Ideal Decompositions for Vector Addition Systems

S. Schmitz
joint work with J. Leroux

ENS Cachan & CNRS & INRIA, Université Paris-Saclay

Séminaire Vérification, IRIF
October 24th, 2016

Outline

- vector addition systems (VAS)
  and their reachability problem
- ideals of well-quasi-orders
- a counter-example guided abstraction refinement
  (CEGAR) procedure
- the KLMST decomposition algorithm
  named after Sacerdote and Tenney (1977), Mayr (1981),
  Kosaraju (1982), and Lambert (1992)

Vector Addition Systems (VAS)

(Karp and Miller, 1969)

Syntax

- dimension $\mathbf{d} \in \mathbb{N}$
- finite set $\mathbf{A} \subseteq_{\text{fin}} \mathbb{Z}^{\mathbf{d}}$ of actions $\mathbf{a} \in \mathbf{A}$

Semantics

- configurations $\mathbf{u}, \mathbf{v}, \ldots \in \mathbb{N}^{\mathbf{d}}$
- transitions $\mathbf{u} \xrightarrow{\mathbf{a}} \mathbf{v} \in \mathbb{N}^{\mathbf{d}} \times \mathbf{A} \times \mathbb{N}^{\mathbf{d}}$ with $\mathbf{v} = \mathbf{u} + \mathbf{a}$

Vector Addition Systems (VAS)

(Karp and Miller, 1969)

Syntax

- dimension $d \in \mathbb{N}$
- finite set $\mathbf{A} \subseteq_{\text{fin}} \mathbb{Z}^d$ of actions $\mathbf{a} \in \mathbf{A}$

Semantics

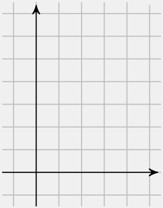
- configurations $\mathbf{u}, \mathbf{v}, \ldots \in \mathbb{N}^d$
- transitions $\mathbf{u} \xrightarrow{\mathbf{a}} \mathbf{v} \in \mathbb{N}^d \times \mathbf{A} \times \mathbb{N}^d$ with $\mathbf{v} = \mathbf{u} + \mathbf{a}$

Example VAS

Example

$d = 2$

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

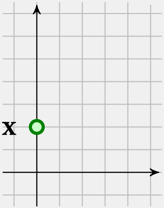


Example VAS

Example

$d = 2$

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

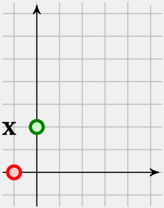


$\mathbf{x}$=(0,2)

Example VAS

Example

$$d = 2 \qquad \mathbf{A} = \left\{ \quad , \quad \right\}$$

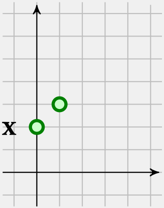


$\mathbf{x} = (0,2) \longrightarrow (-1,0) \notin \mathbb{N}^2$

Example VAS

Example

$$d = 2 \qquad\qquad \mathbf{A} = \{$$  ,  $$\}$$



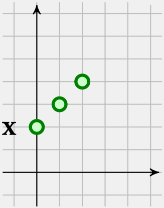
$\mathbf{x}=(0,2)\longrightarrow(1,3)$

Example VAS

Example

$d = 2$

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

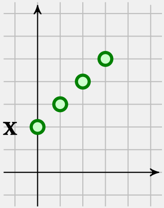


$\mathbf{x}=(0,2)$  $\longrightarrow (1,3)$  $\longrightarrow (2,4)$

Example VAS

Example

$$d = 2 \qquad \mathbf{A} = \left\{ \quad , \quad \right\}$$

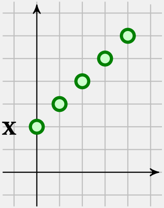


$$\mathbf{x} = (0,2) \longrightarrow (1,3) \longrightarrow (2,4) \longrightarrow (3,5)$$

Example VAS

Example

$$d = 2 \qquad\qquad \mathbf{A} = \left\{ \quad , \quad \right\}$$

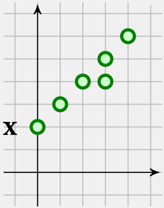



$$\mathbf{x} = (0,2) \longrightarrow (1,3) \longrightarrow (2,4) \longrightarrow (3,5) \longrightarrow (4,6)$$

Example VAS

Example

$$d = 2 \qquad \mathbf{A} = \{\ ,\ \}$$



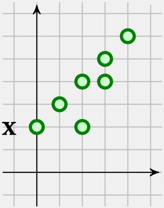
$$\mathbf{x} = (0,2) \longrightarrow (1,3) \longrightarrow (2,4) \longrightarrow (3,5) \longrightarrow (4,6) \longrightarrow (3,4)$$

Example VAS

Example

$d = 2$

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

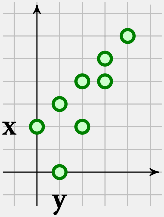


$\mathbf{x}=(0,2) \longrightarrow (1,3) \longrightarrow (2,4) \longrightarrow (3,5) \longrightarrow (4,6) \longrightarrow (3,4) \longrightarrow (2,2)$

Example VAS

Example

$$d = 2 \qquad \mathbf{A} = \left\{ \quad , \quad \right\}$$



$$\mathbf{x}{=}(0{,}2) \longrightarrow (1{,}3) \longrightarrow (2{,}4) \longrightarrow (3{,}5) \longrightarrow (4{,}6) \longrightarrow (3{,}4) \longrightarrow (2{,}2) \longrightarrow (0{,}1){=}\mathbf{y}$$

Runs and Preruns

Definition (Prerun)

A prerun is an element

$$(\mathbf{u},\ (\mathbf{u}_1,\mathbf{a}_1,\mathbf{v}_1)\cdots(\mathbf{u}_k,\mathbf{a}_k,\mathbf{v}_k),\ \mathbf{v})$$

from $\mathrm{PreRuns}_{\mathbf{A}} \stackrel{\text{def}}{=} \mathbb{N}^d \times (\mathbb{N}^d \times \mathbf{A} \times \mathbb{N}^d)^* \times \mathbb{N}^d$

Definition (Run)

A prerun is connected (is a run) if

(source) $\mathbf{u} = \mathbf{u}_1$

(transitions) $\forall 1 \leqslant j \leqslant k,\ \mathbf{u}_j + \mathbf{a}_j = \mathbf{v}_j$

(contiguity) $\forall 1 < j \leqslant k,\ \mathbf{v}_{j-1} = \mathbf{u}_j$

(target) $\mathbf{v}_k = \mathbf{v}$

The Reachability Problem

$\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \stackrel{\text{def}}{=} \{\rho \in \mathrm{PreRuns}_{\mathbf{A}} \mid \rho$ is a run with source $\mathbf{x}$ and target $\mathbf{y}\}$

VAS Reachability

input $\mathbf{A} \subseteq_{\text{fin}} \mathbb{Z}^d, \mathbf{x}, \mathbf{y} \in \mathbb{N}^d$

question Is $\mathbf{y}$ reachable from $\mathbf{x}$ in $\mathbf{A}$?
I.e., is $\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \neq \emptyset$?

Theorem (Mayr, 1981; Kosaraju, 1982; Lambert, 1992; Leroux, 2011)

VAS Reachability is decidable.

- by the KLMST decomposition algorithm (Mayr, 1981; Kosaraju, 1982; Lambert, 1992)
- by Presburger invariants (Leroux, 2011)

The Reachability Problem

$\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \stackrel{\text{def}}{=} \{\rho \in \mathrm{PreRuns}_{\mathbf{A}} \mid \rho \text{ is a run with source } \mathbf{x} \text{ and target } \mathbf{y}\}$

VAS Reachability

input $\mathbf{A} \subseteq_{\text{fin}} \mathbb{Z}^d, \mathbf{x},\mathbf{y} \in \mathbb{N}^d$

question Is $\mathbf{y}$ reachable from $\mathbf{x}$ in $\mathbf{A}$?
I.e., is $\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \neq \emptyset$?

Theorem (Mayr, 1981; Kosaraju, 1982; Lambert, 1992; Leroux, 2011)

VAS Reachability is decidable.

- by the KLMST decomposition algorithm (Mayr, 1981; Kosaraju, 1982; Lambert, 1992)
- by Presburger invariants (Leroux, 2011)

The Reachability Problem

$\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \stackrel{\text{def}}{=} \{\rho \in \mathsf{PreRuns}_{\mathbf{A}} \mid \rho \text{ is a run with source } \mathbf{x} \text{ and target } \mathbf{y}\}$

VAS Reachability

input $\mathbf{A} \subseteq_{\text{fin}} \mathbb{Z}^d, \mathbf{x},\mathbf{y} \in \mathbb{N}^d$

question Is $\mathbf{y}$ reachable from $\mathbf{x}$ in $\mathbf{A}$?
I.e., is $\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \neq \emptyset$?

Theorem (Mayr, 1981; Kosaraju, 1982; Lambert, 1992; Leroux, 2011)

VAS Reachability is decidable.

- by the KLMST decomposition algorithm (Mayr, 1981; Kosaraju, 1982; Lambert, 1992)
- by Presburger invariants (Leroux, 2011)

The Reachability Problem

$\text{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \stackrel{\text{def}}{=} \{\rho \in \text{PreRuns}_{\mathbf{A}} \mid \rho \text{ is a run with source } \mathbf{x} \text{ and target } \mathbf{y}\}$

VAS Reachability

input: $\mathbf{A} \subseteq_{\text{fin}} \mathbb{Z}^d, \mathbf{x},\mathbf{y} \in \mathbb{N}^d$

question: Is $\mathbf{y}$ reachable from $\mathbf{x}$ in $\mathbf{A}$?
I.e., is $\text{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \neq \emptyset$?

Theorem (Mayr, 1981; Kosaraju, 1982; Lambert, 1992; Leroux, 2011)

VAS Reachability is decidable.

