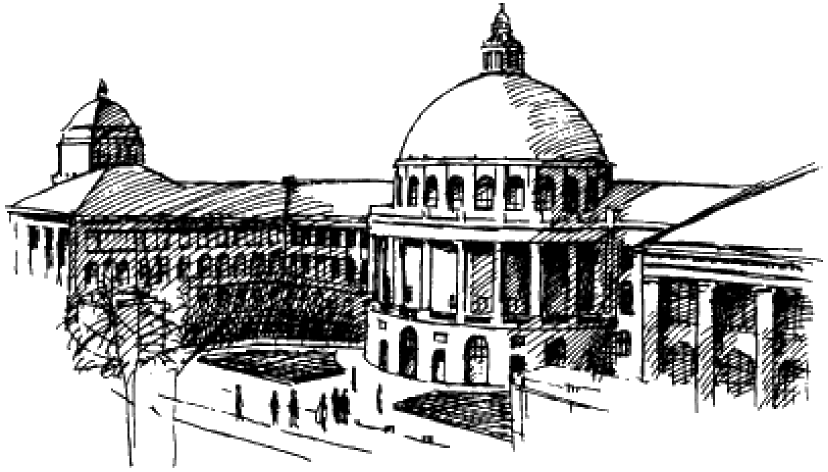
Fast Polyhedra Abstract Domain



Gagandeep Singh   Markus Püschel   Martin Vechev

Department of Computer Science

ETH Zurich



Polyhedra Domain Analysis

Automatic Discovery of Linear Restraints Among Variables of a Program, POPL'78

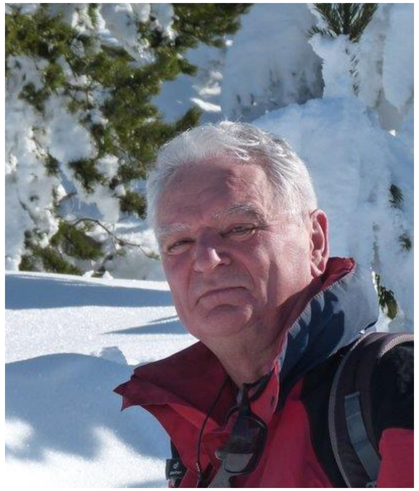
Polyhedra Domain Analysis

Automatic Discovery of Linear Restraints Among Variables of a Program, POPL'78

Introduced by Patrick Cousot and Nicolas Halbwachs

Represents linear constraints between program variables

Patrick Cousot



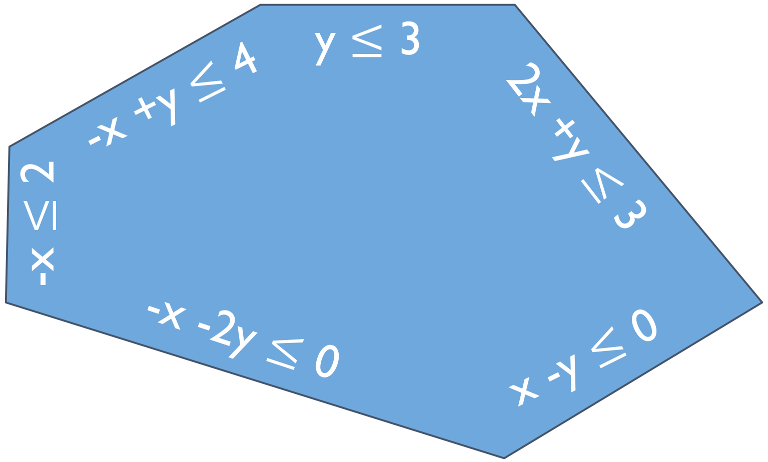
Nicolas Halbwachs

Polyhedra Domain Analysis

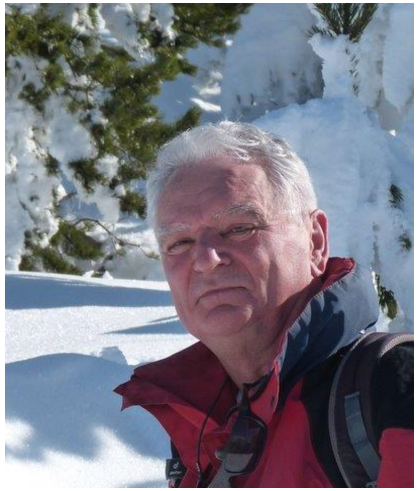
Automatic Discovery of Linear Restraints Among Variables of a Program, POPL'78

Introduced by Patrick Cousot and Nicolas Halbwachs

Represents linear constraints between program variables



Patrick Cousot



Nicolas Halbwachs

Polyhedra Domain Analysis

Polyhedra Domain Analysis

```
if(*){
      y:=2x-1;
}
else{
      y:=2x-2;
}
assert(y<=2x);
```

Polyhedra Domain Analysis

```
if(*){
        y:=2x-1;
}
else{
        y:=2x-2;
}
assert(y<=2x);
```

Abstract Domain	Can Prove the Assertion?
Interval	✗
Pentagon	✗
Zones	✗
Octagon	✗
Polyhedra	✓

Polyhedra Domain Analysis

```
if(*){
        y:=2x-1;
}
else{
        y:=2x-2;
}
assert(y<=2x);
```

Abstract Domain	Can Prove the Assertion?
Interval	✗
Pentagon	✗
Zones	✗
Octagon	✗
Polyhedra	✓

Polyhedra analysis: time and space exponential in number of variables

This work: contributions

This work: contributions

Online decomposition:
reduction in space and time
without losing precision

This work: contributions

Online decomposition:
reduction in space and time
without losing precision

Constant factor improvements
via reduced operation count and
cache optimizations

This work: contributions

Online decomposition:
reduction in space and time without losing precision

Constant factor improvements
via reduced operation count and cache optimizations

ELINA elina.ethz.ch

Complete end-to-end implementation

This work: contributions

Online decomposition:
reduction in space and time without losing precision

Constant factor improvements
via reduced operation count and cache optimizations

ELINA elina.ethz.ch

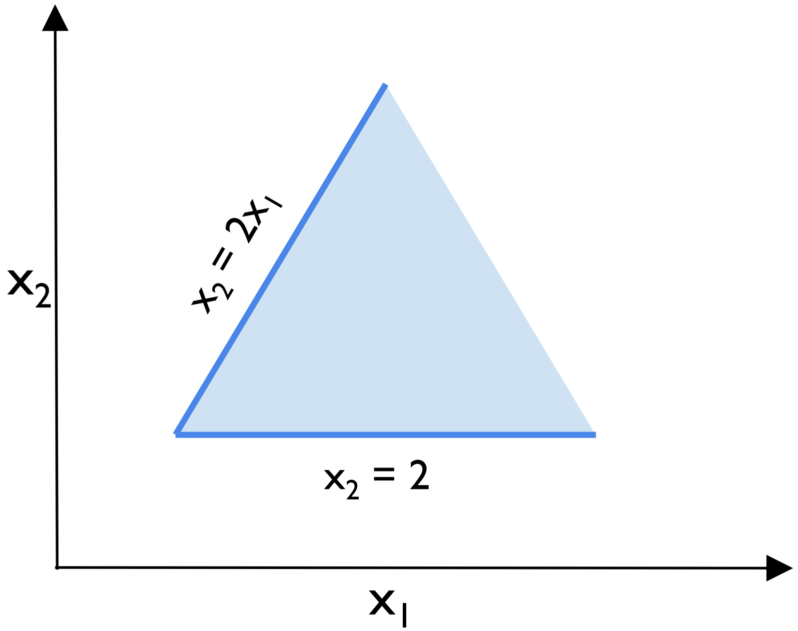
Complete end-to-end implementation

Driver	NewPolka	PPL	ELINA
➢ 500 var ➢ 39K LOC	OOM (> 12 GB)	OOM (> 12 GB)	4 sec 0.9 GB
➢ 650 var ➢ 25K LOC	TO (> 4 hr)	TO (> 4 hr)	2 sec 0.4 GB

