Abstraction-based Incremental Inductive Coverability for Petri nets

in 180 seconds

Jiawen Kang   YunJun Bai   Li Jiao

State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing, China

June 2021

Coverability problem of Petri nets

Functionality of our algorithm
 - determining for a target marking m_t whether m_t is coverable in a Petri net

Definition
 - m_t is coverable if there exists a reachable marking m_r from m_0 such that $m_t \preccurlyeq m_r$.

State-of-art method

IC3 for coverability of Petri nets

- compute an inductive invariant

- maintain a sequence of over-approximations of forward-reachable markings

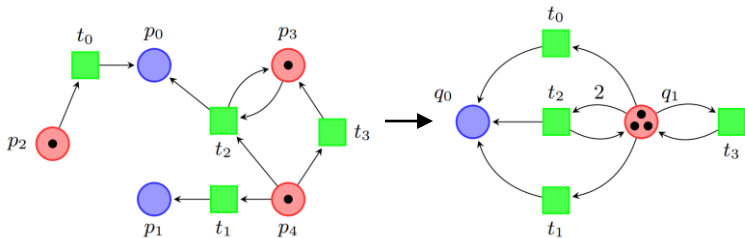- solve the coverability problem of Petri nets without using SMT solvers

Perform better?

IC3 works on Petri nets with high dimensionality directly

Perform better?

A method **P**lace **M**erge **A**bstraction(PMA) to reduce dimensionality of Petri nets

Merge some places of original Petri net into **one,** get an abstract Petri net with lower dimensionality.
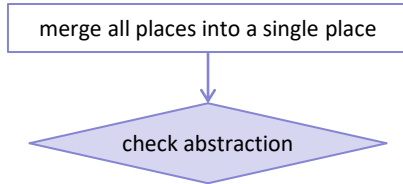
Perform better?

Improve the outperformance of IC3

- combine IC3 with abstraction in CEGAR framework
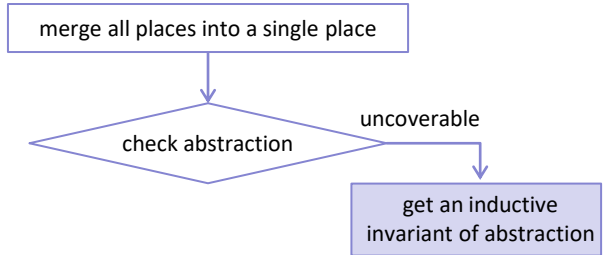
- refine abstraction when necessary

- IC3+PMA

merge all places into a single place

IC3+PMA algorithm
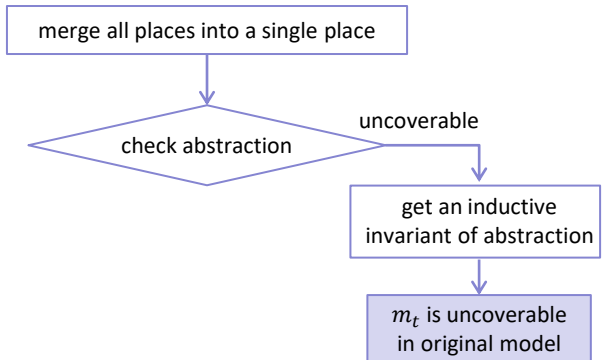
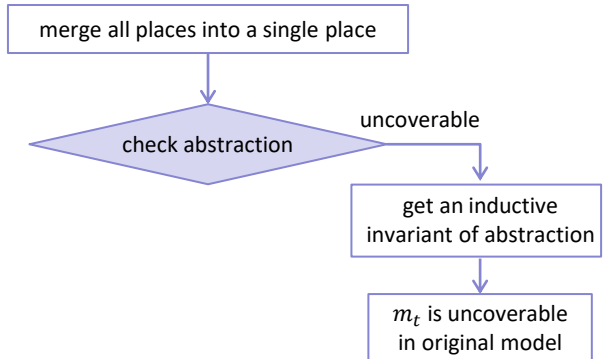merge all places into a single place

check abstraction

IC3+PMA algorithm

```
┌─────────────────────────────────────┐
│  merge all places into a single place │
└─────────────────────────────────────┘
                    │
                    ▼
        ◇─────────────────────◇   uncoverable
        ◇   check abstraction   ◇──────────────┐
        ◇─────────────────────◇                │
                                                ▼
                                ┌──────────────────────────┐
                                │     get an inductive       │
                                │  invariant of abstraction  │
                                └──────────────────────────┘
```

