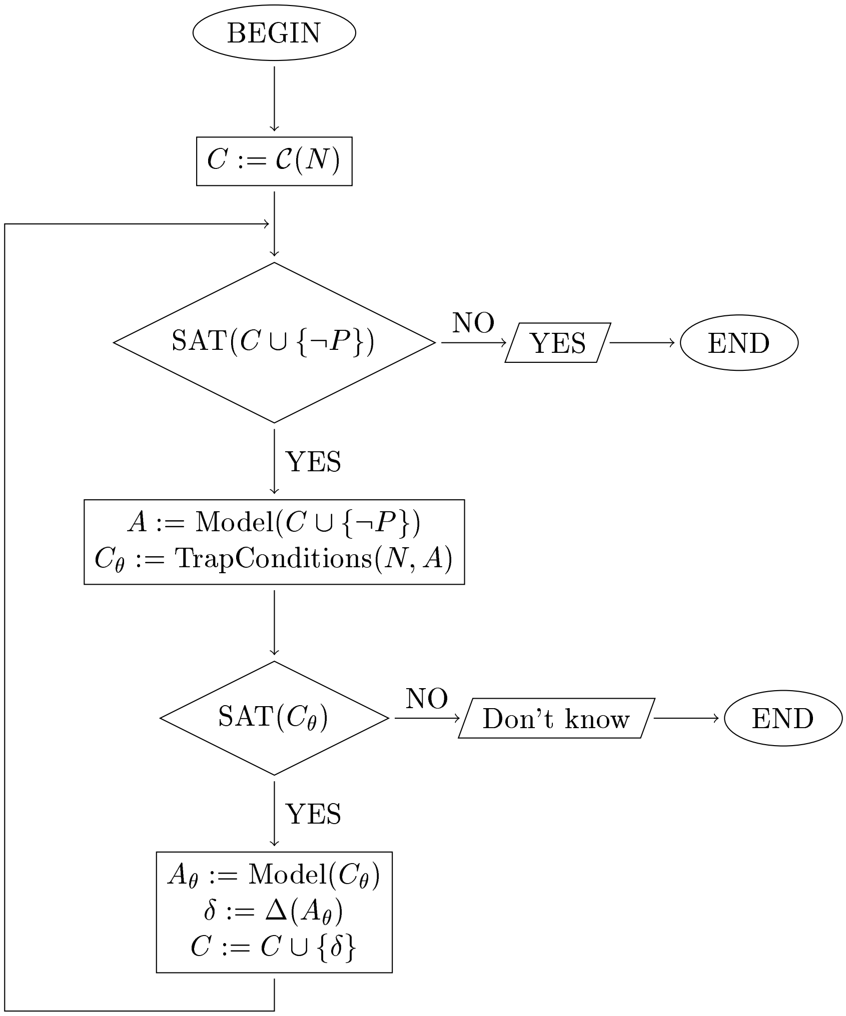
