

A Relational Trace Logic for Vector Addition Systems with Application to Context-Freeness

Jérôme Leroux, M. Praveen, Grégoire Sutre

Univ. Bordeaux & CNRS, LaBRI, UMR 5800, Talence, France

CONCUR 2013, Buenos Aires, Argentina, August 2013

Table of Contents

- 1 The Context-Freeness Problem for VAS
- 2 Simple Witnesses of Non-Context-Freeness
- 3 A Relational Trace Logic for VAS with EXPSPACE Solvability
- 4 Conclusion

Table of Contents

- 1 The Context-Freeness Problem for VAS
- 2 Simple Witnesses of Non-Context-Freeness
- 3 A Relational Trace Logic for VAS with EXPSPACE Solvability
- 4 Conclusion

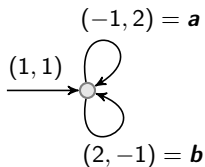
Vector Addition Systems

Definition

A **vector addition system** is a pair $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$ where

- $\mathbf{A} \subseteq \mathbb{Z}^d$: finite set of **actions**
- $\mathbf{c}_{\text{init}} \in \mathbb{N}^d$: **initial configuration**

$$\begin{aligned}\mathbf{A} &= \{(-1, 2), (2, -1)\} \\ \mathbf{c}_{\text{init}} &= (1, 1)\end{aligned}$$

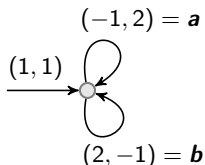
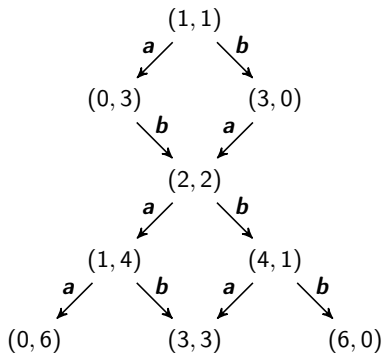


Vector Addition Systems

Definition

A **vector addition system** is a pair $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$ where

- $\mathbf{A} \subseteq \mathbb{Z}^d$: finite set of **actions**
- $\mathbf{c}_{\text{init}} \in \mathbb{N}^d$: **initial configuration**

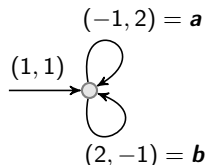
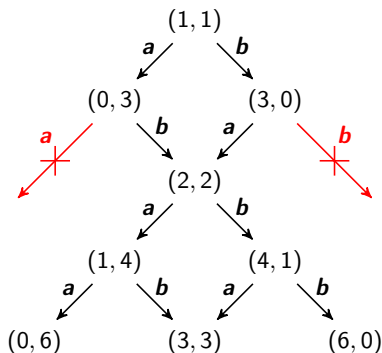


Vector Addition Systems

Definition

A **vector addition system** is a pair $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$ where

- $\mathbf{A} \subseteq \mathbb{Z}^d$: finite set of **actions**
- $\mathbf{c}_{\text{init}} \in \mathbb{N}^d$: **initial configuration**



Definition

A **trace** is a sequence $\mathbf{a}_1, \dots, \mathbf{a}_n$ such that

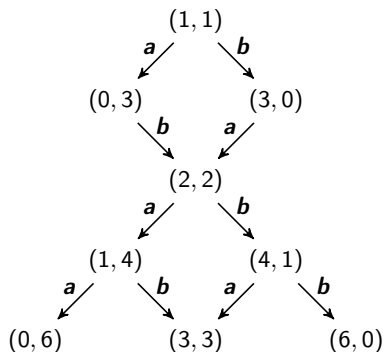
$$c_{\text{init}} \xrightarrow{\mathbf{a}_1} c_1 \cdots c_{n-1} \xrightarrow{\mathbf{a}_n} c_n$$

Trace Language

Definition

A **trace** is a sequence a_1, \dots, a_n such that

$$c_{\text{init}} \xrightarrow{a_1} c_1 \cdots c_{n-1} \xrightarrow{a_n} c_n$$



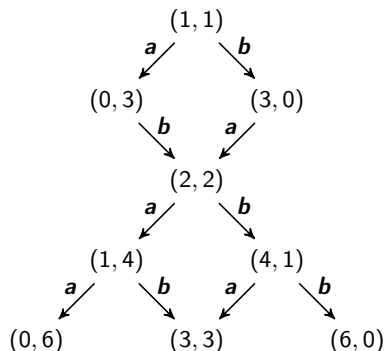
- **abb** is a trace
- **aa** is **not** a trace

