Y. Thierry-Mieg
yann.thierry-mieg@lip6.fr

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

The example MyHealth Portal is described in [1]. It is translated to a Petri net in [2] and checked to see if the provenance of a variable is always in the regular language

$$Patient(Secretary + \varepsilon)Nurse + Doctor + \varepsilon.$$

It was then used as one of the benchmarks for the tool Petrinizer in [3]. Models found in [4] where converted to PNML thanks to an ITS-Tools [5] library.

The source model has an initial marking ($l_0 \geq 1$) constraint rather than a single initial marking, this is used in the MCC to scale the model up.

References

1. A. Barth, J. C. Mitchell, A. Datta, and S. Sundaram. Privacy and utility in business processes. In CSF, pages 279–294. IEEE Computer Society, 2007.
2. R. Majumdar, R. Meyer, and Z. Wang. Static provenance verification for message passing programs. In SAS, volume 7935 of Lecture Notes in Computer Science, pages 366–387. Springer, 2013.
3. J. Esparza, R. Ledesma-Garza, R. Majumdar, P. J. Meyer, and F. Niksic. An smt-based approach to coverability analysis. In CAV, volume 8559 of Lecture Notes in Computer Science, pages 603–619. Springer, 2014
4. Klara J. Meyer, Petrinizer repository, https://github.com/meyerphi/petrinizer.
5. Y. Thierry-Mieg, Homepage of ITS-tools https://lip6.github.io/ITSTools-web/

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
M	The number of initial tokens in place **l0**.	2 4 6 8 10 12 14 16 18 20 22 24

Size of the model

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

number of places:	312
number of transitions:	5 431
number of arcs:	28 790

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]

[a] 16032 arcs are not simple free choice, e.g., the arc from place "l1" (which has 24 outgoing transitions) to transition "t2" (which has 2 input places).
[b] transitions "t2" and "t3" share a common input place "l1", but only the former transition has input place "x0_AA_q0".

Y. Thierry-Mieg
yann.thierry-mieg@lip6.fr

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) ..... ✗

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* ..... ?
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
2	?	?	?	≥ 12 (r)
4	?	?	?	≥ 14 (s)
6	?	?	?	≥ 16 (t)
8	?	?	?	≥ 18 (u)
10	?	?	?	≥ 20 (v)
12	?	?	?	≥ 22 (w)
14	?	?	?	≥ 24 (x)
16	?	?	?	≥ 26 (y)
18	?	?	?	≥ 28 (z)
20	?	?	?	≥ 30 (aa)
22	?	?	?	≥ 32 (ab)
24	?	?	?	≥ 34 (ac)

(c) 5424 transitions are not of a state machine, e.g., transition "t2".
(d) 312 places are not of a marked graph, e.g., place "l0".
(e) stated by CÆSAR.BDD version 3.7 on all 12 instances (12 different instances).
(f) from place "l0" one cannot reach place "ch0_AA_q0".
(g) there exist 72 source places, e.g., place "ch0_AA_q0".
(h) there exist 2 sink places, e.g., place "l110".
(i) stated by CÆSAR.BDD version 3.7 on all 12 instances (12 different instances).
(j) stated by CÆSAR.BDD version 3.7 on all 12 instances (12 different instances).
(k) 2089 transitions are not loop free, e.g., transition "t20".
(l) 3624 transitions are not conservative, e.g., transition "t26".
(m) 168 transitions are not subconservative, e.g., transition "t26".
(n) the definition of Nested-Unit Petri Nets (NUPN) is available from http://mcc.lip6.fr/nupn.php
(o) stated by CÆSAR.BDD version 3.7 on all 12 instances (12 different instances).
(p) 242 places, at least, are never marked, e.g., place "l8".
(q) 5204 transitions, at least, can never fire, e.g., transition "t3".
(r) lower bound given by the number of initial tokens.
(s) lower bound given by the number of initial tokens.

Y. Thierry-Mieg
yann.thierry-mieg@lip6.fr

(t) lower bound given by the number of initial tokens.
(u) lower bound given by the number of initial tokens.
(v) lower bound given by the number of initial tokens.
(w) lower bound given by the number of initial tokens.
(x) lower bound given by the number of initial tokens.
(y) lower bound given by the number of initial tokens.
(z) lower bound given by the number of initial tokens.
(aa) lower bound given by the number of initial tokens.
(ab) lower bound given by the number of initial tokens.
(ac) lower bound given by the number of initial tokens.