Witnesses For Vector Addition Systems

Jérôme Leroux

LaBRI (CNRS and University of Bordeaux), France.

September 21, 2015

Vector Addition Systems

Definition

A vector addition system (VAS) is a finite set $\mathbf{A} \subseteq \mathbb{Z}^d$.

$$
\begin{array}{ccccc}
 & \mathbf{A} & & & \\
 & \uplus & & & \\
 & \mathbf{a} & & & \\
\mathbf{x} & \longrightarrow & \mathbf{y} & \Longleftrightarrow & \mathbf{x} + \mathbf{a} = \mathbf{y} \\
\pitchfork & & \pitchfork & & \\
\mathbb{N}^d & & \mathbb{N}^d & &
\end{array}
$$

Central Model

VAS natural model:

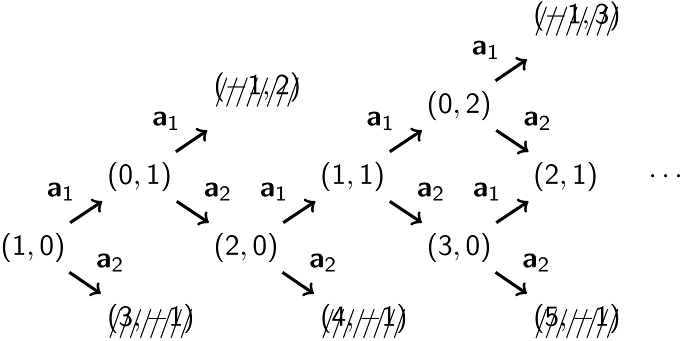
- Concurent systems.
- Parametrized systems.
- Energy Games.
- Encoding satisfiability problems for data logics.

Equivalent to other models:

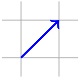
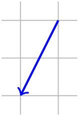
- Petri nets.
- Petri nets with states.
- Vector addition systems with states.
- Minsky machines without zero test.

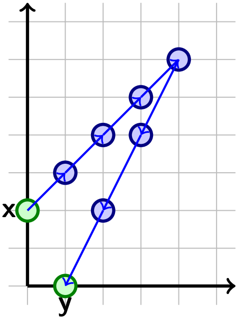
Reachability Graph View Point

$\mathbf{A} = \{\mathbf{a}_1, \mathbf{a}_2\}$ with $\mathbf{a}_1 = (-1, 1)$ and $\mathbf{a}_2 = (2, -1)$



Geometrical View Point

$\mathbf{A} = \{$  ,  $\}$



Decidability

Decidable problems:

- Termination.
- Boundedness.
- Coverability.
- Reachability.

Open problems:

- Semilinearity.
- Homestate.

Undecidable problems:

- Reachability set equality.
- CTL model checking.
- Many games.

Decidability by RECORE

A problem that is recursively enumerable and co recursively enumerable is decidable.

$\Rightarrow$ A problem is decidable if there exist:

- checkable witnesses when the property hold.
- checkable witnesses when the propety does not hold.

Table of Contents

Table of Contents

Coverability Problem

A final configuration $\mathbf{c}_{\text{final}}$ is coverable from an initial configuration $\mathbf{c}_{\text{init}}$ by a VAS $\mathbf{A}$ if:

$$\mathbf{c}_{\text{init}} \xrightarrow{\mathbf{A}^*} (\mathbf{c}_{\text{final}} + \mathbb{N}^d)$$

Definition (Coverability problem)

Deciding if $\mathbf{c}_{\text{final}}$ is coverable from $\mathbf{c}_{\text{init}}$ for a VAS $\mathbf{A}$.

Application: Safety properties [mutual exclusion]

Definition (Coverability Witnesses)

A word $w \in \mathbf{A}^*$ and a configuration $\mathbf{e} \in \mathbb{N}^d$ such that:

$$\mathbf{c}_{\text{init}} \xrightarrow{w} (\mathbf{c}_{\text{final}} + \mathbf{e})$$

Worst case $|w|$ doubly exponentialy long.
The coverability problem is EXPSPACE-complete.

[C. Rachoff:TCS'78].

[E. Cardoza, R. J. Lipton, A. R. Meyer:STOC'76].

