Widenings for Powerset Domains with Applications to Finite Sets of Polyhedra

Roberto BAGNARA, Enea ZAFFANELLA
University of Parma, Italy

Patricia M. HILL,
University of Leeds, United Kingdom

MOTIVATIONS

➜ The design of abstract domains is a difficult task . . .

MOTIVATIONS

- The design of abstract domains is a difficult task ...
- ...thus, there continues to be strong interest in techniques that derive enhanced abstract domains by applying systematic constructions to simpler, existing domains [Cousot and Cousot, POPL'79].

Motivations

- The design of abstract domains is a difficult task ...
- ...thus, there continues to be strong interest in techniques that derive enhanced abstract domains by applying systematic constructions to simpler, existing domains [Cousot and Cousot, POPL'79].
- Most studies concentrate on the definition of the carrier of the enhanced abstract domain, since (under suitable hypotheses) the optimal abstract operators can be induced from it.

MOTIVATIONS

- The design of abstract domains is a difficult task . . .
- . . . thus, there continues to be strong interest in techniques that derive enhanced abstract domains by applying systematic constructions to simpler, existing domains [Cousot and Cousot, POPL'79].
- Most studies concentrate on the definition of the carrier of the enhanced abstract domain, since (under suitable hypotheses) the optimal abstract operators can be induced from it.
- But the optimal operators are often difficult to implement, motivating the interest on generic techniques whereby correct domain operations are derived (semi-) automatically from those of the base-level domains [Cortesi et al., SCP'00; Cousot and Cousot, POPL'79; Filé and Ranzato, TCS'99].

MOTIVATIONS

- The design of abstract domains is a difficult task . . .
- . . . thus, there continues to be strong interest in techniques that derive enhanced abstract domains by applying systematic constructions to simpler, existing domains [Cousot and Cousot, POPL'79].
- Most studies concentrate on the definition of the carrier of the enhanced abstract domain, since (under suitable hypotheses) the optimal abstract operators can be induced from it.
- But the optimal operators are often difficult to implement, motivating the interest on generic techniques whereby correct domain operations are derived (semi-) automatically from those of the base-level domains [Cortesi et al., SCP'00; Cousot and Cousot, POPL'79; Filé and Ranzato, TCS'99].
- Among the abstract operators, widenings are special: besides correctness, a proper widening operator also has to provide a finite convergence guarantee.

GOAL AND PLAN OF THE TALK

➜ Our goal: consider a disjunctive refinement of an abstract domain and provide parametric constructions for lifting any widening defined on the base-level domain to a proper widening on the enhanced domain.

Goal and Plan of the Talk

➜ Our goal: consider a disjunctive refinement of an abstract domain and provide parametric constructions for lifting any widening defined on the base-level domain to a proper widening on the enhanced domain.

➜ Plan of the talk:

1. clarify what we mean by proper widening;
2. present the finite powerset construction;
3. present two different strategies for transforming an extrapolation operator into a proper widening.

Goal and Plan of the Talk

➜ Our goal: consider a disjunctive refinement of an abstract domain and provide parametric constructions for lifting any widening defined on the base-level domain to a proper widening on the enhanced domain.

➜ Plan of the talk:

1. clarify what we mean by proper widening;
2. present the finite powerset construction;
3. present two different strategies for transforming an extrapolation operator into a proper widening.

➜ Throughout the talk, we will instantiate the concepts on the finite powerset domain built upon the abstract domain of convex polyhedra, a non-toy example having several practical applications.

The Abstract Interpretation Framework

An instance of [Cousot and Cousot, JLC '92, Section 7].

- ➜ The concrete domain $\langle C, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$ is a complete lattice;
- ➜ The concrete approximation relation $c_1 \sqsubseteq c_2$ holds if c_1 is a stronger property than c_2;
- ➜ The concrete semantics is $c = \mathcal{F}^{\omega}(\bot)$, where $\mathcal{F} \colon C \to C$ is continuous.

THE ABSTRACT INTERPRETATION FRAMEWORK

An instance of [Cousot and Cousot, JLC '92, Section 7].

- ➜ The concrete domain $\langle C, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$ is a complete lattice;
- ➜ The concrete approximation relation $c_1 \sqsubseteq c_2$ holds if c_1 is a stronger property than c_2;
- ➜ The concrete semantics is $c = \mathcal{F}^\omega(\bot)$, where $\mathcal{F} \colon C \to C$ is continuous.
- ➜ The abstract domain $\langle D, \vdash, \mathbf{0}, \oplus \rangle$ is a join-semilattice;
- ➜ The two domains are related by a monotonic and injective concretization function $\gamma \colon D \to C$; thus, the abstract partial order $\vdash$ is indeed the approximation relation induced on D by γ.
- ➜ We assume the existence of a sound monotonic abstract semantic function $\mathcal{F}^\sharp \colon D \to D$, so that

$$\forall c \in C : \forall d \in D : c \sqsubseteq \gamma(d) \implies \mathcal{F}(c) \sqsubseteq \gamma\bigl(\mathcal{F}^\sharp(d)\bigr).$$

A WORKING EXAMPLE (I)

- A collecting semantics gathering relational information about the possible values of numerical variables can be based on the concrete domain:

$$\langle \wp(\mathbb{R}^n), \subseteq, \varnothing, \mathbb{R}^n, \cup, \cap \rangle.$$

- The abstract domain of closed convex polyhedra [Cousot and Halbwachs, POPL'78] is the (non-complete) lattice

$$\widehat{\mathbb{CP}}_n := \langle \mathbb{CP}_n, \subseteq, \varnothing, \mathbb{R}^n, \uplus, \cap \rangle$$

which is related to the concrete domain by $\gamma(\mathcal{P}) := \mathcal{P}$.

PROBLEMS IN THE ABSTRACT SEMANTICS COMPUTATION

➜ The "limit" of the abstract computation may not be representable in the abstract domain (e.g., a circle is not a polyhedron);

➜ Reaching a post-fixpoint of the abstract semantic function may require an infinite number of computation steps;

➜ Even when the abstract computation is intrinsically finite, it may be practically unfeasible if it requires too many abstract iterations; for instance,

```
x := 0;
while (x < 1000) do
  x := x+1; y := f(x);
endwhile
```

Widening operators try to solve all of these problems at once.

Definition of Widening Operator

A minor variant of the classical one [Cousot and Cousot, PLILP'92]:

- ➜ The partial operator $\nabla \colon D \times D \rightarrowtail D$ is a widening if
  - ① $\forall d_1, d_2 \in D : d_1 \vdash d_2 \implies d_2 \vdash d_1 \nabla d_2$;
  - ② for each increasing chain $d_0 \vdash d_1 \vdash \cdots$, the increasing chain defined by $d'_0 := d_0$ and $d'_{i+1} := d'_i \nabla (d'_i \oplus d_{i+1})$, for $i \in \mathbb{N}$, is not strictly increasing.
- ➜ Note: any widening ∇ induces on D a partial order relation $\vdash_\nabla$ satisfying the ACC; this is defined as the reflexive and transitive closure of $\left\{ (d_1, d) \in D \times D \;\middle|\; \exists d_2 \in D \,.\, d_1 \Vdash d_2 \land d = d_1 \nabla d_2 \right\}$.

Definition of Widening Operator

A minor variant of the classical one [Cousot and Cousot, PLILP'92]:

- The partial operator $\nabla \colon D \times D \rightarrowtail D$ is a widening if
  ① $\forall d_1, d_2 \in D : d_1 \vdash d_2 \implies d_2 \vdash d_1 \nabla d_2$;
  ② for each increasing chain $d_0 \vdash d_1 \vdash \cdots$, the increasing chain defined by $d'_0 := d_0$ and $d'_{i+1} := d'_i \nabla (d'_i \oplus d_{i+1})$, for $i \in \mathbb{N}$, is not strictly increasing.
- Note: any widening ∇ induces on D a partial order relation $\vdash_\nabla$ satisfying the ACC; this is defined as the reflexive and transitive closure of $\{ (d_1, d) \in D \times D \mid \exists d_2 \in D \mathrel{.} d_1 \Vdash d_2 \wedge d = d_1 \nabla d_2 \}$.
- The upward iteration sequence with widenings (starting from $\mathbf{0} \in D$)

$$d_{i+1} = \begin{cases} d_i, & \text{if } \mathcal{F}^\sharp(d_i) \vdash d_i; \\ d_i \nabla \bigl(d_i \oplus \mathcal{F}^\sharp(d_i)\bigr), & \text{otherwise;} \end{cases}$$

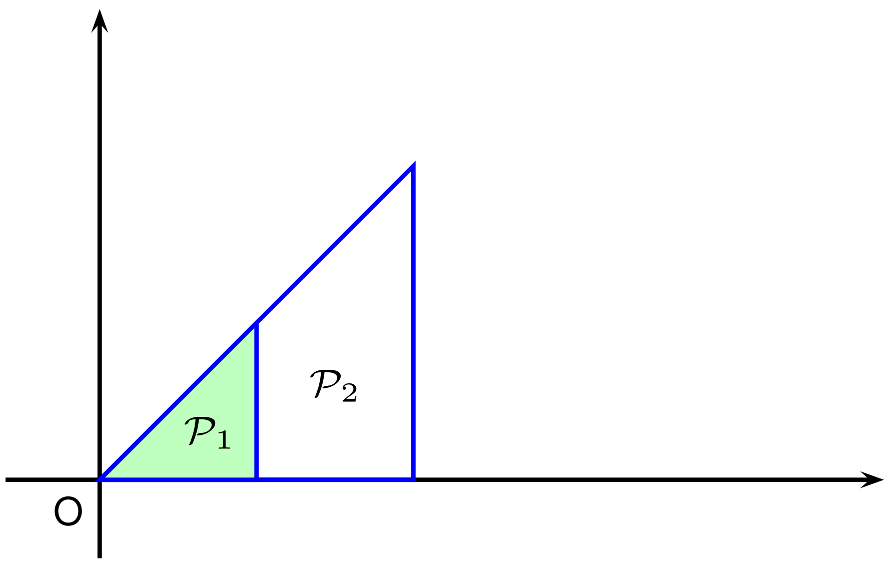
converges after a finite number of iterations.

A Working Example (II)

- ➜ The abstract domain $\widehat{\mathbb{CP}}_n$ has infinite ascending chains;
- ➜ It comes equipped with the standard widening [Cousot and Halbwachs, POPL'78] or other widenings improving upon it [Bagnara et al., SAS'03].

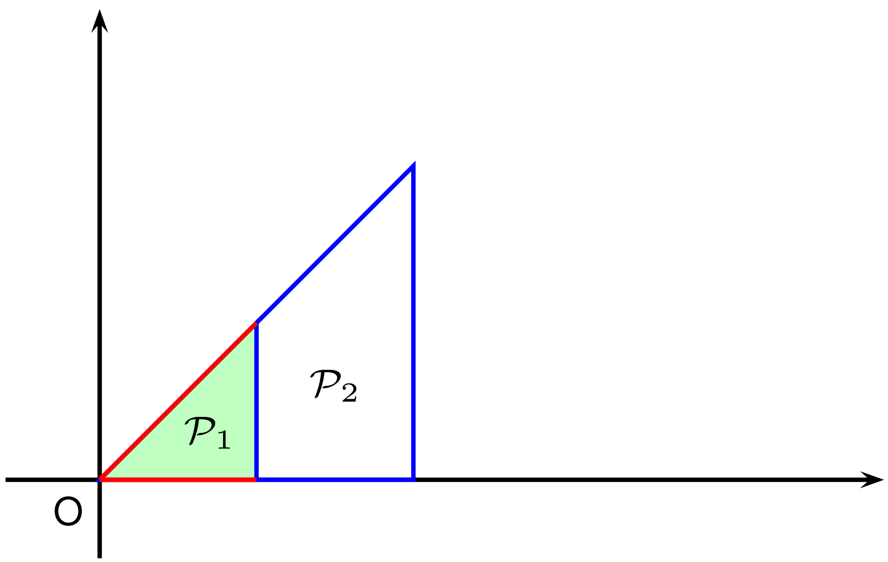
A Working Example (II)

- ➜ The abstract domain $\widehat{\mathbb{CP}}_n$ has infinite ascending chains;
- ➜ It comes equipped with the standard widening [Cousot and Halbwachs, POPL'78] or other widenings improving upon it [Bagnara et al., SAS'03].



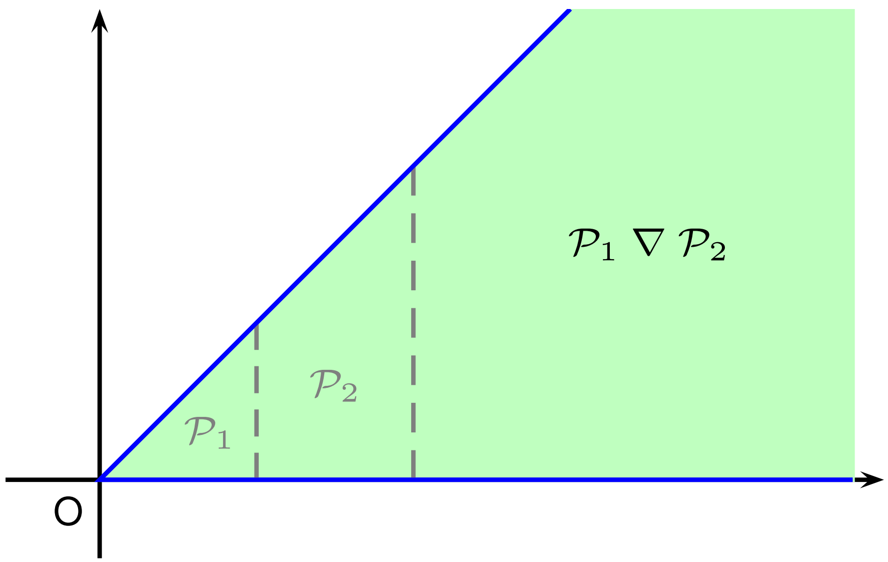
A WORKING EXAMPLE (II)

- ➜ The abstract domain $\widehat{\mathbb{CP}}_n$ has infinite ascending chains;
- ➜ It comes equipped with the standard widening [Cousot and Halbwachs, POPL'78] or other widenings improving upon it [Bagnara et al., SAS'03].



A WORKING EXAMPLE (II)

- ➜ The abstract domain $\widehat{\mathbb{CP}}_n$ has infinite ascending chains;
- ➜ It comes equipped with the standard widening [Cousot and Halbwachs, POPL'78] or other widenings improving upon it [Bagnara et al., SAS'03].



THE FINITE POWERSET CONSTRUCTION (I)

➜ Similar to the disjunctive completion of [Cousot and Cousot, POPL'79], obtained by a variant of the down-set completion construction of [Cousot and Cousot, JLP '92].

THE FINITE POWERSET CONSTRUCTION (I)

- Similar to the disjunctive completion of [Cousot and Cousot, POPL'79], obtained by a variant of the down-set completion construction of [Cousot and Cousot, JLP '92].
- An element of the powerset is a non-redundant and finite collection of objects of the base domain: each object in the collection has to be maximal wrt the partial order $\vdash$.

THE FINITE POWERSET CONSTRUCTION (I)

- Similar to the disjunctive completion of [Cousot and Cousot, POPL'79], obtained by a variant of the down-set completion construction of [Cousot and Cousot, JLP '92].
- An element of the powerset is a non-redundant and finite collection of objects of the base domain: each object in the collection has to be maximal wrt the partial order $\vdash$.
- The finite powerset domain over $\hat{D}$ is the join-semilattice

$$\hat{D}_{\mathrm{P}} := \langle \wp_{\mathrm{fn}}(D, \vdash), \vdash_{\mathrm{P}}, \mathbf{0}_{\mathrm{P}}, \oplus_{\mathrm{P}} \rangle,$$

where $\mathbf{0}_{\mathrm{P}} := \varnothing$ and $S_1 \oplus_{\mathrm{P}} S_2 := \Omega_D^{\vdash}(S_1 \cup S_2)$.