Trace Language

Definition

A **trace** is a sequence a_1, \dots, a_n such that

$$c_{\text{init}} \xrightarrow{a_1} c_1 \cdots c_{n-1} \xrightarrow{a_n} c_n$$



- **abb** is a trace
- **aa** is **not** a trace

Definition

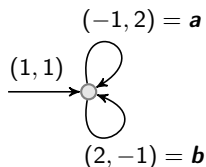
The **trace language** is the set of all traces

The Context-Freeness Problem

Definition

Input: A VAS $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$

Output: Is the trace language of $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$ context-free?

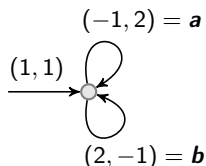


The Context-Freeness Problem

Definition

Input: A VAS $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$

Output: Is the trace language of $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$ context-free?



Its trace language is **not** context-free:

$$L \cap (ab)^* a^* b^* = \{(ab)^n a^m b^p \mid n + 1 \geq m \wedge n + 1 + 2m \geq p\}$$

Regularity

- Decidable [Valk&Vidal-Naquet 81, Ginzburg&Yoeli 80]
 - ▶ Non-regular \Leftrightarrow the coverability graph contains a cycle $\mathbf{x} \xrightarrow{\sigma} \mathbf{x}$ with $\|\Delta(\sigma)\|^- \neq \emptyset$
- EXPSPACE-complete [Demri 10]
 - ▶ Witness: trace $u_1\sigma_1 \cdots u_k\sigma_k$ such that $L \cap (u_1\sigma_1^* \cdots u_k\sigma_k^*)$ is not regular
 - ▶ Length at most doubly-exponential (in $|\mathbf{A}|$)

$$\Delta(\mathbf{a}_1 \cdots \mathbf{a}_n) = \mathbf{a}_1 + \cdots + \mathbf{a}_n$$

$$\begin{aligned} \|\mathbf{v}\|^+ &= \{i \mid \mathbf{v}(i) > 0\} \\ \|\mathbf{v}\|^- &= \{i \mid \mathbf{v}(i) < 0\} \end{aligned}$$

Regularity and Context-Freeness: State of the Art

Regularity

- Decidable [Valk&Vidal-Naquet 81, Ginzburg&Yoeli 80]
 - ▶ Non-regular \Leftrightarrow the coverability graph contains a cycle $\mathbf{x} \xrightarrow{\sigma} \mathbf{x}$ with $\|\Delta(\sigma)\|^- \neq \emptyset$
- EXPSPACE-complete [Demri 10]
 - ▶ Witness: trace $u_1\sigma_1 \cdots u_k\sigma_k$ such that $L \cap (u_1\sigma_1^* \cdots u_k\sigma_k^*)$ is not regular
 - ▶ Length at most doubly-exponential (in $|\mathbf{A}|$)

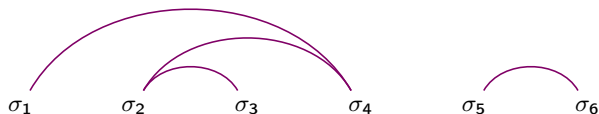
Context-Freeness

- Decidable [Schwer 92]
 - ▶ Complex criterion, based on the coverability graph
- Decidable [Leroux&Penelle&Sutre 13]
 - ▶ Witness: trace $u_1\sigma_1 \cdots u_k\sigma_k$ such that $L \cap (u_1\sigma_1^* \cdots u_k\sigma_k^*)$ is not context-free

Table of Contents

- 1 The Context-Freeness Problem for VAS
- 2 Simple Witnesses of Non-Context-Freeness
- 3 A Relational Trace Logic for VAS with EXPSpace Solvability
- 4 Conclusion

Matching Schemes



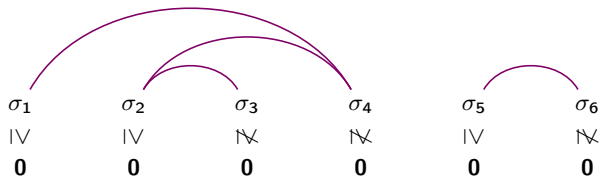
Definition

A **matching scheme** is a tuple $(\sigma_1, \dots, \sigma_k, U)$ such that

- $\sigma_1, \dots, \sigma_k$: words in \mathbf{A}^*
- U : binary relation on $\{1, \dots, k\}$ that is **nested**:

$$\begin{aligned}(s, t) \in U &\Rightarrow s \leq t \\ (r, t) \in U \wedge (s, u) \in U &\Rightarrow \neg(r < s < t < u)\end{aligned}$$

