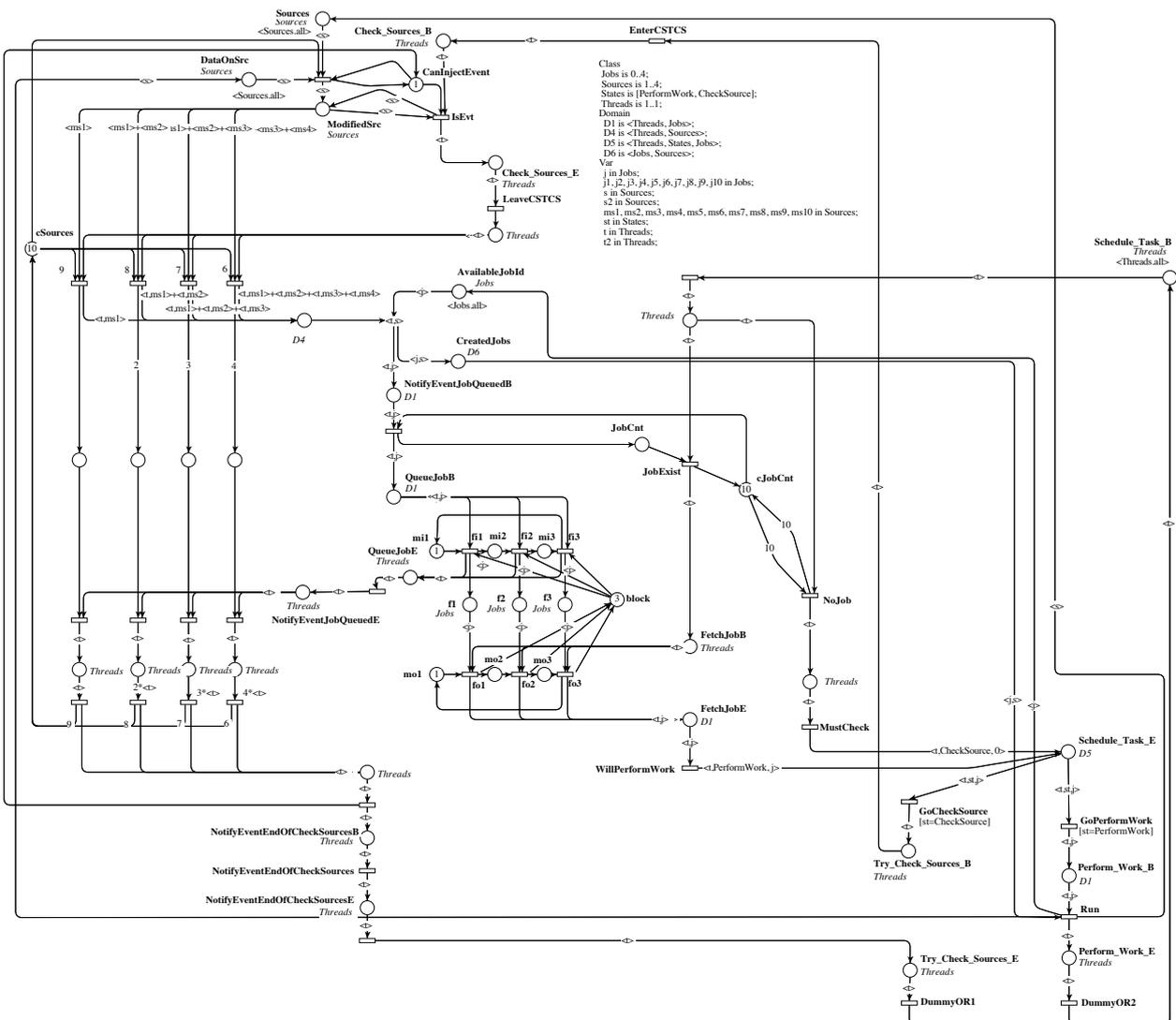


This form is a summary description of the model entitled "PolyORBNT" proposed for the Model Checking Contest @ Petri Nets. Models can be given in several instances parameterized by scaling parameters. Colored nets can be accompanied by one or many equivalent, unfolded P/T nets. Models are given together 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 developed at Telecom ParisTech and Université P. & M. Curie (LIP6) between 2000 and 2006. Its main characteristics is to be "schizophrenic", 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 objects, etc.). It was also experimented to elaborate high-critical dexecution infrastructure for distributed systems. Thus, to ensure reliability, some aspects of this middleware where architected together with a formal modeling for verification purpose (see referenced paper). This model describes one of the **PolyORB** implementation that was proved to be deadlock-free as well as starvation-free.

This model implements a core component of **PolyORB** where all the concurrency is dealt with: the  $\mu$ Broker. It represents its monotasking implementation. Unfortunately, due to some loss of data during a disk crash, this model is not the final version of the work.