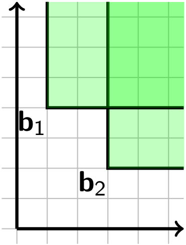
Definition (Uncoverability Witnesses)

A finite set $\mathbf{B} \subseteq \mathbb{N}^d$ denoting a set $\mathbf{C} = \bigcup_{\mathbf{b} \in \mathbf{B}} \mathbf{b} + \mathbb{N}^d$ such that:

- For every $\mathbf{x} \xrightarrow{\mathbf{a}} \mathbf{y}$ we have:

$$\mathbf{y} \in \mathbf{C} \Rightarrow \mathbf{x} \in \mathbf{C}$$

- $\mathbf{c}_{\text{init}} \notin \mathbf{C}$
- $\mathbf{c}_{\text{final}} \in \mathbf{C}$



Let:

$$\mathbf{C} = \left\{ \mathbf{c} \in \mathbb{N}^d \mid \mathbf{c} \xrightarrow{\mathbf{A}^*} (\mathbf{c}_{\mathsf{final}} + \mathbb{N}^d) \right\}$$

$$\mathbf{B} = \min_{\leq}(\mathbf{C})$$

Just observe that $\mathbf{C} = \bigcup_{\mathbf{b} \in \mathbf{B}} \mathbf{b} + \mathbb{N}^d$.

$\mathbf{C}$ is computable with a backward algorithm in at most a double exponential number of iterations with $\mathbf{C}_0 = \mathbf{c}_{\mathsf{final}} + \mathbb{N}^d$ and:

$$\mathbf{C}_{n+1} = \{ \mathbf{c} \in \mathbb{N}^d \mid \mathbf{c} \xrightarrow{\mathbf{A}} \mathbf{C}_n \}$$

[L. Bozzelli, P. Ganty:RP'11]

[R. Lazic, S. Schmitz:RP'15]

Reachability Problem

A final configuration $\mathbf{c}_{\text{final}}$ is <u>reachable</u> from an initial configuration $\mathbf{c}_{\text{init}}$ by a VAS $\mathbf{A}$ if:

$$\mathbf{c}_{\text{init}} \xrightarrow{\mathbf{A}^*} \mathbf{c}_{\text{final}}$$

Definition (Reachability problem)

Deciding if $\mathbf{c}_{\text{final}}$ is reachable from $\mathbf{c}_{\text{init}}$ for a VAS $\mathbf{A}$.

Application:

- More general safety properties.
- Inclusion of Petri nets/ VASes languages.

[M. Heizmann, J. Hoenicke, A. Podelski:CAV'12]

Definition (Reachability Witnesses)

A word $w \in \mathbf{A}^*$ such that:

$$\mathbf{c}_{\text{init}} \xrightarrow{w} \mathbf{c}_{\text{final}}$$

$|w|$ is bounded by $O(F_{\omega^3})$.

[J. Leroux, S. Schmitz:LICS'15]

Definition (Unreachability Witnesses)

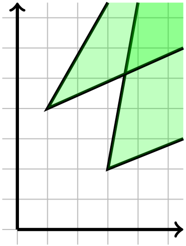
A Presburger formula ϕ denoting a set $\mathbf{C} \subseteq \mathbb{N}^d$ such that:

- For every $\mathbf{x} \xrightarrow{\mathbf{a}} \mathbf{y}$ we have:

$$\mathbf{y} \in \mathbf{C} \quad \Rightarrow \quad \mathbf{x} \in \mathbf{C}$$

- $\mathbf{c}_{\mathrm{init}} \notin \mathbf{C}$
- $\mathbf{c}_{\mathrm{final}} \in \mathbf{C}$

[J. Leroux:TURING'100].



Theorem

A set $\mathbf{C} \subseteq \mathbb{N}^d$ is definable in the Presburger arithmetic iff it is a finite union of linear sets:

$$\{\mathbf{b} + n_1\mathbf{p}_1 + \cdots + n_k\mathbf{p}_k \mid n_1, \ldots, n_k \in \mathbb{N}\}$$

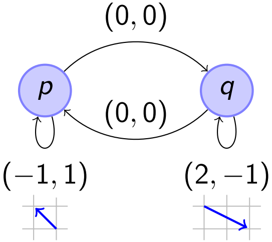
[S. Ginsburg and E. H. Spanier: Pacific journal of mathematics'66]

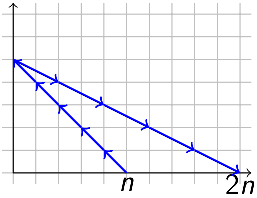
Let **C** be defined as:

$$\mathbf{C} = \left\{ \mathbf{c} \in \mathbb{N}^d \mid \mathbf{c} \xrightarrow{\mathbf{A}^*} \mathbf{c}_{\mathsf{final}} \right\}$$

C may not be definable in Presburger if $d > 5$.

