Computing Vector Addition System Reachability Sets

Jérôme Leroux

LaBRI (CNRS and University of Bordeaux), France.

Vector Addition Systems

Definition

Vector addition system (VAS) : finite set $\mathbf{A} \subseteq \mathbb{Z}^d$.
Actions : $\mathbf{a} \in \mathbf{A}$.

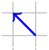
$\mathbf{A} = \{\mathbf{a}_1, \mathbf{a}_2\}$ with $\mathbf{a}_1 =$  $= (-1, 1)$

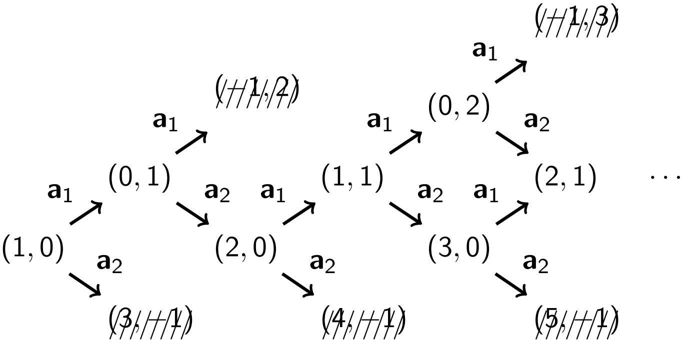
and $\mathbf{a}_2 =$  $= (2, -1)$

Semantics

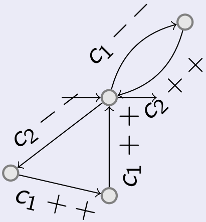
Definition

Configurations : $\mathbf{x} \in \mathbb{N}^d$.
Transition relation : $\mathbf{x} \xrightarrow{\mathbf{a}} \mathbf{y}$ if $\mathbf{x}, \mathbf{y} \in \mathbb{N}^d$, $\mathbf{a} \in \mathbf{A}$ and $\mathbf{y} = \mathbf{x} + \mathbf{a}$.

$\mathbf{A} = \{\mathbf{a}_1, \mathbf{a}_2\}$ with $\mathbf{a}_1 =$  $= (-1, 1)$
and $\mathbf{a}_2 =$  $= (2, -1)$

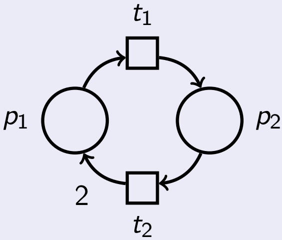


Minsky Machines without $= 0$



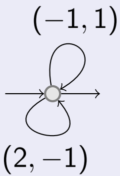
$\sim$

Petri nets



$\sim$

VAS with states



$\sim$

VAS

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

The Reachability Problem

Reachability Problem

INPUT : $\mathbf{A}$, a VAS
$(\mathbf{c}_{\text{init}}, \mathbf{c}_{\text{final}})$, a pair of configurations.

OUTPUT : $\mathbf{c}_{\text{init}} \xrightarrow{\mathbf{a}_1} \ldots \xrightarrow{\mathbf{a}_k} \mathbf{c}_{\text{final}}$ for some actions $\mathbf{a}_1, \ldots, \mathbf{a}_k$?

Central Problem

- Many VAS Problems reduce to the VAS reachability:
  - Boundedness / Place boundedness.
  - Safety.
  - Reversibility.
  - Coverability.
  - ...
- Other problems reduce to the VAS reachability.
  - Satisifiability of some logics on data words [Bojanczyk & David & Muscholl & Schwentick & Segoufin '06 '11]
  - Software Model Checking [Heizmann & Hoenicke & Podelski '13]
  - ...