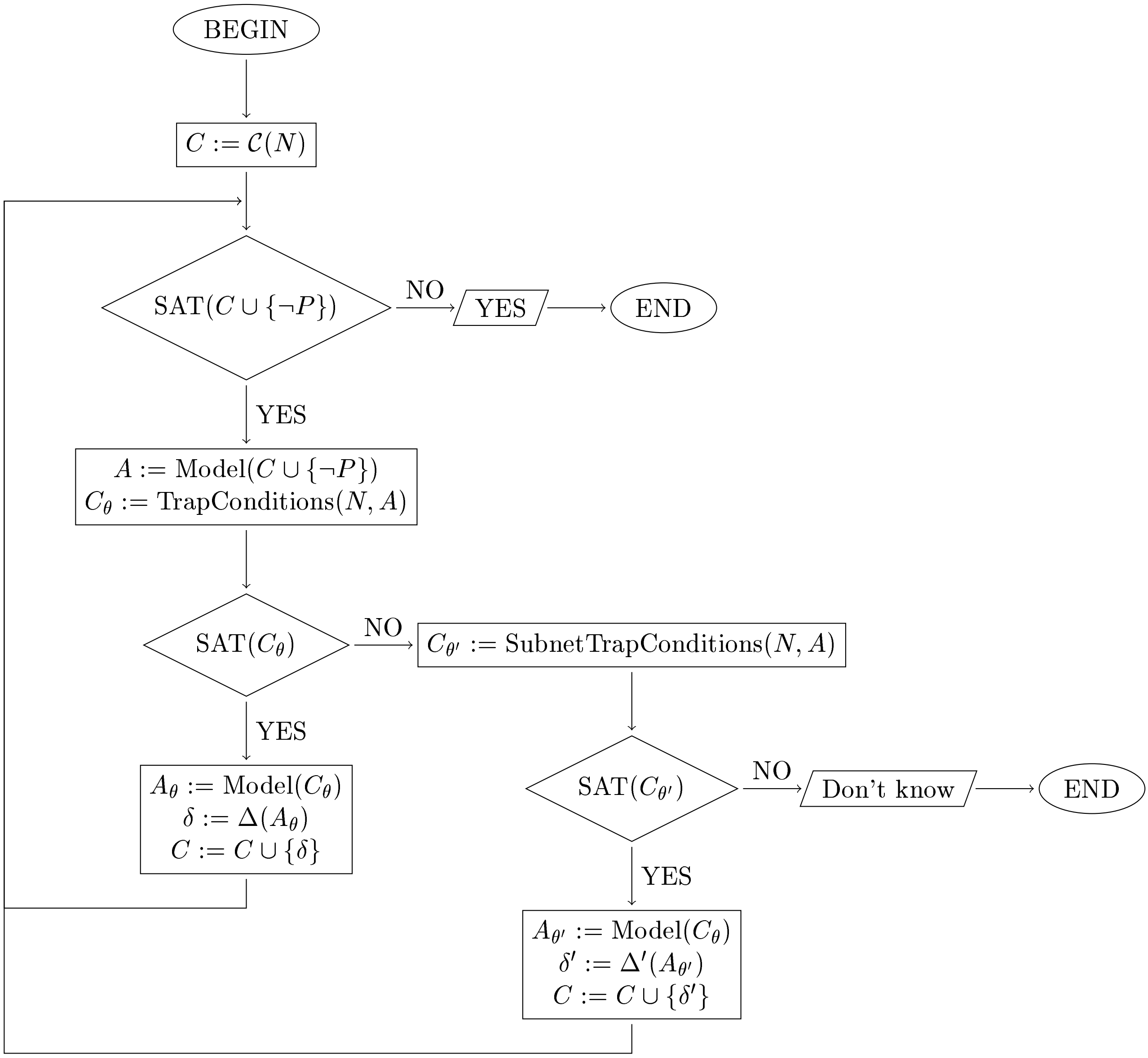
1 Method

