On constructivity of galois connections

On Constructivity of Galois Connections

Francesco Ranzato

Dipartimento di Matematica, University of Padova, Italy

Abstract. Abstract interpretation-based static analyses rely on abstract domains of program properties, such as intervals or congruences for integer variables. Galois connections (GCs) between posets provide the most widespread and useful formal tool for mathematically specifying abstract domains. Darais and Van Horn [2016] put forward a notion of constructive Galois connection for unordered sets (rather than posets), which allows to define abstract domains in a so-called mechanized and calculational proof style and therefore enables the use of proof assistants like Coq and Agda for automatically extracting certified algorithms of static analysis. We show here that constructive GCs are isomorphic, in a mathematical meaning which includes sound abstract functions, to so-called partitioning GCs — an already known class of GCs which allows to cast standard set partitions as an abstract domain. Darais and Van Horn [2016] further provide a notion of constructive Galois connection for posets, which we prove to be mathematically isomorphic to plain GCs. Drawing on these findings, we put forward purely partitioning GCs, a novel class of constructive abstract domains for a mechanized approach to abstract interpretation. We show that this class of abstract domains allows us to represent a set partition in a flexible way while retaining a constructive approach to Galois connections.

1 Introduction

Abstract interpretation [4,5] is probably the most used and successful technique for defining approximations of program semantics (or, more in general, of computing systems) to be used for designing provably sound static program analyzers. Abstract domains play a crucial role in any abstract interpretation, since they encode, both logically for reasoning purposes and practically for implementations, which program properties are computed by a static analysis. Since its beginning [4], one major insight of abstract interpretation is given by the use of Galois connections (GCs) for defining abstract domains. A specification of an abstract domain D through a Galois connection prescribes that: (1) both concrete and abstract domains, C and D, are partially ordered, and typically they give rise to complete lattices; (2) concrete and abstract domains are related by a pair of so-called abstraction $\alpha : C \to D$ and concretization $\gamma : D \to C$ maps; (3) α and γ give rise to an adjunction relation: $\alpha(c) \leq_D d \Leftrightarrow c \leq_C \gamma(d)$. GCs carry both advantages and drawbacks. One major benefit of GCs is the so-called calculational style for defining abstract operations [2,17]. If $f : C \to C$ is any concrete operation involved by some semantic definition (e.g., integer addition or multiplication) then a corresponding correct approximation on A is defined by $\alpha \circ f \circ \gamma : A \to A$, which turns out to be the best possible approximation of f on the abstract domain A and, as envisioned by Cousot [2], allows to systematically derive abstract operations

in a correct-by-design manner. On the negative side, GCs have two main weaknesses. First, GCs formalize an ideal situation where each concrete property in C has a unique best abstract approximation in D. Some very useful and largely used abstract domains cannot be defined by a GC, convex polyhedra being a prominent example of abstract domain where no abstraction map can be defined [9]. This problem motivated weaker abstract interpretation frameworks which only need concretization maps [6]. Secondly, it turns out that abstraction maps of GCs cannot be mechanized [18,20], meaning that one cannot use automatic formal proof systems like Coq in order to extract certified algorithms of abstract interpretation, e.g., based on best correct approximations $\alpha \circ f \circ \gamma$, since the existence of an abstraction map would require a non-constructive axiom (see [20, Section 3.3.2]). In other terms, the calculational approach of abstract interpretation cannot be automatized. Notably, Verasco [15,16] (and its precursor described in [1]) is a static analyzer for C which has been formally designed and verified using the Coq proof assistant, and is based on abstract interpretation using concretization maps only. This latter motivation was one starting point of Darais and Van Horn [10] for investigating constructive versions of Galois connections, together with the observation that many useful abstract domains, even if defined by an abstraction map, still would permit a mechanization of their soundness proofs. Also, Darais and Van Horn's approach [10] generalizes 'Galculator' [24], which is a proof assistant based on a given algebra of Galois connections.