THE FINITE POWERSET CONSTRUCTION (II)

- The partial order $\vdash_{\mathrm{P}}$ corresponds to the Hoare's powerdomain ordering:
  $S_1 \vdash_{\mathrm{P}} S_2 \iff \forall d_1 \in S_1 : \exists d_2 \in S_2 \,.\, d_1 \vdash d_2$.
- A kind of Egli-Milner partial order relation will be also used:
  $S_1 \vdash_{\mathrm{EM}} S_2 \iff S_1 = \mathbf{0}_{\mathrm{P}} \vee \bigl(S_1 \vdash_{\mathrm{P}} S_2 \wedge \forall d_2 \in S_2 : \exists d_1 \in S_1 \,.\, d_1 \vdash d_2\bigr)$.

THE FINITE POWERSET CONSTRUCTION (II)

➜ The partial order $\vdash_{\mathrm{P}}$ corresponds to the Hoare's powerdomain ordering: $S_1 \vdash_{\mathrm{P}} S_2 \iff \forall d_1 \in S_1 : \exists d_2 \in S_2 \mathrel{.} d_1 \vdash d_2$.

➜ A kind of Egli-Milner partial order relation will be also used: $S_1 \vdash_{\mathrm{EM}} S_2 \iff S_1 = \mathbf{0}_{\mathrm{P}} \vee \big(S_1 \vdash_{\mathrm{P}} S_2 \wedge \forall d_2 \in S_2 : \exists d_1 \in S_1 \mathrel{.} d_1 \vdash d_2\big)$.

➜ The concretization function is $\gamma_{\mathrm{P}} : \wp_{\mathrm{fn}}(D, \vdash) \to C$ defined by

$$\gamma_{\mathrm{P}}(S) := \bigsqcup \{\, \gamma(d) \mid d \in S \,\}.$$

It is monotonic, but not necessarily injective.

The Finite Powerset Construction (II)

- The partial order $\vdash_{\mathrm{P}}$ corresponds to the Hoare's powerdomain ordering: $S_1 \vdash_{\mathrm{P}} S_2 \iff \forall d_1 \in S_1 : \exists d_2 \in S_2 \,.\, d_1 \vdash d_2$.
- A kind of Egli-Milner partial order relation will be also used: $S_1 \vdash_{\mathrm{EM}} S_2 \iff S_1 = \mathbf{0}_{\mathrm{P}} \vee \big(S_1 \vdash_{\mathrm{P}} S_2 \wedge \forall d_2 \in S_2 : \exists d_1 \in S_1 \,.\, d_1 \vdash d_2\big)$.
- The concretization function is $\gamma_{\mathrm{P}} \colon \wp_{\mathrm{fn}}(D, \vdash) \rightarrow C$ defined by

  $$\gamma_{\mathrm{P}}(S) := \bigsqcup \{\, \gamma(d) \mid d \in S \,\}.$$

  It is monotonic, but not necessarily injective.
- A correct abstract semantic function $\mathcal{F}_{\mathrm{P}}^{\sharp} \colon \wp_{\mathrm{fn}}(D, \vdash) \rightarrow \wp_{\mathrm{fn}}(D, \vdash)$ is assumed. This can be defined as the element-wise lifting

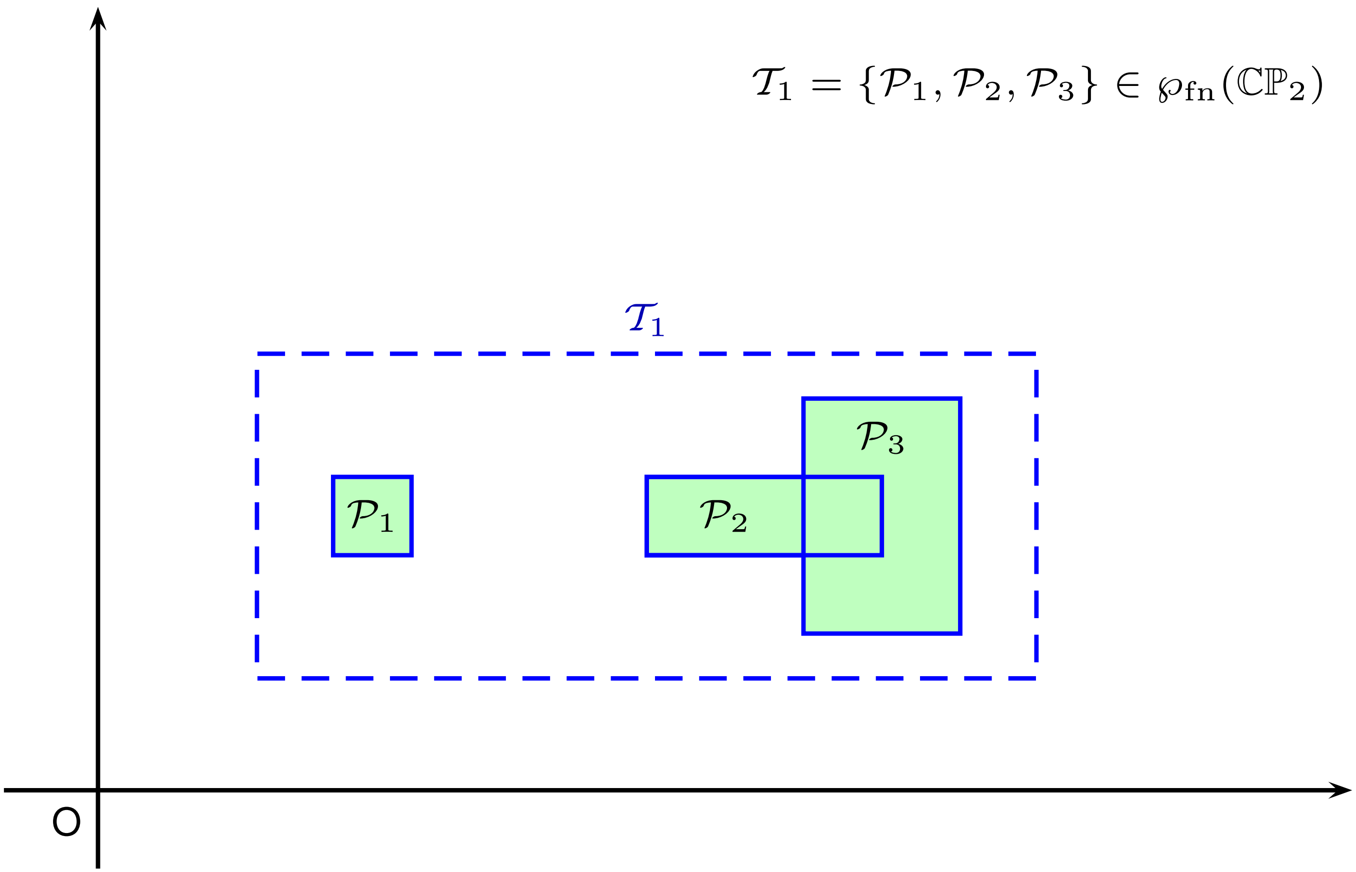
  $$\mathcal{F}_{\mathrm{P}}^{\sharp}(S) := \Omega_D^{\vdash}\Big(\{\, \mathcal{F}^{\sharp}(d) \mid d \in S \,\}\Big),$$

  provided, e.g., the concrete function $\mathcal{F}$ is additive.

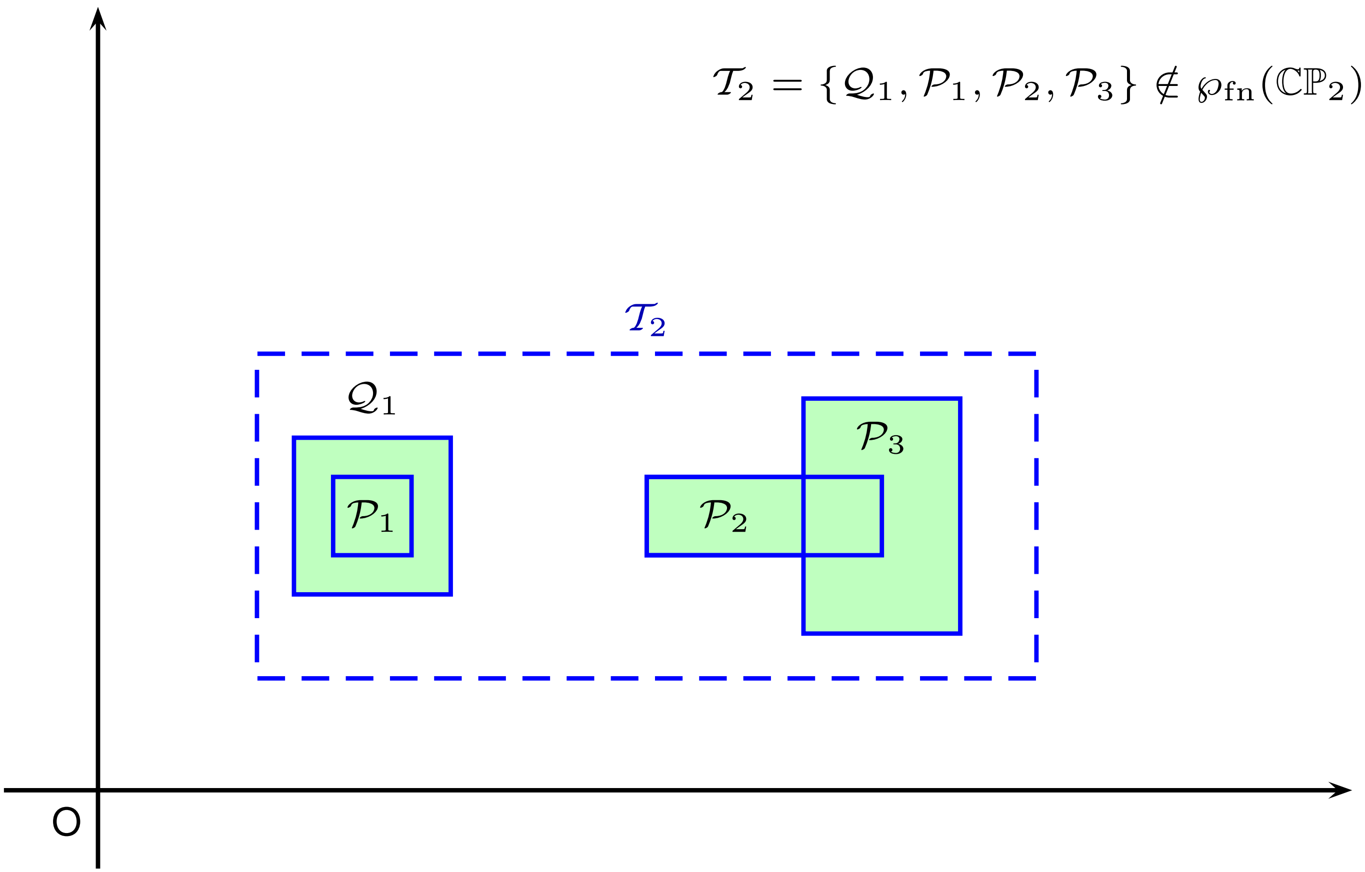
A WORKING EXAMPLE (III)

- The finite powerset of closed convex polyhedra is the (non-complete) join-semilattice $(\widehat{\mathbb{CP}_n})_{\mathrm{P}} := \langle \wp_{\mathrm{fn}}(\mathbb{CP}_n, \subseteq), \subseteq_{\mathrm{P}}, \varnothing, \uplus_{\mathrm{P}} \rangle$.
- The induced concretization function is $\gamma_{\mathrm{P}}(\mathcal{S}) := \bigcup \mathcal{S}$.
- Since additivity corresponds to linearity, many well-known abstract semantics operators (e.g., affine image and pre-image operators, conjunctions of linear constraints, projections, embeddings, etc.) can be easily lifted from $\widehat{\mathbb{CP}_n}$ to the powerset $(\widehat{\mathbb{CP}_n})_{\mathrm{P}}$.

A Working Example (iv)



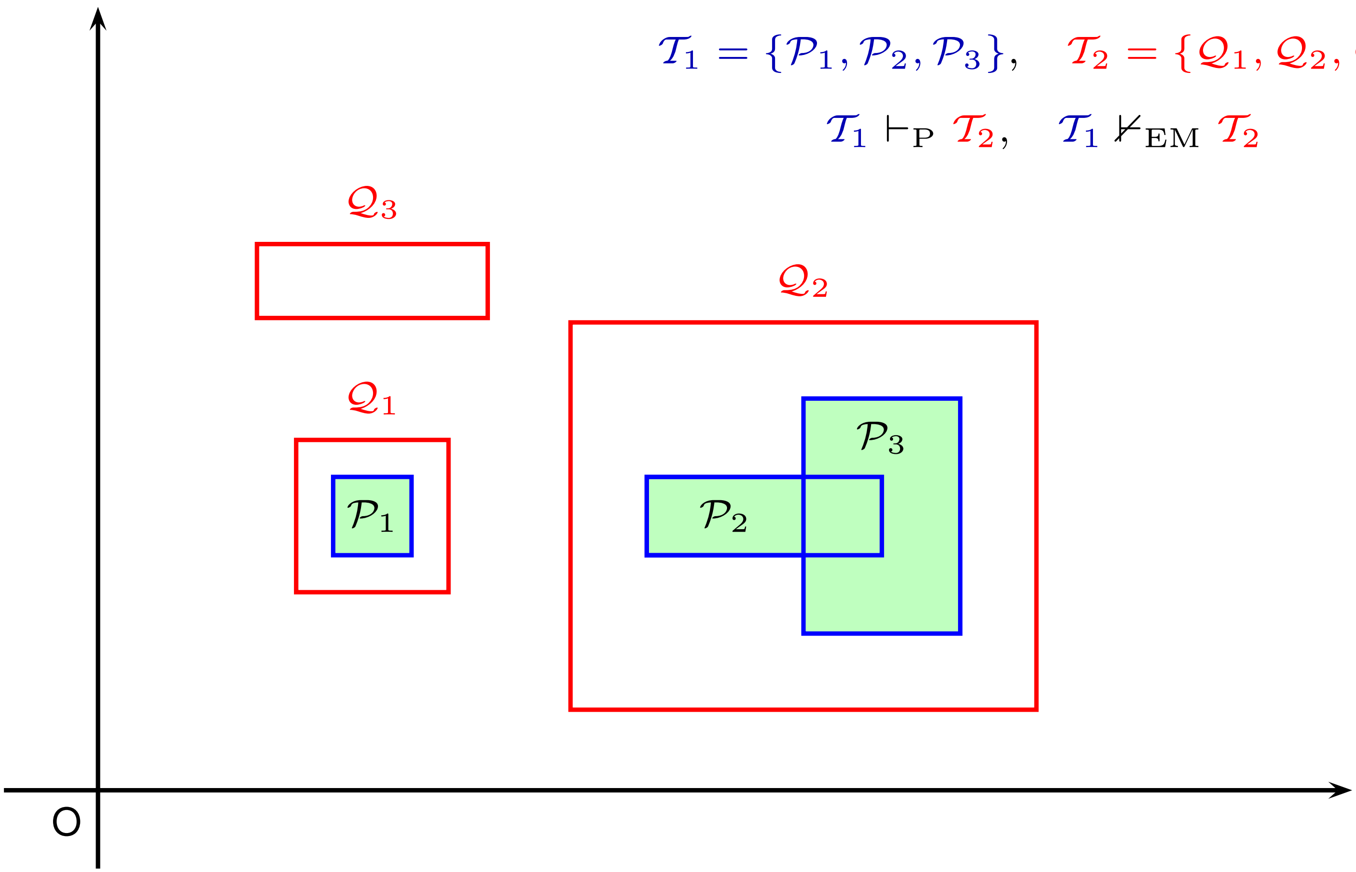
A Working Example (v)



A Working Example (vi)

$$\mathcal{T}_1 = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3\}, \quad \mathcal{T}_2 = \{\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3\}$$

$$\mathcal{T}_1 \vdash_{\mathrm{P}} \mathcal{T}_2, \quad \mathcal{T}_1 \nvdash_{\mathrm{EM}} \mathcal{T}_2$$



Problems in the Abstract Computation (Again)

- ➜ Infinite ascending chain may be obtained even when the base-level domain satisfies the ACC;
- ➜ The "limit" of the abstract computation may not be representable in the abstract domain (e.g., infinite collections of polyhedra);
- ➜ The element-wise lifting of ∇ is not a widening on $\hat{D}_{\mathrm{P}}$, since
  - ① the lifting may not be an upper bound operator, because the base-level widening ∇ may be undefined on some pairs;
  - ② the finite convergence guarantee can be lost.