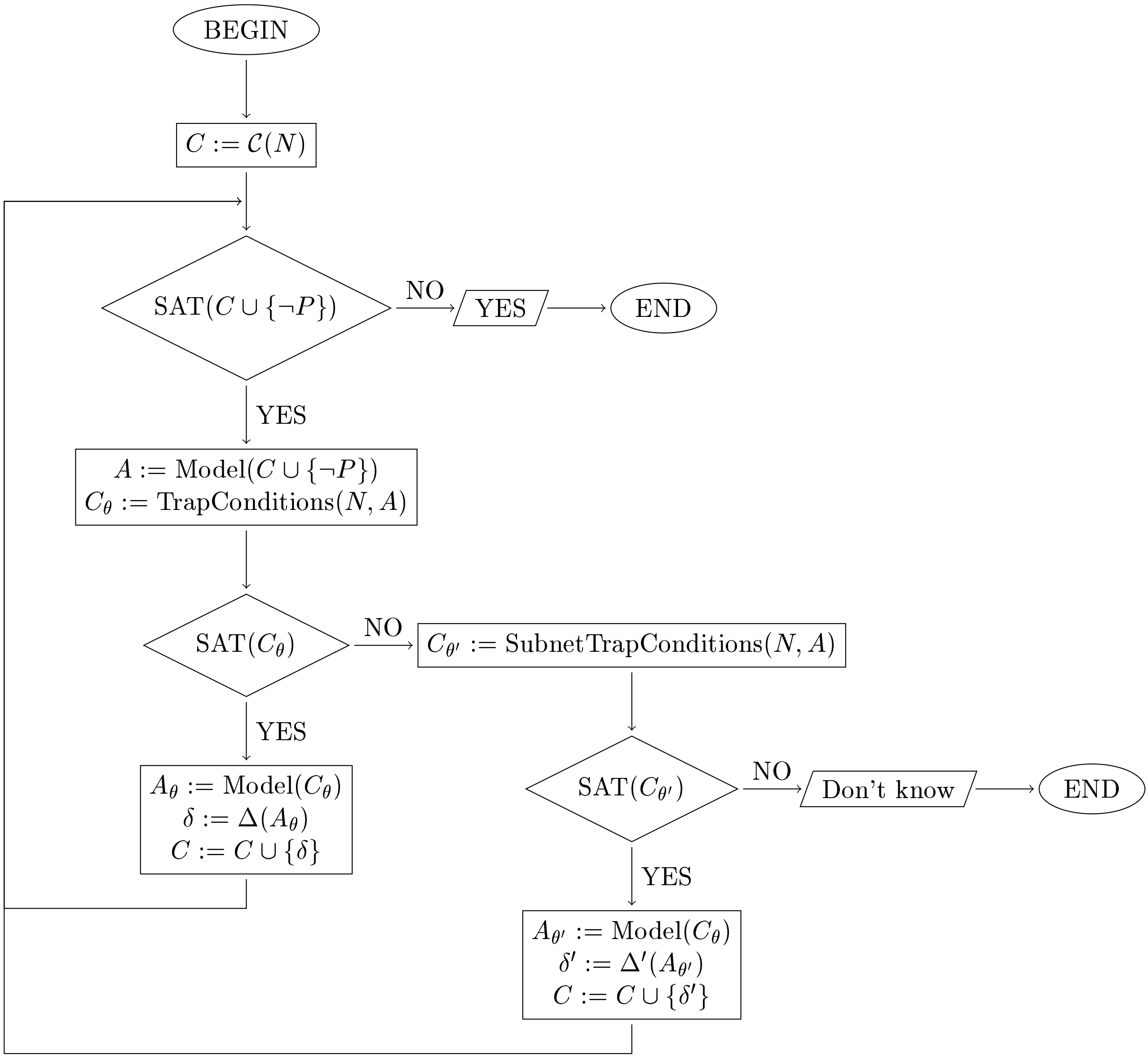
1.1 With trap refinement



1.2 With trap and subnet trap refinement



1.3 General refinement method



1.4 State space exploration

function SAFETY(N, M, D)
    if $unsafe(N, M)$ **then**
        return unsafe
    else if $safe(N, M)$ **then**
        return safe
    else if $D = 0$ **then**
        return don't know

```
    else
        ∀M → M_i : R_i ← SAFETY(N, M, D − 1)
        if ∃R_i : R_i = unsafe then
            return unsafe
        else if ∃R_i : R_i = don't know then
            return don't know
        else   ▷ ∀R_i : R_i = safe
            return safe
        end if
    end if
end function
```

2 Petri nets tested

2.1 Peterson's Algorithm

Taken from Javier's notes on petri nets (http://www7.in.tum.de/um/courses/petri/SS2013/PNSkript.pdf, p. 16). Tested with trap refinement.

2.1.1 Constraints C_0

$$
\begin{aligned}
p_1 &= 1 - u_1 + u_6 \\
p_2 &= 0 + u_1 - u_2 - u_3 \\
p_3 &= 0 + u_2 + u_3 - u_4 - u_5 \\
p_4 &= 0 + u_4 + u_5 - u_6 \\
q_1 &= 1 - v_1 + v_6 \\
q_2 &= 0 + v_1 - v_2 - v_3 \\
q_3 &= 0 + v_2 + v_3 - v_4 - v_5 \\
q_4 &= 0 + v_4 + v_5 - v_6 \\
(m_1 = f) &= 1 - u_1 + u_6 \\
(m_1 = t) &= 0 + u_1 - u_6 \\
(m_2 = f) &= 1 - v_1 + v_6 \\
(m_2 = t) &= 0 + v_1 - v_6 \\
(hold = 1) &= 1 + u_2 - v_3 \\
(hold = 2) &= 0 - u_2 + v_3 \\
p_4 &\geq 1 \\
q_4 &\geq 1 \\
\forall p \in S \cup T: \quad p &\geq 0
\end{aligned}
$$

$$\delta_1 = p_3 \vee q_2 \vee (m_2 = f) \vee (hold = 2)$$
$$\delta_2 = p_2 \vee q_3 \vee (m_1 = f) \vee (hold = 1)$$