Constructive Galois connections (acronym CGCs) [10] stem from the observation that for many commonly used abstract domains[1]: (1) the concrete domain is a powerset (also called collecting) domain $\wp(A)$ of an unordered carrier domain A; (2) the abstraction map α on the powerset $\wp(A)$ is defined as a lifting to the powerset of a basic abstraction function η, called extraction, which is defined just on the carrier domain A and takes values belonging to an unordered abstract domain B, that is, $\eta : A \to B$; (3) the concretization (or interpretation) map $\mu : B \to \wp(A)$ provides a meaning in $\wp(A)$ to basic abstract values ranging in B; (4) the standard α/γ adjunction relation of GCs can be equivalently reformulated in terms of the following correspondence between η and μ: for all $a \in A$ and $b \in B$,

$$a \in \mu(b) \Leftrightarrow \eta(a) = b \qquad \text{(CGC-Corr)}$$

The intuition is similar to GCs: b approximates a set containing a iff b is the abstraction of a. Moreover, CGCs allow to give a soundness condition for pairs of concrete and abstract functions which are defined on the carrier concrete and abstract domains A and B. As a simple example taken from [10, Section 2], the standard parity (toy) abstraction for integer variables can be defined as a CGC as follows. The carrier concrete domain is $\mathbb{Z}$, the unordered parity domain is $\mathbb{P} = \{\textit{even}, \textit{odd}\}$, while abstraction $\mathrm{parity} : \mathbb{Z} \to \mathbb{P}$ and concretization $\mu : \mathbb{P} \to \wp(\mathbb{Z})$ mappings are straightforwardly defined and satisfy (CGC-Corr): $z \in \mu(a) \Leftrightarrow \mathrm{parity}(z) = a$. Also, from a successor concrete operation $\mathrm{succ} : \mathbb{Z} \to \mathbb{Z}$ one can constructively derive a sound abstract successor $\mathrm{succ}_\sharp : \mathbb{P} \to \mathbb{P}$ such that $\mathrm{succ}_\sharp(\textit{even}) = \textit{odd}$ and $\mathrm{succ}_\sharp(\textit{odd}) = \textit{even}$.

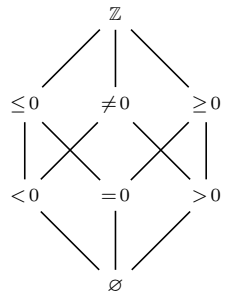
Darais and Van Horn [10] further provide a notion of constructive Galois connection for posets (acronym CGP), where the carrier concrete domain A and the abstract domain

[1] We follow the notation used in [10].

B are posets (rather than unordered sets), and where the above condition (CGC-Corr) is replaced by:

$$a \in \mu(b) \Leftrightarrow \eta(a) \leq_B b \qquad \text{(CGP-Corr)}$$

This enables a constructive definition for ordered abstract domains like the following abstract lattice Sign:



whose partial order relation $\leq_{\mathrm{Sign}}$ encodes an approximation relation between its abstract values and where $\eta : \mathbb{Z} \to \mathrm{Sign}$ and $\mu : \mathrm{Sign} \to \wp(\mathbb{Z})$. Here, $\eta(a)$ provides the sign of $a \in \mathbb{Z}$ in the subset $\{<0, =0, >0\} \subseteq \mathrm{Sign}$, so that $\eta(a) = b$ of (CGC-Corr) is weakened to $\eta(a) \leq_{\mathrm{Sign}} b$.

Contributions. Our initial observation was that CGCs always encode a partition of the concrete carrier set A. As a simple example, for the above parity domain $\mathbb{P}$, the induced partition of the carrier concrete domain $\mathbb{Z}$ obviously consists of two blocks: $\{z \in \mathbb{Z} \mid z \text{ even}\}$ and $\{z \in \mathbb{Z} \mid z \text{ odd}\}$. Conversely, if an abstract domain D of a powerset domain $\wp(A)$ is defined through a standard Galois connection $\mathcal{G}$ and D does not induce an underlying partition of the carrier set A then we observed that the GC $\mathcal{G}$ cannot be equivalently formulated by a CGC. Abstract domains which encode a partition of a given carrier set have been previously studied and formalized as so-called partitioning Galois connections (PGCs) or elementwise set abstractions [3,7,8]. Intuitively, a Galois connection defining a domain D which abstracts a concrete powerset domain $\wp(A)$ is called partitioning [7,22] when D represents a partition $\mathcal{P}$ of the set A, namely when there exists a partition $\mathcal{P}$ of A such that any $\gamma(d) \in \wp(A)$ is a union of blocks of $\mathcal{P}$. For example, the GC defining the abstract domain Sign above is partitioning, where the induced partition of $\mathbb{Z}$ consists of the blocks $\{z \in \mathbb{Z} \mid z < 0\}$, $\{0\}$ and $\{z \in \mathbb{Z} \mid z > 0\}$.

