# Widening Operators for Powerset Domains*

Roberto Bagnara[1], Patricia M. Hill[2], and Enea Zaffanella[1]

[1] Department of Mathematics, University of Parma, Italy
{bagnara,zaffanella}@cs.unipr.it
[2] School of Computing, University of Leeds, UK
hill@comp.leeds.ac.uk

**Abstract.** The *finite powerset construction* upgrades an abstract domain by allowing for the representation of finite disjunctions of its elements. In this paper we define three generic widening operators for the finite powerset abstract domain. The widenings are obtained by lifting any widening operator defined on the base-level abstract domain and are parametric with respect to the specification of a few additional operators. We illustrate the proposed techniques by instantiating our widenings on powersets of convex polyhedra, a domain for which no non-trivial widening operator was previously known.

## 1 Introduction

The design and implementation of effective, expressive and efficient abstract domains for data-flow analysis and model-checking is a very difficult task. For this reason, starting with [12], there continues to be strong interest in techniques that derive enhanced abstract domains by applying systematic constructions on simpler, existing domains. Disjunctive completion, direct product, reduced product and reduced power are the first and most famous constructions of this kind [12]; several variations of them as well as others constructions have been proposed in the literature.

Once the carrier of the enhanced abstract domain has been obtained by one of these systematic constructions, the abstract operations can be defined, as usual, as the optimal approximations of the concrete ones. While this completely solves the specification problem, it usually leaves the implementation problem with the designer and gives no guarantees about the efficiency (or even the computability) of the resulting operations. This motivates the importance of generic techniques whereby correct, even though not necessarily optimal, domain operations are derived automatically or semi-automatically from those of the domains the construction operates upon [9, 12, 19].

This paper focuses on the derivation of widening operators for a kind of disjunctive refinement we call *finite powerset construction*. As far as we know, this

* This work has been partly supported by MURST projects "Aggregate- and Number-Reasoning for Computing: from Decision Algorithms to Constraint Programming with Multisets, Sets, and Maps" and "Constraint Based Verification of Reactive Systems."

is the first time that the problem of deriving non-trivial, provably correct widening operators in a domain refinement is tackled successfully. We also present its specialization to finite powersets of convex polyhedra. Not only is this included to help the reader gain a better intuition regarding the underlying approach but also to provide a definitely non-toy instance that is practically useful for applications such as data-flow analysis and model checking. Sets of polyhedra are implemented in Polylib [25, 29] and its successor *PolyLib* [26], even though no widenings are provided. Sets of polyhedra, represented with Presburger formulas made available by the Omega library [24, 27], are used in the verifier described in [8]; there, an extrapolation operator (i.e., a widening without convergence guarantee) on sets of polyhedra is described. Another extrapolation operator is implemented in the automated verification tool described in [17], where sets of polyhedra are represented using the clp(q, r) constraint library [23].

The rest of the paper is structured as follows: Section 2 recalls the basic concepts and notations needed in this paper; Section 3 defines the finite powerset construction as a disjunctive refinement for any abstract domain that is a join-semilattice; Section 4 gives three alternative strategies for upgrading any widening for the base-level domain into a proper widening for the finite powerset domain; Section 5 shows a possible way to control the precision/efficiency trade-off of these widenings. Section 6 concludes. Appendix A contains the proofs of all the stated results.

## 2 Preliminaries

For a set $S$, $\wp(S)$ is the powerset of $S$, whereas $\wp_{\mathrm{f}}(S)$ is the set of all the *finite* subsets of $S$; the cardinality of $S$ is denoted by $\#\,S$. The first limit ordinal is denoted by $\omega$. Let $\mathcal{O}$ be a set equipped with a well-founded ordering '$\succ$'. If $M$ and $N$ are finite multisets over $\mathcal{O}$, $\#(n, M)$ denotes the number of occurrences of $n \in \mathcal{O}$ in $M$ and $M \gg N$ means that there exists $j \in \mathcal{O}$ such that $\#(j, M) > \#(j, N)$ and, for each $k \in \mathcal{O}$ with $k \succ j$, we have $\#(k, M) = \#(k, N)$. The relation '$\gg$' is well-founded [18].

### 2.1 Abstract Interpretation

In the literature, several abstract interpretation frameworks have been proposed that are able to establish a formal relationship between the behaviors of programs when observed at different levels of abstraction. The main difference between these frameworks usually concerns the trade-off between their general applicability and the strength of the formal results that can be established. In this paper we will adopt the framework proposed in [14, Section 7], where the correspondence between the concrete and the abstract domains is induced from a concrete approximation relation and a concretization function. Since we are not aiming at maximum generality, for the sole purpose of simplifying the presentation, we will consider a particular instance of the framework by assuming a few additional but non-essential domain properties. The resulting construction will

be adequate for our purposes, since it still allows for algebraically weak abstract domains.

The concrete domain is modeled as a complete lattice of semantic properties $\langle C, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$; as usual, the concrete approximation relation $c_1 \sqsubseteq c_2$ holds if $c_1$ is a stronger property than $c_2$ (i.e., $c_2$ approximates $c_1$). The concrete semantics $c \in C$ of a program is formalized as the least fixpoint of a continuous (concrete) semantic function $\mathcal{F}\colon C \to C$, which is iteratively computed starting from the bottom element, so that

$$c = \mathcal{F}^{\omega}(\bot) := \bigsqcup_{\delta < \omega} \big(\mathcal{F}^{\delta}(\bot)\big).$$

The abstract domain $\hat{D} = \langle D, \vdash, \mathbf{0}, \oplus \rangle$ is modeled as a join-semilattice (i.e., the least upper bound $d_1 \oplus d_2$ exists for all $d_1, d_2 \in D$). We will overload '$\oplus$' so that, for each $S \in \wp_{\mathrm{f}}(D)$, $\bigoplus S$ denotes the least upper bound of $S$. The abstract domain $\hat{D}$ is related to the concrete domain by a monotonic and injective concretization function $\gamma\colon D \to C$. Monotonicity and injectivity mean that the abstract partial order '$\vdash$' is indeed the approximation relation induced on $D$ by the concretization function $\gamma$. For all $d_1, d_2 \in D$, we will use the notation $d_1 \Vdash d_2$ to mean that $d_1 \vdash d_2$ and $d_1 \neq d_2$. We assume the existence of a monotonic abstract semantic function $\mathcal{F}^{\sharp}\colon D \to D$ that is sound with respect to $\mathcal{F}\colon C \to C$:

$$\forall c \in C : \forall d \in D : c \sqsubseteq \gamma(d) \implies \mathcal{F}(c) \sqsubseteq \gamma\big(\mathcal{F}^{\sharp}(d)\big). \tag{1}$$

This local correctness condition ensures that each concrete iterate can be safely approximated by computing the corresponding abstract iterate (starting from the bottom element $\mathbf{0} \in D$). However, due to the weaker algebraic properties satisfied by the abstract domain, the abstract upward iteration sequence may not converge. Even when it converges, it may fail to do so in a finite number of steps, therefore being useless for the purposes of static analysis.

*Widening operators* [10, 11, 14, 15] provide a simple and general characterization for enforcing and accelerating convergence. We will adopt a minor variation of the classical definition of widening operator (see footnote 6 in [15, p. 275]).

**Definition 1. (Widening.)** *Let $\langle D, \vdash, \mathbf{0}, \oplus \rangle$ be a join-semilattice. The partial operator $\nabla\colon D \times D \rightarrowtail D$ is a* widening *if*

1. *$d_1 \vdash d_2$ implies that $d_1 \nabla d_2$ is defined and $d_2 \vdash d_1 \nabla d_2$, for each $d_1, d_2 \in D$;*
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.*

Any widening operator '$\nabla$' induces a corresponding partial ordering '$\vdash_{\nabla}$' on the domain $D$; this is defined as the reflexive and transitive closure of the relation $\big\{ (d_1, d) \in D \times D \;\big|\; \exists d_2 \in D \,.\, d_1 \Vdash d_2 \wedge d = d_1 \nabla d_2 \big\}$. The relation '$\vdash_{\nabla}$' satisfies the ascending chain condition. We write $d_1 \Vdash_{\nabla} d_2$ to denote $d_1 \vdash_{\nabla} d_2$ and $d_1 \neq d_2$.

It can be proved that the *upward iteration sequence with widenings* starting at the bottom element $d_0 := \mathbf{0}$ and defined by

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

converges after a finite number $j \in \mathbb{N}$ of iterations [15]. Note that the widening is always applied to arguments $d = d_i$ and $d' = d_i \oplus \mathcal{F}^\sharp(d_i)$ satisfying $d \Vdash d'$. Also, when condition (1) holds, the post-fixpoint $d_j \in D$ of $\mathcal{F}^\sharp$ is a correct approximation of the concrete semantics, i.e., $\mathcal{F}^\omega(\bot) \sqsubseteq \gamma(d_j)$.

### 2.2 The Abstract Domain of Polyhedra

In this section, we instantiate the abstract interpretation framework sketched above by presenting the well-known abstract domain of closed convex polyhedra. This domain will be used throughout the paper to illustrate the generic widening techniques that will be defined.

Let $\mathbb{R}^n$, where $n > 0$, be the $n$-dimensional real vector space. The set $\mathcal{P} \subseteq \mathbb{R}^n$ is a *closed and convex polyhedron* (*polyhedron*, for short) if and only if $\mathcal{P}$ can be expressed as the intersection of a finite number of closed affine half-spaces of $\mathbb{R}^n$. The set $\mathbb{CP}_n$ of closed convex polyhedra on $\mathbb{R}^n$, when partially ordered by subset inclusion, is a lattice having the empty set and $\mathbb{R}^n$ as the bottom and top elements, respectively; the binary meet operation is set-intersection, whereas the binary join operation, denoted by '$\uplus$', is called *convex polyhedral hull* (*poly-hull*, for short). Therefore, we have the abstract domain

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

This domain can be related to several concrete domains, depending on the intended application. One example of a concrete domain is the complete lattice

$$\hat{\mathsf{A}}_n := \big\langle \wp(\mathbb{R}^n), \subseteq, \varnothing, \mathbb{R}^n, \cup, \cap \big\rangle.$$

Note that $\widehat{\mathbb{CP}}_n$ is a meet-sublattice of $\hat{\mathsf{A}}_n$, sharing the same bottom and top elements. Another example is the complete lattice

$$\hat{\mathsf{B}}_n := \big\langle \wp_c(\mathbb{R}^n), \subseteq, \varnothing, \mathbb{R}^n, \cup_c, \cap \big\rangle,$$

where $\wp_c(\mathbb{R}^n)$ is the set of all topologically closed and convex subsets of $\mathbb{R}^n$ and the join operation '$\cup_c$' returns the smallest topologically closed and convex set containing its arguments. Note that $\widehat{\mathbb{CP}}_n$ is a sublattice of $\hat{\mathsf{B}}_n$. As a final example of concrete domain for some analysis, consider the complete lattice

$$\hat{\mathsf{C}}_n := \big\langle \wp(\mathbb{CP}_n), \subseteq, \varnothing, \mathbb{CP}_n, \cup, \cap \big\rangle.$$

The abstract domain $\widehat{\mathbb{CP}}_n$, which is a join-semilattice, is related to the concrete domains shown above by the concretization functions $\gamma^{\mathsf{A}} \colon \mathbb{CP}_n \to \wp(\mathbb{R}^n)$,

$\gamma^{\mathsf{B}}\colon \mathbb{CP}_n \to \wp_c(\mathbb{R}^n)$ and $\gamma^{\mathsf{C}}\colon \mathbb{CP}_n \to \wp(\mathbb{CP}_n)$: for each $\mathcal{P} \in \mathbb{CP}_n$, we have both $\gamma^{\mathsf{A}}(\mathcal{P}) := \mathcal{P}$ and $\gamma^{\mathsf{B}}(\mathcal{P}) := \mathcal{P}$, and $\gamma^{\mathsf{C}}(\mathcal{P}) := \downarrow\mathcal{P} := \{\, \mathcal{Q} \in \mathbb{CP}_n \mid \mathcal{Q} \subseteq \mathcal{P} \,\}$. All these concretization functions are trivially monotonic and injective.

For each choice of the concrete domain $C \in \big\{\wp(\mathbb{R}^n), \wp_c(\mathbb{R}^n), \wp(\mathbb{CP}_n)\big\}$, the continuous semantic function $\mathcal{F}\colon C \to C$ and the corresponding monotonic abstract semantic function $\mathcal{F}^\sharp\colon \mathbb{CP}_n \to \mathbb{CP}_n$, which is assumed to be correct, are deliberately left unspecified. The domain $\widetilde{\mathbb{CP}}_n$ contains infinite ascending chains having no least upper bound in $\mathbb{CP}_n$. Thus, the convergence of the abstract iteration sequence has to be guaranteed by the adoption of widening operators.

### 2.3 Widening the Polyhedral Domain

The first widening on polyhedra was introduced in [16] and refined in [20]. This operator, denoted by '$\nabla_s$', has been termed *standard widening* and used almost universally. Its formal specification requires some further notation and concepts related to the domain of polyhedra.

Any vector $\boldsymbol{v} \in \mathbb{R}^n$ is regarded as a matrix in $\mathbb{R}^{n\times 1}$ so that it can be manipulated with the usual matrix operations of addition, multiplication (both by a scalar and by another matrix), and transposition, which is denoted by $\boldsymbol{v}^{\mathrm{T}}$. For each $i = 1, \ldots\ n$, the $i$-th component of the vector $\boldsymbol{v} \in \mathbb{R}^n$ is denoted by $v_i$. The *scalar product* of $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^n$, denoted $\langle \boldsymbol{v}, \boldsymbol{w} \rangle$, is $\boldsymbol{v}^{\mathrm{T}}\boldsymbol{w} = \sum_{i=1}^{n} v_i w_i$. The vector of $\mathbb{R}^n$ having all components equal to zero is denoted by $\mathbf{0}$.

Let $V = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\} \subseteq \mathbb{R}^n$ be a finite set of vectors. The *orthogonal* of $V$ is

$$V^{\perp} := \big\{\, \boldsymbol{w} \in \mathbb{R}^n \;\big|\; \forall \boldsymbol{v} \in V : \langle \boldsymbol{v}, \boldsymbol{w} \rangle = 0 \,\big\}.$$

The vectors in $V$ are said *affinely independent* if the only solution of the system of equations $\big\{\sum_{i=1}^{m} \lambda_i \boldsymbol{v}_i = \mathbf{0},\ \sum_{i=1}^{m} \lambda_i = 0\big\}$ is $\lambda_i = 0$, for each $i = 1, \ldots, m$. If $k \leq n+1$ is the maximum number of affinely independent points of a polyhedron $\mathcal{P} \in \mathbb{CP}_n$, then the *dimension of* $\mathcal{P}$, denoted as $\dim(\mathcal{P})$, is $k - 1$.

For each vector $\boldsymbol{a} \in \mathbb{R}^n$ and scalar $b \in \mathbb{R}$, where $\boldsymbol{a} \neq \mathbf{0}$, the linear non-strict inequality constraint $\langle \boldsymbol{a}, \boldsymbol{x} \rangle \geq b$ defines a topologically closed affine half-space of $\mathbb{R}^n$. The linear equality constraint $\langle \boldsymbol{a}, \boldsymbol{x} \rangle = b$ defines an affine hyperplane of $\mathbb{R}^n$ (i.e., the intersection of the affine half-spaces $\langle \boldsymbol{a}, \boldsymbol{x} \rangle \geq b$ and $\langle -\boldsymbol{a}, \boldsymbol{x} \rangle \geq -b$). We do not distinguish between syntactically different constraints defining the same affine half-space so that, for example, $x \geq 2$ and $2x \geq 4$ are the same constraint. Thus, each polyhedron $\mathcal{P}$ can be represented by a finite system of linear equality and non-strict inequality constraints $\mathcal{C}$ and we write $\mathcal{P} = \mathrm{con}(\mathcal{C})$.

