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 $A \subseteq \mathbb{Z}^d$.

$$A \ni a \quad \xrightarrow{} \quad y \iff x + a = y$$
Central Model

VAS natural model:
- Concurrent 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.
A = \{a_1, a_2\} with a_1 = (-1, 1) and a_2 = (2, -1)
Geometrical View Point

\[ A = \{ x, y \} \]
Decidability

Decidable problems:
- Termination.
- Boundedness.
- Coverability.
- Reachability.

Open problems:
- Semilinearity.
- Homestate.

Undecidable problems:
- Reachability set equality.
- CTL model checking.
- Many games.
A problem that is recursively enumerable and co recursively enumerable is decidable.

⇒ A problem is decidable if there exist:

- checkable witnesses when the property hold.
- checkable witnesses when the property does not hold.
1 Introduction

2 Witnesses For Coverability And Reachability

3 Two Open Problems About Witnesses

4 Well Quasi Orders And Ideals

5 Conclusion
1. Introduction

2. Witnesses For Coverability And Reachability

3. Two Open Problems About Witnesses

4. Well Quasi Orders And Ideals

5. Conclusion
A final configuration \( c_{\text{final}} \) is coverable from an initial configuration \( c_{\text{init}} \) by a VAS \( A \) if:

\[
c_{\text{init}} \xrightarrow{A^*} (c_{\text{final}} + \mathbb{N}^d)
\]

**Definition (Coverability problem)**

Deciding if \( c_{\text{final}} \) is coverable from \( c_{\text{init}} \) for a VAS \( A \).

**Application:** Safety properties [mutual exclusion]
Definition (Coverability Witnesses)

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

\[
c_{\text{init}} \xrightarrow{w} (c_{\text{final}} + e)
\]

Worst case \( |w| \) doubly exponential 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 \( B \subseteq \mathbb{N}^d \) denoting a set \( C = \bigcup_{b \in B} b + \mathbb{N}^d \) such that:

- For every \( x \xrightarrow{a} y \) we have:
  \[ y \in C \Rightarrow x \in C \]
- \( c_{\text{init}} \notin C \)
- \( c_{\text{final}} \in C \)
Let:

\[ C = \left\{ c \in \mathbb{N}^d \mid c \xrightarrow{A^*} (c_{\text{final}} + \mathbb{N}^d) \right\} \]

\[ B = \min(C) \]

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

\( C \) is computable with a backward algorithm in at most a double exponential number of iterations with \( C_0 = c_{\text{final}} + \mathbb{N}^d \) and:

\[ C_{n+1} = \left\{ c \in \mathbb{N}^d \mid c \xrightarrow{A} C_n \right\} \]

[L. Bozzelli, P. Ganty:RP’11]

[R. Lazic, S. Schmitz:RP’15]
A final configuration $c_{\text{final}}$ is reachable from an initial configuration $c_{\text{init}}$ by a VAS $A$ if:

$$c_{\text{init}} \xrightarrow{A^*} c_{\text{final}}$$

**Definition (Reachability problem)**

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

**Application:**

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

[M. Heizmann, J. Hoenicke, A. Podelski: CAV’12]
Definition (Reachability Witnesses)

A word $w \in A^*$ such that:

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

[J. Leroux, S. Schmitz: LICS’15]
Definition (Unreachability Witnesses)

A Presburger formula \( \phi \) denoting a set \( C \subseteq \mathbb{N}^d \) such that:

- For every \( x \xrightarrow{a} y \) we have:
  \[ y \in C \implies x \in C \]
- \( c_{\text{init}} \notin C \)
- \( c_{\text{final}} \in C \)

[J. Leroux: TURING'100].

Theorem

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

\[ \{ b + n_1p_1 + \cdots + n_kp_k \mid n_1, \ldots, n_k \in \mathbb{N} \} \]

Let $\mathbf{C}$ be defined as:

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

$\mathbf{C}$ may not be definable in Presburger if $d > 5$.

[J. Hopcroft, J.-J. Pansiot:TCS'79]
Let $C$ be defined as:

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

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

[J. Hopcroft, J.-J. Pansiot: TCS'79]
# Table of Contents

1. Introduction

2. Witnesses For Coverability And Reachability

3. Two Open Problems About Witnesses

4. Well Quasi Orders And Ideals

5. Conclusion
Semilinearity

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

**Definition (Semilinearity problem)**
Deciding if a VAS $A$ is semilinear from an initial configuration $c_{\text{init}}$.

**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 $\sigma_1, \ldots, \sigma_k \in A^*$ such that the following set:

$$C = \left\{ c \in \mathbb{N}^d \mid \text{cinit} \xrightarrow{\sigma_1^* \ldots \sigma_k^*} \text{c} \right\}$$

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

$$x \in C \Rightarrow y \in C$$

[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 $C_{\text{home}}$ of configurations is called a home for a VAS $A$ from a set $C_{\text{init}}$ of initial configuration if:

$$\forall c \in C_{\text{init}} A^* \rightarrow c \iff c \rightarrow A^* C_{\text{home}}$$

Definition (Homestate Problem)

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

Decidable if there exists a finite set $B \subseteq \mathbb{N}^d$ and vectors $p_1, \ldots, p_k \in \mathbb{N}^d$ such that:

$$C_{\text{home}} = \bigcup_{b \in B} \left\{ b + n_1 p_1 + \cdots + n_k p_k \mid n_1, \ldots, n_k \in \mathbb{N} \right\}$$

Definition (Non Homestate Witnesses)

- A configuration \( c \),
- A witness of reachability of \( c \) from \( c_{\text{init}} \), and
- A witness of unreachability of \( c \) to \( C_{\text{home}} \).
Theorem

Given two VASes $A$, $B$ and two configurations $c_{\text{init}}$ and $c_{\text{final}}$ the following property is undecidable:

$$\forall c \quad c_{\text{init}} \xrightarrow{A^*} c \iff c \xrightarrow{B^*} c_{\text{final}}$$

[M. Hack: TCS'76]
A VAS $A$ is said to be conservative if $a_1 + \cdots + a_d = 0$ for every $(a_1, \ldots, a_d) \in A$.