Double Representation of Polyhedron

Double Representation of Polyhedron

Constraints

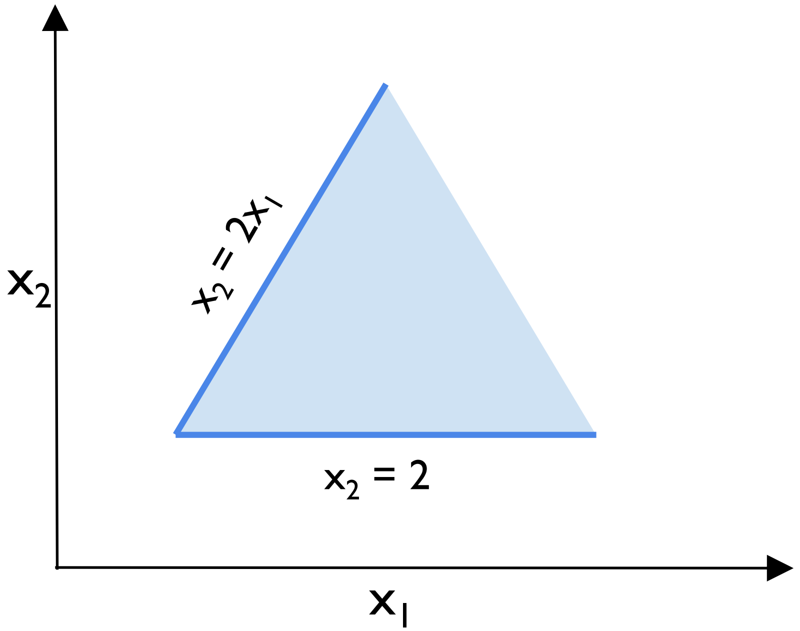


$\mathcal{C}$ = {$-x_2 \leq -2$, $x_2 \leq 2x_1$}

m: number of constraints

Double Representation of Polyhedron

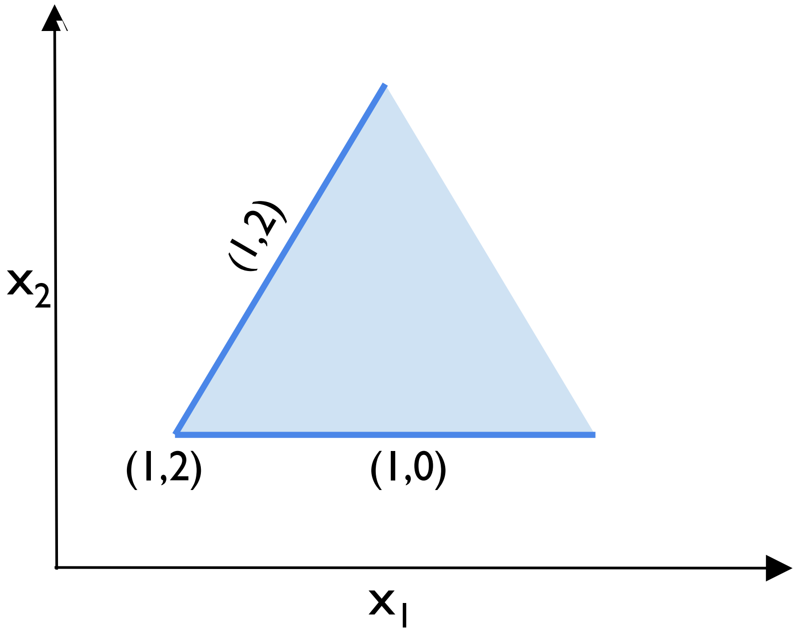
Constraints



$\mathcal{C} = \{-x_2 \leq -2, x_2 \leq 2x_1\}$

m: number of constraints

Generators



Vertices $\mathcal{V} = \{(1,2)\}$,

Rays $\mathcal{R} = \{(1,2), (1,0)\}$,

Lines $\mathcal{Z} = \emptyset$

g: number of generators

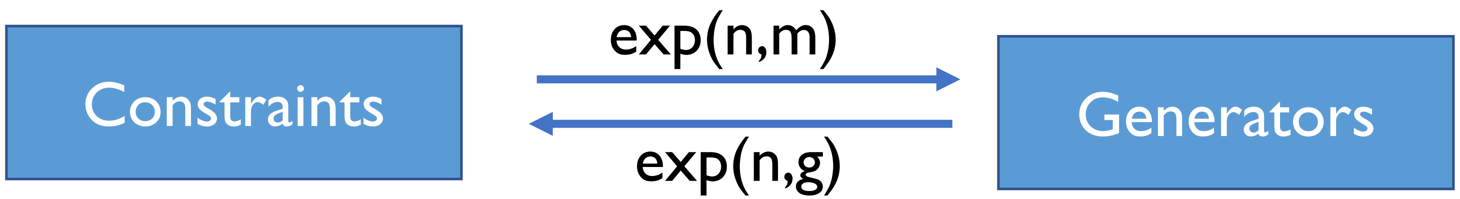
Asymptotic Time Complexity of Polyhedra

Asymptotic Time Complexity of Polyhedra

Operator	Constraints	Generators	Both
Join (⊔)	exp(n,m)	$O(ng)$	$O(ng)$
Meet (⊓)	$O(nm)$	exp(n,g)	$O(nm)$
Inclusion (⊑)	exp(n,m)	exp(n,g)	$O(ngm)$
Assignment	$O(nm^2)$	$O(ng)$	$O(ng)$
Conditional	$O(n)$	exp(n,g)	$O(n)$

Asymptotic Time Complexity of Polyhedra

Operator	Constraints	Generators	Both
Join (⊔)	*exp(n,m)*	$O(ng)$	$O(ng)$
Meet (⊓)	$O(nm)$	*exp(n,g)*	$O(nm)$
Inclusion (⊑)	*exp(n,m)*	*exp(n,g)*	$O(ngm)$
Assignment	$O(nm^2)$	$O(ng)$	$O(ng)$
Conditional	$O(n)$	*exp(n,g)*	$O(n)$



Key Idea: Online Decomposition

Key Idea: Online Decomposition

Polyhedron

$\{x_1 \leq 2x_2,$
$x_2 = 2,$
$x_1 + x_2 + 2x_3 \leq 5,$

$x_4 - x_5 \leq 3,$
$x_5 = 1,$

$x_6 = 2\}$

Key Idea: Online Decomposition

Polyhedron

$\{x_1 \leq 2x_2,$
$x_2 = 2,$
$x_1 + x_2 + 2x_3 \leq 5,$
$x_4 - x_5 \leq 3,$
$x_5 = 1,$
$x_6 = 2\}$

