Vector Addition System Reachability Problem

Jérôme Leroux

LaBRI (CNRS and University of Bordeaux), France.

January 20, 2011

Vector Addition System Reachability Problem

Definition

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

$\mathbf{A}$ set of actions.
$\mathbb{N}^d$ set of markings.

A run is a non-empty word $\rho = \mathbf{m}_0 \ldots \mathbf{m}_k$ of markings such that:

$$\forall j \in \{1, \ldots, k\} \qquad \mathbf{m}_j \; \in \; \mathbf{m}_{j-1} + \mathbf{A}$$

In this case, $\mathbf{m}_k$ is said to be reachable from $\mathbf{m}_0$.

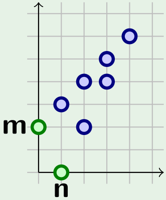
Theorem (Mayr 1981, Kosaraju 1982)

The reachability problem is decidable.

Reachable Case

Example

A = {  ,  }

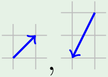


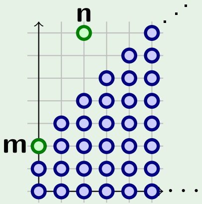
n is reachable from **m**.

$$\rho = (0,2)\ (1,3)\ (2,4)\ (3,5)\ (4,6)\ (3,4)\ (2,2)\ (1,0)$$

Unreachable Case

Example

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



n is not reachable from **m**.

$$\phi(x_1, x_2) \ := \ 0 \leq x_1 \ \wedge \ 0 \leq x_2 \ \wedge \ x_2 \leq x_1 + 2$$

Vector addition systems are equivalent to other models:

- Vector addition systems with states
- Petri nets.

VASS

Definition

A vector addition system with states (VASS) is a graph $G = (Q, \Delta)$ where:

Q is a non-empty finite set of control states

$\Delta \subseteq Q \times \mathbb{Z}^d \times Q$ is a finite set of transitions.

$Q \times \mathbb{N}^d$ set of configurations

A run is a non-empty word $(q_0, \mathbf{m}_0) \ldots (q_k, \mathbf{m}_k)$ of configurations such that $(q_{j-1}, \mathbf{m}_j - \mathbf{m}_{j-1}, q_j) \in \Delta$ for every $j \in \{1, \ldots, k\}$.
In this case $(q_k, \mathbf{m}_k)$ is said to be reachable from $(q_0, \mathbf{m}_0)$.

Let $\mathbf{A}$ be a VAS.

We introduce the VASS $G = (\{q\}, \Delta)$ with $\Delta = \{q\} \times \mathbf{A} \times \{q\}$.

Lemma

$\mathbf{n}$ is reachable from $\mathbf{m}$ in the VAS $\mathbf{A}$
if and only if
$(q, \mathbf{n})$ is reachable from $(q, \mathbf{m})$ in the VASS G.

Reductions : VASS 2 VAS

Assume that $G = (Q, \Delta)$ is a VASS without any self loop and such that $Q = \{1, \ldots, k\}$.

We introduce the unitary vector $\mathbf{e}_i$:

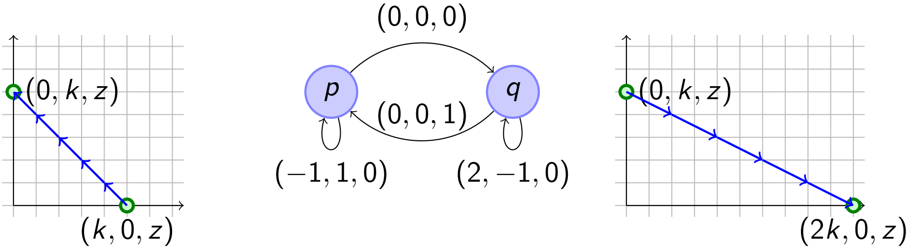
$$\mathbf{e}_i = (0, \ldots, 0, \underset{\substack{\uparrow \\ i}}{1}, 0, \ldots, 0)$$

We introduce the VAS $\mathbf{A} = \{(\mathbf{e}_j - \mathbf{e}_i, \mathbf{z}) \mid (i, \mathbf{z}, j) \in \Delta\}$.

Lemma

$(j, \mathbf{n})$ is reachable from $(i, \mathbf{m})$ in the VASS G
if and only if
$(\mathbf{e}_j, \mathbf{n})$ is reachable from $(\mathbf{e}_i, \mathbf{m})$ in the the VAS $\mathbf{A}$.

The Hopcroft-Pansiot 1979 Example



Configurations reachable from $(p, (1, 0, 0))$

$$\{p\} \times \{(x, y, z) \in \mathbb{N}^3 \mid x + y \leq 2^z\}$$
$$\cup\{q\} \times \{(x, y, z) \in \mathbb{N}^3 \mid x + 2y \leq 2^{z+1}\}$$

Equivalence Problem

Definition (Equivalence Problem)

INPUT : $(\mathbf{A}_1, \mathbf{m}_1)$ and $(\mathbf{A}_2, \mathbf{m}_2)$ two vector addition systems equipped with initial markings.

OUTPUT : Decide the equality of the reachability sets.

Theorem (Hack 1976)

The equivalence problem is undecidable.

$\Longrightarrow$ No decidable logic for denoting reachability sets.

Subconclusion

Some equivalent models:

- Vector addition systems (ideal for proofs)
- Vector addition systems with states (ideal for examples)
- Petri nets (ideal for modeling parallel processes)

No decidable logic for denoting reachability sets.
In the sequel, we show that there is a decidable logic for geometrical properties asymptotically verified by these sets:

Example

$$\{p\} \times \{(x,y,z) \in \mathbb{N}^3 \mid x + y \leq 2^z\}$$
$$\cup \{q\} \times \{(x,y,z) \in \mathbb{N}^3 \mid x + 2y \leq 2^{z+1}\}$$

$\Longrightarrow$ x and y can be very large compared to z.

Outline

Definition (Vector Spaces)

A set $\mathbf{V} \subseteq \mathbb{Q}^d$ is called a vector space if $\mathbf{0} \in \mathbf{V}$, $\mathbf{V} + \mathbf{V} \subseteq \mathbf{V}$ and $\mathbb{Q}\mathbf{V} \subseteq \mathbf{V}$.

Example

The vector spaces $\mathbf{V}$ included in $\mathbb{Q}^2$ are exactly:

- The whole set $\mathbb{Q}^2$,
- The line vector spaces $\mathbb{Q}\mathbf{v}$ with $\mathbf{v} \neq (0,0)$, or
- The zero vector space $\{(0,0)\}$.

Lemma

For every vector space $\mathbf{V} \subseteq \mathbb{Q}^d$ *there exists at most* d *vectors* $\mathbf{v}_1, \ldots, \mathbf{v}_r \in \mathbf{V}$ *satisfying:*

$$\mathbf{V} = \mathbb{Q}\mathbf{v}_1 + \cdots + \mathbb{Q}\mathbf{v}_r$$

Definition (Rank)

The rank of a vector space $\mathbf{V}$ is the minimal $r \in \mathbb{N}$ denoted by $\text{rank}(\mathbf{V})$ such that there exists a sequence $\mathbf{v}_1, \ldots, \mathbf{v}_r$ of vectors in $\mathbf{V}$ satisfying:

$$\mathbf{V} = \mathbb{Q}\mathbf{v}_1 + \cdots + \mathbb{Q}\mathbf{v}_r$$

Example

The vector spaces $\mathbf{V}$ included in $\mathbb{Q}^2$ are exactly:

- $\text{rank}(\mathbf{V}) = 2$: The whole set $\mathbb{Q}^2$,
- $\text{rank}(\mathbf{V}) = 1$: The line vector spaces $\mathbb{Q}\mathbf{v}$ with $\mathbf{v} \neq (0,0)$, or
- $\text{rank}(\mathbf{V}) = 0$: The zero vector space $\{(0,0)\}$.

Strict Monotonic Property

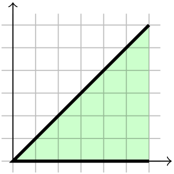
Lemma (Strict Monotonic Property)

$\mathrm{rank}(\mathbf{V}) < \mathrm{rank}(\mathbf{W})$ *for every vector spaces* $\mathbf{V} \subset \mathbf{W}$.

Definition

A set $\mathbf{C} \subseteq \mathbb{Q}^d$ is said to be conic if $\mathbf{0} \in \mathbf{C}$, $\mathbf{C} + \mathbf{C} \subseteq \mathbf{C}$ and $\mathbb{Q}_{\geq 0}\mathbf{C} \subseteq \mathbf{C}$. A conic set $\mathbf{C}$ is said to be finitely generated if there exist $\mathbf{c}_1, \ldots, \mathbf{c}_k \in \mathbf{C}$ such that:

$$\mathbf{C} = \mathbb{Q}_{\geq 0}\mathbf{c}_1 + \cdots + \mathbb{Q}_{\geq 0}\mathbf{c}_k$$



$$\mathbb{Q}_{\geq 0}(1, 1) + \mathbb{Q}_{\geq 0}(1, 0)$$

Vector Spaces And Conic Sets

Lemma

The set $\mathbf{V} = \mathbf{C} - \mathbf{C}$ is a vector space for every conic set $\mathbf{C}$. This vector space is the unique minimal one that contains $\mathbf{C}$.

Definition

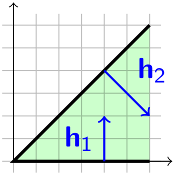
The vector space $\mathbf{V} = \mathbf{C} - \mathbf{C}$ is called the vector space generated by the conic set $\mathbf{C}$.