- by the KLMST decomposition algorithm (Mayr, 1981; Kosaraju, 1982; Lambert, 1992)
- by Presburger invariants (Leroux, 2011)

Decomposition Theorem

Theorem (Leroux and S., 2015)

The KLMST decomposition algorithm computes the ideal decomposition of

$$\downarrow \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \stackrel{def}{=} \{\rho' \in \mathrm{PreRuns}_{\mathbf{A}} \mid \exists \rho \in \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \,.\, \rho' \trianglelefteq \rho\}$$

- entails decidability of VAS Reachability:

$$\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = \emptyset \text{ iff } \downarrow \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = \emptyset$$

Upcoming

- definition of a wqo over preruns (Jančar, 1990)
- wqo ideals (Finkel and Goubault-Larrecq, 2009, 2012)

Decomposition Theorem

Theorem (Leroux and S., 2015)

The KLMST decomposition algorithm computes the ideal decomposition of

$$\downarrow \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \stackrel{def}{=} \{\rho' \in \mathrm{PreRuns}_{\mathbf{A}} \mid \exists \rho \in \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \,.\, \rho' \trianglelefteq \rho\}$$

- entails decidability of VAS Reachability:

$$\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = \emptyset \text{ iff } \downarrow \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = \emptyset$$

Upcoming

- definition of a wqo over preruns (Jančar, 1990)
- wqo ideals (Finkel and Goubault-Larrecq, 2009, 2012)

Decomposition Theorem

Theorem (Leroux and S., 2015)

The KLMST decomposition algorithm computes the ideal decomposition of

$$\downarrow \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \stackrel{def}{=} \{\rho' \in \mathrm{PreRuns}_{\mathbf{A}} \mid \exists \rho \in \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})\,.\,\rho' \trianglelefteq \rho\}$$

- entails decidability of VAS Reachability:

$$\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = \emptyset \text{ iff } \downarrow \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = \emptyset$$

Upcoming

- definition of a wqo over preruns (Jančar, 1990)
- wqo ideals (Finkel and Goubault-Larrecq, 2009, 2012)

Decomposition Theorem

Theorem (Leroux and S., 2015)

The KLMST decomposition algorithm computes the ideal decomposition of

$$\downarrow \mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \stackrel{def}{=} \{\rho' \in \mathsf{PreRuns}_{\mathbf{A}} \mid \exists \rho \in \mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \,.\, \rho' \trianglelefteq \rho\}$$

- entails decidability of VAS Reachability:

$$\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = \emptyset \text{ iff } \downarrow \mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = \emptyset$$

Upcoming

- definition of a wqo over preruns (Jančar, 1990)
- wqo ideals (Finkel and Goubault-Larrecq, 2009, 2012)

Well-Quasi-Orders (wqo)

Definition

A quasi-order $(X, \leqslant)$ is a wqo if in any infinite sequence $x_0, x_1, \ldots$ of elements of X, $\exists i < j$ s.t. $x_i \leqslant x_j$.

Example

- finite sets with equality $(X, =)$
- natural numbers $(\mathbb{N}, \leqslant)$
- Dickson's Lemma: if $(A, \leqslant_A)$ and $(B, \leqslant_B)$ are wqos, then $(A \times B, \leqslant_\times)$ is a wqo, where $(a, b) \leqslant_\times (a', b')$ iff $a \leqslant_A a'$ and $b \leqslant_B b'$
- Higman's Lemma: if $(A, \leqslant)$ is a wqo, then $(A^*, \leqslant_*)$ is a wqo, where $u \leqslant_* v$ iff $u = a_1 \cdots a_k$ and $v = v_0 b_1 v_1 \cdots v_{k-1} b_k v_k$ with $v_0, \ldots, v_k \in A^*$ and $\forall 1 \leqslant j \leqslant k \,.\, a_j \leqslant b_j \in A$.

Well-Quasi-Orders (wqo)

Definition

A quasi-order $(X, \leqslant)$ is a wqo if in any infinite sequence $x_0, x_1, \ldots$ of elements of X, $\exists i < j$ s.t. $x_i \leqslant x_j$.

Example

- finite sets with equality $(X, =)$
- natural numbers $(\mathbb{N}, \leqslant)$
- Dickson's Lemma: if $(A, \leqslant_A)$ and $(B, \leqslant_B)$ are wqos, then $(A \times B, \leqslant_\times)$ is a wqo, where $(a, b) \leqslant_\times (a', b')$ iff $a \leqslant_A a'$ and $b \leqslant_B b'$
- Higman's Lemma: if $(A, \leqslant)$ is a wqo, then $(A^*, \leqslant_*)$ is a wqo, where $u \leqslant_* v$ iff $u = a_1 \cdots a_k$ and $v = v_0 b_1 v_1 \cdots v_{k-1} b_k v_k$ with $v_0, \ldots, v_k \in A^*$ and $\forall 1 \leqslant j \leqslant k \,.\, a_j \leqslant b_j \in A$.

Well-Quasi-Orders (wqo)

Definition

A quasi-order $(X, \leqslant)$ is a wqo if in any infinite sequence $x_0, x_1, \ldots$ of elements of X, $\exists i < j$ s.t. $x_i \leqslant x_j$.

Example

- finite sets with equality $(X, =)$
- natural numbers $(\mathbb{N}, \leqslant)$
- Dickson's Lemma: if $(A, \leqslant_A)$ and $(B, \leqslant_B)$ are wqos, then $(A \times B, \leqslant_\times)$ is a wqo, where $(a, b) \leqslant_\times (a', b')$ iff $a \leqslant_A a'$ and $b \leqslant_B b'$
- Higman's Lemma: if $(A, \leqslant)$ is a wqo, then $(A^*, \leqslant_*)$ is a wqo, where $u \leqslant_* v$ iff $u = a_1 \cdots a_k$ and $v = v_0 b_1 v_1 \cdots v_{k-1} b_k v_k$ with $v_0, \ldots, v_k \in A^*$ and $\forall 1 \leqslant j \leqslant k \,.\, a_j \leqslant b_j \in A$.

Well-Quasi-Orders (wqo)

Definition

A quasi-order $(X, \leqslant)$ is a wqo if in any infinite sequence $x_0, x_1, \ldots$ of elements of X, $\exists i < j$ s.t. $x_i \leqslant x_j$.

Example

- finite sets with equality $(X, =)$
- natural numbers $(\mathbb{N}, \leqslant)$
- Dickson's Lemma: if $(A, \leqslant_A)$ and $(B, \leqslant_B)$ are wqos, then $(A \times B, \leqslant_\times)$ is a wqo, where $(a,b) \leqslant_\times (a',b')$ iff $a \leqslant_A a'$ and $b \leqslant_B b'$
- Higman's Lemma: if $(A, \leqslant)$ is a wqo, then $(A^*, \leqslant_*)$ is a wqo, where $u \leqslant_* v$ iff $u = a_1 \cdots a_k$ and $v = v_0 b_1 v_1 \cdots v_{k-1} b_k v_k$ with $v_0, \ldots, v_k \in A^*$ and $\forall 1 \leqslant j \leqslant k \,.\, a_j \leqslant b_j \in A$.

Prerun Embeddings

- $(\mathbb{N}^{\mathrm{d}}, \leqslant)$ is a wqo for the componentwise ordering
- $(\mathbb{N}^{\mathrm{d}} \times \mathbf{A} \times \mathbb{N}^{\mathrm{d}}, \preceq)$ is a wqo, where $(\mathbf{u}, \mathbf{a}, \mathbf{v}) \preceq (\mathbf{u}', \mathbf{b}, \mathbf{v}')$ iff $\mathbf{u} \leqslant \mathbf{u}'$, $\mathbf{a} = \mathbf{b}$, and $\mathbf{v} \leqslant \mathbf{v}'$
- $((\mathbb{N}^{\mathrm{d}} \times \mathbf{A} \times \mathbb{N}^{\mathrm{d}})^*, \preceq_*)$ is a wqo
- Jančar (1990): $(\mathrm{PreRuns}_{\mathbf{A}}, \trianglelefteq)$ is a wqo, where $(\mathbf{u}, w, \mathbf{v}) \trianglelefteq (\mathbf{u}', w', \mathbf{v}')$ iff $\mathbf{u} \leqslant \mathbf{u}'$, $w \preceq_* w'$, and $\mathbf{v} \leqslant \mathbf{v}'$

Prerun Embeddings

- $(\mathbb{N}^d, \leqslant)$ is a wqo for the componentwise ordering
- $(\mathbb{N}^d \times \mathbf{A} \times \mathbb{N}^d, \preceq)$ is a wqo, where $(\mathbf{u}, \mathbf{a}, \mathbf{v}) \preceq (\mathbf{u}', \mathbf{b}, \mathbf{v}')$ iff $\mathbf{u} \leqslant \mathbf{u}'$, $\mathbf{a} = \mathbf{b}$, and $\mathbf{v} \leqslant \mathbf{v}'$
- $((\mathbb{N}^d \times \mathbf{A} \times \mathbb{N}^d)^*, \preceq_*)$ is a wqo
- Jančar (1990): $(\mathrm{PreRuns}_{\mathbf{A}}, \trianglelefteq)$ is a wqo, where $(\mathbf{u}, w, \mathbf{v}) \trianglelefteq (\mathbf{u}', w', \mathbf{v}')$ iff $\mathbf{u} \leqslant \mathbf{u}'$, $w \preceq_* w'$, and $\mathbf{v} \leqslant \mathbf{v}'$

Prerun Embeddings

- $(\mathbb{N}^d, \leqslant)$ is a wqo for the componentwise ordering
- $(\mathbb{N}^d \times \mathbf{A} \times \mathbb{N}^d, \preceq)$ is a wqo, where
  $(\mathbf{u}, \mathbf{a}, \mathbf{v}) \preceq (\mathbf{u}', \mathbf{b}, \mathbf{v}')$ iff $\mathbf{u} \leqslant \mathbf{u}'$, $\mathbf{a} = \mathbf{b}$, and $\mathbf{v} \leqslant \mathbf{v}'$
- $((\mathbb{N}^d \times \mathbf{A} \times \mathbb{N}^d)^*, \preceq_*)$ is a wqo
- Jančar (1990): $(\mathrm{PreRuns}_{\mathbf{A}}, \trianglelefteq)$ is a wqo, where
  $(\mathbf{u}, w, \mathbf{v}) \trianglelefteq (\mathbf{u}', w', \mathbf{v}')$ iff $\mathbf{u} \leqslant \mathbf{u}'$, $w \preceq_* w'$, and $\mathbf{v} \leqslant \mathbf{v}'$

Prerun Embeddings

- $(\mathbb{N}^d, \leqslant)$ is a wqo for the componentwise ordering
- $(\mathbb{N}^d \times \mathbf{A} \times \mathbb{N}^d, \preceq)$ is a wqo, where
  $(\mathbf{u}, \mathbf{a}, \mathbf{v}) \preceq (\mathbf{u}', \mathbf{b}, \mathbf{v}')$ iff $\mathbf{u} \leqslant \mathbf{u}'$, $\mathbf{a} = \mathbf{b}$, and $\mathbf{v} \leqslant \mathbf{v}'$
- $((\mathbb{N}^d \times \mathbf{A} \times \mathbb{N}^d)^*, \preceq_*)$ is a wqo
- Jančar (1990): $(\mathrm{PreRuns}_{\mathbf{A}}, \trianglelefteq)$ is a wqo, where
  $(\mathbf{u}, w, \mathbf{v}) \trianglelefteq (\mathbf{u}', w', \mathbf{v}')$ iff $\mathbf{u} \leqslant \mathbf{u}'$, $w \preceq_* w'$, and $\mathbf{v} \leqslant \mathbf{v}'$

Characterising WQOs

Upward closure: $\uparrow S \stackrel{\text{def}}{=} \{x \in X \mid \exists s \in S \,.\, s \leqslant x\}$.

