Abderahman Kriouile and Wendelin Serwe
Abderahman.Kriouile@st.com

This form is a summary description of the model entitled "ARMCacheCoherency" 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 ACE specification proposed by ARM is becoming a de facto industrial standard for system-level cache coherence in heterogeneous systems on chip.

The present P/T net was derived from a formal specification of ACE developed by STMicroelectronics and INRIA Grenoble/LIG laboratory. This specification is written in LNT (*LOTOS New Technology*), which 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 2670-line long and models a system with two ACE masters and one ACE-Lite master, where:

- global constraints are included;
- one ACE master may execute MakeUnique, ReadOnce, and WriteBack transactions;
- the other ACE master executes no transactions;
- the ACE-Lite master executes ReadOnce transactions.

The 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

Abderahman Kriouile and Wendelin Serwe. *Formal Analysis of the ACE Specification for Cache Coherent Systems-on-Chip*. Proceedings of the 18th International Workshop on Formal Methods for Industrial Critical Systems (FMICS'13). Lecture Notes in Computer Science 8187, pp. 108-122, 2013. http://hal.inria.fr/hal-00858521/en

ARM. *AMBA AXI and ACE Protocol Specification*, version ARM IHI 0022E, February 2013. http://infocenter.arm.com/help/topic/com.arm.doc.ihi0022e

Scaling parameter

This model is not parameterized.

Size of the model

number of places:	87
number of transitions:	33676
number of arcs:	246935

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]

[a] 123325 arcs are not free choice, e.g., the arc from place 1 (which has 4425 outgoing transitions) to transition 132 (which has 3 input places).

Abderahman Kriouile and Wendelin Serwe
Abderahman.Kriouile@st.com

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)
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* ..... ✗ (o)
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* ..... ✓ (p)
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:	3.206E+8 (q)
number of transition firings:	2.234E+10 (r)
max. number of tokens per place:	1 (s)
max. number of tokens per marking:	12

(b) 33541 transitions are not of a state machine, e.g., transition 0.
(c) 87 places are not of a marked graph, e.g., place 0.
(d) stated by CÆSAR.BDD version 1.5.
(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) 22262 transitions are not loop free, e.g., transition 6.
(k) transition 0 is not conservative.
(l) transition 0 is not subconservative.
(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 2.0.
(p) stated by CÆSAR.BDD version 2.0.
(q) stated by CÆSAR.BDD version 2.0; confirmed at MCC'2014 by Marcie and PNMC.
(r) computed at MCC'2014 by Marcie.
(s) confirmed at MCC'2014 by GretSPN and Marcie.