling parameter values).
(j) stated by CÆSAR.BDD version 2.0 on all 18 instances (see all aforementioned scaling parameter values).
(k) stated by CÆSAR.BDD version 2.0 on all 18 instances (see all aforementioned scaling parameter values).
(l) stated by PNML2NUPN 1.3.0 on all 18 instances (see all aforementioned scaling parameter values).
(m) stated by PNML2NUPN 1.3.0 on all 18 instances (see all aforementioned scaling 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]
**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* ..... ?
**quasi-live** — *for every transition t, there exists a reachable marking in which t can fire* ..... ?
**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 |
|---|---|---|---|---|
| $(S=2, J=4, T=6)$ | $1.408 \times 10^{8}$ [q] | ? | ? | $\geq 58$ [r] |
| $(S=2, J=4, T=8)$ | $3.532 \times 10^{9}$ [s] | ? | ? | $\geq 62$ |
| $(S=2, J=4, T=10)$ | $8.246 \times 10^{10}$ [t] | ? | ? | $\geq 66$ |
| $(S=2, J=6, T=6)$ | $2.550 \times 10^{8}$ [u] | ? | ? | $\geq 60$ |
| $(S=2, J=6, T=8)$ | $6.219 \times 10^{9}$ [v] | ? | ? | $\geq 64$ |
| $(S=2, J=6, T=10)$ | $1.414 \times 10^{11}$ [w] | ? | ? | $\geq 68$ |
| $(S=4, J=4, T=6)$ | ? | ? | ? | $\geq 62$ |
| $(S=4, J=4, T=8)$ | ? | ? | ? | $\geq 66$ |
| $(S=4, J=4, T=10)$ | ? | ? | ? | $\geq 70$ |
| $(S=4, J=6, T=6)$ | ? | ? | ? | $\geq 64$ |
| $(S=4, J=6, T=8)$ | ? | ? | ? | $\geq 68$ |
| $(S=4, J=6, T=10)$ | ? | ? | ? | $\geq 72$ |
| $(S=6, J=4, T=4)$ | ? | ? | ? | $\geq 62$ |
| $(S=6, J=4, T=6)$ | ? | ? | ? | $\geq 66$ |
| $(S=6, J=4, T=8)$ | ? | ? | ? | $\geq 70$ |
| $(S=6, J=6, T=4)$ | ? | ? | ? | $\geq 64$ |
| $(S=6, J=6, T=6)$ | ? | ? | ? | $\geq 68$ |
| $(S=6, J=6, T=8)$ | ? | ? | ? | $\geq 72$ |

[o] in the initial marking, there exist 3 places containing between 9 and 10 tokens.
[p] checked by GreatSPN on December 2013; confirmed at MCC'2014 by GreatSPN, Lola, and Tapaal on all P/T instances. Presence of deadlocks is "normal" because the model is not the last version described in the referenced paper.
[q] computed with GreatSPN on December 2013, this is actually an estimation from the symbolic reachability graph.
[r] lower bound given by the number of initial tokens.
[s] computed with GreatSPN on December 2013, this is actually an estimation from the symbolic reachability graph.
[t] computed with GreatSPN on December 2013, this is actually an estimation from the symbolic reachability graph.
[u] computed with GreatSPN on December 2013, this is actually an estimation from the symbolic reachability graph.
[v] computed with GreatSPN on December 2013, this is actually an estimation from the symbolic reachability graph.
[w] computed with GreatSPN on December 2013, this is actually an estimation from the symbolic reachability graph.