The subsets of equality and inequality constraints in $\mathcal{C}$ are denoted by $\mathrm{eq}(\mathcal{C})$ and $\mathrm{ineq}(\mathcal{C})$, respectively. When $\mathcal{P} = \mathrm{con}(\mathcal{C}) \neq \varnothing$, we say that $\mathcal{C}$ is in *minimal form* if and only if $\#\,\mathrm{eq}(\mathcal{C}) = n - \dim(\mathcal{P})$ and there does not exist $\mathcal{C}' \subset \mathcal{C}$ such that $\mathrm{con}(\mathcal{C}') = \mathcal{P}$. All constraint systems in minimal form describing a given polyhedron have the same cardinality. For each linear constraint $\beta$ of the form $\big(\langle \boldsymbol{a}, \boldsymbol{x} \rangle \geq b\big)$ or $\big(\langle \boldsymbol{a}, \boldsymbol{x} \rangle = b\big)$, let $\mathrm{slope}(\beta) := \boldsymbol{a}$; for each constraint system $\mathcal{C}'$, let $\mathrm{slope}(\mathcal{C}') := \big\{\, \mathrm{slope}(\beta) \;\big|\; \beta \in \mathcal{C}' \,\big\}$. A constraint system $\mathcal{C}$ is in *orthogonal form* if it is in minimal form and $\mathrm{slope}(\mathrm{ineq}(\mathcal{C})) \subseteq \mathrm{slope}(\mathrm{eq}(\mathcal{C}))^{\perp}$. All constraint

systems in orthogonal form describing a given polyhedron have identical sets of inequality constraints.

The following definition of standard widening requires that each equality constraint is split into the two corresponding linear inequalities; thus, for each constraint system $\mathcal{C}$, we define

$$\mathrm{repr}_{\geq}(\mathcal{C}) := \Big\{ \langle -\boldsymbol{a}, \boldsymbol{x} \rangle \geq -b \;\Big|\; \big(\langle \boldsymbol{a}, \boldsymbol{x} \rangle = b\big) \in \mathcal{C} \Big\} \cup \Big\{ \langle \boldsymbol{a}, \boldsymbol{x} \rangle \geq b \;\Big|\; \big(\langle \boldsymbol{a}, \boldsymbol{x} \rangle \geq b\big) \in \mathcal{C} \vee \big(\langle \boldsymbol{a}, \boldsymbol{x} \rangle = b\big) \in \mathcal{C} \Big\}.$$

**Definition 2. (Standard widening.)** *For $i = 1, 2$, let $\mathcal{P}_i = \mathrm{con}(\mathcal{C}_i) \in \mathbb{CP}_n$, where the constraint system $\mathcal{C}_1$ is either inconsistent or in minimal form. Then, the polyhedron $\mathcal{P}_1 \nabla_s \mathcal{P}_2 \in \mathbb{CP}_n$ is defined as*

$$\mathcal{P}_1 \nabla_s \mathcal{P}_2 = \begin{cases} \mathcal{P}_2, & \text{if } \mathcal{P}_1 = \varnothing; \\ \mathrm{con}(\mathcal{C}'_1 \cup \mathcal{C}'_2), & \text{otherwise;} \end{cases}$$

*where*

$$\mathcal{C}'_1 := \Big\{ \beta_1 \in \mathrm{repr}_{\geq}(\mathcal{C}_1) \;\Big|\; \mathcal{P}_2 \subseteq \mathrm{con}\big(\{\beta_1\}\big) \Big\},$$

$$\mathcal{C}'_2 := \left\{ \beta_2 \in \mathrm{repr}_{\geq}(\mathcal{C}_2) \;\middle|\; \begin{array}{l} \exists \beta_1 \in \mathrm{repr}_{\geq}(\mathcal{C}_1) \,. \\ \quad \mathcal{P}_1 = \mathrm{con}\Big(\big(\mathrm{repr}_{\geq}(\mathcal{C}_1) \setminus \{\beta_1\}\big) \cup \{\beta_2\}\Big) \end{array} \right\}.$$

The constraints in $\mathcal{C}'_1$ are those that would have been selected when using the original proposal of [16], whereas the constraints in $\mathcal{C}'_2$ are added to ensure that this widening is a well defined operator on the domain of polyhedra (i.e., it does not depend on the particular constraint representations).

The second widening we summarize here is in fact a generalization of the framework presented in [4], which was based on an idea proposed in [7]. The framework is designed so that all its instances are indeed widening operators and it relies on a strict partial ordering relation on $\mathbb{CP}_n$ incorporating a notion of, so to speak, "limited growth" or "growth that cannot be indefinite" (graphically, a descending parabola).

**Definition 3. ('$\curvearrowright$'.)** *For $i = 1, 2$, let $\mathcal{P}_i = \mathrm{con}(\mathcal{C}_i) \in \mathbb{CP}_n$ where, if $\mathcal{P}_i \neq \varnothing$, $\mathcal{C}_i$ is in orthogonal form. The relation $\curvearrowright_s \subseteq \mathbb{CP}_n \times \mathbb{CP}_n$ is such that $\mathcal{P}_1 \curvearrowright_s \mathcal{P}_2$ if and only if $\mathcal{P}_1 \subset \mathcal{P}_2$ and either $\mathcal{P}_1 = \varnothing$ or at least one of the following holds:*

$$\dim(\mathcal{P}_1) < \dim(\mathcal{P}_2); \tag{2}$$

$$\mathrm{ineq}(\mathcal{C}_1) \supset \mathrm{ineq}(\mathcal{C}_2). \tag{3}$$

*We denote by '$\curvearrowright$' any ordering on $\mathbb{CP}_n$ that is a refinement of '$\curvearrowright_s$' and satisfies the ascending chain condition.*

Note that the orthogonality condition for the constraint systems of the polyhedra ensures that the relation '$\curvearrowright_s$' is well defined. Because of conditions (2) and (3)

it can be shown that the application of '$\nabla_s$' will always yield a polyhedron that is related to the previous iterate by any '$\frown$' ordering. That is, $\mathcal{P}_1 \frown \mathcal{P}_1 \nabla_s \mathcal{P}_2$ for any $\mathcal{P}_1 \subset \mathcal{P}_2 \in \mathbb{CP}_n$.

Let $h\colon \mathbb{CP}_n^2 \to \mathbb{CP}_n$ be an upper bound operator on $\mathbb{CP}_n$ and

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

By construction, '$\tilde{\nabla}$' is an upper bound operator at least as precise as '$\nabla_s$' and it still satisfies $\mathcal{P}_1 \frown \mathcal{P}_1 \tilde{\nabla} \mathcal{P}_2$.

In [4, 5], after defining a suitable refinement of the '$\frown_s$' ordering relation, an instance of the '$\tilde{\nabla}$' widening schema is proposed that uses several extrapolation heuristics. For a formal definition of this improved widening operator, we refer the reader to [4].

## 3 A Disjunctive Refinement

Traditionally, semantic domains have been designed incrementally by applying suitable domain constructors to basic components. In this respect, the theory of abstract interpretation makes no exception and systematic ways of composing or enhancing abstract domains have been proposed since [12]. In this section, we present the *finite powerset* operator, which is a domain refinement similar to disjunctive completion [12] and is obtained by a variant of the *down-set completion* construction presented in [13]. The following notation and definitions are mainly borrowed from [2, Section 6].

**Definition 4. (Non-redundancy.)** *Let $\hat{D} = \langle D, \vdash, \mathbf{0}, \oplus \rangle$ be a join-semilattice. The set $S \in \wp(D)$ is called* non-redundant *with respect to '$\vdash$' if and only if $\mathbf{0} \notin S$ and $\forall d_1, d_2 \in S : d_1 \vdash d_2 \implies d_1 = d_2$. The set of finite non-redundant subsets of $D$ (with respect to '$\vdash$') is denoted by $\wp_{\mathrm{fn}}(D, \vdash)$. The reduction function $\Omega^{\vdash}_D\colon \wp_{\mathrm{f}}(D) \to \wp_{\mathrm{fn}}(D, \vdash)$ mapping each finite set into its non-redundant counterpart is defined, for each $S \in \wp_{\mathrm{f}}(D)$, by*

$$\Omega^{\vdash}_D(S) := S \setminus \{\, d \in S \mid d = \mathbf{0} \vee \exists d' \in S \,.\, d \Vdash d' \,\}.$$

The restriction to the finite subsets reflects the fact that here we are mainly interested in an abstract domain where disjunctions are implemented by explicit collections of elements of the base-level abstract domain. As a consequence of this restriction, for any $S \in \wp_{\mathrm{f}}(D)$ such that $S \neq \{\mathbf{0}\}$, $\Omega^{\vdash}_D(S)$ is the (finite) set of the maximal elements of $S$.

**Definition 5. (Finite powerset domain.)** *Let $\hat{D} := \langle D, \vdash, \mathbf{0}, \oplus \rangle$ be a join-semilattice. The* finite powerset domain *over $\hat{D}$ is the join-semilattice*

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

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

The approximation ordering '$\vdash_{\text{P}}$' induced by '$\oplus_{\text{P}}$' is the Hoare powerdomain partial order [1], so that $S_1 \vdash_{\text{P}} S_2$ if and only if

$$\forall d_1 \in S_1 : \exists d_2 \in S_2 \,.\, d_1 \vdash d_2.$$

A sort of Egli-Milner partial order relation [1] will also be useful: $S_1 \vdash_{\text{EM}} S_2$ holds if and only if either $S_1 = \mathbf{0}_{\text{P}}$ or $S_1 \vdash_{\text{P}} S_2$ and

$$\forall d_2 \in S_2 : \exists d_1 \in S_1 \,.\, d_1 \vdash d_2.$$

An *(Egli-Milner) connector* for $\hat{D}_{\text{P}}$, denoted by '$\boxplus_{\text{EM}}$' is any upper bound operator for the Egli-Milner ordering on $\wp_{\text{fn}}(D, \vdash)$. Note that although a *least* upper bound for '$\vdash_{\text{EM}}$' may not exist, a connector can always be defined; for instance, we can let $S_1 \boxplus_{\text{EM}} S_2 := \{\bigoplus(S_1 \cup S_2)\}$.

Besides the requirement on finiteness, another difference with respect to the down-set completion of [13] is that we are dropping the assumption about the complete distributivity of the concrete domain. This is possible because our semantic domains are not necessarily related by Galois connections, so that this property does not have to be preserved.

The finite powerset domain is related to the concrete domain by means of the concretization function $\gamma_{\text{P}} \colon \wp_{\text{fn}}(D, \vdash) \to C$ defined by

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

Note that $\gamma_{\text{P}}$ is monotonic but not necessarily injective. For $S_1, S_2 \in \wp_{\text{fn}}(D, \vdash)$, we write $S_1 \equiv_{\gamma_{\text{P}}} S_2$ to denote that the two abstract elements actually denote the same concrete element, i.e., when $\gamma_{\text{P}}(S_1) = \gamma_{\text{P}}(S_2)$. It is easy to see that '$\equiv_{\gamma_{\text{P}}}$' is a congruence relation on $\hat{D}_{\text{P}}$. As noted in [13], non-redundancy only provides a partial, syntactic form of reduction. On the other hand, requiring the full, semantic form of reduction for a finite powerset domain can be computationally very expensive.

A correct abstract semantic function $\mathcal{F}^\sharp_{\text{P}} \colon \wp_{\text{fn}}(D, \vdash) \to \wp_{\text{fn}}(D, \vdash)$ on the finite powerset domain may be provided by an ad-hoc definition. More often, if the concrete semantic function $\mathcal{F} \colon C \to C$ satisfies suitable hypotheses, $\mathcal{F}^\sharp_{\text{P}}$ can be safely induced from the abstract semantic function $\mathcal{F}^\sharp \colon D \to D$. For instance, if $\mathcal{F}$ is additive, we can define $\mathcal{F}^\sharp_{\text{P}}$ as follows [12, 19]:

$$\mathcal{F}^\sharp_{\text{P}}(S) := \Omega^{\vdash}_{D}\Big(\{\, \mathcal{F}^\sharp(d) \mid d \in S \,\}\Big).$$

### 3.1 The Finite Powerset Domain of Polyhedra

The polyhedral domain $(\widehat{\mathbb{CP}}_n)_{\text{P}}$, having carrier $\wp_{\text{fn}}(\mathbb{CP}_n, \subseteq)$, is the finite powerset domain over $\widehat{\mathbb{CP}}_n$. The approximation ordering is '$\subseteq_{\text{P}}$' where, for each $\mathcal{S}_1, \mathcal{S}_2 \in \wp_{\text{fn}}(\mathbb{CP}_n, \subseteq)$,

$$\mathcal{S}_1 \subseteq_{\text{P}} \mathcal{S}_2 \iff \forall \mathcal{P}_1 \in \mathcal{S}_1 : \exists \mathcal{P}_2 \in \mathcal{S}_2 \,.\, \mathcal{P}_1 \subseteq \mathcal{P}_2.$$

Let $\gamma_{\mathrm{P}}^{\mathsf{A}}$, $\gamma_{\mathrm{P}}^{\mathsf{B}}$ and $\gamma_{\mathrm{P}}^{\mathsf{C}}$ denote the (powerset) concretization functions induced by $\gamma^{\mathsf{A}}$, $\gamma^{\mathsf{B}}$ and $\gamma^{\mathsf{C}}$, respectively. Then, the relation '$\equiv_{\gamma_{\mathrm{P}}^{\mathsf{A}}}$' makes two finite sets of polyhedra equivalent if and only if they have the same set-union. The general problem of deciding the semantic equivalence with respect to $\gamma_{\mathrm{P}}^{\mathsf{A}}$ of two finite (non-redundant) collections of polyhedra is known to be computationally hard [28]. For $\gamma_{\mathrm{P}}^{\mathsf{B}}$, the relation '$\equiv_{\gamma_{\mathrm{P}}^{\mathsf{B}}}$' makes two finite sets of polyhedra equivalent if and only if they have the same poly-hull, so that the powerset construction provides no benefit at all. Finally, $\gamma_{\mathrm{P}}^{\mathsf{C}}$ is injective so that '$\equiv_{\gamma_{\mathrm{P}}^{\mathsf{C}}}$' coincides with the identity congruence relation.

*Example 1.* For the polyhedral domain $(\widehat{\mathbb{CP}}_1)_{\mathrm{P}}$, let[3]

$$\mathcal{T}_0 := \big\{\{0 \le x \le 2\}, \{1 \le x \le 2\}, \{3 \le x \le 4\}, \{4 \le x \le 5\}\big\},$$
$$\mathcal{T}_1 := \big\{\{0 \le x \le 2\}, \{3 \le x \le 4\}, \{4 \le x \le 5\}\big\},$$
$$\mathcal{T}_2 := \big\{\{0 \le x \le 1\}, \{1 \le x \le 2\}, \{3 \le x \le 5\}\big\}.$$

Then $\mathcal{T}_0 \notin \wp_{\mathrm{fn}}(\mathbb{CP}_1, \subseteq)$, but $\mathcal{T}_1 = \Omega^{\subseteq}_{\mathbb{CP}_1}(\mathcal{T}_0) \in \wp_{\mathrm{fn}}(\mathbb{CP}_1, \subseteq)$. Also, $\mathcal{T}_1 \equiv_{\gamma_{\mathrm{P}}^{\mathsf{A}}} \mathcal{T}_2$.

## 4 Widening the Finite Powerset Domain

If the domain refinement of the previous section is meant to be used for static analysis, then a key ingredient that is still missing is a systematic way of ensuring the termination of the analysis. In this section, we describe three widening strategies that rely on the existence of a widening $\nabla\colon D \times D \rightarrowtail D$ on the base-level abstract domain. Note that this assumption is satisfied by most abstract domains used in the context of static analysis.[4] We start by proposing a very general specification of an extrapolation operator that lifts this '$\nabla$' operator to the powerset domain.

**Definition 6. ($h_{\mathrm{P}}^{\nabla}$.)** *A partial operator $h_{\mathrm{P}}^{\nabla}\colon \wp_{\mathrm{fn}}(D, \vdash)^2 \rightarrowtail \wp_{\mathrm{fn}}(D, \vdash)$ is an* extrapolation heuristics for $\hat{D}_{\mathrm{P}}$ *if, for all $S_1, S_2 \in \wp_{\mathrm{fn}}(D, \vdash)$ such that $S_1 \Vdash_{\mathrm{P}} S_2$, $h_{\mathrm{P}}^{\nabla}(S_1, S_2)$ is defined and satisfies the following conditions:*

$$S_2 \vdash_{\mathrm{EM}} h_{\mathrm{P}}^{\nabla}(S_1, S_2); \tag{4}$$
$$\forall d \in h_{\mathrm{P}}^{\nabla}(S_1, S_2) \setminus S_2 : \exists d_1 \in S_1 \,.\, d_1 \Vdash_{\nabla} d. \tag{5}$$

Informally, condition (4) ensures that the result is an upper approximation of $S_2$ in which every element covers at least one element of $S_2$ (i.e., the heuristics cannot add elements that are unrelated to $S_2$); condition (5) ensures that in the resulting set, each element that was not already in $S_2$ originates from an application of '$\nabla$' to an element of $S_1$.