Reachability Relation

Definition

$\xrightsquigarrow{\mathbf{a}_1 \ldots \mathbf{a}_k}$ is equal to $\xrightarrow{\mathbf{a}_1} \ldots \xrightarrow{\mathbf{a}_k}$

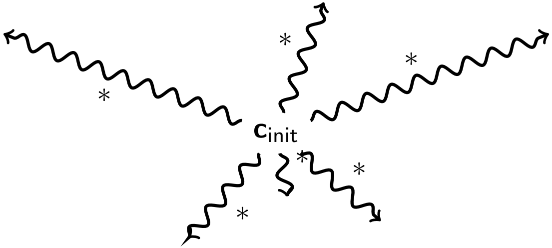
$$\overset{W}{\rightsquigarrow} \quad = \quad \bigcup_{w \in W} \overset{w}{\rightsquigarrow}$$

$$\overset{\mathbf{A}^*}{\rightsquigarrow} \quad = \quad \overset{*}{\rightsquigarrow}$$

Reachability Sets

Definition

$$\text{Reachability set from } \mathbf{c}_{\text{init}} \quad = \quad \left\{ \mathbf{c} \;\middle|\; \mathbf{c}_{\text{init}} \overset{*}{\rightsquigarrow} \mathbf{c} \right\}$$



Reachability set from $\mathbf{c}_{\text{init}}$

=

Most precise inductive invariant containing $\mathbf{c}_{\text{init}}$.

Table of Contents

A Simple Algorithm

Reachability Semi-Algorithm:

INPUT : $(\mathbf{A}, \mathbf{c}_{\text{init}})$ initialized VAS

OUTPUT : The reachability set.

$\mathbf{C} \leftarrow \{\mathbf{c}_{\text{init}}\}$

while $\mathbf{C}$ is not inductive

select an action $\mathbf{a}$

$\mathbf{C} \leftarrow \mathbf{C} \cup \left\{\mathbf{c}' \;\middle|\; \exists \mathbf{c} \in \mathbf{C} \;\; \mathbf{c} \xrightarrow{\mathbf{a}} \mathbf{c}'\right\}$

return $\mathbf{C}$

Remarks:

- Correct !
- Terminates if, and only if, the reachability set is finite.

Monotonicity

Lemma (Monotonicity)

For any configuration $\mathbf{c}$*:*

$$\mathbf{c}_{init} \overset{w}{\rightsquigarrow} \mathbf{c}_{final}$$

$$\Rightarrow$$

$$\begin{matrix}\mathbf{c}_{init} \\ + \\ \mathbf{c}\end{matrix} \overset{w}{\rightsquigarrow} \begin{matrix}\mathbf{c}_{final} \\ + \\ \mathbf{c}\end{matrix}$$

Proof:

$\mathbf{x} \xrightarrow{\mathbf{a}} \mathbf{y}$

$\Rightarrow \mathbf{y} = \mathbf{x} + \mathbf{a}$

$\Rightarrow (\mathbf{y} + \mathbf{c}) = (\mathbf{x} + \mathbf{c}) + \mathbf{a}$

$\Rightarrow \begin{matrix}\mathbf{x} \\ + \\ \mathbf{c}\end{matrix} \xrightarrow{\mathbf{a}} \begin{matrix}\mathbf{y} \\ + \\ \mathbf{c}\end{matrix}$

Example of Computation

$\mathbf{A} = \{\mathbf{a}_1, \mathbf{a}_2\}$ with $\mathbf{a}_1 = (-1, 1)$ and $\mathbf{a}_2 = (2, -1)$.
$\mathbf{c}_{\text{init}} = (1, 0)$.