2.1.2 A_1

$$\begin{aligned}
p_1 &= 0\\
p_2 &= 0\\
p_3 &= 0\\
p_4 &= 1\\
q_1 &= 0\\
q_2 &= 0\\
q_3 &= 0\\
q_4 &= 1\\
(m_1 = f) &= 0\\
(m_1 = t) &= 1\\
(m_2 = f) &= 0\\
(m_2 = t) &= 1\\
(hold = 1) &= 1\\
(hold = 2) &= 0\\
u_1 &= 1\\
u_2 &= 0\\
u_3 &= 1\\
u_4 &= 0\\
u_5 &= 1\\
u_6 &= 0\\
v_1 &= 1\\
v_2 &= 1\\
v_3 &= 0\\
v_4 &= 1\\
v_5 &= 0\\
v_6 &= 0
\end{aligned}$$

2.1.3 A_2

$$
\begin{aligned}
p_1 &= 0 \\
p_2 &= 0 \\
p_3 &= 0 \\
p_4 &= 1 \\
q_1 &= 0 \\
q_2 &= 0 \\
q_3 &= 0 \\
q_4 &= 1 \\
(m_1 = f) &= 0 \\
(m_1 = t) &= 1 \\
(m_2 = f) &= 0 \\
(m_2 = t) &= 1 \\
(hold = 1) &= 0 \\
(hold = 2) &= 1 \\
u_1 &= 1 \\
u_2 &= 1 \\
u_3 &= 0 \\
u_4 &= 0 \\
u_5 &= 1 \\
u_6 &= 0 \\
v_1 &= 2 \\
v_2 &= 0 \\
v_3 &= 2 \\
v_4 &= 0 \\
v_5 &= 2 \\
v_6 &= 1
\end{aligned}
$$

2.1.4 $A_{\theta 1}$

$$
\begin{aligned}
p_1 &= 0 \\
p_2 &= 0 \\
p_3 &= 1 \\
p_4 &= 0 \\
q_1 &= 0 \\
q_2 &= 1 \\
q_3 &= 0 \\
q_4 &= 0 \\
(m_1 = f) &= 0 \\
(m_1 = t) &= 0 \\
(m_2 = f) &= 1 \\
(m_2 = t) &= 0 \\
(hold = 1) &= 0 \\
(hold = 2) &= 1
\end{aligned}
$$

2.1.5 $A_{\theta 2}$

$$
\begin{aligned}
p_1 &= 0 \\
p_2 &= 1 \\
p_3 &= 0 \\
p_4 &= 0 \\
q_1 &= 0 \\
q_2 &= 0 \\
q_3 &= 1 \\
q_4 &= 0 \\
(m_1 = f) &= 1 \\
(m_1 = t) &= 0 \\
(m_2 = f) &= 0 \\
(m_2 = t) &= 0 \\
(hold = 1) &= 1 \\
(hold = 2) &= 0
\end{aligned}
$$