Set of factors

$\{x_1 \leq 2x_2,$
$x_2 = 2,$
$x_1 + x_2 + 2x_3 \leq 5\}$

$\{x_4 - x_5 \leq 3,$
$x_5 = 1\}$

$\{x_6 = 2\}$

Key Idea: Online Decomposition

Polyhedron

$\{x_1 \leq 2x_2,$
$x_2 = 2,$
$x_1 + x_2 + 2x_3 \leq 5,$
$x_4 - x_5 \leq 3,$
$x_5 = 1,$
$x_6 = 2\}$

Set of factors

$\{x_1 \leq 2x_2,$
$x_2 = 2,$
$x_1 + x_2 + 2x_3 \leq 5\}$

$\{x_4 - x_5 \leq 3,$
$x_5 = 1\}$

$\{x_6 = 2\}$

Partition (π) = set of blocks

$\{x_1, x_2, x_3\}$

$\{x_4, x_5\}$

$\{x_6\}$

Key Idea: Online Decomposition

Polyhedron

$\{x_1 \leq 2x_2,$
$x_2 = 2,$
$x_1 + x_2 + 2x_3 \leq 5,$
$x_4 - x_5 \leq 3,$
$x_5 = 1,$
$x_6 = 2\}$

Set of factors

$\{x_1 \leq 2x_2,$
$x_2 = 2,$
$x_1 + x_2 + 2x_3 \leq 5\}$

$\{x_4 - x_5 \leq 3,$
$x_5 = 1\}$

$\{x_6 = 2\}$

Partition (π) = set of blocks

$\{x_1, x_2, x_3\}$

$\{x_4, x_5\}$

$\{x_6\}$

working on smaller Polyhedra enables reduction in space and time

Permissible Partitions

Permissible Partitions

Polyhedron

$\{x_1 \leq 2x_2,$
$x_2 = 2,$
$x_1 + x_2 + 2x_3 \leq 5,$

$x_4 - x_5 \leq 3,$
$x_5 = 1,$

$x_6 = 2\}$

Permissible Partitions

Polyhedron	Best (finest) partition (π)
$\{x_1 \leq 2x_2,$ $x_2 = 2,$ $x_1 + x_2 + 2x_3 \leq 5,$	$\{x_1, x_2, x_3\}$
$x_4 - x_5 \leq 3,$ $x_5 = 1,$	$\{x_4, x_5\}$
$x_6 = 2\}$	$\{x_6\}$

Permissible Partitions

Polyhedron	Best (finest) partition (π)	Permissible partition ($\overline{\pi}$)
$\{x_1 \leq 2x_2,$ $x_2 = 2,$ $x_1 + x_2 + 2x_3 \leq 5,$	$\{x_1, x_2, x_3\}$	$\{x_1, x_2, x_3\}$
$x_4 - x_5 \leq 3,$ $x_5 = 1,$	$\{x_4, x_5\}$	$\{x_4, x_5, x_6\}$
$x_6 = 2\}$	$\{x_6\}$	

Permissible Partitions

Polyhedron	Best (finest) partition (π)	Permissible partition ($\overline{\pi}$)	Invalid partition
$\{x_1 \leq 2x_2,$ $x_2 = 2,$ $x_1 + x_2 + 2x_3 \leq 5,$	$\{x_1, x_2, x_3\}$	$\{x_1, x_2, x_3\}$	$\{x_1, x_2\}$
$x_4 - x_5 \leq 3,$ $x_5 = 1,$	$\{x_4, x_5\}$	$\{x_4, x_5, x_6\}$	$\{x_3, x_4, x_5\}$
$x_6 = 2\}$	$\{x_6\}$		$\{x_6\}$

Permissible Partitions

Polyhedron	Best (finest) partition (π)	Permissible partition ($\overline{\pi}$)	Invalid partition
$\{x_1 \leq 2x_2,$ $x_2 = 2,$ $x_1 + x_2 + 2x_3 \leq 5,$	$\{x_1, x_2, x_3\}$	$\{x_1, x_2, x_3\}$	$\{x_1, x_2\}$
$x_4 - x_5 \leq 3,$ $x_5 = 1,$	$\{x_4, x_5\}$	$\{x_4, x_5, x_6\}$	$\{x_3, x_4, x_5\}$
$x_6 = 2\}$	$\{x_6\}$		$\{x_6\}$

Definition: *A partition π is permissible for Polyhedron P, if there are no two variables x_i and x_j in different blocks of π related by a constraint in P*

Partition of Variable Set: Summary

Partition of Variable Set: Summary

The set of all partitions of variable set $\mathcal{X}$ form a lattice ordered by "*finer than*" (<) relation

The best (finest) partition π_P for Polyhedron P is unique

Any $\overline{\pi}$, s.t., $\pi_P < \overline{\pi}$, is permissible

An unconstrained variable x_i yields a singleton set $\{x_i\}$ in the partition

Partition of Variable Set: Summary

The set of all partitions of variable set $\mathcal{X}$ form a lattice ordered by "*finer than*" (<) relation

The best (finest) partition π_P for Polyhedron P is unique

Any $\overline{\pi}$, s.t., $\pi_P < \overline{\pi}$, is permissible

An unconstrained variable x_i yields a singleton set $\{x_i\}$ in the partition

Challenge: maintain permissible partitions for > 30 operators

Operator: Conditional

Operator: Conditional

Definition: *Let* π *be a partition and* $\mathcal{B}$ *be a block, then* $\pi \uparrow \mathcal{B}$ *is the finest partition* π' *such that* $\pi \sqsubseteq \pi$' *and* $\mathcal{B}$ *is a subset of an element of* π'

Theorem (finest partition after conditional):

If $O \neq \perp$ *and let* $\mathcal{B}$ *be block containing all variables appearing in the conditional, then* $\pi_O = \pi_P \uparrow \mathcal{B}$

Operator: Conditional

Definition: *Let π be a partition and $\mathcal{B}$ be a block, then $\pi \uparrow \mathcal{B}$ is the finest partition π' such that $\pi \sqsubseteq \pi$' and $\mathcal{B}$ is a subset of an element of π'*

P	π_P
$\{x_1 \leq 2x_2,$ $x_2 = 2,$ $x_1 + x_2 + 2x_3 \leq 5\}$	$\{x_1, x_2, x_3\}$
$\{x_4 - x_5 \leq 3,$ $x_5 = 1\}$	$\{x_4, x_5\}$
$\{x_6 = 2\}$	$\{x_6\}$

Theorem (finest partition after conditional):

If O $\neq \perp$ and let $\mathcal{B}$ be block containing all variables appearing in the conditional, then $\pi_O = \pi_P \uparrow \mathcal{B}$

Operator: Conditional

Definition: *Let π be a partition and $\mathcal{B}$ be a block, then $\pi \uparrow \mathcal{B}$ is the finest partition π' such that $\pi \sqsubseteq \pi$' and $\mathcal{B}$ is a subset of an element of π'*

P	π_P
$\{x_1 \leq 2x_2,$ $x_2 = 2,$ $x_1 + x_2 + 2x_3 \leq 5\}$	$\{x_1, x_2, x_3\}$
$\{x_4 - x_5 \leq 3,$ $x_5 = 1\}$	$\{x_4, x_5\}$
$\{x_6 = 2\}$	$\{x_6\}$

if($x_2 \leq 2x_4$)