[3] In this and the following examples, we will abuse notation by writing a constraint system $\mathcal{C}$ to denote the polyhedron $\mathcal{P} = \mathrm{con}(\mathcal{C})$.

[4] If the base-level abstract domain $\hat{D}$ is finite or Noetherian, so that it is not necessarily endowed with an explicit widening operator, then a dummy widening can be obtained by considering the least upper bound operator '$\oplus$'.

### 4.1 Powerset Widenings Using Egli-Milner Connectors

For the first widening, we require an additional property for the extrapolation heuristics; together with the previous conditions, this will ensure that *each* element of the resulting set that cover an element of the first argument $S_1$ originates from an application of '$\nabla$' to a (possibly different) element of $S_1$.

**Definition 7. ($\nabla$-connected heuristics.)** *The extrapolation heuristics '$h_{\mathrm{P}}^{\nabla}$' is said to be* $\nabla$-connected *if, for all $S_1, S_2 \in \wp_{\mathrm{fn}}(D, \vdash)$ where $S_1 \Vdash_{\mathrm{P}} S_2$, we have*

$$\forall d \in h_{\mathrm{P}}^{\nabla}(S_1, S_2) \cap S_2 : \big((\exists d_1 \in S_1 \,.\, d_1 \Vdash d) \to (\exists d_1' \in S_1 \,.\, d_1' \Vdash_{\nabla} d)\big). \tag{6}$$

It is straightforward to construct an algorithm for computing a $\nabla$-connected extrapolation heuristics for any given base-level widening '$\nabla$'. The basic idea was proposed in [8] for an abstract domain encoding a set of integer vectors by means of a Presburger formula. Intuitively, for all pairs $(d_1, d_2) \in S_1 \times S_2$ that can be built using the two arguments $S_1$ and $S_2$, we compute $d_1 \nabla d_2$, provided this operation happens to be defined; otherwise, we simply take $d_2$.

**Proposition 1.** *For all $S_1, S_2 \in \wp_{\mathrm{fn}}(D, \vdash)$ such that $S_1 \vdash_{\mathrm{P}} S_2$, let*

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

*Then '$h_{\mathrm{P}}^{\nabla}$' is a $\nabla$-connected extrapolation heuristics for $\hat{D}_{\mathrm{P}}$.*

For the finite powerset domain over $\widehat{\mathbb{CP}}_n$, lines 10–15 of the algorithm specified in [8, Figure 8, page 773] provide an implementation of the heuristics '$h_{\mathrm{P}}^{\nabla}$' defined in Proposition 1, instantiated with the standard widening, '$\nabla_s$', on $\widehat{\mathbb{CP}}_n$.

*Example 2.* To see that the '$h_{\mathrm{P}}^{\nabla}$' defined in Proposition 1 is not a widening for $(\widehat{\mathbb{CP}}_n)_{\mathrm{P}}$, consider the strictly increasing sequence $\mathcal{T}_0 \subseteq_{\mathrm{P}} \mathcal{T}_1 \subseteq_{\mathrm{P}} \cdots$ in $\mathbb{CP}_1$ defined by $\mathcal{T}_j := \{\, \mathcal{P}_i \mid 0 \leq i \leq j \,\}$, where $\mathcal{P}_i := \{x = i\}$, for $i \in \mathbb{N}$. Then, no matter what the specification for '$\nabla$' is, we obtain $h_{\mathrm{P}}^{\nabla}(\mathcal{T}_j, \mathcal{T}_{j+1}) = \mathcal{T}_{j+1}$, for all $j \in \mathbb{N}$. Thus, the "widened" sequence is diverging.

Example 2 shows that, when computing $h_{\mathrm{P}}^{\nabla}(S_1, S_2)$, divergence is caused by those elements of $S_2$ that cover none of the elements occurring in $S_1$, i.e., when $S_1 \not\vdash_{\mathrm{EM}} S_2$. Thus, stabilization can be obtained by replacing $S_2$ with $S_1 \boxplus_{\mathrm{EM}} S_2$, where '$\boxplus_{\mathrm{EM}}$' is a connector for $\hat{D}_{\mathrm{P}}$. We therefore define a simple widening operator on the finite powerset domain that uses a connector to ensure termination.

**Definition 8. (The '$_{\mathrm{EM}}\nabla_{\mathrm{P}}$' widening.)** *Let '$h_{\mathrm{P}}^{\nabla}$' be a $\nabla$-connected extrapolation heuristics and '$\boxplus_{\mathrm{EM}}$' be a connector for $\hat{D}_{\mathrm{P}}$. Let also $S_1, S_2 \in \wp_{\mathrm{fn}}(D, \vdash)$, where $S_1 \Vdash_{\mathrm{P}} S_2$. Then $S_1 \,{}_{\mathrm{EM}}\nabla_{\mathrm{P}}\, S_2 := h_{\mathrm{P}}^{\nabla}(S_1, S_2')$, where*

$$S_2' := \begin{cases} S_2, & \text{if } S_1 \vdash_{\mathrm{EM}} S_2; \\ S_1 \boxplus_{\mathrm{EM}} S_2, & \text{otherwise.} \end{cases}$$

**Theorem 1.** *The '$_{\text{EM}}\nabla_{\text{P}}$' operator is a widening on $\hat{D}_{\text{P}}$.*

*Example 3.* To illustrate the widening operator '$_{\text{EM}}\nabla_{\text{P}}$' we consider the powerset domain $(\widehat{\mathbb{CP}}_1)_{\text{P}}$, with the standard widening '$\nabla_s$' on $\widehat{\mathbb{CP}}_1$ and the trivial connector '$\uplus_{\text{EM}}$' returning the singleton poly-hull of its arguments. Consider the sequence $\mathcal{T}_0 \subseteq_{\text{P}} \mathcal{T}_1 \subseteq_{\text{P}} \cdots$ of Example 2 and the widened sequence $\mathcal{U}_0 \subseteq_{\text{P}} \mathcal{U}_1 \subseteq_{\text{P}} \cdots$ where $\mathcal{U}_0 = \mathcal{T}_0$ and $\mathcal{U}_i = \mathcal{U}_{i-1}\ {}_{\text{EM}}\nabla_{\text{P}}\ (\mathcal{U}_{i-1} \uplus_{\text{P}} \mathcal{T}_i)$, for each $i > 0$. When computing $\mathcal{U}_1$, the second argument of the widening is $\mathcal{U}_0 \uplus_{\text{P}} \mathcal{T}_1 = \mathcal{T}_1$. Note that $\mathcal{U}_0 \vdash_{\text{EM}} \mathcal{T}_1$ does not hold so that the connector is needed. Thus, we obtain

$$\mathcal{U}_1 = h^{\nabla}_{\text{P}}(\mathcal{U}_0, \mathcal{U}_0 \uplus_{\text{EM}} \mathcal{T}_1) = h^{\nabla}_{\text{P}}\Big(\mathcal{U}_0, \big\{\{0 \le x \le 1\}\big\}\Big) = \big\{\{0 \le x\}\big\}.$$

In the next iteration we obtain stabilization. Clearly, in general the precision of this widening will depend on the chosen connector operator.

### 4.2 Powerset Widenings using Set Cardinality

In the iteration sequence in Example 2, there is no finite upper bound on the cardinality of the set being widened. So in the second *cardinality-based* widening specified here, if the cardinality of the given set $S_2$ exceeds a fixed bound $k$ by some $\ell > 0$, we first collapse $S_2$ to a smaller set $S_2'$ by replacing a subset of cardinality $\ell + 1$ by its join (so that $\#\, S_2' \le k$ and $S_2 \vdash_{\text{EM}} S_2'$).

**Definition 9. (Collapsor.)** *The relation* $\text{collapse}_k \subseteq \wp_{\text{fn}}(D, \vdash) \times \wp_{\text{fn}}(D, \vdash)$ *is defined, for each $k \ge 1$, so that* $\text{collapse}_k(S, S')$ *holds if and only if*

$$S' := \begin{cases} S, & \text{if } \#\, S \le k; \\ (S \setminus S'') \oplus_{\text{P}} \{\oplus S''\}, & \text{otherwise, where } S'' \subseteq S \text{ and } \#\, S'' > \#\, S - k. \end{cases}$$

*A unary operator $\Uparrow_k \colon \wp_{\text{fn}}(D, \vdash) \to \wp_{\text{fn}}(D, \vdash)$ is called a* $k$-collapsor *for $\hat{D}_{\text{P}}$ if* $\text{collapse}_k\big(S, \Uparrow_k(S)\big)$ *holds.*

The operator sketched in [8], which uses the '$h^{\nabla}_{\text{P}}$' heuristics defined in Proposition 1, is similar to the widening '$_{\text{EM}}\nabla_{\text{P}}$' for the polyhedral domain $\widehat{\mathbb{CP}}_n$ but, instead of using a connector in the *otherwise* case in Definition 8, it assumes the use of an operator like the collapsor to limit the cardinality of the sets. However, such an approach is not enough to obtain a widening and, even when the cardinality of the set to be widened is fixed so that the collapsor is not required, termination cannot be guaranteed (see Example 11 in Appendix A). We therefore define a particular subclass of extrapolation heuristics for the cardinality-based widening that avoids the problem.

**Definition 10. ($\nabla$-covered heuristics.)** *The extrapolation heuristics '$h^{\nabla}_{\text{P}}$' is said to be* $\nabla$-covered *if, for all $S_1, S_2 \in \wp_{\text{fn}}(D, \vdash)$ such that $S_1 \Vdash_{\text{P}} S_2$, we have*

$$\forall d_1 \in S_1 : \exists d \in h^{\nabla}_{\text{P}}(S_1, S_2)\ .\ d_1 \vdash_{\nabla} d. \tag{7}$$

A $\nabla$-covered extrapolation heuristics can be obtained for any widening '$\nabla$' on the base-level domain $\hat{D}$. One possibility is to selectively replace the standard reduction map '$\Omega_D^{\vdash}$' by a non-standard, widening-based reduction map '$\Omega_D^{\nabla}$'. The idea being that if, in a set in $\wp_{\mathrm{f}}(D)$, one element $d$ entails another $d'$, then instead of just removing the redundant element $d$, '$\Omega_D^{\nabla}$' replaces both $d$ and $d'$ by their widening $d \nabla d'$.

**Definition 11. ($\nabla$-reduction map.)** *An operator $\Omega_D^{\nabla}\colon \wp_{\mathrm{f}}(D) \to \wp_{\mathrm{fn}}(D, \vdash)$ is a $\nabla$-reduction map if, for all $S \in \wp_{\mathrm{f}}(D)$, there exists a sequence $S_0, \ldots, S_m$ of elements of $\wp_{\mathrm{f}}(D)$ such that $S_0 = S$, $S_m = \Omega_D^{\nabla}(S) \in \wp_{\mathrm{fn}}(D, \vdash)$ and, for each $0 < i \leq m$, $S_i = \big(S_{i-1} \setminus \{d, d'\}\big) \cup \{d \nabla d'\}$, where $d, d' \in S_{i-1}$ and $d \Vdash d'$.*

**Proposition 2.** *For all $S_1, S_2 \in \wp_{\mathrm{fn}}(D, \vdash)$ such that $S_1 \vdash_{\mathrm{P}} S_2$, let $h_{\mathrm{P}}^{\nabla}(S_1, S_2) := \Omega_D^{\nabla}(S_1 \cup S_2)$. Then '$h_{\mathrm{P}}^{\nabla}$' is a $\nabla$-covered extrapolation heuristics for $\hat{D}_{\mathrm{P}}$.*

We can now define the *cardinality-based widening* '${}_k\nabla_{\mathrm{P}}$'.

**Definition 12. (The '${}_k\nabla_{\mathrm{P}}$' widening.)** *Let '$h_{\mathrm{P}}^{\nabla}$' be a $\nabla$-covered extrapolation heuristics and '$\Uparrow_k$' be a $k$-collapsor for $\hat{D}_{\mathrm{P}}$, for some $k \geq 1$. Let also $S_1, S_2 \in \wp_{\mathrm{fn}}(D, \vdash)$, where $S_1 \Vdash_{\mathrm{P}} S_2$. Then $S_1 \, {}_k\nabla_{\mathrm{P}} \, S_2 := h_{\mathrm{P}}^{\nabla}(S_1, S_2')$, where*

$$S_2' := \begin{cases} S_2, & \text{if } \# S_2 \leq k; \\ \Uparrow_k(S_2), & \text{otherwise.} \end{cases}$$

**Theorem 2.** *The '${}_k\nabla_{\mathrm{P}}$' operator is a widening on $\hat{D}_{\mathrm{P}}$.*

*Example 4.* To illustrate the widening operator '${}_k\nabla_{\mathrm{P}}$' for $k = 2$, we consider the powerset domain $(\widehat{\mathbb{CP}}_1)_{\mathrm{P}}$ with the standard widening '$\nabla_s$' on $\widehat{\mathbb{CP}}_1$ and a 2-collapsor that, given a non-redundant and finite set of intervals on the $x$-axis, reduces its cardinality to 2 by taking the poly-hull of all the intervals but the one having the smallest lower bound. Consider again the sequence $\mathcal{T}_0 \subseteq_{\mathrm{P}} \mathcal{T}_1 \subseteq_{\mathrm{P}} \cdots$ of Example 2 and the widened sequence $\mathcal{U}_0 \subseteq_{\mathrm{P}} \mathcal{U}_1 \subseteq_{\mathrm{P}} \cdots$ where $\mathcal{U}_0 = \mathcal{T}_0$ and $\mathcal{U}_i = \mathcal{U}_{i-1} \, {}_2\nabla_{\mathrm{P}} \, (\mathcal{U}_{i-1} \uplus_{\mathrm{P}} \mathcal{T}_i)$, for each $i > 0$. As $\mathcal{U}_0 \subset \mathcal{T}_1$, and $\# \mathcal{T}_1 = 2$, we obtain $\mathcal{U}_1 = \mathcal{T}_1$. Again $\mathcal{U}_1 \subset \mathcal{T}_2$. As $\# \mathcal{T}_2 = 3$, we compute $\Uparrow_2(\mathcal{T}_2)$ before applying an '$h_{\mathrm{P}}^{\nabla}$' operator. Thus, we obtain

$$\mathcal{U}_1 = h_{\mathrm{P}}^{\nabla}\big(\mathcal{U}_1, \Uparrow_2(\mathcal{T}_2)\big) = h_{\mathrm{P}}^{\nabla}\Big(\mathcal{U}_1, \big\{\{x = 0\}, \{1 \leq x \leq 2\}\big\}\Big) = \big\{\{x = 0\}, \{1 \leq x\}\big\}.$$

In the next iteration we obtain stabilization. Clearly, the precision of this widening will depend on the value of $k$.

### 4.3 Powerset Widenings Using Finite Convergence Certificates

When trying to prove that an upper bound operator $\boxplus\colon D \times D \to D$ is indeed a widening on the abstract domain $\hat{D}$, a possible tactic is to provide a "convergence certificate." Formally, a *finite convergence certificate* for '$\boxplus$' (on $\hat{D}$) is a triple

$(\mathcal{O}, \succ, \mu)$ where $(\mathcal{O}, \succ)$ is a well-founded ordered set and $\mu\colon D \to \mathcal{O}$, which is called *level mapping*, is such that

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

We will abuse notation by writing $\mu$ to denote the certificate $(\mathcal{O}, \succ, \mu)$.

We now present another widening operator (denoted here by '$_{\mu}\nabla_{\text{P}}$') for the finite powerset domain that requires that the base-level widening '$\nabla$' is provided with a *finitely computable* certificate $\mu$. The computability requirement is important because we will directly use this certificate in the implementation of the new widening. This is also the reason why we cannot directly infer such a certificate from the partial order relation '$\vdash_{\nabla}$', which in general does not come with a computability guarantee.