2.1.6 C_θ

①

$$
\begin{aligned}
p_1 &\implies o\_u_1 \\
p_2 &\implies o\_u_2 \wedge o\_u_3 \\
p_3 &\implies o\_u_4 \wedge o\_u_5 \\
p_4 &\implies o\_u_6 \\
q_1 &\implies o\_v_1 \\
q_2 &\implies o\_v_2 \wedge o\_v_3 \\
q_3 &\implies o\_v_4 \wedge o\_v_5 \\
q_4 &\implies o\_v_6 \\
(m_1 = f) &\implies o\_u_1 \wedge o\_v_4 \\
(m_1 = t) &\implies o\_u_6 \\
(m_2 = f) &\implies o\_v_1 \wedge o\_u_4 \\
(m_2 = t) &\implies o\_v_6 \\
(hold = 1) &\implies o\_v_3 \wedge o\_v_5 \wedge o\_u_3 \\
(hold = 2) &\implies o\_u_3 \wedge o\_u_5 \wedge o\_v_3 \\
o\_u_1 &\implies (p_2 \vee (m_1 = t)) \\
o\_u_2 &\implies (p_3 \vee (hold = 1)) \\
o\_u_3 &\implies (p_3 \vee (hold = 1)) \\
o\_u_4 &\implies (p_4 \vee (m_2 = f)) \\
o\_u_5 &\implies (p_4 \vee (hold = 2)) \\
o\_u_6 &\implies (p_1 \vee (m_1 = f)) \\
o\_v_1 &\implies (q_2 \vee (m_2 = t)) \\
o\_v_2 &\implies (q_3 \vee (hold = 2)) \\
o\_v_3 &\implies (q_3 \vee (hold = 2)) \\
o\_v_4 &\implies (q_4 \vee (m_1 = f)) \\
o\_v_5 &\implies (p_4 \vee (hold = 1)) \\
o\_v_6 &\implies (q_1 \vee (m_2 = f))
\end{aligned}
$$

②

$$p_1 \vee q_1 \vee (m_1 = f) \vee (m_2 = f) \vee (hold = 1)$$

③$_1$

$$\neg p_4 \wedge \neg q_4 \wedge \neg(m_1 = t) \wedge \neg(m_2 = t) \wedge \neg(hold = 1)$$

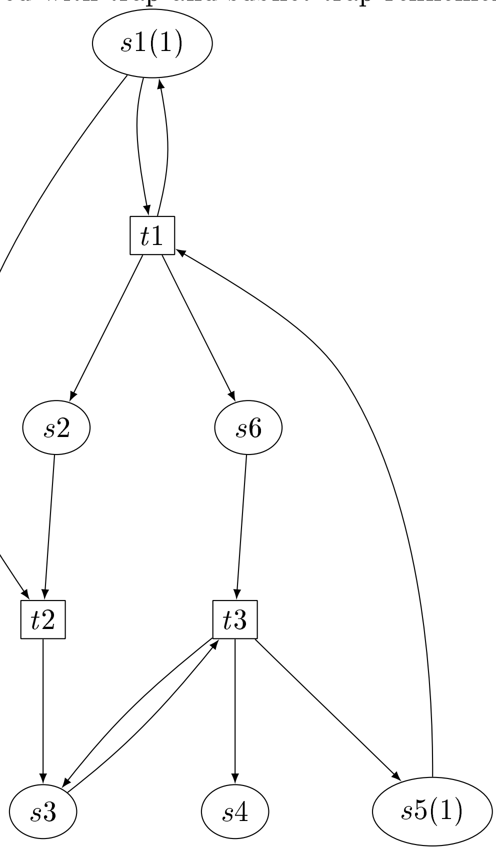
③$_2$

$$\neg p_4 \wedge \neg q_4 \wedge \neg(m_1 = t) \wedge \neg(m_2 = t) \wedge \neg(hold = 2)$$

2.2 Cyclic net

Taken and modified from Stephan Melzer's Dissertation, p. 140.

Tested with trap and subnet trap refinement.



2.2.1 Constraints C_0

$$
\begin{aligned}
s_1 &= 1 \qquad - t_2 \\
s_2 &= 0 + t_1 - t_2 \\
s_3 &= 0 \qquad + t_2 \\
s_4 &= 0 \qquad\qquad + t_3 \\
s_5 &= 1 - t_1 \qquad + t_3 \\
s_6 &= 0 + t_1 \qquad - t_3 \\
s_1 &\geq 1 \\
s_2 \geq 1 \quad s_4 &\geq 1 \\
s_5 &\geq 1 \\
\forall p \in S \cup T : p &\geq 0
\end{aligned}
$$

$$\delta_1' = (t_1 > 0) \wedge (t_2 = 0) \wedge (t_3 > 0) \implies (s_3 > 0)$$

2.2.2 A_1

$$\begin{aligned} s_1 &= 1 \\ s_2 &= 1 \\ s_3 &= 0 \\ s_4 &= 1 \\ s_5 &= 1 \\ s_6 &= 0 \\ t_1 &= 1 \\ t_2 &= 0 \\ t_3 &= 1 \end{aligned}$$

