A Relational Abstraction for Functions

Bertrand Jeannet[1], Thomas Reps[2] and Denis Gopan[2]

1: IRISA/INRIA, Rennes, France

2: University of Madison-Wisconsin, Wisconsin, USA

First International Workshop
on
Numeric and Symbolic Abstract Domains (NSAD'05)
January 21, 2005: Paris, France,

Compositional Design of Abstract Domains

Idea: given $\wp(D_i) \leftrightarrows A_i$, $i = 1, 2$, find an abstract lattice for

- (sets of) relations $R \subseteq D_1 \times D_2$ (eg, $A_1 \times A_2$)
- (sets of) functions $f : D_1 \to D_2$ (eg., $A_1 \to A_2$)

And compose abstractions

Why ?

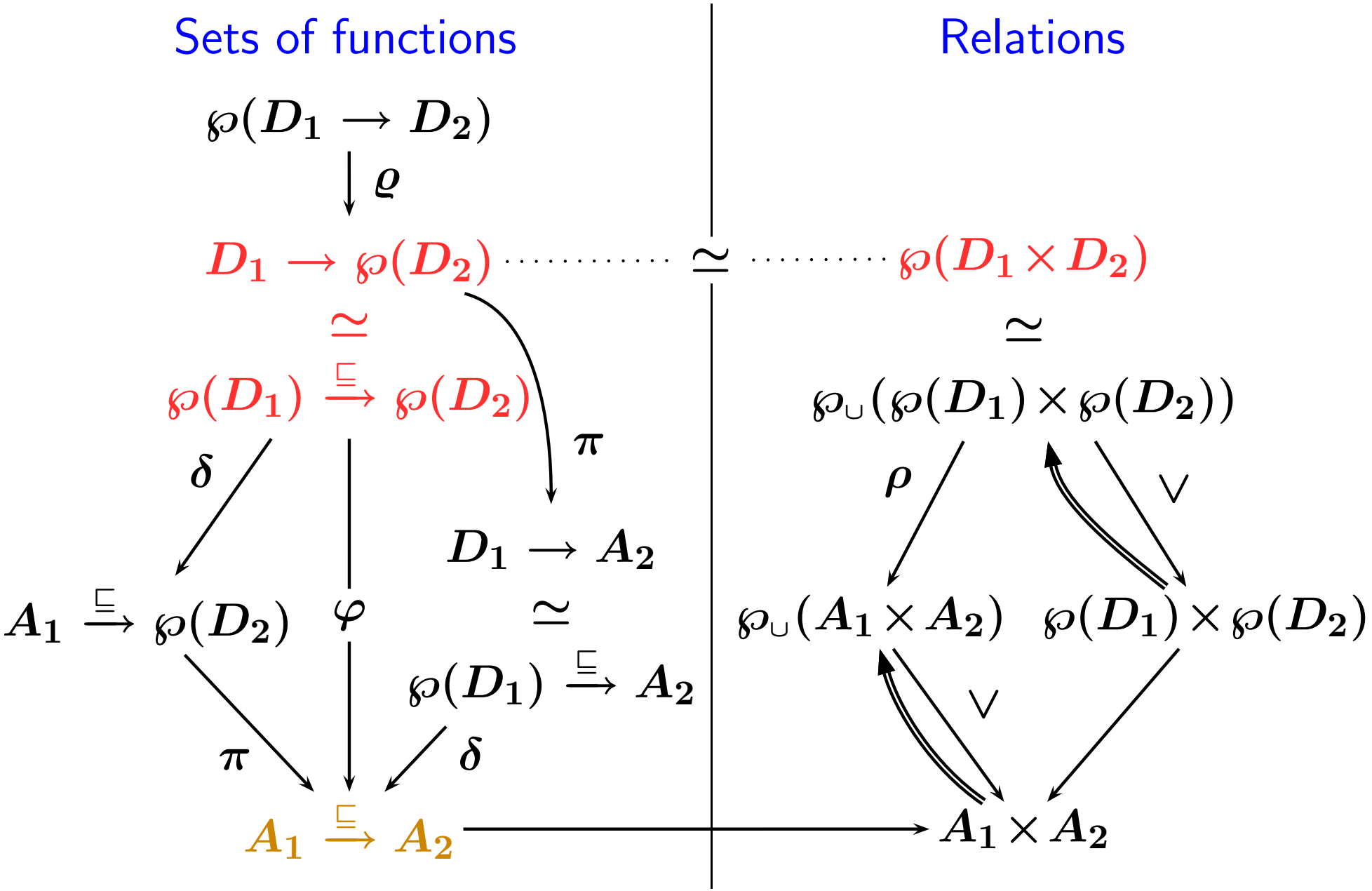
- Structuring complex abstractions (and make them possible)
- Better understanding of the $\neq$ kind of approximations
- Easier comparison of abstract lattices

An important question: The A_i's being finitely representable,
is it so for the composition ?

