Model Checking Coverability Graphs of Vector Addition Systems

Michel Blockelet and Sylvain Schmitz

LSV, ENS Cachan & CNRS, Cachan, France

MFCS 2011, Warsaw, August 25, 2011

Outline

"coverability-like"-properties

known ExpSpace-complete properties for VAS: coverability, boundedness, regularity, ...

this talk

a unifying view based on VAS coverability graphs and CTL model checking

contents

Vector Addition Systems

$\mathcal{S} = \langle \mathsf{V}, \mathsf{x}_0 \rangle$

- V: a finite set of transitions in $\mathbb{Z}^k$,
- x_0: an initial configuration in $\mathbb{N}^k$
- semantics: for x, x' in $\mathbb{N}^k$ and a in V, $\mathsf{x} \xrightarrow{\mathsf{a}} \mathsf{x}'$ iff $\mathsf{x} + \mathsf{a} = \mathsf{x}'$

Example

$\mathcal{S} = \langle \{\mathsf{a}, \mathsf{b}, \mathsf{c}\}, \langle 1, 0, 1 \rangle \rangle$ with transitions $\mathsf{a} = \langle 1, 1, -1 \rangle$, $\mathsf{b} = \langle -1, 0, 1 \rangle$, and $\mathsf{c} = \langle 0, -1, 0 \rangle$:

$$\langle 1, 0, 1 \rangle \xrightarrow{\mathsf{a}} \langle 2, 1, 0 \rangle \stackrel{\mathsf{a}}{\not\rightarrow}$$

Coverability Graph

- finite abstraction of the VAS reachability graph
- allows to decide various properties of the VAS
  (coverability, boundedness, place boundedness, regularity, reversal boundedness, trace boundedness, LTL model-checking, ...)
- but of non-primitive recursive size!
  (Cardoza et al., 1976)

Coverability Tree

(Karp and Miller, 1969)

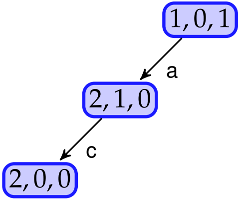
$\mathsf{a} = \langle 1, 1, -1 \rangle$, $\mathsf{b} = \langle -1, 0, 1 \rangle$, $\mathsf{c} = \langle 0, -1, 0 \rangle$:

$\boxed{1, 0, 1}$

Coverability Tree

(Karp and Miller, 1969)

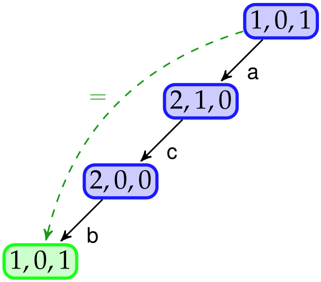
a $= \langle 1, 1, -1\rangle$, b $= \langle -1, 0, 1\rangle$, c $= \langle 0, -1, 0\rangle$:



Coverability Tree

(Karp and Miller, 1969)

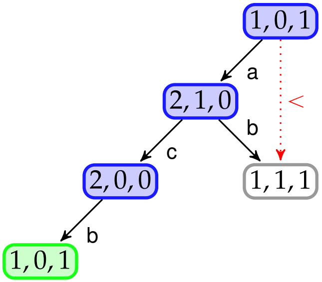
a $= \langle 1, 1, -1 \rangle$, b $= \langle -1, 0, 1 \rangle$, c $= \langle 0, -1, 0 \rangle$:



Coverability Tree

(Karp and Miller, 1969)

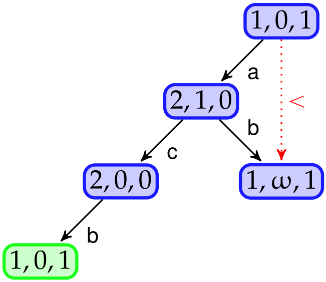
a $= \langle 1, 1, -1 \rangle$, b $= \langle -1, 0, 1 \rangle$, c $= \langle 0, -1, 0 \rangle$:



Coverability Tree

(Karp and Miller, 1969)