[J. Hopcroft, J.-J. Pansiot:TCS'79]



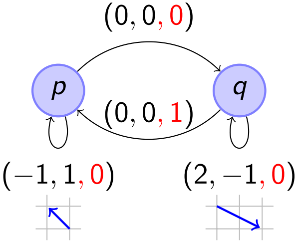


Let **C** be defined as:

$$\mathbf{C} = \left\{ \mathbf{c} \in \mathbb{N}^d \mid \mathbf{c} \xrightarrow{\mathbf{A}^*} \mathbf{c}_{\text{final}} \right\}$$

C may not be definable in Presburger if $d > 5$.

[J. Hopcroft, J.-J. Pansiot:TCS'79]



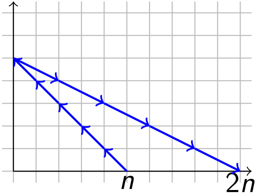


Table of Contents

Semilinearity

A VAS **A** is said to be semilinear from an initial configuration $\mathbf{c}_{\text{init}}$ if the set of reachable configurations from $\mathbf{c}_{\text{init}}$ is definable in the Presburger arithmetic.

Definition (Semilinearity problem)

Deciding if a VAS **A** is semilinear from an initial configuration $\mathbf{c}_{\text{init}}$.

Applications:

- Characterize classes for which the most precise inductive invariant is definable in the Presburger arithmetic.
- Characterize the expressive power of acceleration techniques.

Definition (Semilinearity Witnesses)

A finite sequence of words $\sigma_1, \ldots, \sigma_k \in \mathbf{A}^*$ such that the following set:

$$\mathbf{C} = \left\{ \mathbf{c} \in \mathbb{N}^d \quad \middle| \quad \mathbf{c}_{\text{init}} \xrightarrow{\sigma_1^* \ldots \sigma_k^*} \mathbf{c} \right\}$$

satisfies for every $\mathbf{x} \xrightarrow{\mathbf{a}} \mathbf{y}$:

$$\mathbf{x} \in \mathbf{C} \Rightarrow \mathbf{y} \in \mathbf{C}$$

[J. Leroux:LICS'13]

Definition (Non Semilinearity Witnesses)

???????????

Applications:

- Detect parts of the reachability set that must be over-approximated for deciding the reachability problem with Presburger inductive invariants.

Homestate Problem

A set $\mathbf{C}_{\text{home}}$ of configurations is called a <u>home</u> for a VAS $\mathbf{A}$ from a set $\mathbf{C}_{\text{init}}$ of initial configuration if:

$$\forall \mathbf{c} \quad \mathbf{C}_{\text{init}} \xrightarrow{\mathbf{A}^*} \mathbf{c} \quad \Longrightarrow \quad \mathbf{c} \xrightarrow{\mathbf{A}^*} \mathbf{C}_{\text{home}}$$

Definition (Homestate Problem)

Deciding if a set $\mathbf{C}_{\text{home}}$ denoted by a Presburger formula ϕ_{home} is an home set for a VAS $\mathbf{A}$ from a set of initial configurations $\mathbf{C}_{\text{init}}$ denoted by a Presburger formula ϕ_{init}.

Decidable if there exists a finite set $\mathbf{B} \subseteq \mathbb{N}^d$ and vectors $\mathbf{p}_1, \ldots, \mathbf{p}_k \in \mathbb{N}^d$ such that:

$$\mathbf{C}_{\text{home}} = \bigcup_{\mathbf{b} \in \mathbf{B}} \{\mathbf{b} + n_1\mathbf{p}_1 + \cdots + n_k\mathbf{p}_k \mid n_1, \ldots, n_k \in \mathbb{N}\}$$

[D. Frutos-Escrig, C. Johnen. Technical Report'89]

Definition (Non Homestate Witnesses)

- A configuration $\mathbf{c}$,
- A witness of reachability of $\mathbf{c}$ from $\mathbf{c}_{\text{init}}$, and
- A witness of unreachability of $\mathbf{c}$ to $\mathbf{C}_{\text{home}}$.