$(1, 0) \xrightarrow{\mathbf{a}_1} (0, 1) \xrightarrow{\mathbf{a}_2} (2, 0)$
By monotonicity $\forall n \geq 0$:

$$(n+1, 0) = \begin{matrix}(1,0)\\ +\\ (n,0)\end{matrix} \overset{\mathbf{a}_1\mathbf{a}_2}{\rightsquigarrow} \begin{matrix}(2,0)\\ +\\ (n,0)\end{matrix} = (n+2, 0)$$

By induction $\forall n \geq 0$:

$$(1, 0) \overset{(\mathbf{a}_1\mathbf{a}_2)^n}{\rightsquigarrow} (n+1, 0).$$

$$\mathbf{c}_{\text{init}} \overset{(\mathbf{a}_1\mathbf{a}_2)^*}{\rightsquigarrow} \mathbf{c} \iff \mathbf{c} \in (1, 0) + \mathbb{N}(1, 0)$$

$$\mathbf{c}_{\text{init}} \overset{(\mathbf{a}_1\mathbf{a}_2)^*\mathbf{a}_1^*}{\rightsquigarrow} \mathbf{c} \iff \mathbf{c} \in \{(1, 0), (0, 1)\} + \mathbb{N}(1, 0) + \mathbb{N}(0, 1)$$

Acceleration

Acceleration Semi-Algorithm:

INPUT : $(\mathbf{A}, \mathbf{c}_{\text{init}})$ initialized VAS

OUTPUT : The reachability set.

$\mathbf{C} \leftarrow \{\mathbf{c}_{\text{init}}\}$

while $\mathbf{C}$ is not inductive

  select word σ

$$\mathbf{C} \leftarrow \left\{ \mathbf{c}' \;\middle|\; \exists \mathbf{c} \in \mathbf{C} \;\; \mathbf{c} \overset{\sigma^*}{\rightsquigarrow} \mathbf{c}' \right\}$$

return $\mathbf{C}$

Remarks:

- Correct !
- Implemented in tools : FAST, LASH, TREX, ...

Flat Initialized VAS

Definition (Flat Initialized VAS)

An initialized VAS $(\mathbf{A}, \mathbf{c}_{\text{init}})$ is flat if:

$$\text{Reachability set from } \mathbf{c}_{\text{init}} = \left\{ \mathbf{c} \;\middle|\; \mathbf{c}_{\text{init}} \xrightarrow{\sigma_1^* \ldots \sigma_k^*} \mathbf{c} \right\}$$

for some $\sigma_1, \ldots, \sigma_k \in \mathbf{A}^*$.

Lemma

There exists a terminating execution of the acceleration semi-algorithm from $(\mathbf{A}, \mathbf{c}_{init})$ if, and only if, $(\mathbf{A}, \mathbf{c}_{init})$ is flat.

Deterministic Executions

Theorem

Assume that the line "select word σ" produces an infinite sequence of words such that any finite sequence is a subsequence, then the acceleration semi-algorithm terminates from $(\mathbf{A}, \mathbf{c}_{init})$ if, and only if, $(\mathbf{A}, \mathbf{c}_{init})$ is flat.

Proof.

Just observe that $\mathbf{C} \subseteq \left\{ \mathbf{c}' \;\middle|\; \exists \mathbf{c} \in \mathbf{C} \;\; \mathbf{c} \xrightarrow{\sigma^*} \mathbf{c}' \right\}$. □

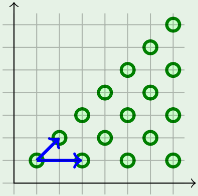
Table of Contents

Presburger Sets

Definition

A Presburger set is a set $\mathbf{X} \subseteq \mathbb{N}^d$ definable in $\mathsf{FO}(\mathbb{N}, +)$.

Example



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

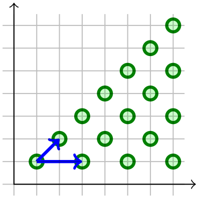
Denoted by:

$$\phi(x, y) \quad := \quad \exists n_1 \exists n_2 \;\; x = 1 + n_1 + 2n_2 \wedge y = 1 + n_1$$

Semilinear Sets

Definition (Ginsburg & Spanier '66)

Linear set : $\mathbf{b} + \mathbb{N}\mathbf{p}_1 + \cdots + \mathbb{N}\mathbf{p}_m$ with $\mathbf{b}, \mathbf{p}_1, \ldots, \mathbf{p}_m \in \mathbb{N}^d$.
Semilinear set : finite union of linear sets.