This talk

- Overview of abstraction for sets of functions
- A more precise, still finitely representable, generic abstract domain for set of functions
- Existing applications: analysis of arrays, shape analysis
- In this talk: focus on semantic aspects (vs algorithmic)

Overview of standard abstractions



Overview of standard abstractions

"Higher-Order Abstract Interpretation (and Application to Comportment Analysis Generalizing Strictness, Termination, Projection and PER Analysis of Functional Languages"
Cousot & Cousot, 1994

Running example (from shape analysis)

$\boldsymbol{U}$: set of (concrete) memory cells

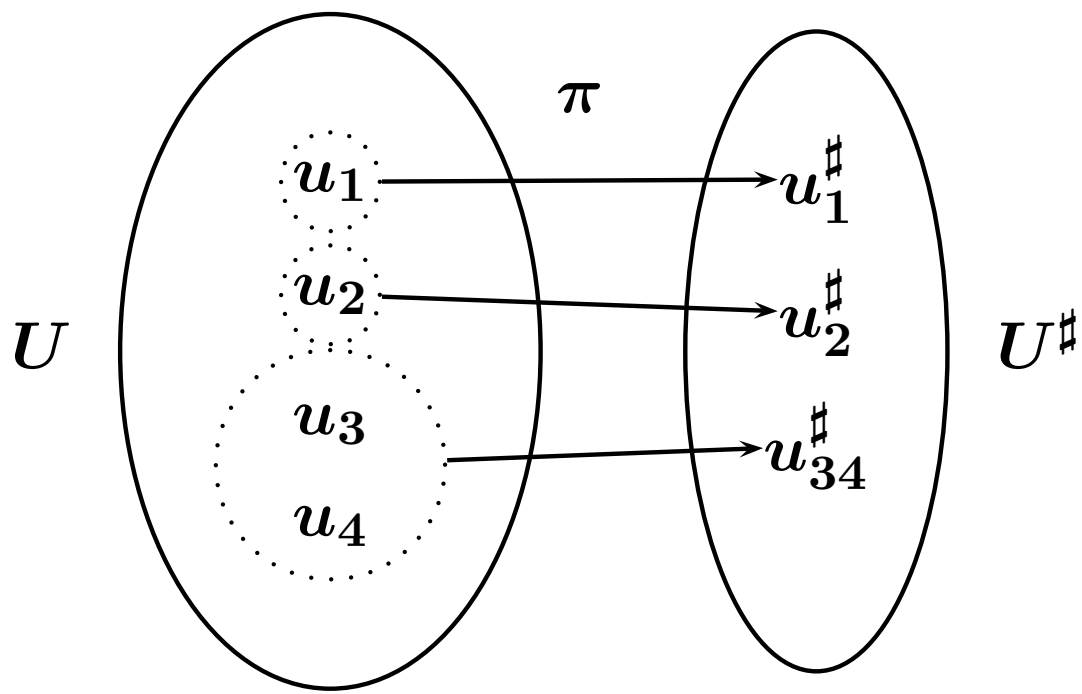
$\boldsymbol{f : U \longrightarrow \mathbb{R}}$: gives the valuation of a real-valued field

Running example (from shape analysis)

U: set of (concrete) memory cells

$f : U \longrightarrow \mathbb{R}$: gives the valuation of a real-valued field

We abstract the domain U by partitioning as follows:



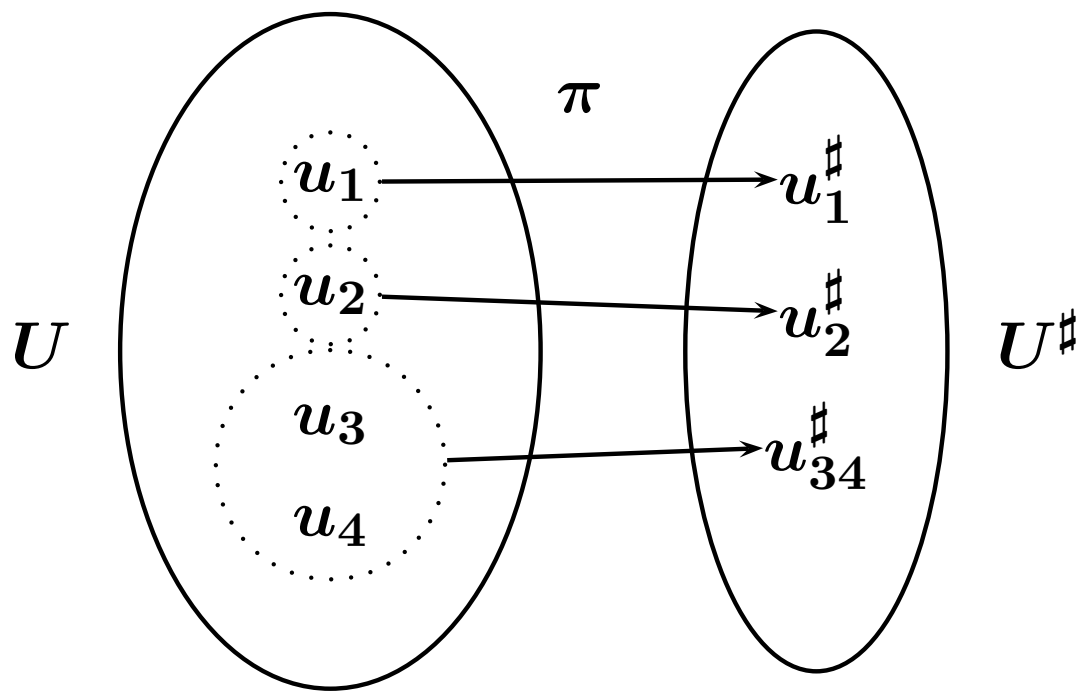
This induces the abstraction $\wp(U) \leftrightarrows U^\sharp_\bot$

Running example (from shape analysis)

U: set of (concrete) memory cells

$f : U \longrightarrow \mathbb{R}$: gives the valuation of a real-valued field

We abstract the domain U by partitioning as follows:



This induces the abstraction $\wp(U) \leftrightarrows U^\sharp_\bot$

We do not abstract the codomain $\mathbb{R}$

Proper use of standard abstractions

Example: shape analysis

Viewing a binary predicate on U as a function $\simeq$ set of pairs

$$\wp(U \times U \to \mathbb{B}) \simeq \wp(U \times U)$$

Proper use of standard abstractions

Example: shape analysis

Viewing a binary predicate on U as a

function		set of pairs
	$\simeq$	
$\wp(U \times U \to \mathbb{B})$		$\wp(U \times U)$
$\downarrow \phi$		$\downarrow \rho$
$U^\sharp \times U^\sharp \to \wp(\mathbb{B})$	$\succeq$	$\wp(U^\sharp \times U^\sharp)$

Proper use of standard abstractions

Example: shape analysis

Viewing a binary predicate on U as a

function		set of pairs
	$\simeq$	
$\wp(U \times U \to \mathbb{B})$		$\wp(U \times U)$
$\downarrow \phi$		$\downarrow \rho$
$U^\sharp \times U^\sharp \to \wp(\mathbb{B})$	$\succeq$	$U^\sharp \times U^\sharp \to \mathbb{B}$

Proper use of standard abstractions

Example: shape analysis

Viewing a binary predicate on U as a function $\simeq$ set of pairs

$$\wp(U \times U \to \mathbb{B}) \simeq \wp(U \times U)$$

$$\downarrow \phi \qquad\qquad \downarrow \rho$$

$$U^\sharp \times U^\sharp \to \wp(\mathbb{B}) \quad \succeq \quad U^\sharp \times U^\sharp \to \mathbb{B}$$

$$U^\sharp \times U^\sharp \to \begin{array}{ccc} & 1/2 & \\ 0 & & 1 \\ & \bot & \end{array} \qquad U^\sharp \times U^\sharp \to \begin{array}{c} 1/2 \\ | \\ 0 \end{array}$$

Proper use of standard abstractions

Example: shape analysis

Viewing a binary predicate on U as a function $\simeq$ set of pairs

$$\wp(U \times U \to \mathbb{B}) \simeq \wp(U \times U)$$

$$\downarrow \phi \qquad\qquad \downarrow \rho$$

$$U^\sharp \times U^\sharp \to \wp(\mathbb{B}) \quad \succeq \quad U^\sharp \times U^\sharp \to \mathbb{B}$$

$$U^\sharp \times U^\sharp \to \begin{array}{ccccc} & & 1/2 & & \\ & \nearrow & & \nwarrow & \\ 0 & & & & 1 \\ & \nwarrow & & \nearrow & \\ & & \bot & & \end{array} \qquad U^\sharp \times U^\sharp \to \begin{array}{c} 1/2 \\ | \\ 0 \end{array}$$

TVLA system [SRW02]

previous approaches [CWZ90,SRW99]

Running example: standard abstraction

$\mathsf{A1} \in \wp(\boldsymbol{U} \longrightarrow \mathbb{R})$
(3 functions)

$$\left\{ \begin{array}{lcl} \boldsymbol{u_1} & \longmapsto & \left[\begin{array}{c}\mathbf{1}\\ \mathbf{2}\\ \mathbf{4}\\ \mathbf{4}\end{array}\right], \left[\begin{array}{c}\mathbf{1}\\ \mathbf{2}\\ \mathbf{5}\\ \mathbf{5}\end{array}\right], \left[\begin{array}{c}\mathbf{2}\\ \mathbf{3}\\ \mathbf{5}\\ \mathbf{6}\end{array}\right] \\ \boldsymbol{u_2} & \longmapsto & \\ \boldsymbol{u_3} & \longmapsto & \\ \boldsymbol{u_4} & \longmapsto & \end{array} \right\}$$

Running example: standard abstraction

$$\mathsf{A1} \in \wp(U \longrightarrow \mathbb{R})$$

(3 functions)

$$\left\{ \begin{array}{lcl} u_1 & \mapsto & \left[\begin{array}{c}1\\2\\4\\4\end{array}\right], \left[\begin{array}{c}1\\2\\5\\5\end{array}\right], \left[\begin{array}{c}2\\3\\5\\6\end{array}\right] \\ u_2 & \mapsto & \\ u_3 & \mapsto & \\ u_4 & \mapsto & \end{array} \right\}$$

α_ϱ

$$\mathsf{D} \in U \longrightarrow \wp(\mathbb{R})$$

$$\left\{ \begin{array}{lcl} u_1 & \mapsto & \left[\begin{array}{c}\{1,2\}\\\{2,3\}\\\{4,5\}\\\{4,5,6\}\end{array}\right] \\ u_2 & \mapsto & \\ u_3 & \mapsto & \\ u_4 & \mapsto & \end{array} \right\}$$

Running example: standard abstraction

$$\mathsf{A1} \in \wp(U \longrightarrow \mathbb{R})$$

(3 functions)

$$\left\{ \begin{array}{lcl} u_1 & \mapsto & \begin{bmatrix}1\\4\\4\end{bmatrix}, \begin{bmatrix}1\\2\\5\\5\end{bmatrix}, \begin{bmatrix}2\\3\\5\\6\end{bmatrix} \\ u_2 & \mapsto & \\ u_3 & \mapsto & \\ u_4 & \mapsto & \end{array} \right\}$$

