Hubert Garavel and Wendelin Serwe
{hubert.garavel,wendelin.serwe}@inria.fr

This form is a summary description of the model entitled "ProductionCell" 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 production cell is a case study proposed in 1995 by Claus Lewerentz and Thomas Lindner of FZI (Forschungszentrum Informatik, Karlsruhe, Germany) to assess various formal methods on one common example.

The production cell serves to process metal blanks which are conveyed to a press by a feed belt. A robot takes each blank from the feed belt and places it into the press. The robot arm withdraws from the press, the press processes the metal blank and opens again. Finally, the robot takes the forged metal plate out of the press and puts it on a deposit belt.

A LOTOS description of the production cell was developed by Hubert Garavel in 1994. In 2013, it was slightly revised and then entirely rewritten in LNT by Wendelin Serwe and Hubert Garavel. LNT (*LOTOS New Technology*) 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 1180-line long (including comments). This LNT specification was translated to LOTOS, and then to an interpreted Petri net using the CADP toolbox. Finally, the present P/T net was obtained by stripping out all dataflow-related information (variables, types, assignments, guards, etc.) from the interpreted Petri net, leading to a NUPN (*Nested-Unit Petri Net*) model translated to PNML using the CÆSAR.BDD tool.

References

Claus Lewerentz and Thomas Lindner. *Formal Development of Reactive Systems – Case Study Production Cell.* Springer, Lecture Notes in Computer Science, vol. 891, 1995.

The source LNT (and LOTOS) files modelling the production cell controller are available from `ftp://ftp.inrialpes.fr/pub/vasy/demos/demo_19`

Scaling parameter

This model is not parameterized.

Size of the model

number of places:	176
number of transitions:	134
number of arcs:	513

Structural properties

ordinary — *all arcs have multiplicity one* ..... ✔
simple free choice — *all (different) transitions with a shared input place have no other input place* ..... ✘ (a)
state machine — *every transition has exactly one input place and exactly one output place* ..... ✘ (b)
marked graph — *every place has exactly one input transition and exactly one output transition* ..... ✘ (c)
connected — *there is an undirected path between every two nodes (places or transitions)* ..... ✔ (d)

(a) 100 arcs are not free choice, e.g., the arc from place 1 (which has 2 outgoing transitions) to transition 40 (which has 2 input places).
(b) 86 transitions are not of a state machine, e.g., transition 0.
(c) 64 places are not of a marked graph, e.g., place 0.
(d) stated by CÆSAR.BDD version 1.5.

Hubert Garavel and Wendelin Serwe
{hubert.garavel,wendelin.serwe}@inria.fr

strongly connected — *there is a directed path between every two nodes (places or transitions)* ..... ✗ (e)
source place(s) — *one or more places have no input transitions* ..... ✓ (f)
sink place(s) — *one or more places have no output transitions* ..... ✗ (g)
source transition(s) — *one or more transitions have no input places* ..... ✗ (h)
sink transitions(s) — *one or more transitions have no output places* ..... ✗ (i)
loop-free — *no transition has an input place that is also an output place* ..... ✓ (j)
conservative — *for each transition, the number of input arcs equals the number of output arcs* ..... ✗ (k)
subconservative — *for each transition, the number of input arcs equals or exceeds the number of output arcs* ..... ✗ (l)
nested units — *places are structured into hierarchically nested sequential units* (m) ..... ✓

Behavioural properties

safe — *in every reachable marking, there is no more than one token on a place* ..... ✓ (n)
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* ..... ?
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 graph

number of reachable markings:	1.1329E+13 (o)
number of transition firings:	1.5338E+14 (p)
max. number of tokens per place:	1 (q)
max. number of tokens per marking:	35 (r)

(e) from place 1 one cannot reach place 0.
(f) place 0 is a source place.
(g) stated by CÆSAR.BDD version 1.5.
(h) stated by CÆSAR.BDD version 1.5.
(i) stated by CÆSAR.BDD version 1.5.
(j) stated by CÆSAR.BDD version 1.5.
(k) 12 transitions are not conservative, e.g., transition 0.
(l) 5 transitions are not subconservative, e.g., transition 2.
(m) the definition of Nested-Unit Petri Nets (NUPN) is available from http://mcc.lip6.fr/nupn.php
(n) safe by construction – stated by the CÆSAR compiler.
(o) stated by CÆSAR.BDD version 1.5; confirmed at MCC'2014 by GreatSPN, Marcie, PNMC, and PNXDD.
(p) computed at MCC'2014.
(q) stated by the CÆSAR compiler; confirmed at MCC'2014 by GreatSPN and Marcie.
(r) computed at MCC'2014 by GreatSPN and Marcie.