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

Presburger Sets = Semilinear Sets

Theorem (Ginsburg & Spanier '66)

Presburger sets = semilinear sets

Corollary

Semilinear sets are closed under union, intersection, complement, projection of components, ...

Some Undecidable Problems

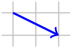
- Given a relation $R \subseteq \mathbb{N}^d \times \mathbb{N}^d$ denoted by a Presburger formula, the following problems are undecidable:
  - R^* is Presburger ? is equal to a given Presburger relation ?
  - $\{\mathbf{y} \in \mathbb{N}^d \mid (\mathbf{c}_{\text{init}}, \mathbf{y}) \in R^*\}$ is Presburger ? is equal to a given Presburger set ?
  - A Minsky machine is Flat ? Its reachability set is Presburger ? is equal to a given Presburger set ?

Fireability

Lemma

For any word $\sigma \in \mathbf{A}^*$, there exists a unique configuration $\mathbf{c}_\sigma$ such that:

$$\mathbf{x} \overset{\sigma}{\rightsquigarrow} \quad \iff \quad \mathbf{x} \geq \mathbf{c}_\sigma$$

$\mathbf{a}_1 =$  $= (-1, 1)$ and $\mathbf{a}_2 =$  $= (2, -1)$.

$$\mathbf{x} \overset{\mathbf{a}_1\mathbf{a}_1\mathbf{a}_2}{\rightsquigarrow}$$

$$\iff$$

$$\mathbf{x} \geq \mathbf{0} \quad \wedge \quad \mathbf{x} + \mathbf{a}_1 \geq \mathbf{0} \quad \wedge \quad \mathbf{x} + \mathbf{a}_1 + \mathbf{a}_1 \geq \mathbf{0} \quad \wedge \quad \mathbf{x} + \mathbf{a}_1 + \mathbf{a}_1 + \mathbf{a}_2 \geq \mathbf{0}$$

$$\iff$$

$$\mathbf{x} \geq (0,0) \quad \wedge \quad \mathbf{x} \geq (1,-1) \quad \wedge \quad \mathbf{x} \geq (2,-2) \quad \wedge \quad \mathbf{x} \geq (0,-1)$$

$$\iff$$

$$\mathbf{x} \geq (2,0)$$

Proof

$\sigma = \mathbf{a}_1 \dots \mathbf{a}_k$:

$$\mathbf{x} \overset{\sigma}{\rightsquigarrow}$$

$$\iff$$

$$\bigwedge_{0 \leq p \leq k} \mathbf{x} + \sum_{j=1}^{p} \mathbf{a}_j \geq \mathbf{0}$$

$$\iff$$

$$\mathbf{x} \geq \mathbf{c}_\sigma$$

where $\mathbf{c}_\sigma(i) = \max_{0 \leq p \leq k} - \sum_{j=1}^{p} \mathbf{a}_j(i)$.

Transitive Closure with Presburger Arithmetic

Theorem (Fribourg '00)

$\overset{\sigma^*}{\rightsquigarrow}$ *is effectively Presburger.*

$\sigma = \mathbf{a}_1 \dots \mathbf{a}_k$:

$$\mathbf{x} \overset{\sigma^n}{\rightsquigarrow} \mathbf{y}$$

$$\Longleftrightarrow$$

$$\mathbf{x} + n \sum_{j=1}^{k} \mathbf{a}_j = \mathbf{y} \text{ and } \forall 0 \leq m < n \;\; \mathbf{x} + m(\sum_{j=1}^{k} \mathbf{a}_j) \geq \mathbf{c}_\sigma$$

Iterating Linear Functions

Theorem (Boigelot'98)

$f : \mathbb{Z}^d \to \mathbb{Z}^d$ function $f(\mathbf{x}) = M\mathbf{x} + \mathbf{v}$ where $M \in \mathbb{Z}^{d \times d}$ and $\mathbf{v} \in \mathbb{Z}^d$.

$$\mathbf{y} \in f^*(\mathbf{x})$$

is definable in $\mathrm{FO}(\mathbb{Z}, \mathbb{N}, +)$ if, and only if,

$$M^* = \{M^n \mid n \in \mathbb{N}\}$$

is finite.