Lemma (Minimal Basis Property)

A qo $(X, \leqslant)$ *is a wqo iff every non-empty subset* $S \subseteq X$ *has a finite set of minimal elements* $\min_{\leqslant} S$.

Lemma (Ascending Chain Property)

A qo $(X, \leqslant)$ *is a wqo iff every ascending chain* $U_0 \subsetneq U_1 \subsetneq \cdots$ *of upward-closed sets is finite.*

Template for many algorithms: represent the sets U_n as $\uparrow(\min_{\leqslant} U_n)$ using finitely many elements.

Characterising WQOs

Downward closure: $\downarrow S \stackrel{\text{def}}{=} \{x \in X \mid \exists s \in S \,.\, x \leqslant s\}$.

Lemma (Minimal Basis Property)

A qo $(X, \leqslant)$ is a wqo iff every non-empty subset $S \subseteq X$ has a finite set of minimal elements $\min_{\leqslant} S$.

Lemma (Descending Chain Property)

A qo $(X, \leqslant)$ is a wqo iff every descending chain $D_0 \supsetneq D_1 \supsetneq \cdots$ of downward-closed sets is finite.

Template for many algorithms: represent the sets U_n as $\uparrow(\min_{\leqslant} U_n)$ using finitely many elements.

Ideals as Canonical Bases

Downward closure: $\downarrow S \stackrel{\text{def}}{=} \{x \in X \mid \exists s \in S \,.\, x \leqslant s\}$.

Lemma (Canonical Ideal Decomposition; Bonnet, 1975)

Every downward-closed subset $D \subseteq X$ of a wqo $(X, \leqslant)$ is the union of a unique finite family of incomparable (for the inclusion) ideals.

Lemma (Descending Chain Property)

A qo $(X, \leqslant)$ is a wqo iff every descending chain $D_0 \supsetneq D_1 \supsetneq \cdots$ of downward-closed sets is finite.

Ideals

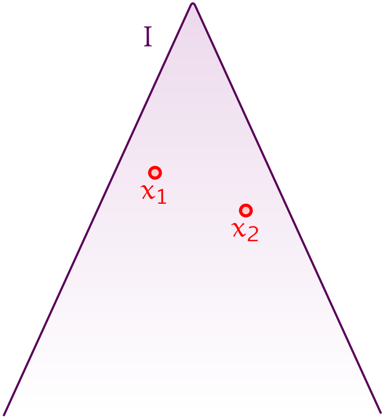
(Bonnet, 1975; Finkel and Goubault-Larrecq, 2009)

- Directed set Δ
  non-empty and $\forall x_1, x_2 \in I$,
  $\exists x. x_1 \leqslant x$ and $x_2 \leqslant x$
- Ideal I
  downwards-closed and directed
- Examples
  - $\downarrow x \in \mathrm{Idl}(X)$ for any x in X
  - $\mathbb{N} \in \mathrm{Idl}(\mathbb{N})$
  - $\{a, b\}^* \in \mathrm{Idl}(\{a, b, c\}^*)$
- Canonical Decompositions
  if $D \subseteq X$ is downwards-closed,
  then $D = I_1 \cup \cdots \cup I_n$

Ideals

(Bonnet, 1975; Finkel and Goubault-Larrecq, 2009)

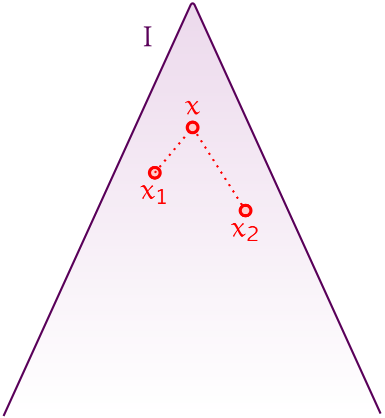
- Directed set Δ
  non-empty and $\forall x_1, x_2 \in I$,
  $\exists x. x_1 \leqslant x$ and $x_2 \leqslant x$
- Ideal I
  downwards-closed and directed
- Examples
  - $\downarrow x \in \mathrm{Idl}(X)$ for any x in X
  - $\mathbb{N} \in \mathrm{Idl}(\mathbb{N})$
  - $\{a, b\}^* \in \mathrm{Idl}(\{a, b, c\}^*)$
- Canonical Decompositions
  if $D \subseteq X$ is downwards-closed,
  then $D = I_1 \cup \cdots \cup I_n$



Ideals

(Bonnet, 1975; Finkel and Goubault-Larrecq, 2009)

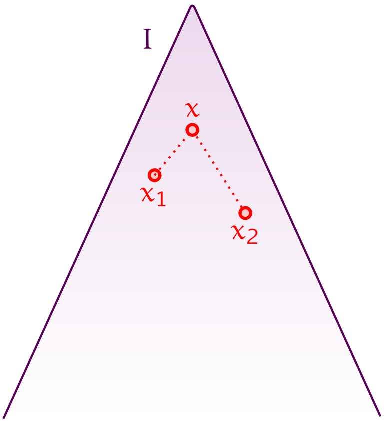
- Directed set Δ
  non-empty and $\forall x_1, x_2 \in I$, $\exists x. x_1 \leqslant x$ and $x_2 \leqslant x$
- Ideal I
  downwards-closed and directed
- Examples
  - $\downarrow x \in \mathrm{Idl}(X)$ for any x in X
  - $\mathbb{N} \in \mathrm{Idl}(\mathbb{N})$
  - $\{a,b\}^* \in \mathrm{Idl}(\{a,b,c\}^*)$
- Canonical Decompositions
  if $D \subseteq X$ is downwards-closed, then $D = I_1 \cup \cdots \cup I_n$



IDEALS

(BONNET, 1975; FINKEL AND GOUBAULT-LARRECQ, 2009)

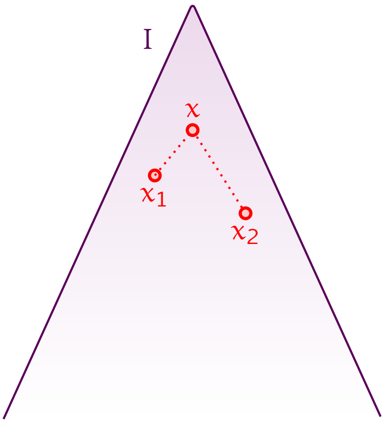
- Directed set Δ
  non-empty and $\forall x_1, x_2 \in I$, $\exists x. x_1 \leqslant x$ and $x_2 \leqslant x$
- Ideal I
  downwards-closed and directed
- Examples
  - $\downarrow x \in \mathrm{Idl}(X)$ for any x in X
  - $\mathbb{N} \in \mathrm{Idl}(\mathbb{N})$
  - $\{a,b\}^* \in \mathrm{Idl}(\{a,b,c\}^*)$
- Canonical Decompositions
  if $D \subseteq X$ is downwards-closed, then $D = I_1 \cup \cdots \cup I_n$



IDEALS

(BONNET, 1975; FINKEL AND GOUBAULT-LARRECQ, 2009)

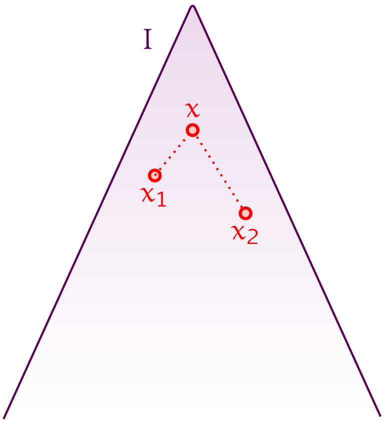
- Directed set Δ
  non-empty and $\forall x_1, x_2 \in I$, $\exists x. x_1 \leqslant x$ and $x_2 \leqslant x$
- Ideal I
  downwards-closed and directed
- Examples
  - $\downarrow x \in \mathrm{Idl}(X)$ for any x in X
  - $\mathbb{N} \in \mathrm{Idl}(\mathbb{N})$
  - $\{a, b\}^* \in \mathrm{Idl}(\{a, b, c\}^*)$
- Canonical Decompositions
  if $D \subseteq X$ is downwards-closed, then $D = I_1 \cup \cdots \cup I_n$



Ideals

(Bonnet, 1975; Finkel and Goubault-Larrecq, 2009)

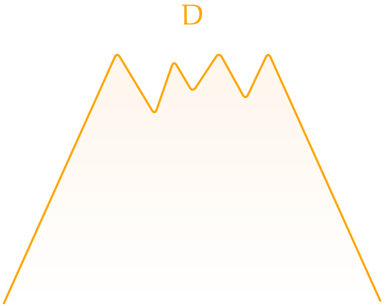
- Directed set Δ
  non-empty and $\forall x_1, x_2 \in I$, $\exists x. x_1 \leqslant x$ and $x_2 \leqslant x$
- Ideal I
  downwards-closed and directed
- Examples
  - $\downarrow x \in \mathrm{Idl}(X)$ for any x in X
  - $\mathbb{N} \in \mathrm{Idl}(\mathbb{N})$
  - $\{a, b\}^* \in \mathrm{Idl}(\{a, b, c\}^*)$
- Canonical Decompositions
  if $D \subseteq X$ is downwards-closed, then $D = I_1 \cup \cdots \cup I_n$



Ideals

(Bonnet, 1975; Finkel and Goubault-Larrecq, 2009)