*Example 5.* For the polyhedral domain $\widehat{\mathbb{CP}}_n$ and the standard widening '$\nabla_s$', a certificate $\mu$ can be inferred from any limited growth ordering relation '$\curvearrowright$' satisfying Definition 3, by letting

$$\begin{aligned}
\mu(\mathcal{P}) \succ \mu(\mathcal{Q}) &\iff \mathcal{P} \curvearrowright \mathcal{Q}, \\
\mu(\mathcal{P}) = \mu(\mathcal{Q}) &\iff (\mathcal{P} \not\curvearrowright \mathcal{Q}) \wedge (\mathcal{Q} \not\curvearrowright \mathcal{P}).
\end{aligned}$$

An alternative and slightly simpler certificate $(\mathcal{O}_s, \succ_s, \mu_s)$ can be directly provided by taking $\mathcal{O}_s$ to be the pair $(\mathbb{N}, \mathbb{N})$, '$\succ_s$' the lexicographic ordering of the pair using $>$ for the individual ordering of the components and $\mu_s\colon \mathbb{CP}_n \to \mathcal{O}_s$ be defined as the level mapping

$$\mu_s(\mathcal{P}) = \big(n - \dim(\mathcal{P}), \#\,\mathcal{C}\big),$$

where $\mathcal{C}$ is any constraint system in minimal form defining $\mathcal{P}$.

For the widening operator '$\hat{\nabla}$' on $\widehat{\mathbb{CP}}_n$ proposed in [4], a certificate can be obtained by considering the level mapping $\mu_b\colon \mathbb{CP}_n \to \mathcal{O}_b$ induced, as shown above, by the specific limited growth ordering relation defined in [4].

Given a certificate $\mu$ for a widening '$\nabla$' on $\hat{D}$, we can define a suitable limited growth ordering relation '$\curvearrowright_{\text{P}}$' for the finite powerset domain $\hat{D}_{\text{P}}$ that satisfies the ascending chain condition.

**Definition 13. (The '$\curvearrowright_{\text{P}}$' relation.)** *The relation $\curvearrowright_{\text{P}} \subseteq \wp_{\text{fn}}(D, \vdash) \times \wp_{\text{fn}}(D, \vdash)$ induced by the certificate $\mu$ for '$\nabla$' is such that, for each $S_1, S_2 \in \wp_{\text{fn}}(D, \vdash)$, $S_1 \curvearrowright_{\text{P}} S_2$ if and only if either one of the following conditions holds:*

$$\mu\big(\bigoplus S_1\big) \succ \mu\big(\bigoplus S_2\big); \tag{8}$$

$$\mu\big(\bigoplus S_1\big) = \mu\big(\bigoplus S_2\big) \wedge \#\,S_1 > 1 \wedge \#\,S_2 = 1; \tag{9}$$

$$\mu\big(\bigoplus S_1\big) = \mu\big(\bigoplus S_2\big) \wedge \#\,S_1 > 1 \wedge \#\,S_2 > 1 \wedge \tilde{\mu}(S_1) \gg \tilde{\mu}(S_2), \tag{10}$$

*where, for each $S \in \wp_{\text{fn}}(D, \vdash)$, $\tilde{\mu}(S)$ denotes the multiset over $\mathcal{O}$ obtained by applying $\mu$ to each abstract element in $S$.*

**Proposition 3.** *The '$\curvearrowright_{\mathrm{P}}$' relation satisfies the ascending chain condition.*

Intuitively, the relation '$\curvearrowright_{\mathrm{P}}$' will induce a certificate $\mu_{\mathrm{P}} \colon \hat{D}_{\mathrm{P}} \to \mathcal{O}_{\mathrm{P}}$ for the new widening. Namely, by defining $\mu_{\mathrm{P}}(S_1) \succ_{\mathrm{P}} \mu_{\mathrm{P}}(S_2)$ if and only if $S_1 \curvearrowright_{\mathrm{P}} S_2$, we will obtain $\mu_{\mathrm{P}}(S_1) \succ_{\mathrm{P}} \mu_{\mathrm{P}}(S_1 \mathbin{{}_{\mu}\nabla_{\mathrm{P}}} S_2)$.

The specification of our "certificate-based widening" assumes the existence of a *subtract* operation for the base-level domain. It is expected that a specific subtraction would be provided for each domain; here we just indicate a minimal specification.

**Definition 14. (Subtraction.)** *The partial operator $\ominus \colon D \times D \rightarrowtail D$ is a* subtraction *for $\hat{D}$ if, for all $d_1, d_2 \in D$ such that $d_2 \vdash d_1$, we have $d_1 \ominus d_2 \vdash d_1$ and $d_1 = (d_1 \ominus d_2) \oplus d_2$.*

A trivial subtraction operator can always be defined as $d_1 \ominus d_2 := d_1$. In practice, when designing a widening, the actual subtraction operator would be expected to lose as little precision as possible.

*Example 6.* In $\widehat{\mathbb{CP}}_n$, the function $\mathrm{diff} \colon \mathbb{CP}_n \times \mathbb{CP}_n \to \mathbb{CP}_n$ is defined so that, for any $\mathcal{P}, \mathcal{Q} \in \mathbb{CP}_n$, $\mathrm{diff}(\mathcal{P}, \mathcal{Q})$ denotes the smallest closed and convex polyhedron containing the set difference $\mathcal{P} \setminus \mathcal{Q}$. Then, if $\mathcal{Q} \subseteq \mathcal{P}$, we have $\mathrm{diff}(\mathcal{P}, \mathcal{Q}) \subseteq \mathcal{P}$ and

$$\begin{aligned} \mathcal{P} &= (\mathcal{P} \setminus \mathcal{Q}) \cup \mathcal{Q} \\ &= \mathrm{diff}(\mathcal{P}, \mathcal{Q}) \cup \mathcal{Q} \\ &= \mathrm{diff}(\mathcal{P}, \mathcal{Q}) \uplus \mathcal{Q}, \end{aligned}$$

so that 'diff' is a subtraction.

We can now define the *certificate-based widening* '$_{\mu}\nabla_{\mathrm{P}}$'.

**Definition 15. (The '$_{\mu}\nabla_{\mathrm{P}}$' widening.)** *Let '$\curvearrowright_{\mathrm{P}}$' be the limited growth ordering induced by the certificate $\mu$ for '$\nabla$' and let '$\boxplus_{\mathrm{P}}$' be any upper bound operator on $\hat{D}_{\mathrm{P}}$. Let $S_1, S_2 \in \wp_{\mathrm{fn}}(D, \vdash)$ be such that $S_1 \Vdash_{\mathrm{P}} S_2$. Also, if $\bigoplus S_1 \Vdash \bigoplus(S_1 \boxplus_{\mathrm{P}} S_2)$, let $d \in D$ be defined as $d := \big(\bigoplus S_1 \nabla \bigoplus(S_1 \boxplus_{\mathrm{P}} S_2)\big) \ominus \big(\bigoplus(S_1 \boxplus_{\mathrm{P}} S_2)\big)$. Then*

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

In the first case, we simply return the upper bound $S_1 \boxplus_{\mathrm{P}} S_2$, since this is enough to ensure a strict decrease in the level mapping. In the second case, the join of $S_1$ is strictly more precise than the join of $S_1 \boxplus_{\mathrm{P}} S_2$, so that we apply '$\nabla$' to them and then, using the subtraction operator, improve the obtained result, since $S_1 \curvearrowright_{\mathrm{P}} (S_1 \boxplus_{\mathrm{P}} S_2) \oplus_{\mathrm{P}} \{d\}$ holds. In the last case, since the join of $S_1$ is equivalent to the join of $S_1 \boxplus_{\mathrm{P}} S_2$, we return the singleton consisting of the join itself, as originally proposed in [12, Section 9].

**Theorem 3.** *The '$_{\mu}\nabla_{\mathrm{P}}$' operator is a widening on $\hat{D}_{\mathrm{P}}$.*

*Example 7.* To illustrate the last two cases of Definition 15, consider the domain $(\widehat{\mathbb{CP}}_1)_{\mathrm{P}}$, with the standard widening '$\nabla_s$' for $\widehat{\mathbb{CP}}_1$, certified by the level mapping $\mu_s$ defined in Example 5 and the upper bound '$\boxplus_{\mathrm{P}}$' defined as '$\oplus_{\mathrm{P}}$', so that we will always have $S_1 \boxplus_{\mathrm{P}} S_2 = S_2$.

Let $\mathcal{T}_1 = \{\{0 \leq x \leq 1\}\}$ and $\mathcal{T}_2 = \{\{0 \leq x \leq 1\}, \{2 \leq x \leq 3\}\}$. Then $\mathcal{T}_1 \not\curlywedge_{\mathrm{P}} \mathcal{T}_2$, so that the condition for the first case in Definition 15 does not hold. The poly-hulls of $\mathcal{T}_1$ and $\mathcal{T}_2$ are $\{0 \leq x \leq 1\}$ and $\{0 \leq x \leq 3\}$, respectively, so that the condition for the second case holds. Since $\biguplus \mathcal{T}_1 \nabla_s \biguplus \mathcal{T}_2 = \{0 \leq x\}$, then by letting the polyhedron $\mathcal{P}$ be the element $d$ as specified in Definition 15, we obtain $\mathcal{P} = \mathrm{diff}(\{0 \leq x\}, \{0 \leq x \leq 3\}) = \{3 \leq x\}$, so that

$$\mathcal{T}_1 \,{}_{\mu}\nabla_{\mathrm{P}}\, \mathcal{T}_2 = \mathcal{T}_2 \uplus_{\mathrm{P}} \{\mathcal{P}\} = \{\{0 \leq x \leq 1\}, \{2 \leq x \leq 3\}, \{3 \leq x\}\}.$$

Now let $\mathcal{T}_3 = \{\{x = 1\}, \{x = 3\}\}$ and $\mathcal{T}_4 = \{\{x = 1\}, \{x = 2\}, \{x = 3\}\}$. Then $\mathcal{T}_3 \not\curlywedge_{\mathrm{P}} \mathcal{T}_4$, so that the condition for the first case in Definition 15 does not hold. Moreover, $\biguplus \mathcal{T}_3 = \biguplus \mathcal{T}_4 = \{1 \leq x \leq 3\}$, so that neither the second case applies. Thus, $\mathcal{T}_3 \,{}_{\mu}\nabla_{\mathrm{P}}\, \mathcal{T}_4 = \{\{1 \leq x \leq 3\}\}$.

As shown in the example above, Definition 15 does not require that the upper bound operator '$\boxplus_{\mathrm{P}}$' is based on the base-level widening '$\nabla$'. Moreover, the scheme of Definition 15 can be easily extended to any finite set of heuristically chosen upper bound operators on $\hat{D}_{\mathrm{P}}$, still obtaining a proper widening operator for the powerset domain. The simplest heuristics, already used in the example above, is the one taking $\boxplus_{\mathrm{P}} := \oplus_{\mathrm{P}}$. If this fails to ensure a decrease in the level mapping, another possibility is the adoption of an extrapolation heuristics '$h^{\nabla}_{\mathrm{P}}$' for $\hat{D}_{\mathrm{P}}$. Anyway, many variations could be defined, depending on the required precision/efficiency trade-off. In the following section, we investigate one of these possibilities, which originates as a generalization of an idea proposed in [8].

## 5 Merging Elements According to a Congruence Relation

When computing a powerset widening $S_1 \nabla_{\mathrm{P}} S_2$, no matter if it is based on an Egli-Milner connector, a $k$-collapsor, or a finite convergence certificate, some of the elements occurring in the second argument $S_2$ can be *merged together* (i.e., joined) without compromising the finite convergence guarantee. This merging operation can be guided by a congruence relation on the finite powerset domain $\hat{D}_{\mathrm{P}}$, the idea being that a well-chosen relation will benefit the precision/efficiency trade-off of the widening.

One option is to use semantics preserving congruence relations, i.e., refinements of the congruence relation '$\equiv_{\gamma_{\mathrm{P}}}$'. The availability of relatively efficient but incomplete tests for semantic equivalence can thus be exploited to improve the efficiency and/or the precision of the analysis. As the purpose of this paper is to provide generic widening procedures for powersets that are independent of the underlying domains and hence, of any intended concretizations, here we define these congruences in a way that is independent of the particular concrete domain

adopted. Two such relations are the *identity congruence* relation, where no non-trivial equivalence is assumed, and the $\oplus$-*congruence* relation, where sets that have the same join are equivalent. Note that both these have the useful property that congruent elements have the same join. However, the identity congruence allows for no merging at all and hence it will have no influence on the convergence of the iteration sequence; on the other hand, the $\oplus$-congruence allows for a complete merging of the abstract collection and is usually the basis of the default, roughest heuristics for ensuring termination. We now define a congruence relation that lies between these extremes and still preserves the mentioned property.

**Definition 16. ('$\lhd$' and '$\bowtie$'.)** *The* content *relation* $\lhd \subseteq \wp_{\mathrm{fn}}(D,\vdash) \times \wp_{\mathrm{fn}}(D,\vdash)$ *is such that* $S_1 \lhd S_2$ *holds if and only if for all* $S_1' \in \wp_{\mathrm{fn}}(D,\vdash)$ *where* $S_1' \vdash_{\mathrm{P}} S_1$ *there exists* $S_1'' \in \wp_{\mathrm{fn}}(D,\vdash)$ *such that* $\bigoplus S_1' = \bigoplus S_1''$ *and* $S_1'' \vdash_{\mathrm{P}} S_2$. *The* same-content *relation* $\bowtie \subseteq \wp_{\mathrm{fn}}(D,\vdash) \times \wp_{\mathrm{fn}}(D,\vdash)$ *is such that* $S_1 \bowtie S_2$ *holds if and only if* $S_1 \lhd S_2$ *and* $S_2 \lhd S_1$.

Thus, for any $S, S' \in \wp_{\mathrm{fn}}(D,\vdash)$, we have that $S \vdash_{\mathrm{P}} S'$ implies that $S \lhd S'$ so that $S \lhd \{\bigoplus S\}$, since $S \vdash_{\mathrm{P}} \{\bigoplus S\}$. Moreover, if $S$ is a singleton, then $S' \vdash_{\mathrm{P}} S$ if and only if $S' \lhd S$. Note that '$\bowtie$' is a congruence relation on $\hat{D}_{\mathrm{P}}$.

Observe that the identity congruence relation can be obtained by strengthening the conditions in the definition of '$\lhd$', replacing $\bigoplus S_1' = \bigoplus S_1''$ with $S_1' = S_1''$; and the $\oplus$-congruence can be obtained by weakening the conditions, replacing $S_1'' \vdash_{\mathrm{P}} S_2$ with $\bigoplus S_1'' \vdash \bigoplus S_2$. Thus the same-content relation is a compromise between keeping all the information provided by the explicit set structure, as done by the identity congruence, and losing all of this information, as occurs with the $\oplus$-congruence.

For the finite powerset domain of polyhedra $(\widehat{\mathbb{CP}}_n)_{\mathrm{P}}$, the content relation '$\lhd$' corresponds to the condition that all the points in polyhedra in the first set are contained by polyhedra in the second set; and hence, the same-content congruence relation '$\bowtie$' coincides with the induced congruence relation '$\equiv_{\gamma_{\mathrm{P}}^{\mathrm{A}}}$'.

**Proposition 4.** *For all* $\mathcal{S}_1, \mathcal{S}_2 \in \wp_{\mathrm{fn}}(\mathbb{CP}_n, \subseteq)$, $\mathcal{S}_1 \bowtie \mathcal{S}_2$ *if and only if* $\mathcal{S}_1 \equiv_{\gamma_{\mathrm{P}}^{\mathrm{A}}} \mathcal{S}_2$.

