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
The design of abstract domains is a difficult task...
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].
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 $\langle C, \sqsubseteq, \bot, T, \sqcup, \sqcap \rangle$ 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 $\mathcal{F}: C \to C$ is continuous.
The Abstract Interpretation Framework

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

→ The concrete domain $\langle C, \subseteq, \bot, \top, \sqcup, \sqcap \rangle$ 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 $\mathcal{F} : C \to C$ is continuous.
→ The abstract domain $\langle D, \vdash, 0, \oplus \rangle$ is a join-semilattice;
→ The two domains are related by a monotonic and injective concretization function $\gamma : D \to C$; thus, the abstract partial order $\vdash$ is indeed the approximation relation induced on $D$ by $\gamma$.
→ We assume the existence of a sound monotonic abstract semantic function $\mathcal{F}^\# : D \to D$, so that

$$\forall c \in C : \forall d \in D : c \sqsubseteq \gamma(d) \implies \mathcal{F}(c) \sqsubseteq \gamma(\mathcal{F}^\#(d)).$$
A Working Example (I)

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

\[ \langle \emptyset(\mathbb{R}^n), \subseteq, \emptyset, \mathbb{R}^n, \cup, \cap \rangle. \]

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

\[ \widehat{\mathbb{C}P}_n := \langle \mathbb{C}P_n, \subseteq, \emptyset, \mathbb{R}^n, \cup, \cap \rangle \]

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,

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

Widening operators try to solve all of these problems at once.
A minor variant of the classical one [Cousot and Cousot, PLILP’92]:

- The partial operator $\nabla : D \times D \rightarrow D$ 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 $\nabla$ induces on $D$ a partial order relation $\vdash\nabla$ satisfying the ACC; this is defined as the reflexive and transitive closure of $\{ (d_1, d) \in D \times D \mid \exists d_2 \in D . d_1 \vdash d_2 \land d = d_1 \nabla d_2 \}$. 
DEFINITION OF WIDENING OPERATOR

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

→ The partial operator $\nabla : D \times D \rightarrow D$ 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 $\nabla$ induces on $D$ a partial order relation $\vdash_{\nabla}$ satisfying the ACC; this is defined as the reflexive and transitive closure of \{ $(d_1, d) \in D \times D \mid \exists d_2 \in D . d_1 \vdash d_2 \land d = d_1 \nabla d_2$ \}.

→ The upward iteration sequence with widenings (starting from $0 \in D$)

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

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 $\widehat{CP}_n$ 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].
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 $\triangleright$. 

The Finite Powerset Construction (I)
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 $\triangleright$.

→ The finite powerset domain over $\hat{D}$ is the join-semilattice

$$\hat{D}_P := \langle \phi_{fn}(D, \triangleright), \triangleright_P, 0_P, \oplus_P \rangle,$$

where $0_P := \emptyset$ and $S_1 \oplus_P S_2 := \Omega_D^+(S_1 \cup S_2)$. 
The Finite Powerset Construction (II)

The partial order $\vdash_P$ corresponds to the Hoare’s powerdomain ordering:

\[ S_1 \vdash_P S_2 \iff \forall d_1 \in S_1 : \exists d_2 \in S_2 . d_1 \vdash d_2. \]

A kind of Egli-Milner partial order relation will be also used:

\[ S_1 \vdash_{EM} S_2 \iff S_1 = 0_P \lor (S_1 \vdash_P S_2 \land \forall d_2 \in S_2 : \exists d_1 \in S_1 . d_1 \vdash d_2). \]
THE FINITE POWERSET CONSTRUCTION (II)

- The partial order $\vdash_P$ corresponds to the Hoare’s powerdomain ordering:
  $$S_1 \vdash_P S_2 \iff \forall d_1 \in S_1 : \exists d_2 \in S_2 . d_1 \vdash d_2.$$  

- A kind of Egli-Milner partial order relation will be also used:
  $$S_1 \vdash_{EM} S_2 \iff S_1 = 0_P \lor (S_1 \vdash_P S_2 \land \forall d_2 \in S_2 : \exists d_1 \in S_1 . d_1 \vdash d_2).$$

- The concretization function is $\gamma_P : \wp_{fn}(D, \vdash) \rightarrow C$ defined by
  $$\gamma_P(S) := \bigsqcup \{ \gamma(d) \mid d \in S \}.$$  

  It is monotonic, but not necessarily injective.
The Finite Powerset Construction (II)

→ The partial order \( \vdash_P \) corresponds to the Hoare's powerdomain ordering:
\[
S_1 \vdash_P S_2 \iff \forall d_1 \in S_1 : \exists d_2 \in S_2 . \ d_1 \vdash d_2.
\]

→ A kind of Egli-Milner partial order relation will be also used:
\[
S_1 \vdash_{EM} S_2 \iff S_1 = \mathbf{0}_P \lor (S_1 \vdash_P S_2 \land \forall d_2 \in S_2 : \exists d_1 \in S_1 . \ d_1 \vdash d_2).
\]

→ The concretization function is \( \gamma_P : \wp_{fn}(D, \vdash) \to C \) defined by
\[
\gamma_P(S) := \bigsqcup \{ \gamma(d) \mid d \in S \}.
\]

It is monotonic, but not necessarily injective.

