Regular Separators for VASS Coverability Languages

43rd IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, Hyderabad

Chris Köcher    Georg Zetzsche

Max Planck Institute for Software Systems, Kaiserslautern

December 18, 2023
Motivation

- **Vector Addition Systems with States (VASS)**
  - NFA with finitely many non-negative counters
  - Equivalent to Petri Nets
  - Model the behavior of concurrent systems

- **Why (regular) separability?**
  - Safety verification consists of deciding disjointness of two languages, like event sequences
    - that are consistent with the behavior of a system component and reaching an undesirable state.
  - A regular separator certifies disjointness.
Vector Addition Systems with States (1)

\[ \mathcal{V} = \left( Q, \Sigma, \Delta, s, t \right) \]

- **finite set of states**
- **input alphabet**
- **finite set of transitions**

\[ p \xrightarrow{a|\vec{v}} q \]

with \( p, q \in Q \), \( a \in \Sigma \cup \{\varepsilon\} \), \( \vec{v} \in \mathbb{Z}^d \)

fails, since \( 3 - 4 < 0 \)
Vector Addition Systems with States (1)

\[ V = (Q, \Sigma, \Delta, s, t) \]

finite set of states

finite set of transitions \( p \xrightarrow{a|\vec{v}} q \)

with \( p, q \in Q, a \in \Sigma \cup \{\varepsilon\}, \vec{v} \in \mathbb{Z}^d \)

input alphabet

\( s, t \in Q \) source and target state

fails, since \( 3 - 4 < 0 \)
Vector Addition Systems with States (1)

\[ \mathcal{V} = (Q, \Sigma, \Delta, s, t) \]

- finite set of states
- input alphabet
- finite set of transitions

\[ s, t \in Q \text{ source and target state} \]

\[ a | \vec{v} \rightarrow q \]

with \( p, q \in Q, a \in \Sigma \cup \{\varepsilon\}, \vec{v} \in \mathbb{Z}^d \)

Diagram:

- States: \( s, t \)
- Transitions:
  - \( a | (2,1) \)
  - \( b | (-1,1) \)
  - \( a | (1,1) \)
  - \( b | (1,0) \)
  - \( a | (2,-4) \)

Matrix:

\[
\begin{array}{cc}
0 & 0 \\
\end{array}
\]

Matrix:

\[
\begin{array}{ccc}
a & a & b & a \\
\end{array}
\]

Note: The diagram and matrix illustrate the vector addition system \( \mathcal{V} \) with states and transitions.
Vector Addition Systems with States (1)

\( \mathcal{V} = (Q, \Sigma, \Delta, s, t) \)

finite set of states

input alphabet

finite set of transitions \( p \xrightarrow{a|\vec{v}} q \)

with \( p, q \in Q, a \in \Sigma \cup \{\varepsilon\}, \vec{v} \in \mathbb{Z}^d \)

s, t \in Q source and target state

finite set of states

2 1

a

b

a

b

a

s

a | (2, 1)

b | (−1, 1)

a | (1, 1)

b | (1, 0)

a | (2, −4)

t

fails, since 3 − 4 < 0
Vector Addition Systems with States (1)

\[ V = (Q, \Sigma, \Delta, s, t) \]

- finite set of **states**
- input alphabet
- finite set of **transitions** \( p \xrightarrow{a|\vec{v}} q \) with \( p, q \in Q \), \( a \in \Sigma \cup \{\varepsilon\} \), \( \vec{v} \in \mathbb{Z}^d \)

\[ s, t \in Q \text{ source and target state} \]

- \( a \mid (2, 1) \)
- \( b \mid (-1, 1) \)
- \( a \mid (1, 1) \)
- \( b \mid (1, 0) \)
- \( a \mid (2, -4) \)
Vector Addition Systems with States (1)

\[ \mathcal{V} = (Q, \Sigma, \Delta, s, t) \]

- finite set of **states**
- input alphabet
- finite set of **transitions** \( p \rightarrow q \)
  with \( p, q \in Q, a \in \Sigma \cup \{ \epsilon \}, \vec{v} \in \mathbb{Z}^d \)

\[ s, t \in Q \text{ source and target state} \]

\[ a \mid (2, 1) \]
\[ b \mid (-1, 1) \]
\[ a \mid (1, 1) \]
\[ b \mid (1, 0) \]
\[ a \mid (2, -4) \]
Vector Addition Systems with States (1)

\[ \mathcal{V} = \left( Q, \Sigma, \Delta, s, t \right) \]

