Silvano Dal Zilio
dalzilio@laas.fr

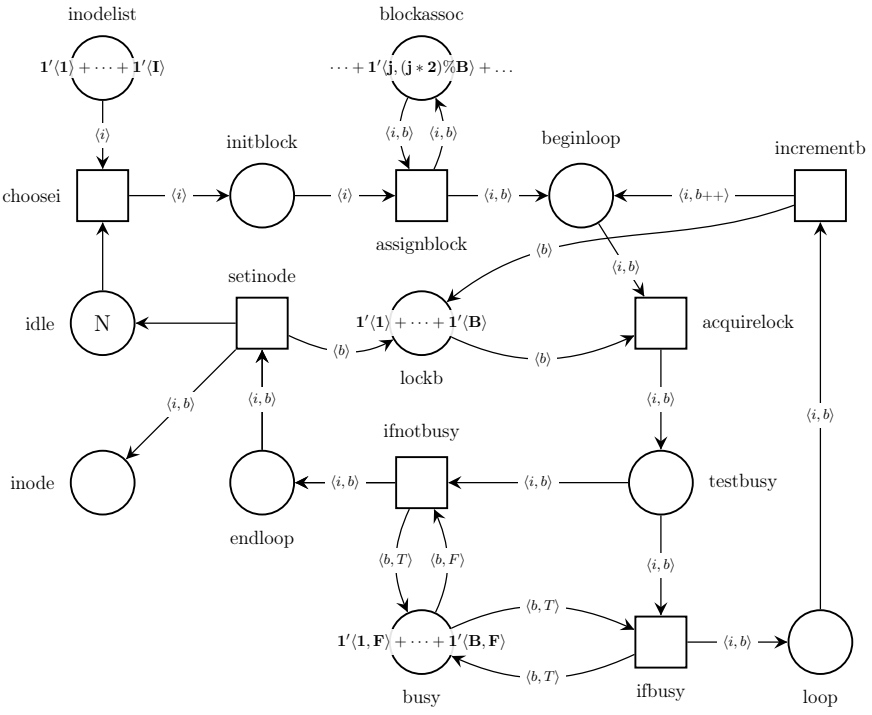
This form is a summary description of the model entitled "FileSystem" proposed for the Model Checking Contest @ Petri Nets. Models can be given in several instances parameterized by scaling parameters. Colored nets can be accompanied by one or many equivalent, unfolded P/T nets. Models are given together with property files (possibly, one per model instance) giving a set of properties to be checked on the model.

Description

We give a symmetric net interpretation of a synchronization idiom found in the Frangipani distributed file system [3]. This example has been proposed as a benchmark for dynamic partial-order methods [1,2].

We model the behaviour of a multi-threaded file server, with N threads, each executing the same program (as shown at the right of the figure below). The goal is to physically allocate a set of I files into a disk containing B distinct blocks. We assume that the data of each file occupies exactly one block. The server keeps a data structure, called an inode, that associate each file descriptor ($i \in 1..I$) with a pointer to a disk block ($b \in 1..B$). Each disk block b has a busy bit, busy[b], indicating whether the block has already been allocated. Since the file system is multi-threaded, this data structure is guarded by mutual exclusive locks, with lockb[b] protecting access to the busy bit busy[b].

The code for each thread starts by selecting an unallocated file descriptor, i. To reduce lock contention, the first block address that is being tested depends on the value of i, using the formula $b := (i * 2) \,\%\, B$. Then the thread searches for a free block to allocate to that inode, incrementally. In our version of this system, once the thread completes its task, it can start again with a new inode.




```
i := choose(1...I);
b := (i*2) % B;
while (true) {
   acquire(lockb[b]);
   if (busy[b] == F) {
      busy[b] := T;
      inode[i] := b;
      release(lockb[b]);
      exit();
   }
   release(lockb[b]);
   b := (b+1) % B;
}
```

Graphical representation of model FileSystem-COL (left) and pseudocode for the associated program (right).