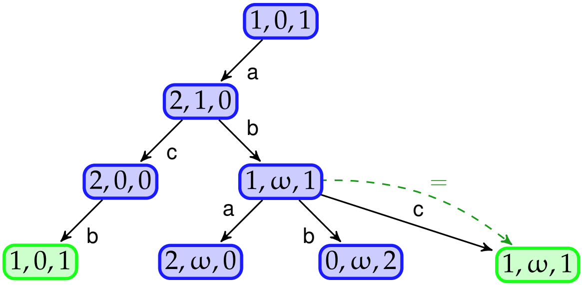
a $= \langle 1,1,-1\rangle$, b $= \langle -1,0,1\rangle$, c $= \langle 0,-1,0\rangle$:



Coverability Tree

(Karp and Miller, 1969)

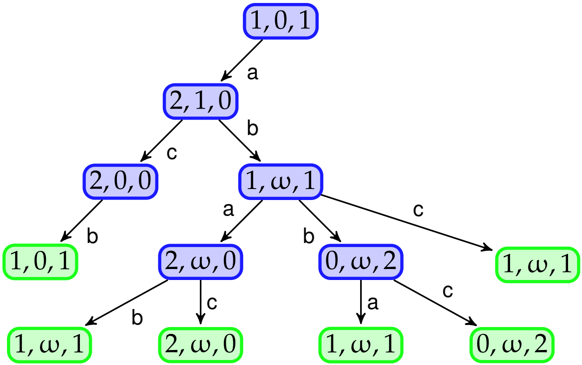
a $= \langle 1, 1, -1\rangle$, b $= \langle -1, 0, 1\rangle$, c $= \langle 0, -1, 0\rangle$:



Coverability Tree

(Karp and Miller, 1969)

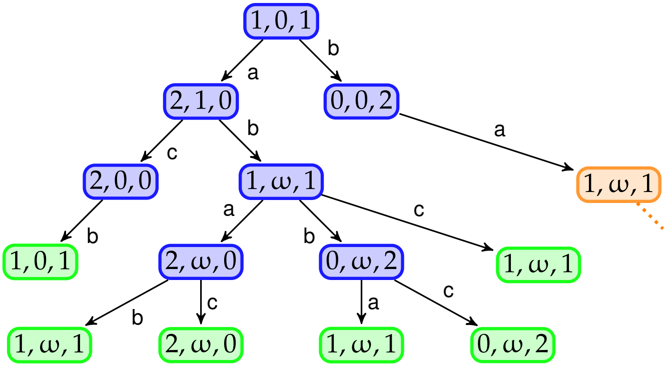
a $= \langle 1, 1, -1 \rangle$, b $= \langle -1, 0, 1 \rangle$, c $= \langle 0, -1, 0 \rangle$:



Coverability Tree

(Karp and Miller, 1969)

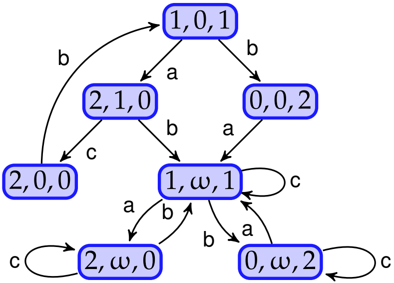
$\mathsf{a} = \langle 1, 1, -1 \rangle$, $\mathsf{b} = \langle -1, 0, 1 \rangle$, $\mathsf{c} = \langle 0, -1, 0 \rangle$:



Coverability Graph

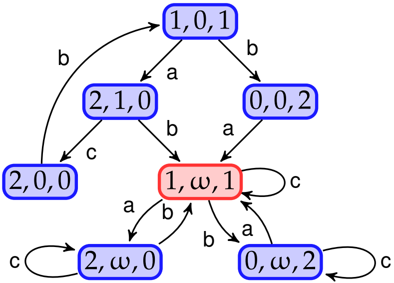
(Valk and Vidal-Naquet, 1981)

a $= \langle 1, 1, -1 \rangle$, b $= \langle -1, 0, 1 \rangle$, c $= \langle 0, -1, 0 \rangle$:



Coverability Graph

a $= \langle 1,1,-1\rangle$, b $= \langle -1,0,1\rangle$, c $= \langle 0,-1,0\rangle$:



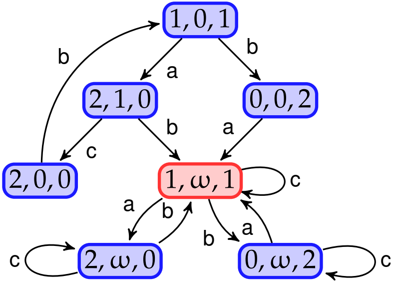
coverability:

is some x $\geqslant \langle 1,5,1\rangle$ reachable?