- **finite set of states** \( Q \)
- **input alphabet** \( \Sigma \)
- **source and target state** \( s, t \in Q \)
- **finite set of transitions** \( p \xrightarrow{a|\vec{v}} q \)
  - with \( p, q \in Q, a \in \Sigma \cup \{ \epsilon \}, \vec{v} \in \mathbb{Z}^d \)

![Diagram](image)

\[ a | (2,1) \quad b | (-1,1) \quad a | (1,1) \quad b | (1,0) \quad a | (2,-4) \]

\[ \begin{array}{cc}
3 & 2 \\
\end{array} \]

\[ a \quad a \quad b \quad a \]

fails, since \( 3 - 4 < 0 \)
Vector Addition Systems with States (1)

\[ V = \left( Q, \Sigma, \Delta, s, t \right) \]

- finite set of states
- input alphabet
- finite set of transitions
- \( s, t \in Q \) source and target state

 transitions: \( p \xrightarrow{a|\vec{v}} q \) with \( p, q \in Q, a \in \Sigma \cup \{\varepsilon\}, \vec{v} \in \mathbb{Z}^d \)

Diagram:
- States: \( s, t \)
- Transitions:
  - \( a \mid (2,1) \)
  - \( a \mid (1,1) \)
  - \( a \mid (2,-4) \)
  - \( b \mid (-1,1) \)
  - \( b \mid (1,0) \)

Matrix: \[
\begin{bmatrix}
2 & 3 \\
\end{bmatrix}
\]

Matrix with inputs: \[
\begin{bmatrix}
a & a & b & a \\
a & b & a & b \\
\end{bmatrix}
\]
Vector Addition Systems with States (1)

\[ \mathcal{V} = (Q, \Sigma, \Delta, s, t) \]

- Finite set of states
- Input alphabet
- Finite set of transitions

\[ s, t \in Q \text{ source and target state} \]

\[ p \xrightarrow{a | \vec{v}} q \]

with \( p, q \in Q, a \in \Sigma \cup \{\varepsilon\}, \vec{v} \in \mathbb{Z}^d \)

\begin{align*}
\mathcal{V} & \quad \text{finite set of states} \\
\Sigma & \quad \text{input alphabet} \\
\Delta & \quad \text{finite set of transitions} \\
s, t & \quad \text{source and target state}
\end{align*}
Vector Addition Systems with States (1)

\[ \mathcal{V} = (Q, \Sigma, \Delta, s, t) \]

- **finite set of states** \( s, t \in Q \)
- **input alphabet** \( \Sigma \)
- **finite set of transitions** \( p \xrightarrow{a|\vec{v}} q \) with \( p, q \in Q, a \in \Sigma \cup \{\varepsilon\}, \vec{v} \in \mathbb{Z}^d \)

**Example:**

- \( s \) is a source state, and \( t \) is a target state.
- Transition from \( s \) to \( t \) with input \( a \) and vector \( (2, 1) \).
- Transition from \( t \) to \( s \) with input \( a \) and vector \( (2, -4) \).
- Transition from \( s \) to itself with input \( b \) and vector \( (1, 0) \), fails since \( 3 - 4 < 0 \).

States:

- \( s \) and \( t \)

Input alphabet:

- \( \Sigma \)

Vector addition operations:

- \( (2, 1) \) from \( s \) to \( t \)
- \( (1, 0) \) from \( s \) to itself
- \( (2, -4) \) from \( t \) to \( s \)
Reachability language:

\[ L_{\text{reach}}(\mathcal{V}) = \{ w \in \Sigma^* \mid (s, \vec{0}) \xrightarrow{w} (t, \vec{0}) \} \]

Coverability language:

\[ L_{\text{cov}}(\mathcal{V}) = \{ w \in \Sigma^* \mid \exists \vec{v} \in \mathbb{N}^d: (s, \vec{0}) \xrightarrow{w} (t, \vec{v}) \geq (t, \vec{0}) \} \]
Regular Separability (1)

Problem

- Given two languages $K, L \subseteq \Sigma^*$.  
- Is there a regular language $R \subseteq \Sigma^*$ with $K \subseteq R$ and $L \cap R = \emptyset$?

Note: Regular Separability $\neq$ Disjointness!
Theorem (Czerwiński et al. @ CONCUR 2018)

Let $\mathcal{V}$ and $\mathcal{W}$ be two VASS. Then $L_{\text{cov}}(\mathcal{V})$ and $L_{\text{cov}}(\mathcal{W})$ are regular separable if, and only if, $L_{\text{cov}}(\mathcal{V}) \cap L_{\text{cov}}(\mathcal{W}) = \emptyset$.

- Hence: Regular Separability for VASS coverability languages is decidable!
- Note: Decidability of Regular Separability for $L_{\text{reach}}(\mathcal{V})$ and $L_{\text{reach}}(\mathcal{W})$ is still open!