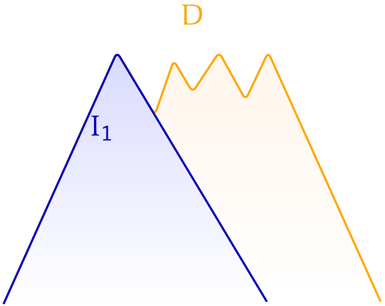
- Directed set Δ
  non-empty and $\forall x_1, x_2 \in I$, $\exists x. x_1 \leqslant x$ and $x_2 \leqslant x$
- Ideal I
  downwards-closed and directed
- Examples
  - $\downarrow x \in \mathrm{Idl}(X)$ for any x in X
  - $\mathbb{N} \in \mathrm{Idl}(\mathbb{N})$
  - $\{a,b\}^* \in \mathrm{Idl}(\{a,b,c\}^*)$
- Canonical Decompositions
  if $D \subseteq X$ is downwards-closed, then $D = I_1 \cup \cdots \cup I_n$



Ideals

(Bonnet, 1975; Finkel and Goubault-Larrecq, 2009)

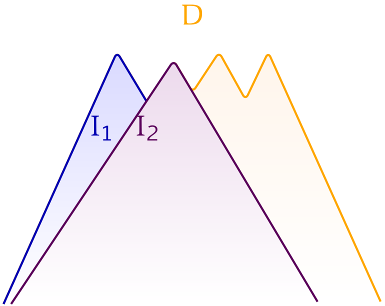
- Directed set Δ
  non-empty and $\forall x_1, x_2 \in I$, $\exists x. x_1 \leqslant x$ and $x_2 \leqslant x$
- Ideal I
  downwards-closed and directed
- Examples
  - $\downarrow x \in \mathrm{Idl}(X)$ for any x in X
  - $\mathbb{N} \in \mathrm{Idl}(\mathbb{N})$
  - $\{a, b\}^* \in \mathrm{Idl}(\{a, b, c\}^*)$
- Canonical Decompositions
  if $D \subseteq X$ is downwards-closed, then $D = I_1 \cup \cdots \cup I_n$



Ideals

(Bonnet, 1975; Finkel and Goubault-Larrecq, 2009)

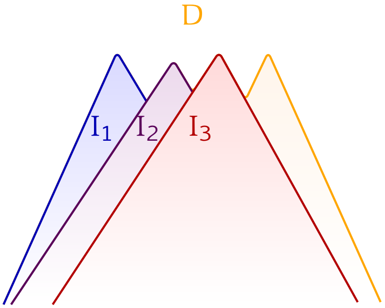
- Directed set Δ
  non-empty and $\forall x_1, x_2 \in I$,
  $\exists x. x_1 \leqslant x$ and $x_2 \leqslant x$
- Ideal I
  downwards-closed and directed
- Examples
  - $\downarrow x \in \mathrm{Idl}(X)$ for any x in X
  - $\mathbb{N} \in \mathrm{Idl}(\mathbb{N})$
  - $\{a,b\}^* \in \mathrm{Idl}(\{a,b,c\}^*)$
- Canonical Decompositions
  if $D \subseteq X$ is downwards-closed,
  then $D = I_1 \cup \cdots \cup I_n$



Ideals

(Bonnet, 1975; Finkel and Goubault-Larrecq, 2009)

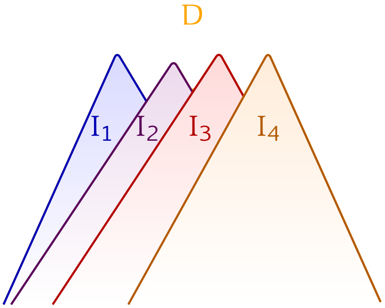
- Directed set Δ
  non-empty and $\forall x_1, x_2 \in I$, $\exists x. x_1 \leqslant x$ and $x_2 \leqslant x$
- Ideal I
  downwards-closed and directed
- Examples
  - $\downarrow x \in \mathrm{Idl}(X)$ for any x in X
  - $\mathbb{N} \in \mathrm{Idl}(\mathbb{N})$
  - $\{a,b\}^* \in \mathrm{Idl}(\{a,b,c\}^*)$
- Canonical Decompositions
  if $D \subseteq X$ is downwards-closed, then $D = I_1 \cup \cdots \cup I_n$



Ideals

(Bonnet, 1975; Finkel and Goubault-Larrecq, 2009)

- Directed set Δ
  non-empty and $\forall x_1, x_2 \in I$, $\exists x. x_1 \leqslant x$ and $x_2 \leqslant x$
- Ideal I
  downwards-closed and directed
- Examples
  - $\downarrow x \in \mathrm{Idl}(X)$ for any x in X
  - $\mathbb{N} \in \mathrm{Idl}(\mathbb{N})$
  - $\{a,b\}^* \in \mathrm{Idl}(\{a,b,c\}^*)$
- Canonical Decompositions
  if $D \subseteq X$ is downwards-closed, then $D = I_1 \cup \cdots \cup I_n$



Effectivity

- represent canonical decompositions $D = I_1 \sqcup \cdots \sqcup I_k$ where the I_j's are maximal for inclusion
- must allow effective operations over ideals: $I \subseteq J$, $I \cap J$, $I \setminus {\uparrow}x$ for $x \in X$
- Finkel and Goubault-Larrecq (2009, 2012): effective representations exist for all the wqos in this talk
- for Cartesian products: $\mathrm{Idl}(A \times B) = \{I \times J \mid I \in \mathrm{Idl}(A) \text{ and } J \in \mathrm{Idl}(B)\}$
- for finite sequences: $\mathrm{Idl}(X^*)$ are products defined by:

$$P ::= \varepsilon \mid A \cdot P \qquad \text{(products)}$$

$$A ::= (I + \varepsilon) \mid (I_1 \sqcup \cdots \sqcup I_n)^* \qquad \text{(atoms)}$$

where $I, I_1, \ldots, I_n$ range over $\mathrm{Idl}(X)$

Effectivity

- represent canonical decompositions $D = I_1 \sqcup \cdots \sqcup I_k$ where the I_j's are maximal for inclusion
- must allow effective operations over ideals: $I \subseteq J$, $I \cap J$, $I \setminus \uparrow x$ for $x \in X$
- Finkel and Goubault-Larrecq (2009, 2012): effective representations exist for all the wqos in this talk
- for Cartesian products: $\mathrm{Idl}(A \times B) = \{I \times J \mid I \in \mathrm{Idl}(A) \text{ and } J \in \mathrm{Idl}(B)\}$
- for finite sequences: $\mathrm{Idl}(X^*)$ are products defined by:

$$P ::= \varepsilon \mid A \cdot P \qquad \text{(products)}$$
$$A ::= (I + \varepsilon) \mid (I_1 \sqcup \cdots \sqcup I_n)^* \qquad \text{(atoms)}$$

where $I, I_1, \ldots, I_n$ range over $\mathrm{Idl}(X)$

EFFECTIVITY

- represent canonical decompositions $D = I_1 \sqcup \cdots \sqcup I_k$ where the I_j's are maximal for inclusion
- must allow effective operations over ideals: $I \subseteq J$, $I \cap J$, $I \setminus \uparrow x$ for $x \in X$
- Finkel and Goubault-Larrecq (2009, 2012): effective representations exist for all the wqos in this talk
- for Cartesian products: $\mathrm{Idl}(A \times B) = \{I \times J \mid I \in \mathrm{Idl}(A) \text{ and } J \in \mathrm{Idl}(B)\}$
- for finite sequences: $\mathrm{Idl}(X^*)$ are products defined by:

$$P ::= \varepsilon \mid A \cdot P \qquad \text{(products)}$$

$$A ::= (I + \varepsilon) \mid (I_1 \sqcup \cdots \sqcup I_n)^* \qquad \text{(atoms)}$$

where $I, I_1, \ldots, I_n$ range over $\mathrm{Idl}(X)$

Effectivity

- represent canonical decompositions $D = I_1 \sqcup \cdots \sqcup I_k$ where the I_j's are maximal for inclusion
- must allow effective operations over ideals: $I \subseteq J$, $I \cap J$, $I \setminus \uparrow x$ for $x \in X$
- Finkel and Goubault-Larrecq (2009, 2012): effective representations exist for all the wqos in this talk
- for Cartesian products: $\mathsf{Idl}(A \times B) = \{I \times J \mid I \in \mathsf{Idl}(A) \text{ and } J \in \mathsf{Idl}(B)\}$
- for finite sequences: $\mathsf{Idl}(X^*)$ are products defined by:

$$P ::= \varepsilon \mid A \cdot P \qquad \text{(products)}$$

$$A ::= (I + \varepsilon) \mid (I_1 \sqcup \cdots \sqcup I_n)^* \qquad \text{(atoms)}$$

where $I, I_1, \ldots, I_n$ range over $\mathsf{Idl}(X)$

An Abstraction Refinement Procedure (CEGAR)

Build a sequence $D_0 \supsetneq D_1 \supsetneq \cdots$ of $\downarrow$-closed sets s.t.

$$\forall n\,.\,{\downarrow}\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \subseteq D_n$$

initially $D_0 \stackrel{\text{def}}{=} \mathsf{PreRuns}_{\mathbf{A}}$

$\forall n$
- if $D_n = I \sqcup D$ and $\exists \rho \in I \setminus {\downarrow}\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$,

  $$D_{n+1} \stackrel{\text{def}}{=} D \cup (I \setminus {\uparrow}\rho)$$

- otherwise stop:

  $$D_n = {\downarrow}\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$$

terminates by Descending Chain Property

An Abstraction Refinement Procedure (CEGAR)

Build a sequence $D_0 \supsetneq D_1 \supsetneq \cdots$ of $\downarrow$-closed sets s.t.

$$\forall n\,.\,\downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \subseteq D_n$$

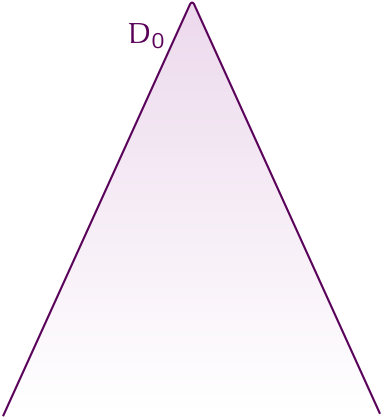
initially $D_0 \stackrel{\text{def}}{=} \mathrm{PreRuns}_{\mathbf{A}}$