Our first contribution shows that CGCs are isomorphic to PGCs in the following precise meaning. We define two invertible transforms $\mathbb{T}_{\mathrm{PGC}}$ and $\mathbb{T}_{\mathrm{CGC}}$ such that: (1) $\mathbb{T}_{\mathrm{PGC}}$ transforms any CGC into a PGC; (2) $\mathbb{T}_{\mathrm{CGC}}$ transforms any PGC into a CGC; (3) the transforms are one the inverse of the other, i.e., $\mathbb{T}_{\mathrm{CGC}} \circ \mathbb{T}_{\mathrm{PGC}} = \mathrm{id} = \mathbb{T}_{\mathrm{PGC}} \circ \mathbb{T}_{\mathrm{CGC}}$. Moreover, this isomorphism includes the soundness of abstract operations, meaning that we extend the transforms $\mathbb{T}_{\mathrm{PGC}}$ and $\mathbb{T}_{\mathrm{CGC}}$ in order to convert a pair $\langle f, f^\sharp \rangle$ of concrete and sound abstract operations on a CGC $\mathcal{C}$ to a pair of concrete and sound abstract operations $\mathbb{T}_{\mathrm{PGC}}(\langle f, f^\sharp \rangle)$ on the PGC $\mathbb{T}_{\mathrm{PGC}}(\mathcal{C})$, and analogously the other way round from PGCs to CGCs.

Secondly, we studied Darais and Van Horn's CGPs, in order to investigate whether they can be similarly characterized as a suitable subclass of Galois connections. We

show that CGPs are mathematically equivalent to plain GCs of a powerdomain, meaning that here we define two transforms $\mathbb{T}_{\text{GC}}$ and $\mathbb{T}_{\text{CGP}}$ that give rise to an isomorphism between standard Galois connections relating an abstract domain B to a powerdomain $\wp^{\downarrow}(A)$ and CGPs of the ordered abstract domain B into the carrier set A. Therefore, it turns out that CGPs do not identify a proper subclass of Galois connections.

It is worth remarking that the above transforms $\mathbb{T}_{\text{CGC}}$ and $\mathbb{T}_{\text{CGP}}$ are nonconstructive, meaning that the definitions of $\mathbb{T}_{\text{CGC}}(\mathcal{G})$ and $\mathbb{T}_{\text{CGP}}(\mathcal{G})$ rely on the abstraction map which determines their input Galois connection $\mathcal{G}$. Nonetheless, these transforms are still useful since they provide a formal definition to be used for manually designing a constructive abstract domain starting from a partitioning Galois connection or any Galois connection of a concrete powerdomain.

Drawing on these results, our third contribution is the definition of a novel class of constructive Galois connections, called *purely constructive* GCs (PCGCs). The basic idea underlying PCGCs is as follows. CGCs essentially represent a partition $\mathcal{P}$ of the concrete carrier domain A encoded through an abstract domain B. We showed that this encoding of $\mathcal{P}$ can also be viewed as an implicit representation for all the possible unions of blocks in $\mathcal{P}$. Hence, this observation can be naturally generalized by allowing to select which unions of blocks of $\mathcal{P}$ to consider in the abstract domain B. In other terms, B may be defined as a partition $\mathcal{P}$ of A together with an explicit choice of some unions of blocks of $\mathcal{P}$, where this selection may range from none to all (where all boils down to CGCs). As an example, consider a sign abstraction like $\mathrm{Sign}^{\neq} \triangleq \mathrm{Sign} \smallsetminus \{\neq 0\}$, where the abstract value $\neq 0$ is taken out from the above abstract lattice Sign. Then, it turns out that $\mathrm{Sign}^{\neq}$ cannot be formalized as a CGC, although $\mathrm{Sign}^{\neq}$ still represents a partition of $\mathbb{Z}$. In fact, $\mathrm{Sign}^{\neq}$ just lacks a representation for the union of the two blocks $\{z \in \mathbb{Z} \mid z < 0\}$ and $\{z \in \mathbb{Z} \mid z > 0\}$, i.e., it precisely lacks the removed abstract value $\neq 0$ which would represent this union. In our setting, $\mathrm{Sign}^{\neq}$ can be defined as a PCGC. More precisely, a PCGC of a poset abstract domain B into an unordered concrete carrier set A is defined by $\eta : A \to B$ and $\mu : B \to \wp(A)$ which satify the following two conditions:

$$a \in \mu(\eta(a')) \;\Leftrightarrow\; \eta(a) = \eta(a') \qquad \text{(PCGC-Corr}_1\text{)}$$

$$a \in \mu(b) \;\Leftrightarrow\; \eta(a) \leq_B b \qquad \text{(PCGC-Corr}_2\text{)}$$

Therefore, (PCGC-Corr$_2$) exactly coincides with (CGP-Corr), while (PCGC-Corr$_1$) is a weakening of (CGC-Corr) because it amounts to (CGC-Corr) restricted to abstract values ranging in $\eta(A)$. Thus, as an example, we have that $\mathrm{Sign}^{\neq}$ is a CGP because (PCGC-Corr$_2$) clearly holds, i.e. $a \in \mu(b) \Leftrightarrow \eta(a) \leq_{\mathrm{Sign}^{\neq}} b$ holds, while $\mathrm{Sign}^{\neq}$ is not a CGC because, e.g., $2 \in \mu(\geq 0)$ while $\eta(2) \neq \geq 0$ so that the condition (CGC-Corr) does not hold. On the other hand, let us remark that the weakening (PCGC-Corr$_1$) instead does hold, so that $\mathrm{Sign}^{\neq}$ turns out to be a PCGC. Thus, PCGCs still represent a partition $\mathcal{P}$ of the concrete carrier domain as CGCs do, while retaining a constructive approach to abstract interpretation and providing a flexible way of representing unions of blocks in $\mathcal{P}$. Also, PCGCs come together with a definition of sound abstract operations and of the notion of completeness commonly used in abstract interpretation.

2 Background

Notation. Let $f : A \to B$, $g : A \to \wp(B)$ and $h : \wp(A) \to B$, $k : A \to C$, where A and B are sets and C is a complete lattice with lub $\vee$. We then use the following definitions:

powerset (or collecting) lifting:	$f^{\diamond} : \wp(A) \to \wp(B)$	$f^{\diamond}(X) \triangleq \{f(x) \mid x \in X\}$
singleton powerset lifting:	$f^{\triangleright} : A \to \wp(B)$	$f^{\triangleright}(a) \triangleq \{f(b)\}$
domain powerset lifting:	$g^{*} : \wp(A) \to \wp(B)$	$g^{*}(X) \triangleq \cup_{x \in X} g(x)$
singleton lowering:	$h^{\{\}} : A \to B$	$h^{\{\}}(a) \triangleq h(\{a\})$
lub domain powerset lifting:	$k^{\vee} : \wp(A) \to C$	$k^{\vee}(X) \triangleq \vee_{a \in X} k(a)$

Somewhere we use $f(X)$ as an alternative notation for $f^{\diamond}(X)$. If $f, f' : A \to C$ and C is a poset then we write $f \sqsubseteq f'$ when for any $a \in A$, $f(a) \leq_C f'(c)$. If A is a poset and $X \subseteq A$ then $\downarrow X \triangleq \{y \in A \mid \exists x \in X. y \leq x\}$, and, in turn, $\wp^{\downarrow}(A) \triangleq \{X \in \wp(A) \mid X = \downarrow X\}$ denotes the downward powerdomain of A, which is a complete lattice when it is ordered by subset inclusion. We use $\downarrow a$ as a shorthand for $\downarrow\{a\}$. Recall that any set A can be viewed as a poset w.r.t. the so-called discrete partial order $\leq_d$: for all $x, y \in A$, $x \leq_d y$ iff $x = y$. Let us also recall that $\mathcal{P} \subseteq \wp(A)$ is a partition of A when: (1) $B \in \mathcal{P} \Rightarrow B \neq \varnothing$; (2) if $B_1, B_2 \in \mathcal{P}$ and $B_1 \neq B_2$ then $B_1 \cap B_2 = \varnothing$; (3) $\cup_{B \in \mathcal{P}} B = A$.