(Karp and Miller, 1969)

Coverability Graph

$\mathsf{a} = \langle 1, 1, -1 \rangle$, $\mathsf{b} = \langle -1, 0, 1 \rangle$, $\mathsf{c} = \langle 0, -1, 0 \rangle$:



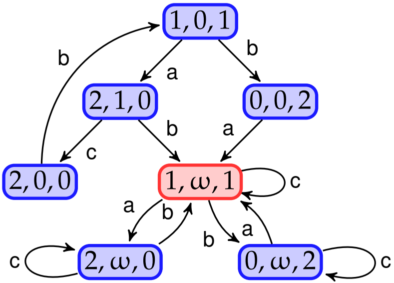
boundedness:

is the set of reachable configurations finite?

(Karp and Miller, 1969)

Coverability Graph

a $= \langle 1, 1, -1 \rangle$, b $= \langle -1, 0, 1 \rangle$, c $= \langle 0, -1, 0 \rangle$:

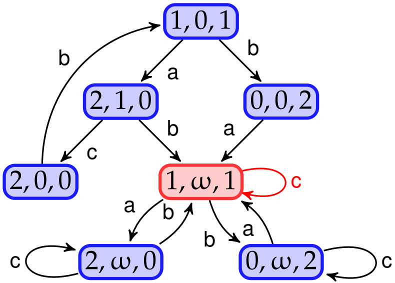


place boundedness:

is the set of reachable values on coordinate 2 finite?

Coverability Graph

$a = \langle 1, 1, -1 \rangle$, $b = \langle -1, 0, 1 \rangle$, $c = \langle 0, -1, 0 \rangle$:



regularity:

is the set $L = \{w \in V^* \mid \exists x \in \mathbb{N}^k, x_0 \xrightarrow{w} x\}$ regular?

(Valk and Vidal-Naquet, 1981)

(no: $L \cap (ab)^* c^* = (ab)^n c^{\leqslant n}$)

Coverability Graph

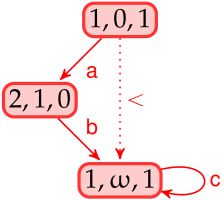
- finite abstraction of the VAS reachability graph
- allows to decide various properties of the VAS
  (coverability, boundedness, place boundedness, regularity, reversal boundedness, trace boundedness, LTL model-checking, ...)
- but of non-primitive recursive size!
  (Cardoza et al., 1976)

Coverability Graph

- finite abstraction of the VAS reachability graph
- allows to decide various properties of the VAS
  (coverability, boundedness, place boundedness, regularity, reversal boundedness, trace boundedness, LTL model-checking, . . .)
- but of non-primitive recursive size!
  (Cardoza et al., 1976)

Partial Cover

$\mathsf{a} = \langle 1, 1, -1\rangle$, $\mathsf{b} = \langle -1, 0, 1\rangle$, $\mathsf{c} = \langle 0, -1, 0\rangle$:



Idea of the paper: a "small" witness for coverability, boundedness, place boundedness, regularity, . . .

based on Rackoff (1978)

$\mathrm{PrECTL}_{\geqslant}(\mathsf{F})$

Syntax

$$\varphi ::= \top \mid \bot \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \mathsf{EF}_{\psi}\varphi \mid \mu(j) \geqslant c$$

with $c \in \mathbb{N} \cup \{\omega\}$ and ψ a QFP formula with k free variables

Semantics

Over partial covers:

$$\begin{aligned} s \models \mathsf{EF}_{\psi}\varphi \quad & \text{iff } \exists \pi = s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} \cdots \in \mathit{Paths}(s), \exists n \leqslant |\pi|, \\ & \qquad \mathrm{PA} \models \psi\Big(\sum_{i=1}^{n} a_i\Big) \text{ and } s_n \models \varphi, \\ s \models \mu(j) \geqslant c \quad & \text{iff } \ell(s)(j) \geqslant c\,. \end{aligned}$$

$\mathrm{PrECTL}_{\geqslant}(\mathsf{F})$

Syntax

$$\varphi ::= \top \mid \bot \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \mathsf{EF}_{\psi}\varphi \mid \mu(j) \geqslant c$$