*Example 8.* For $\mathcal{T}_1, \mathcal{T}_2 \in \wp_{\mathrm{fn}}(\mathbb{CP}_1, \subseteq)$ as defined in Example 1, we have $\mathcal{T}_1 \bowtie \mathcal{T}_2$. Consider also $\mathcal{T}_3, \mathcal{T}_4 \in \wp_{\mathrm{fn}}(\mathbb{CP}_1, \subseteq)$ where

$$\mathcal{T}_3 := \big\{\{0 \le x \le 3\}, \{1 \le x \le 5\}\big\}, \qquad \mathcal{T}_4 := \big\{\{0 \le x \le 5\}\big\}.$$

Then $\mathcal{T}_3 \bowtie \mathcal{T}_4$ and also $\mathcal{T}_2 \lhd \mathcal{T}_4$ although the converse does not hold. To see this, let $S_1$, $S_2$, and $S_2'$ in Definition 16 be $\mathcal{T}_2$, $\mathcal{T}_4$, and $\mathcal{T}_4' := \big\{\{x = 2.5\}\big\}$, respectively. Then, if $\mathcal{T}_4''$ is such that $\biguplus \mathcal{T}_4'' = \biguplus \mathcal{T}_4'$ and $\mathcal{T}_4'' \subseteq_{\mathrm{P}} \mathcal{T}_4'$, we must have $\mathcal{T}_4'' = \mathcal{T}_4' \not\subseteq_{\mathrm{P}} \mathcal{T}_2$; hence, although $\mathcal{T}_4 = \big\{\biguplus \mathcal{T}_2\big\}$, we have $\mathcal{T}_4 \not\lhd \mathcal{T}_2$.

We now define an operation *merger* that is parametric with respect to the congruence relation and replaces selected subsets by congruent singleton sets.

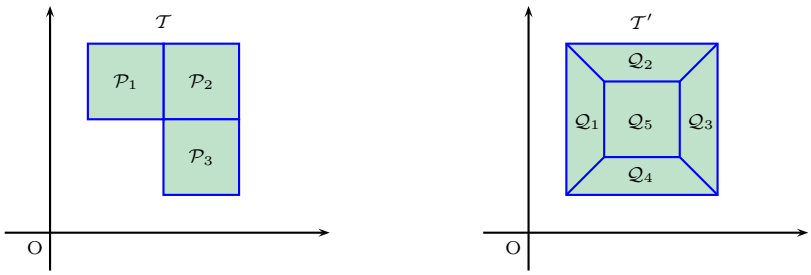


**Fig. 1.** Merging polyhedra according to '$\bowtie$'.

**Definition 17. (Merge and mergers.)** *Let $R$ be a congruence relation on $\hat{D}_{\mathrm{P}}$. Then the* merge *relation* $\mathrm{merge}_R \subseteq \wp_{\mathrm{fn}}(D,\vdash) \times \wp_{\mathrm{fn}}(D,\vdash)$ *for $R$ is such that* $\mathrm{merge}_R(S_1, S_2)$ *holds if and only if $S_1 \vdash_{\mathrm{P}} S_2$ and*

$$\forall d_2 \in S_2 : \exists S_1' \subseteq S_1 \,.\, d_2 = \bigoplus S_1' \wedge \{d_2\}\ R\ S_1'.$$

*A set $S \in \wp_{\mathrm{fn}}(D,\vdash)$ is* fully-merged for $R$, *if* $\mathrm{merge}_R(S, S')$ *implies $S = S'$; $S$ is* pairwise-merged for $R$ *if, for all $d_1, d_2 \in S$, we have that $\{d_1, d_2\}$ is fully-merged. An operator $\uparrow_R \colon \wp_{\mathrm{fn}}(D,\vdash) \to \wp_{\mathrm{fn}}(D,\vdash)$ is a* merger *for $R$ if* $\mathrm{merge}_R(S, \uparrow_R S)$ *holds.*

Observe that, for all $S \in \wp_{\mathrm{fn}}(D,\vdash)$, we have $S \vdash_{\mathrm{EM}} \uparrow_R S$.

As $R$ is a congruence relation on $\hat{D}_{\mathrm{P}}$, for any merger '$\uparrow_R$' for $R$ and $S \in \hat{D}_{\mathrm{P}}$, $S\ R\ (\uparrow_R S)$ holds. For any congruence relation $R$ on $\hat{D}_{\mathrm{P}}$ that refines the $\oplus$-congruence relation, we can always merge a set to obtain one that is fully- or pairwise-merged.

**Proposition 5.** *Let $R$ be congruence relation on $\hat{D}_{\mathrm{P}}$ that refines the $\oplus$-congruence relation. Then there exists a merger '$\uparrow_R$' such that, for all $S \in \wp_{\mathrm{fn}}(D,\vdash)$, $\uparrow_R S$ is fully-merged (resp., pairwise-merged).*

For the finite powerset domain over $\widehat{\mathbb{CP}}_n$, lines 1–9 of the algorithm specified in [8, Figure 8, page 773] define a merger operator '$\uparrow_{\bowtie}$' such that, for each finite set $\mathcal{S}$ of polyhedra, $\uparrow_{\bowtie} \mathcal{S}$ is pairwise-merged.

*Example 9.* Figure 1 shows two examples of sets of polyhedra. In the left-hand diagram, the set $\mathcal{T} = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3\}$ of three squares is not pairwise-merged for '$\bowtie$' since $\mathcal{P}_1 \cup \mathcal{P}_2$ and $\mathcal{P}_2 \cup \mathcal{P}_3$ are convex polyhedra. Both $\mathcal{T}_1 = \{\mathcal{P}_1 \cup \mathcal{P}_2, \mathcal{P}_3\}$ and $\mathcal{T}_2 = \{\mathcal{P}_1, \mathcal{P}_2 \cup \mathcal{P}_3\}$ are fully-merged and hence pairwise-merged for '$\bowtie$', and $\mathrm{merge}_{\bowtie}(\mathcal{T}, \mathcal{T}_i)$ holds for $i = 1, 2$. In the right-hand diagram, the set $\mathcal{T}' = \{\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3, \mathcal{Q}_4, \mathcal{Q}_5\}$ is pairwise-merged but not fully-merged for '$\bowtie$'. Since $\mathcal{Q}' := \bigcup \mathcal{T}'$ is a convex polyhedron, the singleton set $\{\mathcal{Q}'\}$ is fully-merged and hence pairwise-merged for '$\bowtie$' and $\mathrm{merge}_{\bowtie}\big(\mathcal{T}', \{\mathcal{Q}'\}\big)$ holds.

## 6 Conclusion

We have studied the problem of endowing any abstract domain obtained by means of the finite powerset construction with a provably correct widening operator. We have proposed three generic widening operators and we have instantiated our techniques, which are completely general, on powersets of convex polyhedra, an abstract domain that is being used for static analysis and abstract model-checking and for which no non-trivial widening operator was previously known.

We have extended the *Parma Polyhedra Library* (PPL) [3, 6], a modern C++ library for the manipulation of convex polyhedra, with a prototype implementation of the certificate-based widening and its variant employing the 'widening up to' technique [21, 22]. The experimental work has just started, but the initial results obtained are very encouraging as our new widening compares favorably, both in terms of precision and efficiency, with the extrapolation operator of [8].

## References


1. S. Abramsky and A. Jung. Domain theory. In S. Abramsky, D. M. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 3, chapter 1, pages 1–168. Clarendon Press, Oxford, UK, 1994.
2. R. Bagnara. A hierarchy of constraint systems for data-flow analysis of constraint logic-based languages. *Science of Computer Programming*, 30(1–2):119–155, 1998.
3. R. Bagnara, P. M. Hill, E. Ricci, and E. Zaffanella. *The Parma Polyhedra Library User's Manual*. Department of Mathematics, University of Parma, Parma, Italy, release 0.5 edition, April 2003. Available at `http://www.cs.unipr.it/ppl/`.
4. R. Bagnara, P. M. Hill, E. Ricci, and E. Zaffanella. Precise widening operators for convex polyhedra. In R. Cousot, editor, *Static Analysis: Proceedings of the 10th International Symposium*, volume 2694 of *Lecture Notes in Computer Science*, pages 337–354, San Diego, California, USA, 2003. Springer-Verlag, Berlin.
5. R. Bagnara, P. M. Hill, E. Ricci, and E. Zaffanella. Precise widening operators for convex polyhedra. Quaderno 312, Dipartimento di Matematica, Università di Parma, Italy, 2003. Available at `http://www.cs.unipr.it/Publications/`.
6. R. Bagnara, E. Ricci, E. Zaffanella, and P. M. Hill. Possibly not closed convex polyhedra and the Parma Polyhedra Library. In M. V. Hermenegildo and G. Puebla, editors, *Static Analysis: Proceedings of the 9th International Symposium*, volume 2477 of *Lecture Notes in Computer Science*, pages 213–229, Madrid, Spain, 2002. Springer-Verlag, Berlin.
7. F. Besson, T. P. Jensen, and J.-P. Talpin. Polyhedral analysis for synchronous languages. In A. Cortesi and G. Filé, editors, *Static Analysis: Proceedings of the 6th International Symposium*, volume 1694 of *Lecture Notes in Computer Science*, pages 51–68, Venice, Italy, 1999. Springer-Verlag, Berlin.
8. T. Bultan, R. Gerber, and W. Pugh. Model-checking concurrent systems with unbounded integer variables: Symbolic representations, approximations, and experimental results. *ACM Transactions on Programming Languages and Systems*, 21(4):747–789, 1999.
9. A. Cortesi, B. Le Charlier, and P. Van Hentenryck. Combinations of abstract domains for logic programming: Open product and generic pattern construction. *Science of Computer Programming*, 38(1–3):27–71, 2000.

10. P. Cousot and R. Cousot. Static determination of dynamic properties of programs. In B. Robinet, editor, *Proceedings of the Second International Symposium on Programming*, pages 106–130. Dunod, Paris, France, 1976.
11. P. Cousot and R. Cousot. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Proceedings of the Fourth Annual ACM Symposium on Principles of Programming Languages*, pages 238–252, New York, 1977. ACM Press.
12. P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Proceedings of the Sixth Annual ACM Symposium on Principles of Programming Languages*, pages 269–282, New York, 1979. ACM Press.
13. P. Cousot and R. Cousot. Abstract interpretation and applications to logic programs. *Journal of Logic Programming*, 13(2&3):103–179, 1992.
14. P. Cousot and R. Cousot. Abstract interpretation frameworks. *Journal of Logic and Computation*, 2(4):511–547, 1992.
15. P. Cousot and R. Cousot. Comparing the Galois connection and widening/narrowing approaches to abstract interpretation. In M. Bruynooghe and M. Wirsing, editors, *Proceedings of the 4th International Symposium on Programming Language Implementation and Logic Programming*, volume 631 of *Lecture Notes in Computer Science*, pages 269–295, Leuven, Belgium, 1992. Springer-Verlag, Berlin.
16. P. Cousot and N. Halbwachs. Automatic discovery of linear restraints among variables of a program. In *Conference Record of the Fifth Annual ACM Symposium on Principles of Programming Languages*, pages 84–96, Tucson, Arizona, 1978. ACM Press.
17. G. Delzanno and A. Podelski. Model checking in CLP. In R. Cleaveland, editor, *Tools and Algorithms for Construction and Analysis of Systems, 5th International Conference, TACAS '99*, volume 1579 of *Lecture Notes in Computer Science*, pages 223–239, Amsterdam, The Netherlands, 1999. Springer-Verlag, Berlin.
18. N. Dershowitz and Z. Manna. Proving termination with multiset orderings. *Communications of the ACM*, 22(8):465–476, 1979.
19. G. Filé and F. Ranzato. The powerset operator on abstract interpretations. *Theoretical Computer Science*, 222:77–111, 1999.
20. N. Halbwachs. *Détermination Automatique de Relations Linéaires Vérifiées par les Variables d'un Programme*. Thèse de 3ème cycle d'informatique, Université scientifique et médicale de Grenoble, Grenoble, France, March 1979.
21. N. Halbwachs. Delay analysis in synchronous programs. In C. Courcoubetis, editor, *Computer Aided Verification: Proceedings of the 5th International Conference*, volume 697 of *Lecture Notes in Computer Science*, pages 333–346, Elounda, Greece, 1993. Springer-Verlag, Berlin.
22. N. Halbwachs, Y.-E. Proy, and P. Roumanoff. Verification of real-time systems using linear relation analysis. *Formal Methods in System Design*, 11(2):157–185, 1997.
23. C. Holzbaur. OFAI clp(q,r) manual, edition 1.3.3. Technical Report TR-95-09, Austrian Research Institute for Artificial Intelligence, Vienna, 1995.
24. W. Kelly, V Maslov, W. Pugh, E. Rosser, T. Shpeisman, and D. Wonnacott. The Omega library interface guide. Technical Report CS-TR-3445, Department of Computer Science, University of Maryland, College Park, MD, USA, 1995.
25. H. Le Verge. A note on Chernikova's algorithm. *Publication interne* 635, IRISA, Campus de Beaulieu, Rennes, France, 1992.

26. V. Loechner. *PolyLib*: A library for manipulating parameterized polyhedra. Available at `http://icps.u-strasbg.fr/~loechner/polylib/`, March 1999. Declares itself to be a continuation of [29].
27. W. Pugh. A practical algorithm for exact array dependence analysis. *Communications of the ACM*, 35(8):102–114, 1992.
28. D. Srivastava. Subsumption and indexing in constraint query languages with linear arithmetic constraints. *Annals of Mathematics and Artificial Intelligence*, 8(3–4):315–343, 1993.
29. D. K. Wilde. A library for doing polyhedral operations. Master's thesis, Oregon State University, Corvallis, Oregon, December 1993. Also published as IRISA *Publication interne* 785, Rennes, France, 1993.

# A Proofs

**Proof (of Proposition 1 on page 10).** Let $S := S_2 \cup \Omega^{\vdash}_D(S')$, where

$$S' := \{\, d_1 \nabla d_2 \in D \mid d_1 \in S_1, d_2 \in S_2, d_1 \Vdash d_2 \,\}.$$

Then, by hypothesis, $h^{\nabla}_{\text{P}}(S_1, S_2) = \Omega^{\vdash}_D(S)$. To prove that '$h^{\nabla}_{\text{P}}$' is a $\nabla$-connected extrapolation heuristics for $\hat{D}_{\text{P}}$, we need to prove that properties (4) and (5) of Definition 6 and property (6) of Definition 7 hold.

We first show that property (4) of Definition 6 holds. Suppose $d_2 \in S_2$. Then, as $S_2 \subseteq S$, we have $d_2 \in S$. By Definition 4, there exists $d'_2 \in \Omega^{\vdash}_D(S)$ such that $d_2 \vdash d'_2$. Thus, by Definition 5, $S_2 \vdash_{\text{P}} h^{\nabla}_{\text{P}}(S_1, S_2)$. Suppose next that $d \in h^{\nabla}_{\text{P}}(S_1, S_2) \setminus S_2$. Then $d \in \Omega^{\vdash}_D(S') \subseteq S'$, so that there exists $d_1 \in S_1$ and $d_2 \in S_2$ such that $d = d_1 \nabla d_2$. Since '$\nabla$' is a widening on $\hat{D}$, $d_2 \vdash d$. Thus, it follows that $S_2 \vdash_{\text{EM}} h^{\nabla}_{\text{P}}(S_1, S_2)$.

Secondly we show that property (5) of Definition 6 and property (6) of Definition 7 hold. Let $d \in h^{\nabla}_{\text{P}}(S_1, S_2)$ and $d_1 \in S_1$ be such that $d_1 \Vdash d$.

We first suppose that $d \in S_2$ and show that $d \in S'$. As $d_1 \Vdash d$, $d_1 \nabla d$ is defined and is in $S'$. As '$\nabla$' is a widening, $d \vdash d_1 \nabla d$. By Definition 4, there exists $d' \in \Omega^{\vdash}_D(S')$ such that $d_1 \nabla d \vdash d'$. However $\Omega^{\vdash}_D(S') \subseteq S$ so that, again by Definition 4, there exists $d'' \in \Omega^{\vdash}_D(S) = h^{\nabla}_{\text{P}}(S_1, S_2)$ such that $d' \vdash d''$ and hence, by transitivity of '$\vdash$', $d \vdash d''$. Since $d, d'' \in h^{\nabla}_{\text{P}}(S_1, S_2) \in \wp_{\text{fn}}(D, \vdash)$ we must have $d = d' = d''$ so that $d \in S'$.