Matching Schemes



Definition

A **matching scheme** is a tuple $(\sigma_1, \dots, \sigma_k, U)$ such that

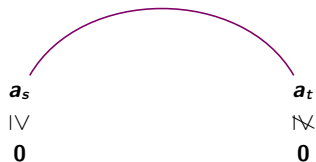
- $\sigma_1, \dots, \sigma_k$: words in \mathbf{A}^*
- U : binary relation on $\{1, \dots, k\}$ that is **nested**:

$$(s, t) \in U \Rightarrow s \leq t$$
$$(r, t) \in U \wedge (s, u) \in U \Rightarrow \neg(r < s < t < u)$$

- For every $(s, t) \in U$, $\Delta(\sigma_s) \geq \mathbf{0}$ and $\Delta(\sigma_t) \not\geq \mathbf{0}$

Loss by Matching $(s, t) \in U$

Consider the case of single actions: $\sigma_s = \mathbf{a}_s$ and $\sigma_t = \mathbf{a}_t$

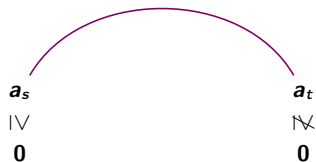


$$\begin{aligned}\mathbf{a}_s &= (1, 1) \\ \mathbf{a}_t &= (-1, -2)\end{aligned}$$

Use one \mathbf{a}_s to do as many \mathbf{a}_t as possible. What do we lose?

Loss by Matching $(s, t) \in U$

Consider the case of single actions: $\sigma_s = \mathbf{a}_s$ and $\sigma_t = \mathbf{a}_t$



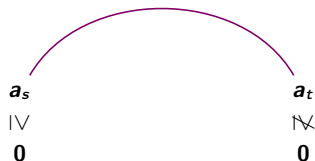
$$\begin{aligned}\mathbf{a}_s &= (1, 1) \\ \mathbf{a}_t &= (-1, -2) \\ \lambda_{s,t} &= \frac{1}{2}\end{aligned}$$

Use one \mathbf{a}_s to do as many \mathbf{a}_t as possible. What do we lose?

Ratio: $\lambda_{s,t} = \max \{ \lambda \in \mathbb{Q} \mid \mathbf{a}_s + \lambda \mathbf{a}_t \geq \mathbf{0} \}$

Loss by Matching $(s, t) \in U$

Consider the case of single actions: $\sigma_s = \mathbf{a}_s$ and $\sigma_t = \mathbf{a}_t$



$$\mathbf{a}_s = (1, 1)$$

$$\mathbf{a}_t = (-1, -2)$$

$$\lambda_{s,t} = \frac{1}{2}$$

$$\text{lost}(s, t) = \{1\}$$

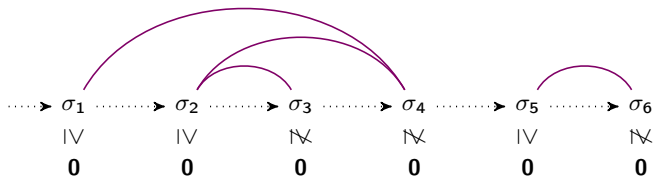
Use one \mathbf{a}_s to do as many \mathbf{a}_t as possible. What do we lose?

Ratio: $\lambda_{s,t} = \max \{ \lambda \in \mathbb{Q} \mid \mathbf{a}_s + \lambda \mathbf{a}_t \geq \mathbf{0} \}$

Definition

$$\text{lost}(s, t) = \|\mathbf{a}_s + \lambda_{s,t} \mathbf{a}_t\|^+$$

Witnesses of Non-Context-Freeness

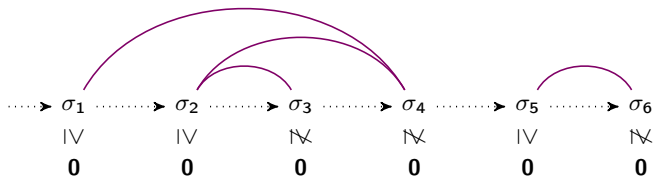


Definition

A **witness of non-context-freeness** is a tuple $(\sigma_1, \dots, \sigma_k, U)$ such that