2.2.3 $A_{\theta'1}$

$$\begin{aligned} s_1 &= 0 \\ s_2 &= 0 \\ s_3 &= 1 \\ s_4 &= 0 \\ s_5 &= 0 \\ s_6 &= 0 \end{aligned}$$

2.2.4 C_θ

$$\begin{aligned} s_1 &\implies o\_t_1 \wedge o\_t_2 \\ s_2 &\implies o\_t_2 \\ s_3 &\implies o\_t_3 \\ s_4 &\implies true \\ s_5 &\implies o\_t_1 \\ s_6 &\implies o\_t_2 \\ o\_t_1 &\implies (s_1 \vee s_2 \vee s_6) \\ o\_t_2 &\implies s_3 \\ o\_t_3 &\implies (s_3 \vee s_4 \vee s_5) \end{aligned}$$

$$s_1 \vee s_5$$

$$\neg s_1 \wedge \neg s_2 \wedge \neg s_4 \wedge \neg s_5$$

2.2.5 $C_{\theta'}$

$$\begin{aligned}
s_1 &\implies o_t_1 \wedge o_t_2 \\
s_2 &\implies o_t_2 \\
s_3 &\implies o_t_3 \\
s_4 &\implies true \\
s_5 &\implies o_t_1 \\
s_6 &\implies o_t_2 \\
o_t_1 = (t_1 > 0) &\implies (s_1 \vee s_2 \vee s_6) \\
o_t_2 = (t_2 > 0) &\implies s_3 \\
o_t_3 = (t_3 > 0) &\implies (s_3 \vee s_4 \vee s_5)
\end{aligned}$$

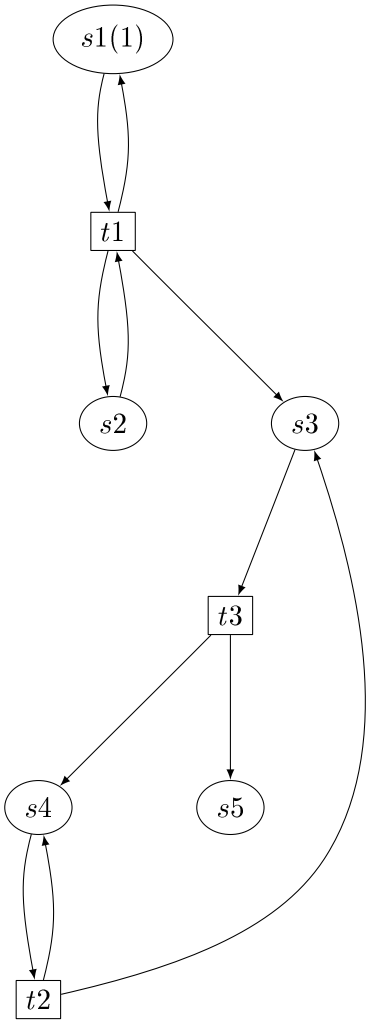
$$(t_1 = 1) \wedge (t_2 = 0) \wedge (t_3 = 1)$$

$$s_1 \vee s_2 \vee s_3 \vee s_4 \vee s_5 \vee s_6$$

$$\neg s_1 \wedge \neg s_2 \wedge \neg s_4 \wedge \neg s_5$$

2.3 Empty trap condition net

Tested with trap, subnet trap and empty trap refinement.



2.4 Constraints C_0

$$
\begin{aligned}
s_1 &= 1 \\
s_2 &= 0 \\
s_3 &= 0 + t_1 + t_2 - t_3 \\
s_4 &= 0 \qquad\qquad\quad + t_3 \\
s_5 &= 0 \qquad\qquad\quad + t_3 \\
s_5 &\geq 1 \\
\forall p \in S \cup T : p &\geq 0
\end{aligned}
$$

$$\delta_1 = (t_1 > 0) \wedge (t_3 > 0) \implies (t_1 > 0)\delta_2 \qquad\qquad = (t_1 > 0) \implies false$$

2.5 A_1

$$\begin{aligned}
s_1 &= 1\\
s_2 &= 0\\
s_3 &= 0\\
s_4 &= 1\\
s_5 &= 1\\
t_1 &= 0\\
t_2 &= 1\\
t_3 &= 1
\end{aligned}$$