Duality

Theorem (Duality)

Let $\mathbf{V}$ *be a vector space. A conic set* $\mathbf{C} \subseteq \mathbf{V}$ *is* *finitely generated* *if and only if there exists a finite set* $\mathbf{H} \subseteq \mathbf{V} \backslash \{\mathbf{0}\}$ *such that:*

$$\mathbf{C} = \bigcap_{\mathbf{h} \in \mathbf{H}} \left\{ \mathbf{c} \in \mathbf{V} \mid \sum_{i=1}^{d} \mathbf{h}(i)\mathbf{c}(i) \geq 0 \right\}$$

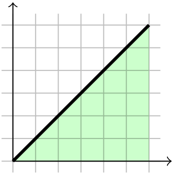


$$\mathbf{V} = \mathbb{Q}^2$$

$$\mathbf{C} = \mathbb{Q}_{\geq 0}(1,1) + \mathbb{Q}_{\geq 0}(1,0)$$

$$\mathbf{H} = \{\mathbf{h}_1, \mathbf{h}_2\}$$

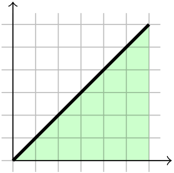
A conic set that is <u>not</u> finitely generated:



$$\{(0,0)\} \cup \{(c_1, c_2) \in \mathbb{Q}^2_{\geq 0} \mid 0 < c_2 \leq c_1\}$$

Definition

A conic set **C** is said to be definable if there exists a formula in $\text{FO}(\mathbb{Q}, +, \leq, 0)$ denoting **C**.



$$\phi(x_1, x_2) \quad = \quad (x_1 = 0 \ \wedge \ x_2 = 0) \ \vee \ ((\neg \ x_2 \leq 0) \ \wedge \ x_2 \leq x_1)$$

Lemma

Every finitely generated conic set is definable.

Proof.

The conic set $\mathbf{C} = \mathbb{Q}_{\geq 0}\mathbf{c}_1 + \cdots + \mathbb{Q}_{\geq 0}\mathbf{c}_k$ is denoted by the formula $\phi(x_1, \ldots, x_d)$ equals to:

$$\exists \lambda_1 \ldots \exists \lambda_k \left(\bigwedge_{j=1}^{k} 0 \leq \lambda_j \right) \wedge \left(\bigwedge_{i=1}^{d} x_i = \sum_{j=1}^{k} \lambda_j \mathbf{c}_j(i) \right)$$

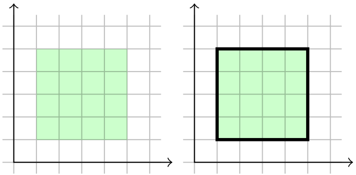
□

Definition

The topological closure of $\mathbf{X} \subseteq \mathbb{Q}^d$ is the set $\overline{\mathbf{X}}$ of vectors $\mathbf{y} \in \mathbb{Q}^d$ such that for all $\varepsilon \in \mathbb{Q}_{>0}$ the following intersection is non empty:

$$\mathbf{X} \cap (\mathbf{y} + (-\varepsilon, \varepsilon)^d) \neq \emptyset$$

Let $\mathbf{X} = (1,5) \times (1,5)$. Then $\overline{\mathbf{X}} = [1,5] \times [1,5]$.



Lemma

$\overline{\mathbf{X} \cup \mathbf{Y}} = \overline{\mathbf{X}} \cup \overline{\mathbf{Y}}$

$\mathbf{X} \subseteq \overline{\mathbf{X}}$

$\overline{\mathbf{X}} + \overline{\mathbf{Y}} \subseteq \overline{\mathbf{X} + \mathbf{Y}}$

$\mathbb{Q}_{\geq 0}\overline{\mathbf{X}} \subseteq \overline{\mathbb{Q}_{\geq 0}\mathbf{X}}$

Example

$\overline{\mathbf{X} + \mathbf{Y}} \neq \overline{\mathbf{X}} + \overline{\mathbf{Y}}$ with:
$\mathbf{X} = \{\mathbf{x} \in \mathbb{Q}^2_{>0} \mid \mathbf{x}(2) = \frac{1}{\mathbf{x}(1)}\}$ and
$\mathbf{Y} = \mathbb{Q}_{\geq 0}(0, -1)$.

Example

$\overline{\mathbb{Q}_{\geq 0}\mathbf{X}} \neq \mathbb{Q}_{\geq 0}\overline{\mathbf{X}}$ with:
$\mathbf{X} = \{\mathbf{x} \in \mathbb{Q}^2_{>0} \mid \mathbf{x}(2) = \frac{1}{\mathbf{x}(1)}\}$

Corollary

The topological closure of a conic set is a conic set.

Proof.

$\mathbf{0} \in \mathbf{C} \subseteq \overline{\mathbf{C}}$
$\overline{\mathbf{C}} + \overline{\mathbf{C}} \subseteq \overline{\mathbf{C} + \mathbf{C}} \subseteq \overline{\mathbf{C}}$
$\mathbb{Q}_{\geq 0}\overline{\mathbf{C}} \subseteq \overline{\mathbb{Q}_{\geq 0}\mathbf{C}} \subseteq \overline{\mathbf{C}}$

□

Lemma

The topological closure of a set definable in $\mathrm{FO}(\mathbb{Q}, +, \leq, 0)$ *is a finite union of finitely generated conic sets.*

Example

$\mathbf{X} = \mathbf{X}_1 \cup \mathbf{X}_2 \cup \mathbf{X}_3$ with:
$\mathbf{X}_1 = \{(x, y) \in \mathbb{Q}^2 \mid 2x + 3y > 0 \wedge x - y \geq 0\}$
$\mathbf{X}_2 = \{(x, y) \in \mathbb{Q}^2 \mid x > 0 \wedge x - y > 0\}$
$\mathbf{X}_3 = \{(x, y) \in \mathbb{Q}^2 \mid x > 0 \wedge y > 0 \wedge -x - y > 0\}$

Then
$\overline{\mathbf{X}} = \overline{\mathbf{X}}_1 \cup \overline{\mathbf{X}}_2 \cup \overline{\mathbf{X}}_3$ with:
$\overline{\mathbf{X}}_1 = \{(x, y) \in \mathbb{Q}^2 \mid 2x + 3y \geq 0 \wedge x - y \geq 0\}$
$\overline{\mathbf{X}}_2 = \{(x, y) \in \mathbb{Q}^2 \mid x \geq 0 \wedge x - y \geq 0\}$
$\overline{\mathbf{X}}_3 = \emptyset$

Lemma

The topological closure of a definable conic set is a finitely generated conic set.

Lemma

Let $\mathbf{C}$ *be a definable conic set.*
Since $\mathbf{C}$ *is a conic set then* $\overline{\mathbf{C}}$ *is a conic set.*
Since $\mathbf{C}$ *is definable then* $\overline{\mathbf{C}} = \bigcup_{j=1}^{k} \mathbf{C}_j$ *with* $\mathbf{C}_j$ *a finitely generated conic set.*

Just observe that in this case:

$$\overline{\mathbf{C}} = \sum_{j=1}^{k} \mathbf{C}_j$$

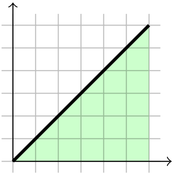
Definition

A conic set $\mathbf{C} \subseteq \mathbb{Q}^d$ is said to be locally finitely generated if for every vector space $\mathbf{V} \subseteq \mathbb{Q}^d$ the conic set $\overline{\mathbf{C} \cap \mathbf{V}}$ is finitely generated.

Theorem

A conic set is definable if and only if it is locally finitely generated.

Example:



- With $\mathbf{V} = \mathbb{Q}^2$ we have $\overline{\mathbf{C} \cap \mathbf{V}} = \mathbb{Q}_{\geq 0}(1,1) + \mathbb{Q}_{\geq 0}(1,0)$.
- With $\mathbf{V} = \mathbb{Q}\mathbf{v}$ then $\overline{\mathbf{C} \cap \mathbf{V}}$ is $\{(0,0)\}$, $\mathbb{Q}_{\geq 0}\mathbf{v}$, or $-\mathbb{Q}_{\geq 0}\mathbf{v}$.
- With $\mathbf{V} = \{(0,0)\}$ then $\overline{\mathbf{C} \cap \mathbf{V}} = \{(0,0)\}$.

Proof : The simple way

Assume that $\mathbf{C}$ is a definable conic set.
For every vector space $\mathbf{V}$ the conic set $\mathbf{C} \cap \mathbf{V}$ is definable.
From the previous lemma $\overline{\mathbf{C} \cap \mathbf{V}}$ is finitely generated.
Thus $\mathbf{C}$ is locally finitely generated.

Lemma

Let $\mathbf{C}$ *be a conic set such that* $\overline{\mathbf{C}}$ *is finitely generated and* $\mathbf{C} \cap \mathbf{V}$ *is definable for every vector space* $\mathbf{V} \subset \mathbf{C} - \mathbf{C}$*. Then* $\mathbf{C}$ *is definable.*

Proof.

Let $\mathbf{W} = \mathbf{C} - \mathbf{C}$. There exists a finite set $\mathbf{H} \subseteq \mathbf{W} \backslash \{\mathbf{0}\}$ such that:

$$\overline{\mathbf{C}} = \bigcap_{\mathbf{h} \in \mathbf{H}} \left\{ \mathbf{c} \in \mathbf{W} \mid \sum_{i=1}^{d} \mathbf{h}(i)\mathbf{c}(i) \geq 0 \right\}$$

We prove that $\mathbf{X} \subseteq \mathbf{C}$ where $\mathbf{X} = \bigcap_{\mathbf{h} \in \mathbf{H}} \left\{ \mathbf{c} \in \mathbf{W} \mid \sum_{i=1}^{d} \mathbf{h}(i)\mathbf{c}(i) > 0 \right\}$.

Observe that $\mathbf{C} = \mathbf{X} \cup \bigcup_{\mathbf{h} \in \mathbf{H}} (\mathbf{C} \cap \mathbf{V_h})$ where:

$$\mathbf{V_h} = \left\{ \mathbf{v} \in \mathbf{W} \mid \sum_{i=1}^{d} \mathbf{h}(i)\mathbf{c}(i) = 0 \right\}$$

□

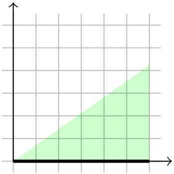
Proof : The other way

H_k : Locally finitely generated conic sets $\mathbf{C}$ such that $\text{rank}(\mathbf{C} - \mathbf{C}) \leq k$ are definable.

H_0 is clearly true since $\text{rank}(\mathbf{C} - \mathbf{C}) = 0$ implies $\mathbf{C} = \{\mathbf{0}\}$. Assume H_k true and let $\mathbf{C}$ be a locally definable conic set such that $\text{rank}(\mathbf{W}) = k + 1$ where $\mathbf{W} = \mathbf{C} - \mathbf{C}$. We observe that $\overline{\mathbf{C}}$ is finitely generated and for every vector space $\mathbf{V} \subset \mathbf{W}$ the conic set $\mathbf{C} \cap \mathbf{V}$ is locally finitely generated. Since $\text{rank}(\mathbf{V}) < \text{rank}(\mathbf{W}) \leq k + 1$ we can apply H_k. We deduce that $\mathbf{C} \cap \mathbf{V}$ definable. From the previous lemma we deduce that $\mathbf{C}$ is definable. Thus H_{k+1} is true.