Since, by hypothesis, $h^{\nabla}_{\text{P}}(S_1, S_2) \subseteq S_2 \cup S'$ and, by the previous paragraph, $d \in S_2$ implies that $d \in S'$, it follows that, in all cases, we must have $d \in S'$. Thus there exists $d'_1 \in S_1$ and $d_2 \in S_2$ such that $d = d'_1 \nabla d_2$ and hence $d'_1 \Vdash_{\nabla} d$. Therefore both properties (5) of Definition 6 and (6) of Definition 7 hold. □

**Proof (of Theorem 1 on page 11).** We first prove that that condition (1) in Definition 1 holds, i.e., that $S_2 \vdash_{\text{P}} S_1 \,{}_{\text{EM}}\nabla_{\text{P}}\, S_2$. Assume the notation and the hypotheses introduced in Definition 8 and let $T := S_1 \,{}_{\text{EM}}\nabla_{\text{P}}\, S_2 = h^{\nabla}_{\text{P}}(S_1, S'_2)$. By definition of '$\boxplus_{\text{EM}}$', we have $S_2 \vdash_{\text{EM}} S_1 \boxplus_{\text{EM}} S_2$. Thus, in both the cases of the definition of $S'_2$, we obtain $S_2 \vdash_{\text{EM}} S'_2$, which implies $S_2 \vdash_{\text{P}} S'_2$. Moreover, by Definition 6, $S'_2 \vdash_{\text{P}} T$ so that, by transitivity of '$\vdash_{\text{P}}$', $S_2 \vdash_{\text{P}} T$.

We now prove condition (2) holds in Definition 1. Suppose $T_0 \vdash_{\text{P}} T_1 \vdash_{\text{P}} \cdots$ is an increasing chain of elements in $\wp_{\text{fn}}(D, \vdash)$ and consider the widened sequence defined by $U_0 := T_0$ and, for each $i > 0$, $U_i := U_{i-1} \,{}_{\text{EM}}\nabla_{\text{P}}\, (U_{i-1} \oplus_{\text{P}} T_i)$. As we have already shown that condition (1) in Definition 1 holds, $(U_{i-1} \oplus_{\text{P}} T_i) \vdash_{\text{P}} U_i$ so that, by transitivity of '$\vdash_{\text{P}}$', $U_{i-1} \vdash_{\text{P}} U_i$. Thus $U_0 \vdash_{\text{P}} U_1 \vdash_{\text{P}} \cdots$ is another increasing chain in $\wp_{\text{fn}}(D, \vdash)$. We need to show that the widened sequence converges in a finite number of steps.

For each $i > 0$, consider the successive widened iterates $U_{i-1}$ and $U_i$, so that, according to Definition 8, we can write $U_i = h_{\text{P}}^{\nabla}(U_{i-1}, S_2')$, where in both the cases for the definition of $S_2'$ we have $U_{i-1} \vdash_{\text{EM}} S_2'$. Since '$h_{\text{P}}^{\nabla}$' is a $\nabla$-connected extrapolation heuristics, by property (4) of Definition 6, we have $S_2' \vdash_{\text{EM}} U_i$ and, by transitivity of '$\vdash_{\text{EM}}$', $U_{i-1} \vdash_{\text{EM}} U_i$. Moreover, in the above context, the properties (5) of Definition 6 and (6) of Definition 7 can be rewritten to the simpler property:

$$\forall d' \in U_i : \exists d \in U_{i-1} \,.\, d \vdash_{\nabla} d'. \tag{11}$$

Let $W_i \subseteq D \times D$ be defined so that $(d, d') \in W_i$ holds if and only if $d \in U_{i-1}$, $d' \in U_i$ and $d \Vdash_{\nabla} d'$. Thus, by property (11), we have

$$\forall d' \in U_i \setminus U_{i-1} : \exists d \in U_{i-1} \,.\, (d, d') \in W_i. \tag{12}$$

For each $i \in \mathbb{N}$, consider the finite directed graph $G_i = (V_i, E_i)$, where

- the set of vertices $V_i \subseteq D$ is $V_i := \bigcup\{\, U_j \mid 0 \leq j \leq i \,\}$;
- the set of edges $E_i \subseteq V_i \times V_i$ is $E_i := \bigcup\{\, W_j \mid 0 < j \leq i \,\}$.

Furthermore, consider the (*a priori*, possibly infinite) graph $G = (V, E)$ such that $V = \bigcup_{i \geq 0} V_i$ and $E = \bigcup_{i \geq 0} E_i = \bigcup_{i \geq 1} W_i$. We will now show that $G$ is a finite and acyclic graph, so that, by property (12), '${}_{\text{EM}}\nabla_{\text{P}}$' is a widening. Namely, we will prove the following properties for the graph $G$, which combined together imply that $G$ is a finite and acyclic graph:

1. $G$ has no infinite paths;
2. $G$ has a finite number of connected components;
3. $G$ is finitely branching, i.e., each vertex has finite outdegree.

To prove $G$ has no infinite paths, suppose $p := d_0 \to d_1 \to \cdots \to d_i \to \cdots$ is a (possibly infinite) path in $G$. By the definition of $G$, if $(d_{k-1}, d_k)$ is an edge in $p$ for some $k > 0$, then there exists an index $j > 0$ such that $(d_{k-1}, d_k) \in W_j$. By definition of $W_j$, we know that $d_{k-1} \Vdash_{\nabla} d_k$. Thus, we have a strictly increasing sequence $d_0 \Vdash_{\nabla} d_1 \Vdash_{\nabla} \cdots \Vdash_{\nabla} d_i \Vdash_{\nabla} \cdots$ and hence, as '$\Vdash_{\nabla}$' satisfies the ascending chain condition, the path $p$ must be finite.

We now prove that the graph $G$ has a finite number of connected components. Consider, for any $i > 0$ the graph $G_i = (V_i, E_i)$. Then, by property (12), for each vertex $d_i$ in $V_i$ either $d_i \in V_{i-1}$ or there is an edge $(d_{i-1}, d_i)$ in $E_i$ where $d_{i-1} \in U_{i-1} \subseteq V_{i-1}$. Thus, for all $i \in \mathbb{N}$, the number of components of $G_i$ is no more than the number of components of $G_{i-1}$. As the number of components of $G_0$ is $\# U_0$, the number of components of $G$ is no more than $\# U_0$.

Finally, to prove that $G$ is finitely branching, consider any vertex $d \in V$. Suppose that, for some index $i > 0$, there exists $(d, d') \in E_i \setminus E_{i-1}$ (note that $(d, d') \notin E_0$ because $E_0 = \varnothing$). Then $(d, d') \in W_i$. Thus, by definition of $W_i$, $d \in U_{i-1}$ and $d' \in U_i \setminus U_{i-1}$ and $d \Vdash d'$. However, for all indices $j \geq i$, as $U_i \vdash_{\mathrm{P}} U_j$, there exists $d_j \in U_j$ such that $d' \vdash d_j$ so that $d \Vdash d_j$; as $U_j$ is a non-redundant set (in the sense of Definition 4), $d \notin U_j$. Thus all outgoing edges from $d$ are in $E_i$. As the set $E_i$ is finite, $d$ has a finite number of outgoing edges. □

**Proof (of Proposition 2 on page 12).** Let $S = S_1 \cup S_2$, so that $h^{\nabla}_{\mathrm{P}}(S_1, S_2) = \Omega^{\nabla}_D(S)$. By Definition 11, there exists $m \in \mathbb{N}$ and a sequence $T_0, \ldots, T_m$ in $\wp_{\mathrm{f}}(D)$ where $T_0 = S$, $T_m = \Omega^{\nabla}_D(S) \in \wp_{\mathrm{fn}}(D, \vdash)$ and, for each $0 < i \leq m$, there exists $d, d' \in T_{i-1}$ such that $d \Vdash d'$ and $T_i = \big(T_{i-1} \setminus \{d, d'\}\big) \cup \{d \nabla d'\}$. Thus, for all $d \in T_{i-1}$ there exists $d' \in T_i$ such that $d \vdash_{\nabla} d'$. We prove, for all $0 \leq i \leq m$, the following properties hold:

$$\forall d \in S_2 : \exists d_i \in T_i \,.\, d \vdash d_i; \tag{13}$$

$$\forall d_i \in T_i : \exists d \in S_2 \,.\, d \vdash d_i; \tag{14}$$

$$\forall d_i \in T_i \setminus S : \exists d \in S_1 \,.\, d \Vdash_{\nabla} d_i; \tag{15}$$

$$\forall d \in S_1 : \exists d_i \in T_i \,.\, d \vdash_{\nabla} d_i. \tag{16}$$

Letting $i = m$ in properties (13) and (14) we obtain $S_2 \vdash_{\mathrm{EM}} \Omega^{\nabla}_D(S)$, so that property (4) in Definition 6 holds. Since $S_1 \vdash_{\mathrm{P}} S_2$ and $T_m \in \wp_{\mathrm{fn}}(D, \vdash)$, we have $T_m \setminus S = T_m \setminus S_2$; thus, letting $i = m$ in property (15), we obtain that property (5) in Definition 6 holds. Thus '$h^{\nabla}_{\mathrm{P}}$' is an extrapolation heuristics for $\hat{D}_{\mathrm{P}}$. Moreover, letting $i = m$ in property (16), we obtain that property (7) in Definition 10 holds, so that '$h^{\nabla}_{\mathrm{P}}$' is $\nabla$-covered.

We now prove the four properties by induction on $i$. For the base case, we have $i = 0$ and $T_0 = S = S_1 \cup S_2$, so that all the properties hold trivially. For the inductive case, assuming that $m > 0$, consider an index $j$ such that $0 < j \leq m$ and all the properties hold for all $i \geq 0$ where $0 \leq i < j$; we show they also hold when $i = j$. By Definition 11, if $d_{j-1} \in T_{j-1}$, then there exists $d_j \in T_j$ such that either $d_{j-1} = d_j$ or there exists $d'_{j-1} \in T_{j-1}$ such that $d_{j-1} \Vdash d'_{j-1} \neq d_j$ and $d_j = d_{j-1} \nabla d'_{j-1}$; in both cases, $d_{j-1} \vdash_{\nabla} d_j$. Thus, assuming properties (13), (14), (15) and (16) hold for $i = j - 1$, they also hold for $i = j$. □

**Proof (of Theorem 2 on page 12).** We first prove that condition (1) holds in Definition 1, i.e., that $S_2 \vdash_{\mathrm{P}} S_1 \,{}_k\nabla_{\mathrm{P}}\, S_2$. Assume the notation and the hypotheses introduced in Definition 12 and let $T := S_1 \,{}_k\nabla_{\mathrm{P}}\, S_2 = h^{\nabla}_{\mathrm{P}}(S_1, S'_2)$. By Definition 9, $S_2 \vdash_{\mathrm{P}} \Uparrow_k(S_2)$. Thus, in both the cases of the definition of $S'_2$, we obtain $S_2 \vdash_{\mathrm{P}} S'_2$. Moreover, by Definition 6, $S'_2 \vdash_{\mathrm{P}} T$ so that, by transitivity of '$\vdash_{\mathrm{P}}$', $S_2 \vdash_{\mathrm{P}} T$.

We now prove condition (2) holds in Definition 1. Suppose $T_0 \vdash_{\mathrm{P}} T_1 \vdash_{\mathrm{P}} \cdots$ is an increasing chain of elements in $\wp_{\mathrm{fn}}(D, \vdash)$ and consider the widened sequence defined by $U_0 := T_0$ and, for each $i > 0$, $U_i := U_{i-1} \,{}_k\nabla_{\mathrm{P}}\, (U_{i-1} \oplus_{\mathrm{P}} T_i)$. As we have already shown that condition (1) in Definition 1 holds, $(U_{i-1} \oplus_{\mathrm{P}} T_i) \vdash_{\mathrm{P}} U_i$ so that, by transitivity of '$\vdash_{\mathrm{P}}$', $U_{i-1} \vdash_{\mathrm{P}} U_i$. Thus $U_0 \vdash_{\mathrm{P}} U_1 \vdash_{\mathrm{P}} \cdots$ is another increasing chain in $\wp_{\mathrm{fn}}(D, \vdash)$.

For each $i > 0$, consider the successive widened iterates $U_{i-1}$ and $U_i$. According to Definition 12, we have $U_i = h_{\text{P}}^{\nabla}(U_{i-1}, S'_i)$, where

$$S_i := U_{i-1} \oplus_{\text{P}} T_i;$$
$$S'_i := \begin{cases} S_i, & \text{if } \# S_i \leq k; \\ \Uparrow_k(S_i), & \text{otherwise.} \end{cases}$$

By Definition 9, in both the cases for the definition of $S'_i$, we have $U_{i-1} \vdash_{\text{P}} S'_i$ and $\# S'_i \leq k$. For an arbitrary $j \in \mathbb{N}$, let $d_j \in U_j$. Then, by condition (7) in Definition 10, there exists $d_{j+1} \in U_{j+1}$ such that $d_j \vdash_{\nabla} d_{j+1}$. By transitivity, for all $i > j$, there exists $d_i \in U_i$ such that $d_j \vdash_{\nabla} d_i$. As the '$\Vdash_{\nabla}$' relation satisfies the ascending chain condition, there exist $m \in \mathbb{N}$ and $d_m \in U_m$ such that, for all $i \geq m$, $d_m \in U_i$.

Suppose that the widening iteration does not converge in a finite number of steps. Then, by the point above, there must exist an index $\ell \in \mathbb{N}$ such that $\#(U_{\ell-1} \cap U_\ell) = k$. By definition of $S'_\ell$, we have $U_{\ell-1} \vdash_{\text{P}} S'_\ell \vdash_{\text{P}} U_\ell$ and $\# S'_\ell \leq k$. Thus, by Definition 4, we obtain both $S'_\ell = U_{\ell-1} \cap U_\ell$ and $U_{\ell-1} = S'_\ell$. By condition (4) of Definition 6, we know that $S'_\ell \vdash_{\text{EM}} U_\ell$, so that $U_\ell = S'_\ell = U_{\ell-1}$. Thus, the widening iteration converges, contradicting the assumption made at the beginning of this paragraph. □

In order to prove Proposition 3, we first define a minor variant (a coarsening) of the '$\curvearrowright_{\text{P}}$' relation and show that it satisfies the ascending chain condition.

**Definition 18. (The '$\curvearrowright_{\text{L}}$' relation.)** *The relation $\curvearrowright_{\text{L}} \subseteq \wp_{\text{fn}}(D, \vdash) \times \wp_{\text{fn}}(D, \vdash)$ induced by the certificate $\mu$ for '$\nabla$' is such that, for each $S_1, S_2 \in \wp_{\text{fn}}(D, \vdash)$, $S_1 \curvearrowright_{\text{L}} S_2$ if and only if either one of the following conditions holds:*

$$\mu\big(\bigoplus S_1\big) \succ \mu\big(\bigoplus S_2\big);$$
$$\mu\big(\bigoplus S_1\big) = \mu\big(\bigoplus S_2\big) \wedge \tilde{\mu}(S_1) \gg \tilde{\mu}(S_2).$$

**Lemma 1.** *The '$\curvearrowright_{\text{L}}$' relation on $\hat{D}_{\text{P}}$ satisfies the ascending chain condition.*

*Proof.* By assumption, $(\mathcal{O}, \succ, \mu)$ is a finite convergence certificate for the base-level widening operator '$\nabla$', so that '$\succ$' is a well-founded ordering on $\mathcal{O}$. As noted in Section 2, letting $\mathcal{M}(\mathcal{O})$ denote the set of all the multisets having elements in $\mathcal{O}$, the (strict) multiset ordering relation $\gg \subseteq \mathcal{M}(\mathcal{O}) \times \mathcal{M}(\mathcal{O})$ induced by '$\succ$' is also well-founded. As a consequence, the lexicographic product of '$\succ$' and '$\gg$' is a well-founded partial order relation on the product $\mathcal{O} \times \mathcal{M}(\mathcal{O})$. Note that, by Definition 18, $S_1 \curvearrowright_{\text{L}} S_2$ holds if and only if there is a strict decrease in this lexicographic product ordering, so that '$\curvearrowright_{\text{L}}$' satisfies the ascending chain condition. □

**Proof (of Proposition 3 on page 14).** Let $S_0 \curvearrowright_{\text{P}} S_1 \curvearrowright_{\text{P}} \cdots \curvearrowright_{\text{P}} S_i \curvearrowright_{\text{P}} \cdots$ be a chain of abstract elements in the finite powerset domain $\hat{D}_{\text{P}}$. In order to prove that the chain is finite, we will show that, for all indices $i \in \mathbb{N}$ there exists

$j \in \{i+1, i+2\}$ such that $S_i \curvearrowright_{\mathrm{L}} S_j$. The result will then be a consequence of Lemma 1.