Galois Connections. Recall that $\mathcal{G} = \langle \alpha, C, D, \gamma \rangle$ is a Galois connection (GC) when C and D are posets, $\alpha : C \to D$, $\gamma : D \to C$ and $\alpha(c) \leq_D d \Leftrightarrow c \leq_C \gamma(d)$. By following a standard terminology in abstract interpretation, C and D are called concrete and abstract domains, while α and γ are called abstraction and concretization maps. $\mathcal{G}$ is a disjunctive GC when γ is additive (intuitively, this means that $\mathcal{G}$ is able to represent concrete logical disjunctions with no loss of precision). $\mathcal{G}$ is a Galois insertion (GI) when α is surjective, or, equivalently, γ is injective.

Let us also recall some standard definitions and terminology of abstract interpretation [4,5]. Let $f : C \to C$ and $f_\sharp : D \to D$ be, respectively, concrete and abstract functions. We then have the following definitions:

$\langle f, f_\sharp \rangle_{\mathcal{G}}$ is sound if:	$\alpha \circ f \circ \gamma \sqsubseteq f_\sharp$ (equivalently: $\alpha \circ f \sqsubseteq f_\sharp \circ \alpha$)
$\langle f, f_\sharp \rangle_{\mathcal{G}}$ is optimal if:	$\alpha \circ f \circ \gamma = f_\sharp$
$\langle f, f_\sharp \rangle_{\mathcal{G}}$ is backward complete if:	$\alpha \circ f = f_\sharp \circ \alpha$
$\langle f, f_\sharp \rangle_{\mathcal{G}}$ is forward complete if:	$f \circ \gamma = \gamma \circ f_\sharp$
$\langle f, f_\sharp \rangle_{\mathcal{G}}$ is precise if:	$f = \gamma \circ f_\sharp \circ \alpha$

The abstract function $f_{\mathcal{G}} \triangleq \alpha \circ f \circ \gamma$ is called the best correct approximation (b.c.a.) of f induced by $\mathcal{G}$.

Let $\mathcal{G}_1 = \langle \alpha_1, C, D_1, \gamma_1 \rangle$ and $\mathcal{G}_2 = \langle \alpha_2, C, D_2, \gamma_2 \rangle$ be two GCs with a common concrete domain C. $\mathcal{G}_1$ is more precise than $\mathcal{G}_2$, denoted by $\mathcal{G}_1 \sqsubseteq \mathcal{G}_2$, when $\gamma_1 \circ \alpha_1 \sqsubseteq \gamma_2 \circ \alpha_2$; This is the standard definition, where the intuition is that the approximation in D_1 is more precise than in D_2, namely, for any $c \in C$, $\gamma_1(\alpha_1(c)) \leq_C \gamma_2(\alpha_2(c))$. Let us also recall that this happens iff $\gamma_2(\alpha_2(C)) \subseteq \gamma_1(\alpha_1(C))$, i.e., any concrete property

which is precisely represented by D_2 is also precisely represented by D_1. In turn, $\mathcal{G}_1$ and $\mathcal{G}_2$ are called isomorphic when $\mathcal{G}_1 \sqsubseteq \mathcal{G}_2$ and $\mathcal{G}_2 \sqsubseteq \mathcal{G}_1$, i.e., when $\gamma_1 \circ \alpha_1 = \gamma_2 \circ \alpha_2$ holds. Hence, the intuition is that $\mathcal{G}_1$ and $\mathcal{G}_2$ abstractly encode the same properties of C up to a renaming of the abstract values in D_i. This notion can be shifted to abstract functions as follows: If $f_1^\sharp : D_1 \to D_1$ and $f_2^\sharp : D_2 \to D_2$ are two abstract functions for a common concrete function $f : C \to C$ then $f_1^\sharp$ is called isomorphic to $f_2^\sharp$ when $\gamma_1 \circ f_1^\sharp \circ \alpha_1 = \gamma_2 \circ f_2^\sharp \circ \alpha_2$, that is, the following diagram commutes:

$$\begin{array}{ccc} D_1 & \xrightarrow{f_1^\sharp} & D_1 \\ {\scriptstyle\alpha_1}\uparrow & & \downarrow{\scriptstyle\gamma_1} \\ C & & C \\ {\scriptstyle\alpha_2}\downarrow & & \uparrow{\scriptstyle\gamma_2} \\ D_2 & \xrightarrow{f_2^\sharp} & D_2 \end{array}$$