$\forall n$
- if $D_n = I \sqcup D$ and $\exists \rho \in I \setminus \downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

  $D_{n+1} \stackrel{\text{def}}{=} D \cup (I \setminus \uparrow\rho)$
- otherwise stop:

  $D_n = \downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

terminates by Descending Chain Property



An Abstraction Refinement Procedure (CEGAR)

Build a sequence $D_0 \supsetneq D_1 \supsetneq \cdots$ of $\downarrow$-closed sets s.t.

$$\forall n \,.\, \downarrow\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \subseteq D_n$$

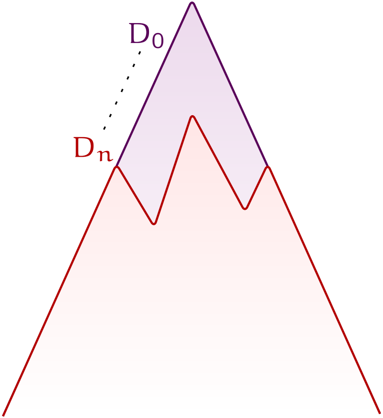
initially $D_0 \stackrel{\text{def}}{=} \mathsf{PreRuns}_{\mathbf{A}}$

$\forall n$
- if $D_n = I \sqcup D$ and $\exists \rho \in I \setminus \downarrow\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$,

  $D_{n+1} \stackrel{\text{def}}{=} D \cup (I \setminus \uparrow\rho)$
- otherwise stop:

  $D_n = \downarrow\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

terminates by Descending Chain Property



An Abstraction Refinement Procedure (CEGAR)

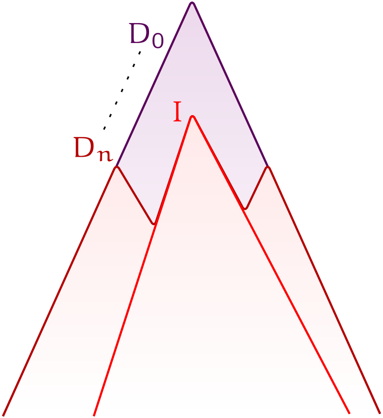
Build a sequence $D_0 \supsetneq D_1 \supsetneq \cdots$ of $\downarrow$-closed sets s.t.

$$\forall n \,.\, \downarrow\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \subseteq D_n$$

initially $D_0 \stackrel{\text{def}}{=} \mathsf{PreRuns}_{\mathbf{A}}$

$\forall n$
- if $D_n = I \sqcup D$ and $\exists \rho \in I \setminus \downarrow\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$, $D_{n+1} \stackrel{\text{def}}{=} D \cup (I \setminus \uparrow\rho)$
- otherwise stop: $D_n = \downarrow\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

terminates by Descending Chain Property



An Abstraction Refinement Procedure (CEGAR)

Build a sequence $D_0 \supsetneq D_1 \supsetneq \cdots$ of $\downarrow$-closed sets s.t.

$$\forall n \,.\, \downarrow \mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \subseteq D_n$$

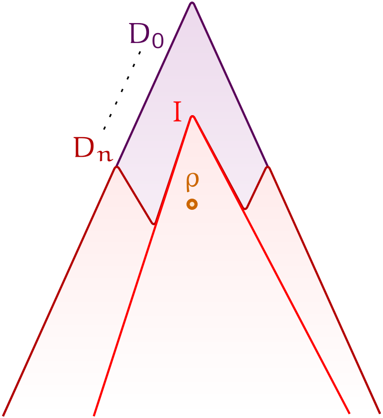
initially $D_0 \stackrel{\text{def}}{=} \mathsf{PreRuns}_{\mathbf{A}}$

$\forall n$
- if $D_n = I \sqcup D$ and $\exists \rho \in I \setminus \downarrow \mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$,

  $D_{n+1} \stackrel{\text{def}}{=} D \cup (I \setminus \uparrow \rho)$
- otherwise stop:

  $D_n = \downarrow \mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

terminates by Descending Chain Property



An Abstraction Refinement Procedure (CEGAR)

Build a sequence $D_0 \supsetneq D_1 \supsetneq \cdots$ of $\downarrow$-closed sets s.t.

$$\forall n \,.\, \downarrow\mathsf{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y}) \subseteq D_n$$

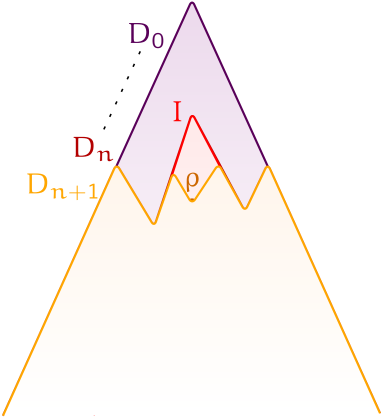
initially $D_0 \stackrel{\text{def}}{=} \mathsf{PreRuns}_{\mathbf{A}}$

$\forall n$
- if $D_n = I \sqcup D$ and $\exists \rho \in I \setminus \downarrow\mathsf{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$,

  $D_{n+1} \stackrel{\text{def}}{=} D \cup (I \setminus \uparrow\rho)$
- otherwise stop:

  $D_n = \downarrow\mathsf{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$

terminates by Descending Chain Property



An Abstraction Refinement Procedure (CEGAR)

Build a sequence $D_0 \supsetneq D_1 \supsetneq \cdots$ of $\downarrow$-closed sets s.t.

$$\forall n\,.\,\downarrow\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \subseteq D_n$$

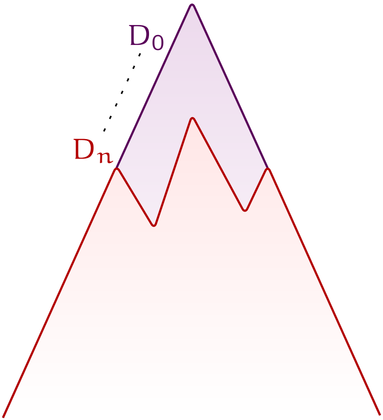
initially $D_0 \stackrel{\text{def}}{=} \mathsf{PreRuns}_{\mathbf{A}}$

$\forall n$
- if $D_n = I \sqcup D$ and $\exists \rho \in I \setminus \downarrow\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$,

  $D_{n+1} \stackrel{\text{def}}{=} D \cup (I \setminus \uparrow\rho)$
- otherwise stop:

  $D_n = \downarrow\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

terminates by Descending Chain Property



An Abstraction Refinement Procedure (CEGAR)

Build a sequence $D_0 \supsetneq D_1 \supsetneq \cdots$ of $\downarrow$-closed sets s.t.

$$\forall n \,.\, \downarrow\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \subseteq D_n$$

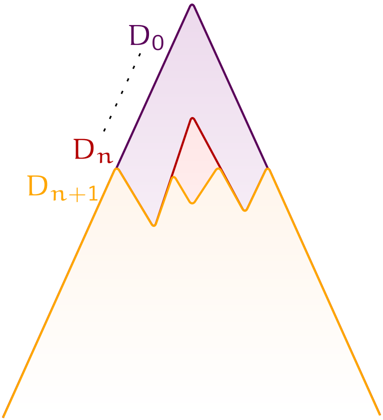
initially $D_0 \stackrel{\text{def}}{=} \mathsf{PreRuns}_{\mathbf{A}}$

$\forall n$
- if $D_n = I \sqcup D$ and $\exists \rho \in I \setminus \downarrow\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$,

  $D_{n+1} \stackrel{\text{def}}{=} D \cup (I \setminus \uparrow\rho)$
- otherwise stop:

  $D_n = \downarrow\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

terminates by Descending Chain Property



Containment Oracles

Ideal Containment (into VAS Runs) Problem

input $\mathbf{A} \subseteq_{\text{fin}} \mathbb{Z}^d$, $\mathbf{x}, \mathbf{y} \in \mathbb{N}^d$, $I \in \mathsf{Idl}(\mathsf{PreRuns}_{\mathbf{A}})$

question $\exists \rho \in I \setminus \downarrow \mathsf{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$?

Proposition

VAS Reachability reduces to Ideal Containment.

Proof.
Because $\downarrow(\mathbf{0}, \varepsilon, \mathbf{0}) \subseteq \downarrow \mathsf{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$ iff $\mathsf{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y}) \neq \emptyset$. □

Proposition

Ideal Containment is decidable.

Proof.
Consequence of the Decomposition Theorem. □

Containment Oracles

Ideal Containment (into VAS Runs) Problem

input $\mathbf{A} \subseteq_{\text{fin}} \mathbb{Z}^d, \mathbf{x}, \mathbf{y} \in \mathbb{N}^d, I \in \mathsf{Idl}(\mathsf{PreRuns}_{\mathbf{A}})$

question Is $I \subseteq \downarrow \mathsf{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$?

Proposition

VAS Reachability reduces to Ideal Containment.

Proof.

Because $\downarrow(\mathbf{0}, \varepsilon, \mathbf{0}) \subseteq \downarrow \mathsf{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$ iff $\mathsf{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y}) \neq \emptyset$. □

Proposition

Ideal Containment is decidable.

Proof.

Consequence of the Decomposition Theorem. □

Containment Oracles

Ideal Containment (into VAS Runs) Problem

input $\mathbf{A} \subseteq_{\text{fin}} \mathbb{Z}^d$, $\mathbf{x},\mathbf{y} \in \mathbb{N}^d$, $I \in \mathsf{Idl}(\mathsf{PreRuns}_{\mathbf{A}})$

question Is $I \subseteq {\downarrow}\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$?

Proposition

VAS Reachability reduces to Ideal Containment.

Proof.

Because ${\downarrow}(\mathbf{0},\varepsilon,\mathbf{0}) \subseteq {\downarrow}\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$ iff $\mathsf{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) \neq \emptyset$. □

Proposition

Ideal Containment is decidable.

Proof.

Consequence of the Decomposition Theorem. □

Containment Oracles

Ideal Containment (into VAS Runs) Problem

input $\mathbf{A} \subseteq_{\text{fin}} \mathbb{Z}^d, \mathbf{x}, \mathbf{y} \in \mathbb{N}^d, I \in \mathsf{Idl}(\mathsf{PreRuns}_{\mathbf{A}})$

question Is $I \subseteq {\downarrow}\mathsf{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$?

Proposition

VAS Reachability reduces to Ideal Containment.