Theorem (finest partition after conditional):

If O $\neq \perp$ and let $\mathcal{B}$ be block containing all variables appearing in the conditional, then $\pi_O = \pi_P \uparrow \mathcal{B}$

Operator: Conditional

Definition: *Let π be a partition and $\mathcal{B}$ be a block, then $\pi \uparrow \mathcal{B}$ is the finest partition π' such that $\pi \sqsubseteq \pi$' and $\mathcal{B}$ is a subset of an element of π'*

P	π_P
$\{x_1 \leq 2x_2,$ $x_2 = 2,$ $x_1 + x_2 + 2x_3 \leq 5\}$	$\{x_1, x_2, x_3\}$
$\{x_4 - x_5 \leq 3,$ $x_5 = 1\}$	$\{x_4, x_5\}$
$\{x_6 = 2\}$	$\{x_6\}$

if($x_2 \leq 2x_4$) →

O	π_O
$\{x_1 \leq 2x_2,$ $x_2 = 2,$ $x_1 + x_2 + 2x_3 \leq 5,$ $x_4 - x_5 \leq 3,$ $x_5 = 1,$ $x_2 \leq 2x_4\}$	$\{x_1, x_2, x_3,$ $x_4, x_5\}$
$\{x_6 = 2\}$	$\{x_6\}$

Theorem (finest partition after conditional):

If O $\neq \perp$ and let $\mathcal{B}$ be block containing all variables appearing in the conditional, then $\pi_O = \pi_P \uparrow \mathcal{B}$

Operator: Conditional

Definition: *Let π be a partition and $\mathcal{B}$ be a block, then $\pi \uparrow \mathcal{B}$ is the finest partition π' such that $\pi \sqsubseteq \pi'$ and $\mathcal{B}$ is a subset of an element of π'*

P	π_P		O	π_O
$\{x_1 \le 2x_2,\ x_2 = 2,\ x_1 + x_2 + 2x_3 \le 5\}$	$\{x_1, x_2, x_3\}$	if($x_2 \le 2x_4$) → $\mathcal{B} = \{x_2, x_4\}$	$\{x_1 \le 2x_2,\ x_2 = 2,\ x_1 + x_2 + 2x_3 \le 5,\ x_4 - x_5 \le 3,\ x_5 = 1,\ x_2 \le 2x_4\}$	$\{x_1, x_2, x_3, x_4, x_5\}$
$\{x_4 - x_5 \le 3,\ x_5 = 1\}$	$\{x_4, x_5\}$			
$\{x_6 = 2\}$	$\{x_6\}$		$\{x_6 = 2\}$	$\{x_6\}$

Theorem (finest partition after conditional):

If O $\neq \perp$ and let $\mathcal{B}$ be block containing all variables appearing in the conditional, then $\pi_O = \pi_P \uparrow \mathcal{B}$

Operator: Assignment

Operator: Assignment

P	π_P
$\{x_1 \leq 2x_2,$ $x_2 = 2,$ $x_1 + x_2 + 2x_3 \leq 5\}$	$\{x_1, x_2, x_3\}$
$\{x_4 - x_5 \leq 3,$ $x_5 = 1\}$	$\{x_4, x_5\}$
$\{x_6 = 2\}$	$\{x_6\}$

Operator: Assignment

P

$\{x_1 \leq 2x_2,$
$x_2 = 2,$
$x_1 + x_2 + 2x_3 \leq 5\}$

$\{x_4 - x_5 \leq 3,$
$x_5 = 1\}$

$\{x_6 = 2\}$

π_P

$\{x_1, x_2, x_3\}$

$\{x_4, x_5\}$

$\{x_6\}$

$x_2 := 2x_4$

Operator: Assignment

P	π_P		O	π_O
$\{x_1 \leq 2x_2,$ $x_2 = 2,$ $x_1 + x_2 + 2x_3 \leq 5\}$	$\{x_1, x_2, x_3\}$		$\{x_1 \leq 4,$ $x_1 + 2x_3 \leq 3,$	$\{x_1, x_3\}$
$\{x_4 - x_5 \leq 3,$ $x_5 = 1\}$	$\{x_4, x_5\}$	$x_2 := 2x_4$ →	$\{x_4 - x_5 \leq 3,$ $x_5 = 1,$ $x_2 = 2x_4\}$	$\{x_2, x_4, x_5\}$
$\{x_6 = 2\}$	$\{x_6\}$		$\{x_6 = 2\}$	$\{x_6\}$

Operator: Assignment

P	π_P		O	π_O
$\{x_1 \leq 2x_2,$ $x_2 = 2,$ $x_1 + x_2 + 2x_3 \leq 5\}$	$\{x_1, x_2, x_3\}$		$\{x_1 \leq 4,$ $x_1 + 2x_3 \leq 3,$	$\{x_1, x_3\}$
$\{x_4 - x_5 \leq 3,$ $x_5 = 1\}$	$\{x_4, x_5\}$	$x_2 := 2x_4$ →	$\{x_4 - x_5 \leq 3,$ $x_5 = 1,$ $x_2 = 2x_4\}$	$\{x_2, x_4, x_5\}$
$\{x_6 = 2\}$	$\{x_6\}$		$\{x_6 = 2\}$	$\{x_6\}$

Theorem (finest partition after assignment):

Let $\mathcal{B}$ be block containing all variables appearing for assignment $\boldsymbol{x_i} := \boldsymbol{e}$, and let π_i = $\{\mathcal{X} \setminus \{\boldsymbol{x_i}\}, \{\boldsymbol{x_i}\}\}$, then $\pi_O = (\pi_P \sqcap \pi_i) \uparrow \mathcal{B}$

Operator: Assignment

P	π_P		O	π_O
$\{x_1 \leq 2x_2,$ $x_2 = 2,$ $x_1 + x_2 + 2x_3 \leq 5\}$	$\{x_1, x_2, x_3\}$		$\{x_1 \leq 4,$ $x_1 + 2x_3 \leq 3,$	$\{x_1, x_3\}$
$\{x_4 - x_5 \leq 3,$ $x_5 = 1\}$	$\{x_4, x_5\}$	$x_2 := 2x_4$ → $\mathcal{B} = \{x_2, x_4\}$	$\{x_4 - x_5 \leq 3,$ $x_5 = 1,$ $x_2 = 2x_4\}$	$\{x_2, x_4, x_5\}$
$\{x_6 = 2\}$	$\{x_6\}$		$\{x_6 = 2\}$	$\{x_6\}$

Theorem (finest partition after assignment):

Let $\mathcal{B}$ be block containing all variables appearing for assignment $x_i := e$, and let $\pi_i = \{\mathcal{X} \setminus \{x_i\}, \{x_i\}\}$, then $\pi_O = (\pi_P \sqcap \pi_i) \uparrow \mathcal{B}$

Lattice Operators

Lattice Operators

Theorem (finest partition for $\sqsubseteq$):

If $P \sqsubseteq Q$ *and* $P \neq \bot$*, then* $\pi_Q \sqsubseteq \pi_P$

Theorem: **(finest partition after $\sqcap$)**:

If $P \sqcap Q \neq \bot$ *, then* $\pi_O = \pi_P \sqcup \pi_Q$

For join ($\sqcup$), no general relationship exists between π_O, π_P and π_Q

Operator: Join ($\sqcup$)

Operator: Join ($\sqcup$)

