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

Coverability Graphs
CTL Model Checking
Small Model Properties
Vector Addition Systems

\[ S = \langle V, x_0 \rangle \]

- \( V \): 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 \( V \), \( x \xrightarrow{a} x' \) iff \( x + a = x' \)

Example

\[ S = \langle \{ a, b, c \}, \langle 1, 0, 1 \rangle \rangle \] with transitions \( a = \langle 1, 1, -1 \rangle \), \( b = \langle -1, 0, 1 \rangle \), and \( c = \langle 0, -1, 0 \rangle \):

\[ \langle 1, 0, 1 \rangle \xrightarrow{a} \langle 2, 1, 0 \rangle \xrightarrow{a} \]
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)

\( a = \langle 1, 1, -1 \rangle, \ b = \langle -1, 0, 1 \rangle, \ c = \langle 0, -1, 0 \rangle: \)
Coverability Tree

(Karp and Miller, 1969)

\[ a = \langle 1, 1, -1 \rangle, \quad b = \langle -1, 0, 1 \rangle, \quad c = \langle 0, -1, 0 \rangle: \]
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)

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

\[
\begin{align*}
&1, 0, 1 \\
\text{a} & \rightarrow 2, 1, 0 \\
\text{b} & \rightarrow 2, 0, 0 \\
& 1, \omega, 1 \\
\text{c} & \rightarrow 1, 0, 1 \\
\text{b} & \rightarrow 2, \omega, 0 \\
& 1, \omega, 1 \\
\text{c} & \rightarrow 1, \omega, 1 \\
& 2, \omega, 0 \\
\text{a} & \rightarrow 0, \omega, 2 \\
\text{b} & \rightarrow 1, \omega, 1 \\
& 0, \omega, 2 \\
\text{c} & \rightarrow 0, \omega, 2
\end{align*}
\]
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 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

\[ \mathbf{a} = \langle 1, 1, -1 \rangle, \mathbf{b} = \langle -1, 0, 1 \rangle, \mathbf{c} = \langle 0, -1, 0 \rangle: \]

**coverability:**

is some \( x \geq \langle 1, 5, 1 \rangle \) reachable?

(Karp and Miller, 1969)
Coverability Graph

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

**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

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

\[
\begin{align*}
\text{regularity:} \quad & \quad \text{is the set } L = \{ w \in V^* \mid \\
& \quad \exists x \in \mathbb{N}^k, x_0 \xrightarrow{w} x \} \text{ regular?} \\
& \quad \text{(Valk and Vidal-Naquet, 1981)} \\
& \quad (\text{no: } L \cap (ab)^*c^* = (ab)^n c^{\leq n})
\end{align*}
\]
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

\[ a = \langle 1, 1, -1 \rangle, \quad b = \langle -1, 0, 1 \rangle, \quad c = \langle 0, -1, 0 \rangle: \]

Idea of the paper: a “small” witness for coverability, boundedness, place boundedness, regularity, …

based on Rackoff (1978)
PrECTL\(\geq (F)\)

**Syntax**

\[ \varphi ::= \top | \bot | \varphi \lor \varphi | \varphi \land \varphi | \text{EF}_\psi \varphi | \mu(j) \geq c \]

with \(c \in \mathbb{N} \cup \{\omega\}\) and \(\psi\) a QFP formula with \(k\) free variables

**Semantics**

Over partial covers:

\[ s \models \text{EF}_\psi \varphi \quad \text{iff} \quad \exists \pi = s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} \cdots \in \text{Paths}(s), \exists n \leq |\pi|, \]

\[ \text{PA} \models \psi(\sum_{i=1}^{n} a_i) \] and \(s_n \models \varphi, \]

\[ s \models \mu(j) \geq c \quad \text{iff} \quad \ell(s)(j) \geq c. \]
PrECTL\(\geq(F)\)