Theorem

Given two VASes $\mathbf{A}, \mathbf{B}$ *and two configurations* $\mathbf{c}_{init}$ *and* $\mathbf{c}_{final}$ *the following property is undecidable:*

$$\forall \mathbf{c} \quad \mathbf{c}_{init} \xrightarrow{\mathbf{A}^*} \mathbf{c} \quad \Longrightarrow \quad \mathbf{c} \xrightarrow{\mathbf{B}^*} \mathbf{c}_{final}$$

[M. Hack:TCS'76]

Conservative VAS

A VAS $\mathbf{A}$ is said to be conservative if $a_1 + \cdots + a_d = 0$ for every $(a_1, \ldots, a_d) \in \mathbf{A}$.

Example:

- Parametrized protocols.

  [S. M. German, A. P. Sistla: journal of ACM'92].

  [B. Aminof, T. Kotek, S. Rubin, F. Spegni, H. Veith: CONCUR14].

- Chemical reactions.

Definition (Homestate Witnesses For Conservative VASes)

A formula ϕ in the Presburger arithmetic denoting a set $\mathbf{C} \subseteq \mathbb{N}^d$, and a sequence $\sigma_1, \ldots, \sigma_k \in \mathbf{A}^*$ such that:

- $\mathbf{C}_{\text{init}} \subseteq \mathbf{C}$ and for every $\mathbf{x} \xrightarrow{\mathbf{a}} \mathbf{y}$ we have $\mathbf{x} \in \mathbf{C} \Rightarrow \mathbf{y} \in \mathbf{C}$.
- for every $\mathbf{c} \in \mathbf{C}$ we have:

$$\mathbf{c} \xrightarrow{\sigma_1^* \ldots \sigma_k^*} \mathbf{C}_{\text{home}}$$

[J. Esparza, P. Ganty, J. Leroux, R. Majumdar: CONCUR'15]

Applications:

- Verification problems for parametrized protocols.
- Well specification problem for population protocols.

[D. Angluin, J. Aspnes, Z. Diamadi, M. J. Fischer, R. Peralta:PODC'04]

Table of Contents

Upward And Downward Closures

Definition

Let $(S, \leq)$ be a quasi ordered set.

$$\uparrow x = \{s \in S \mid x \leq s\} \qquad \downarrow x = \{s \in S \mid s \leq x\}$$

$$\uparrow X = \bigcup_{x \in X} \uparrow x \qquad \downarrow X = \bigcup_{x \in X} \downarrow x$$

X upward closed if $\uparrow X = X$ $\qquad$ X downward closed if $\downarrow X = X$

Ordering Configurations

Let $\mathbb{N}^d$ be ordered with $\leq$ defined by:

$$(x_1, \ldots, x_d) \leq (y_1, \ldots, y_d) \iff \bigwedge_{i=1}^{d} x_i \leq y_i$$

Upward closed sets are finite unions of $\uparrow\mathbf{x}$.

Example

$$\uparrow(1,0,9) = (1,0,9) + \mathbb{N} \times \mathbb{N} \times \mathbb{N}$$

Downward closed sets are finite unions of $X_1 \times \cdots \times X_d$ where X_i is either $\mathbb{N}$ or a set of the form $\{0, \ldots, n\}$ for some $n \in \mathbb{N}$.

Example

$$\downarrow(1,\omega,2) = \{0,1\} \times \mathbb{N} \times \{0,1,2\}$$

Well Quasi Orders (WQO)

Definition

A quasi ordered set $(S, \leq)$ is said to be well if it satisfies one of the following properties.

Lemma

The following properties are equivalent:

- *Sets of incomparable elements and decreasing sequences are finite.*
- *Infinite sequences contain a non decreasing pair.*
- *Infinite sequences contain an infinite non deceasing subsequence.*
- *Non decreasing sequences of upward closed sets are stationnary.*
- *Non increasing sequences of downward closed sets are stationnary.*
- *Upward closed sets are upward closures of finite sets.*

Ideals

Let $(S, \leq)$ be a well quasi ordered set.

Definition

An ideal I is a non-empty downward closed set such that for every $x, y \in I$, there exists $s \in I$ such that $x, y \leq s$.

Theorem

Every downward closed set is the union of a unique finite familly of incomparable ideals.

[M. Kabil, M. Pouzet : Theor. Inform. Appl'92]

[A. Finkel, J. Goubault-Larrecq : STACS'09]

[J.Goubault-Larrecq, P.Karandikar, K.NarayanKumar, Ph. Schnoebelen : In preparation, 2015].