Proof.

Because ${\downarrow}(\mathbf{0}, \varepsilon, \mathbf{0}) \subseteq {\downarrow}\mathsf{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$ iff $\mathsf{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y}) \neq \emptyset$. □

Proposition

Ideal Containment is decidable.

Proof.

Consequence of the Decomposition Theorem. □

Adherence Oracles

Adherence (of VAS Runs) Membership Problem

input $\mathbf{A} \subseteq_{\mathrm{fin}} \mathbb{Z}^{d}, \mathbf{x}, \mathbf{y} \in \mathbb{N}^{d}, I \in \mathrm{Idl}(\mathrm{PreRuns}_{\mathbf{A}})$

question $\exists \Delta \subseteq \mathrm{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$ directed s.t. $\downarrow\Delta = I$?

Claim
In the context of the CEGAR procedure, containment checks are equivalent to adherence membership checks.

Theorem
Adherence Membership is undecidable.

Proof Idea.
By a reduction from Boundedness in Lossy Counter Machines. □

Adherence Oracles

Adherence (of VAS Runs) Membership Problem

input $\mathbf{A} \subseteq_{\text{fin}} \mathbb{Z}^{d}, \mathbf{x}, \mathbf{y} \in \mathbb{N}^{d}, I \in \mathsf{Idl}(\mathsf{PreRuns}_{\mathbf{A}})$

question $\exists \Delta \subseteq \mathsf{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$ directed s.t. $\downarrow\Delta = I$?

Claim

In the context of the CEGAR procedure, containment checks are equivalent to adherence membership checks.

Theorem

Adherence Membership is undecidable.

Proof Idea.

By a reduction from Boundedness in Lossy Counter Machines. $\square$

How to Salvage the CEGAR Procedure?

- both containment and adherence miss a crucial point: if $\downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = D_n = I \sqcup D$, then I is some maximal ideal of $\downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

- find 'nice' invariants of such ideals:

  initially $D_0 \stackrel{\text{def}}{=} \mathrm{PreRuns}_{\mathbf{A}}$ is nice

  $\forall n$
  - if $D_n = I \sqcup D$ and $\exists\rho \in I \setminus \downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$,

    $D_{n+1} \stackrel{\text{def}}{=} D \cup (I \setminus \uparrow\rho)$
  - otherwise stop:

    $D_n = \downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

- template for the KLMST decomposition algorithm

How to Salvage the CEGAR Procedure?

- both containment and adherence miss a crucial point: if $\downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = D_n = I \sqcup D$, then I is some maximal ideal of $\downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

- find 'nice' invariants of such ideals:

  initially $D_0 \stackrel{\text{def}}{=} \mathrm{PreRuns}_{\mathbf{A}}$ is nice

  $\forall n$
  - if $D_n = I \sqcup D$ and $\exists \rho \in I \setminus \downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$, which is decidable,

    $D_{n+1} \stackrel{\text{def}}{=} D \cup (I \setminus \uparrow\rho)$ is nice
  - otherwise stop:

    $D_n = \downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

- template for the KLMST decomposition algorithm

How to Salvage the CEGAR Procedure?

- both containment and adherence miss a crucial point: if $\downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = D_n = I \sqcup D$, then I is some maximal ideal of $\downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

- find 'nice' invariants of such ideals:

  initially $D_0 \stackrel{\text{def}}{=} \mathrm{PreRuns}_{\mathbf{A}}$ is nice

  $\forall n$
  - if $D_n = I \sqcup D$ and $\exists \rho \in I \setminus \downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$, which is decidable,

    $D_{n+1} \stackrel{\text{def}}{=} D \cup (I \setminus \uparrow\rho)$ is nice
  - otherwise stop:

    $D_n = \downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

- template for the KLMST decomposition algorithm

How to Salvage the CEGAR Procedure?

- both containment and adherence miss a crucial point: if $\downarrow\text{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = D_n = I \sqcup D$, then I is some maximal ideal of $\downarrow\text{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$
- find 'nice' invariants of such ideals:

  initially $D_0 \stackrel{\text{def}}{=} \text{PreRuns}_{\mathbf{A}}$ is nice

  $\forall n$
  - if $D_n = I \sqcup D$ and $\exists \rho \in I \setminus \downarrow\text{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$, which is decidable,

    $D_{n+1} \stackrel{\text{def}}{=} D \cup (I \setminus \uparrow\rho)$ is nice
  - otherwise stop:

    $D_n = \downarrow\text{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$
- template for the KLMST decomposition algorithm

How to Salvage the CEGAR Procedure?

- both containment and adherence miss a crucial point: if $\downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = D_n = I \sqcup D$, then I is some maximal ideal of $\downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

- find 'nice' invariants of such ideals:

  initially $D_0 \stackrel{\text{def}}{=} \mathrm{PreRuns}_{\mathbf{A}}$ is nice

  $\forall n$
  - if $D_n = I \sqcup D$ and $\exists \rho \in I \setminus \downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$, which is decidable,

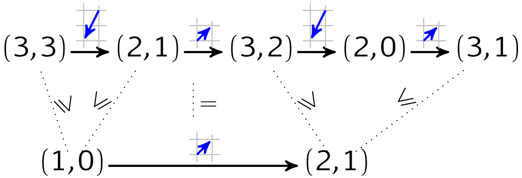
    $D_{n+1} \stackrel{\text{def}}{=} D \cup (I \setminus \uparrow\rho)$ is nice

  - otherwise stop:

    $D_n = \downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

- template for the KLMST decomposition algorithm

Run Embeddings



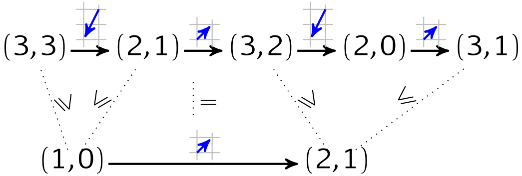
Fix $\rho = \mathbf{c}_0 \xrightarrow{\mathbf{a}_1} \mathbf{c}_1 \cdots \mathbf{c}_{k-1} \xrightarrow{\mathbf{a}_k} \mathbf{c}_k$ from $\text{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$
If $\rho' \trianglerighteq \rho$ is a run, $\exists \mathbf{v}_0, \ldots, \mathbf{v}_{k+1} \in \mathbb{N}^d$ and $\sigma_0, \ldots, \sigma_k \in \mathbf{A}^*$:

$$\rho' = (\mathbf{v}_0 + \mathbf{c}_0) \xrightarrow{\sigma_0} (\mathbf{v}_1 + \mathbf{c}_0) \xrightarrow{\mathbf{a}_1} (\mathbf{v}_1 + \mathbf{c}_1) \cdots (\mathbf{v}_k + \mathbf{c}_{k-1}) \xrightarrow{\mathbf{a}_k} (\mathbf{v}_k + \mathbf{c}_k) \xrightarrow{\sigma_k} (\mathbf{v}_{k+1} + \mathbf{c}_k)$$

Lemma (Run Amalgamation)

If $\rho \trianglelefteq \rho_1, \rho_2$ are runs, then there exists a run $\rho' \trianglerighteq \rho_1, \rho_2$.

Run Embeddings



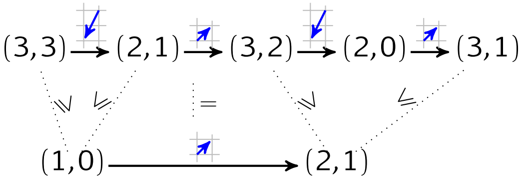
Fix $\rho = \mathbf{c}_0 \xrightarrow{\mathbf{a}_1} \mathbf{c}_1 \cdots \mathbf{c}_{k-1} \xrightarrow{\mathbf{a}_k} \mathbf{c}_k$ from $\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$
If $\rho' \trianglerighteq \rho$ is a run, $\exists \mathbf{v}_0,\ldots,\mathbf{v}_{k+1} \in \mathbb{N}^d$ and $\sigma_0,\ldots,\sigma_k \in \mathbf{A}^*$:

$$\rho' = (\mathbf{v}_0+\mathbf{c}_0) \xrightarrow{\sigma_0} (\mathbf{v}_1+\mathbf{c}_0) \xrightarrow{\mathbf{a}_1} (\mathbf{v}_1+\mathbf{c}_1) \cdots (\mathbf{v}_k+\mathbf{c}_{k-1}) \xrightarrow{\mathbf{a}_k} (\mathbf{v}_k+\mathbf{c}_k) \xrightarrow{\sigma_k} (\mathbf{v}_{k+1}+\mathbf{c}_k)$$

Lemma (Run Amalgamation)

If $\rho \trianglelefteq \rho_1, \rho_2$ are runs, then there exists a run $\rho' \trianglerighteq \rho_1, \rho_2$.

Run Embeddings



Fix $\rho = \mathbf{c}_0 \xrightarrow{\mathbf{a}_1} \mathbf{c}_1 \cdots \mathbf{c}_{k-1} \xrightarrow{\mathbf{a}_k} \mathbf{c}_k$ from $\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$
If $\rho' \trianglerighteq \rho$ is a run, $\exists \mathbf{v}_0,\ldots,\mathbf{v}_{k+1} \in \mathbb{N}^d$ and $\sigma_0,\ldots,\sigma_k \in \mathbf{A}^*$:

$$\rho' = (\mathbf{v}_0+\mathbf{c}_0) \xrightarrow{\sigma_0} (\mathbf{v}_1+\mathbf{c}_0) \xrightarrow{\mathbf{a}_1} (\mathbf{v}_1+\mathbf{c}_1) \cdots (\mathbf{v}_k+\mathbf{c}_{k-1}) \xrightarrow{\mathbf{a}_k} (\mathbf{v}_k+\mathbf{c}_k) \xrightarrow{\sigma_k} (\mathbf{v}_{k+1}+\mathbf{c}_k)$$

Lemma (Run Amalgamation)

If $\rho \trianglelefteq \rho_1,\rho_2$ are runs, then there exists a run $\rho' \trianglerighteq \rho_1,\rho_2$.

Maximal Run Ideals (1/2)

Since $\trianglelefteq$ is a wqo, $B \stackrel{\text{def}}{=} \min_{\trianglelefteq} \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$ is finite:

$$\downarrow \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = \bigcup_{\rho \in B} \downarrow(\uparrow\rho \cap \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}))$$

For any run ρ, $\downarrow(\uparrow\rho \cap \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}))$ is

- non-empty: it contains at least ρ
- directed by run amalgamation
- downward-closed by definition

Proposition

The maximal ideals of $\downarrow \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$ are the ideals of the form $\downarrow(\uparrow\rho \cap \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}))$ for $\rho \in \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$.

