Nicolas Amat, Silvano Dal Zilio, and Thomas Hujsa
dalzilio@laas.fr

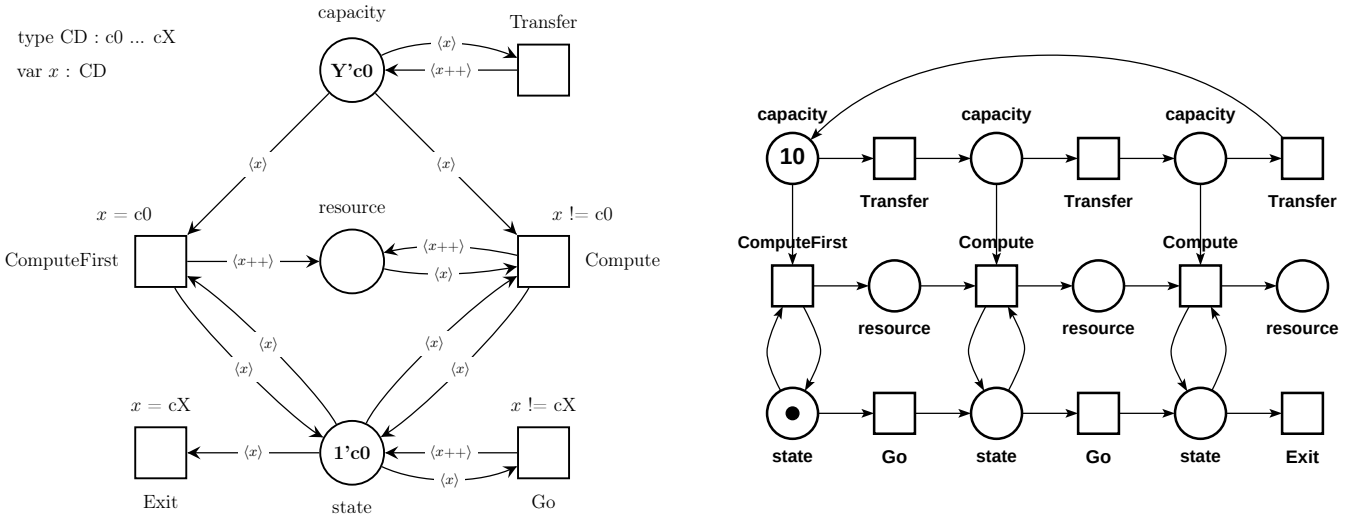
This form is a summary description of the model entitled "CryptoMiner" proposed for the Model Checking Contest @ Petri Nets. Models can be given in several instances parameterized by scaling parameters. Colored nets can be accompanied by one or many equivalent, unfolded P/T nets. Models are given together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

Description

This model corresponds to a processing chain with $X + 1$ steps, each working on a different type of resource, one after another. We provide two different types of instances: CryptoMinerA, which is unbounded; and CryptoMinerB, which is a bounded version of CryptoMinerA obtained by adding a capacity place limiting the number of times a Compute transition can fire.

This is a symmetric net where resources are modelled using a cyclic enumeration type with values c0 ... cX. At each step, only one type of resource can be processed, depending on the value of the token in place state, until we can finally fire Exit.

CryptoMinerA is a parametric version of a model used by Serge Haddad on several works about the coverability problem [1], sometimes referred to as "a day in the life of a banana farmer". We brought this model into the 21st century and propose a symmetric net version representing the life of a cryptocurrency miner. This model was among several benchmarks used to compare the performances of tools for checking reachability problems in [2].



Graphical representation of CryptoMinerB-COL-DXNY (left) and the derived P/T net (right), for the instance $(B, 2, 10)$. *The CryptoMinerA instances are obtained by removing place capacity*

References

1. Finkel, A., Haddad, S., & Khmelnitsky, I. (2019). *Coverability and termination in recursive Petri nets.* In International Conference on Applications and Theory of Petri Nets and Concurrency. Springer.

2. Amat, N., Dal Zilio, S., & Hujsa, T. (2022). *Property directed reachability for generalized Petri nets.* In International Conference on Tools and Algorithms for the Construction and Analysis of Systems. Springer.

Nicolas Amat, Silvano Dal Zilio, and Thomas Hujsa
dalzilio@laas.fr

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
(A, X) or (B, X, Y)	X is the number of different resources in the model (used both for CryptoMinerA and CryptoMinerB instances), whereas Y defines the initial capacity (only for CryptoMinerB instances). These parameters affect the initial marking and do not impact the size of the model	$(A, 3)$, $(A, 5)$, $(A, 10)$, and $(B, 3, 10)$, $(B, 3, 100)$, $(B, 5, 100)$, $(B, 5, 250)$, $(B, 10, 100)$, $(B, 20, 100)$

Size of the colored net model

number of places: 2 for CryptoMinerA instances, 3 for CryptoMinerB instances
number of transitions: 4 for CryptoMinerA instances, 5 for CryptoMinerB instances
number of arcs: 10 for CryptoMinerA instances, 14 for CryptoMinerB instances