P	π_P
$\{x_1 - x_2 \leq 0, x_1 \leq 0\}$	$\{x_1, x_2\}$
$\{x_3 = 1\}$	$\{x_3\}$

Operator: Join ($\sqcup$)

P

$\{x_1 - x_2 \leq 0,$
$x_1 \leq 0\}$

$\{x_3 = 1\}$

π_P

$\{x_1, x_2\}$

$\sqcup$

$\{x_3\}$

Operator: Join ($\sqcup$)

P	π_P		Q	π_Q
$\{x_1 - x_2 \leq 0, x_1 \leq 0\}$	$\{x_1, x_2\}$	$\sqcup$	$\{x_1 \leq 2\}$	$\{x_1\}$
			$\emptyset$	$\{x_2\}$
$\{x_3 = 1\}$	$\{x_3\}$		$\{x_3 = 0\}$	$\{x_3\}$

Operator: Join ($\sqcup$)

P	π_P		Q	π_Q		O	π_O
$\{x_1 - x_2 \leq 0, x_1 \leq 0\}$	$\{x_1, x_2\}$	$\sqcup$	$\{x_1 \leq 2\}$	$\{x_1\}$	$\Rightarrow$	$\{x_1 + 2x_3 \leq 2, -x_3 \leq 0, x_3 \leq 1\}$	$\{x_1, x_3\}$
			$\emptyset$	$\{x_2\}$		$\emptyset$	$\{x_2\}$
$\{x_3 = 1\}$	$\{x_3\}$		$\{x_3 = 0\}$	$\{x_3\}$			

Operator: Join ($\sqcup$)

P	π_P		Q	π_Q		O	π_O
$\{x_1 - x_2 \leq 0, x_1 \leq 0\}$	$\{x_1, x_2\}$		$\{x_1 \leq 2\}$	$\{x_1\}$		$\{x_1 + 2x_3 \leq 2, -x_3 \leq 0, x_3 \leq 1\}$	$\{x_1, x_3\}$
		$\sqcup$	$\emptyset$	$\{x_2\}$	$\Rightarrow$	$\emptyset$	$\{x_2\}$
$\{x_3 = 1\}$	$\{x_3\}$		$\{x_3 = 0\}$	$\{x_3\}$			

$$\pi_P \sqcup \pi_Q = \pi_P \neq \pi_O$$

Operator: Join ($\sqcup$)

P	π_P		Q	π_Q		O	π_O
$\{x_1 - x_2 \leq 0,\ x_1 \leq 0\}$	$\{x_1, x_2\}$	$\sqcup$	$\{x_1 \leq 2\}$	$\{x_1\}$	$\Rightarrow$	$\{x_1 + 2x_3 \leq 2,\ -x_3 \leq 0,\ x_3 \leq 1\}$	$\{x_1, x_3\}$
			$\emptyset$	$\{x_2\}$		$\emptyset$	$\{x_2\}$
$\{x_3 = 1\}$	$\{x_3\}$		$\{x_3 = 0\}$	$\{x_3\}$			

$$\pi_P \sqcup \pi_Q = \pi_P \neq \pi_O$$

$$\pi_P \sqcap \pi_Q = \pi_Q \neq \pi_O$$

Operator: Join ($\sqcup$)

P	π_P		Q	π_Q		O	π_O
$\{x_1 - x_2 \leq 0,\ x_1 \leq 0\}$	$\{x_1, x_2\}$	$\sqcup$	$\{x_1 \leq 2\}$	$\{x_1\}$	$\Rightarrow$	$\{x_1 + 2x_3 \leq 2,\ -x_3 \leq 0,\ x_3 \leq 1\}$	$\{x_1, x_3\}$
			$\emptyset$	$\{x_2\}$		$\emptyset$	$\{x_2\}$
$\{x_3 = 1\}$	$\{x_3\}$		$\{x_3 = 0\}$	$\{x_3\}$			

$$\pi_P \sqcup \pi_Q = \pi_P \neq \pi_O$$

$$\pi_P \sqcap \pi_Q = \pi_Q \neq \pi_O$$

For Join, π_O depends on both P and Q

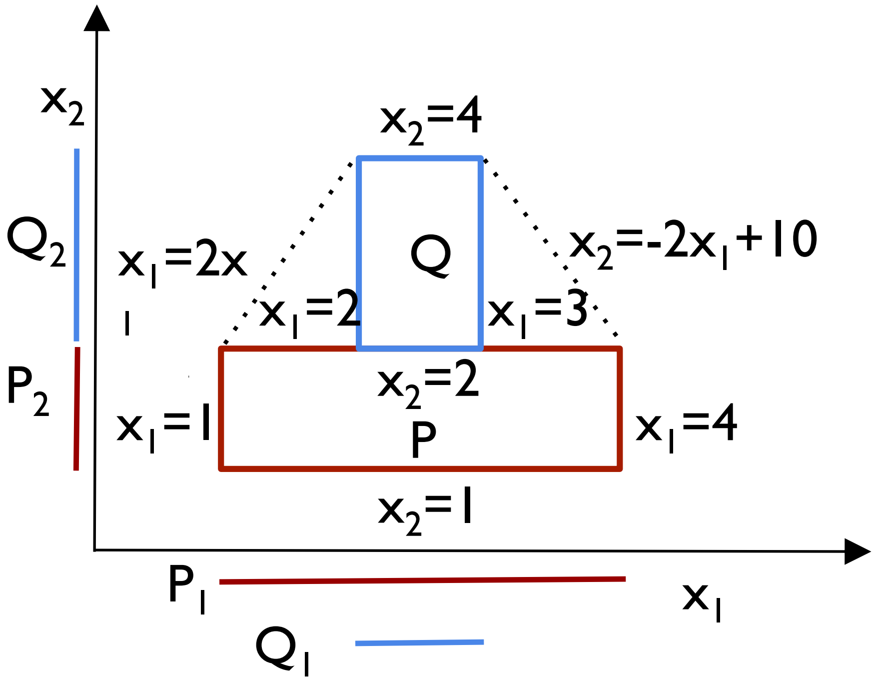
Operator: Join ($\sqcup$)

Operator: Join ($\sqcup$)

Theorem: *Let P and Q be two Polyhedra with the same permissible partition* $\pi = \{\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_r\}$ *and let* $\overline{\pi}$ *be a permissible partition for the join, that is,* $\pi_{P \sqcup Q} \sqsubseteq \overline{\pi}$. *If for any block* $\mathcal{X}_k \in \pi$, $P_k = Q_k$, *then* $\mathcal{X}_k \in \overline{\pi}$