- $(\sigma_1, \dots, \sigma_k, U)$: matching scheme
- $u_1\sigma_1 \cdots u_k\sigma_k$ is a trace for some u_1, \dots, u_k
- $\Delta(\sigma_k) \not\leq \mathbf{0}$ and $\|\Delta(\sigma_k)\|^- \subseteq \bigcup_{(s,t) \in U} \text{lost}(s, t)$
- $\|\Delta(\sigma_t)\|^- \subseteq \|\Delta(\sigma_{s_{\min}(t)})\|^+$ for all $(\cdot, t) \in U$ with $t < k$

Witnesses of Non-Context-Freeness



Definition

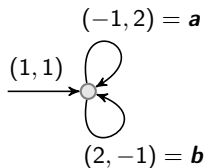
A **witness of non-context-freeness** is a tuple $(\sigma_1, \dots, \sigma_k, U)$ such that

- $\Delta(\sigma_k) \not\leq \mathbf{0}$ and $\|\Delta(\sigma_k)\|^- \subseteq \bigcup_{(s,t) \in U} \text{lost}(s, t)$
- ...

Theorem (Leroux&Penelle&Sutre:2013)

The trace language of $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$ is not context-free iff $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$ admits a witness of non-context-freeness

Witnesses of Non-Context-Freeness: Example



$L \cap (ab)^*a^*b^*$ is not context-free

Witness



- The largest rational λ such that $\Delta(ab) + \lambda\Delta(a) \geq \mathbf{0}$ is $\lambda_{1,2} = 1$
- $\text{lost}(1, 2) = \|\Delta(ab) + 1\Delta(a)\|^+ = \|(0, 3)\|^+ = \{2\}$ contains $\|b\|^-$

Definition

A **witness of non-context-freeness** is a tuple $(\sigma_1, \dots, \sigma_k, U)$ such that

- $\Delta(\sigma_k) \not\preceq \mathbf{0}$ and $\|\Delta(\sigma_k)\|^- \subseteq \bigcup_{(s,t) \in U} \text{lost}(s, t)$
- ...

⇒ Bound k

⇒ **Non-linear** arithmetic constraints over the $\Delta(\sigma_j)$

$$i \in \text{lost}(s, t) \quad \Leftrightarrow \quad \vee \begin{array}{l} \delta_t(i) > 0 \wedge (\delta_s(i) > 0 \vee \|\delta_t\|^- \subseteq \|\delta_s\|^+) \\ \delta_t(i) \leq 0 \wedge \bigvee_{j \neq i} \delta_s(i) \cdot \delta_t(j) < \delta_s(j) \cdot \delta_t(i) \end{array}$$

(δ_j stands for $\Delta(\sigma_j)$)

Proposition

The trace language of $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$ is not context-free iff $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$ admits a witness of non-context-freeness $(\sigma_1, \dots, \sigma_k, U)$ such that

- $k \leq 3d + 1$
- for every $(s, t) \in U$, the ratio $\lambda_{s,t}$ is either 0 or 1

Proposition

The trace language of $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$ is not context-free iff $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$ admits a witness of non-context-freeness $(\sigma_1, \dots, \sigma_k, U)$ such that

- $k \leq 3d + 1$
- for every $(s, t) \in U$, the ratio $\lambda_{s,t}$ is either 0 or 1

Proof:

- Simplify U by keeping only pairs that add new lost components
- At most two pairs (s, t) and $(s_{\min}(t), t)$ for each $i \in \{1, \dots, d\}$
- Remove useless σ_j but keep σ_k

Proposition

The trace language of $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$ is not context-free iff $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$ admits a witness of non-context-freeness $(\sigma_1, \dots, \sigma_k, U)$ such that

- $k \leq 3d + 1$
- for every $(s, t) \in U$, the ratio $\lambda_{s,t}$ is either 0 or 1

Proof:

- Let $(s, t) \in U$ with positive ratio $\lambda_{s,t} = \frac{p}{q}$
- Replacing σ_s by $(\sigma_s)^q$ and σ_t by $(\sigma_t)^p$ yields the ratio $\frac{q}{p} \cdot \frac{p}{q} = 1$
- But this modifies the ratio of other pairs (s', t) and (s, t')
- Follow nesting of U to prevent conflicts