Defining Extrapolation Heuristics

➜ The correctness problem can be solved by defining a ∇-connected extrapolation heuristics $h_{\mathrm{P}}^{\nabla} : \wp_{\mathrm{fn}}(D, \vdash)^2 \rightarrowtail \wp_{\mathrm{fn}}(D, \vdash)$: for all $S_1 \Vdash_{\mathrm{P}} S_2$,

$$S_2 \vdash_{\mathrm{EM}} h_{\mathrm{P}}^{\nabla}(S_1, S_2);$$

$$\forall d \in h_{\mathrm{P}}^{\nabla}(S_1, S_2) \setminus S_2 : \exists d_1 \in S_1 \;.\; d_1 \Vdash_{\nabla} d;$$

$$\forall d \in h_{\mathrm{P}}^{\nabla}(S_1, S_2) \cap S_2 : \big((\exists d_1 \in S_1 \;.\; d_1 \Vdash d) \rightarrow (\exists d_1' \in S_1 \;.\; d_1' \Vdash_{\nabla} d)\big).$$

Defining Extrapolation Heuristics

➜ The correctness problem can be solved by defining a ∇-connected extrapolation heuristics $h_{\mathrm{P}}^{\nabla} \colon \wp_{\mathrm{fn}}(D, \vdash)^2 \rightarrowtail \wp_{\mathrm{fn}}(D, \vdash)$: for all $S_1 \Vdash_{\mathrm{P}} S_2$,

$$S_2 \vdash_{\mathrm{EM}} h_{\mathrm{P}}^{\nabla}(S_1, S_2);$$

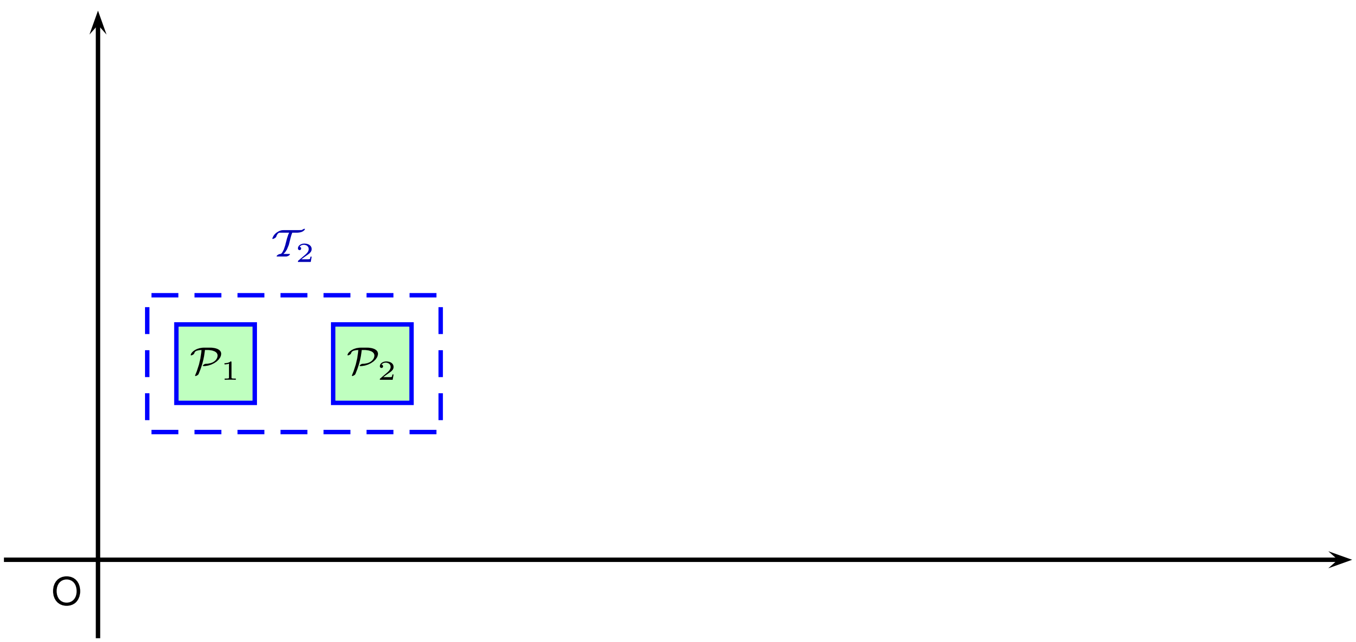
$$\forall d \in h_{\mathrm{P}}^{\nabla}(S_1, S_2) \setminus S_2 : \exists d_1 \in S_1 \;.\; d_1 \Vdash_{\nabla} d;$$

$$\forall d \in h_{\mathrm{P}}^{\nabla}(S_1, S_2) \cap S_2 : \bigl((\exists d_1 \in S_1 \;.\; d_1 \Vdash d) \rightarrow (\exists d_1' \in S_1 \;.\; d_1' \Vdash_{\nabla} d)\bigr).$$

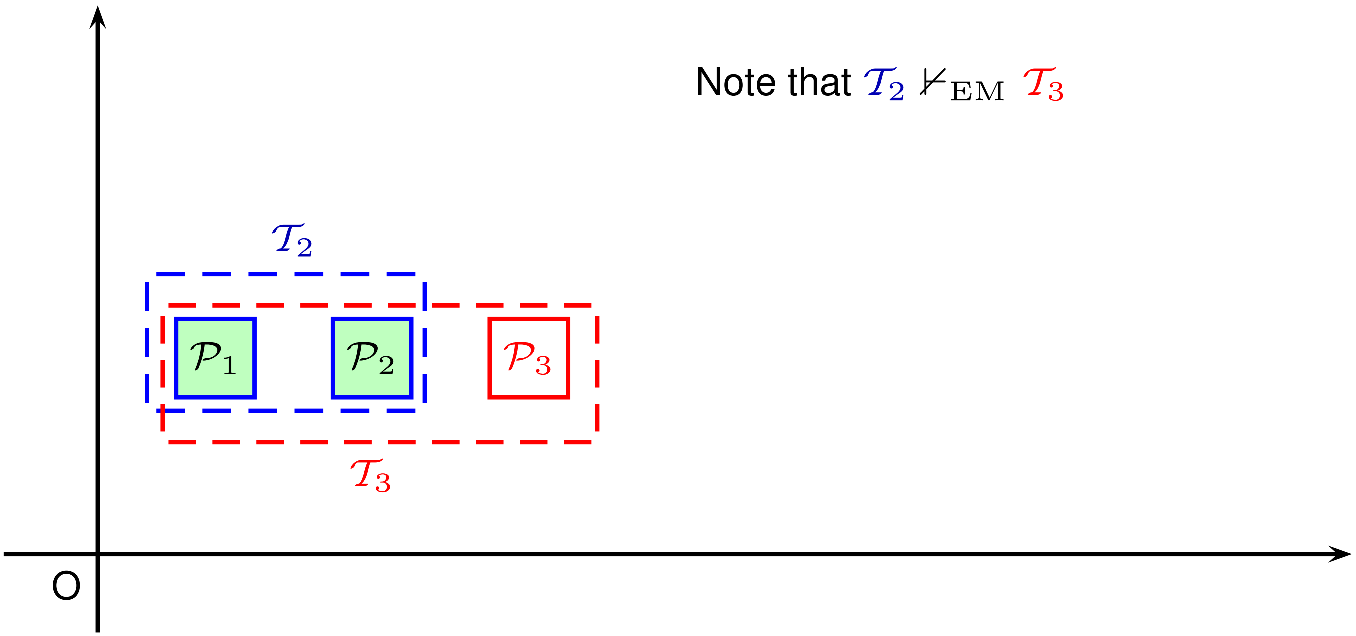
➜ For instance, the following is a generalized and simplified version of an operator proposed by [Bultan et al., TOPLAS'99]:

$$h_{\mathrm{P}}^{\nabla}(S_1, S_2) := S_2 \oplus_{\mathrm{P}} \Omega_D^{\vdash}\bigl(\{\, d_1 \nabla d_2 \in D \mid d_1 \in S_1, d_2 \in S_2, d_1 \Vdash d_2 \,\}\bigr).$$

No Finite Convergence Guarantee (i)

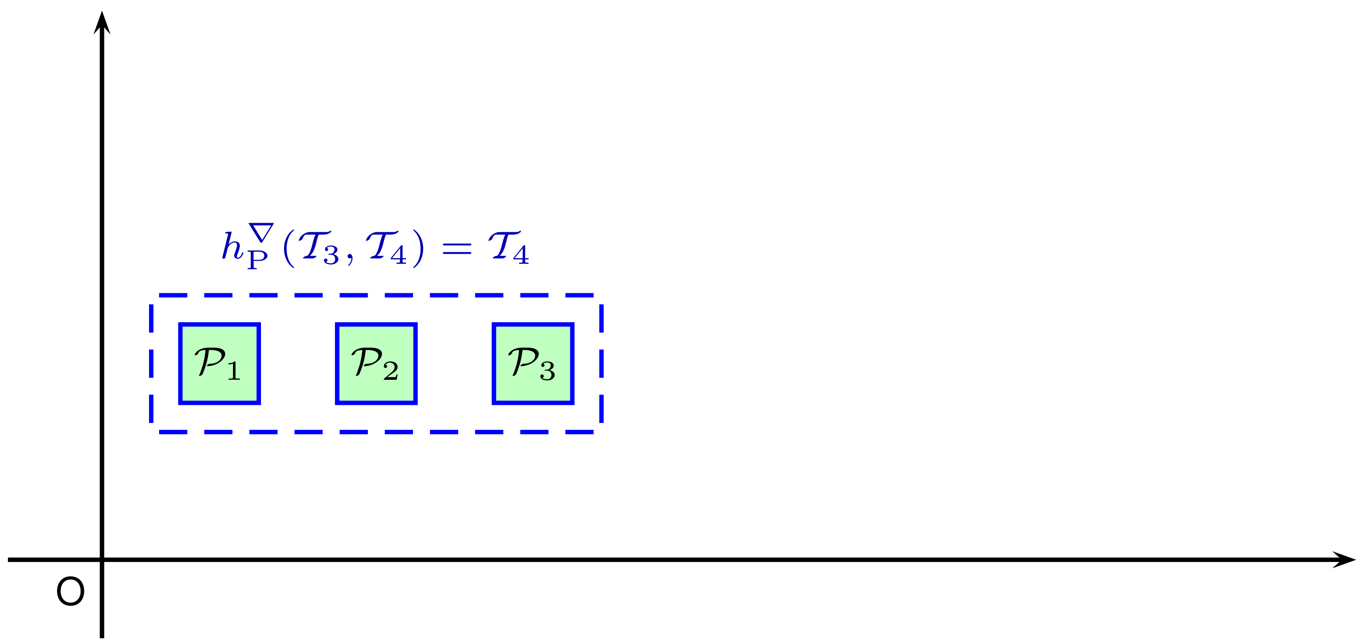


No Finite Convergence Guarantee (II)

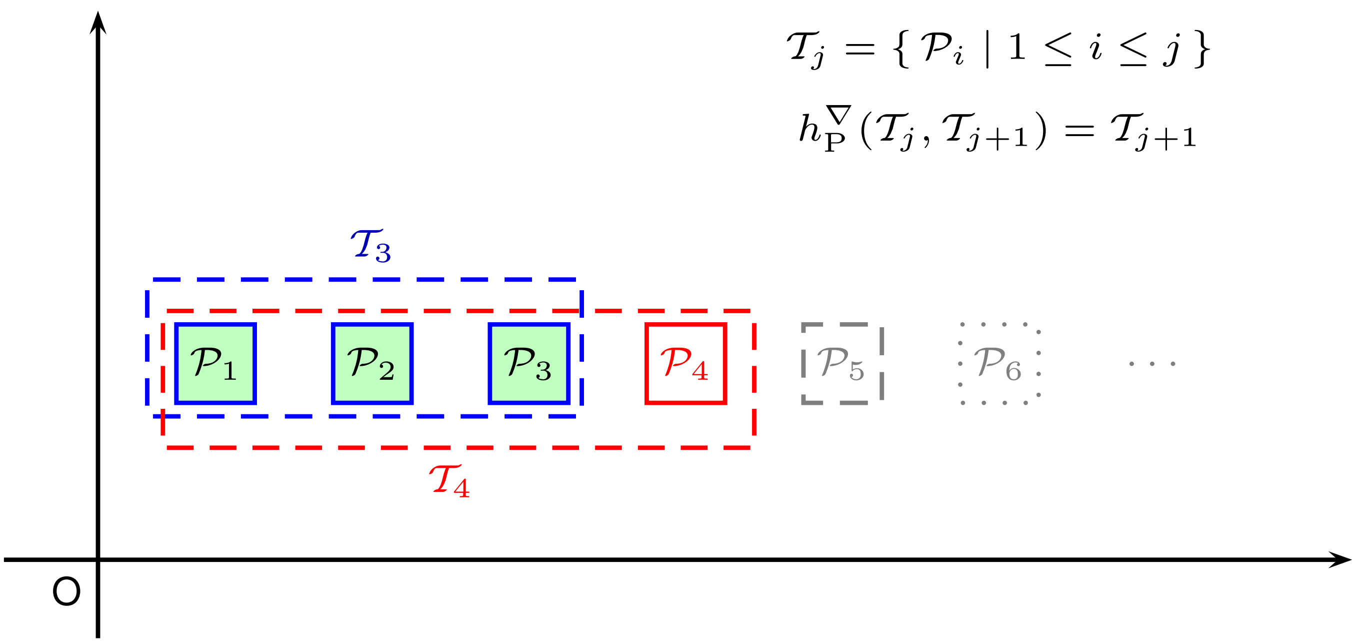


Note that $\mathcal{T}_2 \not\vdash_{\mathrm{EM}} \mathcal{T}_3$

No Finite Convergence Guarantee (III)



No Finite Convergence Guarantee (iv)



$$\mathcal{T}_j = \{ \mathcal{P}_i \mid 1 \leq i \leq j \}$$

$$h_{\mathrm{P}}^{\nabla}(\mathcal{T}_j, \mathcal{T}_{j+1}) = \mathcal{T}_{j+1}$$

WIDENINGS BASED ON A CARDINALITY THRESHOLD?

➜ To solve this convergence problem, the "widening" operator proposed in [Bultan et al., TOPLAS'99] fixes an upper bound $k \in \mathbb{N}$ for the number of disjuncts in an abstract collection. When the second argument S_2 reaches this cardinality threshold, it is replaced by $\Uparrow_k(S_2)$, where some of the disjuncts are collapsed (or "coalesced" [Bourdoncle, JFP'92]), i.e., replaced by their join.

WIDENINGS BASED ON A CARDINALITY THRESHOLD?

➜ To solve this convergence problem, the “widening” operator proposed in [Bultan et al., TOPLAS’99] fixes an upper bound $k \in \mathbb{N}$ for the number of disjuncts in an abstract collection. When the second argument S_2 reaches this cardinality threshold, it is replaced by $\Uparrow_k(S_2)$, where some of the disjuncts are collapsed (or “coalesced” [Bourdoncle, JFP’92]), i.e., replaced by their join.

