Recap Decidable problems for PN

BOUNDEDNESS is $\mathcal{R}(N)$ finite

TERMINATION is $\mathcal{RG}(N)$ acyclic

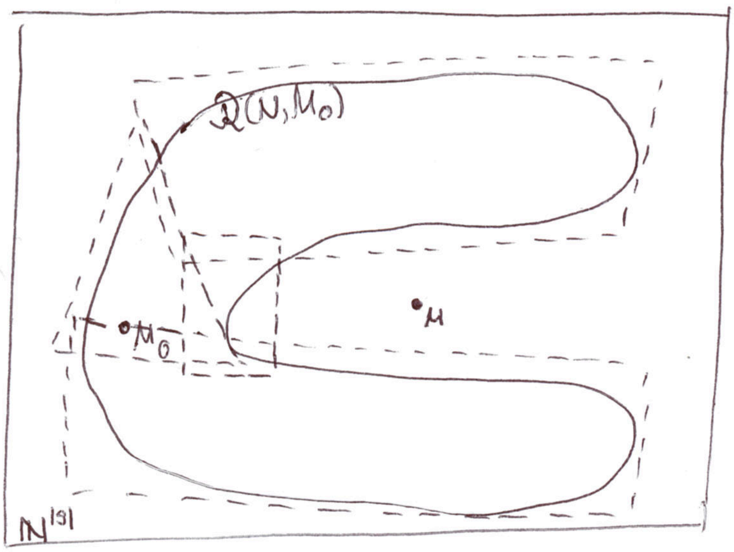
COVERABILITY is $M \in \mathcal{R}(N)\downarrow$
- → K&M non prim rec
- → Rackoff in EXPSPACE
- → Lipton EXPSPACE-hard

(Rackoff + Lipton: EXPSPACE-complete)

REACHABILITY is $M \in \mathcal{R}(N)$ DECIDABLE!

REACHABILITY is $M \in \mathcal{R}(N)$

- Incomplete proof → Sacerslote & Termey
- First proof → Mayr 1981
  → algo had NON PRIM REC complexity
- First simplification → Kosarayu 1982
- Further simplification → Lambert 10 years later
  → Leroux 2009
  → Leroux & Schmitz 2015



① we want to overapprox $\mathcal{R}(N,M_0)$

② Linear ineq are not enough to separate $\mathcal{R}(N,M_0)$ from M (unreach)
↳ source of incompleteness

③ Finite unions of linear sets make the approach complete

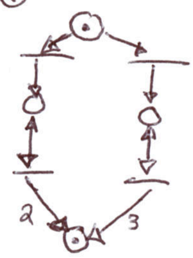
Example

①

$\{1 + 2k_1 + 3k_2 \mid k_1, k_2 \in \mathbb{N}\}$

⟶ Looks fine so far, but:

②

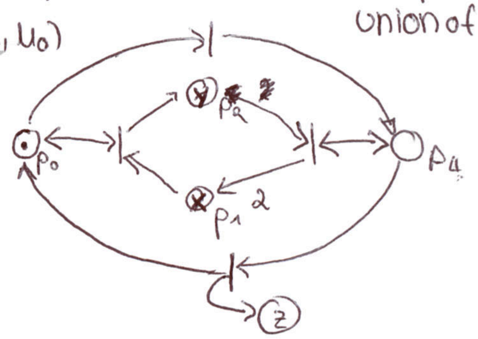


$\left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1+2k_1 \end{pmatrix} \middle| k_1 \in \mathbb{N} \right\}$

$\left\{ \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1+3k_2 \end{pmatrix} \middle| k_2 \in \mathbb{N} \right\}$

③ 5-place Petri-net not representable by union of linear sets

(N, M_0)



$\mathcal{R}(N,M_0) = \{ (1\ x\ y\ z\ 0) \mid 0 < x+y \le 2^z \}$
$\cup \{ (0\ x\ y\ z\ 1) \mid 0 < 2y + x \le 2^z \}$

Def Let $\vec{p} = p_0, \dots, p_n$ be vectors in $\mathbb{N}^k$.
Define

$\mathcal{L}[\vec{p}] := \{ p_0 + k_1 p_1 + \dots + k_n p_n \mid k_i \in \mathbb{N} \}$

A subset $X \subseteq \mathbb{N}^k$ is called LINEAR if there is $\vec{p}$ s.th. $X = \mathcal{L}[\vec{p}]$

A subset of $\mathbb{N}^k$ is called SEMILINEAR if it is a finite union of linear sets

Thm ① For all PN with $|S|<5$. $\mathcal{R}(N,M_0)$ is semilinear.