Encoding by Linear Arithmetic Constraints

The requirement that $\lambda_{s,t} \in \{0, 1\}$ simplifies the encoding of $\text{lost}(s, t)$

$$i \in \text{lost}(s, t) \Leftrightarrow i \in \|\delta_s + \lambda_{s,t}\delta_t\|^+$$

$$\begin{aligned} & \lambda_{s,t} = 0 \wedge \delta_s(i) > 0 \\ \Leftrightarrow & \vee \\ & \lambda_{s,t} = 1 \wedge \delta_s(i) + \delta_t(i) > 0 \end{aligned}$$

$$\lambda_{s,t} = 0 \Leftrightarrow \bigvee_{i=1}^d (\delta_s(i) = 0 \wedge \delta_t(i) < 0)$$

$$\lambda_{s,t} = 1 \Leftrightarrow \delta_s + \delta_t \geq \mathbf{0} \wedge \bigvee_{i=1}^d (\delta_s(i) + \delta_t(i) = 0 \wedge \delta_t(i) < 0)$$

Encoding by Linear Arithmetic Constraints

The requirement that $\lambda_{s,t} \in \{0, 1\}$ simplifies the encoding of $\text{lost}(s, t)$

$$i \in \text{lost}(s, t) \Leftrightarrow i \in \|\delta_s + \lambda_{s,t}\delta_t\|^+$$

$$\begin{aligned} & \lambda_{s,t} = 0 \wedge \delta_s(i) > 0 \\ \Leftrightarrow & \vee \\ & \lambda_{s,t} = 1 \wedge \delta_s(i) + \delta_t(i) > 0 \end{aligned}$$

$$\lambda_{s,t} = 0 \Leftrightarrow \bigvee_{i=1}^d (\delta_s(i) = 0 \wedge \delta_t(i) < 0)$$

$$\lambda_{s,t} = 1 \Leftrightarrow \delta_s + \delta_t \geq 0 \wedge \bigvee_{i=1}^d (\delta_s(i) + \delta_t(i) = 0 \wedge \delta_t(i) < 0)$$

⇒ Need **linear relations** between $\Delta(\sigma_1), \dots, \Delta(\sigma_k)$

Table of Contents

- 1 The Context-Freeness Problem for VAS
- 2 Simple Witnesses of Non-Context-Freeness
- 3 A Relational Trace Logic for VAS with EXPSPACE Solvability**
- 4 Conclusion

Logics for Expressing Properties of VAS Behaviors

Yen's path logic [Yen 92]

- Powerful enough to express witnesses of non-context-freeness
- Model-checking **REACHABILITY-hard** [Atig&Habermehl 09]

Logics solvable in **exponential space**

- Increasing fragment of Yen's path logic [Atig&Habermehl 09]
- Generalized unbounded properties [Demri 10]
- Eventually increasing $\text{PrECTL}_{\geq}(F)$ [Blockelet&Schmitz 11]

Lack the ability to express witnesses of non-context-freeness

- Witnesses need not be increasing
- Generalized unbounded properties are non-relational

Yet Another Logic for VAS Traces: Syntax

Given a trace of the form $u_1 \sigma_1 \cdots u_k \sigma_k$

$\cdots \rightarrow \sigma_1 \cdots \rightarrow \sigma_2 \cdots \rightarrow \sigma_3 \cdots \rightarrow \sigma_4 \cdots \rightarrow \sigma_5 \cdots \rightarrow \sigma_6$

The logic expresses properties of $\Delta(\sigma_1), \dots, \Delta(\sigma_k)$

Definition

$$t ::= z \delta_j(i) \mid t + t \quad (z \in \mathbb{Z}, j \geq 1, 1 \leq i \leq d)$$

$$\phi ::= t \geq n \mid \phi \vee \phi \mid \phi \wedge \phi \quad (n \in \mathbb{N})$$

Variables δ_j are interpreted as $\Delta(\sigma_j)$

Yet Another Logic for VAS Traces: Semantics

Definition (Demri 10)

A trace $u_1 \sigma_1 \cdots u_k \sigma_k$ is **self-covering** when

$$\|\Delta(\sigma_j)\|^- \subseteq \|\Delta(\sigma_1)\|^+ \cup \cdots \cup \|\Delta(\sigma_{j-1})\|^+ \quad (\forall j \leq k)$$