➜ There is an example showing that this strategy may fail to enforce the finite convergence guarantee. The reason is that the reduction operator $\Omega_D^{\vdash}$ interferes with the extrapolation heuristics h_{P}^{∇}, so that the threshold k is never reached.

WIDENINGS BASED ON A CARDINALITY THRESHOLD?

- To solve this convergence problem, the "widening" operator proposed in [Bultan et al., TOPLAS'99] fixes an upper bound $k \in \mathbb{N}$ for the number of disjuncts in an abstract collection. When the second argument S_2 reaches this cardinality threshold, it is replaced by $\Uparrow_k(S_2)$, where some of the disjuncts are collapsed (or "coalesced" [Bourdoncle, JFP'92]), i.e., replaced by their join.
- There is an example showing that this strategy may fail to enforce the finite convergence guarantee. The reason is that the reduction operator $\Omega_D^{\vdash}$ interferes with the extrapolation heuristics h_{P}^{∇}, so that the threshold k is never reached.
- Anyway, the above approach can be "patched" by considering a different extrapolation heuristics (see the TR version of our paper).

WIDENINGS BASED ON EGLI-MILNER CONNECTORS (I)

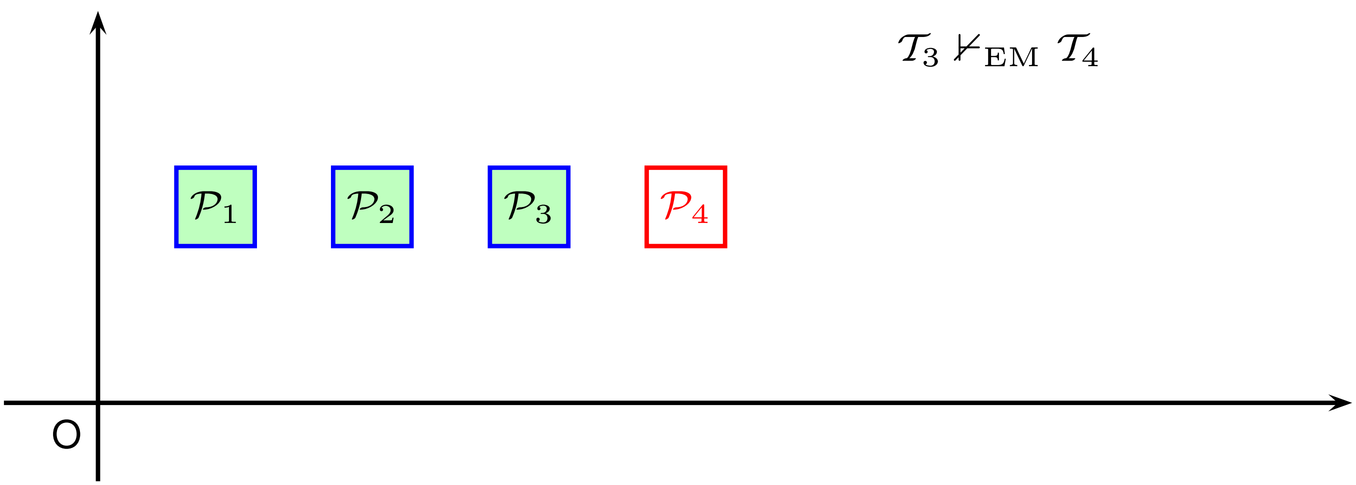
➜ An Egli-Milner connector $\boxplus_{\mathrm{EM}}$ is an upper bound for the relation $\vdash_{\mathrm{EM}}$.

WIDENINGS BASED ON EGLI-MILNER CONNECTORS (I)

- An Egli-Milner connector $\boxplus_{\mathrm{EM}}$ is an upper bound for the relation $\vdash_{\mathrm{EM}}$.
- For any EM-connector $\boxplus_{\mathrm{EM}}$ and any ∇-connected extrapolation heuristics h^{∇}_{P}, let $S_1 \;_{\mathrm{EM}}\nabla_{\mathrm{P}}\; S_2 := h^{\nabla}_{\mathrm{P}}(S_1, S_1 \boxplus_{\mathrm{EM}} S_2)$.

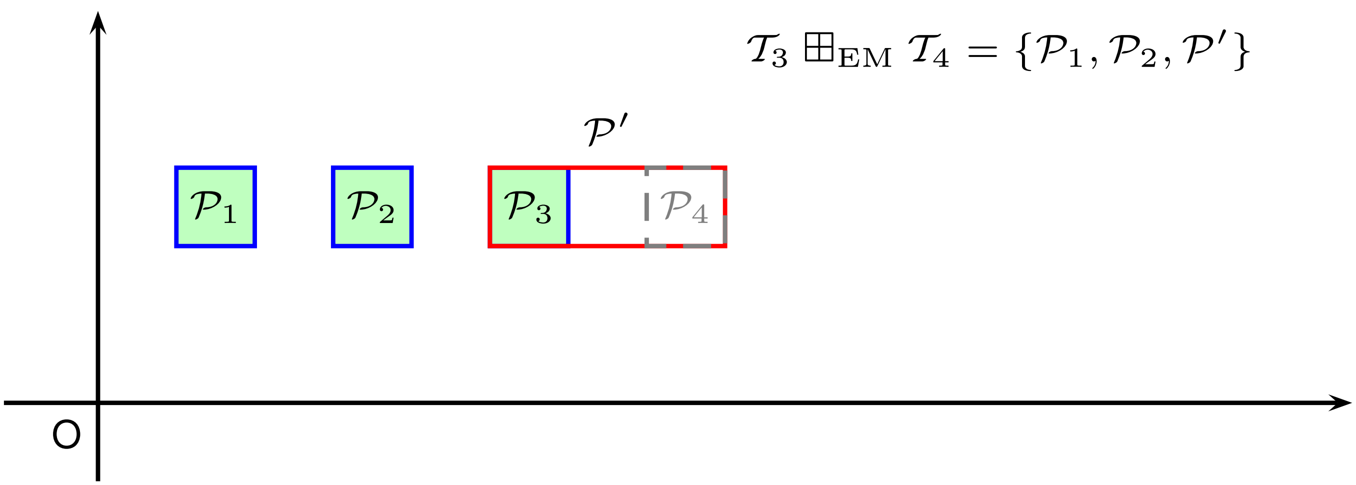
WIDENINGS BASED ON EGLI-MILNER CONNECTORS (I)

- ➜ An Egli-Milner connector $\boxplus_{\mathrm{EM}}$ is an upper bound for the relation $\vdash_{\mathrm{EM}}$.
- ➜ For any EM-connector $\boxplus_{\mathrm{EM}}$ and any ∇-connected extrapolation heuristics h^{∇}_{P}, let $S_1 \;{}_{\mathrm{EM}}\nabla_{\mathrm{P}}\; S_2 := h^{\nabla}_{\mathrm{P}}(S_1, S_1 \boxplus_{\mathrm{EM}} S_2)$.



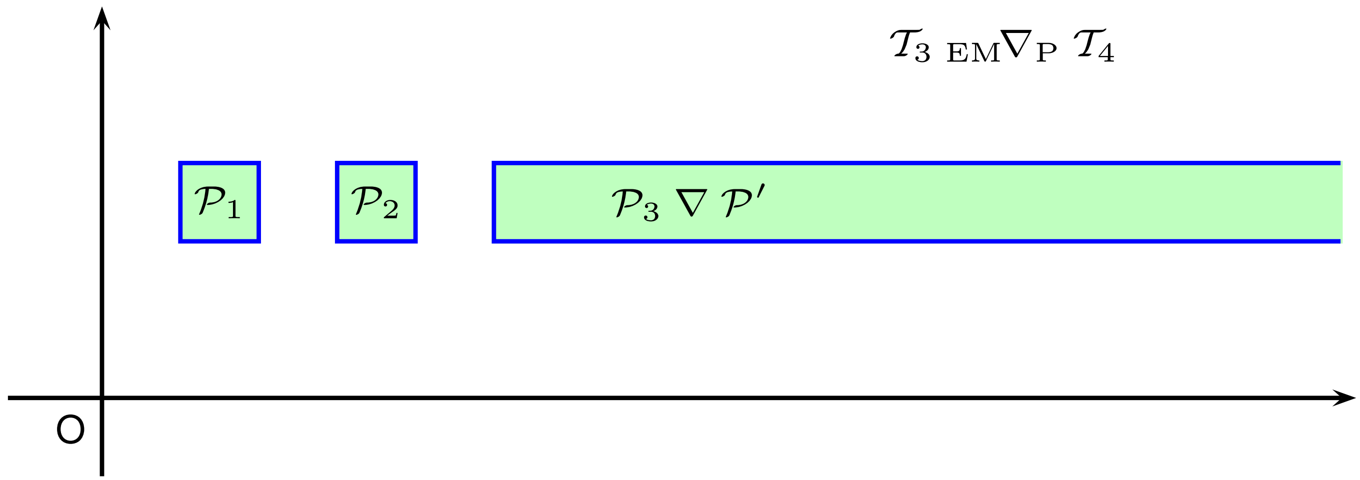
Widenings Based on Egli-Milner connectors (II)

- An Egli-Milner connector $\boxplus_{\mathrm{EM}}$ is an upper bound for the relation $\vdash_{\mathrm{EM}}$;
- For any EM-connector $\boxplus_{\mathrm{EM}}$ and any ∇-connected extrapolation heuristics h_{P}^{∇}, let $S_1 \;{}_{\mathrm{EM}}\nabla_{\mathrm{P}}\; S_2 := h_{\mathrm{P}}^{\nabla}(S_1, S_1 \boxplus_{\mathrm{EM}} S_2)$.



WIDENINGS BASED ON EGLI-MILNER CONNECTORS (III)

- An Egli-Milner connector $\boxplus_{\mathrm{EM}}$ is an upper bound for the relation $\vdash_{\mathrm{EM}}$;
- For any EM-connector $\boxplus_{\mathrm{EM}}$ and any ∇-connected extrapolation heuristics h_{P}^{∇}, let $S_1 \;{}_{\mathrm{EM}}\nabla_{\mathrm{P}}\; S_2 := h_{\mathrm{P}}^{\nabla}(S_1, S_1 \boxplus_{\mathrm{EM}} S_2)$.



WIDENINGS BASED ON CERTIFICATES

- A possible tactic when proving that an upper bound operator $\boxplus\colon D \times D \to D$ is indeed a widening on $\hat{D}$ is to provide a sort of "convergence certificate."

Widenings Based on Certificates

- ➜ A possible tactic when proving that an upper bound operator $\boxplus \colon D \times D \to D$ is indeed a widening on $\hat{D}$ is to provide a sort of "convergence certificate."
- ➜ A finite convergence certificate for $\boxplus$ on $\hat{D}$ is a triple $(\mathcal{O}, \succ, \mu)$ where
  ① $\mathcal{O}$ is a set with well-founded ordering $\succ$;
  ② $\mu \colon D \to \mathcal{O}$, which is called level mapping, satisfies
  $\forall d_1, d_2 \in D : d_1 \Vdash d_2 \implies \mu(d_1) \succ \mu(d_1 \boxplus d_2)$.

Widenings Based on Certificates

➜ A possible tactic when proving that an upper bound operator $\boxplus \colon D \times D \rightarrow D$ is indeed a widening on $\hat{D}$ is to provide a sort of "convergence certificate."

➜ A finite convergence certificate for $\boxplus$ on $\hat{D}$ is a triple $(\mathcal{O}, \succ, \mu)$ where

① $\mathcal{O}$ is a set with well-founded ordering $\succ$;

② $\mu \colon D \rightarrow \mathcal{O}$, which is called level mapping, satisfies

$$\forall d_1, d_2 \in D : d_1 \Vdash d_2 \implies \mu(d_1) \succ \mu(d_1 \boxplus d_2).$$

➜ For instance, a certificate for the standard widening on $\widehat{\mathbb{CP}}_n$ can be obtained by taking $(\mathcal{O}, \succ)$ be the lexicographic product of two copies of $(\mathbb{N}, >)$ and defining $\mu(\mathcal{P}) = \bigl(n - \dim(\mathcal{P}), \# \mathcal{C}\bigr)$, where $\mathcal{C}$ is a constraint system in minimal form for $\mathcal{P}$.

Widenings Based on Certificates

- A possible tactic when proving that an upper bound operator $\boxplus \colon D \times D \to D$ is indeed a widening on $\hat{D}$ is to provide a sort of "convergence certificate."
- A finite convergence certificate for $\boxplus$ on $\hat{D}$ is a triple $(\mathcal{O}, \succ, \mu)$ where
  1. $\mathcal{O}$ is a set with well-founded ordering $\succ$;
  2. $\mu \colon D \to \mathcal{O}$, which is called level mapping, satisfies
     $\forall d_1, d_2 \in D : d_1 \Vdash d_2 \implies \mu(d_1) \succ \mu(d_1 \boxplus d_2)$.
- For instance, a certificate for the standard widening on $\widehat{\mathbb{CP}}_n$ can be obtained by taking $(\mathcal{O}, \succ)$ be the lexicographic product of two copies of $(\mathbb{N}, >)$ and defining $\mu(\mathcal{P}) = \bigl(n - \dim(\mathcal{P}), \#\,\mathcal{C}\bigr)$, where $\mathcal{C}$ is a constraint system in minimal form for $\mathcal{P}$.
- A finitely computable certificate can be used to lift a widening operator on $\hat{D}$ to work on the finite powerset domain $\hat{D}_{\mathrm{P}}$.

Lifting the Certificate on the Powerset Domain

➜ Let $(\mathcal{O}, \succ, \mu)$ be a certificate for a widening ∇ on $\hat{D}$.

LIFTING THE CERTIFICATE ON THE POWERSET DOMAIN

- Let $(\mathcal{O}, \succ, \mu)$ be a certificate for a widening ∇ on $\hat{D}$.
- The relation $\curvearrowright_{\mathrm{P}} \subseteq \wp_{\mathrm{fn}}(D, \vdash) \times \wp_{\mathrm{fn}}(D, \vdash)$ is such that $S_1 \curvearrowright_{\mathrm{P}} S_2$ iff one of the following holds:

$$\mu(\oplus S_1) \succ \mu(\oplus S_2);$$

$$\mu(\oplus S_1) = \mu(\oplus S_2) \wedge \# S_1 > 1 \wedge \# S_2 = 1;$$

$$\mu\bigl(\oplus S_1) = \mu(\oplus S_2) \wedge \# S_1 > 1 \wedge \# S_2 > 1 \wedge \tilde{\mu}(S_1) \gg \tilde{\mu}(S_2)$$

where $\tilde{\mu}(S)$ denotes the multiset over $\mathcal{O}$ obtained by applying μ to each abstract element in S.