An Application

A conic set that is not definable:



$$\mathbf{C} = \{(c_1, c_2) \in \mathbb{Q}_{\geq 0}^2 \mid \sqrt{2}\, c_2 \leq c_1\}$$

The conic set $\mathbf{C}$ is not finitely generated. Let $\mathbf{V} = \mathbb{Q}^2$. Since $\overline{\mathbf{C} \cap \mathbf{V}} = \mathbf{C}$ we deduce that $\mathbf{C}$ is not definable.

Subconclusion

We have introduced the class of definable conic sets and provided an algebraic criterion for membership of conic sets in this class.

Theorem (Algebraic Criterion)

A conic set $\mathbf{C} \subseteq \mathbb{Q}^d$ *is definable in* $\mathsf{FO}\,(\mathbb{Q}, +, \leq, 0)$ *if and only if the conic set* $\overline{\mathbf{C} \cap \mathbf{V}}$ *is finitely generated for every vector space* $\mathbf{V} \subseteq \mathbb{Q}^d$.

Outline

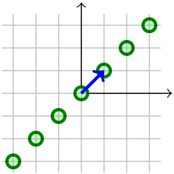
Definition

A <u>lattice</u> is a subset $\mathbf{L} \subseteq \mathbb{Z}^d$ such that $\mathbf{0} \in \mathbf{L}$, $\mathbf{L} + \mathbf{L} \subseteq \mathbf{L}$ and $-\mathbf{L} \subseteq \mathbf{L}$.

Lemma

For every lattice $\mathbf{L}$ *there exists a sequence* $\mathbf{l}_1, \ldots, \mathbf{l}_k \in \mathbf{L}$ *such that:*

$$\mathbf{L} = \mathbb{Z}\mathbf{l}_1 + \cdots + \mathbb{Z}\mathbf{l}_k$$

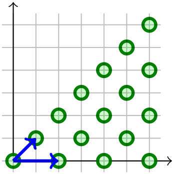


$$\mathbf{L} = \mathbb{Z}(1,1)$$

Definition

A set $\mathbf{P} \subseteq \mathbb{Z}^d$ is said to be periodic if $\mathbf{0} \in \mathbf{P}$ and $\mathbf{P} + \mathbf{P} \subseteq \mathbf{P}$. A periodic set $\mathbf{P}$ is said to be finitely generated if there exist $\mathbf{p}_1, \ldots, \mathbf{p}_k \in \mathbf{P}$ such that:

$$\mathbf{P} = \mathbb{N}\mathbf{p}_1 + \cdots + \mathbb{N}\mathbf{p}_k$$



$$\mathbf{P} = \mathbb{N}(1,1) + \mathbb{N}(2,0)$$

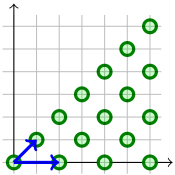
Lattices And Periodic Sets

Lemma

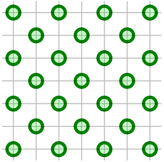
The set $\mathbf{L} = \mathbf{P} - \mathbf{P}$ *is a lattice for every periodic set* $\mathbf{P}$*. This lattice is the unique minimal one that contains* $\mathbf{P}$*.*

Definition

The lattice $\mathbf{L} = \mathbf{P} - \mathbf{P}$ is called the lattice generated by the periodic set $\mathbf{P}$.



$\mathbf{P} = \mathbb{N}(1,1) + \mathbb{N}(2,0)$



$\mathbf{L} = \mathbf{P} - \mathbf{P}$

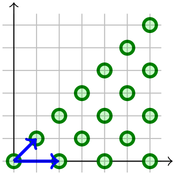
Conic Sets And Periodic Sets

Lemma

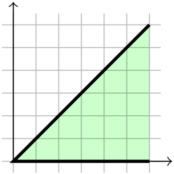
The set $\mathbf{C} = \mathbb{Q}_{\geq 0}\mathbf{P}$ *is a conic set for every periodic set* $\mathbf{P}$*. This conic set is the unique minimal one that contains* $\mathbf{P}$*.*

Definition

The conic set $\mathbf{C} = \mathbb{Q}_{\geq 0}\mathbf{P}$ is called the conic set generated by the periodic set $\mathbf{P}$.



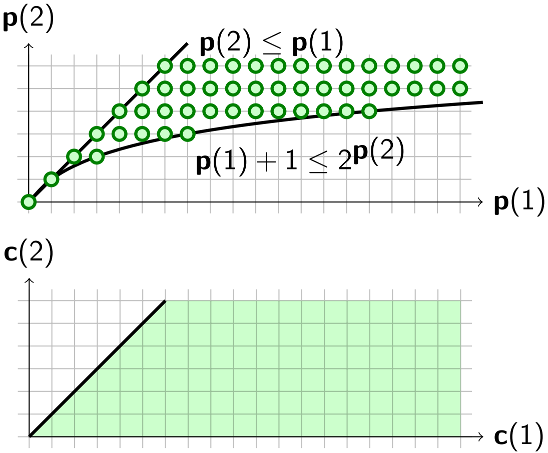
$\mathbf{P} = \mathbb{N}(1,1) + \mathbb{N}(2,0)$



$\mathbf{C} = \mathbb{Q}_{\geq 0}\mathbf{P}$

Definition

A periodic set $\mathbf{P}$ is said to be asymptotically definable if the conic set $\mathbf{C} = \mathbb{Q}_{\geq 0}\mathbf{P}$ is definable in $\mathrm{FO}\left(\mathbb{Q}, +, \leq, 0\right)$.



Lemma

The class of asymptotically definable periodic sets is stable by intersection.

Proof.

Let $\mathbf{P}_1, \mathbf{P}_2$ be two periodic sets. We have:

$$\mathbb{Q}_{\geq 0}(\mathbf{P}_1 \cap \mathbf{P}_2) \;=\; (\mathbb{Q}_{\geq 0}\mathbf{P}_1) \cap (\mathbb{Q}_{\geq 0}\mathbf{P}_2)$$

Assume that:
$\mathbb{Q}_{\geq 0}\mathbf{P}_1$ is denoted by $\phi_1(\mathbf{x})$.
$\mathbb{Q}_{\geq 0}\mathbf{P}_2$ is denoted by $\phi_2(\mathbf{x})$.
Then $\mathbb{Q}_{\geq 0}(\mathbf{P}_1 \cap \mathbf{P}_2)$ is denoted by $\phi_1(\mathbf{x}) \wedge \phi_2(\mathbf{x})$. $\square$

Lemma

The class of asymptotically definable periodic relations is stable by composition.

Proof.

Let $R_1, R_2 \subseteq \mathbb{Z}^d \times \mathbb{Z}^d$ be two periodic relations. We have:

$$\mathbb{Q}_{\geq 0}(R_1 \circ R_2) \ = \ (\mathbb{Q}_{\geq 0} R_1) \circ (\mathbb{Q}_{\geq 0} R_2)$$

Assume that:
$\mathbb{Q}_{\geq 0} R_1$ is denoted by $\phi_1(\mathbf{x}, \mathbf{y})$.
$\mathbb{Q}_{\geq 0} R_2$ is denoted by $\phi_2(\mathbf{y}, \mathbf{z})$.
Then $\mathbb{Q}_{\geq 0}(R_1 \circ R_2)$ is denoted by $\exists \mathbf{y} \ \phi_1(\mathbf{x}, \mathbf{y}) \wedge \phi_2(\mathbf{y}, \mathbf{z})$. □

Subconclusion

We introduced the class of asymptotically definable periodic sets.

From an asymptotically definable periodic set $\mathbf{P}$, we can extract two properties:

- the "repeated motif", i.e. the lattice $\mathbf{L} = \mathbf{P} - \mathbf{P}$ denoted by a finite sequence of vectors in $\mathbf{L}$.
- the "asymptotic direction", i.e. the conic set $\mathbf{C} = \mathbb{Q}_{\geq 0}\mathbf{P}$ denoted by a formula in $\mathrm{FO}(\mathbb{Q}, +, \leq, 0)$.

Stability properties:

- asymptotically definable periodic sets are stable by intersection.
- asymptotically definable periodic relations are stable by composition.

Outline

Presburger Sets

Definition

A set $\mathbf{X} \subseteq \mathbb{Z}^d$ is said to be Presburger if it can be denoted by a formula in $\mathrm{FO}(\mathbb{Z}, +, \leq, 0, 1)$.

Theorem (Ginsburg and Spanier - 1966)

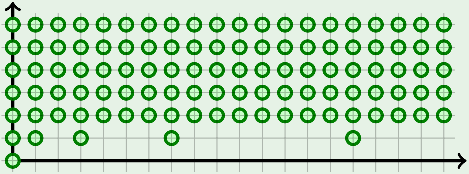
A set $\mathbf{X} \subseteq \mathbb{Z}^d$ is Presburger if and only if it is semilinear, i.e. a finite union of sets $\mathbf{b} + \mathbf{P}$ where $\mathbf{b} \in \mathbb{Z}^d$ and $\mathbf{P} \subseteq \mathbb{Z}^d$ is a finitely generated periodic set.

Almost Semilinear Sets

Definition

A set $\mathbf{X} \subseteq \mathbb{Z}^d$ is said to be almost semilinear if for every Presburger set $\mathbf{S} \subseteq \mathbb{Z}^d$, the set $\mathbf{X} \cap \mathbf{S}$ is a finite union of sets $\mathbf{b} + \mathbf{P}$ where $\mathbf{b} \in \mathbb{Z}^d$ and $\mathbf{P} \subseteq \mathbb{Z}^d$ is an asymptotically definable periodic set.