Size of the derived P/T model instances

Parameter	Number of places	Number of transitions	Number of arcs
(A, X)	$2\,\mathrm{X} + 2$	$2\,\mathrm{X} + 2$	$6\,\mathrm{X} + 4$
(B, X, Y)	$3\,\mathrm{X} + 3$	$3\,\mathrm{X} + 3$	$9\,\mathrm{X} + 7$

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] ..... ✘

[a] stated by CÆSAR.BDD version 3.7 on all 9 instances (CryptoMinerA and CryptoMinerB).
[b] stated by CÆSAR.BDD version 3.7 on all 9 instances (CryptoMinerA and CryptoMinerB).
[c] stated by CÆSAR.BDD version 3.7 on all 9 instances (CryptoMinerA and CryptoMinerB).
[d] stated by CÆSAR.BDD version 3.7 on all 9 instances (CryptoMinerA and CryptoMinerB).
[e] stated by CÆSAR.BDD version 3.7 on all 9 instances (CryptoMinerA and CryptoMinerB).
[f] stated by CÆSAR.BDD version 3.7 on all 9 instances (CryptoMinerA and CryptoMinerB).
[g] stated by CÆSAR.BDD version 3.7 on all 9 instances (CryptoMinerA and CryptoMinerB).
[h] no transition can consume a token of color "cY" from place "resource"; confirmed by CÆSAR.BDD version 3.7 (place "resource_c0" is a sink place).
[i] stated by CÆSAR.BDD version 3.7 on all 9 instances (CryptoMinerA and CryptoMinerB).
[j] stated by CÆSAR.BDD version 3.7 on all 9 instances (CryptoMinerA and CryptoMinerB); transition "Exit" is a sinck transition.
[k] stated by CÆSAR.BDD version 3.7 on all 9 instances (CryptoMinerA and CryptoMinerB).
[l] stated by CÆSAR.BDD version 3.7 on all 9 instances (CryptoMinerA and CryptoMinerB).
[m] it is true for CryptoMinerB instances but false for CryptoMinerA instances; confirmed by CÆSAR.BDD version 3.7.
[n] the definition of Nested-Unit Petri Nets (NUPN) is available from http://mcc.lip6.fr/nupn.php

Nicolas Amat, Silvano Dal Zilio, and Thomas Hujsa
dalzilio@laas.fr

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* ..... ✗
dead transition(s) — *one or more transitions cannot fire from any reachable marking* ..... ✗ [p]
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
$(A,3)$, $(A,5)$, $(A,10)$	∞ [q]	∞	∞	∞
$(B,3,10)$	10 636 [r]	38 126 [s]	10 [t]	11 [u]
$(B,3,100)$	3 004 907 847 [v]	14 272 062 668 [w]	100	101
$(B,5,100)$	3 626 541 971 921 [x]	23 405 636 097 113 [y]	100	101
$(B,5,250)$	3.3357E+16 [z]	2.2538E+17 [aa]	250	251
$(B,10,100)$	1.3682E+18 [ab]	1.4276E+19 [ac]	100	101
$(B,20,100)$	1.4625E+26 [ad]	2.5790E+27 [ae]	100	101

Other properties

The difficulty when analysing an instance of CryptoMiner lies in the presence of constraints that cannot be derived from the state equation alone. For instance, the presence of a token with value cj in place 'resource' implies that the value in place 'state' is different from ci when $i < j$. Unfortunately, with symmetric net, it is not possible to distinguish between different values using the MCC property language. With the derived P/T nets, a corresponding formula would be along the line of the invariant formula INV below. This formula can be used with the CryptoMinerA and CryptoMinerB instances interchangeably.

$$\text{INV} \ : \ \text{AG}\left((\text{state\_c}i = 0) \vee (\text{resource\_c}j = 0)\right) \qquad \text{where } 0 \leq i < j \leq X$$

[o] the initial marking is not safe when $Y \geq 2$, which is the case in all our instances.
[p] this is false when $Y \geq X$, which is the case in all our instances.
[q] place resource is unbounded; checked by TINA version 3.7.0 on January 2023.
[r] computed by TINA version 3.7.0 on January 2023.
[s] computed by TINA version 3.7.0 on January 2023.
[t] the maximal number of tokens is equal to parameter Y, which is the initial marking of place capacity; confirmed by TINA version 3.7.0 on January 2023.
[u] since CryptoMinerB is subconservative, the maximum total number of tokens is $Y + 1$, which is observed in the initial marking; confirmed by TINA version 3.7.0 and by CÆSAR.BDD version 3.7 on January 2023.
[v] computed by TINA version 3.7.0 on January 2023.
[w] computed by TINA version 3.7.0 on January 2023.
[x] computed by TINA version 3.7.0 on January 2023.
[y] computed by TINA version 3.7.0 on January 2023.
[z] computed by TINA version 3.7.0 on January 2023.
[aa] computed by TINA version 3.7.0 on January 2023.
[ab] computed by TINA version 3.7.0 on January 2023.
[ac] computed by TINA version 3.7.0 on January 2023.
[ad] computed by TINA version 3.7.0 on January 2023.
[ae] computed by TINA version 3.7.0 on January 2023.