References

1. Cormac Flanagan, Patrice Godefroid (2005). *Dynamic partial-order reduction for model checking software.* ACM Sigplan Notices 40, no. 1.

2. Frédéric Herbreteau, Sarah Larroze-Jardiné, Gérald Point, Igor Walukiewicz (2024). *Revisiting Stateful Partial-Order Reduction.* CoRR abs/2411.16921.

Silvano Dal Zilio
dalzilio@laas.fr

3. Chandramohan Thekkath, Timothy Mann, and Edward K. Lee (1997). *Frangipani: A scalable distributed file system.* In Proceedings of the sixteenth ACM Symposium on Operating Systems Principles.

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
(N,I,B)	N is the number of concurrent threads, I the number of inodes, and B the number of available blocks.	(2,5,5), (2,10,8), (2,10,10), (2,15,15), (3,10,8), (3,10,10), (3,10,15), (5,10,10), (5,10,15), (8,32,26)

Size of the colored net model

number of places: 11
number of transitions: 7
number of arcs: 25

Size of the derived P/T model instances

Parameter	Number of places	Number of transitions	Number of arcs
N=2,I=5,B=5	156	135	475
N=2,I=10,B=8	455	420	1 490
N=2,I=10,B=10	561	520	1 850
N=2,I=15,B=15	1 216	1 155	4 125
N=3,I=10,B=8	455	420	1 490
N=3,I=10,B=10	561	520	1 850
N=3,I=10,B=15	826	770	2 750
N=5,I=10,B=10	561	520	1 850
N=5,I=10,B=15	826	770	2 750
N=8,I=32,B=26	4 335	4 224	15 136

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]

[a] stated by CÆSAR.BDD version 3.5 on all 10 instances.
[b] stated by CÆSAR.BDD version 3.5 on all 10 instances.
[c] transition *choosei*, for instance, has two input places.
[d] place *lockb*, for instance, has two input transitions.
[e] while the colored model is connected, some places originating from the unfolding of *blockassoc* can be isolated.
[f] the net is not connected and, thus, not strongly connected.
[g] one example are places originating from the unfolding of *inodelist*.
[h] one example are places originating from the unfolding of *inode*.
[i] stated by CÆSAR.BDD version 3.5 on all 10 instances.
[j] stated by CÆSAR.BDD version 3.5 on all 10 instances.
[k] one example is given by transitions originating form *ifbusy*.

Silvano Dal Zilio
dalzilio@laas.fr

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]
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* ..... ✗ [s]
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
(2,5,5)	1 632 [t]	3 600 [u]	2 [v]	22 [w]
(2,10,8)	11 461 842	22 907 308	2	38
(2,10,10)	714 375	1 598 750	2	42
(2,15,15)	14 778 368	35 635 200	2	62
(3,10,8)	27 393 790	74 845 146	3	39
(3,10,10)	4 036 375	13 356 750	3	43
(3,10,15)	1 188 864	4 172 800	3	53
(5,10,10)	34 736 007	181 807 630	5	45
(5,10,15)	12 887 040	72 985 600	5	55
(8,32,26)	?	?	8	124

[l] transition *choosei* is not conservative.
[m] transition *setinode* is not subconservative.
[n] the definition of Nested-Unit Petri Nets (NUPN) is available from http://mcc.lip6.fr/nupn.php
[o] place *idle* is not safe when N $\geq$ 2, but the other places are safe.
[p] depends on the values of the parameters.
[q] depends on the values of the parameters.
[r] there is a deadlock if and only if I $\leq$ B.
[s] the marking of place *inodelist* can only decrease (assuming N $\geq$ 1).
[t] all values in this column were computed by TINA version 3.9.0 on March 2026.
[u] all values in this column were computed by TINA version 3.9.0 on March 2026.
[v] the only non-safe place is *idle*, whose marking is at most N.
[w] the maximum is reached at the initial marking, and is equal to N + 2.(I+B).