Nick Feng, Lina Marso, and Hubert Garavel
lina.marsso@utoronto.ca

This form is a summary description of the model entitled "Health Record" 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 model formally describes a computer system keeping track of personal health information. The users of this system can be patients or healtchcare agents. Patient can consent, provide, and update their personal health information. Agent can request permission, and then access, use, and disclose if authorized. The system has an interface that processes user actions and updates personal health records and their access authorizations. It also manages authorization and revocations. Every user action is logged by the system.

The formal description of the system is written as in LNT, a modern formal method that combines functional languages (to describe data types and user-defined functions operating on typed values) and process calculi (to describe concurrent components that synchronize using rendezvous and communicate via message passing). The LNT specification is 936-line long and parameterized by the number of patients and agents, as well as the maximal number of actions they can perform. Various instances of this model have been produced by varying these parameters, commenting out or not certain parts of code, and triggering or not certain optimizations.

The LNT specification was translated to LOTOS, and then to interpreted Petri nets using the CADP toolbox. Finally, P/T nets were obtained by stripping out all dataflow-related information (variables, types, assignments, guards, etc.) from interpreted Petri nets, leading to NUPN (*Nested-Unit Petri Net*) models translated to PNML using the CÆSAR.BDD tool.

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
N	The models contains 17 instances sorted by increasing complexity.	from 1 to 17

Size of the model

Parameter	Number of places	Number of transitions	Number of arcs	Number of units	HWB code
1	117	218	557	9	2–8–32
2	119	225	577	9	2–8–32
3	121	232	597	9	2–8–32
4	123	239	617	9	2–8–32
5	125	246	637	9	2–8–32
6	154	319	835	11	2–10–42
7	155	320	839	11	2–10–42
8	156	326	855	11	2–10–42
9	157	327	859	11	2–10–42
10	158	333	875	11	2–10–42
11	159	334	879	11	2–10–42
12	160	340	895	11	2–10–42
13	161	341	899	11	2–10–42
14	162	347	915	11	2–10–42
15	163	348	919	11	2–10–42
16	453	594	1333	15	7–8–57
17	624	828	1879	19	7–10–73

Nick Feng, Lina Marso, and Hubert Garavel
lina.marsso@utoronto.ca

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) ..... ✔

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* ..... ? (t)

(a) stated by CÆSAR.BDD version 3.5 on all 17 instances (N varying from 1 to 17).
(b) stated by CÆSAR.BDD version 3.5 on all 17 instances (N varying from 1 to 17).
(c) stated by CÆSAR.BDD version 3.5 on all 17 instances (N varying from 1 to 17).
(d) stated by CÆSAR.BDD version 3.5 on all 17 instances (N varying from 1 to 17).
(e) stated by CÆSAR.BDD version 3.5 on all 17 instances (N varying from 1 to 17).
(f) from place 1 one cannot reach place 0.
(g) place 0 is a source place.
(h) stated by CÆSAR.BDD version 3.5 on all 17 instances (N varying from 1 to 17).
(i) stated by CÆSAR.BDD version 3.5 on all 17 instances (N varying from 1 to 17).
(j) stated by CÆSAR.BDD version 3.5 on all 17 instances (N varying from 1 to 17).
(k) stated by CÆSAR.BDD version 3.5 to be true on 2 instance(s) out of 17, and false on the remaining 15 instance(s).
(l) stated by CÆSAR.BDD version 3.5 on all 17 instances (N varying from 1 to 17).
(m) stated by CÆSAR.BDD version 3.5 on all 17 instances (N varying from 1 to 17).
(n) the definition of Nested-Unit Petri Nets (NUPN) is available from http://mcc.lip6.fr/nupn.php
(o) safe by construction – stated by the CÆSAR compiler.
(p) stated by CÆSAR.BDD version 3.5 to be false on 13 instance(s) out of 17, and unknown on the remaining 4 instance(s).
(q) stated by CÆSAR.BDD version 3.5 to be false on 13 instance(s) out of 17, and unknown on the remaining 4 instance(s).
(r) stated by CÆSAR.BDD version 3.5 to be true on 13 instance(s) out of 17, and unknown on the remaining 4 instance(s).
(s) stated by CÆSAR.BDD version 3.5 to be false on 13 instance(s) out of 17, and unknown on the remaining 4 instance(s).
(t) stated by CÆSAR.BDD version 3.5 to be false on 13 instance(s) out of 17, and unknown on the remaining 4 instance(s).

Nick Feng, Lina Marso, and Hubert Garavel
lina.marsso@utoronto.ca

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
1	1.83784e+06 [u]	?	1	8
2	3.05544e+06 [v]	?	1	8
3	4.77331e+06 [w]	?	1	8
4	7.27557e+06 [x]	?	1	8
5	1.09742e+07 [y]	?	1	8
6	5.05148e+08 [z]	?	1	10
7	5.24712e+08 [aa]	?	1	10
8	8.06932e+08 [ab]	?	1	10
9	8.29535e+08 [ac]	?	1	10
10	1.2277e+09 [ad]	?	1	10
11	1.25247e+09 [ae]	?	1	10
12	1.83934e+09 [af]	?	1	10
13	1.86596e+09 [ag]	?	1	10
14	$\geq$ 2.67268e+09 [ah]	?	1 [ai]	10
15	$\geq$ 2.39028e+09 [aj]	?	1 [ak]	10
16	$\geq$ 1.79404e+12 [al]	?	1 [am]	8
17	$\geq$ 3.03525e+14 [an]	?	1 [ao]	10

[u] stated by CÆSAR.BDD version 3.5.
[v] stated by CÆSAR.BDD version 3.5.
[w] stated by CÆSAR.BDD version 3.5.
[x] stated by CÆSAR.BDD version 3.5.
[y] stated by CÆSAR.BDD version 3.5.
[z] stated by CÆSAR.BDD version 3.5.
[aa] stated by CÆSAR.BDD version 3.5.
[ab] stated by CÆSAR.BDD version 3.5.
[ac] stated by CÆSAR.BDD version 3.5.
[ad] stated by CÆSAR.BDD version 3.5.
[ae] stated by CÆSAR.BDD version 3.5.
[af] stated by CÆSAR.BDD version 3.5.
[ag] stated by CÆSAR.BDD version 3.5.
[ah] stated by CÆSAR.BDD version 3.5.
[ai] stated by the CÆSAR compiler.
[aj] stated by CÆSAR.BDD version 3.5.
[ak] stated by the CÆSAR compiler.
[al] stated by CÆSAR.BDD version 3.5.
[am] stated by the CÆSAR compiler.
[an] stated by CÆSAR.BDD version 3.5.
[ao] stated by the CÆSAR compiler.