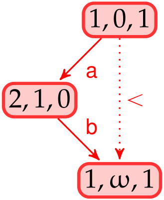
with $c \in \mathbb{N} \cup \{\omega\}$ and ψ a QFP formula with k free variables

Semantics

Over VAS: $\langle \mathsf{V}, \mathsf{x}_0 \rangle \models \varphi$ if $\exists$ partial cover $\mathcal{C}$ s.t. $\mathcal{C} \models \varphi$

Examples

$\mathsf{a} = \langle 1, 1, -1 \rangle$, $\mathsf{b} = \langle -1, 0, 1 \rangle$, $\mathsf{c} = \langle 0, -1, 0 \rangle$:



coverability of x:

$$\mathsf{EF} \bigwedge_{j=1}^{k} \mu(j) \geqslant \mathsf{x}(j)$$

Examples

$\mathsf{a} = \langle 1, 1, -1 \rangle$, $\mathsf{b} = \langle -1, 0, 1 \rangle$, $\mathsf{c} = \langle 0, -1, 0 \rangle$:

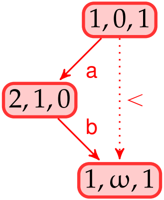
$$\begin{tikzcd}
 & \boxed{1,0,1} \arrow[dl, "\mathsf{a}"] \arrow[dd, dotted, "<"] \\
\boxed{2,1,0} \arrow[dr, "\mathsf{b}"] & \\
 & \boxed{1,\omega,1}
\end{tikzcd}$$

unboundedness:

$$\mathsf{EF} \bigvee_{j=1}^{k} \mu(j) \geqslant \omega$$

Examples

$\mathsf{a} = \langle 1, 1, -1 \rangle$, $\mathsf{b} = \langle -1, 0, 1 \rangle$, $\mathsf{c} = \langle 0, -1, 0 \rangle$:



place unboundedness of j:

$$\mathsf{EF}\mu(j) \geqslant \omega$$

Examples

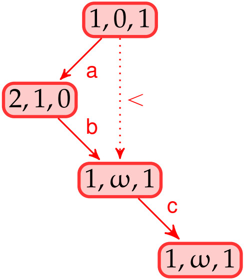
non-regularity:

$$\mathsf{EF} \bigvee_{\substack{I \subseteq \{1,\ldots,k\} \\ I \neq \emptyset}} \bigvee_{I \subseteq J \subseteq \{1,\ldots,k\}} \left(\bigwedge_{j \in J} \mu(j) \geqslant \omega \wedge \mathsf{EF}_{\psi_{I,J}} \top \right)$$

$$\psi_{I,J}(x_1, \ldots, x_k) = \bigwedge_{j \in I} x_j < 0 \wedge \bigwedge_{j \notin J} x_j \geqslant 0$$

Examples

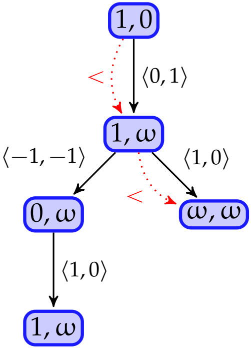
a $= \langle 1, 1, -1 \rangle$, b $= \langle -1, 0, 1 \rangle$, c $= \langle 0, -1, 0 \rangle$:



non-regularity

(Eventually) Increasing Formulæ

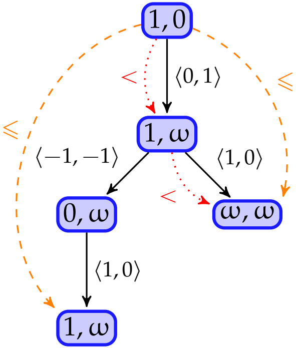
$$\mathsf{EF}_{x_1 \geqslant 0}\,(\mu(2) \geqslant \omega \wedge \mathsf{EF}_{x_1 \geqslant 0 \wedge x_2 < 0} \top \wedge \mathsf{EF}\mu(1) \geqslant \omega)$$



- $\mathrm{PrECTL}_{\geqslant}(\mathsf{F})$ formulæ have *finite tree models*
- *increasing* formulæ
- *eventually increasing* formulæ ($\mathrm{eiPrECTL}_{\geqslant}(\mathsf{F})$): $\mathsf{EF}\varphi$ where φ is increasing