② there are PN with $|S|=5$ where $\mathcal{R}(N,M_0)$ is NOT semilinear

Def Let $N=(S,T,W)$ be a PN. A set $X\subseteq\mathbb{N}^{|S|}$ is a forward inductive invariant if

$$\forall M\in X \quad \forall t\in T \quad M \xrightarrow{t} M' \Rightarrow {}'\in X$$

Example Let $I\in\mathbb{Z}^{|S|}$ be structural invariant ($I^T C=0$) and $k\in\mathbb{Z}$.

$$A_{I,k}=\{M\in\mathbb{N}^{|S|} \mid I^T M=k\}$$

is called forward inductive invariant

Lemma Let X be a fwd. ind. inv. for a PN N then $\mathcal{R}(N,M_0)\subseteq X$ iff $M\in X$

i.e. fwd ind inv containing M_0 is an overapproximation of $\mathcal{R}(N,M_0)$

Example $I^T M \neq I^T M_0 \Rightarrow M\notin\mathcal{R}(M_0)$

can be represented as

$$M\notin A_{I,I^T M_0} \Rightarrow M\notin\mathcal{R}(N,M_0)$$

MAIN RESULT (Leroux)

Let $M\notin\mathcal{R}(N,M_0)$ then $\exists A\subseteq\mathbb{N}^{|S|}$ semi-linear and fwd. ind. inv. s.th $M_0\in A$ and $M\notin A$

Algorithm for $M\in\mathcal{R}(N,M_0)$

Run two semi algorithms in parallel

(A1) Enumerate semilinear sets A (as PA formula φ_A) and check

a) A fwd ind inv $\Leftrightarrow$ Check ψ_A ist sat

b) $M_0\in A$

c) $M\notin A$

→ terminates if $M\notin\mathcal{R}(N,M_0)$

(A2) Enumate runs trying to find $M_0\xrightarrow{\sigma}M$

→ terminates if $M\in\mathcal{R}(N,M_0)$

Def Presburger Arithmetic FO theory over $(\mathbb{N},+,\leq)$

⇝ $\forall x,\ y=x+z,\ x\leq y,\ x\equiv_k y$

Def $X\subseteq\mathbb{N}^k$ is PA-definable if $\exists$ formula in PA with k free var so that

$$X=\left\{\begin{pmatrix} I(x_0)\\ I(x_1)\\ \vdots\\ I(x_k)\end{pmatrix} \,\middle|\, I\models\varphi(\vec{x})\right\}$$

Fact:

① X is semilinear $\Leftrightarrow$ X is PA-definable

② Satisfiability for PA is decidable

Construction

Given $\varphi(\vec{x})$ as PA formula, we constr. a PA formula ψ that is sat iff φ describes a fwd ind. inv.

$$\psi\equiv\underline{\forall M\in\mathbb{N}^{|S|}}\ \forall M'\in\mathbb{N}^{|S|}:\ \Big(\varphi(M)\wedge\bigvee_{t\in T}\underline{M\xrightarrow{t}M'}\Rightarrow\varphi(M')\Big)$$

↳ $\forall m_1\ldots\forall m_k$

↳ $m_1\geq 1\wedge m_2'=m_2+2$

Liveness properties

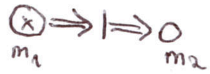
using LTL

① state based ⇝ proposition are places
UNDECIDABLE

② action based ⇝ prop are labels of transitions
DECIDABLE

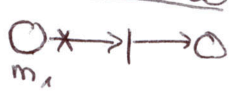
Extensions of Petri nets

① transfer arcs



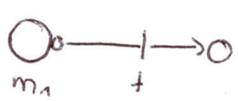
moves all token from m_1 and m_2

② reset arcs



removes all tokens from m_1

③ zero tests



t only fired if $M(m_1)=0$

⇝ all problem undecidable

For ① and ② some decidable

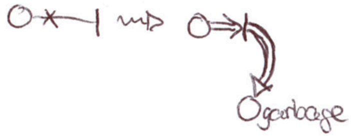
Overview

	PN	TN	RN	IN
TERMINATION	D	D ①	D ①	U
REACHABILITY	D	U	U	③ U
BOUNDEDNESS	D	D ①	② U ④	U
PLACE BOUNDEDNESS	D ⓪	U ②	② U	U
COVERABILITY	D	D	② D	U