→ A correct abstract semantic function \( \mathcal{F}^\#_P : \wp_{fn}(D, \vdash) \to \wp_{fn}(D, \vdash) \) is assumed. This can be defined as the element-wise lifting
\[
\mathcal{F}^\#_P(S) := \Omega_D^\dagger \left( \{ \mathcal{F}^\#(d) \mid d \in S \} \right),
\]
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 $(\mathcal{CP}_n)_P := \langle \phi_{\text{fn}}(\mathcal{CP}_n, \subseteq), \subseteq_P, \emptyset, \emptyset_P \rangle$.

→ The induced concretization function is $\gamma_P(S) := \bigcup S$.

→ 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 $\widehat{\mathcal{CP}}_n$ to the powerset $(\mathcal{CP}_n)_P$. 
A Working Example (iv)

\[ T_1 = \{ P_1, P_2, P_3 \} \in \varphi_{fn}(\mathbb{CP}_2) \]
A WORKING EXAMPLE (V)

\[ T_2 = \{ Q_1, P_1, P_2, P_3 \} \notin \varnothing_{\text{fn}}(\mathbb{CP}^2) \]
A WORKING EXAMPLE (VI)

\[ T_1 = \{P_1, P_2, P_3\}, \quad T_2 = \{Q_1, Q_2, Q_3\} \]

\[ T_1 \vdash_P T_2, \quad \kappa_{EM} T_2 \]
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 $\nabla$ is not a widening on $\hat{D}_P$, since
  1. the lifting may not be an upper bound operator, because the base-level widening $\nabla$ may be undefined on some pairs;
  2. the finite convergence guarantee can be lost.
The correctness problem can be solved by defining a $\nabla$-connected extrapolation heuristics \( h_P : \varphi_{fn}(D, \vdash)^2 \rightarrow \varphi_{fn}(D, \vdash) \): for all \( S_1 \vdash_P S_2 \),

\[
S_2 \vdash_{EM} h_P^\nabla(S_1, S_2);
\]
\[
\forall d \in h_P^\nabla(S_1, S_2) \setminus S_2 : \exists d_1 \in S_1 . d_1 \vdash \nabla d;
\]
\[
\forall d \in h_P^\nabla(S_1, S_2) \cap S_2 : ((\exists d_1 \in S_1 . d_1 \vdash d) \rightarrow (\exists d'_1 \in S_1 . d'_1 \vdash \nabla d)).
\]
Defining Extrapolation Heuristics

→ The correctness problem can be solved by defining a $\nabla$-connected extrapolation heuristics $h_P^\nabla: \varphi_{fn}(D, \vdash)^2 \rightarrow \varphi_{fn}(D, \vdash)$: for all $S_1 \vdash_P S_2$,

$$S_2 \vdash_{EM} h_P^\nabla(S_1, S_2);$$

$$\forall d \in h_P^\nabla(S_1, S_2) \setminus S_2 : \exists d_1 \in S_1 . d_1 \vdash \nabla d;$$

$$\forall d \in h_P^\nabla(S_1, S_2) \cap S_2 : (\exists d_1 \in S_1 . d_1 \vdash d) \rightarrow (\exists d'_1 \in S_1 . d'_1 \vdash \nabla d).$$

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

$$h_P^\nabla(S_1, S_2) := S_2 \oplus_P \Omega_D^\nabla(\{ d_1 \nabla d_2 \in D | d_1 \in S_1, d_2 \in S_2, d_1 \vdash d_2 \}).$$
No Finite Convergence Guarantee (I)

$\mathcal{P}_1 \quad \mathcal{P}_2$

$\mathcal{T}_2$

O
NO FINITE CONVERGENCE GUARANTEE (II)