Example



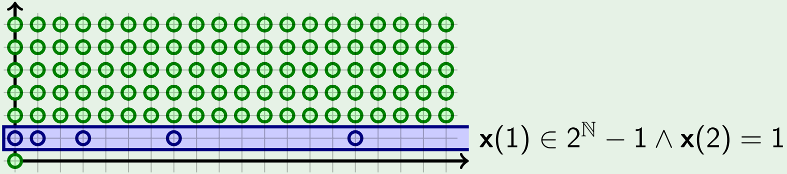
$\mathbf{x}(1) \in 2^{\mathbb{N}} - 1 \wedge \mathbf{x}(2) = 1$

Almost Semilinear Sets

Definition

A set $\mathbf{X} \subseteq \mathbb{Z}^d$ is said to be almost semilinear if for every Presburger set $\mathbf{S} \subseteq \mathbb{Z}^d$, the set $\mathbf{X} \cap \mathbf{S}$ is a finite union of sets $\mathbf{b} + \mathbf{P}$ where $\mathbf{b} \in \mathbb{Z}^d$ and $\mathbf{P} \subseteq \mathbb{Z}^d$ is an asymptotically definable periodic set.

Example



Subconclusion

We introduced the class of almost semilinear sets.

In the sequel we show that this class:

- Contains VAS reachability relations.
- Is sufficient to deduce inductive invariants in the Presburger arithmetic.

Outline

Let $\mathbf{P} \subseteq \mathbb{Z}^d$ be an asymptotically definable periodic set.

Definition

The linearization of $\mathbf{P}$ is:

$$\text{lin}(\mathbf{P}) = (\mathbf{P} - \mathbf{P}) \cap \overline{\mathbb{Q}_{\geq 0}\mathbf{P}}$$

Lemma

$\text{lin}(\mathbf{P})$ *is a finitely generated periodic set.*

Proof.

$\mathbf{L} = \mathbf{P} - \mathbf{P}$ is a lattice.

$\overline{\mathbb{Q}_{\geq 0}\mathbf{P}}$ is a finitely generated conic set. □

Preciseness

The linearization $\text{lin}(\mathbf{P})$ provides an over-approximation of $\mathbf{P}$.
Let $\mathbf{P}_1, \mathbf{P}_2 \subseteq \mathbb{Z}^d$ be two asymptotically definable periodic sets and $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{Z}^d$ be two vectors such that:

$$(\mathbf{b}_1 + \mathbf{P}_1) \ \cap \ (\mathbf{b}_2 + \mathbf{P}_2) = \emptyset$$

In general:

$$(\mathbf{b}_1 + \text{lin}(\mathbf{P}_1)) \ \cap \ (\mathbf{b}_2 + \text{lin}(\mathbf{P}_2)) \neq \emptyset$$

Dimension

Definition

The dimension $\dim(\mathbf{X})$ of a non-empty set $\mathbf{X} \subseteq \mathbb{Z}^d$ is the minimal integer $r \in \{0, \ldots, d\}$ such that:

$$\mathbf{X} \subseteq \bigcup_{j=1}^{k} \mathbf{b}_j + \mathbf{V}_j$$

where $\mathbf{b}_j \in \mathbb{Z}^d$ and $\mathbf{V}_j$ is a vector space satisfying $\text{rank}(\mathbf{V}_j) \leq r$.

$\dim(\emptyset) = -1$ by convention.

Example

$\dim(\mathbb{N}) = 1$
$\dim(\{(0,1),(1,0)\}) = 0$
$\dim(\{(x,y) \in \mathbb{N}^2 \mid x \leq y\}) = 2$

Theorem

Let $\mathbf{P}_1, \mathbf{P}_2 \subseteq \mathbb{Z}^d$ *be two asymptotically definable periodic sets and* $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{Z}^d$ *such that:*

$$(\mathbf{b}_1 + \mathbf{P}_1) \ \cap \ (\mathbf{b}_2 + \mathbf{P}_2) = \emptyset$$

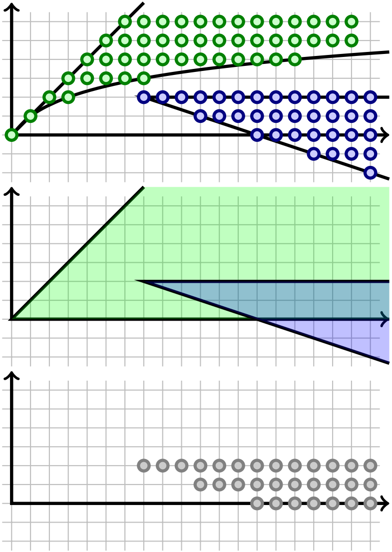
In this case, the set

$$\mathbf{X} = (\mathbf{b}_1 + \mathrm{lin}(\mathbf{P}_1)) \ \cap \ (\mathbf{b}_2 + \mathrm{lin}(\mathbf{P}_2))$$

satisfies:

$$\dim(\mathbf{X}) < \max\{\dim(\mathbf{b}_1 + \mathbf{P}_1), \dim(\mathbf{b}_2 + \mathbf{P}_2)\}$$

Example



Subconclusion

We introduced a way to over-approximate asymptotically definable periodic sets into finitely generated ones. The approximation is proved precise in some sense.

Outline

Context

Let $R \subseteq \mathbb{Z}^d \times \mathbb{Z}^d$ be a relation definable in $\mathrm{FO}(\mathbb{Z}, +, \leq, 0, 1)$.
Decide the membership in the reflexive and transitive closure R^*.

Example

Let $\mathbf{A}$ be a VAS.
We introduce:

$$R = \{(\mathbf{m}, \mathbf{n}) \in \mathbb{N}^d \times \mathbb{N}^d \mid \mathbf{n} - \mathbf{m} \in \mathbf{A}\}$$

Then R^* is the reachability relation.

In general undecidable since the one step reachability relation R of a Minsky machine is definable in $\mathrm{FO}(\mathbb{Z}, +, \leq, 0, 1)$.

Inductive Invariants

Let $R \subseteq \mathbb{Z}^d \times \mathbb{Z}^d$.

Definition

The forward image $\text{post}_R(\mathbf{X})$ of a set $\mathbf{X} \subseteq \mathbb{Z}^d$ by R is defined by:

$$\text{post}_R(\mathbf{X}) = \bigcup_{\mathbf{x} \in \mathbf{X}} \{\mathbf{y} \in \mathbb{Z}^d \mid (\mathbf{x}, \mathbf{y}) \in R\}$$

If $\text{post}_R(\mathbf{X}) \subseteq \mathbf{X}$ then $\mathbf{X}$ is called a forward inductive invariant for R.

Definition

The backward image $\text{pre}_R(\mathbf{Y})$ of a set $\mathbf{Y} \subseteq \mathbb{Z}^d$ by R is defined by:

$$\text{pre}_R(\mathbf{Y}) = \bigcup_{\mathbf{y} \in \mathbf{Y}} \{\mathbf{x} \in \mathbb{Z}^d \mid (\mathbf{x}, \mathbf{y}) \in R\}$$

If $\text{pre}_R(\mathbf{Y}) \subseteq \mathbf{Y}$ then $\mathbf{Y}$ is called a backward inductive invariant for R.

Definition (Separators)

A separator for a binary relation $R \subseteq \mathbb{Z}^d \times \mathbb{Z}^d$ is a pair $(\mathbf{X}, \mathbf{Y})$ of subsets of $\mathbb{Z}^d$ such that $\text{post}_{R^*}(\mathbf{X}) \cap \text{pre}_{R^*}(\mathbf{Y}) = \emptyset$. The set $\mathbf{D} = \mathbb{Z}^d \backslash (\mathbf{X} \cup \mathbf{Y})$ is called the domain. A separator is said to be closed if its domain is empty.

If $(\mathbf{X}, \mathbf{Y})$ is a closed separator for R then $\mathbf{X}$ is a forward invariant and $\mathbf{Y}$ is a backward invariant.

Example

Separators $(\mathbf{X}, \mathbf{Y})$ are included in closed separators, for instance:

$$(\text{post}_{R^*}(\mathbf{X}) \ , \ \mathbb{Z}^d \backslash \text{post}_{R^*}(\mathbf{X}))$$

$$(\mathbb{Z}^d \backslash \text{pre}_{R^*}(\mathbf{Y}) \ , \ \text{pre}_{R^*}(\mathbf{Y}))$$

Main result of this section:

Theorem

Let $R \subseteq \mathbb{Z}^d \times \mathbb{Z}^d$ be a binary relation such that its reflexive and transitive closure R^* is an almost semilinear relation. Presburger separators are included in closed Presburger separators.

Corollary

Let $R \subseteq \mathbb{Z}^d \times \mathbb{Z}^d$ be a binary relation such that its reflexive and transitive closure R^* is an almost semilinear relation. For every $(\mathbf{x}, \mathbf{y}) \notin R^*$ there exists a Presburger forward invariant $\mathbf{I}$ such that $\mathbf{x} \in \mathbf{I}$ and $\mathbf{y} \notin \mathbf{I}$.

Proof.

Observe that $(\{\mathbf{x}\}, \{\mathbf{y}\})$ is a Presburger separator.
There exists a closed Presburger separator $(\mathbf{I}, \mathbf{J})$ such that:
$\{\mathbf{x}\} \subseteq \mathbf{I}$ and $\{\mathbf{y}\} \subseteq \mathbf{J}$.
Since $\mathbf{I} \cap \mathbf{J} = \emptyset$ we get $\mathbf{y} \notin \mathbf{I}$. □

Assume that R^* is almost semilinear.

Lemma

$\text{post}_{R^*}(\mathbf{X})$ *and* $\text{pre}_{R^*}(\mathbf{Y})$ *are almost semilinear sets for every Presburger sets* $\mathbf{X}, \mathbf{Y} \subseteq \mathbb{Z}^d$.

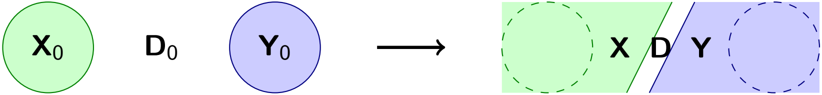
Proof.

