Precise Widening Operators for Convex Polyhedra

Roberto BAGNARA, Patricia M. HILL,
Elisa RICCI, Enea ZAFFANELLA

University of Parma, Italy
University of Leeds, United Kingdom

http://www.cs.unipr.it/ppl/

Motivations

- ➜ Linear Relation Analysis is a key component of many static analysis and (semi-) automatic verification tools.

MOTIVATIONS

- ➜ Linear Relation Analysis is a key component of many static analysis and (semi-) automatic verification tools.
- ➜ Since it has infinite chains, the domain of convex polyhedra has to be provided with precise widening operators.

MOTIVATIONS

- ➜ Linear Relation Analysis is a key component of many static analysis and (semi-) automatic verification tools.
- ➜ Since it has infinite chains, the domain of convex polyhedra has to be provided with precise widening operators.
- ➜ The standard widening (Cousot and Halbwachs, POPL'78) is the one and only champion: since then, no challanger has been proposed.

Motivations

- ➜ Linear Relation Analysis is a key component of many static analysis and (semi-) automatic verification tools.
- ➜ Since it has infinite chains, the domain of convex polyhedra has to be provided with precise widening operators.
- ➜ The standard widening (Cousot and Halbwachs, POPL'78) is the one and only champion: since then, no challanger has been proposed.
- ➜ But some applications need more precision. Solutions include:
  1. the widening delay technique (Cousot, '81);
  2. the widening 'up to' technique (Halbwachs, CAV'93);
  3. various extrapolation operators (no convergence guarantee).

MOTIVATIONS

- ➜ Linear Relation Analysis is a key component of many static analysis and (semi-) automatic verification tools.
- ➜ Since it has infinite chains, the domain of convex polyhedra has to be provided with precise widening operators.
- ➜ The standard widening (Cousot and Halbwachs, POPL'78) is the one and only champion: since then, no challanger has been proposed.
- ➜ But some applications need more precision. Solutions include:
  - ① the widening delay technique (Cousot, '81);
  - ② the widening 'up to' technique (Halbwachs, CAV'93);
  - ③ various extrapolation operators (no convergence guarantee).
- ➜ Our goal: *provide a framework for the definition of new widening operators on convex polyhedra improving upon the precision of the standard widening.*

Different Goals for Widening Operators

As stated in Cousot and Cousot, J. of Logic and Computation, '92:

Different Goals for Widening Operators

As stated in Cousot and Cousot, J. of Logic and Computation, '92:

① Upper bound selection for abstract domains that are algebraically weak.

Different Goals for Widening Operators

As stated in Cousot and Cousot, J. of Logic and Computation, '92:

① Upper bound selection for abstract domains that are algebraically weak.

② *Provide the convergence guarantee for upward iteration sequences, i.e., ensuring convergence in a finite number of steps*.

DIFFERENT GOALS FOR WIDENING OPERATORS

As stated in Cousot and Cousot, J. of Logic and Computation, '92:

① Upper bound selection for abstract domains that are algebraically weak.

② *Provide the convergence guarantee for upward iteration sequences, i.e., ensuring convergence in a finite number of steps*.

③ For both infinite as well as finite abstract domains, speed up the convergence of upward iteration sequences.

DIFFERENT GOALS FOR WIDENING OPERATORS

As stated in Cousot and Cousot, J. of Logic and Computation, ’92:

① Upper bound selection for abstract domains that are algebraically weak.

② *Provide the convergence guarantee for upward iteration sequences, i.e., ensuring convergence in a finite number of steps*.

③ For both infinite as well as finite abstract domains, speed up the convergence of upward iteration sequences.

➜ *Real widenings do provide a convergence guarantee.*

➜ Operators not doing so are better called extrapolation operators.

Definition of Widening Operator

A variant of the classical one (see Cousot and Cousot, PLILP'92):

- The operator $\nabla : L \times L \rightarrowtail L$ is a widening if
  1. $\forall x, y \in L : x \sqsubseteq y \implies y \sqsubseteq x \nabla y$;
  2. for all increasing chains $y_0 \sqsubseteq y_1 \sqsubseteq \cdots$, the increasing chain defined by $x_0 \stackrel{\text{def}}{=} y_0, \ldots, x_{i+1} \stackrel{\text{def}}{=} x_i \nabla y_{i+1}, \ldots$ is not strictly increasing.

Definition of Widening Operator

A variant of the classical one (see Cousot and Cousot, PLILP'92):

- ➜ The operator $\nabla : L \times L \rightarrowtail L$ is a widening if
  - ① $\forall x, y \in L : x \sqsubseteq y \implies y \sqsubseteq x \nabla y$;
  - ② for all increasing chains $y_0 \sqsubseteq y_1 \sqsubseteq \cdots$, the increasing chain defined by $x_0 \stackrel{\text{def}}{=} y_0, \ldots, x_{i+1} \stackrel{\text{def}}{=} x_i \nabla y_{i+1}, \ldots$ is not strictly increasing.
- ➜ The upward iteration sequence with widenings (starting from $x_0 \in L$)

$$x_{i+1} = \begin{cases} x_i, & \text{if } \mathcal{F}(x_i) \sqsubseteq x_i; \\ x_i \nabla \big(x_i \sqcup \mathcal{F}(x_i)\big), & \text{otherwise;} \end{cases}$$

converges after a finite number of iterations.

Definition of Widening Operator

A variant of the classical one (see Cousot and Cousot, PLILP'92):

- The operator $\nabla : L \times L \rightarrowtail L$ is a widening if
  ① $\forall x, y \in L : x \sqsubseteq y \implies y \sqsubseteq x \nabla y$;
  ② for all increasing chains $y_0 \sqsubseteq y_1 \sqsubseteq \cdots$, the increasing chain defined by $x_0 \stackrel{\text{def}}{=} y_0, \ldots, x_{i+1} \stackrel{\text{def}}{=} x_i \nabla y_{i+1}, \ldots$ is not strictly increasing.
- The upward iteration sequence with widenings (starting from $x_0 \in L$)

$$x_{i+1} = \begin{cases} x_i, & \text{if } \mathcal{F}(x_i) \sqsubseteq x_i; \\ x_i \nabla \big(x_i \sqcup \mathcal{F}(x_i)\big), & \text{otherwise;} \end{cases}$$

  converges after a finite number of iterations.
- Note: ∇ always applied to arguments $x = x_i$ and $y = x_i \sqcup \mathcal{F}(x_i)$ satisfying $x \sqsubseteq y$ and $x \neq y$.

The Domain $\mathbb{CP}_n$ of Closed Convex Polyhedra

A lattice with respect to subset inclusion, with infinite chains.

THE DOMAIN $\mathbb{CP}_n$ OF CLOSED CONVEX POLYHEDRA

A lattice with respect to subset inclusion, with infinite chains.

Constraint Representation: $\mathcal{P} = \mathrm{con}(\mathcal{C})$

- $\mathcal{C}$ is a finite set of linear non-strict inequality (resp., equality) constraints.
- No redundant constraint $+$ max number of equalities $\Longrightarrow$ minimal form.
- Inequalities orthogonal wrt equalities $\Longrightarrow$ orthogonal form.

THE DOMAIN $\mathbb{CP}_n$ OF CLOSED CONVEX POLYHEDRA

A lattice with respect to subset inclusion, with infinite chains.

Constraint Representation: $\mathcal{P} = \mathrm{con}(\mathcal{C})$

- $\mathcal{C}$ is a finite set of linear non-strict inequality (resp., equality) constraints.
- No redundant constraint $+$ max number of equalities $\implies$ minimal form.
- Inequalities orthogonal wrt equalities $\implies$ orthogonal form.

Generator Representation: $\mathcal{P} = \mathrm{gen}(\mathcal{G})$

- $\mathcal{G} = (L, R, P)$, where
  - P is a finite set of points of $\mathcal{P}$;
  - R is a finite set of rays (directions of infinity) of $\mathcal{P}$;
  - L is a finite set of lines (bidirectional rays) of $\mathcal{P}$.
- No redundant generator $+$ max number of lines $\implies$ minimal form.
- Points and rays orthogonal wrt lines $\implies$ orthogonal form.

The Standard Widening ∇

- Initially proposed in Cousot and Halbwachs, POPL'78.
- Intuitively, $\mathcal{P}_1 \nabla \mathcal{P}_2$ *is defined by all the constraints of* $\mathcal{P}_1 = \mathrm{con}(\mathcal{C}_1)$ *that are also satisfied by* $\mathcal{P}_2$*.*

THE STANDARD WIDENING ∇

- Initially proposed in Cousot and Halbwachs, POPL'78.
- Intuitively, $\mathcal{P}_1 \nabla \mathcal{P}_2$ *is defined by all the constraints of* $\mathcal{P}_1 = \mathrm{con}(\mathcal{C}_1)$ *that are also satisfied by* $\mathcal{P}_2$.
- Improved in Halbwachs'79 (the PhD thesis), so that it does not depend on the chosen constraint representations.

THE STANDARD WIDENING ∇

- Initially proposed in Cousot and Halbwachs, POPL'78.
- Intuitively, $\mathcal{P}_1 \nabla \mathcal{P}_2$ *is defined by all the constraints of* $\mathcal{P}_1 = \mathrm{con}(\mathcal{C}_1)$ *that are also satisfied by* $\mathcal{P}_2$*.*
- Improved in Halbwachs'79 (the PhD thesis), so that it does not depend on the chosen constraint representations.
- The resulting operator is both precise and efficient: this "*tentative*" definition has been the one and only available approach for 25 years.