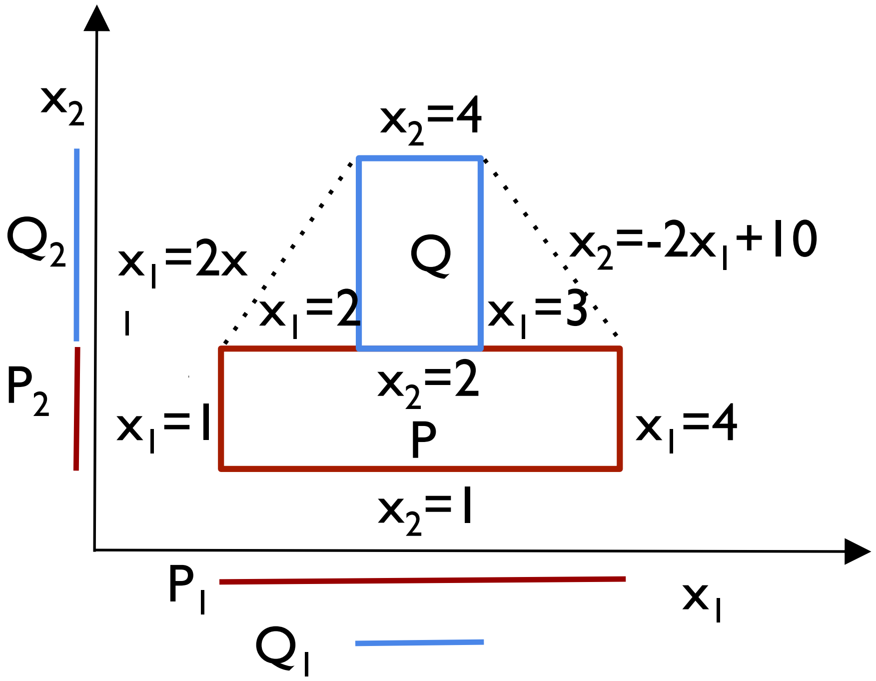
Operator: Join (⊔)

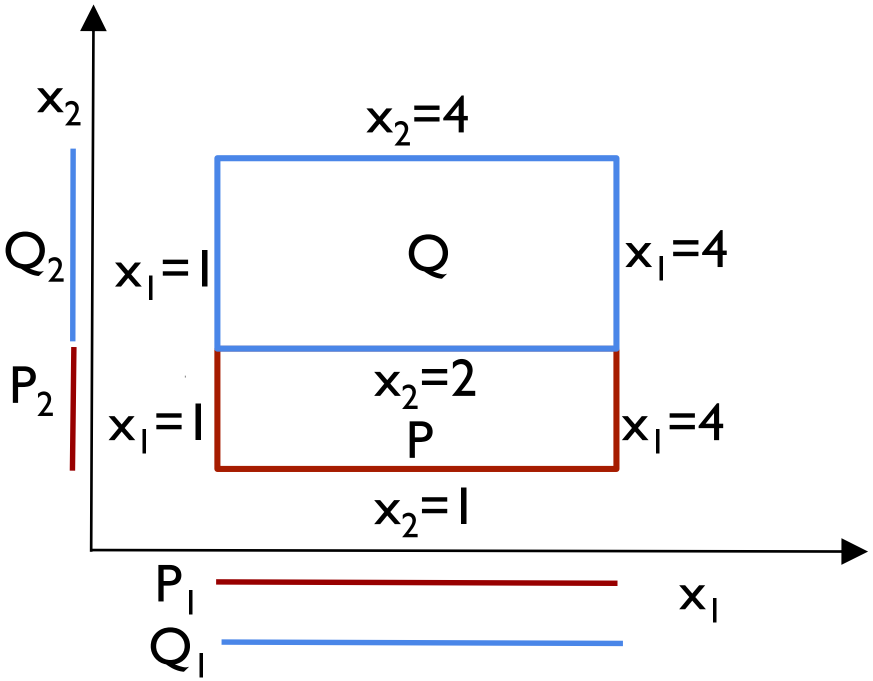
Theorem: *Let P and Q be two Polyhedra with the same permissible partition* $\pi = \{\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_r\}$ *and let* $\overline{\pi}$ *be a permissible partition for the join, that is,* $\pi_{P \sqcup Q} \sqsubseteq \overline{\pi}$. *If for any block* $\mathcal{X}_k \in \pi$, $P_k = Q_k$, *then* $\mathcal{X}_k \in \overline{\pi}$



Operator: Join (⊔)

Theorem: *Let P and Q be two Polyhedra with the same permissible partition* $\pi = \{\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_r\}$ *and let* $\overline{\pi}$ *be a permissible partition for the join, that is,* $\pi_{P \sqcup Q} \sqsubseteq \overline{\pi}$. *If for any block* $\mathcal{X}_k \in \pi$, $P_k = Q_k$, *then* $\mathcal{X}_k \in \overline{\pi}$





Operators with Permissible Partitions

Operators with Permissible Partitions

Theorem (permissible partition after join):

Let $\overline{\pi} = \overline{\pi}_P \sqcup \overline{\pi}_Q$ and $\mathcal{U} = \{\mathcal{X}_k \mid P_k = Q_k, \mathcal{X}_k \in \overline{\pi}\}$.

Then $\overline{\pi}_{P \sqcup Q} = \mathcal{U} \cup \biguplus_{\mathcal{T} \in \overline{\pi} \setminus \mathcal{U}} \mathcal{T}$ *is permissible for* $P \sqcup Q$

Theorem (permissible partition after meet):

$\overline{\pi}_P \sqcup \overline{\pi}_Q$ *is permissible for* $P \sqcap Q$

Theorem (permissible partition after conditional):

If output $O \neq \perp$, then, $\overline{\pi}_P \uparrow \mathcal{B}$ *is permissible for conditional*

Theorem (permissible partition after assignment):

$\overline{\pi}_P \uparrow \mathcal{B}$ *is permissible for the output O of assignment*

Asymptotic Complexity of Operators with Permissible Partitions

Operator	Before (using both)	Our work (using decomposition)
Join ($\sqcup$)	$O(ng)$	$O(\sum_{i=1}^{r} n_i m_i g_i + n_{max} m_{max})$
Meet ($\sqcap$)	$O(nm)$	$O(\sum_{i=1}^{r} n_i m_i)$
Inclusion ($\sqsubseteq$)	$O(ngm)$	$O(\sum_{i=1}^{r} n_i m_i g_i)$
Assignment	$O(ng)$	$O(n_{max} g_{max})$
Conditional	$O(n)$	$O(n_{max})$
Conversion	$exp(n,g)$	$exp(n_{max}, g_{max})$

r: number of blocks

Experimental Evaluation

We compared performance of ELINA against NewPolka and PPL

Using the Seahorn verification framework [CAV'15]

- written in C, analyzes llvm-bitcode
- produces Polyhedra invariants

> 1500 benchmarks from the software verification competition

Time limit: 4 hours

Memory limit: 12 GB

Experimental Evaluation

Experimental Evaluation

Benchmark	Category	LOC	NewPolka		PPL		ELINA		Speedup ELINA vs.	
			time(s)	memory(GB)	time(s)	memory(GB)	time(s)	memory(GB)	NewPolka	PPL
firewire_firedtv	LD	14506	1367	1.7	331	0.9	0.4	0.2	3343	828
net_fddi_skfp	LD	30186	5041	11.2	6142	7.2	9.2	0.9	547	668
mtd_ubi	LD	39334	3633	7	MO	MO	4	0.9	908	>38
usb_core_main0	LD	52152	11084	2.7	4003	1.4	65	2	170	62
tty_synclinkmp	LD	19288	TO	TO	MO	MO	3.4	0.1	>4235	>1186
scsi_advansys	LD	21538	TO	TO	TO	TO	4	0.4	>3600	>3600
staging_vt6656	LD	25340	TO	TO	TO	TO	2	0.4	>7200	>7200
net_ppp	LD	15744	TO	TO	10530	0.15	924	0.3	>16	11.4
p10_l00	CF	592	841	4.2	121	0.9	11	0.8	76	11
p16_l40	CF	1783	MO	MO	MO	MO	11	3	>69	>24
p12_l57	CF	4828	MO	MO	MO	MO	14	0.8	>71	>15
p13_l53	CF	5816	MO	MO	MO	MO	54	2.7	>50	>26
p19_l59	CF	9794	MO	MO	MO	MO	70	1.7	>15	>4
ddv_all	HM	6532	710	1.4	85	0.5	0.05	0.1	12772	1700