Example

Let $f(x) = 2x$. Then $y \in f^*(x) \iff \exists n \in \mathbb{N} \mid y = 2^n x$.

Iterating Guarded Linear Functions

Theorem (Leroux & Finkel '02)

$f : \mathbb{Z}^d \rightarrow \mathbb{Z}^d$ function defined over a set definable in $\mathrm{FO}(\mathbb{Z}, \mathbb{N}, +)$ *by $f(\mathbf{x}) = M\mathbf{x} + \mathbf{v}$ where $M \in \mathbb{Z}^{d \times d}$ is such that M^* is finite and $\mathbf{v} \in \mathbb{Z}^d$.*

$$\mathbf{y} \in f^*(\mathbf{x})$$

is definable in $\mathrm{FO}(\mathbb{Z}, \mathbb{N}, +)$

Iterating Relations

Theorem (Bozga & Gîrlea & Iosif '09)

Let $R \subseteq \mathbb{Z}^d \times \mathbb{Z}^d$ defined as a conjunction of predicates of the form $\substack{+\\-} x \substack{+\\-} y \leq c$ where x, y are free variables and $c \in \mathbb{Z}$. Then R^* is definable in $\mathsf{FO}(\mathbb{Z}, \mathbb{N}, +)$.

Example

$(x, y)R(x', y') := x' - x \leq 1 \wedge x - x' \leq -1 \wedge y' - y \leq 2 \wedge y - y' \leq -2$
Then $(x, y)R^*(x', y') := x' \geq x \wedge 2(x' - x) = (y' - y)$

Example

Acceleration for timed automata.

Acceleration

Acceleration Semi-Algorithm:

INPUT : $(\mathbf{A}, \mathbf{c}_{\text{init}})$ initialized VAS

OUTPUT : The reachability set.

$\mathbf{C} \leftarrow \{\mathbf{c}_{\text{init}}\}$

while $\mathbf{C}$ is not inductive

select word σ

$$\mathbf{C} \leftarrow \left\{ \mathbf{c}' \;\middle|\; \exists \mathbf{c} \in \mathbf{C} \;\; \mathbf{c} \xrightarrow{\sigma^*} \mathbf{c}' \right\}$$

return $\mathbf{C}$

- In theory : terminate on any flat initialized VAS.
- In practice : find good heuristics and good symbolic representations.

Flat Counter Systems Almost Everywhere !

Theorem (Finkel & Leroux '02, Leroux & Sutre '05)

Reachability sets of flat Initialized VAS are effectively semilinear.

"Many known semilinear subclasses of counter automata are flat: reversal bounded counter machines, lossy vector addition systems with states, reversible Petri nets, persistent and conflict-free Petri nets, etc."
[Leroux & Sutre, ATVA 2005]

Theorem (Leroux '13)

An initialized VAS is flat if, and only if, its reachability set is semilinear.

Application:

- Completeness of acceleration techniques.
- Reachability semilinear $\Rightarrow$ effectively semilinear.

Application : Distance of Reachability

Corollary

For any flat initialized VAS $< \mathbf{A}, \mathbf{c}_{init} >$ *there exists a constant* m *such that for every reachable configurations* $\mathbf{c}$ *from* $\mathbf{c}_{init}$, *there exists:*

$$\mathbf{c}_{init} \overset{\sigma}{\rightsquigarrow} \mathbf{c}$$

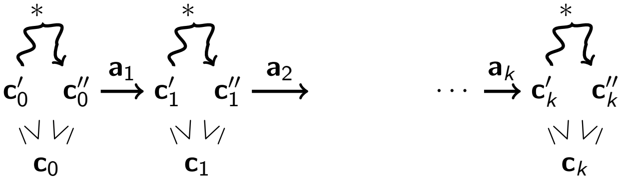
with $|\sigma| \leq m.||\mathbf{c} - \mathbf{c}_{init}||_\infty$