Let $\mathbf{S} \subseteq \mathbb{Z}^d$ be a Presburger set. We have:

$$\text{post}_{R^*}(\mathbf{X}) \cap \mathbf{S} = \{\mathbf{y} \in \mathbb{Z}^d \mid \exists(\mathbf{x}, \mathbf{y}) \in R^* \cap (\mathbf{X} \times \mathbf{S})\}$$

□

Induction

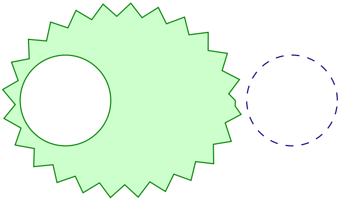


$(\mathbf{X}_0, \mathbf{Y}_0)$ Presburger Separator $\longrightarrow$ $(\mathbf{X}, \mathbf{Y})$ Presburger Separator

with $\dim(\mathbf{D}_0) > \dim(\mathbf{D})$

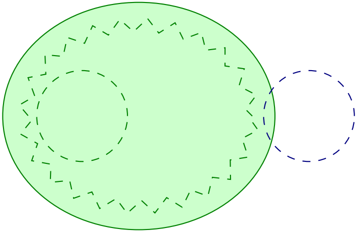
$(\mathbf{X}_0, \mathbf{Y}_0)$ Presburger Separator

$\text{post}_{R^*}(\mathbf{X}_0) \setminus \mathbf{X}_0$



This is a finite union $\bigcup_i (\mathbf{b}_i + \mathbf{P}_i)$.

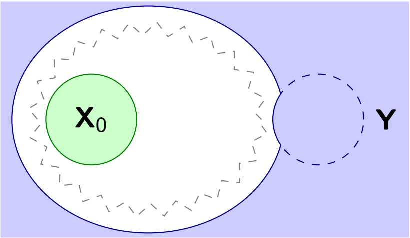
$\mathbf{S} := \mathbf{X}_0 \cup (\bigcup_i (\mathbf{b}_i + \mathrm{lin}(\mathbf{P}_i)))$



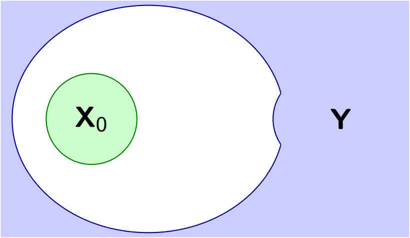
$\mathbf{S}$ is an over-approximation of $\mathrm{post}_{R^*}(\mathbf{X}_0)$.

$\mathbf{S} \cap \mathbf{Y}_0$ is not necessary empty.

$$\mathbf{Y} := \mathbf{Y}_0 \cup (\mathbb{N}^d \backslash \mathbf{S})$$

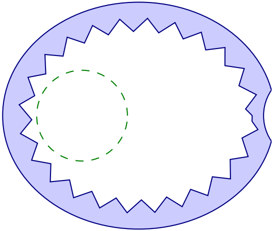


$(\mathbf{X}_0, \mathbf{Y})$ is a Presburger separator such that $\mathbf{Y}_0 \subseteq \mathbf{Y}$



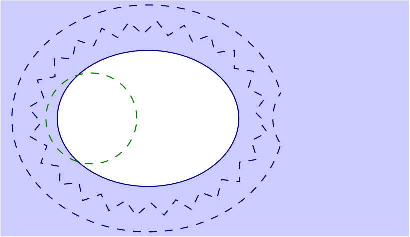
$(\mathbf{X}_0, \mathbf{Y})$ Presburger Separator

$\text{pre}_{R^*}(\mathbf{Y}) \setminus \mathbf{Y}$



This is a finite union $\bigcup_j (\mathbf{c}_j + \mathbf{Q}_j)$.

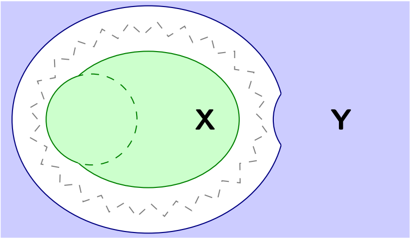
$$\mathbf{T} := \mathbf{Y} \cup (\bigcup_j (\mathbf{c}_j + \mathrm{lin}(\mathbf{Q}_j)))$$



$\mathbf{T}$ is an over-approximation of $\mathrm{pre}_{R^*}(\mathbf{Y})$.

$\mathbf{T} \cap \mathbf{X}_0$ is not necessary empty.

$\mathbf{X} := \mathbf{X}_0 \cup (\mathbb{N}^d \backslash \mathbf{T})$



$(\mathbf{X}, \mathbf{Y})$ is a Presburger separator such that $\mathbf{X}_0 \subseteq \mathbf{X}$

Induction

The domain $\mathbf{D}$ of $(\mathbf{X}, \mathbf{Y})$ satisfies $\mathbf{D} = \mathbf{D}_0 \cap (\bigcup_{i,j} \mathbf{D}_{i,j})$ where:

$$\mathbf{D}_{i,j} = (\mathbf{b}_i + \text{lin}(\mathbf{P}_i)) \cap (\mathbf{c}_j + \text{lin}(\mathbf{Q}_j))$$

As $(\mathbf{b}_i + \mathbf{P}_i) \cap (\mathbf{c}_j + \mathbf{Q}_j) = \emptyset$ we get:

$$\dim(\mathbf{D}_{i,j}) < \max\{\dim(\mathbf{b}_i + \mathbf{P}_i), \dim(\mathbf{c}_j + \mathbf{Q}_j)\}$$

As $\mathbf{b}_i + \mathbf{P}_i$ and $\mathbf{c}_j + \mathbf{Q}_j$ are both included in $\mathbf{D}_0$, we get:

$$\dim(\mathbf{b}_i + \mathbf{P}_i) \leq \dim(\mathbf{D}_0) \qquad \dim(\mathbf{c}_j + \mathbf{Q}_j) \leq \dim(\mathbf{D}_0)$$

Thus:

$$\dim(\mathbf{D}) < \dim(\mathbf{D}_0)$$

Subconclusion

Assume that R is denoted by a Presburger formula and R^* is almost semilinear. The non-membership in R^* can be proved with formulas in the Presburger arithmetic denoting forward inductive invariants for R.

Outline

Well Orders

Definition

An order $\sqsubseteq$ over a set S is said to be well if for every sequence $(s_n)_{n \in \mathbb{N}}$ of elements $s_n \in S$ there exists an increasing sequence $(n_k)_{k \in \mathbb{N}}$ of indexes $n_k \in \mathbb{N}$ such that $(s_{n_k})_{k \in \mathbb{N}}$ is non decreasing for $\sqsubseteq$.

Example

The ordered set $(\mathbb{N}, \leq)$ is well but $(\mathbb{Z}, \leq)$ is not well.

Example (Pigeon Hole Principle)

An ordered set $(S, =)$ is well if and only if S is finite.

Dickson's Lemma

Definition

Let $(S, \sqsubseteq)$ be an ordered set.
We introduce the ordered set $(S^d, \sqsubseteq^d)$ where $\sqsubseteq^d$ is defined component-wise by

$$(s_1, \ldots, s_d) \sqsubseteq^d (t_1, \ldots, t_d) \text{ if } s_i \sqsubseteq t_i \quad \forall i$$

Lemma (Dickson's Lemma)

The order set $(S^d, \sqsubseteq^d)$ is well for every well ordered set $(S, \sqsubseteq)$.

Example

$(\mathbb{N}^d, \leq)$ is well.

Higmann's Lemma

Definition

Let $(S, \sqsubseteq)$ be an ordered set.
We introduce the ordered set $(S^*, \sqsubseteq^*)$ where $\sqsubseteq^*$ is defined by $u \sqsubseteq^* v$ if u and v can be decomposed as follows:

$$\begin{array}{ccccccccc} u & = & & s_1 & & \dots & s_d & \\ & & & \sqcap\!\! | & & & \sqcap\!\! | & \\ v & = & w_0 & t_1 & w_1 & \dots & t_d & w_d \end{array}$$

where $s_j, t_j \in S$.

Lemma (Higmann's Lemma)

The ordered set $(S^*, \sqsubseteq^*)$ is well for every well ordered set $(S, \sqsubseteq)$.

Outline

Vector Addition System Additional Notations

Definition

Let $\rho = \mathbf{m}_0 \ldots \mathbf{m}_k$ be a run of a VAS $\mathbf{A}$. We introduce the action $\mathbf{a}_j = \mathbf{m}_j - \mathbf{m}_{j-1}$ for each $j \in \{1, \ldots, k\}$.

$\mathrm{src}(\rho) = \mathbf{m}_0$ the <u>source</u>.
$\mathrm{tgt}(\rho) = \mathbf{m}_k$ the <u>target</u>.
$\mathrm{lab}(\rho) = \mathbf{a}_1 \ldots \mathbf{a}_k$ the <u>label</u>.

Let $w \in \mathbf{A}^*$ be a word of actions.

Definition

The binary relation $\xrightarrow{w}$ over $\mathbb{N}^d$ is defined by $\mathbf{m} \xrightarrow{w} \mathbf{n}$ if there exists a run ρ such that $\mathrm{src}(\rho) = \mathbf{m}$, $\mathrm{lab}(\rho) = w$ and $\mathrm{tgt}(\rho) = \mathbf{n}$.

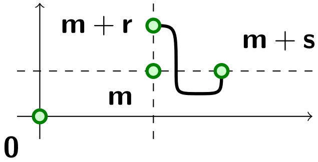
Definition

We denote by $\xrightarrow{*}$ the reachability relation.

Definition (Inspired from Hauschildt 1990)

The production relation of a marking $\mathbf{m}$ is the binary relation $\xrightarrow{*}_{\mathbf{m}}$ defined over the markings by:

$$\mathbf{r} \xrightarrow{*}_{\mathbf{m}} \mathbf{s} \quad \text{if} \quad \mathbf{m} + \mathbf{r} \xrightarrow{*} \mathbf{m} + \mathbf{s}$$



Example

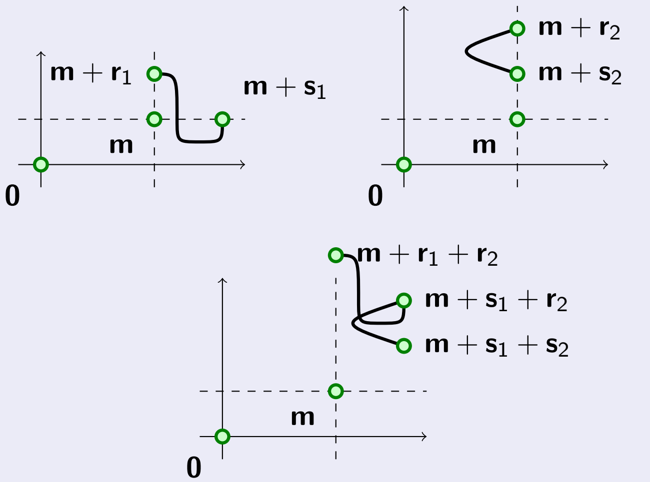
$\xrightarrow{*}_{\mathbf{m}}$ is equal to $\xrightarrow{*}$ when $\mathbf{m} = \mathbf{0}$.