Question

What is the size of a regular separator of $L_{\text{cov}}(\mathcal{V})$ and $L_{\text{cov}}(\mathcal{W})$?

- Czerwiński et al.: doubly exp. lower bound & triply exp. upper bound
Main Theorem

Let $\mathcal{V}$ and $\mathcal{W}$ be two VASS with $\leq n$ states and updates of norm $\leq m$. If $L_{\text{cov}}(\mathcal{V}) \cap L_{\text{cov}}(\mathcal{W}) = \emptyset$ then there is an separating NFA with at most $(n + m)^{2\text{poly}(d)}$ many states.
Proof (1): Reduce to Counter Instructions

- \( \Gamma_d = \{ a_i, \overline{a_i} \mid 1 \leq i \leq d \} \)
  - \( a_i \) increase counter \( i \) by 1
  - \( \overline{a_i} \) decrease counter \( i \) by 1
- \( C_d = \{ w \in \Gamma_d^* \mid \forall \text{ prefixes } v \text{ of } w, 1 \leq i \leq d: |v|_{a_i} \geq |v|_{\overline{a_i}} \} \)

Lemma (Jantzen 1979)

\( L \subseteq \Sigma^* \) is a VASS coverability language iff there is a rational transduction \( T \) with \( L = T(C_d) \).

Corollary

Let \( \mathcal{V} \) and \( \mathcal{W} \) be two VASS and \( T \) be a rational transduction with \( L_{\text{cov}}(\mathcal{W}) = T(C_d) \). Then \( L_{\text{cov}}(\mathcal{V}) \) is regularly separable from \( L_{\text{cov}}(\mathcal{W}) \) iff \( T^{-1}(L_{\text{cov}}(\mathcal{W})) \) is regularly separable from \( C_d \).
Proof (1): Reduce to Counter Instructions

\[ \Gamma_d = \{ a_i, \overline{a_i} \mid 1 \leq i \leq d \} \]
- \( a_i \) increase counter \( i \) by 1
- \( \overline{a_i} \) decrease counter \( i \) by 1

\[ C_d = \{ w \in \Gamma_d^* \mid \forall \text{prefixes } v \text{ of } w, 1 \leq i \leq d : |v|_{a_i} \geq |v|_{\overline{a_i}} \} \]

Lemma (Jantzen 1979)

\( L \subseteq \Sigma^* \) is a VASS coverability language if and only if there is a rational transduction \( T \) with \( L = T(C_d) \).

Corollary

Let \( \mathcal{V} \) and \( \mathcal{W} \) be two VASS and \( T \) be a rational transduction with \( L_{\text{cov}}(\mathcal{W}) = T(C_d) \). Then \( L_{\text{cov}}(\mathcal{V}) \) is regularly separable from \( C_d \).
Proof (1): Reduce to Counter Instructions

- $\Gamma_d = \{a_i, \overline{a}_i \mid 1 \leq i \leq d\}$
  - $a_i$ increase counter $i$ by 1
  - $\overline{a}_i$ decrease counter $i$ by 1
- $C_d = \{w \in \Gamma_d^* \mid \forall$ prefixes $v$ of $w, 1 \leq i \leq d: |v|_{a_i} \geq |v|_{\overline{a}_i}\}$

Lemma (Jantzen 1979)

$L \subseteq \Sigma^*$ is a VASS coverability language iff there is a rational transduction $T$ with $L = T(C_d)$.

Corollary

Let $\mathcal{V}$ and $\mathcal{W}$ be two VASS and $T$ be a rational transduction with $L_{cov}(\mathcal{W}) = T(C_d)$. Then $L_{cov}(\mathcal{V})$ is regularly separable from $L_{cov}(\mathcal{W})$ iff $T^{-1}(L_{cov}(\mathcal{V}))$ is regularly separable from $C_d$. 
Proof (1): Reduce to Counter Instructions

Let $\mathcal{V}$ and $\mathcal{W}$ be two VASS and $T$ be a rational transduction with $\mathcal{L}_{\text{cov}}(\mathcal{W}) = T(C_d)$. Then $\mathcal{L}_{\text{cov}}(\mathcal{V})$ is regularly separable from $\mathcal{L}_{\text{cov}}(\mathcal{W})$ iff $T^{-1}(\mathcal{L}_{\text{cov}}(\mathcal{W}))$ is regularly separable from $C_d$. 