There exists $\sigma_1, \ldots, \sigma_k \in \mathbf{A}^*$ such that:

$$\text{Reachability set from } \mathbf{c}_{\text{init}} \quad = \quad \left\{ \mathbf{c} \;\middle|\; \mathbf{c}_{\text{init}} \overset{\sigma_1^* \ldots \sigma_k^*}{\rightsquigarrow} \mathbf{c} \right\}$$

Table of Contents

Well Preorder $\trianglelefteq$ on Runs



$$\mathbf{c}_0 \xrightarrow{\ \mathbf{a}_1\ } \mathbf{c}_1 \xrightarrow{\ \mathbf{a}_2\ } \mathbf{c}_2 \quad \cdots \xrightarrow{\ \mathbf{a}_k\ } \mathbf{c}_k$$

Theorem (Jančar '90, Leroux '11 '12)

$\trianglelefteq$ is a well preorder, i.e.:

$$\forall \rho_0, \rho_1, \cdots \qquad \exists i_0 < i_1 < \cdots \quad \Big| \quad \rho_{i_0} \trianglelefteq \rho_{i_1} \trianglelefteq \cdots$$

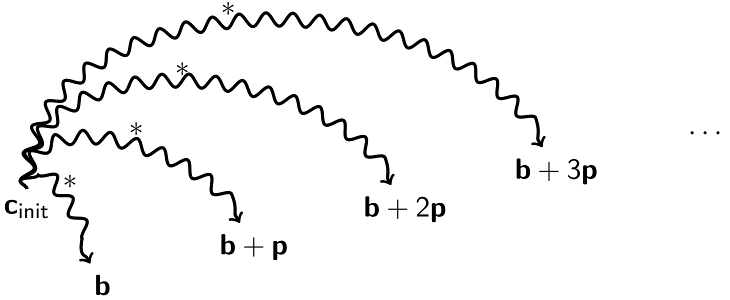
Extracting Cycles

$$\mathbf{c}_0 + \mathbf{v}_0 \xrightarrow{\sigma_0} \mathbf{c}_0 + \mathbf{v}_1 \xrightarrow{\mathbf{a}_1} \mathbf{c}_1 + \mathbf{v}_1 \xrightarrow{\sigma_1} \mathbf{c}_1 + \mathbf{v}_2 \xrightarrow{\mathbf{a}_2} \cdots \xrightarrow{\mathbf{a}_k} \mathbf{c}_k + \mathbf{v}_k \xrightarrow{\sigma_k} \mathbf{c}_k + \mathbf{v}_{k+1}$$

$$\Longrightarrow \quad \forall n \geq 1$$

$$\mathbf{c}_0 + n\mathbf{v}_0 \xrightarrow{\sigma_0^n} \mathbf{c}_0 + n\mathbf{v}_1 \xrightarrow{\mathbf{a}_1} \mathbf{c}_1 + n\mathbf{v}_1 \xrightarrow{\sigma_1^n} \mathbf{c}_1 + n\mathbf{v}_2 \xrightarrow{\mathbf{a}_2} \cdots \xrightarrow{\mathbf{a}_k} \mathbf{c}_k + n\mathbf{v}_k \xrightarrow{\sigma_k^n} \mathbf{c}_k + n\mathbf{v}_{k+1}$$