Syntax

\[ \phi ::= \top \mid \perp \mid \phi \lor \phi \mid \phi \land \phi \mid EF\psi \phi \mid \mu(j) \geq c \]

with \(c \in \mathbb{N} \cup \{\omega\}\) and \(\psi\) a QFP formula with \(k\) free variables

Semantics

Over VAS: \(\langle V, x_0 \rangle \models \phi\) if \(\exists\) partial cover \(\mathcal{C}\) s.t. \(\mathcal{C} \models \phi\)
Examples

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

\[
\begin{align*}
1, 0, 1 & \quad a \quad 2, 1, 0 \quad b \\
1, 0, 1 & \quad b \quad 1, \omega, 1
\end{align*}
\]

coverability of \( x: \)

\[
\text{EF} \bigwedge_{j=1}^{k} \mu(j) \geq x(j)
\]
**Examples**

\[ a = \langle 1, 1, -1 \rangle, \quad b = \langle -1, 0, 1 \rangle, \quad c = \langle 0, -1, 0 \rangle: \]

\[
\begin{align*}
1, 0, 1 \\
\uparrow \quad a \\
2, 1, 0 \\
\downarrow b \\
1, \omega, 1 \\
\end{align*}
\]

**unboundedness:**

\[
\text{EF} \bigvee_{j=1}^{k} \mu(j) \geq \omega
\]
Examples

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

\[
\begin{array}{c}
1, 0, 1 \\
2, 1, 0 \\
1, \omega, 1
\end{array}
\]

place unboundedness of \(j:\)

\[\text{EF} \mu(j) \geq \omega\]
Examples

**non-regularity:**

\[
\begin{align*}
\operatorname{EF} & \bigvee_{I \subseteq \{1, \ldots, k\} \atop I \neq \emptyset} \bigvee_{J \subseteq \{1, \ldots, k\}} \\
& \left( \bigwedge_{j \in J} \mu(j) \geq \omega \land \operatorname{EF}_{\psi_{I,J}} \top \right) \\
\psi_{I,J}(x_1, \ldots, x_k) & = \bigwedge_{j \in I} x_j < 0 \land \bigwedge_{j \notin J} x_j \geq 0
\end{align*}
\]
Examples

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

\[
\begin{array}{c}
1, 0, 1 \\
2, 1, 0 \\
1, \omega, 1 \\
1, \omega, 1
\end{array}
\]

\( a \rightarrow \langle 1, 0, 1 \rangle \)
\( b \rightarrow \langle 2, 1, 0 \rangle \)
\( c \rightarrow \langle 1, \omega, 1 \rangle \)

\text{non-regularity}
(Eventually) Increasing Formulae

\[ \text{EF}_{x_1 \geq 0} (\mu(2) \geq \omega) \land \text{EF}_{x_1 \geq 0 \land x_2 < 0} \top \land \text{EF} \mu(1) \geq \omega) \]

- **PrECTL\(_\geq\)(F) formulae** have *finite tree models*
- **increasing formulae**
- **eventually increasing formulae** (eiPrECTL\(_\geq\)(F)):

  \[ \text{EF} \varphi \text{ where } \varphi \text{ is increasing} \]
(Eventually) Increasing Formulae

$$\text{EF}_{x_1 \geq 0} (\mu(2) \geq \omega \land \text{EF}_{x_1 \geq 0 \land x_2 < 0} \top \land \text{EF} \mu(1) \geq \omega)$$

- \(\text{PrECTL}_{\geq} (F)\) formulae have finite tree models
- increasing formulae
- eventually increasing formulae (\(\text{eiPrECTL}_{\geq} (F)\)): \(\text{EF} \phi\) where \(\phi\) is increasing
(Eventually) Increasing Formulae

$$\text{EF}_{x_1 \geq 0} (\mu(2) \geq \omega \land \text{EF}_{x_1 \geq 0 \land x_2 < 0} \top \land \text{EF} \mu(1) \geq \omega)$$

- PrECTL$\geq$(F) formulae have finite tree models
- increasing formulae
- eventually increasing formulae (eiPrECTL$\geq$(F)):
  $\text{EF} \varphi$ where $\varphi$ is increasing
Complexity

Theorem

The VAS model-checking problem for $\text{eiPrECTL} \ supseteq (F)$ formulæ is ExpSPACE-complete.