Lifting the Certificate on the Powerset Domain

- Let $(\mathcal{O}, \succ, \mu)$ be a certificate for a widening ∇ on $\hat{D}$.
- The relation $\curvearrowright_{\mathrm{P}} \subseteq \wp_{\mathrm{fn}}(D, \vdash) \times \wp_{\mathrm{fn}}(D, \vdash)$ is such that $S_1 \curvearrowright_{\mathrm{P}} S_2$ iff one of the following holds:

$$\mu(\oplus S_1) \succ \mu(\oplus S_2);$$

$$\mu(\oplus S_1) = \mu(\oplus S_2) \land \# S_1 > 1 \land \# S_2 = 1;$$

$$\mu\big(\oplus S_1) = \mu(\oplus S_2) \land \# S_1 > 1 \land \# S_2 > 1 \land \tilde{\mu}(S_1) \gg \tilde{\mu}(S_2)$$

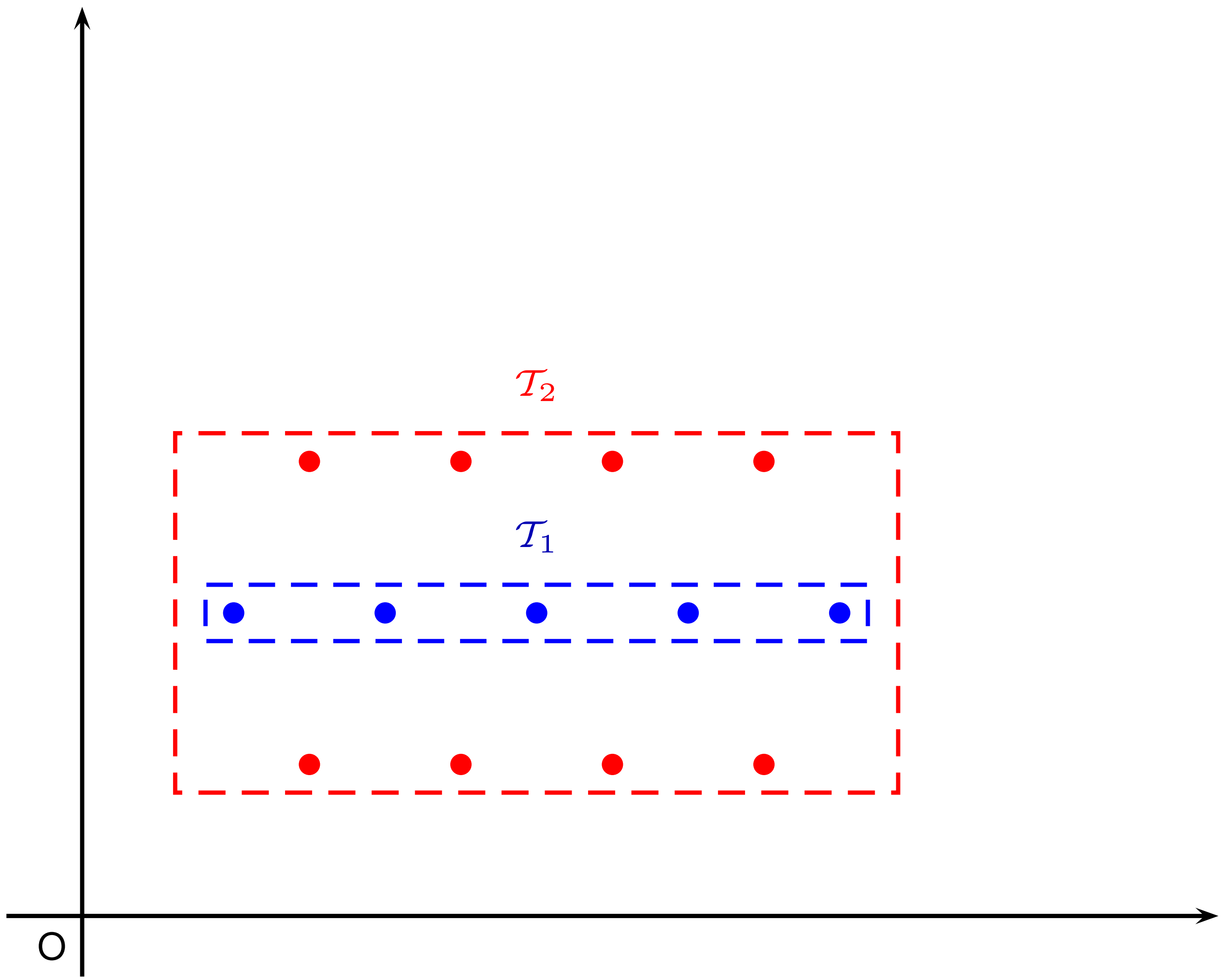
where $\tilde{\mu}(S)$ denotes the multiset over $\mathcal{O}$ obtained by applying μ to each abstract element in S.

- $\curvearrowright_{\mathrm{P}}$ satisfies the ACC.
- Intuitively, a certificate $(\mathcal{O}_{\mathrm{P}}, \succ_{\mathrm{P}}, \mu_{\mathrm{P}})$ for $\hat{D}_{\mathrm{P}}$ will be defined as

$$\mu_{\mathrm{P}}(S_1) \succ_{\mathrm{P}} \mu_{\mathrm{P}}(S_2) \iff S_1 \curvearrowright_{\mathrm{P}} S_2;$$

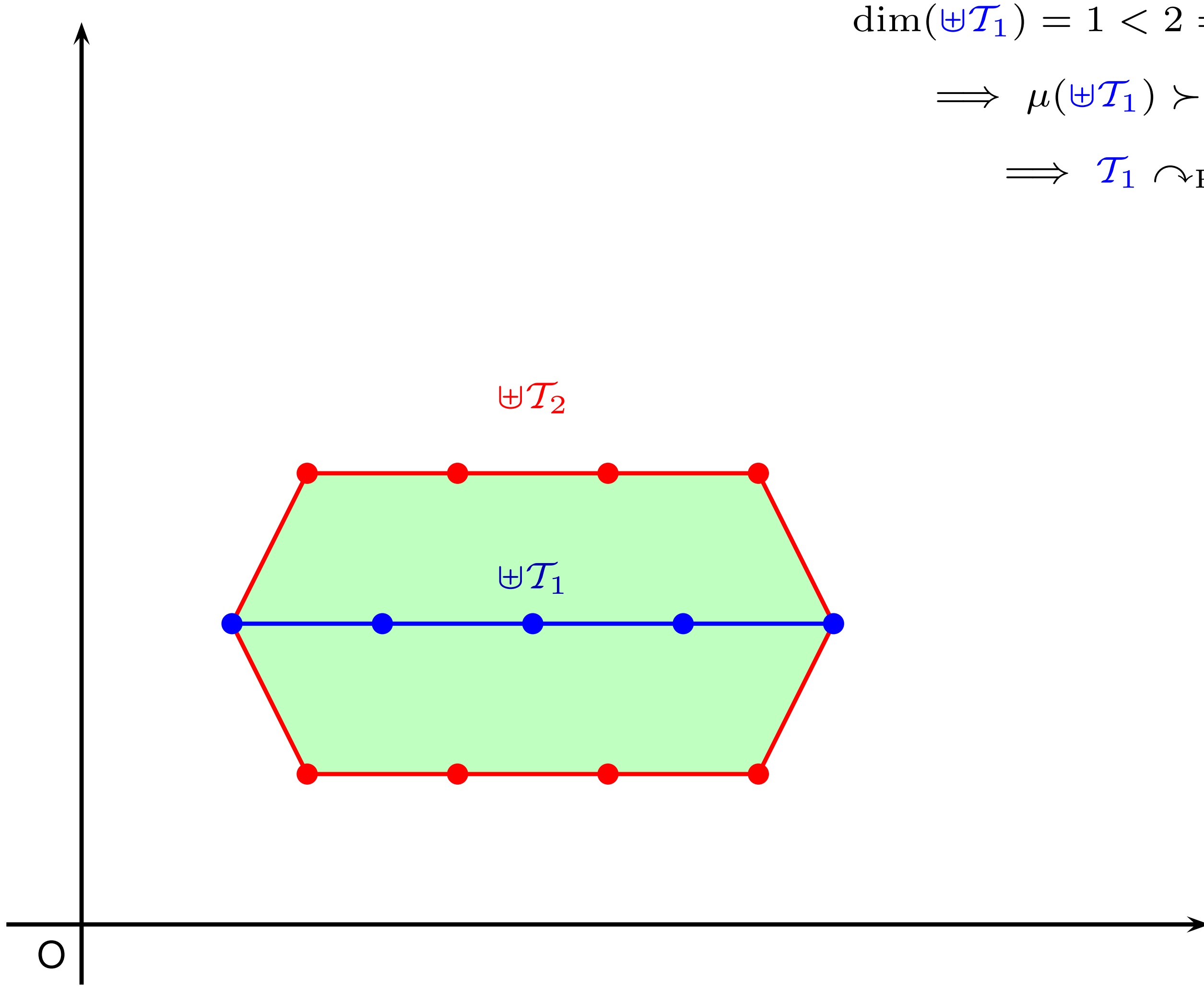
$$\mu_{\mathrm{P}}(S_1) = \mu_{\mathrm{P}}(S_2) \iff S_1 \not\curvearrowright_{\mathrm{P}} S_2 \land S_2 \not\curvearrowright_{\mathrm{P}} S_1.$$

Lifting the Certificate: 1st Case (i)



Lifting the Certificate: 1st Case (ii)

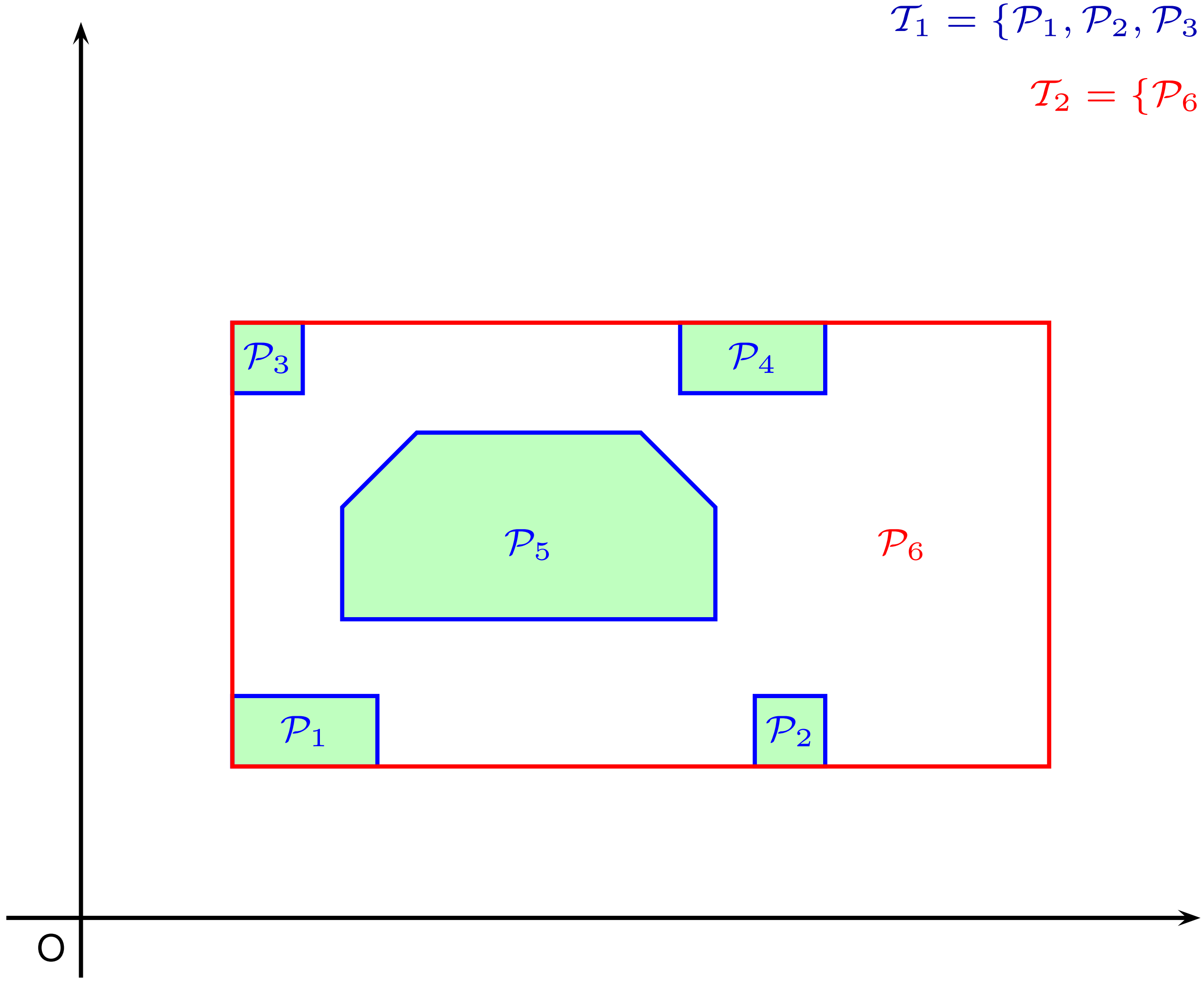
$$\dim(\uplus \mathcal{T}_1) = 1 < 2 = \dim(\uplus \mathcal{T}_2)$$
$$\implies \mu(\uplus \mathcal{T}_1) \succ \mu(\uplus \mathcal{T}_2)$$
$$\implies \mathcal{T}_1 \curvearrowright_{\mathrm{P}} \mathcal{T}_2$$



Lifting the Certificate: 2nd Case (i)

$\mathcal{T}_1 = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{P}_4, \mathcal{P}_5\}$

$\mathcal{T}_2 = \{\mathcal{P}_6\}$

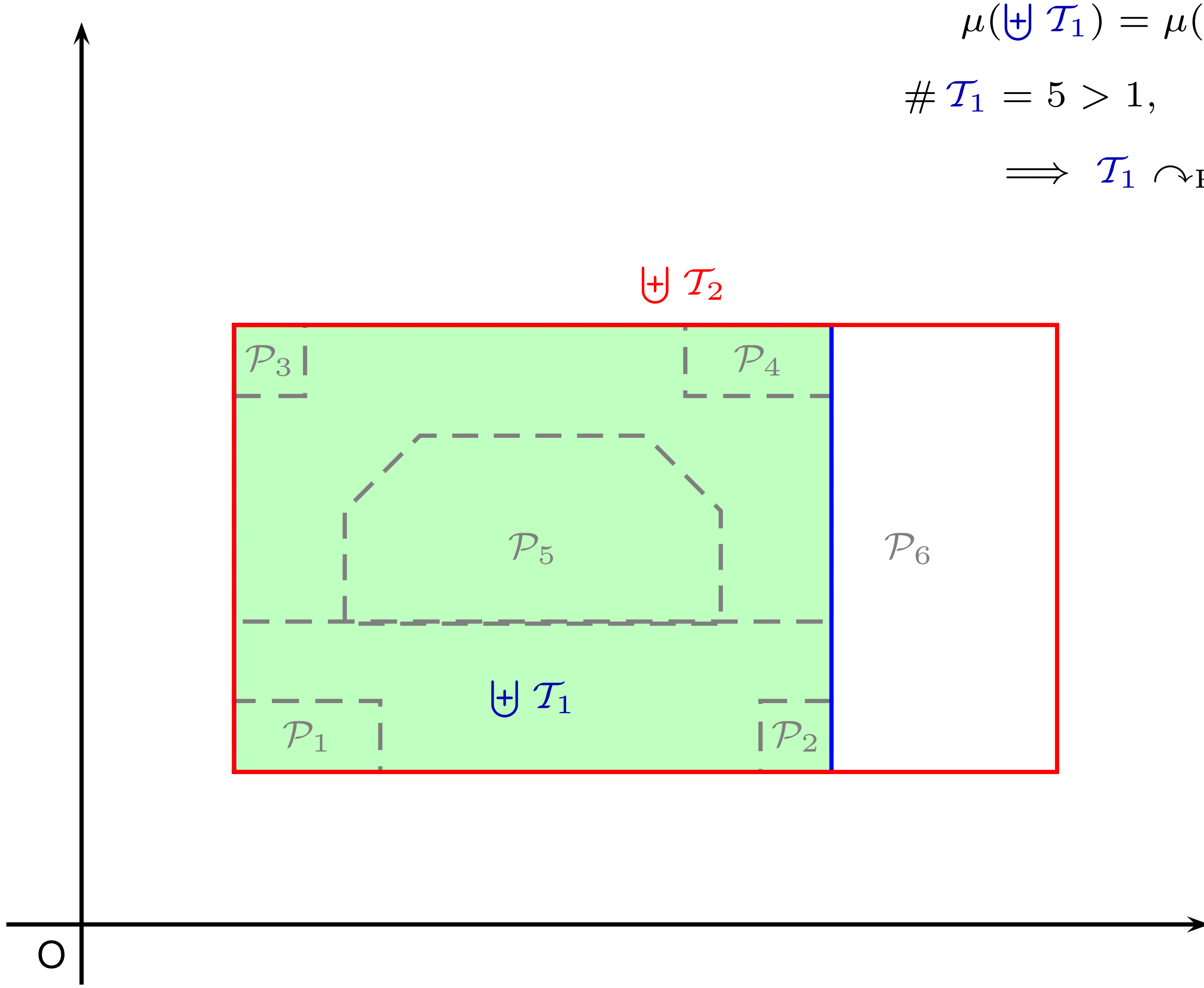


Lifting the Certificate: 2nd Case (ii)