Definition

$$\begin{aligned} u_1 \sigma_1 \cdots u_k \sigma_k \models \phi & \text{ if } \phi[\Delta(\sigma_j) / \delta_j] \text{ holds} \\ \langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle \models \phi & \text{ if } u_1 \sigma_1 \cdots u_k \sigma_k \models \phi \text{ for some s.-c. trace} \end{aligned}$$

- ⇒ The model-checking problem **would** become REACHABILITY-hard if
- arbitrary traces were allowed
 - intermediate steps were forbidden ($u_j = \varepsilon$)

A Few Example Properties

Unboundedness: $\bigvee_{i=1}^d \delta_1(i) \geq 1$

Place unboundedness: $\bigvee_{j=1}^d \delta_j(p) \geq 1$

Non-regularity: $\bigvee_{i=1}^d -\delta_{d+1}(i) \geq 1$

Non-context-freeness: $\bigvee_{k=1}^{3d+1} \bigvee_{\substack{U \subseteq \{1, \dots, k\} \\ \text{nested}}} \dots \delta_s(i) + \delta_t(i) = 0 \dots$

Main Technical Result: Small Model Property

Theorem

If there is a self-covering trace in $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle$ satisfying ϕ , then there is one of length at most

$$2^{p(|\mathbf{A}|+|\phi|)} \cdot c^{(d \cdot k(\phi))^3}$$

where p is a polynomial and c is a constant

Corollary

The model-checking problem $\langle \mathbf{A}, \mathbf{c}_{\text{init}} \rangle \stackrel{?}{\models} \phi$ is EXPSPACE-complete

Corollary

The context-freeness problem for VAS is EXPSPACE-complete

Overview of the Proof: Bounding Intermediate Words

$$c_{\text{init}} \xrightarrow{u_1} c_1 \xrightarrow{\sigma_1} c'_1 \cdots \xrightarrow{u_k} c_k \xrightarrow{\sigma_k} c'_k \qquad |\sigma_1| + \cdots + |\sigma_k| \leq L$$

$$\sigma \rightsquigarrow (b^-, b^+)$$

$$c \xrightarrow{\sigma} c' \Leftrightarrow c \xrightarrow{b^-} \cdot \xrightarrow{b^+} c'$$

Overview of the Proof: Bounding Intermediate Words

$$c_{\text{init}} \xrightarrow{u_1} c_1 \xrightarrow{\sigma_1} c'_1 \cdots \xrightarrow{u_k} c_k \xrightarrow{\sigma_k} c'_k \quad |\sigma_1| + \cdots + |\sigma_k| \leq L$$

$$\sigma \rightsquigarrow (b^-, b^+) \quad c \xrightarrow{\sigma} c' \Leftrightarrow c \xrightarrow{b^-} \cdot \xrightarrow{b^+} c'$$

New VAS: $\begin{bmatrix} a \\ 0 \end{bmatrix}$, $\begin{bmatrix} b_j^- \\ 1 \end{bmatrix}$, $\begin{bmatrix} b_j^+ \\ 1 \end{bmatrix}$ ($a \in \mathbf{A}, 1 \leq j \leq k$)

$$c_{\text{init}} \xrightarrow{w} \cdot \geq \begin{bmatrix} 0 \\ 2k \end{bmatrix} \quad w = \begin{bmatrix} u_1 \\ 0 \end{bmatrix} \begin{bmatrix} b_1^- \\ 1 \end{bmatrix} \begin{bmatrix} b_1^+ \\ 1 \end{bmatrix} \cdots \begin{bmatrix} u_k \\ 0 \end{bmatrix} \begin{bmatrix} b_k^- \\ 1 \end{bmatrix} \begin{bmatrix} b_k^+ \\ 1 \end{bmatrix}$$

Overview of the Proof: Bounding Intermediate Words

$$c_{\text{init}} \xrightarrow{u_1} c_1 \xrightarrow{\sigma_1} c'_1 \cdots \xrightarrow{u_k} c_k \xrightarrow{\sigma_k} c'_k \quad |\sigma_1| + \cdots + |\sigma_k| \leq L$$

$$\sigma \rightsquigarrow (b^-, b^+) \quad c \xrightarrow{\sigma} c' \Leftrightarrow c \xrightarrow{b^-} \cdot \xrightarrow{b^+} c'$$