THE STANDARD WIDENING ∇

- Initially proposed in Cousot and Halbwachs, POPL'78.
- Intuitively, $\mathcal{P}_1 \nabla \mathcal{P}_2$ *is defined by all the constraints of* $\mathcal{P}_1 = \mathrm{con}(\mathcal{C}_1)$ *that are also satisfied by* $\mathcal{P}_2$*.*
- Improved in Halbwachs'79 (the PhD thesis), so that it does not depend on the chosen constraint representations.
- The resulting operator is both precise and efficient: this "*tentative*" definition has been the one and only available approach for 25 years.
- Can we improve its precision? (Perhaps, trading some efficiency.)

The Limited Growth Ordering Relation

➜ Variant of a well-founded ordering defined in Besson *et al.*, SAS'99.

The Limited Growth Ordering Relation

- Variant of a well-founded ordering defined in Besson *et al.*, SAS'99.
- For $i = 1, 2$, let $\mathcal{P}_i = \mathrm{con}(\mathcal{C}_i) = \mathrm{gen}(\mathcal{G}_i)$,
  where $\mathcal{C}_i$ is in minimal form and $\mathcal{G}_i = (L_i, R_i, P_i)$ is in orthogonal form;
- the relation $\mathcal{P}_1 \curvearrowright \mathcal{P}_2$ holds if and only if $\mathcal{P}_1 \subset \mathcal{P}_2$ and
  at least one of the following conditions holds:

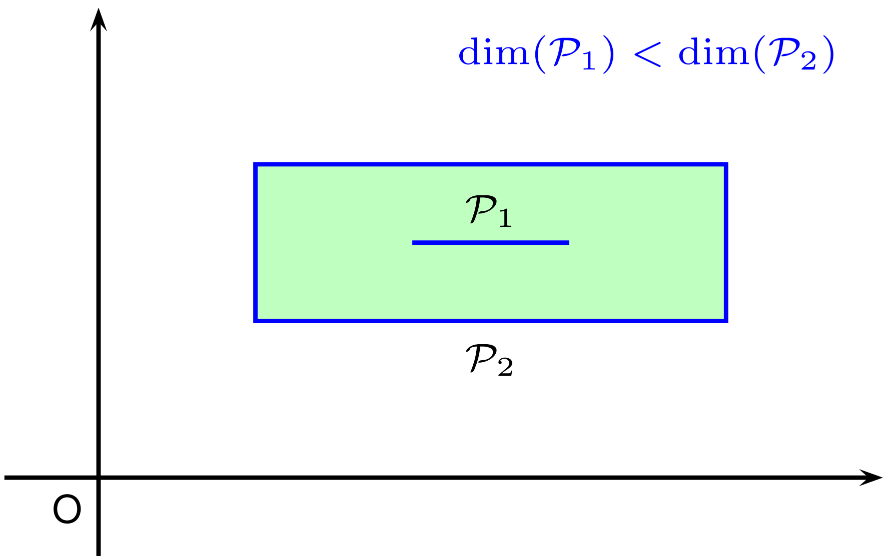
THE LIMITED GROWTH ORDERING RELATION

- Variant of a well-founded ordering defined in Besson *et al.*, SAS'99.
- For $i = 1, 2$, let $\mathcal{P}_i = \mathrm{con}(\mathcal{C}_i) = \mathrm{gen}(\mathcal{G}_i)$,
  where $\mathcal{C}_i$ is in minimal form and $\mathcal{G}_i = (L_i, R_i, P_i)$ is in orthogonal form;
- the relation $\mathcal{P}_1 \curvearrowright \mathcal{P}_2$ holds if and only if $\mathcal{P}_1 \subset \mathcal{P}_2$ and
  at least one of the following conditions holds:
  ① $\dim(\mathcal{P}_1) < \dim(\mathcal{P}_2)$;
  ② $\dim\bigl(\mathrm{lin.space}(\mathcal{P}_1)\bigr) < \dim\bigl(\mathrm{lin.space}(\mathcal{P}_2)\bigr)$;
  ③ $\# \mathcal{C}_1 > \# \mathcal{C}_2$;
  ④ $\# \mathcal{C}_1 = \# \mathcal{C}_2 \wedge \# P_1 > \# P_2$;
  ⑤ $\# \mathcal{C}_1 = \# \mathcal{C}_2 \wedge \# P_1 = \# P_2 \wedge \kappa(R_1) \gg \kappa(R_2)$.

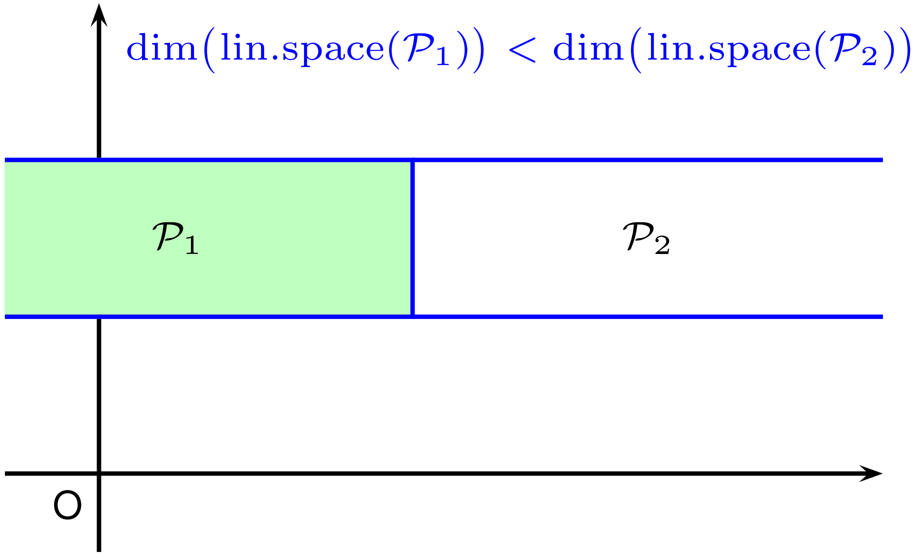
THE LIMITED GROWTH ORDERING RELATION

- Variant of a well-founded ordering defined in Besson *et al.*, SAS'99.
- For $i = 1, 2$, let $\mathcal{P}_i = \mathrm{con}(\mathcal{C}_i) = \mathrm{gen}(\mathcal{G}_i)$,
  where $\mathcal{C}_i$ is in minimal form and $\mathcal{G}_i = (L_i, R_i, P_i)$ is in orthogonal form;
- the relation $\mathcal{P}_1 \curvearrowright \mathcal{P}_2$ holds if and only if $\mathcal{P}_1 \subset \mathcal{P}_2$ and
  at least one of the following conditions holds:
  ① $\dim(\mathcal{P}_1) < \dim(\mathcal{P}_2)$;
  ② $\dim\bigl(\mathrm{lin.space}(\mathcal{P}_1)\bigr) < \dim\bigl(\mathrm{lin.space}(\mathcal{P}_2)\bigr)$;
  ③ $\#\mathcal{C}_1 > \#\mathcal{C}_2$;
  ④ $\#\mathcal{C}_1 = \#\mathcal{C}_2 \wedge \#P_1 > \#P_2$;
  ⑤ $\#\mathcal{C}_1 = \#\mathcal{C}_2 \wedge \#P_1 = \#P_2 \wedge \kappa(R_1) \gg \kappa(R_2)$.
- Relation $\curvearrowright$ satisfies the ascending chain condition on $\mathbb{CP}_n$.

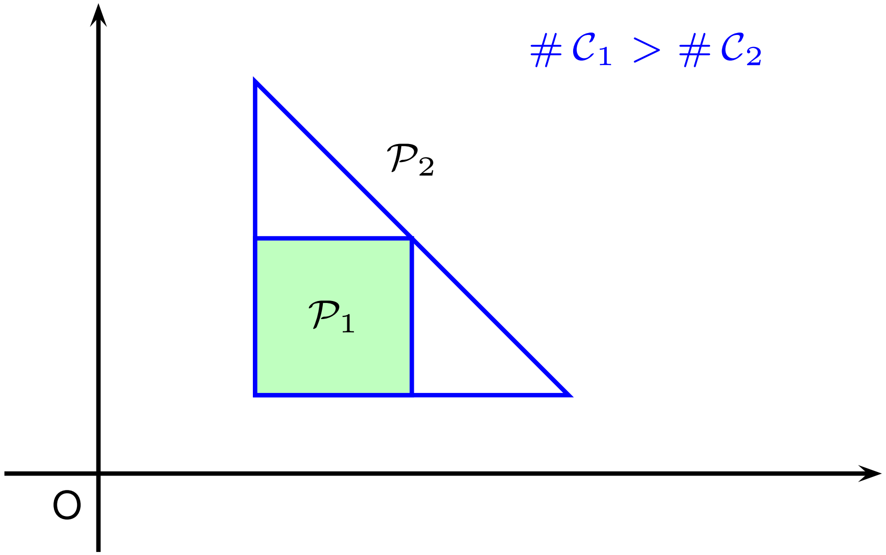
EXAMPLES FOR $\mathcal{P}_1 \curvearrowright \mathcal{P}_2$: CASE 1