(Eventually) Increasing Formulæ

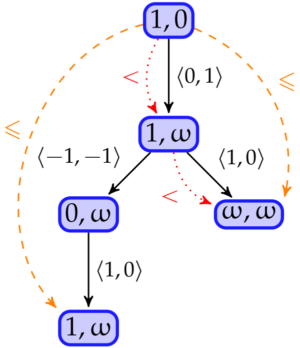
$$\mathsf{EF}_{x_1 \geqslant 0}\,(\mu(2) \geqslant \omega \wedge \mathsf{EF}_{x_1 \geqslant 0 \wedge x_2 < 0} \top \wedge \mathsf{EF}\mu(1) \geqslant \omega)$$



- $\mathrm{PrECTL}_{\geqslant}(\mathsf{F})$ formulæ have *finite tree models*
- *increasing* formulæ
- *eventually increasing* formulæ ($\mathrm{eiPrECTL}_{\geqslant}(\mathsf{F})$): $\mathsf{EF}\varphi$ where φ is increasing

(Eventually) Increasing Formulæ

$$\mathsf{EF}_{x_1 \geqslant 0}\,(\mu(2) \geqslant \omega \wedge \mathsf{EF}_{x_1 \geqslant 0 \wedge x_2 < 0}\top \wedge \mathsf{EF}\mu(1) \geqslant \omega)$$



- $\mathrm{PrECTL}_{\geqslant}(\mathsf{F})$ formulæ have *finite tree models*
- *increasing* formulæ
- *eventually increasing* formulæ ($\mathrm{eiPrECTL}_{\geqslant}(\mathsf{F})$): $\mathsf{EF}\varphi$ where φ is increasing

Complexity

Theorem

The VAS model-checking problem for eiPrECTL$_{\geqslant}(\mathsf{F})$ formulæ is ExpSpace*-complete.*

- lower bound: coverability (Cardoza et al., 1976),
- upper bound: small model ($\sim 2^{2^{O(k)\cdot|\mathsf{V}|\cdot|\varphi|}}$)

Proof Idea

(based on Rackoff, 1978)

Construct a small model by induction on i, $0 \leqslant i \leqslant k$:

- allow negative values in coordinates $j > i$ in models,
- ignore coverability constraints $\mu(j) \geqslant c$ for $j > i$ and $c < \omega$ (noted $\varphi_{|_i}$)
- called i-*admissible* models.

Small Bounded Models

(based on Rackoff, 1978)

(i, r)-*bounded* partial cover: all finite values on coordinates $\leqslant i$ are $< r$.

Lemma

$\mathcal{C} \models \varphi_{|_i}$ *and* $\mathcal{C}$ (i, r)*-bounded imply* $\exists \mathcal{C}', \mathcal{C}' \models \varphi_{|_i}$ *with* $|\mathcal{C}'| \leqslant (2^{|V|}r)^{(k+|\varphi|)^d}$ *for some constant* d.

(based on small solutions to QFP/LIP instances, e.g. Papadimitriou, 1981)

Main Induction

(using ideas from Rackoff, 1978; Atig and Habermehl, 2011)

Small i-admissible model of size $\leqslant g(i)$ *regardless of initial state*:

- base $i = 0$:
  $g(0)$ by reduction to LIP,
- ind. step $i + 1$:
  set $r = 2^{|V|} \cdot g(i) + 2^{|\varphi|}$
  - $(i + 1, r)$-bounded: use small bounded model,
  - not $(i + 1, r)$-bounded

finally: $g(k) \leqslant 2^{2^{kd} \cdot |V| \cdot |\varphi|}$.

Main Induction

(using ideas from Rackoff, 1978; Atig and Habermehl, 2011)

Small i-admissible model of size $\leqslant g(i)$ *regardless of initial state*:

- base $i = 0$:
  $g(0)$ by reduction to LIP,
- ind. step $i + 1$:
  set $r = 2^{|V|} \cdot g(i) + 2^{|\varphi|}$
  - $(i + 1, r)$-bounded: use small bounded model,
  - not $(i + 1, r)$-bounded

finally: $g(k) \leqslant 2^{2^{kd} \cdot |V| \cdot |\varphi|}$.