Note that $T_2 \kappa_{EM} T_3$
NO FINITE CONVERGENCE GUARANTEE (III)

\[ h_P^\nabla (T_3, T_4) = T_4 \]

\[ \mathcal{P}_1 \quad \mathcal{P}_2 \quad \mathcal{P}_3 \]
**No Finite Convergence Guarantee (iv)**

\[ T_j = \{ \mathcal{P}_i \mid 1 \leq i \leq j \} \]

\[ h_P^n(T_j, T_{j+1}) = T_{j+1} \]
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 $\Omega_D^+$ interferes with the extrapolation heuristics $h_P^\triangledown$, 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 $\Omega_D$ 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 $\square_{EM}$ is an upper bound for the relation $\vdash_{EM}$. 
Widenings Based on Egli-Milner Connectors (I)

- An Egli-Milner connector $\boxplus_{EM}$ is an upper bound for the relation $\vdash_{EM}$.
- For any EM-connector $\boxplus_{EM}$ and any $\triangledown$-connected extrapolation heuristics $h^\triangledown_P$, let $S_{1EM} \triangledown_P S_2 := h^\triangledown_P(S_1, S_1 \boxplus_{EM} S_2)$. 
Widenings Based on Egli-Milner Connectors (I)

- An Egli-Milner connector $\boxdot_{EM}$ is an upper bound for the relation $\models_{EM}$.
- For any EM-connector $\boxdot_{EM}$ and any $\nabla$-connected extrapolation heuristics $h_P^\nabla$, let $S_{1EM\nabla_P}S_2 := h_P^\nabla(S_1, S_1 \boxdot_{EM} S_2)$.
Widenings Based on Egli-Milner Connectors (II)

- An Egli-Milner connector $\Box_{EM}$ is an upper bound for the relation $\vdash_{EM}$;
- For any EM-connector $\Box_{EM}$ and any $\nabla$-connected extrapolation heuristics $h^\nabla_P$, let $S_{1\ EM}\nabla_P\ S_2 := h^\nabla_P(S_1, S_1 \Box_{EM} S_2)$.
Widenings Based on Egli-Milner Connectors (III)

- An Egli-Milner connector $\boxdot_{\text{EM}}$ is an upper bound for the relation $\vdash_{\text{EM}}$;
- For any EM-connector $\boxdot_{\text{EM}}$ and any $\nabla$-connected extrapolation heuristics $h_P$, let $S_{1 \boxdot_{\text{EM}} \nabla P} S_2 := h_P(S_1, S_1 \boxdot_{\text{EM}} S_2)$.
A possible tactic when proving that an upper bound operator $\langle \cdot \rangle : D \times D \to D$ is indeed a widening on $\hat{D}$ is to provide a sort of “convergence certificate.”
A possible tactic when proving that an upper bound operator $\square : D \times D \rightarrow D$ is indeed a widening on $\hat{D}$ is to provide a sort of “convergence certificate.”

A finite convergence certificate for $\square$ on $\hat{D}$ is a triple $(\mathcal{O}, \succ, \mu)$ where
1. $\mathcal{O}$ is a set with well-founded ordering $\succ$;
2. $\mu : D \rightarrow \mathcal{O}$, which is called level mapping, satisfies

$$\forall d_1, d_2 \in D : d_1 \sqsupset d_2 \implies \mu(d_1) \succ \mu(d_1 \square d_2).$$
Widenings Based on Certificates

→ A possible tactic when proving that an upper bound operator \( \boxplus: D \times D \to D \) 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. \( \mu: D \to \mathcal{O} \), which is called level mapping, satisfies
     \[
     \forall d_1, d_2 \in D : d_1 \models d_2 \implies \mu(d_1) \succ \mu(d_1 \boxplus d_2).
     \]

→ For instance, a certificate for the standard widening on \( \widehat{\mathcal{C}P_n} \) can be obtained by taking \((\mathcal{O}, \succ)\) be the lexicographic product of two copies of \((\mathbb{N}, >)\) and defining \( \mu(\mathcal{P}) = (n - \dim(\mathcal{P}), \# \mathcal{C}) \), 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 $\boxhat : D \times D \to D$ is indeed a widening on $\hat{D}$ is to provide a sort of “convergence certificate.”