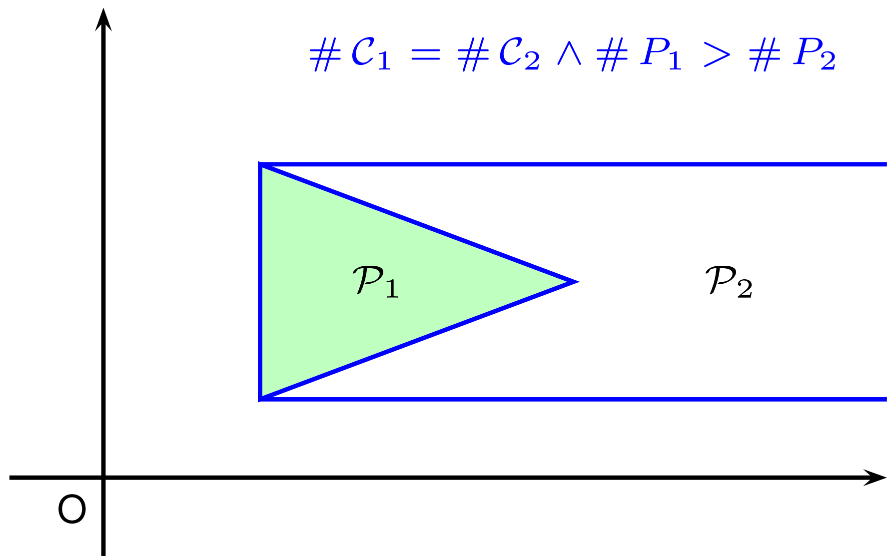
EXAMPLES FOR $\mathcal{P}_1 \curvearrowright \mathcal{P}_2$: CASE 2



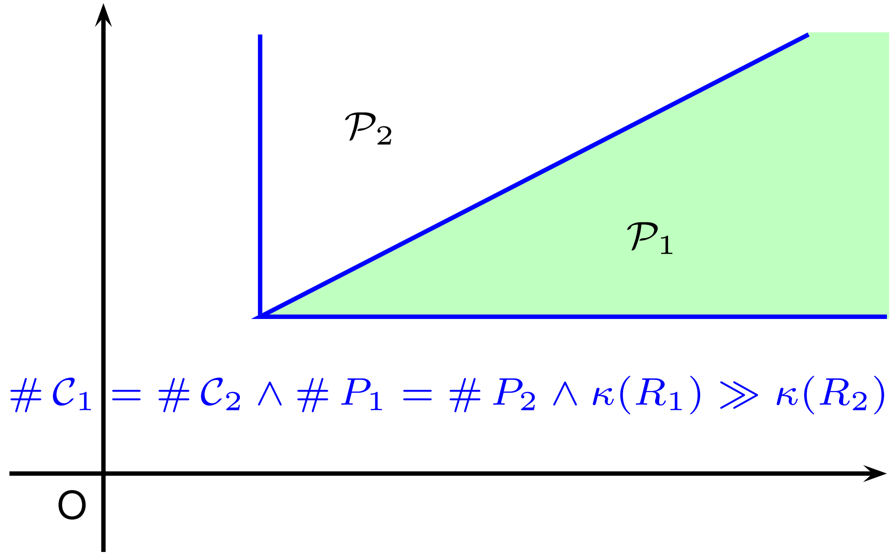
EXAMPLES FOR $\mathcal{P}_1 \curvearrowright \mathcal{P}_2$: CASE 3



EXAMPLES FOR $\mathcal{P}_1 \curvearrowright \mathcal{P}_2$: CASE 4



EXAMPLES FOR $\mathcal{P}_1 \curvearrowright \mathcal{P}_2$: CASE 5



A Framework for Defining New Widenings

The key results.

- ➜ The standard widening satisfies $\mathcal{P}_1 \curvearrowright \mathcal{P}_1 \nabla \mathcal{P}_2$.
  (This is not the case for the ordering defined in Besson *et al.*, SAS'99.)

A Framework for Defining New Widenings

The key results.

- The standard widening satisfies $\mathcal{P}_1 \curvearrowright \mathcal{P}_1 \nabla \mathcal{P}_2$.
  (This is not the case for the ordering defined in Besson *et al.*, SAS'99.)
- For any upper bound operator $h \colon \mathbb{CP}_n \times \mathbb{CP}_n \to \mathbb{CP}_n$, define

$$\mathcal{P}_1 \tilde{\nabla} \mathcal{P}_2 \stackrel{\text{def}}{=} \begin{cases} h(\mathcal{P}_1, \mathcal{P}_2), & \text{if } \mathcal{P}_1 \curvearrowright h(\mathcal{P}_1, \mathcal{P}_2) \subset \mathcal{P}_1 \nabla \mathcal{P}_2; \\ \mathcal{P}_1 \nabla \mathcal{P}_2, & \text{otherwise.} \end{cases}$$

A Framework for Defining New Widenings

The key results.

- The standard widening satisfies $\mathcal{P}_1 \curvearrowright \mathcal{P}_1 \nabla \mathcal{P}_2$.
  (This is not the case for the ordering defined in Besson *et al.*, SAS'99.)
- For any upper bound operator $h \colon \mathbb{CP}_n \times \mathbb{CP}_n \to \mathbb{CP}_n$, define

$$\mathcal{P}_1 \mathbin{\tilde{\nabla}} \mathcal{P}_2 \stackrel{\mathrm{def}}{=} \begin{cases} h(\mathcal{P}_1, \mathcal{P}_2), & \text{if } \mathcal{P}_1 \curvearrowright h(\mathcal{P}_1, \mathcal{P}_2) \subset \mathcal{P}_1 \nabla \mathcal{P}_2; \\ \mathcal{P}_1 \nabla \mathcal{P}_2, & \text{otherwise.} \end{cases}$$

Then:
① $\tilde{\nabla}$ is a widening operator;

A Framework for Defining New Widenings

The key results.

- ➜ The standard widening satisfies $\mathcal{P}_1 \curvearrowright \mathcal{P}_1 \nabla \mathcal{P}_2$.
  (This is not the case for the ordering defined in Besson *et al.*, SAS'99.)
- ➜ For any upper bound operator $h \colon \mathbb{CP}_n \times \mathbb{CP}_n \to \mathbb{CP}_n$, define

$$\mathcal{P}_1 \mathbin{\tilde{\nabla}} \mathcal{P}_2 \stackrel{\text{def}}{=} \begin{cases} h(\mathcal{P}_1, \mathcal{P}_2), & \text{if } \mathcal{P}_1 \curvearrowright h(\mathcal{P}_1, \mathcal{P}_2) \subset \mathcal{P}_1 \nabla \mathcal{P}_2; \\ \mathcal{P}_1 \nabla \mathcal{P}_2, & \text{otherwise.} \end{cases}$$

Then:

① $\tilde{\nabla}$ is a widening operator;

② $\tilde{\nabla}$ is at least as precise as the standard widening.

1ST HEURISTICS: DO NOT WIDEN

Let h be the least upper bound, so that $h(\mathcal{P}_1, \mathcal{P}_2) = \mathcal{P}_2$.

1st Heuristics: Do Not Widen

Let h be the least upper bound, so that $h(\mathcal{P}_1, \mathcal{P}_2) = \mathcal{P}_2$.

- ➜ Applicable whenever $\mathcal{P}_1 \curvearrowright \mathcal{P}_2$.
- ➜ No precision loss: to be tried before all other techniques.
- ➜ Already suggested by Cousot and Cousot, PLILP'92.

1st Heuristics: Do Not Widen

Let h be the least upper bound, so that $h(\mathcal{P}_1, \mathcal{P}_2) = \mathcal{P}_2$.

- Applicable whenever $\mathcal{P}_1 \curvearrowright \mathcal{P}_2$.
- No precision loss: to be tried before all other techniques.
- Already suggested by Cousot and Cousot, PLILP'92.
- All the other techniques may safely assume $\mathcal{P}_1 \not\curvearrowright \mathcal{P}_2$.
- Since by hypothesis $\mathcal{P}_1 \subset \mathcal{P}_2$, we can also assume

$$\begin{aligned} \mathrm{aff.hull}(\mathcal{P}_1) &= \mathrm{aff.hull}(\mathcal{P}_2), \\ \mathrm{lin.space}(\mathcal{P}_1) &= \mathrm{lin.space}(\mathcal{P}_2). \end{aligned}$$

2ND HEURISTICS: COMBINING CONSTRAINTS

Let $h_c(\mathcal{P}_1, \mathcal{P}_2) \stackrel{\text{def}}{=} \mathrm{con}(\mathcal{C}_\oplus) \cap (\mathcal{P}_1 \nabla \mathcal{P}_2)$, where

- ➜ $\mathcal{C}_\nabla$ are the constraints of the standard widening;
- ➜ $\mathcal{C}_\oplus \stackrel{\text{def}}{=} \left\{ \oplus(\mathcal{C}_{\boldsymbol{p}}) \;\middle|\; \begin{array}{l} \boldsymbol{p} \in P_1, \mathrm{sat\_con}\big(\boldsymbol{p}, \mathrm{ineq}(\mathcal{C}_\nabla)\big) = \varnothing, \\ \mathcal{C}_{\boldsymbol{p}} = \mathrm{sat\_con}\big(\boldsymbol{p}, \mathrm{ineq}(\mathcal{C}_2)\big) \neq \varnothing \end{array} \right\}$.
- ➜ $\oplus$ is a (deliberately left unspecified) convex combination.