Let $i \in \mathbb{N}$. Note that, by assumption, we have $S_i \curvearrowright_{\mathrm{P}} S_{i+1} \curvearrowright_{\mathrm{P}} S_{i+2}$. We distinguish three cases.

If $S_i \curvearrowright_{\mathrm{P}} S_{i+1}$ holds by virtue of condition (8) of Definition 13, then we have $\mu\big(\bigoplus S_i\big) \succ \mu\big(\bigoplus S_{i+1}\big)$, which implies $S_i \curvearrowright_{\mathrm{L}} S_{i+1}$. Similarly, if $S_i \curvearrowright_{\mathrm{P}} S_{i+1}$ holds by virtue of condition (10) of Definition 13, then we have $\mu\big(\bigoplus S_i\big) = \mu\big(\bigoplus S_{i+1}\big)$ and $\tilde{\mu}(S_i) \gg \tilde{\mu}(S_{i+1})$, which again implies $S_i \curvearrowright_{\mathrm{L}} S_{i+1}$. Thus, in these two cases we can take $j := i+1$.

Otherwise, $S_i \curvearrowright_{\mathrm{P}} S_{i+1}$ must hold by virtue of condition (9) of Definition 13, so that $\mu\big(\bigoplus S_i\big) = \mu\big(\bigoplus S_{i+1}\big)$ and $\# S_{i+1} = 1$. However, $S_{i+1} \curvearrowright_{\mathrm{P}} S_{i+2}$ also holds and, by the above condition on the cardinality of $S_{i+1}$, this may only happen by virtue of condition (8) of Definition 13, so that $\mu\big(\bigoplus S_{i+1}\big) \succ \mu\big(\bigoplus S_{i+2}\big)$. Thus, $\mu\big(\bigoplus S_i\big) = \mu\big(\bigoplus S_{i+1}\big) \succ \mu\big(\bigoplus S_{i+2}\big)$ and, by taking $j := i+2$, we obtain $S_i \curvearrowright_{\mathrm{L}} S_j$. □

**Proof (of Theorem 3 on page 14).** Let $S_1, S_2 \in \wp_{\mathrm{fn}}(D, \vdash)$, where $S_1 \Vdash_{\mathrm{P}} S_2$ and let $T := S_1 \,{}_{\mu}\nabla_{\mathrm{P}}\, S_2$. We first prove that condition (1) in Definition 1 holds, i.e., $S_2 \vdash_{\mathrm{P}} T$. Consider each of the three cases in Definition 15 separately. If the first case applies, then $T = S_1 \boxplus_{\mathrm{P}} S_2$ and the result holds because, by hypothesis, '$\boxplus_{\mathrm{P}}$' is an upper bound operator on $\hat{D}_{\mathrm{P}}$. If the second case applies, then $T = (S_1 \boxplus_{\mathrm{P}} S_2) \oplus_{\mathrm{P}} \{d\}$. Since '$\oplus_{\mathrm{P}}$' is the least upper bound operator, the result follows once again by the hypothesis on '$\boxplus_{\mathrm{P}}$'. If the third and last case applies, then $T = \big\{\bigoplus S_2\big\}$, so that the result holds trivially by definition of '$\vdash_{\mathrm{P}}$'.

We now prove that condition (2) in Definition 1 holds. By Proposition 3, '$\curvearrowright_{\mathrm{P}}$' satisfies the ascending chain condition; hence, to complete the proof it is sufficient to show that $S_1 \curvearrowright_{\mathrm{P}} T$.

Consider each of the three cases in Definition 15. If the first case is applied, then the applicability conditions trivially ensure that $S_1 \curvearrowright_{\mathrm{P}} T$.

Suppose now the second case is applied, so that $T = (S_1 \boxplus_{\mathrm{P}} S_2) \oplus_{\mathrm{P}} \{d\}$, where

$$\begin{aligned} d &:= d_1 \ominus d_2; \\ d_1 &:= \bigoplus S_1 \nabla \bigoplus (S_1 \boxplus_{\mathrm{P}} S_2); \\ d_2 &:= \bigoplus (S_1 \boxplus_{\mathrm{P}} S_2). \end{aligned}$$

Note that the applicability condition $\bigoplus S_1 \Vdash \bigoplus (S_1 \boxplus_{\mathrm{P}} S_2)$ for this case ensures that the required base-level widening application in the computation of the abstract element $d_1 \in D$ is well defined. Moreover, since '$\nabla$' is an upper bound operator on $\hat{D}$, we have $d_2 \vdash d_1$, so that also the subtraction application in the computation of the abstract element $d \in D$ is well defined. By Definition 14, we

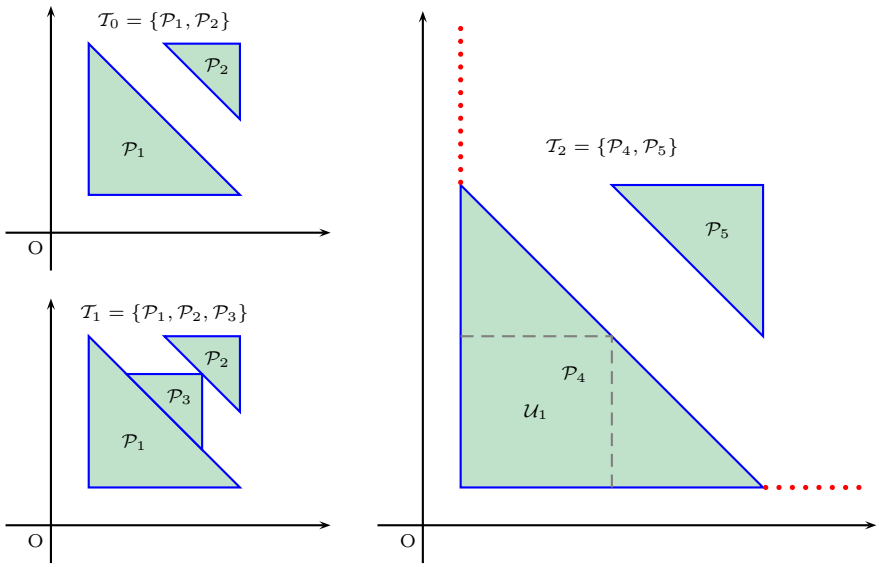


**Fig. 2.** The condition $\#\mathcal{U}_1 > 1$ is needed to obtain a proper widening.

know that $d_1 = (d_1 \ominus d_2) \oplus d_2$. As a consequence, we obtain

$$\begin{aligned}
\bigoplus T &= \bigoplus\big((S_1 \boxplus_{\mathrm{P}} S_2) \oplus_{\mathrm{P}} \{d\}\big) \\
&= d \oplus \big(\bigoplus(S_1 \boxplus_{\mathrm{P}} S_2)\big) \\
&= d \oplus d_2 \\
&= (d_1 \ominus d_2) \oplus d_2 \\
&= d_1 \\
&= \bigoplus S_1 \nabla \bigoplus(S_1 \boxplus_{\mathrm{P}} S_2).
\end{aligned}$$

Since '$\mu$' is a certificate for the base-level widening '$\nabla$', we obtain

$$\mu\big(\bigoplus S_1\big) \succ \mu\big(\bigoplus S_1 \nabla \bigoplus(S_1 \boxplus_{\mathrm{P}} S_2)\big) = \mu\big(\bigoplus T\big),$$

so that by condition (8) of Definition 13, $S_1 \curvearrowright_{\mathrm{P}} T$.

Finally, if the last case is applied, then $T = \big\{\bigoplus S_2\big\}$ so that $\bigoplus T = \bigoplus S_2$. By hypothesis, since '$\boxplus_{\mathrm{P}}$' is an upper bound operator, we have $S_1 \Vdash_{\mathrm{P}} S_2 \vdash_{\mathrm{P}} S_1 \boxplus_{\mathrm{P}} S_2$, so that we obtain $\bigoplus S_1 \vdash \bigoplus S_2 \vdash \bigoplus(S_1 \boxplus_{\mathrm{P}} S_2)$. Since the condition for the second case of Definition 15 does not hold, we have $\bigoplus S_1 = \bigoplus(S_1 \boxplus_{\mathrm{P}} S_2)$, which implies $\bigoplus S_1 = \bigoplus S_2 = \bigoplus T$ and $\mu\big(\bigoplus S_1\big) = \mu\big(\bigoplus T\big)$. Also note that $\# T = 1$ and, since $S_1 \Vdash_{\mathrm{P}} S_2 \vdash_{\mathrm{P}} T$, it must be $\# S_1 > 1$. Therefore condition (9) of Definition 13 is satisfied and $S_1 \curvearrowright_{\mathrm{P}} T$. □

It should be noted that case (9) of Definition 13 has been introduced so as to ensure that $S_1 \curvearrowright_{\mathrm{P}} \big\{\bigoplus S_2\big\}$ holds in the last case of the specification of '${}_{\mu}\nabla_{\mathrm{P}}$', therefore inducing a strict decrease in the corresponding level mapping. This

made also necessary the addition of the extra conditions on the cardinalities of $S_1$ and $S_2$ in case (10) of Definition 13, since otherwise we would have obtained a relation violating the ascending chain condition, as illustrated by the following example.

*Example 10.* Consider the finite powerset domain $(\widehat{\mathbb{CP}}_2)_{\mathrm{P}}$, with the standard widening '$\nabla_s$' on the base-level domain $\mathbb{CP}_2$, certified by the level mapping '$\mu_s$' defined in Example 5 and the upper bound '$\boxplus_{\mathrm{P}}$' defined as '$\oplus_{\mathrm{P}}$', so that we will always have $S_1 \boxplus_{\mathrm{P}} S_2 = S_2$. Consider an iteration sequence $\mathcal{T}_0 \subseteq_{\mathrm{P}} \mathcal{T}_1 \subseteq_{\mathrm{P}} \cdots$ starting with the sets of polyhedra illustrated in Figure 2, where $\mathcal{T}_0 = \{\mathcal{P}_1, \mathcal{P}_2\}$ is shown in the top left diagram and $\mathcal{T}_1 = \mathcal{T}_0 \uplus_{\mathrm{P}} \{\mathcal{P}_3\}$ is shown in the bottom left diagram. For the widened sequence, $\mathcal{U}_0 := \mathcal{T}_0$ and, since $\mathcal{U}_0 \subseteq_{\mathrm{P}} \mathcal{T}_1$, we have to compute $\mathcal{U}_1 := \mathcal{U}_0 \,{}_{\mu}\nabla_{\mathrm{P}}\, \mathcal{T}_1 = \mathcal{T}_0 \,{}_{\mu}\nabla_{\mathrm{P}}\, \mathcal{T}_1$. As $\biguplus \mathcal{T}_0 = \biguplus \mathcal{T}_1$, $\# \mathcal{T}_1 > 1$ and[5]

$$\tilde{\mu}_s(\mathcal{T}_0) = \{(0,3)^2\} \not\gg \{(0,3)^3\} = \tilde{\mu}_s(\mathcal{T}_1),$$

the last case applies in Definition 15 so that $\mathcal{U}_1 = \{\biguplus \mathcal{T}_1\}$, as is indicated in the lower square in the right-hand diagram of Figure 2. Now let $\mathcal{T}_2 = \{\mathcal{P}_4, \mathcal{P}_5\}$ consist of the two triangles bounded by solid lines in the right-hand diagram. Note that $\mathcal{U}_1 \subseteq_{\mathrm{P}} \mathcal{T}_2$, so that we have to compute the widened iterate $\mathcal{U}_2 := \mathcal{U}_1 \,{}_{\mu}\nabla_{\mathrm{P}}\, \mathcal{T}_2$. Since

$$\mu_s\big(\biguplus \mathcal{U}_1\big) = (0,4) = \mu_s\big(\biguplus \mathcal{T}_2\big)$$

but

$$\tilde{\mu}_s(\mathcal{U}_1) = \{(0,4)^1\} \gg \{(0,3)^2\} = \tilde{\mu}_s(\mathcal{T}_2),$$

without the extra condition $\# \mathcal{U}_1 > 1$ in case (10) of Definition 13, we would have $\mathcal{U}_1 \curvearrowright_{\mathrm{P}} \mathcal{T}_2$. Thus, we would apply the first case in the definition of '$\,{}_{\mu}\nabla_{\mathrm{P}}$', obtaining $\mathcal{U}_2 = \mathcal{T}_2$. However, it is easy to note that $\mathcal{U}_2 = \mathcal{T}_2$ has the same structure of $\mathcal{U}_0 = \mathcal{T}_0$ (the former can be obtained from the latter by a suitable affine image transformation) so that the sequence $\mathcal{T}_i$ and the corresponding "widened" sequence $\mathcal{U}_i$ can be extended indefinitely without obtaining convergence (in a finite number of steps). In contrast, since we require the condition $\# \mathcal{U}_1 > 1$, the second case of Definition 15 applies and $\mathcal{U}_1 \,{}_{\mu}\nabla_{\mathrm{P}}\, \mathcal{T}_2$ is the (unbounded) polyhedron indicated by the dotted lines in the right-hand diagram.

**Proof (of Proposition 4 on page 16).** The finite powerset domain $(\widehat{\mathbb{CP}}_n)_{\mathrm{P}}$ is related to the concrete domain $\hat{\mathsf{A}}_n$ defined in Section 2.2 by the concretization function $\gamma^{\mathsf{A}}_{\mathrm{P}}$ induced from $\gamma^{\mathsf{A}}$, where $\gamma^{\mathsf{A}}(\mathcal{P}) = \mathcal{P}$ for each $\mathcal{P} \in \mathbb{CP}_n$. Namely, for each $\mathcal{S} \in \wp_{\mathrm{fn}}(\mathbb{CP}_n, \subseteq)$, we have $\gamma^{\mathsf{A}}_{\mathrm{P}}(\mathcal{S}) = \bigcup \mathcal{S}$. Therefore, we have to show that, for all $\mathcal{S}_1, \mathcal{S}_2 \in \wp_{\mathrm{fn}}(\mathbb{CP}_n, \subseteq)$, $\mathcal{S}_1 \bowtie \mathcal{S}_2$ if and only if $\bigcup \mathcal{S}_1 = \bigcup \mathcal{S}_2$.

First we assume that $\bigcup \mathcal{S}_1 \subseteq \bigcup \mathcal{S}_2$ and show that $\mathcal{S}_1 \triangleleft \mathcal{S}_2$. Consider an arbitrary element $\mathcal{S}'_1 \in \wp_{\mathrm{fn}}(\mathbb{CP}_n, \subseteq)$ such that $\mathcal{S}'_1 \vdash_{\mathrm{P}} \mathcal{S}_1$. Let

$$\mathcal{S}''_1 = \Omega^{\subseteq}_{\mathbb{CP}_n}\big(\{\, \mathcal{P}'_1 \cap \mathcal{P}_2 \in \mathbb{CP}_n \mid \mathcal{P}'_1 \in \mathcal{S}'_1, \mathcal{P}_2 \in \mathcal{S}_2 \,\}\big)$$

[5] In this example a multiset is denoted as a set where each element carries in a superscript the corresponding number of occurrences. For instance, we write $M = \{a^3, b^2\}$ to mean that element $a$ and $b$ occur (in multiset $M$) 3 and 2 times, respectively.

so that $\bigcup \mathcal{S}_1'' = \bigcup \mathcal{S}_1' \cap \bigcup \mathcal{S}_2$. By definition, $\mathcal{S}_1' \vdash_{\text{P}} \mathcal{S}_1$ implies $\bigcup \mathcal{S}_1' \subseteq \bigcup \mathcal{S}_1$; also, by hypothesis, $\bigcup \mathcal{S}_1 \subseteq \bigcup \mathcal{S}_2$, so that $\bigcup \mathcal{S}_1' \subseteq \bigcup \mathcal{S}_2$. Therefore $\bigcup \mathcal{S}_1'' = \bigcup \mathcal{S}_1'$ and $\bigcup \mathcal{S}_1'' \subseteq \bigcup \mathcal{S}_2$. Thus, by Definition 16, $\mathcal{S}_1 \lhd \mathcal{S}_2$. By a symmetric argument, we can prove that $\bigcup \mathcal{S}_2 \subseteq \bigcup \mathcal{S}_1$ implies $\mathcal{S}_2 \lhd \mathcal{S}_1$. Thus, again by Definition 16, we obtain that $\mathcal{S}_1 \equiv_{\gamma_{\text{P}}^{\text{A}}} \mathcal{S}_2$ implies $\mathcal{S}_1 \bowtie \mathcal{S}_2$.

