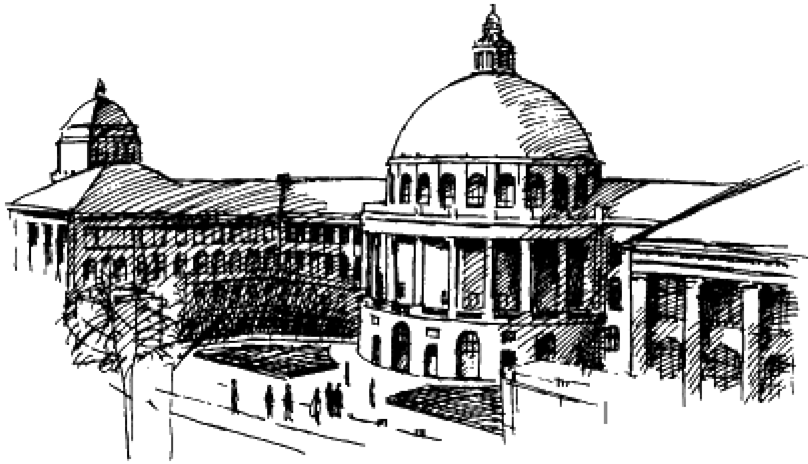
A Practical Construction for Decomposing Numerical Abstract Domains



Gagandeep Singh Markus Püschel Martin Vechev

Department of Computer Science

ETH zürich



Numerical abstract domains

Numerical Domain	**Representable Constraints** ($c \in \mathbb{Q}$ or $\mathbb{R}$)	Cost and Expressivity
Interval	$\pm x_i \leq c$	
Pentagon	$(\pm x_i \leq c)$ or $(x_i \leq x_j)$	
Zones	$(\pm x_i \leq c)$ or $(x_i - x_j \leq c)$	
Octagon	$(\pm x_i \leq c)$ or $(\pm x_i \pm x_j \leq c)$	
TVPI	$a_i x_i + a_j x_j \leq c, a_i \in \mathbb{Z}$	
Polyhedra	$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \leq c, a_i \in \mathbb{Z}$	

Static analysis with precise numerical domains is expensive

Domain transformers

Octagon

// abstract program state: $\{-x_1 - x_2 \leq 0, -x_2 \leq 0, -x_3 - x_4 \leq 0\}$

// program statement: **If** $(x_2 + x_3 + x_4 \leq 1)$

Best, Exponential

$\{-x_1 - x_2 \leq 0, -x_2 \leq 0, -x_3 - x_4 \leq 0, x_2 \leq 1, x_3 + x_4 \leq 1, -x_1 \leq 1\}$

Standard, Quadratic

$\{-x_1 - x_2 \leq 0, -x_2 \leq 0, -x_3 - x_4 \leq 0, x_3 + x_4 \leq 1\}$

Trivial, Constant

$\{\}$

Best abstract transformers for even less precise domains are expensive

Online decomposition

Octagon

Numerical domain analysis can be made **faster** through online decomposition

$\mathcal{J}$	$\pi_{\mathcal{J}}$		$\mathcal{J}'$	$\pi_{\mathcal{J}'}$
$\{-x_1 - x_2 \leq 0, -x_2 \leq 0\}$	$\{x_1, x_2\}$	If$(x_2 + x_3 + x_4 \leq 1)$ $\longrightarrow$	$\{-x_1 - x_2 \leq 0, -x_2 \leq 0\}$	$\{x_1, x_2\}$
$\{-x_3 - x_4 \leq 0\}$	$\{x_3, x_4\}$		$\{-x_3 - x_4 \leq 0, x_3 + x_4 \leq 1\}$	$\{x_3, x_4\}$

- Decomposing standard Octagon analysis ([PLDI 2015])
- Decomposing standard Polyhedra analysis ([SAS 2003, POPL2017])

Limitations of prior work

- Numerical abstract domains and their transformers
  - ad hoc design
  - guided by cost precision tradeoff
  - tailored for specific use cases