Lemma

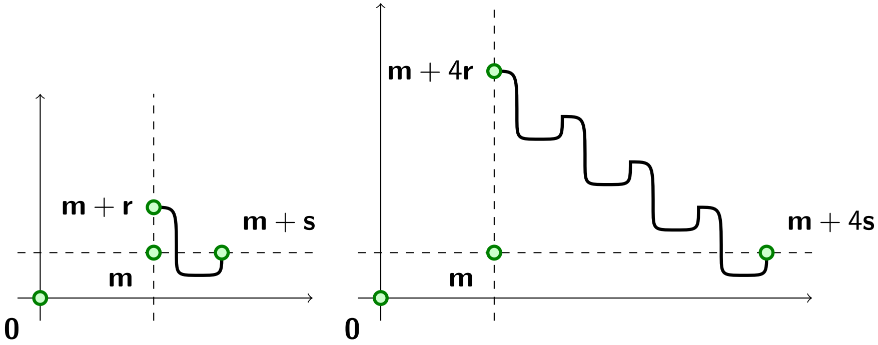
Production relations are periodic.

Proof.

$$\mathbf{r}_1 \xrightarrow{*}_{\mathbf{m}} \mathbf{s}_1 \quad \text{and} \quad \mathbf{r}_2 \xrightarrow{*}_{\mathbf{m}} \mathbf{s}_2 \quad \text{implies} \quad \mathbf{r}_1 + \mathbf{r}_2 \xrightarrow{*}_{\mathbf{m}} \mathbf{s}_1 + \mathbf{s}_2$$



Application : Iterate



Main result of this section:

Theorem

Production relations are asymptotically definable.

I.e. the following relation is definable in FO $(\mathbb{Q}, +, \leq, 0)$:

$$\mathbb{Q}_{\geq 0} \xrightarrow{*}_{\mathbf{m}} \quad = \quad \{(\lambda \mathbf{r}, \lambda \mathbf{s}) \mid \lambda \in \mathbb{Q}_{\geq 0} \text{ and } \mathbf{r} \xrightarrow{*}_{\mathbf{m}} \mathbf{s}\}$$

Relaxing Components

We introduce an element $\infty \notin \mathbb{N}$ and we let $\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$.

Definition

A vector $\mathbf{x} \in \mathbb{N}_\infty^d$ is called an extended marking. The set $I = \{i \in \{1, \ldots, d\} \mid \mathbf{x}(i) = \infty\}$ is called the set of relaxed components.

Let $\mathbf{m} \in \mathbb{N}^d$ and $I \subseteq \{1, \ldots, d\}$. The extended marking $\mathbf{m}^I$ obtained from $\mathbf{m}$ by relaxing components in I is defined by:

$$\mathbf{m}^I(i) = \begin{cases} \infty & \text{if } i \in I \\ \mathbf{m}(i) & \text{if } i \notin I \end{cases}$$

Example

Let $\mathbf{m} = (1, 2, 1000)$ and $I = \{3\}$ then $\mathbf{m}^I = (1, 2, \infty)$.

Definition

We introduce the binary relations $\xrightarrow{\mathbf{a}}$ over the set of extended markings relaxed over the same set of components I by $\mathbf{x} \xrightarrow{\mathbf{a}} \mathbf{y}$ if:

$$\forall i \notin I \quad \mathbf{y}(i) = \mathbf{x}(i) + \mathbf{a}(i)$$

An extended run is a non-empty word $\rho = \mathbf{x}_0 \ldots \mathbf{x}_k$ of extended markings relaxed over the same set I such that for every $j \in \{1, \ldots, d\}$ there exists $\mathbf{a}_j \in \mathbf{A}$ such that $\mathbf{x}_{j-1} \xrightarrow{\mathbf{a}_j} \mathbf{x}_j$.

Let $\rho = \mathbf{m}_0 \ldots \mathbf{m}_k$ and $I \subseteq \{1, \ldots, d\}$. The extended run ρ^I obtained from ρ by relaxing components in I is defined by $\rho^I = \mathbf{m}_0^I \ldots \mathbf{m}_k^I$.

Example

Let $\rho = (0,0,100)(0,1,99)\ldots(0,100,0)$ be a run.
Let $I = \{2,3\}$.
Then $\rho^I = (0,\infty,\infty)\ldots(0,\infty,\infty)$.

Recall that $\xrightarrow{*}_{\mathbf{m}}$ is asymptotically definable if and only for every vector space $V \subseteq \mathbb{Q}^d \times \mathbb{Q}^d$ the following conic set is finitely generated:

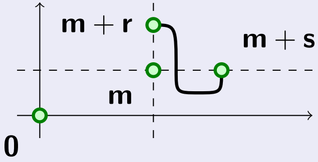
$$\overline{\mathbb{Q}_{\geq 0} \xrightarrow{*}_{\mathbf{m},V}}$$

where:

$$\xrightarrow{*}_{\mathbf{m},V} \;=\; \{(\mathbf{r},\mathbf{s}) \in V \mid \mathbf{r} \xrightarrow{*}_{\mathbf{m}} \mathbf{s}\}$$

Definition

Let $\Omega_{\mathbf{m},V}$ be the set of runs of the following form with $(\mathbf{r},\mathbf{s}) \in V$:



$$\Omega_{\mathbf{m},V} = \bigcup_{(\mathbf{r},\mathbf{s}) \in \xrightarrow{*}_{\mathbf{m},V}} \{\text{runs } \rho \mid \text{src}(\rho) = \mathbf{m}+\mathbf{r} \ \wedge \ \text{tgt}(\rho) = \mathbf{m}+\mathbf{s}\ \}$$

Reachability Graphs

Definition

We introduce:

$$\mathbf{Q}_{\mathbf{m},V} = \bigcup_{\rho \in \Omega_{\mathbf{m},V}} \{\mathbf{q} \in \mathbb{N}^d \mid \mathbf{q} \text{ occurs in } \rho\}$$

$$\mathbf{Q}_{\mathbf{m},V}(i) = \{\mathbf{q}(i) \mid \mathbf{q} \in \mathbf{Q}_{\mathbf{m},V}\}$$

$$I_{\mathbf{m},V} = \{i \in \{1, \ldots, d\} \mid \mathbf{Q}_{\mathbf{m},V}(i) \text{ is infinite}\}$$

We introduce the finite graph $G_{\mathbf{m},V} = (\mathbf{X}, \Delta)$ defined by:

- $\mathbf{X} = \{\mathbf{q}^{I_{\mathbf{m},V}} \mid \mathbf{q} \in \mathbf{Q}_{\mathbf{m},V}\}$.
- Δ is the set of triples $(\mathbf{x}, \mathbf{a}, \mathbf{y}) \in \mathbf{X} \times \mathbf{A} \times \mathbf{X}$ such that $\mathbf{x} \xrightarrow{a} \mathbf{y}$.

An Approximation

We introduce an approximation of $\xrightarrow{*}_{\mathbf{m},V}$

Definition

We introduce the relation $R_{\mathbf{m},V}$ of couples $(\mathbf{r},\mathbf{s}) \in (\mathbb{N}^d \times \mathbb{N}^d) \cap V$ such that (1) $\mathbf{r}(i) = 0$ and $\mathbf{s}(i) = 0$ for every $i \notin I_{\mathbf{m},V}$, and (2) there exist a cycle in $G_{\mathbf{m},V}$ on the state $\mathbf{m}^{I_{\mathbf{m},V}}$ labeled by a word $\mathbf{a}_1 \ldots \mathbf{a}_k$ such that:

$$\mathbf{r} + \sum_{j=1}^{k} \mathbf{a}_j = \mathbf{s}$$

Lemma

We have:

$$\xrightarrow{*}_{\mathbf{m},V} \quad \subseteq \quad R_{\mathbf{m},V}$$

Proof.

Let $(\mathbf{r},\mathbf{s})$ in $\xrightarrow{*}_{\mathbf{m},V}$. There exists a run $\rho = \mathbf{m}_0 \ldots \mathbf{m}_k$ in $\Omega_{\mathbf{m},V}$ such that $\mathbf{m}_0 = \mathbf{m} + \mathbf{r}$ and $\mathbf{m}_k = \mathbf{m} + \mathbf{s}$.

Since $\mathbf{m} + \mathbb{N}\mathbf{r}$ and $\mathbf{m} + \mathbb{N}\mathbf{s}$ are included in $\mathbf{Q}_{\mathbf{m},V}$ we deduce that $\mathbf{r}(i) > 0$ or $\mathbf{s}(i) > 0$ implies $i \in I_{\mathbf{m},V}$. Hence:

$$\mathbf{m}_0^{I_{\mathbf{m},V}} = \mathbf{m}^{I_{\mathbf{m},V}} \qquad \mathbf{m}_k^{I_{\mathbf{m},V}} = \mathbf{m}^{I_{\mathbf{m},V}}$$

We deduce that $(\mathbf{r},\mathbf{s}) \in R_{\mathbf{m},V}$ from the following cycle where $\mathbf{a}_j = \mathbf{m}_j - \mathbf{m}_{j-1}$:

$$\mathbf{m}_0^{I_{\mathbf{m},V}} \xrightarrow{\mathbf{a}_1} \cdots \xrightarrow{\mathbf{a}_k} \mathbf{m}_k^{I_{\mathbf{m},V}}$$

□

In general the other inclusion is wrong but let us try proving it:

$$R_{\mathbf{m},V} \quad \subseteq \quad \xrightarrow{*}_{\mathbf{m}}$$

Let $(\mathbf{r},\mathbf{s}) \in R_{\mathbf{m},V}$. Then $(\mathbf{r},\mathbf{s}) \in (\mathbb{N}^d \times \mathbb{N}^d) \cap V$ and there exist a cycle in $G_{\mathbf{m},V}$ on the state $\mathbf{m}^{I_{\mathbf{m},V}}$ labeled by a word $\mathbf{a}_1 \dots \mathbf{a}_k$ such that:

$$\mathbf{r} + \sum_{j=1}^{k} \mathbf{a}_j = \mathbf{s}$$

We deduce that:

$$(\mathbf{m}+\mathbf{r})^{I_{\mathbf{m},V}} \xrightarrow{\mathbf{a}_1 \dots \mathbf{a}_k} (\mathbf{m}+\mathbf{s})^{I_{\mathbf{m},V}}$$

However in general we do not have

$$\mathbf{m}+\mathbf{r} \xrightarrow{\mathbf{a}_1 \dots \mathbf{a}_k} \mathbf{m}+\mathbf{s}$$

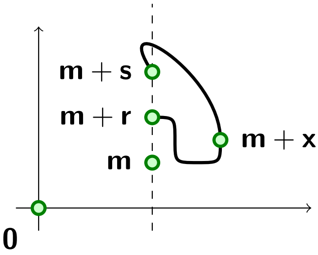
since components in $I_{\mathbf{m},V}$ relaxed in the first case are integers in the second case.