$$\mu(\biguplus \mathcal{T}_1) = \mu(\biguplus \mathcal{T}_2)$$

$$\# \mathcal{T}_1 = 5 > 1, \quad \# \mathcal{T}_2 = 1$$

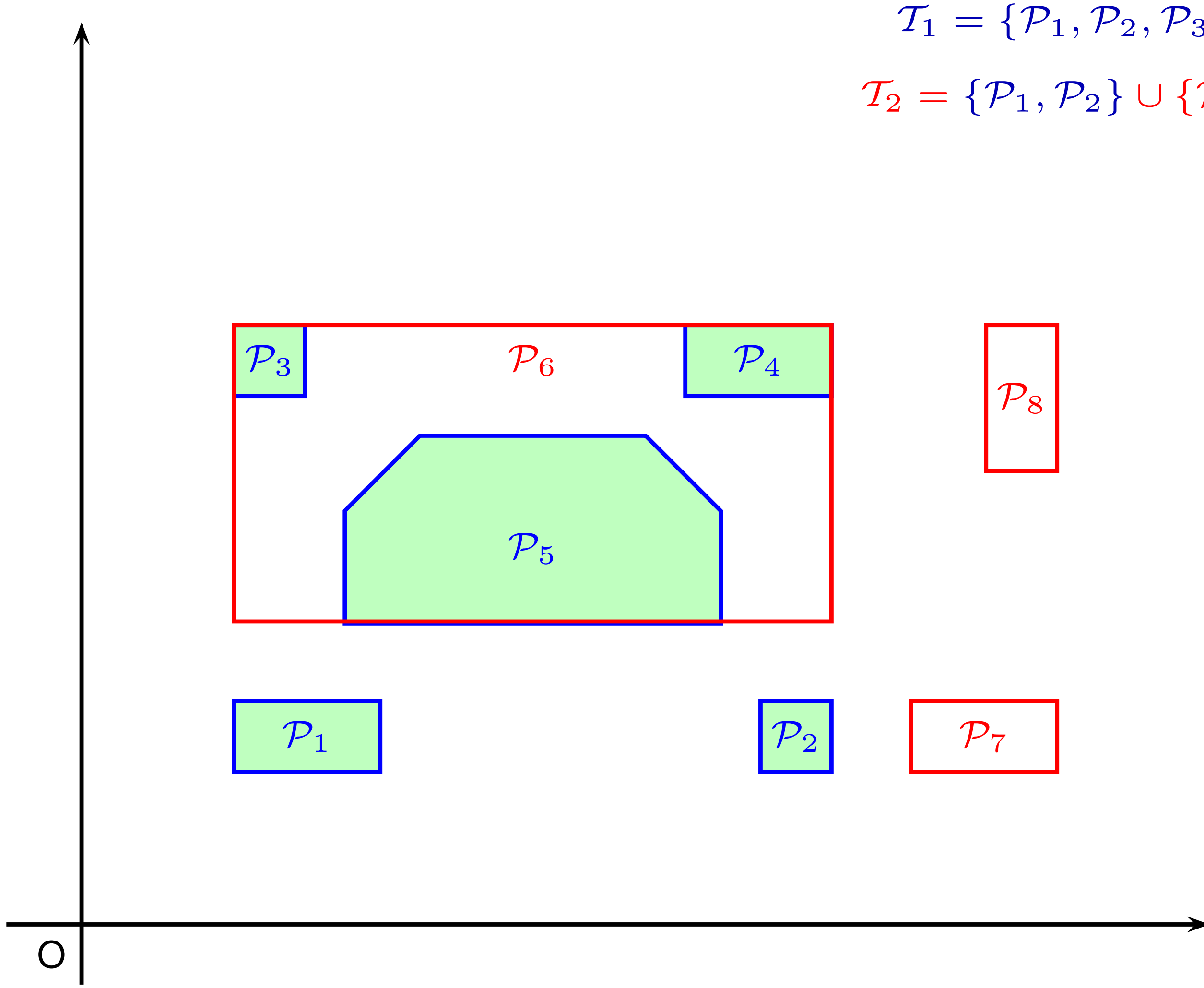
$$\Longrightarrow \mathcal{T}_1 \curvearrowright_{\mathrm{P}} \mathcal{T}_2$$



Lifting the Certificate: 3rd Case (i)

$$\mathcal{T}_1 = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{P}_4, \mathcal{P}_5\}$$

$$\mathcal{T}_2 = \{\mathcal{P}_1, \mathcal{P}_2\} \cup \{\mathcal{P}_6, \mathcal{P}_7, \mathcal{P}_8\}$$

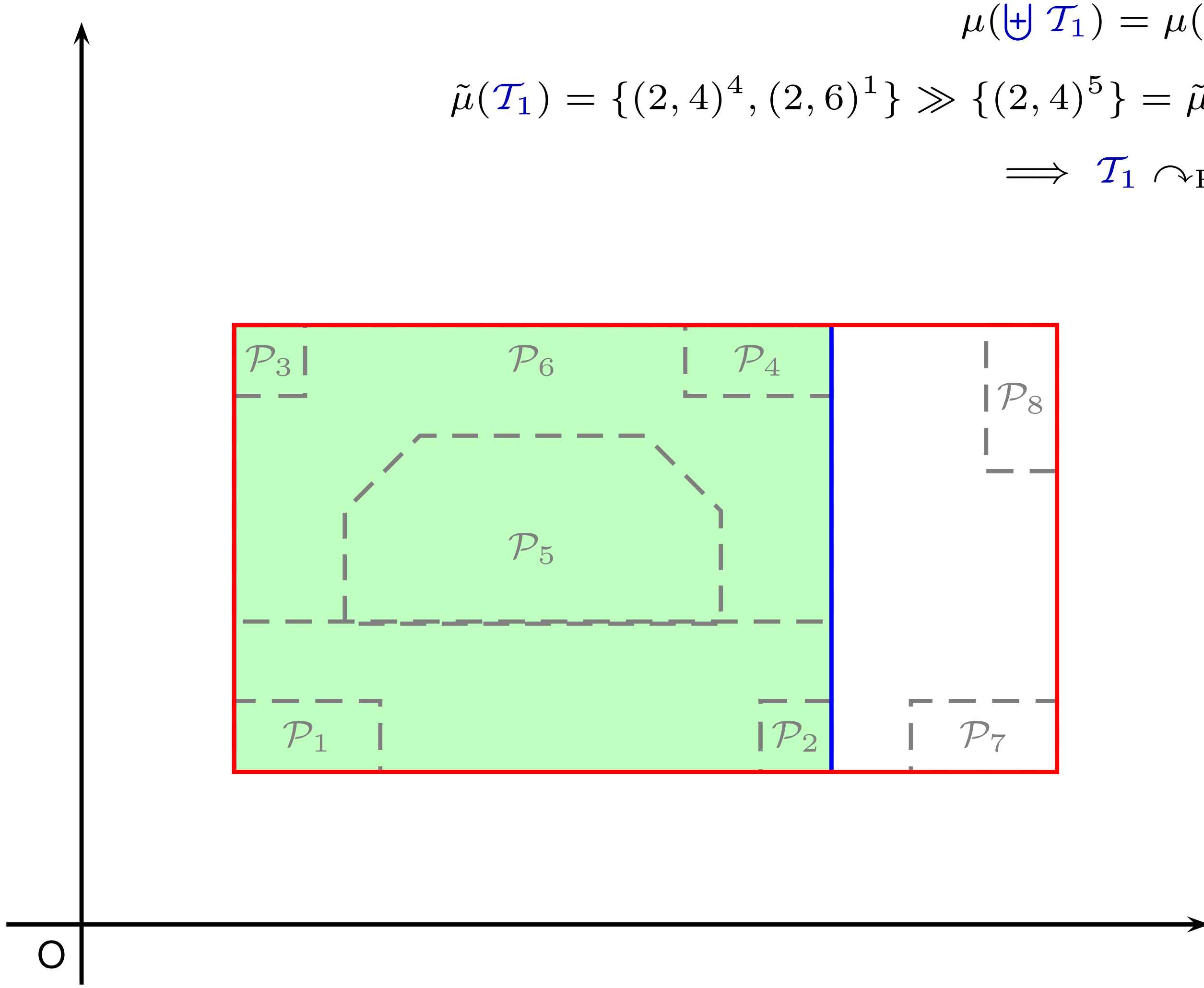


Lifting the Certificate: 3rd Case (ii)

$$\mu(\biguplus \mathcal{T}_1) = \mu(\biguplus \mathcal{T}_2)$$

$$\tilde{\mu}(\mathcal{T}_1) = \{(2,4)^4, (2,6)^1\} \gg \{(2,4)^5\} = \tilde{\mu}(\mathcal{T}_2)$$

$$\implies \mathcal{T}_1 \curvearrowright_{\mathrm{P}} \mathcal{T}_2$$



A Certificate-Based Widening

- A subtraction for $\hat{D}$ is a partial operator $\ominus \colon D \times D \rightarrowtail D$ such that $d_2 \vdash d_1$ implies both $d_1 \ominus d_2 \vdash d_1$ and $d_1 = (d_1 \ominus d_2) \oplus d_2$.
- For $\widehat{\mathbb{CP}}_n$, the closed convex set-difference operator is a subtraction.

A CERTIFICATE-BASED WIDENING

- A subtraction for $\hat{D}$ is a partial operator $\ominus \colon D \times D \rightarrowtail D$ such that $d_2 \vdash d_1$ implies both $d_1 \ominus d_2 \vdash d_1$ and $d_1 = (d_1 \ominus d_2) \oplus d_2$.
- For $\widehat{\mathbb{CP}}_n$, the closed convex set-difference operator is a subtraction.
- A certificate-based widening ${}_\mu\nabla_{\mathrm{P}}$ is such that

$$S_1 \; {}_\mu\nabla_{\mathrm{P}} \; S_2 := \begin{cases} S_1 \boxplus_{\mathrm{P}} S_2, & \text{if } S_1 \curvearrowright_{\mathrm{P}} S_1 \boxplus_{\mathrm{P}} S_2; \\ (S_1 \boxplus_{\mathrm{P}} S_2) \oplus_{\mathrm{P}} \{d\}, & \text{if } \bigoplus S_1 \Vdash \bigoplus (S_1 \boxplus_{\mathrm{P}} S_2); \\ \{\bigoplus S_2\}, & \text{otherwise.} \end{cases}$$

where $\boxplus_{\mathrm{P}}$ is an arbitrary upper bound operator for $\hat{D}_{\mathrm{P}}$ and
$d = \left(\bigoplus S_1 \nabla \bigoplus (S_1 \boxplus_{\mathrm{P}} S_2)\right) \ominus \left(\bigoplus (S_1 \boxplus_{\mathrm{P}} S_2)\right)$.

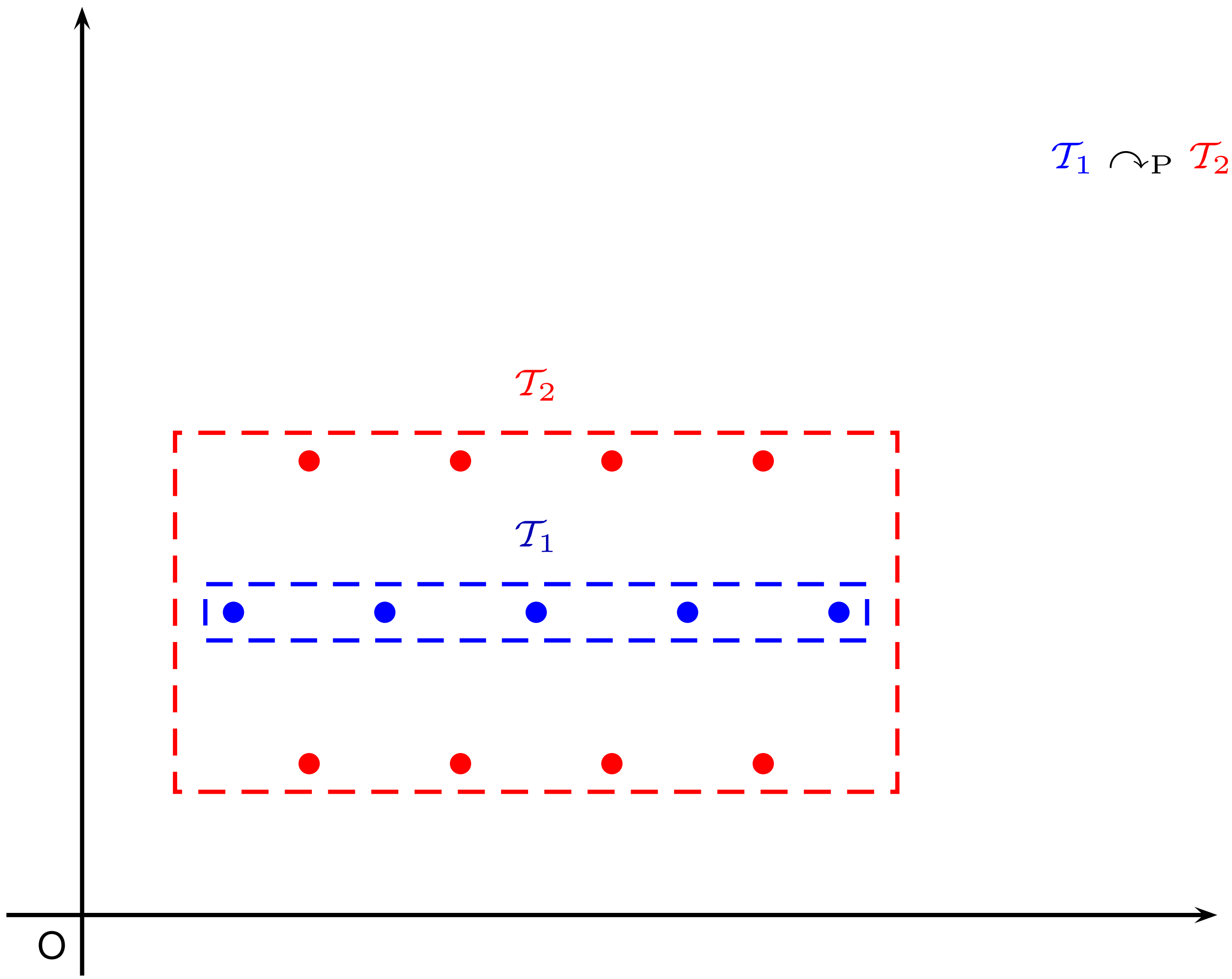
A Certificate-Based Widening

- A subtraction for $\hat{D}$ is a partial operator $\ominus \colon D \times D \rightarrowtail D$ such that $d_2 \vdash d_1$ implies both $d_1 \ominus d_2 \vdash d_1$ and $d_1 = (d_1 \ominus d_2) \oplus d_2$.
- For $\widehat{\mathbb{CP}}_n$, the closed convex set-difference operator is a subtraction.
- A certificate-based widening ${}_{\mu}\nabla_{\mathrm{P}}$ is such that