Informally, *we ensure that each non-redundant point $\boldsymbol{p} \in \mathcal{P}_1$ that was lying on a facet of $\mathcal{P}_2$ will still lie on a facet of $h_c(\mathcal{P}_1, \mathcal{P}_2)$.*

2ND HEURISTICS: COMBINING CONSTRAINTS

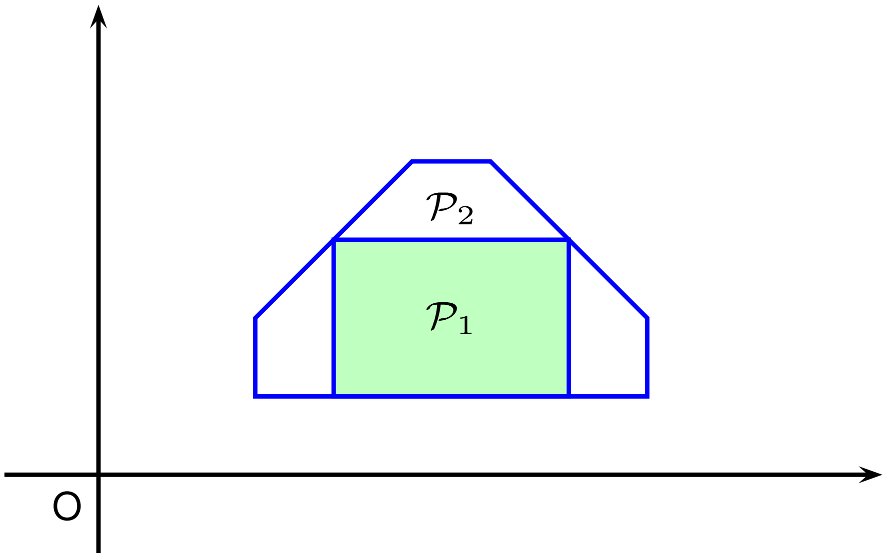
Let $h_c(\mathcal{P}_1, \mathcal{P}_2) \stackrel{\text{def}}{=} \text{con}(\mathcal{C}_\oplus) \cap (\mathcal{P}_1 \nabla \mathcal{P}_2)$, where

- ➜ $\mathcal{C}_\nabla$ are the constraints of the standard widening;
- ➜ $\mathcal{C}_\oplus \stackrel{\text{def}}{=} \left\{ \oplus(\mathcal{C}_{\boldsymbol{p}}) \;\middle|\; \begin{array}{l} \boldsymbol{p} \in P_1, \text{sat\_con}\big(\boldsymbol{p}, \text{ineq}(\mathcal{C}_\nabla)\big) = \varnothing, \\ \mathcal{C}_{\boldsymbol{p}} = \text{sat\_con}\big(\boldsymbol{p}, \text{ineq}(\mathcal{C}_2)\big) \neq \varnothing \end{array} \right\}$.
- ➜ $\oplus$ is a (deliberately left unspecified) convex combination.

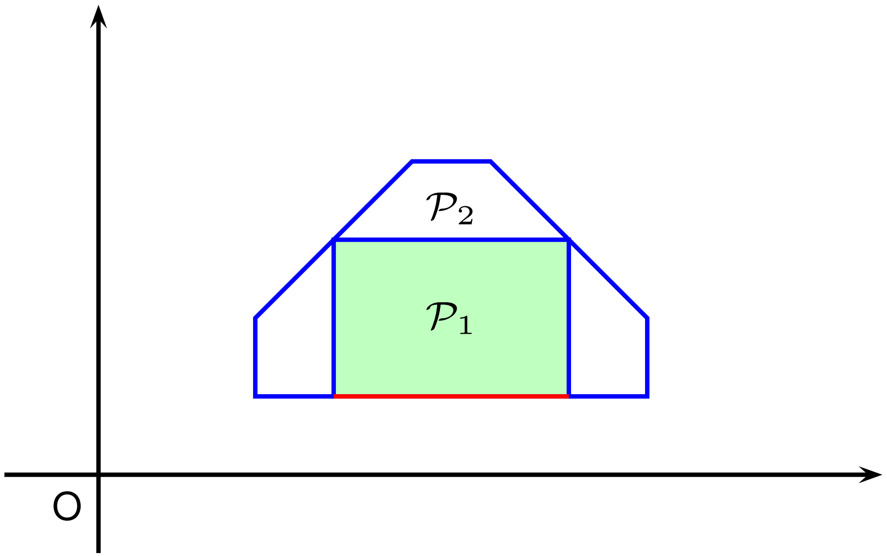
Informally, *we ensure that each non-redundant point $\boldsymbol{p} \in \mathcal{P}_1$ that was lying on a facet of $\mathcal{P}_2$ will still lie on a facet of $h_c(\mathcal{P}_1, \mathcal{P}_2)$.*

- ➜ Besson et al., SAS'99 suggest to average the constraints in $\mathcal{C}_{\boldsymbol{p}}$.
- ➜ Afterall, the choice of $\oplus$ is arbitrary: we opted for a simpler combination.
- ➜ A similar heuristics, with no convergence guarantee, was proposed by Henzinger et al., CDC'01.

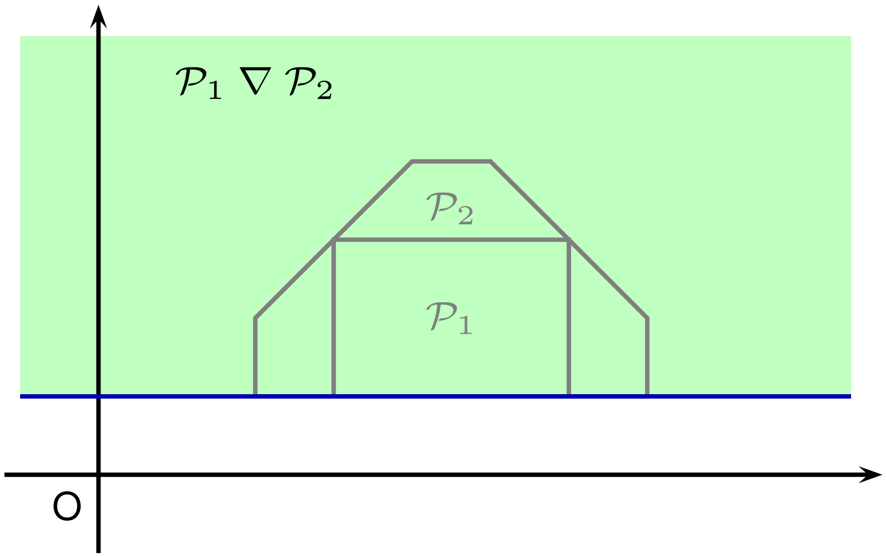
Standard Widening vs. Combining Constraints (i)



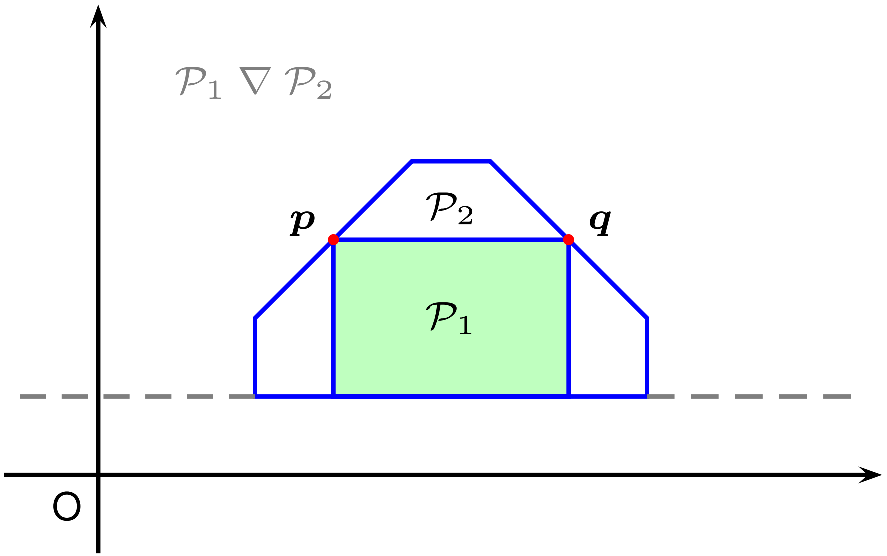
STANDARD WIDENING VS. COMBINING CONSTRAINTS (II)



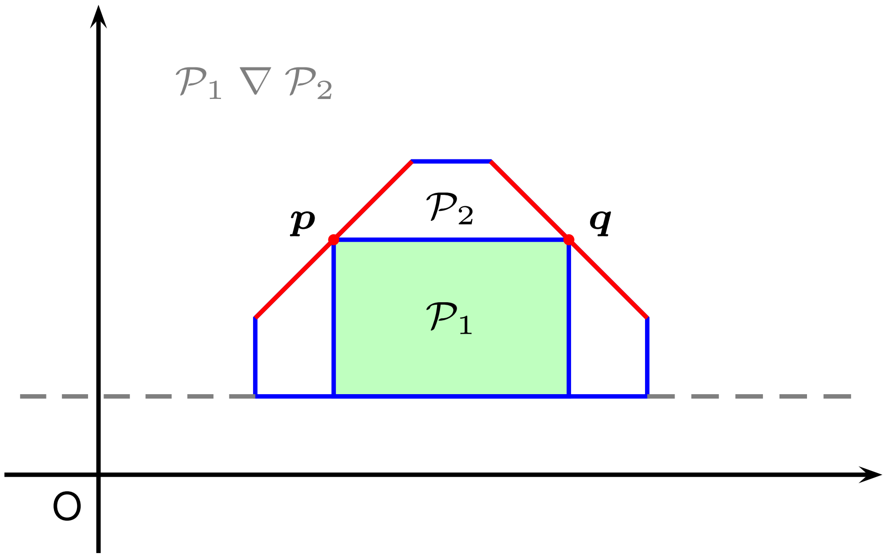
Standard Widening vs. Combining Constraints (iii)