α_ϱ

$$\mathsf{D} \in U \longrightarrow \wp(\mathbb{R})$$

$$\left\{ \begin{array}{lcl} u_1 & \mapsto & \begin{bmatrix}\{1,2\}\\\{2,3\}\\\{4,5\}\\\{4,5,6\}\end{bmatrix} \\ u_2 & \mapsto & \\ u_3 & \mapsto & \\ u_4 & \mapsto & \end{array} \right\} \xrightarrow{\alpha_\delta} \left\{ \begin{array}{lcl} u_1^\sharp & \mapsto & \begin{bmatrix}\{1,2\}\\\{2,3\}\\\{4,5,6\}\end{bmatrix} \\ u_2^\sharp & \mapsto & \\ u_{34}^\sharp & \mapsto & \end{array} \right\}$$

$$\mathsf{E} \in U^\sharp \longrightarrow \wp(\mathbb{R}))$$

Running example: standard abstraction

$\mathsf{A1} \in \wp(U \longrightarrow \mathbb{R})$
(3 functions)

$$\left\{ \begin{array}{lcl} u_1 & \mapsto & \begin{bmatrix} 1 \\ 2 \\ 4 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 5 \\ 5 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 5 \\ 6 \end{bmatrix} \\ u_2 & \mapsto & \\ u_3 & \mapsto & \\ u_4 & \mapsto & \end{array} \right\}$$

$\mathsf{A4} \in \wp(U \longrightarrow \mathbb{R})$
(36 functions)

$$\left\{ \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} \begin{array}{c} x \in \{1,2\} \\ y \in \{2,3\} \\ z, w \in \{4,5,6\} \end{array} \right\}$$

α_ϱ

$\mathsf{D} \in U \longrightarrow \wp(\mathbb{R})$

$$\left\{ \begin{array}{lcl} u_1 & \mapsto & \begin{bmatrix} \{1,2\} \\ \{2,3\} \\ \{4,5\} \\ \{4,5,6\} \end{bmatrix} \\ u_2 & \mapsto & \\ u_3 & \mapsto & \\ u_4 & \mapsto & \end{array} \right\}$$

α_δ

$\mathsf{E} \in U^\sharp \longrightarrow \wp(\mathbb{R}))$

$$\left\{ \begin{array}{lcl} u_1^\sharp & \mapsto & \begin{bmatrix} \{1,2\} \\ \{2,3\} \\ \{4,5,6\} \end{bmatrix} \\ u_2^\sharp & \mapsto & \\ u_{34}^\sharp & \mapsto & \end{array} \right\}$$

γ

Running example: standard abstraction

A1 $\in \wp(U \longrightarrow \mathbb{R})$
(3 functions)

$$\left\{ \begin{array}{lll} u_1 & \mapsto & \left[\begin{array}{c}1\\2\\4\\4\end{array}\right], \left[\begin{array}{c}1\\2\\5\\5\end{array}\right], \left[\begin{array}{c}2\\3\\5\\6\end{array}\right] \\ u_2 & \mapsto & \\ u_3 & \mapsto & \\ u_4 & \mapsto & \end{array} \right\}$$

A4 $\in \wp(U \longrightarrow \mathbb{R})$
(36 functions)

$$\left\{ \left[\begin{array}{c}x\\y\\z\\w\end{array}\right] \begin{array}{c} x \in \{1,2\} \\ y \in \{2,3\} \\ z,w \in \{4,5,6\} \end{array} \right\}$$

Information lost:

$$f(u_1) + 1 = f(u_2)$$

$$f(u_2) + 2 \leq f(u_3) \leq f(u_2) + 3$$

$$f(u_2) + 2 \leq f(u_4) \leq f(u_2) + 3$$

Running example: new abstraction

$\mathsf{A1} \in \wp(U \to \mathbb{R})$

(3 functions)

$$\left\{ \begin{array}{lll} u_1 & \mapsto & \left[\begin{array}{c}1\\1\\2\end{array}\right], \left[\begin{array}{c}1\\2\\3\end{array}\right], \left[\begin{array}{c}2\\3\\5\end{array}\right] \\ u_2 & \mapsto & \\ u_3 & \mapsto & \\ u_4 & \mapsto & \end{array} \right\}$$

Running example: new abstraction

$\mathsf{A1} \in \wp(U \to \mathbb{R})$

(3 functions)

$$\left\{ \begin{array}{lcl} u_1 & \mapsto & \begin{bmatrix}1\\1\\2\end{bmatrix}, \begin{bmatrix}1\\2\\3\end{bmatrix}, \begin{bmatrix}2\\3\\5\end{bmatrix} \\ u_2 & \mapsto & \begin{bmatrix}2\\2\\3\end{bmatrix}, \begin{bmatrix}2\\3\\4\end{bmatrix}, \begin{bmatrix}3\\4\\5\end{bmatrix} \\ u_3 & \mapsto & \begin{bmatrix}4\\5\\6\end{bmatrix}, \begin{bmatrix}5\\6\\7\end{bmatrix}, \begin{bmatrix}5\\6\\7\end{bmatrix} \\ u_4 & \mapsto & \begin{bmatrix}4\\5\\6\end{bmatrix}, \begin{bmatrix}5\\6\\7\end{bmatrix}, \begin{bmatrix}5\\6\\7\end{bmatrix} \end{array} \right\}$$