Example

$$\text{Ideals}(\mathbb{N}^d, \leq) = \{\downarrow \mathbf{x} \mid \mathbf{x} \in \mathbb{N}_\omega^d\} \quad \text{with} \quad \mathbb{N}_\omega = \mathbb{N} \cup \{\omega\}$$

Dickson's Lemma

The cartesian product $(S_1, \leq_1) \times (S_2, \leq_2)$ of two quasi ordered sets is the quasi ordered set $(S, \leq)$ defined by:

$$(x_1, x_2) \leq (y_1, y_2) \iff x_1 \leq_1 y_1 \ \wedge \ x_2 \leq_2 y_2$$

Lemma (Dickson's Lemma)

The cartesian product of two well quasi oredered sets is well.
Moreover, in that case:

$$\text{Ideals}(S_1, \leq_1) \times (S_2, \leq_2) = \{I_1 \times I_2 \mid (I_1, I_2) \in \text{Ideals}(S_1, \leq_1) \times \text{Ideals}(S_2, \leq_2)\}$$

Higman's Lemma

The star $(S, \leq)^*$ of a quasi ordered set $(S, \leq)$ is the quasi ordered set $(S^*, \leq_*)$ where S^* is the set of words over S, and $\leq_*$ is defined by $w \leq_* w'$ iff

$$w' \in S^* \uparrow s_1 \; S^* \ldots \uparrow s_k \; S^*$$

where $s_1, \ldots, s_k \in S$ satisfy $w = s_1 \ldots s_k$.

Lemma (Higman's Lemma)

The star of a well quasi ordered set is well.
Moreover, in that case, ideals of $(S, \leq)^*$ are finite concatenations $A_1 \ldots A_k$ where A_j is a language of the form:

- $\{\varepsilon\} \cup I$ *where* $I \in \mathrm{Ideals}(S, \leq)$, *or*
- D^* *where D is a finite union of ideals of $(S, \leq)$.*

[P. Jullien:PhD'69]

[P. A. Abdulla, A. Collomb-Annichini, A. Bouajjani, B. Jonsson:FMSD'04]

[M. Kabil, M. Pouzet : Theor. Inform. Appl'92]

[A. Finkel, J. Goubault-Larrecq : STACS'09]

Example

Let $(A, =)$ where A is a finite alphabet.
$\text{Ideals}(A, =) = \{\{a\} \mid a \in A\}$.
Ideals of $(A, =)^*$ have the following form:

$$D_0^* \{\varepsilon, a_1\} D_1^* \ldots \{\varepsilon, a_k\} D_k^*$$

where $D_0, \ldots, D_k \subseteq A$ and $a_1, \ldots, a_k \in A$.

Application :

- Analysis of lossy channel systems [LRE].

  [P. A. Abdulla, A. Collomb-Annichini, A. Bouajjani, B. Jonsson:FMSD'04]

Preruns

Let $\mathbf{A} \subseteq \mathbb{Z}^d$ be a VAS.

Definition (Preruns)

A prerun is a triple:

$$(\mathbf{x}, (\mathbf{x}_1, \mathbf{a}_1, \mathbf{y}_1) \ldots (\mathbf{x}_k, \mathbf{a}_k, \mathbf{y}_k), \mathbf{y}) \quad \in \quad \mathbb{N}^d \times (\mathbb{N}^d \times \mathbf{A} \times \mathbb{N}^d)^* \times \mathbb{N}^d$$

We introduce $(\text{preruns}(\mathbf{A}), \trianglelefteq)$ defined as:

$$(\mathbb{N}^d, \leq) \times ((\mathbb{N}^d, \leq) \times (\mathbf{A}, =) \times (\mathbb{N}^d, \leq))^* \times (\mathbb{N}^d, \leq)$$

Lemma

$(\text{preruns}(\mathbf{A}), \trianglelefteq)$ *is well.*

[P. Jančar:TCS90]

Ideals Of Preruns

Ideals of $(\text{preruns}(\mathbf{A}), \trianglelefteq)$ have the form:

$$(\downarrow\mathbf{x}) \times (\bigcup_{t \in T_0} \downarrow t)(\{\varepsilon\} \cup \downarrow t_1)(\bigcup_{t \in T_1} \downarrow t) \ldots (\{\varepsilon\} \cup \downarrow t_k)(\bigcup_{t \in T_k} \downarrow t) \times (\downarrow\mathbf{y})$$

where:

- $\mathbf{x}, \mathbf{y} \in \mathbb{N}_\omega^d$.
- $t_1, \ldots, t_k \in \mathbb{N}_\omega^d \times \mathbf{A} \times \mathbb{N}_\omega^d$.
- $T_0, \ldots, T_k$ are finite subsets of $\mathbb{N}_\omega^d \times \mathbf{A} \times \mathbb{N}_\omega^d$.