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

1. $\mathcal{O}$ is a set with well-founded ordering $\succ$;
2. $\mu : D \to \mathcal{O}$, which is called level mapping, satisfies
   $$\forall d_1, d_2 \in D : d_1 \sqsupseteq d_2 \implies \mu(d_1) \succ \mu(d_1 \boxhat d_2).$$

→ For instance, a certificate for the standard widening on $\widehat{\mathbb{C}P_n}$ can be obtained by taking $(\mathcal{O}, \succ)$ be the lexicographic product of two copies of $(\mathbb{N}, \succ)$ and defining $\mu(\mathcal{P}) = (n - \dim(\mathcal{P}), \# \mathcal{C})$, 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 $\hat{D}_P$. 
LIFTING THE CERTIFICATE ON THE POWERSET DOMAIN

Let \((O, >, \mu)\) be a certificate for a widening \(\nabla\) on \(\hat{D}\).
LIFTING THE CERTIFICATE ON THE POWERSET DOMAIN

→ Let \((\mathcal{O}, \succ, \mu)\) be a certificate for a widening \(\triangledown\) on \(\mathcal{D}\).

→ The relation \(\bowtie_P \subseteq \wpfn(D, \triangleright) \times \wpfn(D, \triangleright)\) is such that \(S_1 \bowtie_P S_2\) iff one of the following holds:

\[
\begin{align*}
\mu(\oplus S_1) & > \mu(\oplus S_2); \\
\mu(\oplus S_1) &= \mu(\oplus S_2) \land \# S_1 > 1 \land \# S_2 = 1; \\
\mu(\oplus S_1) &= \mu(\oplus S_2) \land \# S_1 > 1 \land \# S_2 > 1 \land \tilde{\mu}(S_1) \gg \tilde{\mu}(S_2)
\end{align*}
\]

where \(\tilde{\mu}(S)\) denotes the multiset over \(\mathcal{O}\) obtained by applying \(\mu\) to each abstract element in \(S\).
Let $\langle \mathcal{O}, \succ, \mu \rangle$ be a certificate for a widening $\sqcup$ on $\hat{D}$.

The relation $\bowtie \subseteq \wp(D, \sqcup) \times \wp(D, \sqcup)$ is such that $S_1 \bowtie S_2$ iff one of the following holds:

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

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

$\bowtie$ satisfies the ACC.

Intuitively, a certificate $\langle \mathcal{O}_P, \succ, \mu_P \rangle$ for $\hat{D}_P$ will be defined as

- $\mu_P(S_1) \succ \mu_P(S_2) \iff S_1 \bowtie S_2$;
- $\mu_P(S_1) = \mu_P(S_2) \iff S_1 \not\bowtie S_2 \land S_2 \not\bowtie S_1$. 
LIFTING THE CERTIFICATE: 1ST CASE (I)
LIFTING THE CERTIFICATE: 1ST CASE (II)

\[ \dim(\mathcal{T}_1) = 1 < 2 = \dim(\mathcal{T}_2) \]

\[ \implies \mu(\mathcal{T}_1) > \mu(\mathcal{T}_2) \]

\[ \implies \mathcal{T}_1 \preceq \mathcal{T}_2 \]
LIFTING THE CERTIFICATE: 2ND CASE (I)

\[ T_1 = \{ P_1, P_2, P_3, P_4, P_5 \} \]

\[ T_2 = \{ P_6 \} \]
LIFTING THE CERTIFICATE: 2ND CASE (II)

\[ \mu(\bigcup T_1) = \mu(\bigcup T_2) \]

\[ \# T_1 = 5 > 1, \quad \# T_2 = 1 \]

\[ \implies T_1 \bowtie_T T_2 \]
LIFTING THE CERTIFICATE: 3RD CASE (I)

\[ T_1 = \{ P_1, P_2, P_3, P_4, P_5 \} \]
\[ T_2 = \{ P_1, P_2 \} \cup \{ P_6, P_7, P_8 \} \]
LIFTING THE CERTIFICATE: 3RD CASE (ii)

\[ \mu(\bigcup T_1) = \mu(\bigcup T_2) \]

\[ \tilde{\mu}(T_1) = \{(2, 4)^4, (2, 6)^1\} \gg \{(2, 4)^5\} = \tilde{\mu}(T_2) \]

\[ \implies T_1 \sim_F T_2 \]
A CERTIFICATE-BASED WIDENING

- A subtraction for $\hat{D}$ is a partial operator $\ominus: D \times D \rightarrow D$ 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 $\text{cP}_n$, the closed convex set-difference operator is a subtraction.
A Certificate-Based Widening

→ A subtraction for $\hat{D}$ is a partial operator $\ominus : D \times D \mapsto D$ 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 $\mathcal{CP}_n$, the closed convex set-difference operator is a subtraction.