Maximal Run Ideals (1/2)

Since $\trianglelefteq$ is a wqo, $B \stackrel{\text{def}}{=} \min_{\trianglelefteq} \text{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$ is finite:

$$\downarrow \text{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y}) = \bigcup_{\rho \in B} \downarrow(\uparrow \rho \cap \text{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y}))$$

For any run ρ, $\downarrow(\uparrow \rho \cap \text{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y}))$ is

- non-empty: it contains at least ρ
- directed by run amalgamation
- downward-closed by definition

Proposition

The maximal ideals of $\downarrow \text{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$ are the ideals of the form $\downarrow(\uparrow \rho \cap \text{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y}))$ for $\rho \in \text{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$.

Maximal Run Ideals (1/2)

Since $\trianglelefteq$ is a wqo, $B \stackrel{\text{def}}{=} \min_{\trianglelefteq} \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$ is finite:

$$\downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = \bigcup_{\rho\in B} \downarrow(\uparrow\rho \cap \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}))$$

For any run ρ, $\downarrow(\uparrow\rho \cap \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}))$ is

- non-empty: it contains at least ρ
- directed by run amalgamation
- downward-closed by definition

Proposition

The maximal ideals of $\downarrow\mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$ are the ideals of the form $\downarrow(\uparrow\rho \cap \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}))$ for $\rho \in \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$.

Maximal Run Ideals (1/2)

Since $\trianglelefteq$ is a wqo, $B \stackrel{\text{def}}{=} \min_{\trianglelefteq} \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$ is finite:

$$\downarrow \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = \bigcup_{\rho \in B} \downarrow(\uparrow \rho \cap \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}))$$

For any run ρ, $\downarrow(\uparrow \rho \cap \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}))$ is

- non-empty: it contains at least ρ
- directed by run amalgamation
- downward-closed by definition

Proposition

The maximal ideals of $\downarrow \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$ are the ideals of the form $\downarrow(\uparrow \rho \cap \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}))$ for $\rho \in \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$.

Maximal Run Ideals (2/2)

Transformer Relations

- $\overset{\mathbf{c}}{\curvearrowright} \overset{\text{def}}{=} \{(\mathbf{u},\mathbf{v}) \mid \exists\sigma \in \mathbf{A}^* \,.\, \mathbf{u}+\mathbf{c} \xrightarrow{\sigma} \mathbf{v}+\mathbf{c}\}$
- $\overset{\mathbf{c}}{\curvearrowright}$ is periodic: it contains $\mathbf{0}$, and if $\mathbf{u} \overset{\mathbf{c}}{\curvearrowright} \mathbf{v}$ and $\mathbf{u}' \overset{\mathbf{c}}{\curvearrowright} \mathbf{v}'$, then $\mathbf{u}+\mathbf{u}' \overset{\mathbf{c}}{\curvearrowright} \mathbf{v}+\mathbf{v}'$

Decomposition of $\uparrow\rho \cap \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

- let $\rho = \mathbf{c}_0 \xrightarrow{\mathbf{a}_1} \mathbf{c}_1 \cdots \mathbf{c}_{k-1} \xrightarrow{\mathbf{a}_k} \mathbf{c}_k$
- consider all the $(k+1)$-tuples $(\mathbf{v}_0,\mathbf{v}_1),(\mathbf{v}_1,\mathbf{v}_2),\ldots,(\mathbf{v}_{k-1},\mathbf{v}_k)$ s.t. $\mathbf{v}_0 \overset{\mathbf{c}_0}{\curvearrowright} \mathbf{v}_1 \overset{\mathbf{c}_1}{\curvearrowright} \cdots \overset{\mathbf{c}_k}{\curvearrowright} \mathbf{v}_k$
  every projection $\mathbf{P}_j \overset{\text{def}}{=} \{(\mathbf{v}_j,\mathbf{v}_{j+1}) \mid \ldots\}$ is also periodic
- define Ω_j as the set of runs $\mathbf{v}_j+\mathbf{c}_j \xrightarrow{\sigma_j} \mathbf{v}_{j+1}+\mathbf{c}_j$ for each j

Maximal Run Ideals (2/2)

Transformer Relations

- $\overset{\mathbf{c}}{\curvearrowright} \overset{\text{def}}{=} \{(\mathbf{u},\mathbf{v}) \mid \exists \sigma \in \mathbf{A}^* \,.\, \mathbf{u}+\mathbf{c} \xrightarrow{\sigma} \mathbf{v}+\mathbf{c}\}$
- $\overset{\mathbf{c}}{\curvearrowright}$ is periodic: it contains $\mathbf{0}$, and if $\mathbf{u} \overset{\mathbf{c}}{\curvearrowright} \mathbf{v}$ and $\mathbf{u}' \overset{\mathbf{c}}{\curvearrowright} \mathbf{v}'$, then $\mathbf{u}+\mathbf{u}' \overset{\mathbf{c}}{\curvearrowright} \mathbf{v}+\mathbf{v}'$

Decomposition of $\uparrow\rho \cap \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$

- let $\rho = \mathbf{c}_0 \xrightarrow{\mathbf{a}_1} \mathbf{c}_1 \cdots \mathbf{c}_{k-1} \xrightarrow{\mathbf{a}_k} \mathbf{c}_k$
- consider all the $(k+1)$-tuples $(\mathbf{v}_0,\mathbf{v}_1),(\mathbf{v}_1,\mathbf{v}_2),\ldots,(\mathbf{v}_{k-1},\mathbf{v}_k)$ s.t. $\mathbf{v}_0 \overset{\mathbf{c}_0}{\curvearrowright} \mathbf{v}_1 \overset{\mathbf{c}_1}{\curvearrowright} \cdots \overset{\mathbf{c}_k}{\curvearrowright} \mathbf{v}_k$ every projection $\mathbf{P}_j \overset{\text{def}}{=} \{(\mathbf{v}_j,\mathbf{v}_{j+1}) \mid \ldots\}$ is also periodic
- define Ω_j as the set of runs $\mathbf{v}_j+\mathbf{c}_j \xrightarrow{\sigma_j} \mathbf{v}_{j+1}+\mathbf{c}_j$ for each j

Marked Witness Graphs

Example

$$\mathbf{A} = \{\mathbf{a}, \mathbf{b}\} \text{ where } \mathbf{a} = (1,1,-1) \qquad \mathbf{b} = (-1,0,1)$$

$$\mathbf{c}_j = (1,0,1) \qquad \mathbf{P}_j = \{((0,0,0),(0,n,0)) \mid n \in \mathbb{N}\}$$

$$\Omega_j = \{\mathbf{c}_j \xrightarrow{w_1 \cdots w_n} \mathbf{c}_j + (0,n,0) \mid n \in \mathbb{N}, w_i \in \{\mathbf{ab}, \mathbf{ba}\}\}$$

$$\begin{tikzcd}
& (1,0,1) \arrow[dl, "\mathbf{a}"'] \arrow[dr, "\mathbf{b}"] & \\
(2,1,0) \arrow[dr, "\mathbf{b}"'] & & (0,0,2) \arrow[dl, "\mathbf{a}"] \\
& (1,1,1) & \\
& \vdots & \\
& (1,n-1,1) \arrow[dl, "\mathbf{a}"'] \arrow[dr, "\mathbf{b}"] & \\
(2,n,0) \arrow[dr, "\mathbf{b}"'] & & (0,n-1,2) \arrow[dl, "\mathbf{a}"] \\
& (1,n,1) &
\end{tikzcd}$$

Marked Witness Graphs

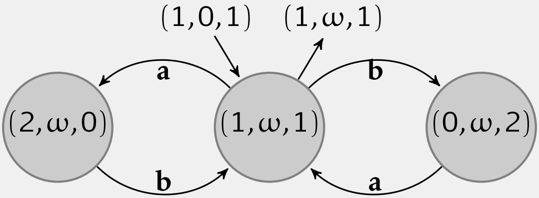
Each Ω_j can be represented as a finite marked witness graph M_j.

Example

$$\mathbf{A} = \{\mathbf{a}, \mathbf{b}\} \text{ where } \mathbf{a} = (1,1,-1) \qquad \mathbf{b} = (-1,0,1)$$

$$\mathbf{c}_j = (1,0,1) \qquad \mathbf{P}_j = \{((0,0,0),(0,n,0)) \mid n \in \mathbb{N}\}$$

$$\Omega_j = \{\mathbf{c}_j \xrightarrow{w_1 \cdots w_n} \mathbf{c}_j + (0,n,0) \mid n \in \mathbb{N}, w_i \in \{\mathbf{ab}, \mathbf{ba}\}\}$$



Marked Witness Graph Sequences

Back to $\rho = \mathbf{c}_0 \xrightarrow{\mathbf{a}_1} \mathbf{c}_1 \cdots \mathbf{c}_{k-1} \xrightarrow{\mathbf{a}_k} \mathbf{c}_k$:

- $\uparrow\rho \cap \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$ can be represented using a sequence of marked witness graphs and actions from $\mathbf{A}$:

$$\xi = M_0, \mathbf{a}_1, M_1, \ldots, \mathbf{a}_k, M_k$$

- conversely, each such sequence defines an associated set of runs Ω_ξ and an associated prerun ideal I_ξ.
- conditions on such sequences:
  - consistent markings (Mayr, 1981)
  - θ condition (Kosaraju, 1982)
  - perfectness condition (Lambert, 1992)

Lemma (Perfectness implies Adherence Membership)

If ξ is perfect then $I_\xi = \downarrow\Omega_\xi$.

Marked Witness Graph Sequences

Back to $\rho = \mathbf{c}_0 \xrightarrow{\mathbf{a}_1} \mathbf{c}_1 \cdots \mathbf{c}_{k-1} \xrightarrow{\mathbf{a}_k} \mathbf{c}_k$:

- $\uparrow\rho \cap \mathrm{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$ can be represented using a sequence of marked witness graphs and actions from $\mathbf{A}$:

$$\xi = M_0, \mathbf{a}_1, M_1, \ldots, \mathbf{a}_k, M_k$$

- conversely, each such sequence defines an associated set of runs Ω_ξ and an associated prerun ideal I_ξ.
- conditions on such sequences:
  - consistent markings (Mayr, 1981)
  - θ condition (Kosaraju, 1982)
  - perfectness condition (Lambert, 1992)

Lemma (Perfectness implies Adherence Membership)

If ξ is perfect then $I_\xi = \downarrow\Omega_\xi$.