$\alpha^{\vee}_{\varrho,\delta}$

$\mathsf{B1} \in \wp(U^\sharp \to \wp(\mathbb{R}))$

$$\left\{ \begin{array}{lcl} u_1^\sharp & \mapsto & \begin{bmatrix}\{1\}\\\{1\}\\\{2\}\end{bmatrix}, \begin{bmatrix}\{1\}\\\{2\}\\\{3\}\end{bmatrix}, \begin{bmatrix}\{2\}\\\{3\}\\\{5\}\end{bmatrix} \\ u_2^\sharp & \mapsto & \begin{bmatrix}\{2\}\\\{2\}\\\{3\}\end{bmatrix}, \begin{bmatrix}\{2\}\\\{3\}\\\{4\}\end{bmatrix}, \begin{bmatrix}\{3\}\\\{4\}\\\{5\}\end{bmatrix} \\ u_{34}^\sharp & \mapsto & \begin{bmatrix}\{4\}\\\{5\}\\\{6\}\end{bmatrix}, \begin{bmatrix}\{5\}\\\{6\}\\\{7\}\end{bmatrix}, \begin{bmatrix}\{5,6\}\\\{6\}\\\{7\}\end{bmatrix} \end{array} \right\}$$

Running example: new abstraction

$\mathsf{A1} \in \wp(\boldsymbol{U} \longrightarrow \mathbb{R})$

(3 functions)

$$\left\{ \begin{array}{lcl} \boldsymbol{u_1} & \longmapsto & \left[\begin{array}{c}\mathbf{1}\\ \mathbf{2}\\ \mathbf{4}\\ \mathbf{4}\end{array}\right], \left[\begin{array}{c}\mathbf{1}\\ \mathbf{2}\\ \mathbf{5}\\ \mathbf{5}\end{array}\right], \left[\begin{array}{c}\mathbf{2}\\ \mathbf{3}\\ \mathbf{5}\\ \mathbf{6}\end{array}\right] \\ \boldsymbol{u_2} & \longmapsto & \\ \boldsymbol{u_3} & \longmapsto & \\ \boldsymbol{u_4} & \longmapsto & \end{array} \right\}$$

$\boldsymbol{\alpha^{\vee}_{\varrho,\delta}}$

$\mathsf{B1} \in \wp(\boldsymbol{U}^{\sharp} \longrightarrow \wp(\mathbb{R}))$

$$\left\{ \begin{array}{lcl} \boldsymbol{u}^{\sharp}_{\mathbf{1}} & \longmapsto & \left[\{\mathbf{1}\}\right], \left[\{\mathbf{1}\}\right], \left[\{\mathbf{2}\}\right] \\ \boldsymbol{u}^{\sharp}_{\mathbf{2}} & \longmapsto & \left[\{\mathbf{2}\}\right], \left[\{\mathbf{2}\}\right], \left[\{\mathbf{3}\}\right] \\ \boldsymbol{u}^{\sharp}_{\mathbf{34}} & \longmapsto & \left[\{\mathbf{4}\}\right], \left[\{\mathbf{5}\}\right], \left[\{\mathbf{5},\mathbf{6}\}\right] \end{array} \right\} \boldsymbol{\alpha_{\eta}} \left\{ \begin{array}{lcl} \boldsymbol{u}^{\sharp}_{\mathbf{1}} & \longmapsto & \left[\begin{array}{c}\mathbf{1}\\ \mathbf{2}\\ \mathbf{4}\end{array}\right], \left[\begin{array}{c}\mathbf{1}\\ \mathbf{2}\\ \mathbf{5}\end{array}\right], \left[\begin{array}{c}\mathbf{2}\\ \mathbf{3}\\ \mathbf{5}\end{array}\right], \left[\begin{array}{c}\mathbf{2}\\ \mathbf{3}\\ \mathbf{6}\end{array}\right] \\ \boldsymbol{u}^{\sharp}_{\mathbf{2}} & \longmapsto & \\ \boldsymbol{u}^{\sharp}_{\mathbf{34}} & \longmapsto & \end{array} \right\}$$

$\mathsf{C} \in \boldsymbol{U}^{\sharp} \longrightarrow \mathbb{R}$

Running example: new abstraction

A1 $\in \wp(U \to \mathbb{R})$

(3 functions)

$$\left\{ \begin{array}{lll} u_1 & \mapsto & \left[\begin{array}{c}1\\2\\4\\4\end{array}\right], \left[\begin{array}{c}1\\2\\5\\5\end{array}\right], \left[\begin{array}{c}2\\3\\5\\6\end{array}\right] \\ u_2 & \mapsto & \\ u_3 & \mapsto & \\ u_4 & \mapsto & \end{array} \right\}$$

B2 $\in \wp(U^\sharp \to \wp(\mathbb{R}))$

$$\left\{ \begin{array}{lll} u_1^\sharp & \mapsto & \left[\begin{array}{c}\{1\}\\\{2\}\\\{4,5\}\end{array}\right], \left[\begin{array}{c}\{2\}\\\{3\}\\\{5,6\}\end{array}\right] \\ u_2^\sharp & \mapsto & \\ u_{34}^\sharp & \mapsto & \end{array} \right\}$$

$\alpha^\vee_{\varrho,\delta}$ $\qquad$ γ_η

B1 $\in \wp(U^\sharp \to \wp(\mathbb{R}))$

$$\left\{ \begin{array}{lll} u_1^\sharp & \mapsto & \left[\begin{array}{c}\{1\}\\\{2\}\\\{4\}\end{array}\right], \left[\begin{array}{c}\{1\}\\\{2\}\\\{5\}\end{array}\right], \left[\begin{array}{c}\{2\}\\\{3\}\\\{5,6\}\end{array}\right] \\ u_2^\sharp & \mapsto & \\ u_{34}^\sharp & \mapsto & \end{array} \right\}$$