Definition

An intraproduction for $(\mathbf{m}, V)$ is a tuple $(\mathbf{r}, \mathbf{x}, \mathbf{s})$ such that:

$$\mathbf{r} \xrightarrow{*}_{\mathbf{m}} \mathbf{x} \xrightarrow{*}_{\mathbf{m}} \mathbf{s}$$

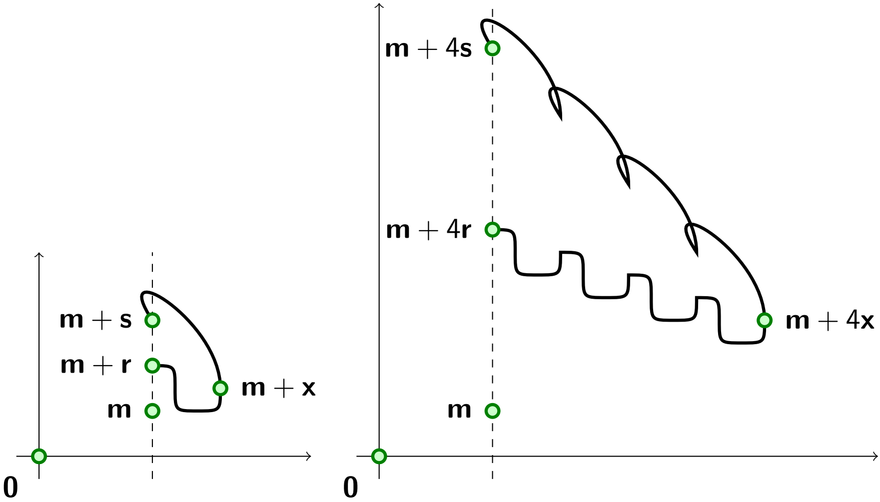
and such that $(\mathbf{r}, \mathbf{s}) \in V$.



with $V = \{(\mathbf{u}, \mathbf{v}) \mid \mathbf{u}(1) = \mathbf{v}(1) = 0\}$.

Application

$\mathbf{m} + \mathbb{N}\mathbf{x} \subseteq \mathbf{Q}_{\mathbf{m},V}$ for every intraproduction $(\mathbf{r}, \mathbf{x}, \mathbf{s})$ for $(\mathbf{m}, V)$.



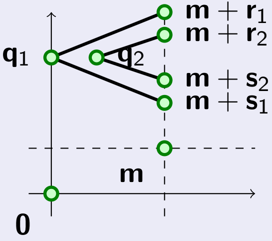
Lemma

For every $i \in I_{\mathbf{m},V}$ there exists an intraproduction $(\mathbf{r}, \mathbf{x}, \mathbf{s})$ for $(\mathbf{m}, V)$ such that $\mathbf{x}(i) > 0$.

Proof.

There exist $\mathbf{q}_1 \leq \mathbf{q}_2$ in $\mathbf{Q}_{\mathbf{m},V}$ such that $\mathbf{q}_1(i) < \mathbf{q}_2(i)$.
Let $(\mathbf{r}_1, \mathbf{s}_1)$ and $(\mathbf{r}_2, \mathbf{s}_2)$ in V such that:

$$\mathbf{m} + \mathbf{r}_1 \xrightarrow{u_1} \mathbf{q}_1 \xrightarrow{v_1} \mathbf{m} + \mathbf{s}_1 \qquad \mathbf{m} + \mathbf{r}_2 \xrightarrow{u_2} \mathbf{q}_2 \xrightarrow{v_2} \mathbf{m} + \mathbf{s}_2$$



$$\mathbf{m} + (\mathbf{r}_1 + \mathbf{r}_2) \xrightarrow{u_2 v_1} \mathbf{m} + (\mathbf{r}_1 + \mathbf{s}_1 + \mathbf{q}_2 - \mathbf{q}_1) \xrightarrow{u_1 v_2} \mathbf{m} + (\mathbf{s}_1 + \mathbf{s}_2)$$

Lemma (Simultaneously Large Components)

For every $n \in \mathbb{N}$ *there exists* $\mathbf{q}_n \in \mathbf{Q}_{\mathbf{m},V}$ *such that for every* $i \in \{1, \ldots, d\}$*:*

$$\begin{cases} \mathbf{q}_n(i) = \mathbf{m}(i) & \text{if } i \not\in I_{\mathbf{m},V} \\ \mathbf{q}_n(i) \geq \mathbf{m}(i) + n & \text{if } i \in I_{\mathbf{m},V} \end{cases}$$

Proof.

For each $i \in I_{\mathbf{m},V}$ there exists an intraproduction $(\mathbf{r}_i, \mathbf{x}_i, \mathbf{s}_i)$ such that $\mathbf{x}_i(i) > 0$. Since $\xrightarrow{*}_{\mathbf{m},V}$ is periodic we deduce that the set of intraproductions is periodic. Hence the following tuple is an intraproduction:

$$(\mathbf{r}, \mathbf{x}, \mathbf{s}) = \sum_{i \in I_{\mathbf{m},V}} (\mathbf{r}_i, \mathbf{x}_i, \mathbf{s}_i)$$

Observe that $\mathbf{x}(i) > 0$ for every $i \in I_{\mathbf{m},V}$. Moreover since $\mathbf{m} + \mathbb{N}\mathbf{x} \subseteq \mathbf{Q}_{\mathbf{m},V}$ we deduce that $\mathbf{x}(i) > 0$ implies that $i \in I_{\mathbf{m},V}$.
Just consider $\mathbf{q}_n = \mathbf{m} + n\mathbf{x}$. □

Lemma

We have:

$$R_{\mathbf{m},V} \quad \subseteq \quad \overline{\mathbb{Q}_{\geq 0} \xrightarrow{*}_{\mathbf{m},V}}$$

Proof.

Let $(\mathbf{r},\mathbf{s}) \in R_{\mathbf{m},V}$. Then $(\mathbf{r},\mathbf{s}) \in (\mathbb{N}^d \times \mathbb{N}^d) \cap V$ and there exists a cycle in $G_{\mathbf{m},V}$ on the state $\mathbf{m}^{I_{\mathbf{m},V}}$ labeled by a word $w = \mathbf{a}_1 \ldots \mathbf{a}_k$ such that $\mathbf{r} + \sum_{j=1}^{k} \mathbf{a}_j = \mathbf{s}$.

We deduce that $(\mathbf{m}+\mathbf{r})^{I_{\mathbf{m},V}} \xrightarrow{w} (\mathbf{m}+\mathbf{s})^{I_{\mathbf{m},V}}$. There exists $n \in \mathbb{N}$ large enough such that $\mathbf{q}_n + \mathbf{r} \xrightarrow{w} \mathbf{q}_n + \mathbf{s}$. As $\xrightarrow{*}_{\mathbf{q}_n}$ is periodic we deduce $\mathbf{q}_n + h\mathbf{r} \xrightarrow{*} \mathbf{q}_n + h\mathbf{s}$ for every $h \in \mathbb{N}$.

As $\mathbf{q}_n \in \mathbf{Q}_{\mathbf{m},V}$ we have $\mathbf{m} + \mathbf{r}' \xrightarrow{*} \mathbf{q}_n \xrightarrow{*} \mathbf{m} + \mathbf{s}'$ for some $(\mathbf{r}',\mathbf{s}') \in (\mathbb{N}^d \times \mathbb{N}^d) \cap V$.

Therefore $\mathbf{m} + \mathbf{r}' + h\mathbf{r} \xrightarrow{*} \mathbf{m} + \mathbf{s}' + h\mathbf{s}$ and $(\mathbf{r}',\mathbf{s}') + h(\mathbf{r},\mathbf{s}) \subseteq \xrightarrow{*}_{\mathbf{m},V}$. Hence $\frac{(\mathbf{r}',\mathbf{s}')}{h} + (\mathbf{r},\mathbf{s}) \in \mathbb{Q}_{\geq 0} \xrightarrow{*}_{\mathbf{m},V}$ for every $h \in \mathbb{N}_{>0}$.

□

We have proved:

Lemma

$$\overline{\mathbb{Q}_{\geq 0} \xrightarrow{*}_{\mathbf{m},V}} = \overline{\mathbb{Q}_{\geq 0} R_{\mathbf{m},V}}$$

We deduce:

Theorem

Production relations are asymptotically definable.

Proof.

Since $R_{\mathbf{m},V}$ is Presburger as the Parikh image of a regular language, we deduce that $\overline{\mathbb{Q}_{\geq 0} R_{\mathbf{m},V}}$ is finitely generated. Hence $\overline{\mathbb{Q}_{\geq 0} \xrightarrow{*}_{\mathbf{m},V}}$ is finitely generated for every vector space $V \subseteq \mathbb{Q}^d \times \mathbb{Q}^d$. We have proved that $\mathbb{Q}_{\geq 0} \xrightarrow{*}_{\mathbf{m}}$ is definable. □

Subconclusion

We have proved that for every marking $\mathbf{m} \in \mathbb{N}^d$ the following relation is definable in FO$(\mathbb{Q}, +, \leq, 0)$:

$$\mathbb{Q}_{\geq 0} \xrightarrow{*}_{\mathbf{m}} \;=\; \{(\lambda \mathbf{r}, \lambda \mathbf{s}) \mid \lambda \in \mathbb{Q}_{\geq 0}\ \mathbf{r} \xrightarrow{*}_{\mathbf{m}} \mathbf{s}\}$$

Outline

Main result of this section:

Theorem

The reachability relation $\xrightarrow{*}$ is almost semilinear.