→ A certificate-based widening $\mu \nabla_P$ is such that

$$S_1 \mu \nabla_P S_2 := \begin{cases} S_1 \boxplus_P S_2, & \text{if } S_1 \bowtie_P S_1 \boxplus_P S_2; \\ (S_1 \boxplus_P S_2) \ominus_P \{d\}, & \text{if } \ominus S_1 \vdash \ominus (S_1 \boxplus_P S_2); \\ \{\ominus S_2\}, & \text{otherwise}. \end{cases}$$

where $\boxplus_P$ is an arbitrary upper bound operator for $\hat{D}_P$ and $d = (\ominus S_1 \nabla \ominus (S_1 \boxplus_P S_2)) \ominus (\ominus (S_1 \boxplus_P S_2))$. 
A Certificate-Based Widening

→ A subtraction for $\hat{D}$ is a partial operator $\ominus: D \times D \mapsto D$ 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 $\mathcal{CP}_n$, the closed convex set-difference operator is a subtraction.

→ A certificate-based widening $\mu \nabla_P$ is such that

$$S_1 \mu \nabla_P S_2 := \begin{cases} S_1 \boxplus_P S_2, & \text{if } S_1 \curlyvee_P S_1 \boxplus_P S_2; \\ (S_1 \boxplus_P S_2) \oplus_P \{d\}, & \text{if } \bigoplus S_1 \vdash \bigoplus (S_1 \boxplus_P S_2); \\ \{\oplus S_2\}, & \text{otherwise}. \end{cases}$$

where $\boxplus_P$ is an arbitrary upper bound operator for $\hat{D}_P$ and $d = (\bigoplus S_1 \nabla \bigoplus (S_1 \boxplus_P S_2)) \ominus (\bigoplus (S_1 \boxplus_P S_2))$.

→ In the next examples we consider $\boxplus_P := \oplus_P$, so that $S_1 \boxplus_P S_2 = S_2$. 

A Certificate-Based Widening
CERTIFICATE-BASED WIDENING: 1ST CASE (I)
CERTIFICATE-BASED WIDENING: 1ST CASE (II)

\[ T_1 \mu \nabla_p T_2 = T_2 \]
CERTIFICATE-BASED WIDENING: 2ND CASE (I)

\[ T_1 = \{ \mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3 \} \]

\[ T_2 = T_1 \cup \{ \mathcal{P}_4 \} \]

\[ T_1 \not\prec P T_2 \]
CERTIFICATE-BASED WIDENING: 2ND CASE (II)

\[ \forall \mathcal{T}_1 \vdash \forall \mathcal{T}_2 \]

\[ \mathcal{P}_1 \quad \mathcal{P}_2 \quad \mathcal{P}_3 \quad \mathcal{P}_4 \]

\[ \mathcal{Q}_1 \quad \mathcal{Q}_2 \]
\textbf{Certificate-Based Widening: 2nd Case (iii)}

\[ \mu(\mathcal{T}_1) \not\succ \mu(\mathcal{T}_1 \lor \mathcal{T}_2) \]
\[ \implies T_1 \bowtie P \mathcal{T}_1 \lor \mathcal{T}_2 \]
CERTIFICATE-BASED WIDENING: 2ND CASE (iv)

\[ T_1 \mu \triangledown_P T_2 = T_2 \cup \{ d \} \]

\[ d = (\mathcal{P}_1 \triangledown \mathcal{P}_2) \ominus \mathcal{P}_2 \]

\[ \mathcal{P}_1 \]

\[ \mathcal{P}_2 \]

\[ \mathcal{P}_3 \]

\[ \mathcal{P}_4 \]
CERTIFICATE-BASED WIDENING: LAST CASE (I)

\[ T_1 = \{ \mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{P}_4 \} \]
\[ T_2 = T_1 \cup \{ \mathcal{P}_5, \mathcal{P}_6, \mathcal{P}_7 \} \]
\[ T_1 \not\preceq_{P} T_2 \]
CERTIFICATE-BASED WIDENING: LAST CASE (II)

\[ T_1 \mu \triangledown_P T_2 = \{ \cup T_2 \} \]

\[ \text{Diagram with sets } P_1, P_2, P_3, P_4, P_5, P_6, P_7 \]

\[ \cup T_1 = \cup T_2 \]
INSTANTIATING THE CERTIFICATE-BASED WIDENING

We can consider any finite set of upper bound operators $\oplus_P^1, \ldots, \oplus_P^m$, therefore tuning the precision/complexity tradeoff of the widening.
We can consider any finite set of upper bound operators $\bigoplus^1 P, \ldots, \bigoplus^m P$, therefore tuning the precision/complexity tradeoff of the widening.

In particular, when computing $S_1 \bigtriangleup_P S_2$, 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 $\hat{D}_P$. 

**Instantiating the Certificate-Based Widening**
CONCLUSION

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

→ We have studied 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;
We have studied 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 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/