IC3+PMA algorithm

merge all places into a single place

check abstraction

uncoverable

get an inductive
invariant of abstraction

m_t is uncoverable
in original model

IC3+PMA algorithm

merge all places into a single place

check abstraction

uncoverable

get an inductive invariant of abstraction

m_t is uncoverable in original model

IC3+PMA algorithm

merge all places into a single place

coverable   check abstraction   uncoverable

get a counter-example π

get an inductive invariant of abstraction

m_t is uncoverable in original model
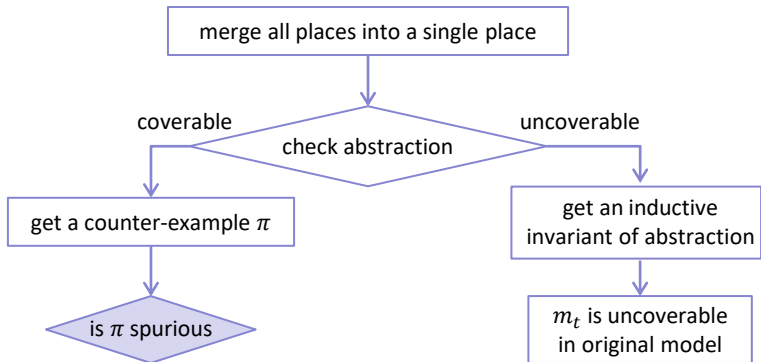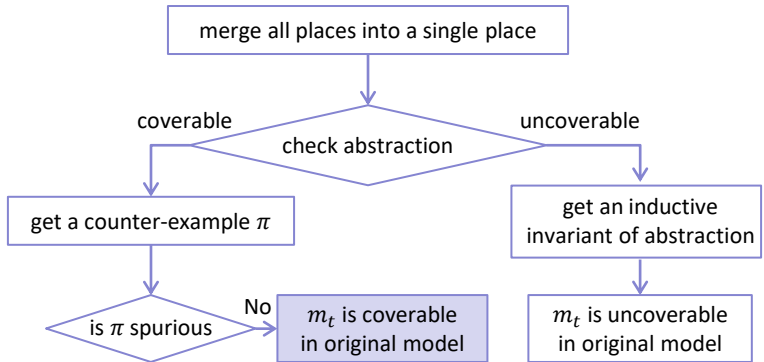
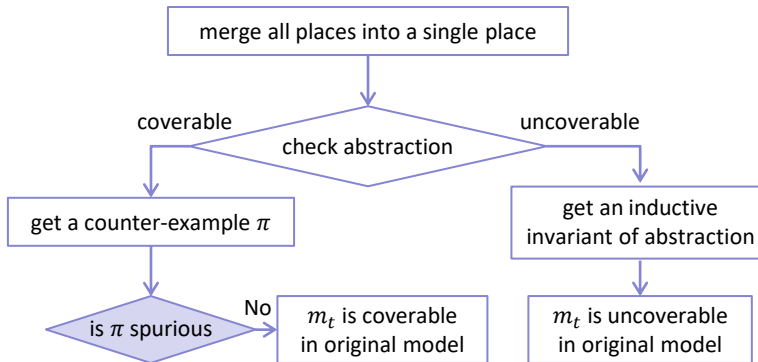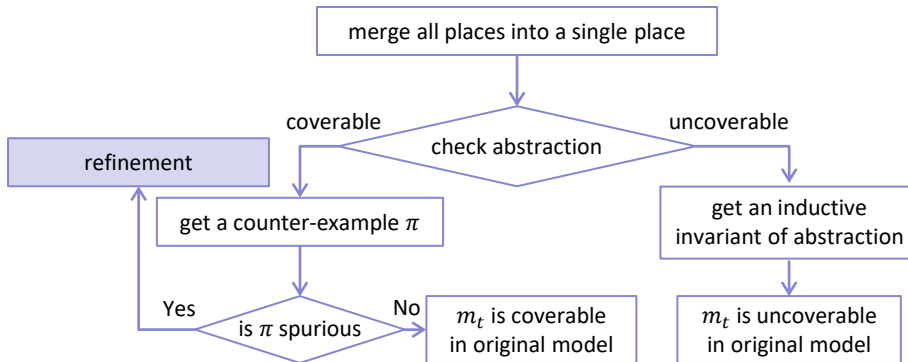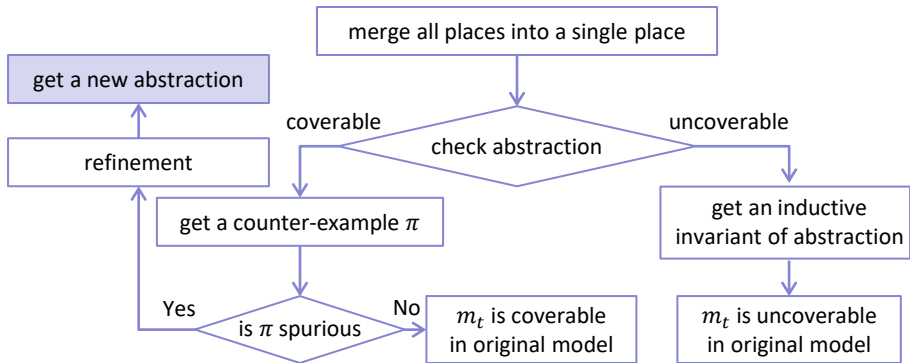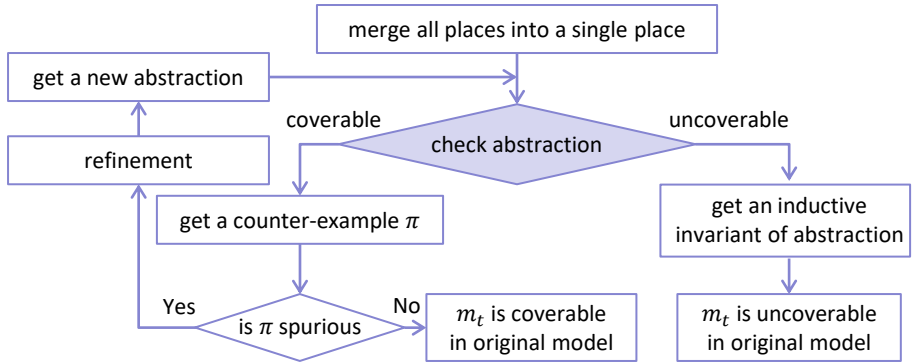# IC3+PMA algorithm