α_η

C $\in U^\sharp \to \mathbb{R}$

$$\left\{ \begin{array}{lll} u_1^\sharp & \mapsto & \left[\begin{array}{c}1\\2\\4\end{array}\right], \left[\begin{array}{c}1\\2\\5\end{array}\right], \left[\begin{array}{c}2\\3\\5\end{array}\right], \left[\begin{array}{c}2\\3\\6\end{array}\right] \\ u_2^\sharp & \mapsto & \\ u_{34}^\sharp & \mapsto & \end{array} \right\}$$

Running example: new abstraction

A1 $\in \wp(U \to \mathbb{R})$

(3 functions)

$$\left\{ \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 2 \\ 4 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 5 \\ 5 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 5 \\ 6 \end{bmatrix} \right\}$$

A3 $\in \wp(U \to \mathbb{R})$

(8 functions)

$$\left\{ \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 2 \\ x \\ y \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ x \\ y \end{bmatrix} \right\}_{x,y \in \{4,5\} \quad x,y \in \{5,6\}}$$

$\alpha^{\vee}_{\varrho,\delta}$

B1 $\in \wp(U^\sharp \to \wp(\mathbb{R}))$

$$\left\{ \begin{bmatrix} u_1^\sharp \\ u_2^\sharp \\ u_{34}^\sharp \end{bmatrix} \mapsto \begin{bmatrix} \{1\} \\ \{2\} \\ \{4\} \end{bmatrix}, \begin{bmatrix} \{1\} \\ \{2\} \\ \{5\} \end{bmatrix}, \begin{bmatrix} \{2\} \\ \{3\} \\ \{5,6\} \end{bmatrix} \right\}$$

α_η

C $\in U^\sharp \to \mathbb{R}$

γ

$$\left\{ \begin{bmatrix} u_1^\sharp \\ u_2^\sharp \\ u_{34}^\sharp \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 5 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 5 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 6 \end{bmatrix} \right\}$$

Running example: new abstraction

$\mathsf{A1} \in \wp(U \to \mathbb{R})$
(3 functions)

$$\left\{ \begin{array}{lll} u_1 & \mapsto & \begin{bmatrix} 1 \\ 2 \\ 4 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 5 \\ 5 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 5 \\ 6 \end{bmatrix} \\ u_2 & \mapsto & \\ u_3 & \mapsto & \\ u_4 & \mapsto & \end{array} \right\}$$

$\mathsf{A3} \in \wp(U \to \mathbb{R})$
(8 functions)

$$\left\{ \begin{array}{lll} u_1 & \mapsto & \begin{bmatrix} 1 \\ 2 \\ x \\ y \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ x \\ y \end{bmatrix} \\ u_2 & \mapsto & \\ u_3 & \mapsto & \\ u_4 & \mapsto & \end{array} \right\}$$

$x,y \in \{4,5\}$ $\quad$ $x,y \in \{5,6\}$

Information kept:

$$f(u_1) + 1 = f(u_2)$$

$$f(u_2) + 2 \leq f(u_3) \leq f(u_2) + 3$$

$$f(u_2) + 2 \leq f(u_4) \leq f(u_2) + 3$$

Hence the name relational function-abstraction

Information lost: $3 \to 8$ functions instead of $3 \to 36$!

New abstraction: first step $\alpha^{\vee}_{\varrho,\delta}$

Disjunctive completion of $\alpha_\delta \circ \alpha_\varrho$ (classical abstractions)

$\wp(D_1 \to D_2) \underset{\alpha^{\vee}_{\varrho,\delta}}{\overset{\gamma^{\vee}_{\varrho,\delta}}{\leftrightarrows}} \wp(A_1 \xrightarrow{\sqsubseteq} \wp(D_2))$ is defined by

$$\alpha^{\vee}_{\varrho,\delta}(F) = \bigcup_{f \in F} \{f^\sharp \mid \forall a_1 : f^\sharp(a_1) = f(\gamma_1(a_1))\}$$

$$\gamma^{\vee}_{\varrho,\delta}(F^\sharp) = \bigcup_{f^\sharp \in F^\sharp} \{f \mid \forall d_1 : f(d_1) \in f^\sharp(\alpha_1(d_1))\}$$

"Merges $f(d_1)$ and $f(d'_1)$ when d_1 and d'_1 are merged by α_1."
"Never Merges $f(d_1)$ and $f'(d_1)$."

Running example: first abstraction step

A1 $\in \wp(U \to \mathbb{R})$
(3 functions)

$$\left\{ \begin{bmatrix} u_1 \mapsto 1 \\ u_2 \mapsto 2 \\ u_3 \mapsto 4 \\ u_4 \mapsto 4 \end{bmatrix}, \begin{bmatrix} u_1 \mapsto 1 \\ u_2 \mapsto 2 \\ u_3 \mapsto 5 \\ u_4 \mapsto 5 \end{bmatrix}, \begin{bmatrix} u_1 \mapsto 2 \\ u_2 \mapsto 3 \\ u_3 \mapsto 5 \\ u_4 \mapsto 6 \end{bmatrix} \right\}$$

A2 $\in \wp(U \to \mathbb{R})$
(6 functions)

$$\left\{ \begin{bmatrix} u_1 \mapsto 1 \\ u_2 \mapsto 2 \\ u_3 \mapsto 4 \\ u_4 \mapsto 4 \end{bmatrix}, \begin{bmatrix} u_1 \mapsto 1 \\ u_2 \mapsto 2 \\ u_3 \mapsto 5 \\ u_4 \mapsto 5 \end{bmatrix}, \begin{bmatrix} u_1 \mapsto 2 \\ u_2 \mapsto 3 \\ u_3 \mapsto x \\ u_4 \mapsto y \end{bmatrix} \right\}_{x,y \in \{5,6\}}$$