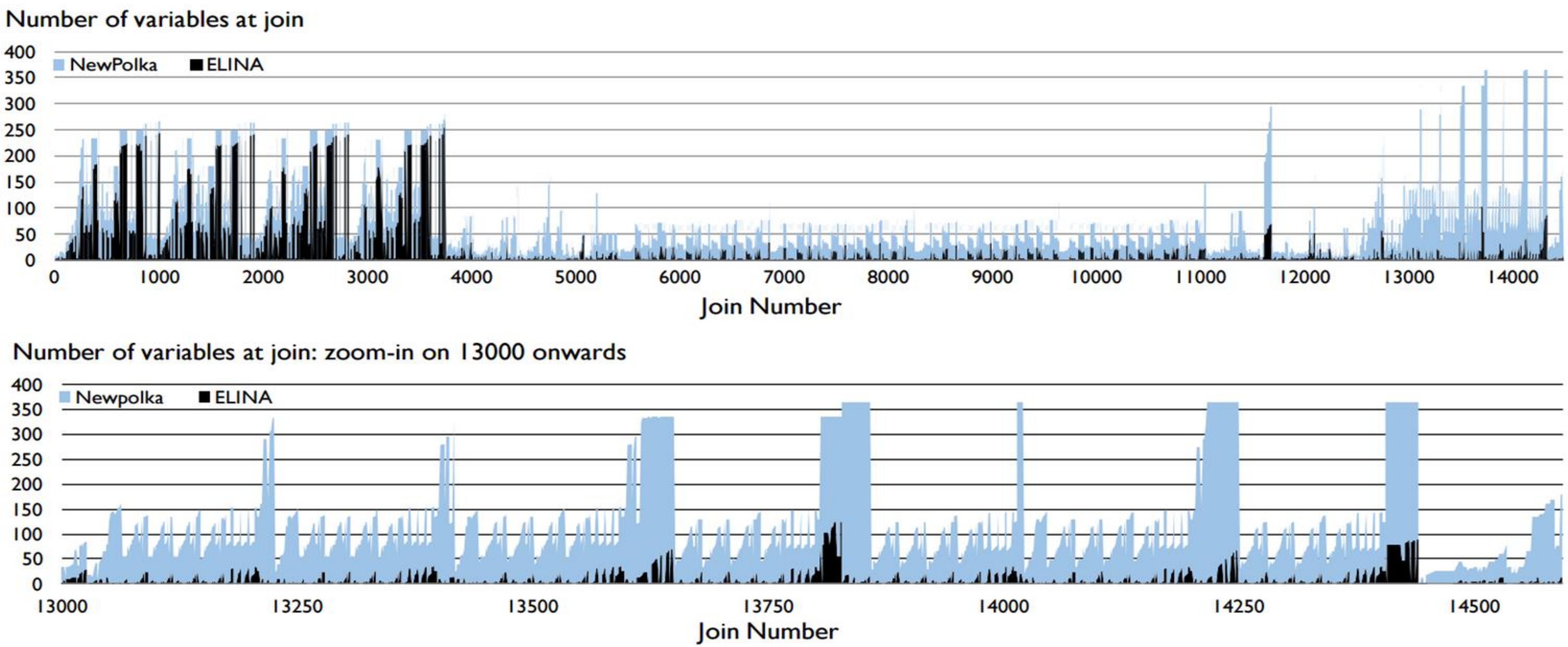
Experimental Evaluation

Benchmark	Category	LOC	NewPolka		PPL		ELINA		Speedup ELINA vs.	
			time(s)	memory(GB)	time(s)	memory(GB)	time(s)	memory(GB)	NewPolka	PPL
firewire_firedtv	LD	14506	1367	1.7	331	0.9	0.4	0.2	3343	828
net_fddi_skfp	LD	30186	5041	11.2	6142	7.2	9.2	0.9	547	668
mtd_ubi	LD	39334	3633	7	MO	MO	4	0.9	908	>38
usb_core_main0	LD	52152	11084	2.7	4003	1.4	65	2	170	62
tty_synclinkmp	LD	19288	TO	TO	MO	MO	3.4	0.1	>4235	>1186
scsi_advansys	LD	21538	TO	TO	TO	TO	4	0.4	>3600	>3600
staging_vt6656	LD	25340	TO	TO	TO	TO	2	0.4	>7200	>7200
net_ppp	LD	15744	TO	TO	10530	0.15	924	0.3	>16	11.4
p10_l00	CF	592	841	4.2	121	0.9	11	0.8	76	11
p16_l40	CF	1783	MO	MO	MO	MO	11	3	>69	>24
p12_l57	CF	4828	MO	MO	MO	MO	14	0.8	>71	>15
p13_l53	CF	5816	MO	MO	MO	MO	54	2.7	>50	>26
p19_l59	CF	9794	MO	MO	MO	MO	70	1.7	>15	>4
ddv_all	HM	6532	710	1.4	85	0.5	0.05	0.1	12772	1700

Experimental Evaluation

Benchmark	Category	LOC	NewPolka		PPL		ELINA		Speedup ELINA vs.	
			time(s)	memory(GB)	time(s)	memory(GB)	time(s)	memory(GB)	NewPolka	PPL
firewire_firedtv	LD	14506	1367	1.7	331	0.9	0.4	0.2	3343	828
net_fddi_skfp	LD	30186	5041	11.2	6142	7.2	9.2	0.9	547	668
mtd_ubi	LD	39334	3633	7	MO	MO	4	0.9	908	>38
usb_core_main0	LD	52152	11084	2.7	4003	1.4	65	2	170	62
tty_synclinkmp	LD	19288	TO	TO	MO	MO	3.4	0.1	>4235	>1186
scsi_advansys	LD	21538	TO	TO	TO	TO	4	0.4	>3600	>3600
staging_vt6656	LD	25340	TO	TO	TO	TO	2	0.4	>7200	>7200
net_ppp	LD	15744	TO	TO	10530	0.15	924	0.3	>16	11.4
p10_l00	CF	592	841	4.2	121	0.9	11	0.8	76	11
p16_l40	CF	1783	MO	MO	MO	MO	11	3	>69	>24
p12_l57	CF	4828	MO	MO	MO	MO	14	0.8	>71	>15
p13_l53	CF	5816	MO	MO	MO	MO	54	2.7	>50	>26
p19_l59	CF	9794	MO	MO	MO	MO	70	1.7	>15	>4
ddv_all	HM	6532	710	1.4	85	0.5	0.05	0.1	12772	1700