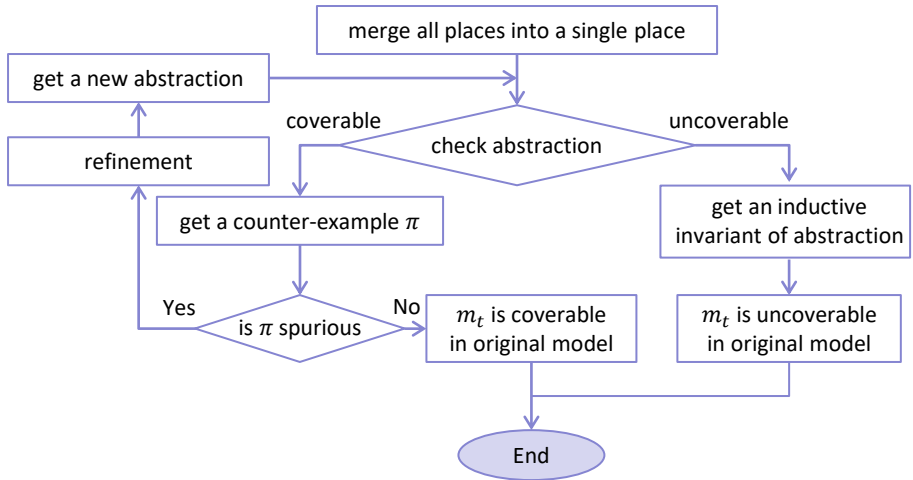
IC3+PMA algorithm

IC3+PMA algorithm

IC3+PMA algorithm

merge all places into a single place

check abstraction

coverable

uncoverable

refinement

get a counter-example π

get an inductive invariant of abstraction

is π spurious

Yes

No

m_t is coverable in original model

m_t is uncoverable in original model

IC3+PMA algorithm

merge all places into a single place

coverable

uncoverable

check abstraction

get a new abstraction

refinement

get a counter-example π

get an inductive
invariant of abstraction

Yes

No

is π spurious

m_t is coverable
in original model

m_t is uncoverable
in original model

IC3+PMA algorithm

IC3+PMA algorithm

Thank You For Your Attention