Drawback: Prior work cannot be reused for new domain transformers

Required: Universal construction for decomposing numerical domains

Contributions

Original

Abstract element + Transformer
80 vars

→ Black box construction →

Decomposed

32 vars

3 vars

28 vars

17 vars

Our decomposed analysis

- Significantly fast
- Always sound
- Monotonic → Under practical conditions
- Precise → Under practical conditions

Complete end-to-end implementation

- Polyhedra
- Octagon
- Zones

ELINA elina.ethz.ch

Benchmark: >30K LOC, >550 vars

Analysis	Poly	Oct	Zones
Original	6142 s	28 s	3 s
Decomposed	4.4 s	1.9 s	1.5 s

Requirements on numerical abstract domains

- An abstract element $\mathcal{I}$ in domain $\mathcal{D}$ is conjunction of finite number of representable constraints
- The concretization function γ for $\mathcal{D}$ should be meet preserving

$$\gamma(\mathcal{I} \cap \mathcal{J}) = \gamma(\mathcal{I}) \cap \gamma(\mathcal{J})$$

- The ordering of abstract elements in the domain satisfies:

$$\mathcal{I} \sqsubseteq \mathcal{I}' \Leftrightarrow \gamma(\mathcal{I}) \subseteq \gamma(\mathcal{I}')$$

Partitioning variable set $\mathcal{X}$

Octagon

$\mathcal{J}$	Finest unique partition $\pi_\mathcal{J}$	$\mathcal{J}$	A permissible partition $\bar{\pi}_\mathcal{J}$	An invalid partition
$\{-x_1 - x_2 \leq 0\}$	$\{x_1, x_2\}$	$\{-x_1 - x_2 \leq 0\}$	$\{x_1, x_2\}$	$\{x_1, x_3\}$
$\{x_3 \leq 0\}$	$\{x_3\}$	$\{x_3 \leq 0, x_4 \leq 0\}$	$\{x_3, x_4\}$	$\{x_2\}$
$\{x_4 \leq 0\}$	$\{x_4\}$			$\{x_4\}$

- Expensive to maintain finest partitions thus online decomposition maintains permissible partitions

Decomposable transformers

Polyhedra

//abstract program state: $\{x_1 + x_2 \le 0\}$ $\{x_1, x_2\}$

$\{x_3 + x_4 \le 5\}$ $\{x_3, x_4\}$

//program statement: **If** $(x_5 + x_6 \le 0)$

Non-decomposable

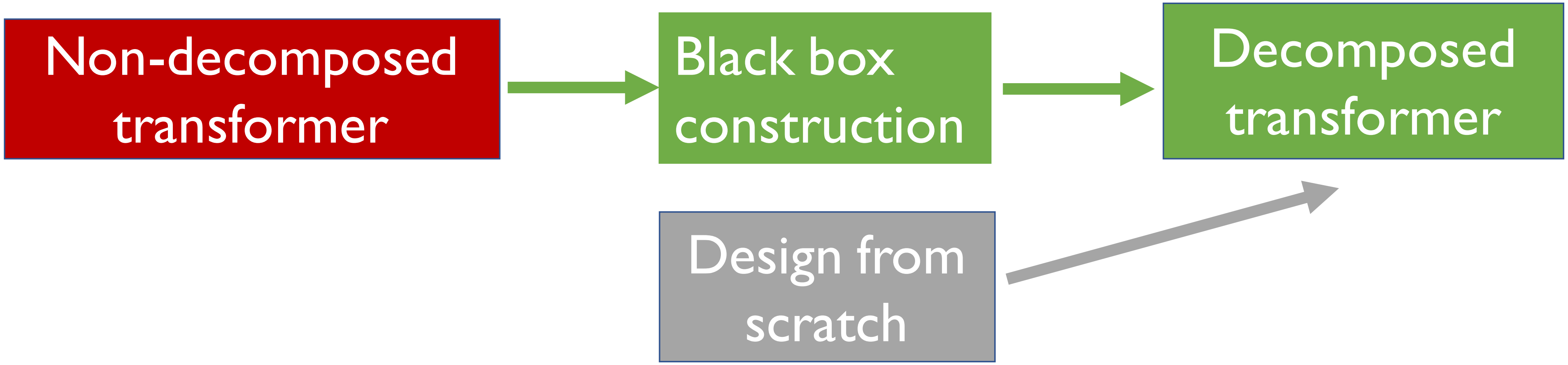
$\mathcal{J}'$ $\{x_1 + x_2 + x_3 + x_4 + x_5 + x_6 \le 5\}$