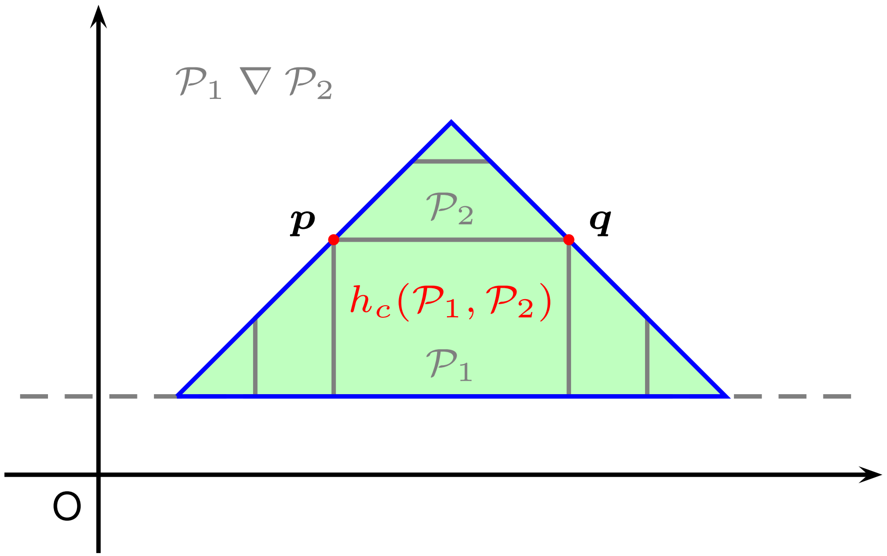
Standard Widening vs. Combining Constraints (iv)



STANDARD WIDENING VS. COMBINING CONSTRAINTS (V)



Standard Widening vs. Combining Constraints (vi)



3RD HEURISTICS: EVOLVING POINTS

➜ A (slightly simpler) variant of the extrapolation operator '$\propto$' defined in Henzinger and Ho, Hibrid Systems II, 95.

➜ Also similar to another operator sketched in Besson et al., SAS'99.

3RD HEURISTICS: EVOLVING POINTS

➜ A (slightly simpler) variant of the extrapolation operator '$\propto$' defined in Henzinger and Ho, Hibrid Systems II, 95.

➜ Also similar to another operator sketched in Besson et al., SAS'99.

➜ Consider the set of rays

$$R \stackrel{\mathrm{def}}{=} \left\{ \boldsymbol{p}_2 - \boldsymbol{p}_1 \;\middle|\; \boldsymbol{p}_1 \in P_1, \boldsymbol{p}_2 \in P_2 \setminus P_1 \right\}.$$

➜ Informally, *each point $\boldsymbol{p}_2 \in P_2 \setminus P_1$ is seen as an evolution of point $\boldsymbol{p}_1 \in P_1$. By generating the ray $\boldsymbol{p}_2 - \boldsymbol{p}_1$, we extrapolate this evolution towards infinity.*

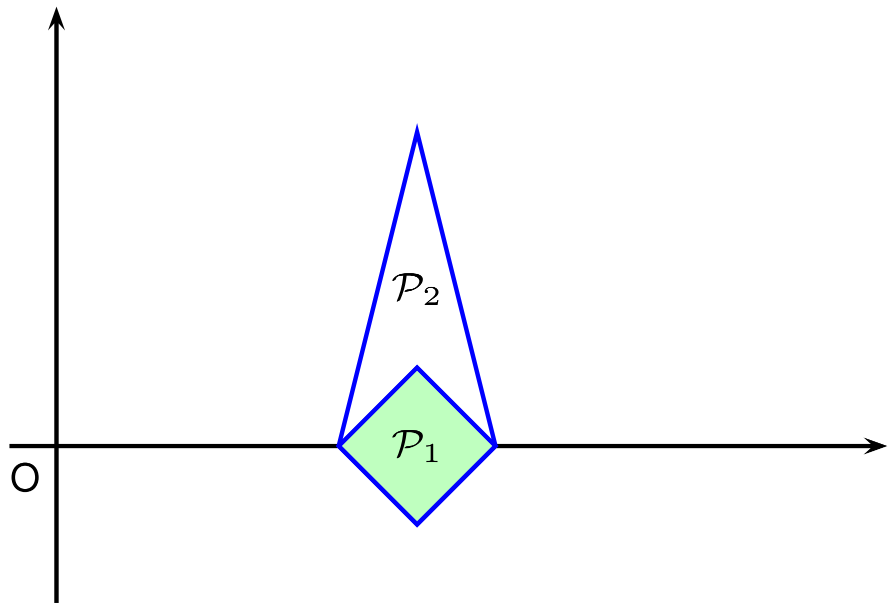
3RD HEURISTICS: EVOLVING POINTS

- A (slightly simpler) variant of the extrapolation operator '$\propto$' defined in Henzinger and Ho, Hibrid Systems II, 95.
- Also similar to another operator sketched in Besson et al., SAS'99.
- Consider the set of rays

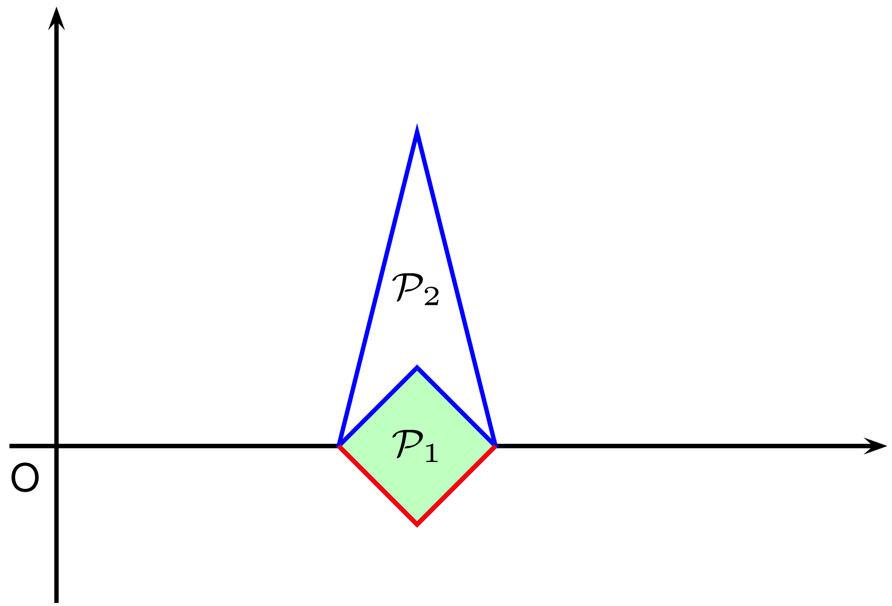
$$R \stackrel{\text{def}}{=} \{\, \boldsymbol{p}_2 - \boldsymbol{p}_1 \;\big|\; \boldsymbol{p}_1 \in P_1, \boldsymbol{p}_2 \in P_2 \setminus P_1 \,\}.$$

- Informally, *each point $\boldsymbol{p}_2 \in P_2 \setminus P_1$ is seen as an evolution of point $\boldsymbol{p}_1 \in P_1$. By generating the ray $\boldsymbol{p}_2 - \boldsymbol{p}_1$, we extrapolate this evolution towards infinity.*
- Thus, let $h_p(\mathcal{P}_1, \mathcal{P}_2) \stackrel{\text{def}}{=} \mathrm{gen}\big((L_2, R_2 \cup R, P_2)\big) \cap (\mathcal{P}_1 \nabla \mathcal{P}_2)$.