Main Induction

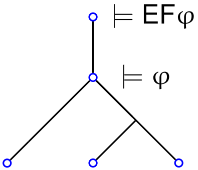
(using ideas from Rackoff, 1978; Atig and Habermehl, 2011)

Small i-admissible model of size $\leqslant g(i)$ *regardless of initial state*:

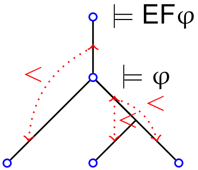
- base $i = 0$:
  $g(0)$ by reduction to LIP,
- ind. step $i + 1$:
  set $r = 2^{|V|} \cdot g(i) + 2^{|\varphi|}$
  - $(i + 1, r)$-bounded: use small bounded model,
  - not $(i + 1, r)$-bounded

finally: $g(k) \leqslant 2^{2^{kd} \cdot |V| \cdot |\varphi|}$.

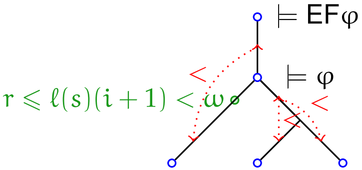
Case Not $(i + 1, r)$-Bounded



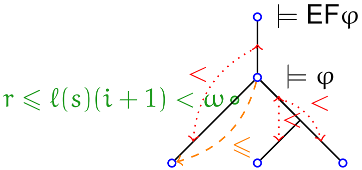
Case Not $(i+1, r)$-Bounded



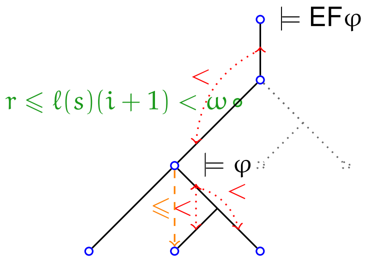
Case Not $(i+1, r)$-Bounded



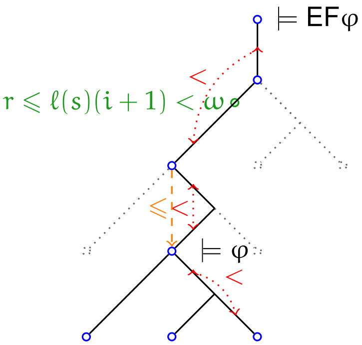
Case Not $(i+1, r)$-Bounded



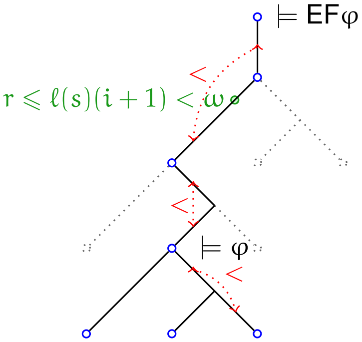
Case Not $(i+1, r)$-Bounded



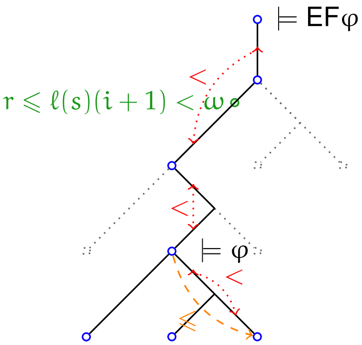
Case Not $(i+1,r)$-Bounded



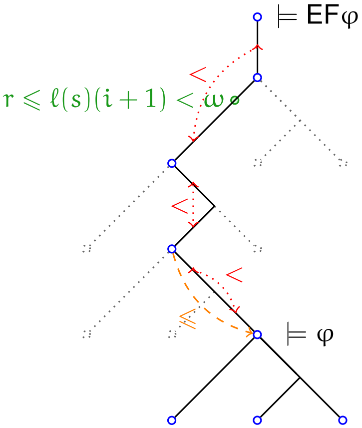
Case Not $(i+1, r)$-Bounded



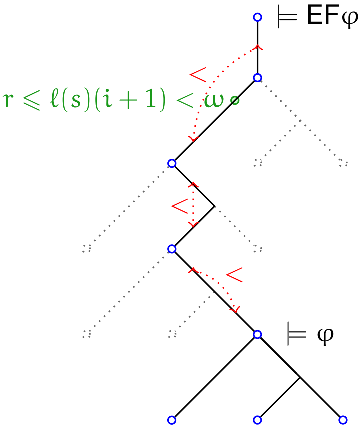
Case Not $(i+1, r)$-Bounded



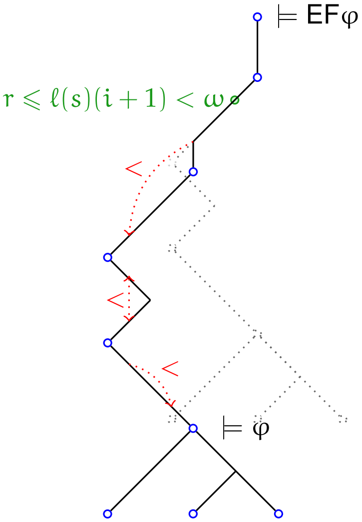
Case Not $(i+1, r)$-Bounded



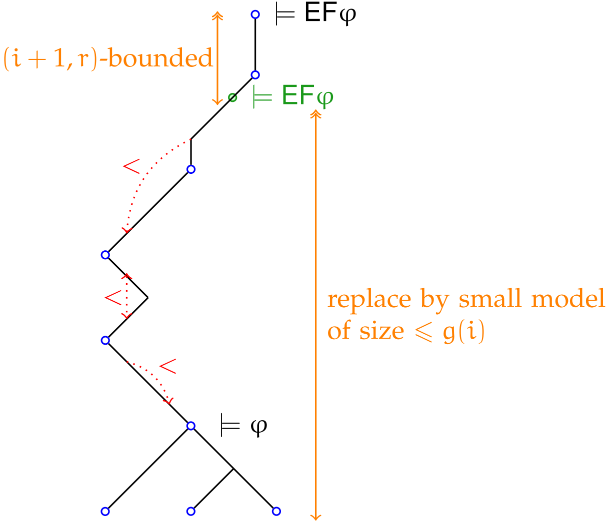
Case Not $(i + 1, r)$-Bounded



Case Not $(i+1, r)$-Bounded



Case Not $(i+1, r)$-Bounded



Main Induction

(using ideas from Rackoff, 1978; Atig and Habermehl, 2011)

Small i-admissible model of size $\leqslant g(i)$ *regardless of initial state*:

- base $i = 0$:
  $g(0)$ by reduction to LIP,
- ind. step $i + 1$:
  set $r = 2^{|V|} \cdot g(i) + 2^{|\varphi|}$
  - $(i+1, r)$-bounded: use small bounded model,
  - not $(i+1, r)$-bounded