Marked Witness Graph Sequences

Back to $\rho = \mathbf{c}_0 \xrightarrow{\mathbf{a}_1} \mathbf{c}_1 \cdots \mathbf{c}_{k-1} \xrightarrow{\mathbf{a}_k} \mathbf{c}_k$:

- $\uparrow\rho \cap \text{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y})$ can be represented using a sequence of marked witness graphs and actions from $\mathbf{A}$:

$$\xi = M_0, \mathbf{a}_1, M_1, \ldots, \mathbf{a}_k, M_k$$

- conversely, each such sequence defines an associated set of runs Ω_ξ and an associated prerun ideal I_ξ.
- perfectness condition on such sequences

Lemma (Perfectness implies Adherence Membership)

If ξ is perfect then $I_\xi = \downarrow\Omega_\xi$.

Theorem

There exists a finite set Ξ of perfect marked witness graph sequences s.t. $\downarrow\text{Runs}_{\mathbf{A}}(\mathbf{x},\mathbf{y}) = \bigcup_{\xi\in\Xi} I_\xi$.

KLMST Algorithm (schematically)

Construct a sequence $\Xi_0, \Xi_1, \ldots$ of finite sets of marked witness graph sequences with $\forall n$

$$D_n \stackrel{\text{def}}{=} \bigcup_{\xi \in \Xi_n} I_\xi \supseteq \downarrow \mathrm{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$$

initially Ξ_0 is s.t. $D_0 = \mathrm{PreRuns}_{\mathbf{A}}$

$\forall n$
- if $\Xi_n = \{\xi\} \uplus \Xi$ and ξ is not perfect, which is decidable:

  $$\Xi_{n+1} \stackrel{\text{def}}{=} \Xi \cup (\mathrm{decompose}(\xi))$$

- otherwise stop:

  $$D_n = \downarrow \mathrm{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$$

terminates via a ranking function argument

KLMST Algorithm (schematically)

Construct a sequence $\Xi_0, \Xi_1, \ldots$ of finite sets of marked witness graph sequences with $\forall n$

$$D_n \stackrel{\text{def}}{=} \bigcup_{\xi \in \Xi_n} I_\xi \supseteq {\downarrow}\mathrm{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$$

initially Ξ_0 is s.t. $D_0 = \mathrm{PreRuns}_{\mathbf{A}}$

$\forall n$

- if $\Xi_n = \{\xi\} \uplus \Xi$ and ξ is not perfect, which is decidable:

  $$\Xi_{n+1} \stackrel{\text{def}}{=} \Xi \cup (\mathrm{decompose}(\xi))$$

- otherwise stop:

  $$D_n = {\downarrow}\mathrm{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$$

terminates via a ranking function argument

KLMST Algorithm (schematically)

Construct a sequence $\Xi_0, \Xi_1, \ldots$ of finite sets of marked witness graph sequences with $\forall n$

$$D_n \stackrel{\text{def}}{=} \bigcup_{\xi \in \Xi_n} I_\xi \supseteq {\downarrow}\mathrm{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$$

initially Ξ_0 is s.t. $D_0 = \mathrm{PreRuns}_{\mathbf{A}}$

$\forall n$

- if $\Xi_n = \{\xi\} \uplus \Xi$ and ξ is not perfect, which is decidable,

  $$\Xi_{n+1} \stackrel{\text{def}}{=} \Xi \cup (\mathrm{decompose}(\xi))$$

- otherwise stop:

  $$D_n = {\downarrow}\mathrm{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$$

terminates via a ranking function argument

KLMST ALGORITHM (SCHEMATICALLY)

Construct a sequence $\Xi_0, \Xi_1, \dots$ of finite sets of marked witness graph sequences with $\forall n$

$$D_n \stackrel{\text{def}}{=} \bigcup_{\xi \in \Xi_n} I_\xi \supseteq {\downarrow}\mathrm{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$$

initially Ξ_0 is s.t. $D_0 = \mathrm{PreRuns}_{\mathbf{A}}$

$\forall n$

- if $\Xi_n = \{\xi\} \uplus \Xi$ and ξ is not perfect, which is decidable,

  $$\Xi_{n+1} \stackrel{\text{def}}{=} \Xi \cup (\mathrm{decompose}(\xi))$$

- otherwise stop:

  $$D_n = {\downarrow}\mathrm{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$$

terminates via a ranking function argument

KLMST Algorithm (schematically)

Construct a sequence $\Xi_0, \Xi_1, \ldots$ of finite sets of marked witness graph sequences with $\forall n$

$$D_n \stackrel{\text{def}}{=} \bigcup_{\xi \in \Xi_n} I_\xi \supseteq {\downarrow}\mathsf{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$$

initially Ξ_0 is s.t. $D_0 = \mathsf{PreRuns}_{\mathbf{A}}$

$\forall n$
- if $\Xi_n = \{\xi\} \uplus \Xi$ and ξ is not perfect, which is decidable,

  $$\Xi_{n+1} \stackrel{\text{def}}{=} \Xi \cup (\mathrm{decompose}(\xi))$$

- otherwise stop:

  $$D_n = {\downarrow}\mathsf{Runs}_{\mathbf{A}}(\mathbf{x}, \mathbf{y})$$

terminates via a ranking function argument

Concluding Remarks

- ideals as an algorithmic tool to work with downward-closed sets
- new understanding of the KLMST decomposition
  extension to other models (BVASS, PDVAS,...)?
- complexity of VAS Reachability :
  - PSpace-complete with states if $d = 2$ (Blondin et al., 2015)
  - ExpSpace-hard (Lipton, 1976) and in $\mathbf{F}_{\omega^3}$ (Leroux and S., 2015) in general
- to learn more: references in the next slide and *http://arxiv.org/abs/1503.00745* (Leroux and S., 2015)

CONCLUDING REMARKS

- ideals as an algorithmic tool to work with downward-closed sets
- new understanding of the KLMST decomposition extension to other models (BVASS, PDVAS,...)?
- complexity of VAS Reachability :
  - PSPACE-complete with states if $d = 2$ (Blondin et al., 2015)
  - EXPSPACE-hard (Lipton, 1976) and in $\mathbf{F}_{\omega^3}$ (Leroux and S., 2015) in general
- to learn more: references in the next slide and *http://arxiv.org/abs/1503.00745* (Leroux and S., 2015)

Concluding Remarks

- ideals as an algorithmic tool to work with downward-closed sets
- new understanding of the KLMST decomposition
  extension to other models (BVASS, PDVAS,...)?
- complexity of VAS Reachability :
  - PSpace-complete with states if $d = 2$ (Blondin et al., 2015)
  - ExpSpace-hard (Lipton, 1976) and in $\mathbf{F}_{\omega^3}$ (Leroux and S., 2015) in general
- to learn more: references in the next slide and *http://arxiv.org/abs/1503.00745* (Leroux and S., 2015)

Concluding Remarks

- ideals as an algorithmic tool to work with downward-closed sets
- new understanding of the KLMST decomposition extension to other models (BVASS, PDVAS,…)?
- complexity of VAS Reachability :
  - PSpace-complete with states if $d = 2$ (Blondin et al., 2015)
  - ExpSpace-hard (Lipton, 1976) and in $\mathbf{F}_{\omega^3}$ (Leroux and S., 2015) in general
- to learn more: references in the next slide and *http://arxiv.org/abs/1503.00745* *(Leroux and S., 2015)*

References

Blondin, M., Finkel, A., Göller, S., Haase, C., and McKenzie, P., 2015. Reachability in two-dimensional vector addition systems with states is PSPACE-complete. In *Proc. LICS 2015*, pages 32–43. IEEE Press. doi:10.1109/LICS.2015.14.

Bonnet, R., 1975. On the cardinality of the set of initial intervals of a partially ordered set. In *Infinite and finite sets: to Paul Erdős on his 60th birthday, Vol. 1*, Coll. Math. Soc. János Bolyai, pages 189–198. North-Holland.

Finkel, A. and Goubault-Larrecq, J., 2009. Forward analysis for WSTS, part I: Completions. In *Proc. STACS 2009*, volume 3 of *LIPIcs*, pages 433–444. LZI. doi:10.4230/LIPIcs.STACS.2009.1844.

Finkel, A. and Goubault-Larrecq, J., 2012. Forward analysis for WSTS, part II: Complete WSTS. *Logic. Meth. in Comput. Sci.*, 8(3:28):1–35. doi:10.2168/LMCS-8(3:28)2012.

Jančar, P., 1990. Decidability of a temporal logic problem for Petri nets. *Theor. Comput. Sci.*, 74(1):71–93. doi:10.1016/0304-3975(90)90006-4.

Karp, R.M. and Miller, R.E., 1969. Parallel program schemata. *Journal of Computer and System Sciences*, 3(2): 147–195. doi:10.1016/S0022-0000(69)80011-5.

Kosaraju, S.R., 1982. Decidability of reachability in vector addition systems. In *Proc. STOC'82*, pages 267–281. ACM. doi:10.1145/800070.802201.

Lambert, J.L., 1992. A structure to decide reachability in Petri nets. *Theor. Comput. Sci.*, 99(1):79–104. doi:10.1016/0304-3975(92)90173-D.

Leroux, J., 2011. Vector addition system reachability problem: a short self-contained proof. In *Proc. POPL 2011*, pages 307–316. ACM. doi:10.1145/1926385.1926421.

Leroux, J. and Schmitz, S., 2015. Demystifying reachability in vector addition systems. In *Proc. LICS 2015*, pages 56–67. IEEE Press. doi:10.1109/LICS.2015.16.

Lipton, R., 1976. The reachability problem requires exponential space. Technical Report 62, Yale University. http://cpsc.yale.edu/sites/default/files/files/tr63.pdf.

Mayr, E.W., 1981. An algorithm for the general Petri net reachability problem. In *Proc. STOC'81*, pages 238–246. ACM. doi:10.1145/800076.802477.

Sacerdote, G.S. and Tenney, R.L., 1977. The decidability of the reachability problem for vector addition systems. In *Proc. STOC'77*, pages 61–76. ACM. doi:10.1145/800105.803396.