Model of PolyORB's  $\mu$ Broker in its monotasking implementation

## References

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

- J. Hugues, Y. Thierry-Mieg, F. Kordon, L. Pautet, S. Baair, and T. Vergnaud. On the Formal Verification of Middleware Behavioral Properties. *9th International Workshop on Formal Methods for Industrial Critical Systems (FMICS)*, Electronic 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
$(J, S)$	$S$ , the maximum number of sources, and $J$ , the maximum number of simultaneous jobs <sup>(a)</sup> .	$((S = 05, J = 20)), ((S = 10, J = 20)), ((S = 05, J = 30)), ((S = 10, J = 30)), ((S = 05, J = 40)), ((S = 10, J = 40)), ((S = 05, J = 60)), ((S = 10, J = 60)), ((S = 05, J = 80)), ((S = 10, J = 80))$

## Size of the colored net model

number of places: 48  
 number of transitions: 38  
 number of arcs: 140

## Size of the derived P/T model instances

Parameter	Number of places	Number of transitions	Number of arcs
$(S = 5, J = 20)$	349	1210	8824
$(S = 5, J = 30)$	489	1400	9764
$(S = 5, J = 40)$	629	1590	10704
$(S = 5, J = 60)$	909	1970	12584
$(S = 5, J = 80)$	1189	2350	14464
$(S = 10, J = 20)$	474	11760	111119
$(S = 10, J = 30)$	664	12050	112559
$(S = 10, J = 40)$	854	12340	113999
$(S = 10, J = 60)$	1234	12920	116879
$(S = 10, J = 80)$	1614	13500	119759

## Structural properties

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

<sup>(a)</sup> These parameters affect some color definition and thus do not impact the size of the model (in the colored version).

<sup>(b)</sup> see transitions  $\mathbf{fi} < i >$  – the net is not ordinary in all its 10 instances (see all aforementioned scaling parameter values).

<sup>(c)</sup> the net is not ordinary in all its 10 instances (see all aforementioned scaling parameter values).

<sup>(d)</sup> see transition  $\mathbf{f3}$  – the net is not ordinary in all its 10 instances (see all aforementioned scaling parameter values).

<sup>(e)</sup> see place **block** – the net is not ordinary in all its 10 instances (see all aforementioned scaling parameter values).

<sup>(f)</sup> stated by **CÆSAR.BDD** version 2.0 on all 10 instances (see all aforementioned scaling parameter values).

<sup>(g)</sup> stated by **CÆSAR.BDD** version 2.0 on all 10 instances (see all aforementioned scaling parameter values).

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

## Behavioural properties

safe — in every reachable marking, there is no more than one token on a place ..... no <sup>(p)</sup>  
 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 ..... yes <sup>(q)</sup>  
 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
$(S = 5, J = 20)$	$6.766 \times 10^8$ <sup>(r)</sup>	?	?	$\geq 58$ <sup>(s)</sup>
$(S = 5, J = 30)$	$3.439 \times 10^9$ <sup>(t)</sup>	?	?	$\geq 68$
$(S = 5, J = 40)$	?	?	?	$\geq 78$
$(S = 5, J = 60)$	?	?	?	$\geq 98$
$(S = 5, J = 80)$	?	?	?	$\geq 118$
$(S = 10, J = 20)$	$3.397 \times 10^{10}$ <sup>(u)</sup>	?	?	$\geq 68$
$(S = 10, J = 30)$	$1.631 \times 10^{11}$ <sup>(v)</sup>	?	?	$\geq 78$
$(S = 10, J = 40)$	?	?	?	$\geq 88$
$(S = 10, J = 60)$	?	?	?	$\geq 108$
$(S = 10, J = 80)$	?	?	?	$\geq 128$

<sup>(h)</sup> stated by [CÆSAR.BDD](#) version 2.0 on all 10 instances (see all aforementioned scaling parameter values).  
<sup>(i)</sup> stated by [CÆSAR.BDD](#) version 2.0 on all 10 instances (see all aforementioned scaling parameter values).  
<sup>(j)</sup> stated by [CÆSAR.BDD](#) version 2.0 on all 10 instances (see all aforementioned scaling parameter values).  
<sup>(k)</sup> stated by [CÆSAR.BDD](#) version 2.0 on all 10 instances (see all aforementioned scaling parameter values).  
<sup>(l)</sup> see transition **NoJob** – confirmed by [CÆSAR.BDD](#) version 2.0 on all 10 instances (see all aforementioned scaling parameter values).  
<sup>(m)</sup> see transition **IsEvt** – confirmed by [PNML2NUPN](#) 1.3.0 on all 10 instances (see all aforementioned scaling parameter values).  
<sup>(n)</sup> see the transition in input of place **NotifyEventEndOfCheckSourcesB** – confirmed by [PNML2NUPN](#) 1.3.0 on all 10 instances (see all aforementioned scaling parameter values).  
<sup>(o)</sup> the definition of Nested-Unit Petri Nets (NUPN) is available from <http://mcc.lip6.fr/nupn.php>  
<sup>(p)</sup> in the initial marking, there exist 3 places containing between 3 and 10 tokens.  
<sup>(q)</sup> checked by GreatSPN on December 2013; confirmed at MCC'2014 by Helena on all 10 colored instances, and by GreatSPN and Lola on all 10 P/T instances. Presence of deadlock is “normal” because the model is not the last version described in the referenced paper.  
<sup>(r)</sup> computed with GreatSPN on December 2013, this is actually an estimation from the symbolic reachability graph.  
<sup>(s)</sup> lower bound given by the number of initial tokens.  
<sup>(t)</sup> computed with GreatSPN on December 2013, this is actually an estimation from the symbolic reachability graph.  
<sup>(u)</sup> computed with GreatSPN on December 2013, this is actually an estimation from the symbolic reachability graph.  
<sup>(v)</sup> computed with GreatSPN on December 2013, this is actually an estimation from the symbolic reachability graph.