Notice that:

$$\downarrow(\mathbf{u}, \mathbf{a}, \mathbf{v}) = \downarrow\mathbf{u} \times \{a\} \times \downarrow\mathbf{v}$$

Definition

A run is a prerun

$$(\mathbf{x}, (\mathbf{x}_1, \mathbf{a}_1, \mathbf{y}_1) \ldots (\mathbf{x}_k, \mathbf{a}_k, \mathbf{y}_k), \mathbf{y})$$

satisfying for every $1 \leq j \leq k$:

- $\mathbf{y}_{j-1} = \mathbf{x}_j \wedge \mathbf{y}_j = \mathbf{x}_{j+1}$ with the convention $\mathbf{y}_0 = \mathbf{x}$ and $\mathbf{x}_{k+1} = \mathbf{y}$.
- $\mathbf{x}_j \xrightarrow{\mathbf{a}_j} \mathbf{y}_j$.

We let $\text{runs}(\mathbf{x}, \mathbf{A}, \mathbf{y})$ be the set of runs from $\mathbf{x}$ to $\mathbf{y}$.

A CEGAR Approach

The reachability problem reduces to the emptyness of $\downarrow\text{runs}(\mathbf{x}, \mathbf{A}, \mathbf{y})$.

$D := \text{preruns}(\mathbf{A})$
  While there exists a maximal ideal I of D with $I \not\subseteq \downarrow\text{runs}(\mathbf{x}, \mathbf{A}, \mathbf{y})$
    Pick $\pi \in I \setminus \downarrow\text{runs}(\mathbf{x}, \mathbf{A}, \mathbf{y})$
    $D := D \setminus \uparrow\pi$
return D

[J. Leroux, S. Schmitz:LICS'15]

The Kosaraju Approach

Theorem

The Kosaraju algorithm is computing precisely the decomposition of $\downarrow\text{runs}(\mathbf{x}, \mathbf{A}, \mathbf{y})$ *into ideals.*

[J. Leroux, S. Schmitz:LICS'15]

Applications:

- Demystifying the Kosaraju algorithm for deciding the reachability problem.
- Provide a guideline for deciding reachability problems for VAS extensions.

Advertisement

Ideals of the decomposition of $\downarrow \text{runs}(\mathbf{x}, \mathbf{A}, \mathbf{y})$ have the form:

$$(\downarrow \mathbf{x}) \times (\bigcup_{t \in T_0} \downarrow t)(\{\varepsilon\} \cup \downarrow t_1)(\bigcup_{t \in T_1} \downarrow t) \ldots (\{\varepsilon\} \cup \downarrow t_k)(\bigcup_{t \in T_k} \downarrow t) \times (\downarrow \mathbf{y})$$

where $T_j \subseteq \mathbb{N}_\omega^d \times \mathbf{A} \times \mathbb{N}_\omega^d$ denotes the transitions of a strongly connected graph.

Table of Contents

About Witnesses

Many problems on VASes can be decided with simple witnesses.
There exist decidable (EXPSPACE) logics for expressing some of these witnesses:

[H.-C. Yen: Inf. Comput.'92]

[M. F. Atig, P. Habermehl:Int. J. Found. Comput. Sci'11]

[M. Blockelet, S. Schmitz: MFCS'11]

[S. Demri: INFINITY'11]

[J. Leroux, M. Praveen, G. Sutre: CONCUR'13]

The following problems can be decided this way:

- Boundedness/place boundedness/selective unboundedness.
- Regularity/context-freeness. [J. Leroux, V. Penelle, G. Sutre: LICS'13]
- Coverability.
- Termination.

About Ideals

Well-structured transition systems is a powerfull framework for solving coverability questions [A. Finkel, Ph. Schnoebelen: TCS'01]. Concerning reachability ones, we have a new ideal tool.

Possible applications of ideals of runs:

- VAS with 1 zero test.
- VAS with resets.
- Pushdown VAS.
- Branching VAS.
- Data nets.