finally: $g(k) \leqslant 2^{2^{kd} \cdot |V| \cdot |\varphi|}$.

Concluding Remarks

- a characterization of “coverability-like” properties
- simpler to use than (Yen, 1992; Atig and Habermehl, 2011; Demri, 2010)
- see paper for more: decidability/undecidability of larger fragments, satisfiability, etc.

References

Atig, M.F. and Habermehl, P., 2011. On Yen's path logic for Petri nets. *Int. J. Fund. Comput. Sci.*, 22(4):783–799. doi:10.1142/S0129054111008428.

Cardoza, E., Lipton, R.J., and Meyer, A.R., 1976. Exponential space complete problems for Petri nets and commutative semigroups. In *STOC'76*, pages 50–54. ACM Press. doi:10.1145/800113.803630.

Demri, S., 2010. On selective unboundedness of VASS. In Chen, Y.F. and Rezine, A., editors, *INFINITY 2010*, volume 39 of *Elec. Proc. in Theor. Comput. Sci.*, pages 1–15. doi:10.4204/EPTCS.39.1.

Karp, R.M. and Miller, R.E., 1969. Parallel program schemata. *Journal of Computer and System Sciences*, 3(2):147–195. doi:10.1016/S0022-0000(69)80011-5.

Papadimitriou, C.H., 1981. On the complexity of integer programming. *Journal of the ACM*, 28(4):765–768. doi:10.1145/322276.322287.

Rackoff, C., 1978. The covering and boundedness problems for vector addition systems. *Theor. Comput. Sci.*, 6(2):223–231. doi:10.1016/0304-3975(78)90036-1.

Valk, R. and Vidal-Naquet, G., 1981. Petri nets and regular languages. *Journal of Computer and System Sciences*, 23(3):299–325. doi:10.1016/0022-0000(81)90067-2.

Yen, H.C., 1992. A unified approach for deciding the existence of certain Petri net paths. *Inform. and Comput.*, 96(1):119–137. doi:10.1016/0890-5401(92)90059-O.