2.6 A_2

$$\begin{aligned}
s_1 &= 1\\
s_2 &= 0\\
s_3 &= 1\\
s_4 &= 1\\
s_5 &= 1\\
t_1 &= 1\\
t_2 &= 1\\
t_3 &= 1
\end{aligned}$$

2.7 Empty trap $A_{\theta 1}$

$$\begin{aligned}
s_1 &= false\\
s_2 &= false\\
s_3 &= true\\
s_4 &= true\\
s_5 &= false\\
s_6 &= false\\
o_t_1 &= false\\
o_t_2 &= true\\
o_t_3 &= true\\
i_t_1 &= true\\
i_t_2 &= true\\
i_t_3 &= true
\end{aligned}$$

2.8 Empty trap $A_{\theta 2}$

$$\begin{aligned} s_1 &= false \\ s_2 &= true \\ s_3 &= false \\ s_4 &= false \\ s_5 &= false \\ s_6 &= false \\ o\_t_1 &= true \\ o\_t_2 &= true \\ o\_t_3 &= true \\ i\_t_1 &= true \\ i\_t_2 &= true \\ i\_t_3 &= true \end{aligned}$$

3 Refinement methods

3.1 TrapConditions

For a petri net N and an assignment A, find a set S that satisfies

1. S is a trap in the net N.
2. S is marked in the initial marking M_0.
3. S is unmarked in the assignment A.

For such a set S, generate a constraint $\delta = \left(\sum_{s \in S} s \geq 1\right)$, ensuring the trap is marked in any assignment.

3.2 SubnetTrapConditions

For a petri net N and an assignment A, construct a subnet N' from N that contains only the transitions that are fired in A. For the net N', find a set S that satisfies

1. S is a trap in the subnet N'.
2. S contains a place with an incoming transition in N'.
3. S is unmarked in the assignment A.

For such a set S, generate a constraint $\delta = \left(\bigwedge_{t \in T_1}(t > 0) \wedge \bigwedge_{t \in T_2}(t = 0) \implies \sum_{s \in S} s \geq 1\right)$, where T_1 are the transitions fired in A and T_2 are the transitions not fired in A. This ensures the trap is marked in the corresponding subnet.

3.3 EmptyTrapConditions

For a petri net N and an assignment A, find a set S that satisfies

1. S is a trap in the net N.
2. S is unmarked in the inital marking M_0.
3. a transition in $S^\bullet$ is fired in A
4. no transition in $S^\bullet \setminus^\bullet S$ is fired in A

For such a set S, generate a constraint $\delta = \left(\bigvee_{t \in S^\bullet}(t > 0) \implies \bigvee_{t \in {}^\bullet S \setminus S^\bullet}(t > 0)\right)$ to ensure a proper incoming transition is fired if an outgoing transition is fired.

4 Benchmarks

All benchmarks run on petri nets given by Daniel Kroening.

No refinement methods:

		Our tool			
		positive	don't know	timeout 10 min	
Mist	positive	8	3	0	11
	negative	0	28	0	28
	timeout 1 min	15	23	0	38
		23	54	0	77

Trap refinement:

		Our tool			
		positive	don't know	timeout 10 min	
Mist	positive	8	3	0	11
	negative	0	28	0	28
	timeout 1 min	15	23	0	38
		23	54	0	77

Trap refinement and subnet trap refinement:

		Our tool			
		positive	don't know	timeout 10 min	
Mist	positive	8	3	0	11
	negative	0	28	0	28
	timeout 1 min	15	19	4	38
		23	50	4	77

Trap refinement, subnet trap refinement and empty trap refinement:

		Our tool			
		positive	don't know	timeout 10 min	
Mist	positive	8	3	0	11
	negative	0	27	1	28
	timeout 1 min	15	16	7	38
		23	46	8	77

Trap refinement method and state space exploration up to depth 10:

		Our tool				
		positive	negative	don't know	timeout 1 min	
Mist	positive	8	0	3	0	11
	negative	0	2	26	0	28
	timeout 1 min	15	0	18	5	38
		23	2	47	5	77