$\bar{\pi}_{\mathcal{J}'}\{x_1, x_2, x_3, x_4, x_5, x_6\}$

Decomposable

$\mathcal{J}''$	$\bar{\pi}_{\mathcal{J}''}$
$\{x_1 + x_2 \le 0\}$	$\{x_1, x_2\}$
$\{x_3 + x_4 \le 5\}$	$\{x_3, x_4\}$
$\{x_5 + x_6 \le 0\}$	$\{x_5, x_6\}$

Decomposable transformers



- Conditional
- Assignment
- Meet
- Join
- Widening

Conditional Transformer T_{cond}

Polyhedra

Definition: Let $\mathcal{J}$ be an abstract element in domain $\mathcal{D}$ with the associated permissible partition $\bar{\pi}_{\mathcal{J}}$ and $\sum a_i x_i \leq c$ be the conditional statement then,

$$\mathcal{B}_{cond} := \{x_i \,:\, a_i \neq 0\}$$

$$\mathcal{B}^*_{cond} := \bigcup_{\mathcal{X}_k \cap \mathcal{B}_{cond} \neq \emptyset} \mathcal{X}_k, \;\; \mathcal{X}_k \in \bar{\pi}_{\mathcal{J}}$$

$\mathcal{J}$	$\bar{\pi}_{\mathcal{J}}$
$\{2x_1 - x_2 + 4x_3 \leq 0\}$	$\{x_1, x_2, x_3\}$
$\{2x_4 + 3x_5 \leq 5\}$	$\{x_4, x_5\}$
$\{x_6 = 1\}$	$\{x_6\}$

$$\xrightarrow[\mathcal{B}_{cond} = \{x_3, x_6\}]{\text{If}(x_3 + x_6 \leq 0)}$$

$\mathcal{B}^*_{cond}$

$\{x_1, x_2, x_3, x_6\}$

Conditional Transformer T_{cond}

Octagon

$$\mathcal{J}_O := T^d_{cond}(\mathcal{J}) := T_{cond}\big(\mathcal{J}(\mathcal{B}^*_{cond})\big) \cup \mathcal{J}(\mathcal{X} \setminus \mathcal{B}^*_{cond})$$

$$\bar{\pi}_{\mathcal{J}_O} \coloneqq \{\mathcal{X}_k \in \bar{\pi}_{\mathcal{J}} : \mathcal{X}_k \cap \mathcal{B}^*_{cond} = \emptyset\} \cup \{\mathcal{B}^*_{cond}\}$$

$\mathcal{J}$	$\bar{\pi}_{\mathcal{J}}$		$T^d_{cond}(\mathcal{J})$	$\bar{\pi}_{\mathcal{J}_O}$
$\{x_1 \leq 0\}$	$\{x_1\}$	If$(x_3 \leq 0)$ $\longrightarrow$	$\{x_1 \leq 0\}$	$\{x_1\}$
$\{x_2 + x_3 \leq 0\}$	$\{x_2, x_3\}$	$\mathcal{B}^*_{cond}=\{x_2, x_3\}$	$\{x_2 + x_3 \leq 0,$ $x_3 \leq 0\}$	$\{x_2, x_3\}$

Conditional Transformer T_{cond}

Octagon

Theorem: $\gamma(T_{cond}(\mathcal{J})) = \gamma(T^{d}_{cond}(\mathcal{J}))$ if for any associated permissible partition $\bar{\pi}_{\mathcal{J}}$, the output $T_{cond}(\mathcal{J})$ satisfies:

- $T_{cond}(\mathcal{J}) = \mathcal{J} \cup \mathcal{J}' \cup \mathcal{J}''$ where $\mathcal{J}'$ is a set of non-redundant constraints between the variables from $\mathcal{B}^{*}_{cond}$ only and $\mathcal{J}''$ is a set of redundant constraints between the variables in $\mathcal{X}$
- $\gamma(T_{cond}(\mathcal{J}(\mathcal{B}^{*}_{cond}))) = \gamma(\mathcal{J}(\mathcal{B}^{*}_{cond}) \cup \mathcal{J}')$

$\mathcal{J}$	$\bar{\pi}_{\mathcal{J}}$		$T_{cond}(\mathcal{J})$	
$\{x_1 \leq 0\}$	$\{x_1\}$	If$(x_3 \leq 0)$	$\{x_1 \leq 0,\ x_2 + x_3 \leq 0,\ x_1 + x_3 \leq 0, x_3 \leq 0\}$	$\mathcal{J}'$: $\{x_3 \leq 0\}$
$\{x_2 + x_3 \leq 0\}$	$\{x_2, x_3\}$	$\mathcal{B}^{*}_{cond}$=$\{x_2, x_3\}$		$\mathcal{J}''$: $\{x_1 + x_3 \leq 0\}$

$\gamma(T_{cond}(\mathcal{J}(\mathcal{B}^{*}_{cond}))) = \gamma(\mathcal{J}(\mathcal{B}^{*}_{cond}) \cup \mathcal{J}')$ =$\gamma(\{x_2 + x_3 \leq 0, x_3 \leq 0\})$

Refinement

- The output partition can be refined after computing the output
  - non-invertible assignment
  - join
- Allows us to produce finer output partitions than prior work for
  - Polyhedra
  - Octagon

Experimental Evaluation

- Crab-llvm analyzer
  - intra procedural analysis
  - analyzes llvm bitcode
- Software verification competition benchmarks
  - linux device drivers
  - control flow
- Polyhedra
  - non decomposed transformers from PPL and decomposed from [POPL'17]
- Octagon
  - non decomposed and decomposed transformers from [PLDI'15]
- Zones
  - Implemented non decomposed transformers

Polyhedra

Benchmark	PPL (s)	POPL'17 (s)	POPL'18 (s)	Speedup vs	
				PPL	POPL'17
net_fddi_skfp	6142	9.2	4.4	1386	2
mtd_ubi	MO	4	1.9	∞	2.1
usb_core_main0	4003	65	29	136	2.2
tty_synclinkmp	MO	3.4	2.5	∞	1.4
scsi_advansys	TO	4	3.4	>4183	1.2
staging_vt6656	TO	2	0.5	>28800	4
net_ppp	10530	924	891	11.8	1
p10_l00	121	11	5.4	22.4	2
p16_l40	MO	11	2.9	∞	3.8
p12_l57	MO	14	6.5	∞	2.1
p13_l53	MO	54	25	∞	2.2
p19_l59	MO	70	12	∞	5.9

Octagon

Benchmark	PLDI'15 ND(s)	PLDI'15 D(s)	POPL'18 (s)	Speedup vs	
				ND	D
net_fddi_skfp	28	2.6	1.9	15	1.4
mtd_ubi	3411	979	532	6.4	1.8
usb_core_main0	107	6.1	4.9	22	1.2
tty_synclinkmp	8.2	1	0.8	10	1.2
scsi_advansys	9.3	1.5	0.8	12	1.9
staging_vt6656	4.8	0.3	0.2	24	1.5
net_ppp	11	1.1	1.2	9.2	0.9
p10_l00	20	0.5	0.5	40	1
p16_l40	8.8	0.6	0.5	18	1.2
p12_l57	19	1.2	0.7	27	1.7
p13_l53	43	1.7	1.3	33	1.3
p19_l59	41	2.8	1.2	31	2.2