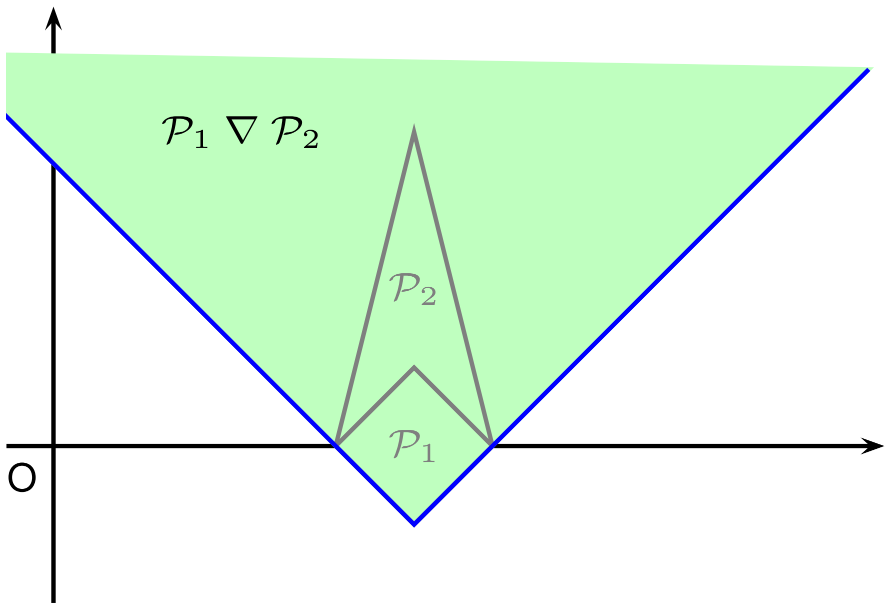
Standard Widening vs. Evolving Points (i)



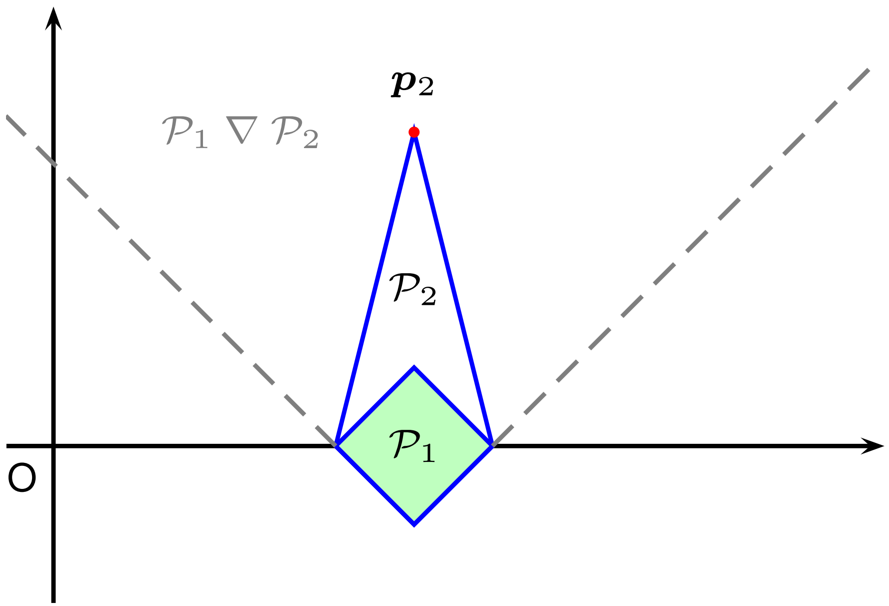
Standard Widening vs. Evolving Points (II)



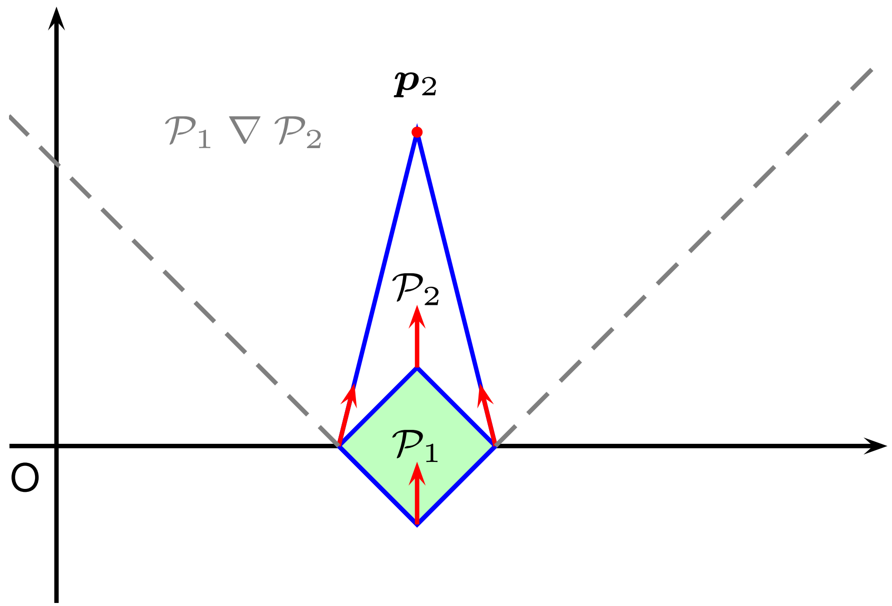
Standard Widening vs. Evolving Points (iii)



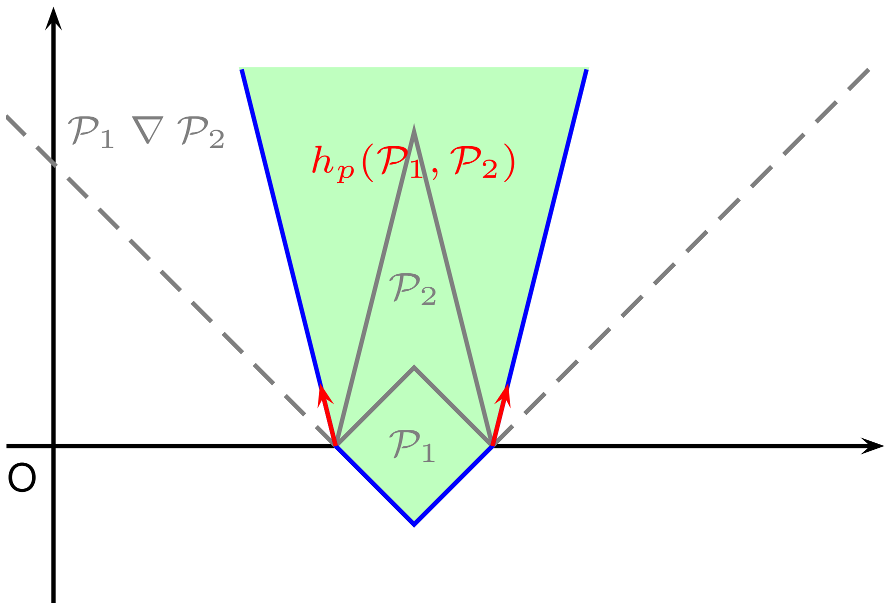
Standard Widening vs. Evolving Points (iv)



Standard Widening vs. Evolving Points (v)



Standard Widening vs. Evolving Points (vi)



4TH HEURISTICS: EVOLVING RAYS

➜ A brand new widening heuristics.

4TH HEURISTICS: EVOLVING RAYS

➜ A brand new widening heuristics.

➜ Define the set of rays

$$R \stackrel{\text{def}}{=} \left\{ \operatorname{evolve}(\boldsymbol{r}_2, \boldsymbol{r}_1) \;\middle|\; \boldsymbol{r}_1 \in R_1, \boldsymbol{r}_2 \in R_2 \setminus R_1 \right\}.$$

➜ Informally, *each ray $\boldsymbol{r}_2 \in R_2 \setminus R_1$ is seen as an evolution of ray $\boldsymbol{r}_1 \in R_1$. We extrapolate this evolution by rotating ray $\boldsymbol{r}_2$, stopping as soon as it touches the boundary of the Cartesian orthant*.

4TH HEURISTICS: EVOLVING RAYS

- ➜ A brand new widening heuristics.
- ➜ Define the set of rays

$$R \stackrel{\text{def}}{=} \bigl\{\, \mathrm{evolve}(\boldsymbol{r}_2, \boldsymbol{r}_1) \bigm| \boldsymbol{r}_1 \in R_1, \boldsymbol{r}_2 \in R_2 \setminus R_1 \,\bigr\}.$$

- ➜ Informally, *each ray $\boldsymbol{r}_2 \in R_2 \setminus R_1$ is seen as an evolution of ray $\boldsymbol{r}_1 \in R_1$. We extrapolate this evolution by rotating ray $\boldsymbol{r}_2$, stopping as soon as it touches the boundary of the Cartesian orthant*.
- ➜ Thus, let $h_r(\mathcal{P}_1, \mathcal{P}_2) \stackrel{\text{def}}{=} \mathrm{gen}\bigl((L_2, R_2 \cup R, P_2)\bigr) \cap (\mathcal{P}_1 \nabla \mathcal{P}_2)$.