**Corollary**
For $k \in \mathbb{N}$ let $B_k \subseteq \Gamma_d^*$ be the following language: $w \in B_k$ iff there is $1 \leq i \leq d$ with
- there is a prefix $v$ of $w$ with $|v|_{a_i} < |v|_{\overline{a_i}}$ and
- each proper prefix $u$ of $v$ satisfies $0 \leq |u|_{a_i} - |u|_{\overline{a_i}} \leq k$

$B_k$ is accepted by a DFA of size $O(k^d)$.

Theorem (Czerwiński & Zetzsche @ LICS 2020)

Let $\mathcal{V}$ and $\mathcal{W}$ be two VASS with $L_{\text{cov}}(\mathcal{V}) \cap L_{\text{cov}}(\mathcal{W}) = \emptyset$ and let $T$ be a rational transduction with $L_{\text{cov}}(\mathcal{W}) = T(C_d)$. Then $B_k$ is a regular separator of $T^{-1}(L_{\text{cov}}(\mathcal{V}))$ and $C_d$ for a $k \in \mathbb{N}$. 
Proof (2): Basic Separators

For $k \in \mathbb{N}$ let $B_k \subseteq \Gamma_d^*$ be the following language: $w \in B_k$ iff there is $1 \leq i \leq d$ with
- there is a prefix $v$ of $w$ with $|v|_{a_i} < |v|_{\overline{a_i}}$ and
- each proper prefix $u$ of $v$ satisfies $0 \leq |u|_{a_i} - |u|_{\overline{a_i}} \leq k$

$B_k$ is accepted by a DFA of size $O(k^d)$.

Theorem (Czerwiński & Zetzsche, LICS 2020)

Let $\mathcal{V}$ and $\mathcal{W}$ be two $\mathcal{V}ASS$ with $L_{\text{cov}}(\mathcal{V}) \cap L_{\text{cov}}(\mathcal{W}) = \emptyset$ and let $T$ be a rational transduction with $L_{\text{cov}}(\mathcal{W}) = T(C_d)$. Then $B_k$ is a regular separator of $T^{-1}(L_{\text{cov}}(\mathcal{V}))$ and $C_d$ for a $k \in \mathbb{N}$. 

Proof (2): Basic Separators

- For $k \in \mathbb{N}$ let $B_k \subseteq \Gamma^*_d$ be the following language: $w \in B_k$ iff there is $1 \leq i \leq d$ with
  - there is a prefix $v$ of $w$ with $|v|_{a_i} < |v|_{\overline{a_i}}$ and
  - each proper prefix $u$ of $v$ satisfies $0 \leq |u|_{a_i} - |u|_{\overline{a_i}} \leq k$

- $B_k$ is accepted by a DFA of size $O(k^d)$.
Proof (3): Covering

Theorem (Rackoff 1978)

Let $\mathcal{V}$ be a VASS, $c$ be a configuration of $\mathcal{V}$, and a vector $\vec{v} \in \mathbb{N}^d$ with $c \rightarrow^*_{\mathcal{V}} (t, \vec{v}) \geq (t, \vec{0})$. Then there is $0 \leq \ell \leq (n + m)^{2\text{poly}(d)}$ and $\vec{w} \in \mathbb{N}^d$ with $c \rightarrow_{\mathcal{V}}^{\ell} (t, \vec{w}) \geq (t, \vec{0})$.

Here, $n$ is the number of states in $\mathcal{V}$ and $m$ is the norm of the counter updates in $\mathcal{V}$.

Theorem

Let $\mathcal{V}$ and $\mathcal{W}$ be two VASS with $L_{\text{cov}}(\mathcal{V}) \cap L_{\text{cov}}(\mathcal{W}) = \emptyset$ and let $T$ be a rational transduction with $L_{\text{cov}}(\mathcal{W}) = T(C_d)$. Then $B_{\text{Rackoff}}(\mathcal{V} \times \mathcal{W})$ is a regular separator of $T^{-1}(L_{\text{cov}}(\mathcal{V}))$ and $C_d$.

Finally, $T(B_{\text{Rackoff}}(\mathcal{V} \times \mathcal{W}))$ is a regular separator of $L_{\text{cov}}(\mathcal{V})$ and $L_{\text{cov}}(\mathcal{W})$. \qed
# Conclusion

- **$d$ as input**
  - $d \geq 2$
  - $d = 1$

- **$d$ fixed**
  - $d \geq 2$
  - $d = 1$

<table>
<thead>
<tr>
<th></th>
<th>NFAs</th>
<th>DFAs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>unary</td>
<td>binary</td>
</tr>
<tr>
<td><strong>2-exp.</strong></td>
<td>poly.</td>
<td>exp.</td>
</tr>
<tr>
<td><strong>3-exp.</strong></td>
<td>poly.</td>
<td>exp.</td>
</tr>
</tbody>
</table>

**Thank you!**