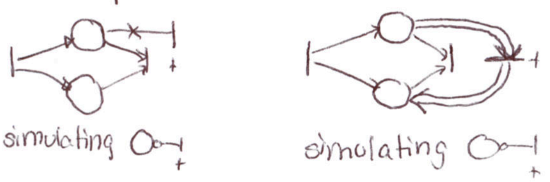
⓪ by KM

① by exercise extending algo for PN

② by garbage place



③ by twin places



simulating

simulating

④ by red of Diophantine eqs

Note by ④ COV for TN, RN cannot be done by adapting K&M

Note PN + 1 inhibitor arc have decidable coverability

Def QOTS $(S, \to, \leq)$ quasi ordered transition sys

① S set of configurations (tipically infinite)

② $\to \subseteq S \times S$ transition relation

③ $\leq \subseteq S \times S$ qo

To replace the termination algorithm from PN we need

① finite branching

② monotonicity

③ $(S, \leq)$ is wqo

monotonicity

$$\forall \quad \begin{array}{ccc} N & \longrightarrow^* & N' \\ \rotatebox{90}{$\leq$} & & \rotatebox{90}{$\leq$} \\ M & \longrightarrow^* & M' \end{array} \quad \exists$$

Def Well Structured Transition Systems (WSTS) is a QOTS $(S, \to, \leq)$ such that

① $(S, \leq)$ is wqo

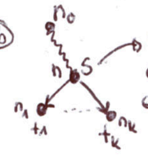
② $\leq$ is a simulation: $\forall \underbrace{s_1 \leq t_1}_{\in S}$ and $s_1 \to s_2$, $\exists t_2 : t_1 \to^{\circledast} t_2 \geq s_2$

$\circledast = *$ weak simulation

$\circledast = +$ transitive simulation

Def Let $s_0 \in S$. FRT(s_0) (finite reach tree from s_0) is a S-labelled directed so that

ⓐ root n_0 is labelled by s_0

ⓑ 

s has a child for each transition $s \to t_i$ — if $\nexists n'$ in the path from n_0 to n that is labelled with s' s.th. $s' \leq s$

n has no child — otherwise ⟿ we say n is subsumed by n'

Note: $s, s', t_1, \dots, t_k \in S$ ⟿ labels, $n, n', n_0 \dots n_k$ nodes

Lemma FRT(s) is finite for every finitely branching WSTS.

Proof by König's lemma: if FRT(s) is inf, it contains an infinite path. By wqo $\leq$ such an infinite path would contain a subsumed node. But that node has no successor by construction ↯

Lemma (WSTS with transitive simulation) $(S, \to, \leq)$ has a non terminating computation tree from $s_0 \in S$ if and only if FRT(s_0) contains a subsumed node.

Proof ($\Rightarrow$) let π be infinite computation from s_0 then $\pi = \pi_1 \pi_2$. π_1 finite labelling a maximum path from the root of FRT(s_0). Since the last node in this path is a leaf, and has no successors (by $\exists \pi$) so n is missed

($\Leftarrow$) $\underset{n_0}{s_0} \longrightarrow^* \underset{n'}{t_1} \longrightarrow^+ \underset{n}{t_2} \geq t_1 \Rightarrow$ by simulation

$s_0 \longrightarrow^* t_1 \longrightarrow^+ t_2 \longrightarrow^* t_3 \geq t_2$

In other words

$$\begin{array}{ccc} t_2 & \longrightarrow^+ & t_3 \\ \rotatebox{90}{$\leq$} & & \rotatebox{90}{$\leq$} \\ t_1 & \longrightarrow^+ & t_2 \end{array}$$

obtain an infinite computation $t_1 \longrightarrow^+ t_2$

Thm TERMINATION is decidable for finitely branching transitive WSTS.