4TH HEURISTICS: EVOLVING RAYS

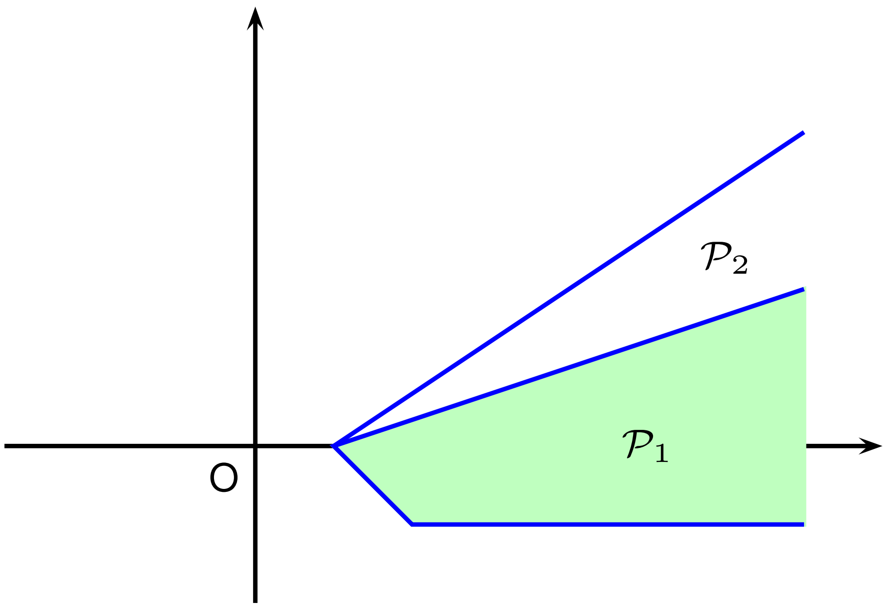
- A brand new widening heuristics.
- Define the set of rays

$$R \stackrel{\text{def}}{=} \left\{ \operatorname{evolve}(\boldsymbol{r}_2, \boldsymbol{r}_1) \;\middle|\; \boldsymbol{r}_1 \in R_1, \boldsymbol{r}_2 \in R_2 \setminus R_1 \right\}.$$

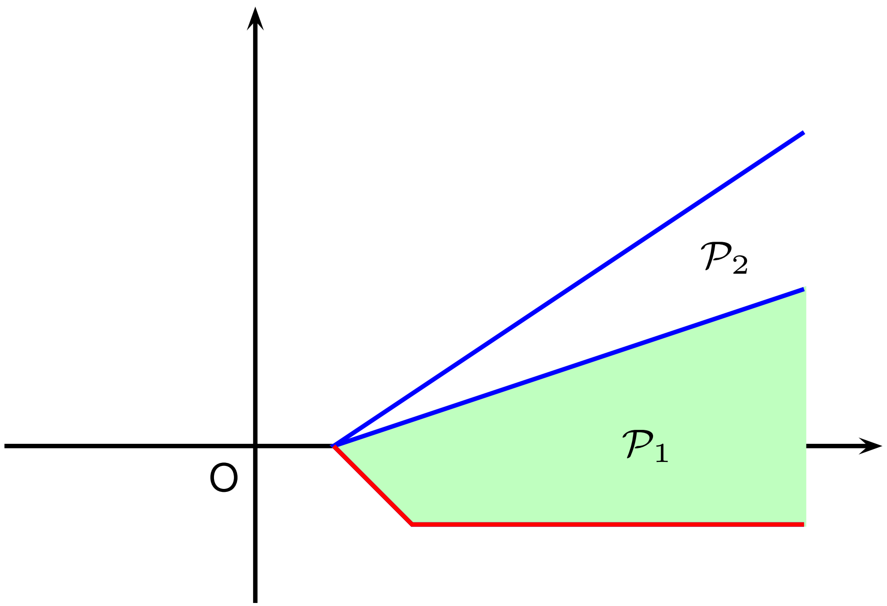
- Informally, *each ray $\boldsymbol{r}_2 \in R_2 \setminus R_1$ is seen as an evolution of ray $\boldsymbol{r}_1 \in R_1$. We extrapolate this evolution by rotating ray $\boldsymbol{r}_2$, stopping as soon as it touches the boundary of the Cartesian orthant*.
- Thus, let $h_r(\mathcal{P}_1, \mathcal{P}_2) \stackrel{\text{def}}{=} \operatorname{gen}\bigl((L_2, R_2 \cup R, P_2)\bigr) \cap (\mathcal{P}_1 \nabla \mathcal{P}_2)$.
- The extrapolation will decrease the total number of non-zero coordinates of the ray $\Longrightarrow$ hopefully satisfying the last case in the definition of the limited growth ordering $\curvearrowright$:

$$\#\mathcal{C}_1 = \#\mathcal{C}_2 \wedge \# P_1 = \# P_2 \wedge \kappa(R_1) \gg \kappa(R_2).$$

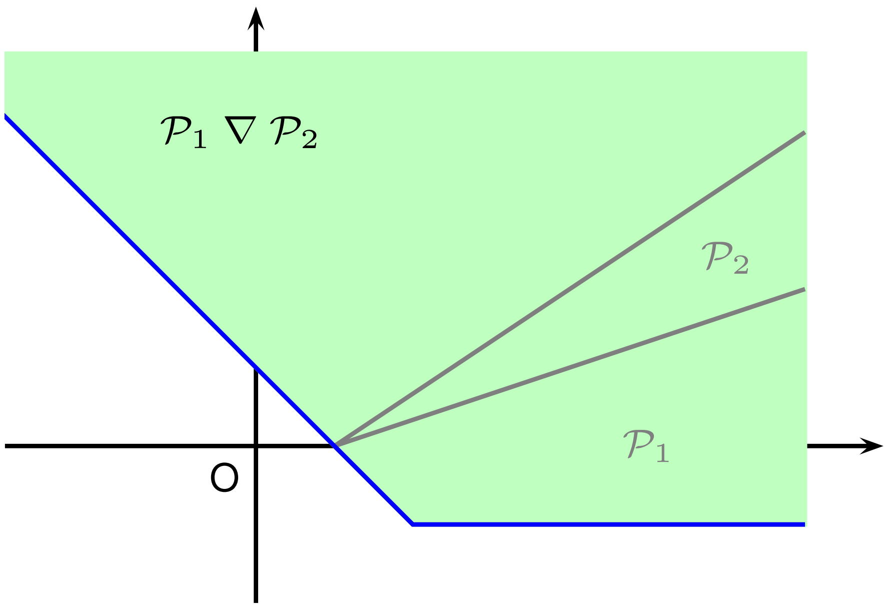
Standard Widening vs. Evolving Rays (i)



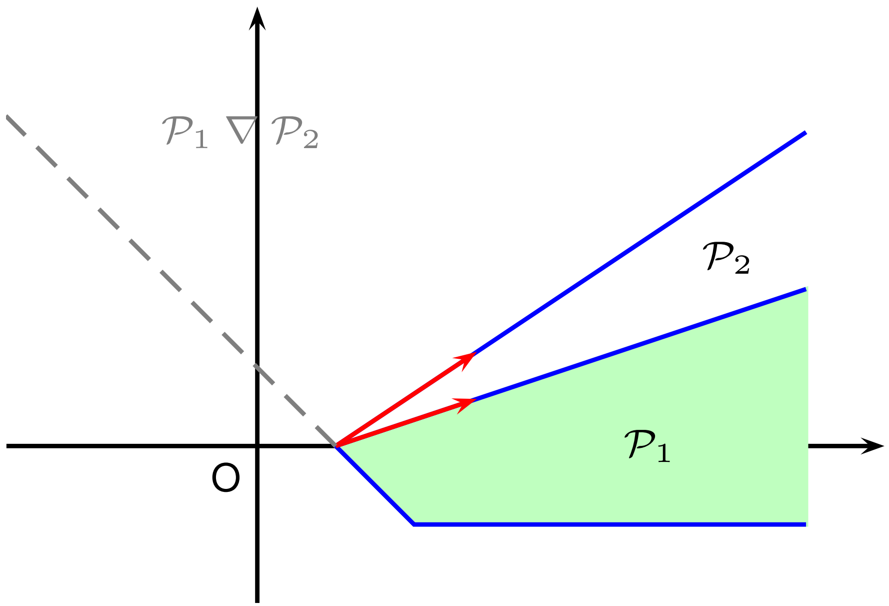
Standard Widening vs. Evolving Rays (ii)



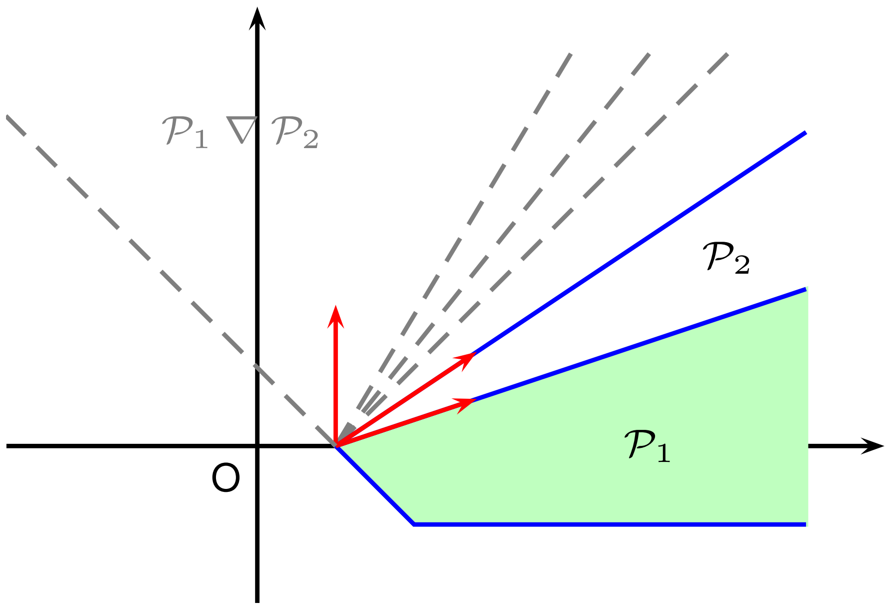
Standard Widening vs. Evolving Rays (iii)



