Jérôme Leroux’s Proof of Decidability of Reachability in Vector Addition Systems

M. Praveen

CMI

April 2014
Vector Addition System (VAS): A finite set $A \subseteq \mathbb{Z}^d$. 

Reachability problem: given $A \subseteq \mathbb{Z}^d$ and $\vec{m}, \vec{m}' \in \mathbb{N}^d$, decide whether $\vec{m} \ast \vec{a} \rightarrow \vec{m}'$.
Preliminaries

- Vector Addition System (VAS): A finite set $A \subseteq \mathbb{Z}^d$. $d$ is the dimension.
Preliminaries

- Vector Addition System (VAS): A finite set $A \subseteq \mathbb{Z}^d$. $d$ is the dimension.

- Let $\vec{m}, \vec{m}' \in \mathbb{N}^d$ and $\vec{a} \in A$. $\vec{m} \xrightarrow{\vec{a}} \vec{m'}$ if $\vec{m'} = \vec{m} + \vec{a}$. 
Preliminaries

- Vector Addition System (VAS): A finite set $A \subseteq \mathbb{Z}^d$. $d$ is the dimension.

- Let $\vec{m}, \vec{m}' \in \mathbb{N}^d$ and $\vec{a} \in A$. $\vec{m} \rightarrow \vec{m}'$ if $\vec{m}' = \vec{m} + \vec{a}$.

- Reachability problem: given $A \subseteq \mathbb{Z}^d$ and $\vec{m}, \vec{m}' \in \mathbb{N}^d$, decide whether $\vec{m} \rightarrow^* \vec{m}'$. 
History

- [Sacerdote & Tenney, 1977]: Decidable, some gaps remained in the proof.
History

- [Sacerdote & Tenney, 1977]: Decidable, some gaps remained in the proof.

- [Mayr, 1981]: Decidable, complete proof.
History

- [Sacerdote & Tenney, 1977]: Decidable, some gaps remained in the proof.

- [Mayr, 1981]: Decidable, complete proof.

- [Kosaraju, 1982]: Simplifications.
History

- [Sacerdote & Tenney, 1977]: Decidable, some gaps remained in the proof.
- [Mayr, 1981]: Decidable, complete proof.
- [Kosaraju, 1982]: Simplifications.
- [Reutenauer, translated by Craig, 1990]: Book with all details of the above proof.
- [Lambert, 1992]: Simplifications.
- [Leroux, 2009]: Alternate proof based on Presburger inductive invariants.
History

- [Sacerdote & Tenney, 1977]: Decidable, some gaps remained in the proof.
- [Mayr, 1981]: Decidable, complete proof.
- [Kosaraju, 1982]: Simplifications.
- [Reutenauer, translated by Craig, 1990]: Book with all details of the above proof.
- [Lambert, 1992]: Simplifications.
History

- [Sacerdote & Tenney, 1977]: Decidable, some gaps remained in the proof.

- [Mayr, 1981]: Decidable, complete proof.

- [Kosaraju, 1982]: Simplifications.

- [Reutenauer, translated by Craig, 1990]: Book with all details of the above proof.

- [Lambert, 1992]: Simplifications.

- [Leroux, 2009]: Alternate proof based on Presburger inductive invariants.
Two Semi-Algorithms in Parallel

First one trying to prove reachability:

- Start enumerating potential certificates for reachability.
Two Semi-Algorithms in Parallel

First one trying to prove reachability:
- Start enumerating potential certificates for reachability.
- Stop if a valid certificate found.
Two Semi-Algorithms in Parallel

First one trying to prove reachability:
  ▶ Start enumerating potential certificates for reachability.
  ▶ Stop if a valid certificate found.

Second one trying to prove unreachability:
  ▶ Start enumerating potential certificates for unreachability.
  ▶ Stop if a valid certificate found.
Certificates for unreachability

\[ \vec{m} \quad \vec{m}' \]

For all \( \vec{x} \in X \), \( \vec{x} \rightarrow \vec{x}' \) implies \( \vec{x}' \in X \).

If \( X \) is Presburger definable, then Presburger formulas are potential certificates for unreachability.
Certificates for unrechability

For all $\vec{x} \in X$, $\vec{x} \rightarrow \vec{x}'$ implies $\vec{x}' \in X$.

If $X$ is Presburger definable, then Presburger formulas are potential certificates for unrechability.
Certificates for unreachability

For all $\vec{x} \in X$, $\vec{x} \xrightarrow{*} \vec{x}'$ implies $\vec{x}' \in X$. 
Certificates for unreachability

For all $\vec{x} \in X$, $\vec{x} \xrightarrow{\vec{m}} \vec{x}'$ implies $\vec{x}' \in X$.

If $X$ is Presburger definable, then Presburger formulas are potential certificates for unreachability.
Separators

\[
\text{post}^* (X_0) \approx (\text{post}^* (X_0)) \setminus (S \cap T)
\]

\[
S^* (Y_0) \approx (S^* (Y_0)) \setminus (X \cap S)
\]
Separators

\[ \text{post}^*(X_0) \]

\[ S \cap T \]
Separators

$S$

$\approx \text{post}^*(X_0)$
Separators

\[ S \approx (\text{post} \ast (X_0)) \]

\[ S \approx (\text{pre} \ast (Y)) \]

\[ X_0 \cap Y \]
Separators

\[ S \approx (\text{post} \ast (X_0)) \]

\[ S \preceq \approx (\text{pre} \ast (Y)) \]

\[ X \cap Y \]
Separators

\[ S \approx (\text{post} \ast (X \cap Y)) \]

\[ \text{pre}^* (Y) \]
Separators

\[ S \approx (\text{post} \ast (X_0)) \]

\[ \text{approx} (\text{pre}^* (Y)) \]

\[ S \cap T \]
$S \cap T$