Zones

Benchmark	Non Decomposed (s)	POPL'18 (s)	Speedup
net_fddi_skfp	3	1.5	2
mtd_ubi	1.4	0.7	2
usb_core_main0	10.3	4.6	2.2
tty_synclinkmp	1.1	0.7	1.6
scsi_advansys	0.9	0.7	1.3
staging_vt6656	0.5	0.2	2.5
net_ppp	1.1	0.7	1.5
p10_l00	1.9	0.4	4.6
p16_l40	1.7	0.7	2.5
p12_l57	3.5	0.9	3.9
p13_l53	8.7	2.1	4.2
p19_l59	9.8	1.6	6.1

Black box construction

$$\mathcal{I}_O := T^d_{cond}(\mathcal{I}) := T_{cond}\big(\mathcal{I}(\mathcal{B}^*_{cond})\big) \cup \mathcal{I}(\mathcal{X} \setminus \mathcal{B}^*_{cond})$$

$$\bar{\pi}_{\mathcal{I}_O} \coloneqq \{\mathcal{X}_k \in \bar{\pi}_{\mathcal{I}} : \mathcal{X}_k \cap \mathcal{B}^*_{cond} = \emptyset\} \cup \{\mathcal{B}^*_{cond}\}$$

$\mathcal{I}$	$\bar{\pi}_{\mathcal{I}}$		$T^d_{cond}(\mathcal{I})$	$\bar{\pi}_{\mathcal{I}_O}$
$\{x_1 \leq 0\}$	$\{x_1\}$	If$(x_3 \leq 0)$ $\longrightarrow$	$\{x_1 \leq 0\}$	$\{x_1\}$
$\{x_2 + x_3 \leq 0\}$	$\{x_2, x_3\}$	$\mathcal{B}^*_{cond} = \{x_2, x_3\}$	$\{x_2 + x_3 \leq 0, x_3 \leq 0\}$	$\{x_2, x_3\}$

Same precision in practice

Theorem: $\gamma(T_{cond}(\mathcal{I})) = \gamma(T^d_{cond}(\mathcal{I}))$ if for any associated permissible partition $\bar{\pi}_{\mathcal{I}}$, the output $T_{cond}(\mathcal{I})$ satisfies:

- $T_{cond}(\mathcal{I}) = \mathcal{I} \cup \mathcal{I}' \cup \mathcal{I}''$ where $\mathcal{I}'$ is a set of non-redundant constraints between the variables from $\mathcal{B}^*_{cond}$ only and $\mathcal{I}''$ is a set of redundant constraints between the variables in $\mathcal{X}$
- $\gamma(T_{cond}(\mathcal{I}(\mathcal{B}^*_{cond}))) = \gamma(\mathcal{I}(\mathcal{B}^*_{cond}) \cup \mathcal{I}')$

$\mathcal{I}$	$\bar{\pi}_{\mathcal{I}}$		$T_{cond}(\mathcal{I})$	
$\{x_1 \leq 0\}$	$\{x_1\}$	If$(x_3 \leq 0)$ $\longrightarrow$	$\{x_1 \leq 0, x_2 + x_3 \leq 0, x_1 + x_3 \leq 0, x_3 \leq 0\}$	$\mathcal{I}'$: $\{x_3 \leq 0\}$
$\{x_2 + x_3 \leq 0\}$	$\{x_2, x_3\}$	$\mathcal{B}^*_{cond} = \{x_2, x_3\}$		$\mathcal{I}''$: $\{x_1 + x_3 \leq 0\}$

$$\gamma(T_{cond}(\mathcal{I}(\mathcal{B}^*_{cond}))) = \gamma(\mathcal{I}(\mathcal{B}^*_{cond}) \cup \mathcal{I}') = \gamma(\{x_2 + x_3 \leq 0, x_3 \leq 0\})$$

15

Complete end-to-end implementation

- Polyhedra
- Octagon
- Zones

ELINA elina.ethz.ch

Benchmark: >30K LOC, >550 vars

Analysis	Poly	Oct	Zones
Original	6142 s	28 s	3 s
Decomposed	4.4 s	1.9 s	1.5 s