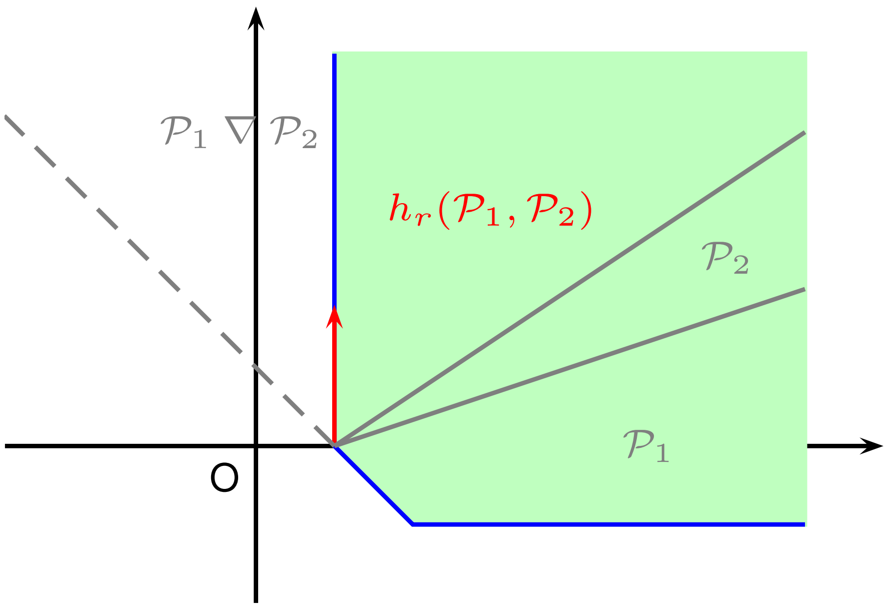
Standard Widening vs. Evolving Rays (iv)



Standard Widening vs. Evolving Rays (v)



Standard Widening vs. Evolving Rays (vi)



The New Widening $\hat{\nabla}$

➜ An instance of the framework: try the four heuristics in the given order, eventually falling back to the standard widening.

$$\mathcal{P}_1 \mathbin{\hat{\nabla}} \mathcal{P}_2 \stackrel{\text{def}}{=} \begin{cases} \mathcal{P}_2, & \text{if } \mathcal{P}_1 \curvearrowright \mathcal{P}_2; \\ h_c(\mathcal{P}_1, \mathcal{P}_2), & \text{if } \mathcal{P}_1 \curvearrowright h_c(\mathcal{P}_1, \mathcal{P}_2) \subset \mathcal{P}_1 \nabla \mathcal{P}_2; \\ h_p(\mathcal{P}_1, \mathcal{P}_2), & \text{if } \mathcal{P}_1 \curvearrowright h_p(\mathcal{P}_1, \mathcal{P}_2) \subset \mathcal{P}_1 \nabla \mathcal{P}_2; \\ h_r(\mathcal{P}_1, \mathcal{P}_2), & \text{if } \mathcal{P}_1 \curvearrowright h_r(\mathcal{P}_1, \mathcal{P}_2) \subset \mathcal{P}_1 \nabla \mathcal{P}_2; \\ \mathcal{P}_1 \nabla \mathcal{P}_2, & \text{otherwise.} \end{cases}$$

THE NEW WIDENING $\hat{\nabla}$

- An instance of the framework: try the four heuristics in the given order, eventually falling back to the standard widening.

$$\mathcal{P}_1 \mathbin{\hat{\nabla}} \mathcal{P}_2 \stackrel{\mathrm{def}}{=} \begin{cases} \mathcal{P}_2, & \text{if } \mathcal{P}_1 \curvearrowright \mathcal{P}_2; \\ h_c(\mathcal{P}_1, \mathcal{P}_2), & \text{if } \mathcal{P}_1 \curvearrowright h_c(\mathcal{P}_1, \mathcal{P}_2) \subset \mathcal{P}_1 \mathbin{\nabla} \mathcal{P}_2; \\ h_p(\mathcal{P}_1, \mathcal{P}_2), & \text{if } \mathcal{P}_1 \curvearrowright h_p(\mathcal{P}_1, \mathcal{P}_2) \subset \mathcal{P}_1 \mathbin{\nabla} \mathcal{P}_2; \\ h_r(\mathcal{P}_1, \mathcal{P}_2), & \text{if } \mathcal{P}_1 \curvearrowright h_r(\mathcal{P}_1, \mathcal{P}_2) \subset \mathcal{P}_1 \mathbin{\nabla} \mathcal{P}_2; \\ \mathcal{P}_1 \mathbin{\nabla} \mathcal{P}_2, & \text{otherwise.} \end{cases}$$

- Uniformly more precise than the standard widening.

The New Widening $\hat{\nabla}$

- An instance of the framework: try the four heuristics in the given order, eventually falling back to the standard widening.

$$\mathcal{P}_1 \mathbin{\hat{\nabla}} \mathcal{P}_2 \stackrel{\text{def}}{=} \begin{cases} \mathcal{P}_2, & \text{if } \mathcal{P}_1 \curvearrowright \mathcal{P}_2; \\ h_c(\mathcal{P}_1, \mathcal{P}_2), & \text{if } \mathcal{P}_1 \curvearrowright h_c(\mathcal{P}_1, \mathcal{P}_2) \subset \mathcal{P}_1 \mathbin{\nabla} \mathcal{P}_2; \\ h_p(\mathcal{P}_1, \mathcal{P}_2), & \text{if } \mathcal{P}_1 \curvearrowright h_p(\mathcal{P}_1, \mathcal{P}_2) \subset \mathcal{P}_1 \mathbin{\nabla} \mathcal{P}_2; \\ h_r(\mathcal{P}_1, \mathcal{P}_2), & \text{if } \mathcal{P}_1 \curvearrowright h_r(\mathcal{P}_1, \mathcal{P}_2) \subset \mathcal{P}_1 \mathbin{\nabla} \mathcal{P}_2; \\ \mathcal{P}_1 \mathbin{\nabla} \mathcal{P}_2, & \text{otherwise.} \end{cases}$$

- Uniformly more precise than the standard widening.
- In general, this does not hold for the final result of upward iteration sequences, because neither the standard widening nor the new one are monotonic operators.

Precision Comparison

Argument size relations for Prolog programs using China $+$ PPL.

Note: carefully chosen widening strategy (Bourdoncle, FMPTA'93)
$+$ widening delay $+$ widening 'up to'.

Precision Comparison

Argument size relations for Prolog programs using China $+$ PPL.

Note: carefully chosen widening strategy (Bourdoncle, FMPTA'93)
$+$ widening delay $+$ widening 'up to'.

	# programs (361)			# predicates (23279)		
k (delay)	improve	degr	incomp	improve	degr	incomp
0	121	-	2	1340	3	2
1	34	-	-	273	-	-
2	29	-	-	222	-	-
3	28	-	-	160	-	-
4	25	-	2	126	2	-
10	25	-	-	124	-	-

Efficiency Comparison

Argument size relations for Prolog programs using China $+$ PPL.

Total analysis time

	std ∇_k		new $\hat{\nabla}_k$	
k (delay)	all	top 20	all	top 20
0	**1.00**	0.72	1.05	0.77
1	1.09	0.79	1.11	0.80
2	1.16	0.83	1.18	0.84
3	1.23	0.88	1.25	0.89
4	1.32	0.95	1.34	0.95
10	1.82	1.23	1.85	1.24

Conclusion

➜ We have defined a framework for the systematic specification of new widening operators:

CONCLUSION

- ➜ We have defined a framework for the systematic specification of new widening operators:
  - ➜ the framework allows any extrapolation operator on the domain of convex polyhedra to be transformed to a widening operator;

Conclusion

- ➜ We have defined a framework for the systematic specification of new widening operators:
  - ➜ the framework allows any extrapolation operator on the domain of convex polyhedra to be transformed to a widening operator;
  - ➜ the framework ensures that these new widenings improve on the precision of the standard widening.

CONCLUSION

- We have defined a framework for the systematic specification of new widening operators:
  - the framework allows any extrapolation operator on the domain of convex polyhedra to be transformed to a widening operator;
  - the framework ensures that these new widenings improve on the precision of the standard widening.
- We have instantiated the framework with extrapolation operators:
  - do nothing, combining constraints, evolving points, evolving rays.

Conclusion

- We have defined a framework for the systematic specification of new widening operators:
  - the framework allows any extrapolation operator on the domain of convex polyhedra to be transformed to a widening operator;
  - the framework ensures that these new widenings improve on the precision of the standard widening.
- We have instantiated the framework with extrapolation operators:
  - do nothing, combining constraints, evolving points, evolving rays.
- This instantiated framework has been implemented in the Parma Polyhedra Library.

Conclusion

- We have defined a framework for the systematic specification of new widening operators:
  - the framework allows any extrapolation operator on the domain of convex polyhedra to be transformed to a widening operator;
  - the framework ensures that these new widenings improve on the precision of the standard widening.
- We have instantiated the framework with extrapolation operators:
  - do nothing, combining constraints, evolving points, evolving rays.
- This instantiated framework has been implemented in the Parma Polyhedra Library.
- A first experimental evaluation has yielded promising results.

Conclusion

- We have defined a framework for the systematic specification of new widening operators:
  - the framework allows any extrapolation operator on the domain of convex polyhedra to be transformed to a widening operator;
  - the framework ensures that these new widenings improve on the precision of the standard widening.
- We have instantiated the framework with extrapolation operators:
  - do nothing, combining constraints, evolving points, evolving rays.
- This instantiated framework has been implemented in the Parma Polyhedra Library.
- A first experimental evaluation has yielded promising results.

The PPL is free software: everything is available at

`http://www.cs.unipr.it/ppl/`