Second we assume that $\bigcup \mathcal{S}_1 \nsubseteq \bigcup \mathcal{S}_2$ and show that $\mathcal{S}_1 \not\lhd \mathcal{S}_2$. By assumption, there exist a point $\boldsymbol{p} \in \mathbb{R}^n$ such that $\boldsymbol{p} \in \big(\bigcup \mathcal{S}_1\big) \setminus \big(\bigcup \mathcal{S}_2\big)$. As a consequence, there must exist a polyhedron $\mathcal{P}_1 \in \mathcal{S}_1$ such that $\boldsymbol{p} \in \mathcal{P}_1$. Consider now the polyhedron $\mathcal{P}_1' := \{\boldsymbol{p}\}$ and the corresponding singleton $\mathcal{S}_1' = \{\mathcal{P}_1'\}$. Note that $\mathcal{S}_1' \vdash_{\text{P}} \mathcal{S}_1$. Moreover, if $\mathcal{S}_1'' \in \wp_{\text{fn}}(\mathbb{CP}_n, \subseteq)$ is such that $\biguplus \mathcal{S}_1'' = \biguplus \mathcal{S}_1'$, then we must have $\mathcal{S}_1'' = \mathcal{S}_1'$. However, since $\boldsymbol{p} \notin \bigcup \mathcal{S}_2$, we also have $\bigcup \mathcal{S}_1'' \nsubseteq \bigcup \mathcal{S}_2$, which implies $\mathcal{S}_1'' \nvdash_{\text{P}} \mathcal{S}_2$. Hence, by Definition 16, $\mathcal{S}_1 \not\lhd \mathcal{S}_2$. By a symmetric argument, we can prove that $\bigcup \mathcal{S}_2 \nsubseteq \bigcup \mathcal{S}_1$ implies $\mathcal{S}_2 \not\lhd \mathcal{S}_1$. Thus, reasoning by contraposition, we obtain that $\mathcal{S}_1 \bowtie \mathcal{S}_2$ implies $\mathcal{S}_1 \equiv_{\gamma_{\text{P}}^{\text{A}}} \mathcal{S}_2$. □

To prove Proposition 5 on page 17, it is convenient to consider *non-redundant merges*, where each of the elements in the original abstract collection participates to just one join operation.

**Definition 19.** *Let $R$ be a congruence relation on $\hat{D}_{\text{P}}$. Let $S_1, S_2 \in \wp_{\text{fn}}(D, \vdash)$, where $S_2 = \{d_1, \ldots, d_m\}$ and $\{S_{1i}\}_{i=1}^m$ is a partition of $S_1$ such that, for each $1 \leq i \leq m$, $\text{merge}_R\big(S_{1i}, \{d_i\}\big)$ holds. Then we write $\text{merge_n}_R(S_1, S_2)$ and say that $S_2$ is a* non-redundant merge *of $S_1$.*

**Lemma 2.** *Let $R$ be a congruence relation on $\hat{D}_{\text{P}}$ that refines the $\oplus$-congruence relation. If $S_1, S_2 \in \wp_{\text{fn}}(D, \vdash)$ where $S_1 \neq S_2$ and $\text{merge}_R(S_1, S_2)$, then there exists $S_2' \neq S_1 \in \wp_{\text{fn}}(D, \vdash)$ such that $\text{merge_n}_R(S_1, S_2')$ and $\# S_2' < \# S_1$.*

*Proof.* By hypothesis, $\text{merge}_R(S_1, S_2)$ and $S_1 \neq S_2$. Thus, by Definition 17, there exists $S_1' \subseteq S_1$ where $S_1'\ R\ \{d_2\}$ and $\{d_2\} \neq S_1'$. Since $R$ refines the $\oplus$-congruence relation, we obtain $d_2 = \bigoplus S_1'$. Thus $\# S_1' > 1$. Let $S_2' = (S_1 \setminus S_1') \oplus_{\text{P}} \{d_2\}$. Then $S_2' \neq S_1$, $\# S_2' < \# S_1$ and, by Definition 17, $\text{merge}_R(S_1, S_2')$. If $S_1 \setminus S_1' \neq \varnothing$, then $\{S_1 \setminus S_1', S_1'\}$ is a partition of $S_1$; otherwise, $\{S_1'\}$ is such a partition. In both cases, by Definition 19, $\text{merge_n}_R(S_1, S_2')$. □

**Proof (of Proposition 5 on page 17).** We first prove, by induction on $\# S$, that there exists $S' \in \wp_{\text{fn}}(D, \vdash)$ such that $\text{merge}_R(S, S')$, $S'$ is fully-merged and, if $S' \neq S$, then $\# S' < \# S$. As '$\text{merge}_R$' is reflexive, the result holds trivially if $S$ is fully-merged. Suppose therefore that $S$ is not fully-merged (so that $\# S > 1$). Then there exists $S'' \in \wp_{\text{fn}}(D, \vdash) \setminus \{S\}$ such that $\text{merge}_R(S, S'')$. By Lemma 2, we can assume that $S''$ is chosen so that $\text{merge_n}_R(S, S'')$ and $\# S'' < \# S$. Therefore we can apply the inductive hypothesis to $S''$; there exists $S' \in \wp_{\text{fn}}(D, \vdash)$ which is fully-merged, $\text{merge}_R(S'', S')$ and $\# S' \leq \# S''$. As '$\text{merge}_R$' is transitive, we obtain $\text{merge}_R(S, S')$ and $\# S < \# S'$.

The merger '$\uparrow_R$' can thus be defined, for each $S \in \wp_{\text{fn}}(D, \vdash)$, as $\uparrow_R S = S$, when $S$ is already fully-merged, and $\uparrow_R S = S'$ as defined above, otherwise. The proof for a pairwise-merger is similar. □

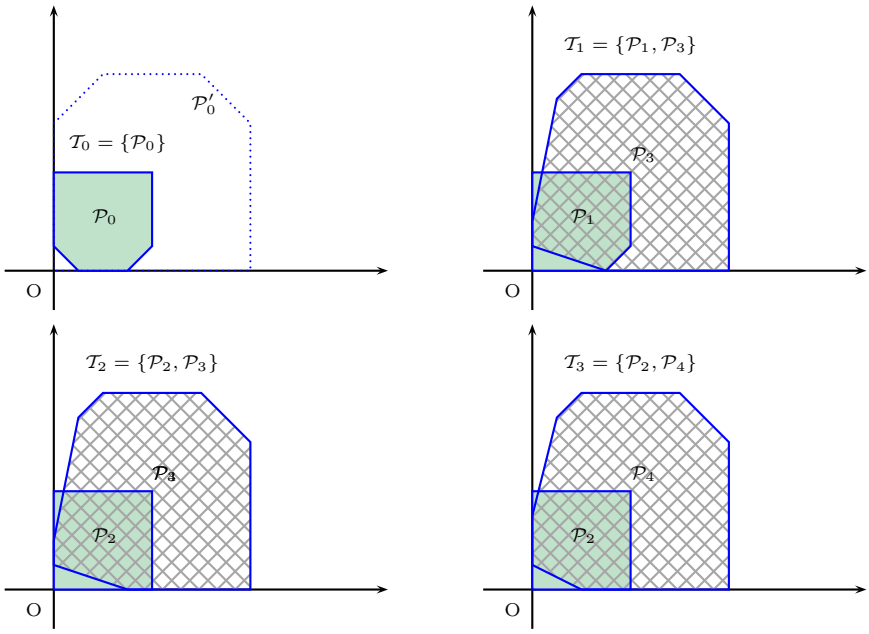


**Fig. 3.** Sequence of sets of polyhedra in Example 11.

The following example shows that, in general, it is not possible to obtain a proper widening operator on the finite powerset domain by coupling an arbitrary (i.e., not $\nabla$-covered) extrapolation heuristics '$h^{\nabla}_{\mathrm{P}}$' with a fixed upper bound for the cardinality of abstract descriptions. It is also shown that even the addition of a merger operator for abstract descriptions, as proposed in [8], is not enough for that purpose.

*Example 11.* Consider the finite powerset domain $(\widehat{\mathbb{CP}}_2)_{\mathrm{P}}$, with '$\nabla_s$' as the widening on the base-level abstract domain $\widehat{\mathbb{CP}}_2$, '$h^{\nabla}_{\mathrm{P}}$' be the extrapolation heuristics for '$\nabla_s$' defined in Proposition 1 (which is also the one used in [8]) and '$\uparrow_{\bowtie}$' be the pairwise-merging operator defined in [8]. Let $\mathcal{P}_0, \mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{P}_4 \in \mathbb{CP}_2$ be defined as

$$\mathcal{P}_0 = \{0 \le x \le 4, 0 \le y \le 4, x - y \le 3, x + y \ge 1\},$$
$$\mathcal{P}_1 = \{0 \le x \le 4, 0 \le y \le 4, x - y \le 3\},$$
$$\mathcal{P}_2 = \{0 \le x \le 4, 0 \le y \le 4\},$$
$$\mathcal{P}_3 = \{0 \le x \le 8, 0 \le y \le 8, x + y \le 14, x - y \ge -6, 5x - y \ge -2, x + 3y \ge 3\},$$
$$\mathcal{P}_4 = \{0 \le x \le 8, 0 \le y \le 8, x + y \le 14, x - y \ge -6, 4x - y \ge -3, x + 2y \ge 2\}.$$

Note that $\mathcal{P}_1 = \mathcal{P}_0 \nabla_s \mathcal{P}_1$ and $\mathcal{P}_2 = \mathcal{P}_1 \nabla_s \mathcal{P}_2$; moreover, for all $i \in \{0, 1, 2\}$, we have $\mathcal{P}_i \not\subseteq \mathcal{P}_3$ and $\mathcal{P}_i \not\subseteq \mathcal{P}_4$.

Consider an increasing sequence $\mathcal{T}_0 \vdash_{\mathrm{P}} \mathcal{T}_1 \vdash_{\mathrm{P}} \mathcal{T}_2 \vdash_{\mathrm{P}} \mathcal{T}_3 \vdash_{\mathrm{P}} \ldots$ starting with elements $\mathcal{T}_0 = \{\mathcal{P}_0\}$, $\mathcal{T}_1 = \{\mathcal{P}_1, \mathcal{P}_3\}$, $\mathcal{T}_2 = \{\mathcal{P}_2, \mathcal{P}_3\}$, and $\mathcal{T}_3 = \{\mathcal{P}_2, \mathcal{P}_4\}$. Then, the

corresponding widened sequence $\mathcal{U}_0 \vdash_{\text{P}} \mathcal{U}_1 \vdash_{\text{P}} \mathcal{U}_2 \vdash_{\text{P}} \mathcal{U}_3 \vdash_{\text{P}} \ldots$, will be computed as follows. Since $\mathcal{U}_0 = \mathcal{T}_0$, in the first iteration (noting that $\mathcal{T}_1$ is fully-merged) we compute

$$\begin{aligned}\mathcal{U}_1 &= h^{\nabla}_{\text{P}}(\mathcal{U}_0, \mathcal{T}_1)\\ &= \{\mathcal{P}_3\} \uplus_{\text{P}} \{\mathcal{P}_0 \nabla_s \mathcal{P}_1\}\\ &= \{\mathcal{P}_1, \mathcal{P}_3\}\\ &= \mathcal{T}_1.\end{aligned}$$

In the second iteration, noting that also $\mathcal{T}_2$ is fully-merged, we obtain

$$\begin{aligned}\mathcal{U}_2 &= h^{\nabla}_{\text{P}}(\mathcal{U}_1, \mathcal{T}_2)\\ &= \{\mathcal{P}_3\} \uplus_{\text{P}} \{\mathcal{P}_1 \nabla_s \mathcal{P}_2\}\\ &= \{\mathcal{P}_2, \mathcal{P}_3\}\\ &= \mathcal{T}_2.\end{aligned}$$

In the third iteration, since also $\mathcal{T}_3$ is fully-merged, letting

$$\mathcal{P}'_0 := \mathcal{P}_3 \nabla_s \mathcal{P}_4 = \{0 \leq x \leq 8, 0 \leq y \leq 8, x + y \leq 14, x - y \geq -6\},$$

we obtain

$$\begin{aligned}\mathcal{U}_3 &= h^{\nabla}_{\text{P}}(\mathcal{U}_2, \mathcal{T}_3)\\ &= \{\mathcal{P}_2\} \uplus_{\text{P}} \{\mathcal{P}_3 \nabla_s \mathcal{P}_4\}\\ &= \{\mathcal{P}_3 \nabla_s \mathcal{P}_4\}\\ &= \{\mathcal{P}'_0\}.\end{aligned}$$

Note that the polyhedron $\mathcal{P}_2$ does not occur in $\mathcal{U}_3$ because it is made redundant by the polyhedron $\mathcal{P}'_0$ (i.e., $\mathcal{P}_2 \subseteq \mathcal{P}'_0$).

Now, the singleton $\mathcal{U}_3 = \{\mathcal{P}'_0\}$ has the same structure as the singleton $\mathcal{U}_0 = \{\mathcal{P}_0\}$, because the polyhedron $\mathcal{P}'_0$ can be obtained from $\mathcal{P}_0$ by a scaling (by a factor 2) followed by a rotation. As a consequence, it is possible to indefinitely extend the sequence $\mathcal{T}_i$ and the corresponding "widened" sequence $\mathcal{U}_i$ without obtaining convergence (in a finite number of steps). Since in the above computation all the abstract elements have cardinality less than or equal to 2, the addition of any (non-trivial) upper bound on the cardinality of the abstract descriptions will have no effect on termination.

Suppose now that, instead of just using the extrapolation heuristics '$h^{\nabla}_{\text{P}}$', we adopt the widening '${}_{\text{EM}}\nabla_{\text{P}}$' with the trivial connector:

$$S_1 \boxplus_{\text{EM}} S_2 := \big\{\bigoplus(S_1 \cup S_2)\big\}.$$

Let $\mathcal{U}'_0 \vdash_{\text{P}} \mathcal{U}'_1 \vdash_{\text{P}} \mathcal{U}'_2 \vdash_{\text{P}} \mathcal{U}'_3 \vdash_{\text{P}} \ldots$, be the corresponding widened sequence. Then instead of obtaining $\mathcal{U}_1 = \{\mathcal{T}_1\}$ we obtain $\mathcal{U}'_1 = \big\{\{x \geq 0, y \geq 0\}\big\}$. Further iterations leave this set unchanged.

Suppose now that, instead of using the extrapolation heuristics '$h^{\nabla}_{\mathrm{P}}$' defined in Proposition 1, we adopt one that is $\nabla$-covered, such as that defined in Proposition 2, and hence use a cardinality-based widening '${}_{k}\nabla_{\mathrm{P}}$' for any $k > 2$. Then we obtain the widened sequence $\mathcal{U}''_0 \vdash_{\mathrm{P}} \mathcal{U}''_1 \vdash_{\mathrm{P}} \mathcal{U}''_2 \vdash_{\mathrm{P}} \ldots$, where $\mathcal{U}''_0 = \mathcal{U}_0$, $\mathcal{U}''_1 = \mathcal{U}_1$ and $\mathcal{U}''_2 = \mathcal{U}_2$ would be computed as before. However in the third iteration we will obtain

$$\begin{aligned}
\mathcal{U}''_3 &= h^{\nabla}_{\mathrm{P}}(\mathcal{U}_2, \mathcal{T}_3) \\
&= \Omega^{\nabla}_{D}\big(\{\mathcal{P}_2, \mathcal{P}_3, \mathcal{P}_4\}\big) \\
&= \Omega^{\nabla}_{D}\big(\{\mathcal{P}_2, \mathcal{P}_3 \nabla_s \mathcal{P}_4\}\big) \\
&= \Omega^{\nabla}_{D}\big(\{\mathcal{P}_2, \mathcal{P}'_0\}\big) \\
&= \{\mathcal{P}_2 \nabla_s \mathcal{P}'_o\} \\
&= \big\{\{x \geq 0, y \geq 0\}\big\},
\end{aligned}$$

which is the same as the set $\mathcal{U}'_1$ computed using '${}_{\mathrm{EM}}\nabla_{\mathrm{P}}$'.