New VAS: $\begin{bmatrix} a \\ 0 \end{bmatrix}$, $\begin{bmatrix} b_j^- \\ 1 \end{bmatrix}$, $\begin{bmatrix} b_j^+ \\ 1 \end{bmatrix}$ ($a \in \mathbf{A}, 1 \leq j \leq k$)

$$c_{\text{init}} \xrightarrow{w} \cdot \geq \begin{bmatrix} \mathbf{0} \\ 2k \end{bmatrix} \quad w = \begin{bmatrix} u_1 \\ 0 \end{bmatrix} \begin{bmatrix} b_1^- \\ 1 \end{bmatrix} \begin{bmatrix} b_1^+ \\ 1 \end{bmatrix} \cdots \begin{bmatrix} u_k \\ 0 \end{bmatrix} \begin{bmatrix} b_k^- \\ 1 \end{bmatrix} \begin{bmatrix} b_k^+ \\ 1 \end{bmatrix}$$

Lemma (Rackoff 78)

If $c_{\text{init}} \xrightarrow{w} \cdot \geq c$ then $c_{\text{init}} \xrightarrow{w'} \cdot \geq c$ for some *short subword* w' of w

Overview of the Proof: Bounding Intermediate Words

$$c_{\text{init}} \xrightarrow{u_1} c_1 \xrightarrow{\sigma_1} c'_1 \cdots \xrightarrow{u_k} c_k \xrightarrow{\sigma_k} c'_k \quad |\sigma_1| + \cdots + |\sigma_k| \leq L$$

$$\sigma \rightsquigarrow (b^-, b^+) \quad c \xrightarrow{\sigma} c' \Leftrightarrow c \xrightarrow{b^-} \cdot \xrightarrow{b^+} c'$$

New VAS: $\begin{bmatrix} a \\ 0 \end{bmatrix}$, $\begin{bmatrix} b_j^- \\ 1 \end{bmatrix}$, $\begin{bmatrix} b_j^+ \\ 1 \end{bmatrix}$ ($a \in \mathbf{A}, 1 \leq j \leq k$)

$$c_{\text{init}} \xrightarrow{w} \cdot \geq \begin{bmatrix} 0 \\ 2k \end{bmatrix} \quad w = \begin{bmatrix} u_1 \\ 0 \end{bmatrix} \begin{bmatrix} b_1^- \\ 1 \end{bmatrix} \begin{bmatrix} b_1^+ \\ 1 \end{bmatrix} \cdots \begin{bmatrix} u_k \\ 0 \end{bmatrix} \begin{bmatrix} b_k^- \\ 1 \end{bmatrix} \begin{bmatrix} b_k^+ \\ 1 \end{bmatrix}$$

$$c_{\text{init}} \xrightarrow{w'} \cdot \geq \begin{bmatrix} 0 \\ 2k \end{bmatrix} \quad w' = \begin{bmatrix} u'_1 \\ 0 \end{bmatrix} \begin{bmatrix} b_1^- \\ 1 \end{bmatrix} \begin{bmatrix} b_1^+ \\ 1 \end{bmatrix} \cdots \begin{bmatrix} u'_k \\ 0 \end{bmatrix} \begin{bmatrix} b_k^- \\ 1 \end{bmatrix} \begin{bmatrix} b_k^+ \\ 1 \end{bmatrix}$$

$\Rightarrow u'_1 \sigma_1 \cdots u'_k \sigma_k$ is a trace of $\langle \mathbf{A}, c_{\text{init}} \rangle$ with $|u'_1| + \cdots + |u'_k| \leq |w'|$ \square

Overview of the Proof: Bounding Cycles

$$c_{\text{init}} \xrightarrow{u_1} c_1 \xrightarrow{\sigma_1} c'_1 \cdots \xrightarrow{u_k} c_k \xrightarrow{\sigma_k} c'_k \models \phi$$

Reduce to finding short σ such that

$$x \xrightarrow{\sigma} x \quad \text{and} \quad \mathbf{Z}\Delta(\sigma) \geq \mathbf{n}$$

where $x \in \mathbb{N}_{\omega}^d$, $\mathbf{Z} \in \mathbb{Z}^{r \times d}$, $\mathbf{n} \in \mathbb{N}^r$

Overview of the Proof: Bounding Cycles

$$c_{\text{init}} \xrightarrow{u_1} c_1 \xrightarrow{\sigma_1} c'_1 \cdots \xrightarrow{u_k} c_k \xrightarrow{\sigma_k} c'_k \models \phi$$

Reduce to finding short σ such that

$$x \xrightarrow{\sigma} x \quad \text{and} \quad \mathbf{Z}\Delta(\sigma) \geq \mathbf{n}$$

$$\text{where } x \in \mathbb{N}_{\omega}^d, \mathbf{Z} \in \mathbb{Z}^{r \times d}, \mathbf{n} \in \mathbb{N}^r$$

Reduce to finding short **reversible** traces and use [Leroux 13]

 J. Leroux.

Vector addition system reversible reachability problem.