Let $\rho = \mathbf{m}_0 \ldots \mathbf{m}_k$ be a run.

$$\mathbf{r}_0 \xrightarrow{*}_{\mathbf{m}_0} \mathbf{r}_1 \xrightarrow{*}_{\mathbf{m}_1} \cdots \xrightarrow{*}_{\mathbf{m}_k} \mathbf{r}_{k+1}$$

Definition (Inspired from Hauschildt)

The production relation of a run $\rho = \mathbf{m}_0 \ldots \mathbf{m}_k$ is the binary relation $\xrightarrow{*}_\rho$ defined by:

$$\xrightarrow{*}_\rho \quad = \quad \xrightarrow{*}_{\mathbf{m}_0} \circ \cdots \circ \xrightarrow{*}_{\mathbf{m}_k}$$

The production relations $\xrightarrow{*}_\rho$ are periodic and asymptotically definable.

Lemma

$$(\mathrm{src}(\rho), \mathrm{tgt}(\rho)) \quad + \quad \xrightarrow{*}_{\rho} \quad \subseteq \quad \xrightarrow{*}$$

Proof.

Let

$$\mathbf{m}_0 \xrightarrow{\mathbf{a}_1} \mathbf{m}_1 \xrightarrow{a_2} \cdots \xrightarrow{a_k} \mathbf{m}_k$$

$$\mathbf{r}_0 \xrightarrow{*}_{\mathbf{m}_0} \mathbf{r}_1 \xrightarrow{*}_{\mathbf{m}_1} \cdots \xrightarrow{*}_{\mathbf{m}_k} \mathbf{r}_{k+1}$$

There exist $w_0, \ldots, w_k \in \mathbf{A}^*$ such that:

$$\mathbf{m}_0 + \mathbf{r}_0 \xrightarrow{w_0} \mathbf{m}_0 + \mathbf{r}_1 \qquad \mathbf{m}_k + \mathbf{r}_k \xrightarrow{w_k} \mathbf{m}_k + \mathbf{r}_{k+1}$$

Hence

$$\mathbf{m}_0 + \mathbf{r}_0 \xrightarrow{w_0 \ \mathbf{a}_1 \ w_1 \ \ldots \ w_k \ \mathbf{a}_k \ w_{k+1}} \mathbf{m}_k + \mathbf{r}_{k+1}$$

□

Definition

We introduce the order $\preceq$ over the set of runs by $\rho \preceq \rho'$ if:

$$(\mathsf{src}(\rho'), \mathsf{tgt}(\rho')) \quad + \quad \xrightarrow{*}_{\rho'} \quad \subseteq \quad (\mathsf{src}(\rho), \mathsf{tgt}(\rho)) \quad + \quad \xrightarrow{*}_{\rho}$$

Theorem

The order $\preceq$ is well.

Proof.

We associate to every run $\rho = \mathbf{m}_0 \ldots \mathbf{m}_k$ the following word $\alpha(\rho)$:

$$\alpha(\rho) = (\mathbf{a}_1, \mathbf{m}_1) \ldots (\mathbf{a}_k, \mathbf{m}_k) \qquad \text{where } \mathbf{a}_j = \mathbf{m}_j - \mathbf{m}_{j-1}$$

We introduce the well order $\sqsubseteq$ over $S = \mathbf{A} \times \mathbb{N}^d$ defined by $(\mathbf{a}, \mathbf{m}) \sqsubseteq (\mathbf{b}, \mathbf{n})$ if $\mathbf{a} = \mathbf{b}$ and $\mathbf{m} \leq \mathbf{n}$. Let ρ' be another run.

Assume $\alpha(\rho) \sqsubseteq^* \alpha(\rho')$:
We have $\alpha(\rho') = w_0(\mathbf{a}_1, \mathbf{m}_1 + \mathbf{r}_1)w_1 \ldots (\mathbf{a}_\mathbf{k}, \mathbf{m}_k + \mathbf{r}_k)w_k$.

Assume $\text{src}(\rho) \leq \text{src}(\rho')$: We have $\text{src}(\rho') = \mathbf{m}_0 + \mathbf{r}_0$.

Assume $\text{tgt}(\rho) \leq \text{tgt}(\rho')$: We have $\text{tgt}(\rho') = \mathbf{m}_k + \mathbf{r}_{k+1}$.

We deduce that $\mathbf{r}_0 \xrightarrow{*}_{\mathbf{m}_1} \mathbf{r}_1 \cdots \xrightarrow{*}_{\mathbf{m}_k} \mathbf{r}_{k+1}$.

$\alpha(\rho) \sqsubseteq^* \alpha(\rho')$, $\text{src}(\rho) \leq \text{src}(\rho')$ and $\text{tgt}(\rho) \leq \text{tgt}(\rho')$ implies $\rho \preceq \rho'$. □

An Application

Let Ω be the set of runs. We have:

$$\xrightarrow{*} \quad = \quad \bigcup_{\rho \in \min_{\preceq} \Omega} (\mathsf{src}(\rho), \mathsf{tgt}(\rho)) \; + \; \xrightarrow{*}_{\rho}$$

Theorem

$\xrightarrow{*}$ *is an almost semilinear relation.*

Proof.

Let us consider $b \in \mathbb{N}^d \times \mathbb{N}^d$ and a finitely generated periodic relation $P \subseteq \mathbb{Z}^d \times \mathbb{Z}^d$. We introduce the set $\Omega_{b,P}$ of runs ρ such that $(\mathrm{src}(\rho), \mathrm{tgt}(\rho)) \in b + P$. We introduce an order $\preceq_P$ over $\Omega_{b,P}$ defined by $\rho \preceq_P \rho'$ if $\rho \preceq \rho'$ and $(\mathrm{src}(\rho'), \mathrm{tgt}(\rho')) \in (\mathrm{src}(\rho), \mathrm{tgt}(\rho)) + P$. Observe that $\preceq_P$ is well over $\Omega_{b,P}$. Moreover we have:

$$(\xrightarrow{*}) \cap (b + P) \quad = \bigcup_{\rho \in \min_{\preceq_P} \Omega_{b,P}} (\mathrm{src}(\rho), \mathrm{tgt}(\rho)) \; + \; ((\xrightarrow{*}_{\rho}) \cap P)$$

Thus $\xrightarrow{*}$ is an almost semilinear relation. □

Corollary

Theorem

Let $\mathbf{A}$ *be a VAS and let* $\mathbf{n}$ *be a marking that is not reachable from a marking* $\mathbf{m}$*. There exists a Presburger formula* ϕ *denoting a forward inductive invariant* $\mathbf{I}$ *such that* $\mathbf{m} \in \mathbf{I}$ *and* $\mathbf{n} \notin \mathbf{I}$*.*

Corollary

The reachability problem is decidable.

Algorithm With an Easy Implementation

Reachability ($\mathbf{m}$, $\mathbf{A}$, $\mathbf{n}$)
    $k \leftarrow 0$
    `repeat forever`
        for each word $\sigma \in \mathbf{A}^k$
            `if` $\mathbf{m} \xrightarrow{\sigma} \mathbf{n}$
                `return` "reachable"
        for each Presburger formula $\phi(\mathbf{x})$ of length k
            `if` $\mathbf{m} \models \phi$, and $\mathbf{n} \models \neg\phi$ and
                $\phi(\mathbf{x}) \wedge \mathbf{y} - \mathbf{x} \in \mathbf{A} \wedge \neg\phi(\mathbf{y})$ unsat
                `return` "unreachable"
        $k \leftarrow k + 1$

Outline

One More Thing...

Let us recall the following example:

Example

Let **A** be a VAS.
We introduce:

$$R = \{(\mathbf{m}, \mathbf{n}) \in \mathbb{N}^d \times \mathbb{N}^d \mid \mathbf{n} - \mathbf{m} \in \mathbf{A}\}$$

Then R^* is the reachability relation.

Thus if R is the one step reachability relation of a VAS, then R^* is an almost semilinear relation.

Monotonicity

Definition (Monotonic)

A relation $R \subseteq \mathbb{N}^d \times \mathbb{N}^d$ is said to be monotonic if $(\mathbf{m}+\mathbf{v}, \mathbf{n}+\mathbf{v}) \in R$ for every $(\mathbf{m}, \mathbf{n}) \in R$ and for every $\mathbf{v} \in \mathbb{N}^d$.

Example

Let $\mathbf{A}$ be a VAS.
We introduce:

$$R = \{(\mathbf{m}, \mathbf{n}) \in \mathbb{N}^d \times \mathbb{N}^d \mid \mathbf{n} - \mathbf{m} \in \mathbf{A}\}$$

R is a monotonic Presburger relation.

Lemma

For every monotonic Presburger relation $R \subseteq \mathbb{N}^d \times \mathbb{N}^d$ *there exist a VASS* G *and two control states* p, q *such that* $(q, (\mathbf{y}_1, \mathbf{y}_2))$ *is reachable from* $(p, (\mathbf{x}_1, \mathbf{x}_2))$ *if and only if:*

$$(\mathbf{x}_1 + \mathbf{x}_2, \mathbf{y}_1 + \mathbf{y}_2) \in R^*$$

Proof.

Based on the decomposition of a monotonic Presburger relation into a finite union of monotonic linear relations. □

Open Problem

Theorem

The reflexive and transitive closure of a monotonic Presburger relation is a monotonic almost semilinear relation.

Open question : Does the class of monotonic almost semilinear relations is stable by reflexive and transitive closure ?

Application : reachability problem for VAS with zero tests.

Outline

Conclusion

- We presented geometrical properties satisfied by VAS reachability sets.
- We proved that the Presburger arithmetic is sufficient for denoting certificates of non-reachability.

Open problems:

- Size of formulas denoting $\mathbb{Q}_{\geq 0} \xrightarrow{*}_{\mathbf{m}}$.
- Find new algorithms for deciding the reachability problem (efficient in practice).
- Extension to the VAS + zero tests. Idea : prove that R^* is almost semilinear for every monotonic almost semilinear relation R.
- Extension to the Branching VAS. Idea : replace the Higmann's lemma by the Kruskal's lemma.
- Close the complexity gap between lower bound and upper bound.
- At least, provide a clear upper bound (in the fast growing hierarchy).