Evaluation



$n_{ELINA} < n_{NewPolka}$, large speedup as conversion is exponential in n

Related Work

Related Work

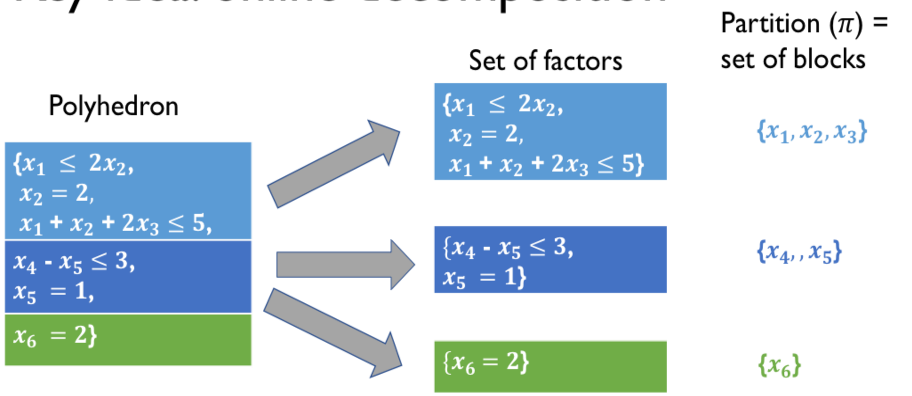
- Variable Packing
  - Blanchet et al. [PLDI’03]
  - decomposition based on syntactic criteria
  - loses precision

- Matrix based decomposition
  - Halbwachs et al. [FMSD’06]
  - does not work with generators
  - decomposition too coarse for join

Conclusion

Conclusion

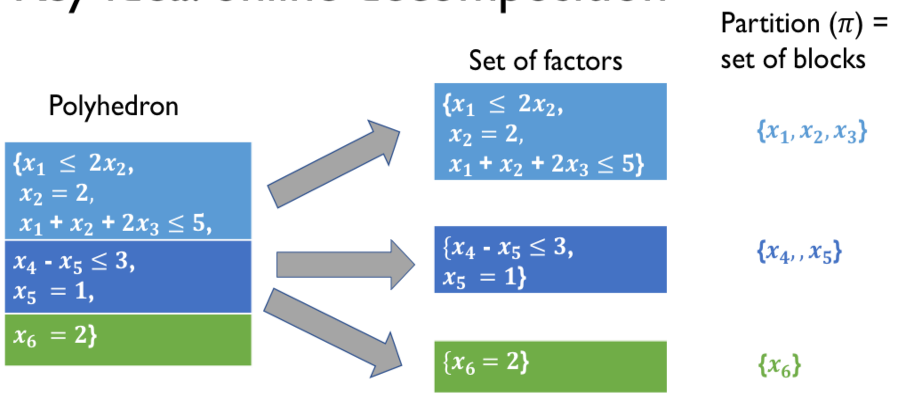
Key idea: online decomposition



Operators work on smaller Polyhedra: Complexity Reduction

Conclusion

Key idea: online decomposition

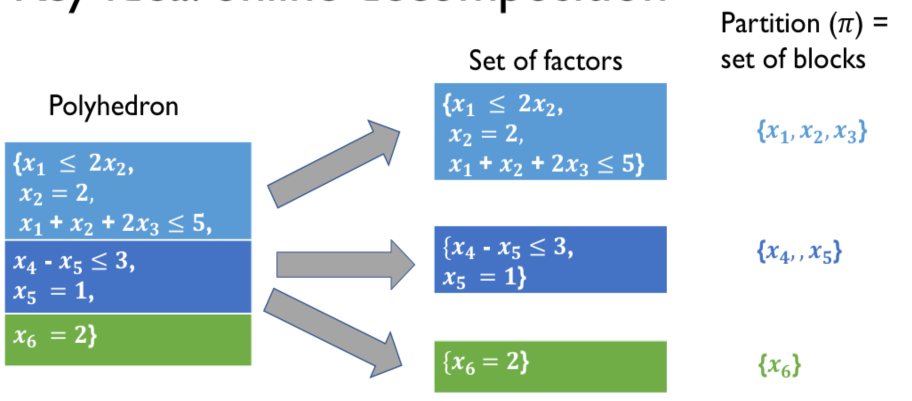


Operators work on smaller Polyhedra: Complexity Reduction

Operator	Both	Online decomposition
Join ($\sqcup$)	$O(ng)$	$O(\sum_{i=1}^{r} n_i m_i g_i + n_{max} m_{max})$
Meet ($\sqcap$)	$O(nm)$	$O(\sum_{i=1}^{r} n_i m_i)$
Inclusion ($\sqsubseteq$)	$O(ngm)$	$O(\sum_{i=1}^{r} n_i m_i g_i)$
Assignment	$O(ng)$	$O(n_{max} g_{max})$
Conditional	$O(n)$	$O(n_{max})$

Conclusion

Key idea: online decomposition



Operators work on smaller Polyhedra: Complexity Reduction

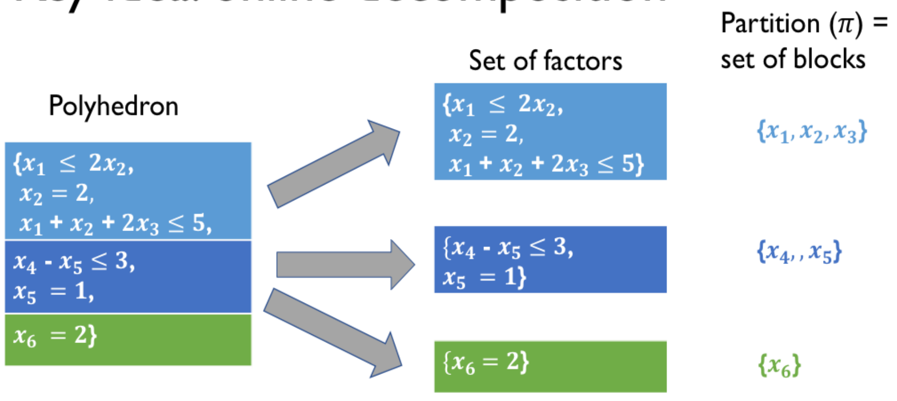
Operator	Both	Online decomposition
Join (⊔)	$O(ng)$	$O(\sum_{i=1}^{r} n_i m_i g_i + n_{max} m_{max})$
Meet (⊓)	$O(nm)$	$O(\sum_{i=1}^{r} n_i m_i)$
Inclusion (⊑)	$O(ngm)$	$O(\sum_{i=1}^{r} n_i m_i g_i)$
Assignment	$O(ng)$	$O(n_{max} g_{max})$
Conditional	$O(n)$	$O(n_{max})$

ELINA

http://elina.ethz.ch

Conclusion

Key idea: online decomposition



Operators work on smaller Polyhedra: Complexity Reduction

Operator	Both	Online decomposition
Join ($\sqcup$)	$O(ng)$	$O(\sum_{i=1}^{r} n_i m_i g_i + n_{max} m_{max})$
Meet ($\sqcap$)	$O(nm)$	$O(\sum_{i=1}^{r} n_i m_i)$
Inclusion ($\sqsubseteq$)	$O(ngm)$	$O(\sum_{i=1}^{r} n_i m_i g_i)$
Assignment	$O(ng)$	$O(n_{max} g_{max})$
Conditional	$O(n)$	$O(n_{max})$

ELINA

http://elina.ethz.ch

Driver	NewPolka	PPL	ELINA
➢ 500 var ➢ 39K LOC	OOM (> 12 GB)	OOM (> 12 GB)	4 sec 0.9 GB
➢ 650 var ➢ 25K LOC	TO (> 4 hr)	TO (> 4 hr)	2 sec 0.4 GB