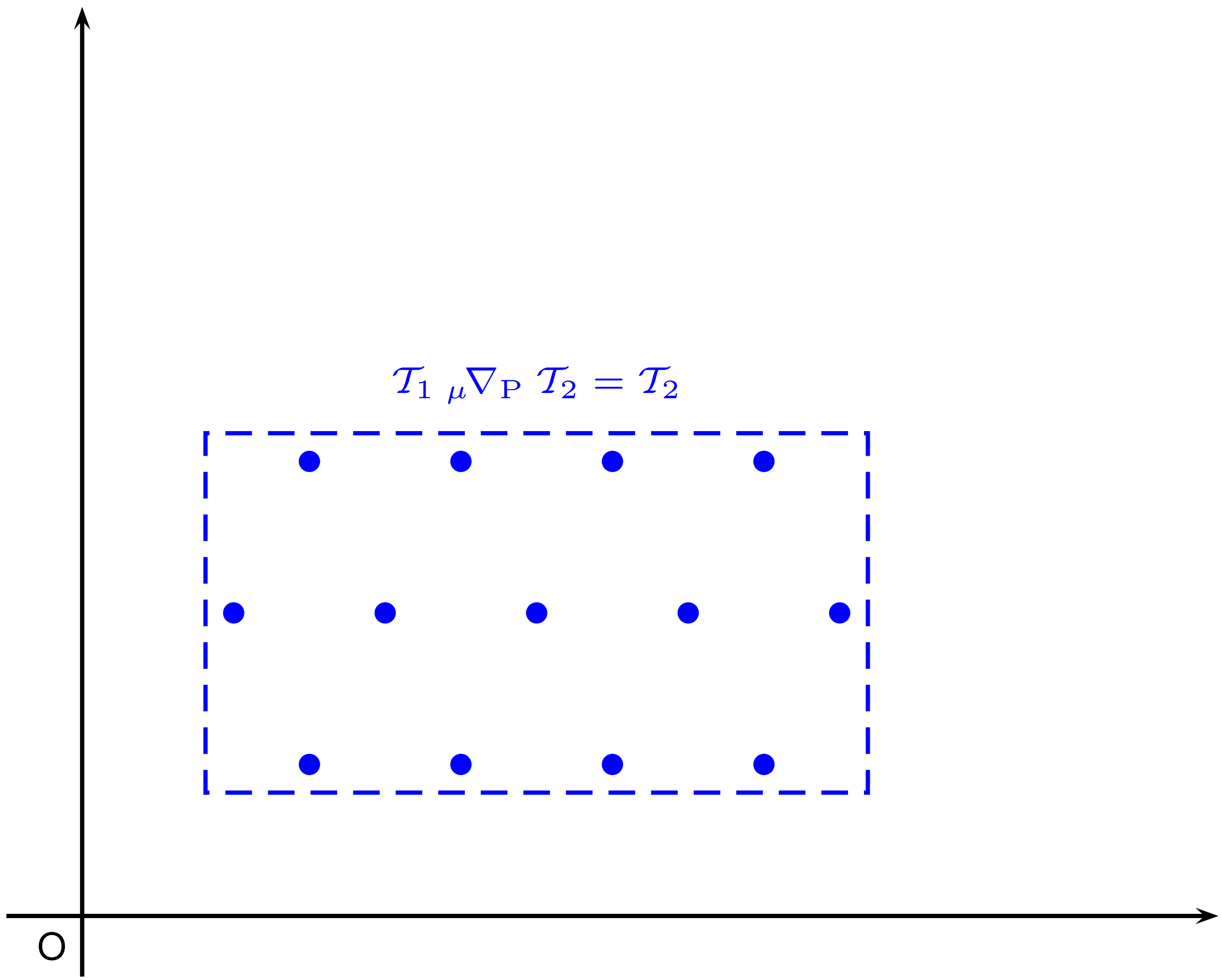
$$S_1 \ {}_{\mu}\nabla_{\mathrm{P}} \ S_2 := \begin{cases} S_1 \boxplus_{\mathrm{P}} S_2, & \text{if } S_1 \curvearrowright_{\mathrm{P}} S_1 \boxplus_{\mathrm{P}} S_2; \\ (S_1 \boxplus_{\mathrm{P}} S_2) \oplus_{\mathrm{P}} \{d\}, & \text{if } \bigoplus S_1 \Vdash \bigoplus (S_1 \boxplus_{\mathrm{P}} S_2); \\ \{\bigoplus S_2\}, & \text{otherwise.} \end{cases}$$

  where $\boxplus_{\mathrm{P}}$ is an arbitrary upper bound operator for $\hat{D}_{\mathrm{P}}$ and
  $d = \left(\bigoplus S_1 \nabla \bigoplus (S_1 \boxplus_{\mathrm{P}} S_2)\right) \ominus \left(\bigoplus (S_1 \boxplus_{\mathrm{P}} S_2)\right)$.
- In the next examples we consider $\boxplus_{\mathrm{P}} := \oplus_{\mathrm{P}}$, so that $S_1 \boxplus_{\mathrm{P}} S_2 = S_2$.

Certificate-Based Widening: 1st Case (i)



Certificate-Based Widening: 1st Case (ii)

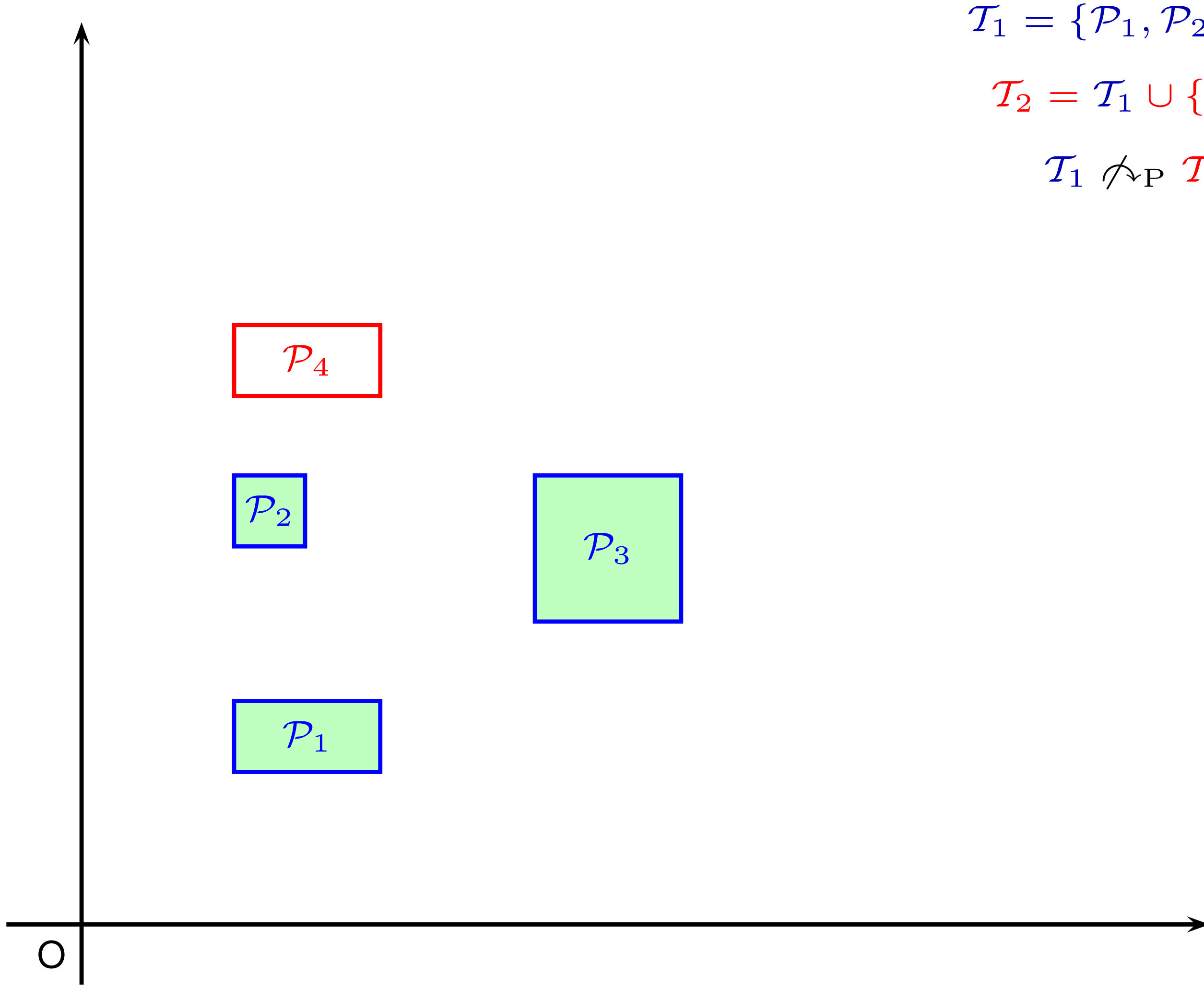


Certificate-Based Widening: 2nd Case (i)

$$\mathcal{T}_1 = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3\}$$

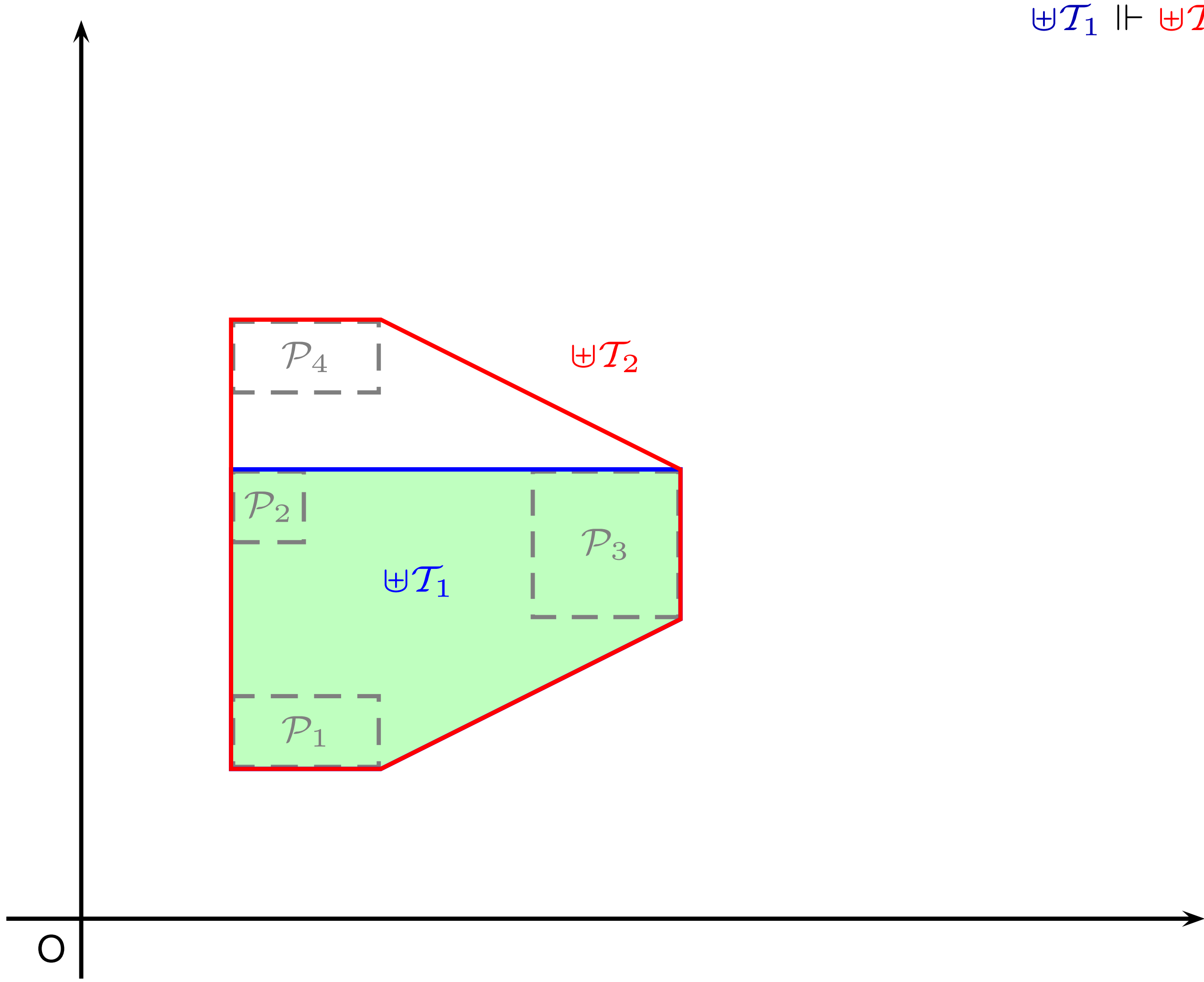
$$\mathcal{T}_2 = \mathcal{T}_1 \cup \{\mathcal{P}_4\}$$

$$\mathcal{T}_1 \not\curvearrowright_{\mathrm{P}} \mathcal{T}_2$$



Certificate-Based Widening: 2nd Case (ii)

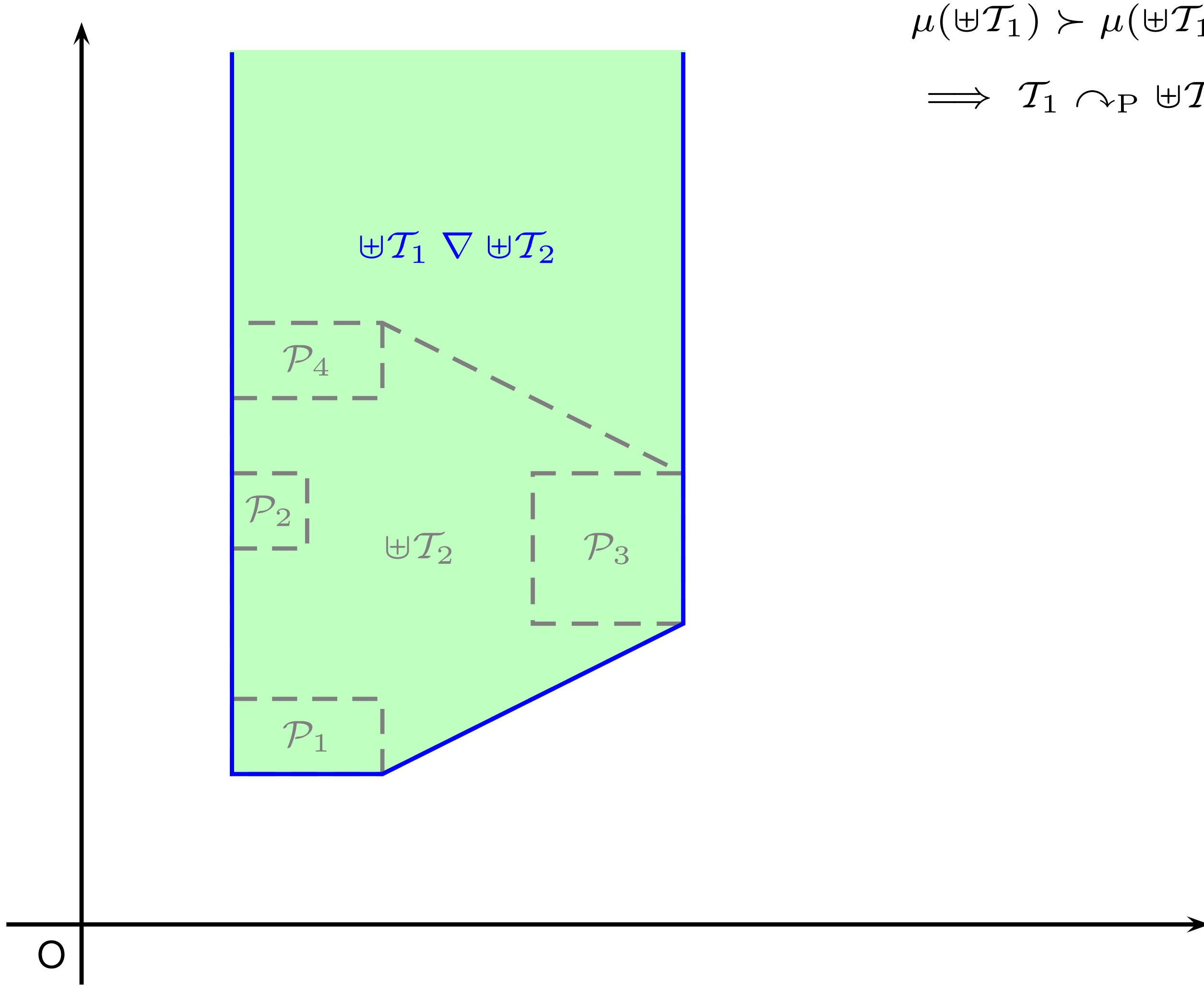
$\uplus \mathcal{T}_1 \Vdash \uplus \mathcal{T}_2$