- lower bound: coverability (Cardoza et al., 1976),
- upper bound: small model ($\sim 2^{O(k)} \cdot |V| \cdot |\varphi|$)
Proof Idea
(based on Rackoff, 1978)

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

- allow negative values in coordinates $j > i$ in models,
- ignore coverability constraints $\mu(j) \geq c$ 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 \(\leq i\) are \(< r\).

Lemma
\([C \models \varphi_i \text{ and } C \text{ (i, r)-bounded imply } \exists C', C' \models \varphi_i \text{ with } |C'| \leq (2^{|V|r})^{(k+|\varphi|)^d} \text{ for some constant } d.}\)

(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 $\leq g(i)$ regardless of initial state:

- **base i = 0:**
  $\quad g(0)$ 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: $g(k) \leq 2^{2^kd \cdot |V| \cdot |\varphi|}$. 
Main Induction
(using ideas from Rackoff, 1978; Atig and Habermehl, 2011)

Small $i$-admissible model of size $\leq g(i)$ 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: $g(k) \leq 2^{2^{|V| \cdot |\varphi|}}$. 
Main Induction
(using ideas from Rackoff, 1978; Atig and Habermehl, 2011)

Small $i$-admissible model of size $\leq g(i)$ 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: $g(k) \leq 2^{2^{kd} \cdot |V| \cdot |\varphi|}$. 
Case Not \((i + 1, r)\)-Bounded

\[ \models \text{EF} \varphi \]

\[ \models \varphi \]
Case Not $(i+1, r)$-Bounded

\[ |= \text{EF} \varphi \]

\[ |= \varphi \]
Case Not \((i + 1, r)\)-Bounded

\[ r \leq \ell(s)(i + 1) < \omega \]

\[ \models \mathbf{EF} \varphi \]

\[ \models \varphi \]
Case Not \((i + 1, r)\)-Bounded

\[ r \leq \ell(s)(i + 1) < \omega \]

\[ \models \text{EF} \varphi \]

\[ \models \varphi \]
Case Not \((i + 1, r)\)-Bounded

\[ r \leq \ell(s)(i + 1) < \omega \]

\[ \models EF \varphi \]

\[ \models \varphi \]

\[ \models \]
Case Not (i + 1, r)-Bounded

\[ r \leq \ell(s)(i + 1) < \omega \]

\[ \models EF \varphi \]
Case Not \((i + 1, r)\)-Bounded

\[ r \leq \ell(s)(i + 1) < \omega \]

\[ \models \varphi \]

\[ \models \mathbf{EF} \varphi \]
Case Not \((i + 1, r)\)-Bounded

\[ r \leq \ell(s)(i + 1) < \omega \]

\[ \models \text{EF} \varphi \]

\[ \models \varphi \]
Case Not $(i + 1, r)$-Bounded

$$r \leq \ell(s)(i + 1) < \omega$$

$$\models EF\varphi$$

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

$$r \leq \ell(s)(i + 1) < \omega$$

Diagram shows transitions and satisfaction of formulas $\models \text{EF } \varphi$ and $\models \varphi$.
Case Not \((i + 1, r)\)-Bounded

\[ r \leq \ell(s)(i + 1) < \omega \]

\[ \models EF \phi \]
Case Not \((i + 1, r)\)-Bounded

\((i + 1, r)\)-bounded

\(\models \text{EF} \varphi\)

replace by small model of size \(\leq g(i)\)
Main Induction
(using ideas from Rackoff, 1978; Atig and Habermehl, 2011)

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

- **base $i = 0$:**
  
  \[ g(0) \text{ by reduction to LIP,} \]

- **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: $g(k) \leq 2^{2^{kd} \cdot |V| \cdot |\varphi|}$. 
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