Example:

- Parametrized protocols.
  
  [S. M. German, A. P. Sistla: journal of ACM’92].
  

- Chemical reactions.
Definition (Homestate Witnesses For Conservative VASes)

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

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

\[ c \xrightarrow{\sigma_1^* \cdots \sigma_k^*} C_{\text{home}} \]

Applications:

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

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

Table of Contents

1 Introduction

2 Witnesses For Coverability And Reachability

3 Two Open Problems About Witnesses

4 Well Quasi Orders And Ideals

5 Conclusion
Upward And Downward Closures

Definition

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

\[
\uparrow x &= \{ s \in S \mid x \leq s \} \\
\uparrow X &= \bigcup_{x \in X} \uparrow x \\
X \text{ upward closed if } \uparrow X &= X \\
\downarrow x &= \{ s \in S \mid s \leq x \} \\
\downarrow X &= \bigcup_{x \in X} \downarrow x \\
X \text{ downward closed if } \downarrow X &= X
\]
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 \( \uparrow x \).

**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**

\[
\downarrow(1, \omega, 2) = \{0, 1\} \times \mathbb{N} \times \{0, 1, 2\}
\]
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 family of incomparable ideals.


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


Example

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

\[(x_1, x_2) \leq (y_1, y_2) \iff x_1 \leq_1 y_1 \land x_2 \leq_2 y_2\]

Lemma (Dickson’s Lemma)

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

\[\text{Ideals}(S_1, \leq_1) \times \text{Ideals}(S_2, \leq_2) = \{ l_1 \times l_2 \mid (l_1, l_2) \in \text{Ideals}(S_1, \leq_1) \times \text{Ideals}(S_2, \leq_2) \}\]
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 \(I \in \text{Ideals}(S, \leq)\), 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]


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

Let \((A, =)\) where \(A\) is a finite alphabet.

Ideals\((A, =) = \{\{a\} \mid a \in A\}\).

Ideals of \((A, =)^*\) have the following form:

\[
D_0^* \{\varepsilon, a_1\} D_1^* \cdots \{\varepsilon, a_k\} D_k^*
\]

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

**Definition (Preruns)**

A prerun is a triple:

$$(x, (x_1, a_1, y_1), \ldots, (x_k, a_k, y_k), y) \in \mathbb{N}^d \times (\mathbb{N}^d \times A \times \mathbb{N}^d)^* \times \mathbb{N}^d$$

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

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

**Lemma**

$(\text{preruns}(A), \sqsubseteq)$ is well.

[P. Jančar: TCS90]
Ideals Of Preruns

Ideals of \((\text{preruns}(A), \subseteq)\) have the form:

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

where:

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

Notice that:

\[
\downarrow (u, a, v) = \downarrow u \times \{a\} \times \downarrow v
\]
Definition

A run is a prerun

\((x, (x_1, a_1, y_1) \ldots (x_k, a_k, y_k), y)\)

satisfying for every \(1 \leq j \leq k\):

- \(y_{j-1} = x_j \land y_j = x_{j+1}\) with the convention \(y_0 = x\) and \(x_{k+1} = y\).
- \(x_j \xrightarrow{a_j} y_j\).

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

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

\[
D := \text{preruns}(A)
\]

While there exists a maximal ideal \( I \) of \( D \) with \( I \not\subseteq \downarrow \text{runs}(x, A, y) \)

Pick \( \pi \in I \setminus \downarrow \text{runs}(x, A, y) \)

\[
D := D \uparrow \pi
\]

return \( D \)

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

Theorem

The Kosaraju algorithm is computing precisely the decomposition of $\downarrow \text{runs}(x, A, y)$ 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.
Ideals of the decomposition of \( \downarrow \text{runs}(x, A, y) \) have the form:

\[
(\downarrow x) \times \left( \bigcup_{t \in T_0} \downarrow t \right) \left( \{\varepsilon\} \cup \downarrow t_1 \right) \left( \bigcup_{t \in T_1} \downarrow t \right) \ldots \left( \{\varepsilon\} \cup \downarrow t_k \right) \left( \bigcup_{t \in T_k} \downarrow t \right) \times (\downarrow y)
\]

where \( T_j \subseteq \mathbb{N}_\omega^d \times A \times \mathbb{N}_\omega^d \) denotes the transitions of a strongly connected graph.
1. Introduction

2. Witnesses For Coverability And Reachability

3. Two Open Problems About Witnesses

4. Well Quasi Orders And Ideals

5. Conclusion
About Witnesses

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

[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.
Well-structured transition systems is a powerful framework for solving coverability questions \cite{FinkelS01}. 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.