$\alpha^{\vee}_{\varrho,\delta}$

B1 $\in \wp(U^\sharp \to \wp(\mathbb{R}))$

$$\left\{ \begin{bmatrix} u_1^\sharp \mapsto \{1\} \\ u_2^\sharp \mapsto \{2\} \\ u_{34}^\sharp \mapsto \{4\} \end{bmatrix}, \begin{bmatrix} u_1^\sharp \mapsto \{1\} \\ u_2^\sharp \mapsto \{2\} \\ u_{34}^\sharp \mapsto \{5\} \end{bmatrix}, \begin{bmatrix} u_1^\sharp \mapsto \{2\} \\ u_2^\sharp \mapsto \{3\} \\ u_{34}^\sharp \mapsto \{5,6\} \end{bmatrix} \right\}$$

$\gamma^{\vee}_{\varrho,\delta}$

New abstraction: second step α_η

In the example's framework, using $U^\sharp \longrightarrow X \simeq X^n$:

$$\begin{array}{ccc} \wp(U^\sharp \longrightarrow \wp(\mathbb{R})) & \underset{\alpha_\eta}{\overset{\gamma_\eta}{\leftrightarrows}} & \wp(U^\sharp \longrightarrow \mathbb{R}) \\ (\wp(\mathbb{R}))^n & & \mathbb{R}^n \end{array}$$

$$\begin{aligned} \alpha_\eta(F) &= \bigcup_{\langle X_1,\ldots,X_n\rangle \in F} X_1 \times \ldots \times X_n \\ \gamma_\eta(F^\sharp) &= \{\langle X_1, \ldots, X_n\rangle \mid X_1 \times \ldots \times X_n \subseteq F^\sharp\} \end{aligned}$$

Non standard meaning of sets of vectors in $\mathbb{R}^n$

as vectors in $\wp(\mathbb{R}^n)$

γ_η returns (maximal) cartesian products included in set $F^\sharp$

New abstraction: second step α_η

Generalization:

$\wp(A_1 \to \wp(D_2)) \underset{\alpha_\eta}{\overset{\gamma_\eta}{\leftrightarrows}} \wp(A_1 \to D_2)$ is defined by

$$\alpha_\eta(F) = \bigcup_{f \in F} \{f^\sharp \mid \forall a_1 : f^\sharp(a_1) \in f(a_1)\}$$

$$\gamma_\eta(F^\sharp) = \{f \mid \forall f^\sharp \in (A_1 \to D_2) : \Big(\forall a_1, f^\sharp(a_1) \in f(a_1)\Big) \Rightarrow f^\sharp \in F^\sharp\}$$

New abstraction: second step α_η

Generalization:

$\wp(A_1 \to \wp(D_2)) \underset{\alpha_\eta}{\overset{\gamma_\eta}{\leftrightarrows}} \wp(A_1 \to D_2)$ is defined by

$$\alpha_\eta(F) = \bigcup_{f \in F} \{f^\sharp \mid \forall a_1 : f^\sharp(a_1) \in f(a_1)\}$$

$$\gamma_\eta(F^\sharp) = \{f \mid \forall f^\sharp \in (A_1 \to D_2) : \Big(\forall a_1, f^\sharp(a_1) \in f(a_1)\Big) \Rightarrow f^\sharp \in F^\sharp\}$$

May be considered as somewhat subtle

Running example: second abstraction step

$$\mathsf{B1} \in \wp(\boldsymbol{U}^\sharp \longrightarrow \wp(\mathbb{R}))$$

$$\left\{ \begin{array}{lcl} \boldsymbol{u}_1^\sharp & \longmapsto & \left[\{\mathbf{1}\}\right], \left[\{\mathbf{1}\}\right], \left[\{\mathbf{2}\}\right] \\ \boldsymbol{u}_2^\sharp & \longmapsto & \left[\{\mathbf{2}\}\right], \left[\{\mathbf{2}\}\right], \left[\{\mathbf{3}\}\right] \\ \boldsymbol{u}_{34}^\sharp & \longmapsto & \left[\{\mathbf{4}\}\right], \left[\{\mathbf{5}\}\right], \left[\{\mathbf{5},\mathbf{6}\}\right] \end{array} \right\}$$

$$\mathsf{B2} \in \wp(\boldsymbol{U}^\sharp \longrightarrow \wp(\mathbb{R}))$$

$$\left\{ \begin{array}{lcl} \boldsymbol{u}_1^\sharp & \longmapsto & \left[\{\mathbf{1}\}\right], \left[\{\mathbf{2}\}\right] \\ \boldsymbol{u}_2^\sharp & \longmapsto & \left[\{\mathbf{2}\}\right], \left[\{\mathbf{3}\}\right] \\ \boldsymbol{u}_{34}^\sharp & \longmapsto & \left[\{\mathbf{4},\mathbf{5}\}\right], \left[\{\mathbf{5},\mathbf{6}\}\right] \end{array} \right\}$$