The One Period Case

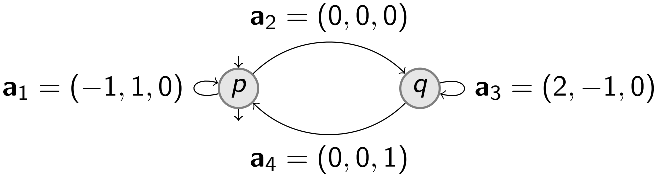


$\rho_n = (\mathbf{c}_{\text{init}} \xrightarrow{w_n} \mathbf{b} + n\mathbf{p})$
$\trianglelefteq$ well preorder $\Rightarrow \exists r \geq 0, s \geq 1\ \rho_r \trianglelefteq \rho_{r+s}$
$\exists \sigma_0, \mathbf{a}_1, \sigma_1 \dots, \mathbf{a}_k, \sigma_k$ such that $\forall n \in \mathbb{N}$:

$$\mathbf{c}_{\text{init}} \xrightarrow{\sigma_0^* \mathbf{a}_1 \sigma_1^* \dots \mathbf{a}_k \sigma_k^*} \mathbf{b} + (r + ns)\mathbf{p}$$

Table of Contents

The Hopcroft-Pansiot 1979 Example



$$(1,0,0) \xrightarrow{\mathbf{a}_1\mathbf{a}_2\mathbf{a}_3\mathbf{a}_4} (2,0,1) \xrightarrow{\mathbf{a}_1^2\mathbf{a}_2\mathbf{a}_3^2\mathbf{a}_4} (4,0,2)\cdots \xrightarrow{\mathbf{a}_1^{2^n}\mathbf{a}_2\mathbf{a}_3^{2^n}\mathbf{a}_4} (2^{n+1},0,n+1)$$

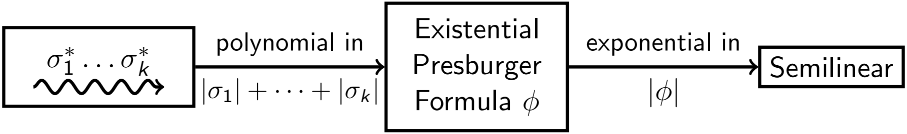
Configurations reachable from $(1, 0, 0)$

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

Complexity

Theorem (Mayr & Meyer '81)

There exist VAS with reachability sets of Ackermann cardinal.



Corollary

There exists semilinear VAS such that $\forall \sigma_1, \ldots, \sigma_k$

$$\textit{Reachability set} \quad = \quad \left\{ \mathbf{c} \;\middle|\; \mathbf{c}_{init} \xrightarrow{\sigma_1^* \ldots \sigma_k^*} \mathbf{c} \right\}$$

implies $|\sigma_1| + \cdots + |\sigma_k|$ *is Ackermann in the size of the VAS.*

Possible Fixes

Acceleration can be combined with:

- Abstract interpretation [Gonnord & Halbwachs '10] [Leroux & Sutre '07]
- Interpolation based techniques [Hojjat & Iosif & Konecny & Kuncak & Ruemmer '12] [Caniart & Fleury & Leroux & Zeitoun '08]

Open Problems

Open Problems:

- $\forall$ semilinear VAS $\exists$ Ackermann words $\sigma_1 \ldots \sigma_k$ such that:

$$\text{Reachability set} \quad = \quad \left\{ \mathbf{c} \;\middle|\; \mathbf{c}_{\text{init}} \xrightarrow{\sigma_1^* \ldots \sigma_k^*} \mathbf{c} \right\}$$

- Ackermann upper bound for semilinear VAS reachability pbm.

Facts:

- Proved for bounded VAS [McAloon '84]
- New proof based on bad sequences for the Dickson's lemma [Figueira & Figueira & Schmitz & Schnoebelen '11]

Table of Contents

Conclusion

Theorem

$$\textit{semilinear VAS} \quad = \quad \textit{flat VAS}$$

Observations:

- $\trianglelefteq$ is central.
- Completeness of tools based on acceleration.

Open problems:

- Complexity of the reachability problem for semilinear VAS.
  - 2 pbms !
- Simple criterion for detecting the VAS not semilinear.
- Improve acceleration techniques with on-demand over-approximations.