Logical Methods in Computer Science, 9(1), 2013.

Table of Contents

- 1 The Context-Freeness Problem for VAS
- 2 Simple Witnesses of Non-Context-Freeness
- 3 A Relational Trace Logic for VAS with EXPSPACE Solvability
- 4 Conclusion

Conclusion

New logic for expressing properties of VAS traces

- Can express linear relations between cycles visited by a run
- Model-checking is EXPSPACE -complete
- Incomparable with existing logics that are solvable in EXPSPACE

Complexity of the context-freeness problem: EXPSPACE -complete

- Simplification and encoding in the logic of the criterion given in [Leroux&Penelle&Sutre 13]
- EXPSPACE -hardness by reduction from the boundedness problem

Conclusion

New logic for expressing properties of VAS traces

- Can express linear relations between cycles visited by a run
- Model-checking is EXPSPACE -complete
- Incomparable with existing logics that are solvable in EXPSPACE

Complexity of the context-freeness problem: EXPSPACE -complete

- Simplification and encoding in the logic of the criterion given in [Leroux&Penelle&Sutre 13]
- EXPSPACE -hardness by reduction from the boundedness problem

Open Problems

- Allow negative constants n in $t \geq n$
 - ▶ Subsumes generalized unbounded properties [Demri 10]
- Existing EXPSPACE logics are incomparable: try to unify them!

There is hopefully still time for ...

Questions ?

Overview of the Proof: Bounding Cycles

Let $\mathbf{c}_{\text{init}} \xrightarrow{u} \mathbf{c} \xrightarrow{\sigma} \mathbf{c}'$ with $\Delta(\sigma) \geq \mathbf{0}$ and $u\sigma \models \phi$, where $\phi = \mathbf{Z}\delta \geq n$

Require in $\mathbf{Z}\delta \geq n$ that $\delta(i)$ has the same sign as $\Delta(\sigma)(i)$

$$\mathbf{Z}\delta \geq n \quad \Leftrightarrow \quad \bigvee_{\text{finite}} \delta \in \mathbf{p}_0 + \mathbb{N}\mathbf{p}_0 + \mathbb{N}\mathbf{p}_1 + \cdots + \mathbb{N}\mathbf{p}_m$$

$$\Delta(\sigma) = \mathbf{p}_0 + \alpha_0\mathbf{p}_0 + \alpha_1\mathbf{p}_1 + \cdots + \alpha_m\mathbf{p}_m$$

Introduce $\mathbf{x} \in \mathbb{N}_w^d$ obtained by iterating σ : $\mathbf{c}_{\text{init}} \xrightarrow{u} \mathbf{c} \xrightarrow{\sigma^\omega} \mathbf{x}$

In $\tilde{\mathbf{A}} = \mathbf{A} \cup \{-\mathbf{p}_0, \dots, -\mathbf{p}_m\}$, the action $-\mathbf{p}_0$ is **reversible** on \mathbf{x} because $\mathbf{x} \xrightarrow{-\mathbf{p}_0} \mathbf{x} \xrightarrow{v} \mathbf{x}$ and $\Delta(v) = \mathbf{p}_0$, where $v = (-\mathbf{p}_0)^{\alpha_0} \cdots (-\mathbf{p}_m)^{\alpha_m} \cdot \sigma$

By [Leroux 13], $\mathbf{x} \xrightarrow{-\mathbf{p}_0} \mathbf{x} \xrightarrow{v'} \mathbf{x}$ for some short v' with $\Delta(v') = \mathbf{p}_0$

Project v' on \mathbf{A} to get a short σ' such that $\mathbf{x} \xrightarrow{\sigma'} \mathbf{x}$ and $\mathbf{Z}\Delta(\sigma') \geq n$

For β large enough, $(u\sigma^\beta)\sigma'$ is a self-covering trace □