α_η

$$\mathsf{C} \in \wp(\boldsymbol{U}^\sharp \longrightarrow \mathbb{R})$$

$$\left\{ \begin{array}{lcl} \boldsymbol{u}_1^\sharp & \longmapsto & \left[\mathbf{1}\right], \left[\mathbf{1}\right], \left[\mathbf{2}\right], \left[\mathbf{2}\right] \\ \boldsymbol{u}_2^\sharp & \longmapsto & \left[\mathbf{2}\right], \left[\mathbf{2}\right], \left[\mathbf{3}\right], \left[\mathbf{3}\right] \\ \boldsymbol{u}_{34}^\sharp & \longmapsto & \left[\mathbf{4}\right], \left[\mathbf{5}\right], \left[\mathbf{5}\right], \left[\mathbf{6}\right] \end{array} \right\}$$

γ_η

New abstraction: third abstraction step (codomain)

In the example's framework, using $(\boldsymbol{U}^\sharp \longrightarrow \boldsymbol{X}) \simeq \boldsymbol{X}^{\boldsymbol{n}}$:

$$\wp(\boldsymbol{U}^\sharp \longrightarrow \mathbb{R}) \underset{\alpha_\eta}{\overset{\gamma_\eta}{\leftrightarrows}} \boldsymbol{A}[\boldsymbol{n}]$$
$$\wp(\mathbb{R}^{\boldsymbol{n}})$$

$\boldsymbol{A}[\boldsymbol{n}]$ may be $\boldsymbol{n}$-dimensional octagons, octahedrons, convex polyhedra, linear equalities, linear congruences ...

New abstraction: third abstraction step (codomain)

In the example's framework, using $(U^\sharp \to X) \simeq X^n$:

$$\wp(U^\sharp \to \mathbb{R}) \underset{\alpha_\eta}{\overset{\gamma_\eta}{\leftrightarrows}} A[n]$$
$$\wp(\mathbb{R}^n)$$

$A[n]$ may be n-dimensional octagons, octahedrons, convex polyhedra, linear equalities, linear congruences ...

Generalization: assuming

- A_1 is of finite cardinality n
- We have an abstraction $\wp(D_2^k) \leftrightarrows A_2[k]$

we abstract $\wp(A_1 \to D_2)$ with $A_2[n]$

If $A_2[n]$ is not relational, ie., if $A_2[n] \simeq (A_2)^n$,

we obtain the classical abstraction $A_1 \overset{\sqsubseteq}{\to} A_2$

Summary and results

Assuming Galois connections

- $\wp(D_1) \leftrightarrows A_1$
- $\wp(D_2^k) \leftrightarrows A_2[k]$

Relational function-abstraction is

$$\wp(D_1 \to D_2) \leftrightarrows \wp(A_1 \to D_2) \underbrace{\leftrightarrows A_2[|A_1|]}_{\text{if } A_1 \text{ is finite}}$$

Theorem 1: $\wp_{\sqcup}(A_1 \xrightarrow{\sqsubseteq} A_2) \succeq A_2[|A_1|] \succeq (A_1 \xrightarrow{\sqsubseteq} A_2)$

First inequality comes down to equality iff $A_2[|A_1|]$ is

disjunctive

Second inequality reduces to equality iff $A_2[|A_1|]$ is

not relational

Summary and results

Assuming Galois connections

- $\wp(D_1) \leftrightarrows A_1$
- $\wp(D_2^k) \leftrightarrows A_2[k]$

Relational function-abstraction is

$$\wp(D_1 \to D_2) \leftrightarrows \wp(A_1 \to D_2) \underbrace{\leftrightarrows A_2[|A_1|]}_{\text{if } A_1 \text{ is finite}}$$

Theorem 1: $\wp_{\sqcup}(A_1 \xrightarrow{\sqsubseteq} A_2) \succeq A_2[|A_1|] \succeq (A_1 \xrightarrow{\sqsubseteq} A_2)$

First inequality comes down to equality iff $A_2[|A_1|]$ is disjunctive

Second inequality reduces to equality iff $A_2[|A_1|]$ is not relational

Theorem 2: $A_2[|A_1|]$ finitely representable if $A_1 \xrightarrow{\sqsubseteq} A_2$ is so: A_1 finite and $A_2[k]$ finitely representable

Applications

Abstraction of arrays: $\boldsymbol{U} \longrightarrow \mathbb{R}$

"Numeric domains with summarized dimensions", GDDRS, TACAS'04

"Numeric analysis of array operations", GRS, POPL'05

Implemented in TVLA system by Denis Gopan

Applications

Abstraction of arrays: $U \longrightarrow \mathbb{R}$

"Numeric domains with summarized dimensions", GDDRS, TACAS'04

"Numeric analysis of array operations", GRS, POPL'05

Implemented in TVLA system by Denis Gopan

Shape Analysis: more generally, in ITVLA,

$$\wp\left(\prod_{p\in\mathcal{P}_1}(U \to \mathbb{B}) \times \prod_{p\in\mathcal{P}_2}(U^2 \to \mathbb{B}) \times \prod_{p\in\mathcal{R}_1}(U \to \mathbb{R})\right)$$

$$\simeq$$

$$\left(\prod_{p\in\mathcal{P}_1}(U \to \mathbb{B}) \times \prod_{p\in\mathcal{P}_2}(U^2 \to \mathbb{B})\right) \to \wp\left(\prod_{p\in\mathcal{R}_1}(U \to \mathbb{R})\right)$$

is abstracted by (roughly speaking)

$$\left(\prod_{p\in\mathcal{P}_1}(U^\sharp \to \wp(\mathbb{B})) \times \prod_{p\in\mathcal{P}_2}((U^\sharp)^2 \to \wp(\mathbb{B}))\right) \to \prod_{p\in\mathcal{R}_1} \mathbf{Pol}[|U^\sharp|]$$