Certificate-Based Widening: 2nd Case (iii)

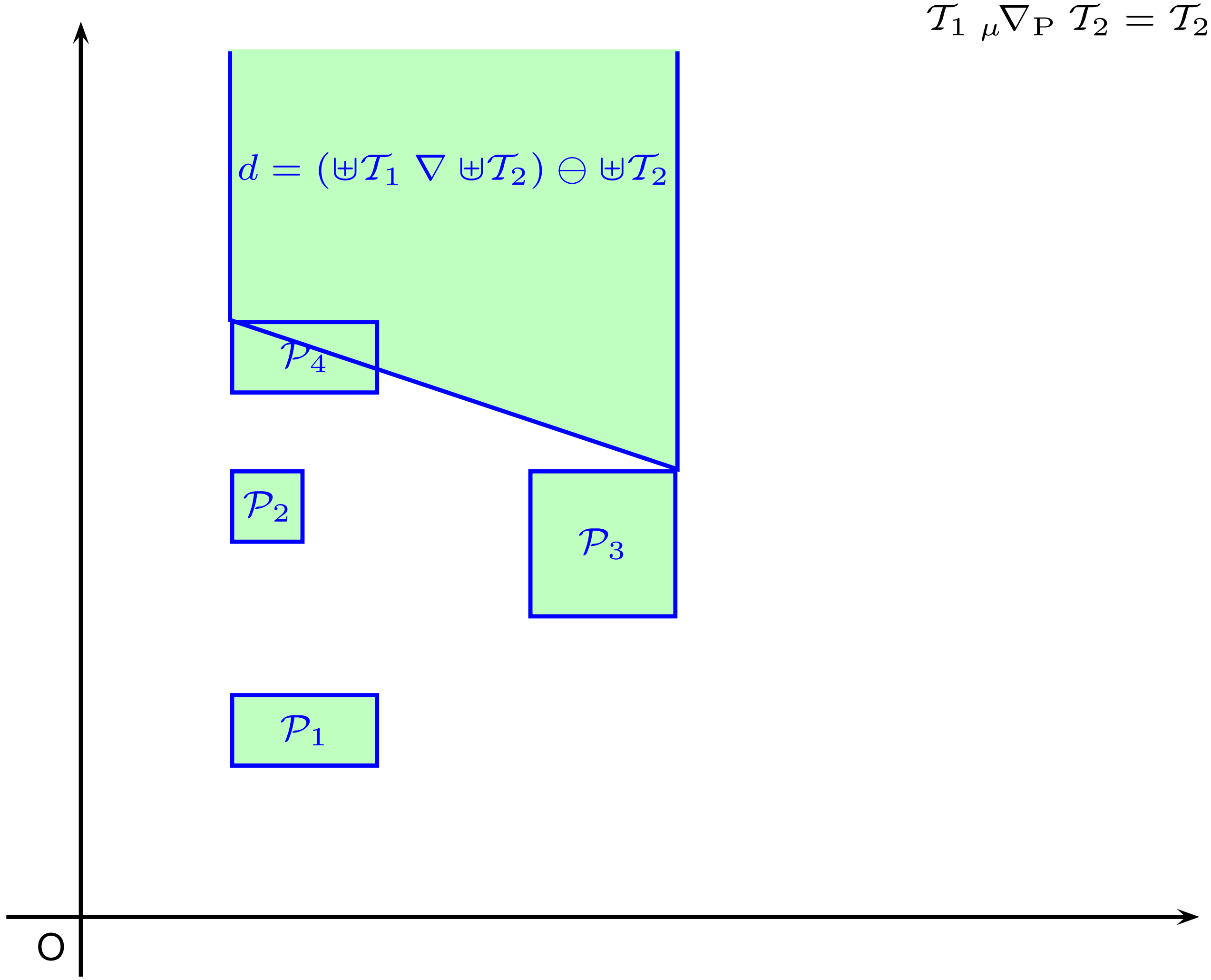
$$\mu(\uplus\mathcal{T}_1) \succ \mu(\uplus\mathcal{T}_1 \nabla \uplus\mathcal{T}_2)$$

$$\implies \mathcal{T}_1 \curvearrowright_{\mathrm{P}} \uplus\mathcal{T}_1 \nabla \uplus\mathcal{T}_2$$



Certificate-Based Widening: 2nd Case (iv)

$\mathcal{T}_1 \ {}_{\mu}\nabla_{\mathrm{P}} \ \mathcal{T}_2 = \mathcal{T}_2 \cup \{d\}$

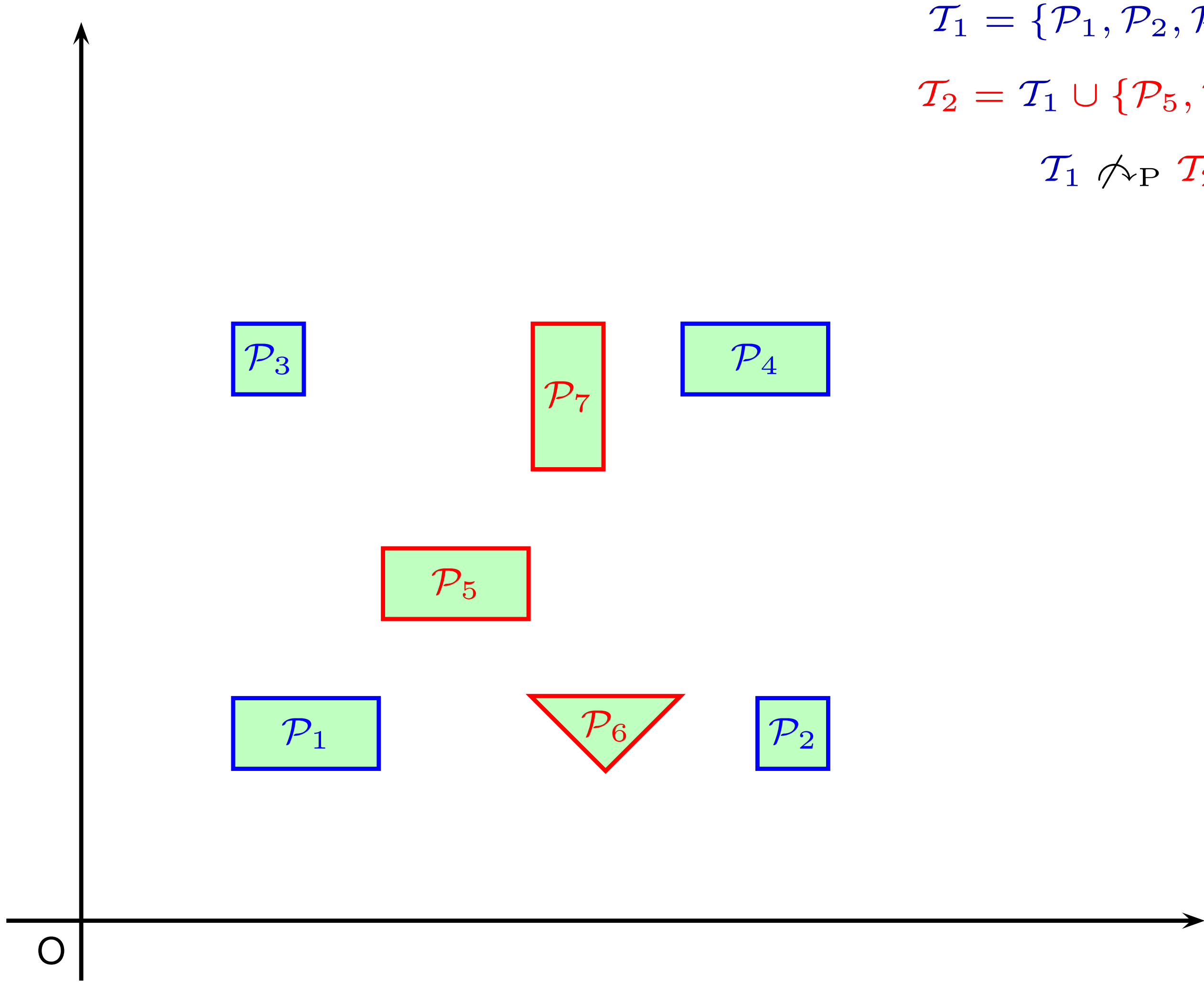


Certificate-Based Widening: Last Case (i)

$$\mathcal{T}_1 = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{P}_4\}$$

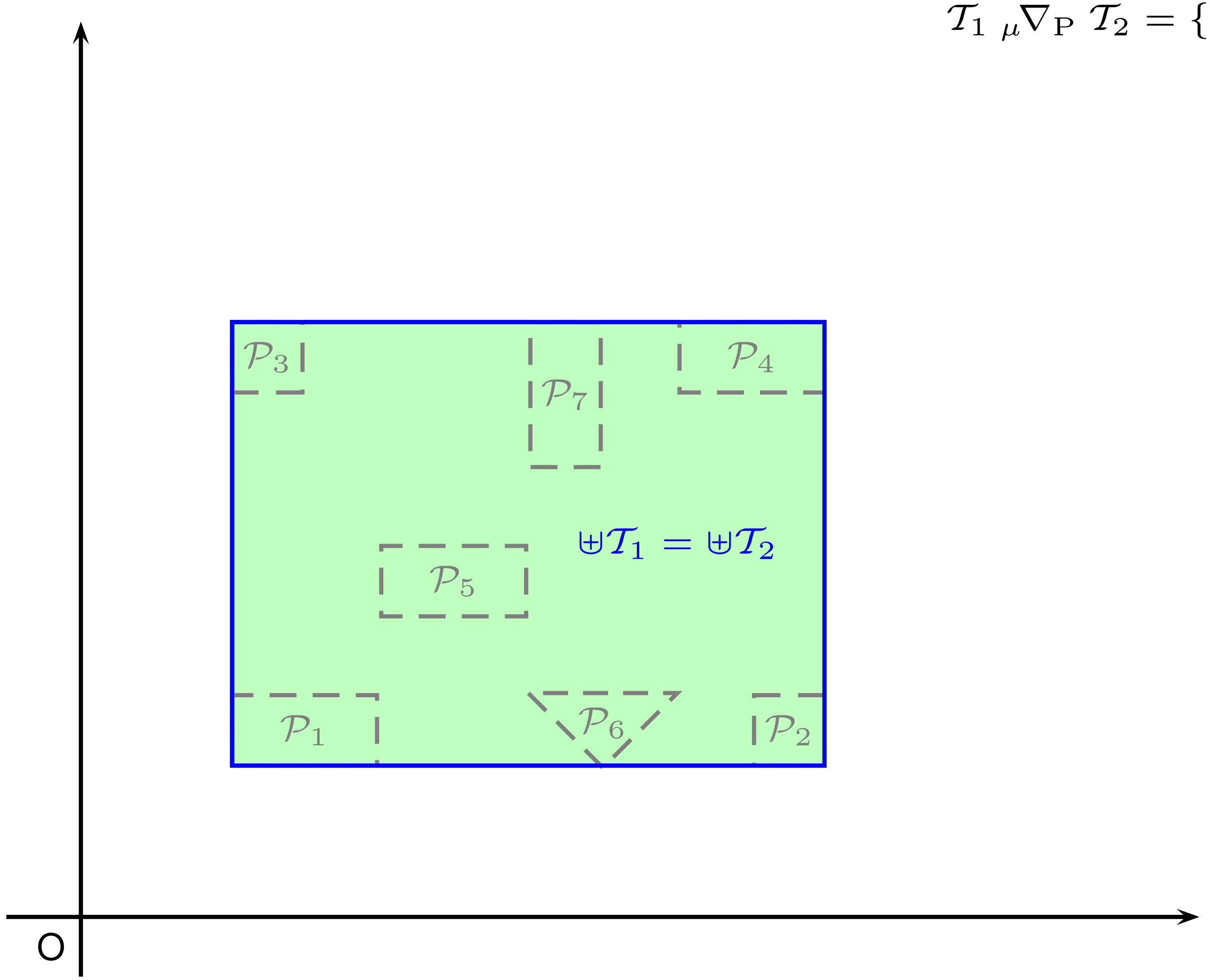
$$\mathcal{T}_2 = \mathcal{T}_1 \cup \{\mathcal{P}_5, \mathcal{P}_6, \mathcal{P}_7\}$$

$$\mathcal{T}_1 \not\curvearrowright_{\mathrm{P}} \mathcal{T}_2$$



Certificate-Based Widening: Last Case (ii)

$\mathcal{T}_1 \ {}_{\mu}\nabla_{\mathrm{P}} \ \mathcal{T}_2 = \{\uplus\mathcal{T}_2\}$



INSTANTIATING THE CERTIFICATE-BASED WIDENING

➜ We can consider any finite set of upper bound operators ${\boxplus_{\mathrm{P}}}^{1}, \ldots, {\boxplus_{\mathrm{P}}}^{m}$, therefore tuning the precision/complexity tradeoff of the widening.

Instantiating the Certificate-Based Widening

- ➜ We can consider any finite set of upper bound operators $\boxplus_{\mathrm{P}}{}^{1}, \ldots, \boxplus_{\mathrm{P}}{}^{m}$, therefore tuning the precision/complexity tradeoff of the widening.
- ➜ In particular, when computing $S_1 \nabla_{\mathrm{P}} S_2$, some of the elements occurring in the second argument S_2 may be merged (i.e., joined) together, without affecting the finite convergence guarantee.
- ➜ A specific merging heuristics was initially proposed in [Bultan et al., TOPLAS'99]; in the paper we discuss how the coarseness of the corresponding approximation can be controlled by a congruence relation on $\hat{D}_{\mathrm{P}}$.

Conclusion

➜ We have studied the the systematic lifting of widening operators for the finite powerset construction:

Conclusion

- We have studied the the systematic lifting of widening operators for the finite powerset construction:
  - we have proposed two widening strategies, either based on the use of a Egli-Milner connector or of a finite convergence certificate; a third strategy, based on a cardinality threshold, is proposed in the TR version of the paper;

CONCLUSION

- We have studied the the systematic lifting of widening operators for the finite powerset construction:
  - we have proposed two widening strategies, either based on the use of a Egli-Milner connector or of a finite convergence certificate; a third strategy, based on a cardinality threshold, is proposed in the TR version of the paper;
  - all construction are parametric in the specification of several auxiliary operators, allowing for a finer control on the efficiency/precision tradeoff.

Conclusion

- We have studied the the systematic lifting of widening operators for the finite powerset construction:
  - we have proposed two widening strategies, either based on the use of a Egli-Milner connector or of a finite convergence certificate; a third strategy, based on a cardinality threshold, is proposed in the TR version of the paper;
  - all construction are parametric in the specification of several auxiliary operators, allowing for a finer control on the efficiency/precision tradeoff.
- The framework has been instantiated on the finite powerset domain of convex polyhedra, providing examples for the choice of the parameters. A preliminary experimental evaluation is ongoing using the Parma Polyhedra Library.

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