3 Constructive Galois Connections

Constructive Galois connections (CGCs) have been put forward by Darais and Van Horn [10, Section 3] to feature a full "calculational" reasoning style in defining abstract domains and operations, which can therefore support an automatic mechanization by proof assistants. CGCs are defined by a Galois connection-like correspondence between sets rather than posets: $\langle \eta, A, B, \mu \rangle$ is a CGC when A and B are mere sets related by two functions $\eta : A \to B$ and $\mu : B \to \wp(A)$ which satisfy the following equivalence:

$$a \in \mu(b) \;\Leftrightarrow\; \eta(a) = b \qquad \text{(CGC-Corr)}$$

The intuition is that A is a carrier set of the concrete powerset domain $\wp(A)$, B is an unordered abstract domain, η is a representation function (also called extraction function) for concrete singletons $\{a\}$, while μ is a concretization function, which give rise to a sort of unordered adjunction relation between A and B. CGCs enjoy the following two key properties.

Lemma 3.1 (CGC properties). *Consider a CGC $\langle \eta, A, B, \mu \rangle$.*

(1) $\eta(a_1) = \eta(a_2) \;\Leftrightarrow\; \mu(\eta(a_1)) = \mu(\eta(a_2)) \;\Leftrightarrow\; \mu(\eta(a_1)) \cap \mu(\eta(a_2)) \neq \varnothing$
(2) $\mu(b) = \varnothing \;\Leftrightarrow\; b \notin \eta(A)$

Thus, the main consequence of Lemma 3.1 is that $\{\mu(\eta(a))\}_{a \in A}$ are the blocks of a partition of A. In fact, we have that: $A = \cup_{a \in A} \mu(\eta(a))$; by (2), any block $\mu(\eta(a))$ is nonempty; by (1), if $\mu(\eta(a_1)) \neq \mu(\eta(a_2))$ then $\mu(\eta(a_1)) \cap \mu(\eta(a_2)) = \varnothing$. The abstract values ranging in $B \setminus \eta(A)$ can be viewed as "useless" abstract values, because, by Lemma 3.1 (2), they all represent the empty set. This leads to a notion of *constructive Galois insertion* (CGI) which is the analogue of standard Galois insertions: $\langle \eta, A, B, \mu \rangle$ is called a CGI when it is a CGC and η is surjective.

Example 3.2. Consider the unordered abstract domain $B \triangleq \{-, 0, +, \bot\}$, the extraction function $\eta : \mathbb{Z} \to B$ which encodes the sign of an integer, and $\mu : B \to \wp(\mathbb{Z})$ defined by: $\mu(-) \triangleq \mathbb{Z}_{<0}$, $\mu(0) \triangleq \{0\}$, $\mu(+) \triangleq \mathbb{Z}_{>0}$, $\mu(\bot) \triangleq \varnothing$. Then $\mathcal{C} = \langle \eta, \mathbb{Z}, B, \mu \rangle$ is clearly a CGC. This is not a CGI because $\eta(\mathbb{Z}) \subsetneq B$. Let us notice that here $\{\mu(\eta(z))\}_{z \in \mathbb{Z}}$ gives rise to the partition $\{\mathbb{Z}_{<0}, \{0\}, \mathbb{Z}_{>0}\}$ of $\mathbb{Z}$ and that, accordingly with Lemma 3.1 (2), $\mu(\bot)$ must necessarily be set to $\varnothing$, since $\bot \notin \eta(B)$. □

Darais and Van Horn [10, Section 3.1] also define constructive Galois connections for posets (acronym CGPs) as follows. A tuple $\langle \eta, A, B, \mu \rangle$ is a CGP when $\langle A, \leq_A \rangle$ and $\langle B, \leq_B \rangle$ are posets, $\eta : A \to B$ and $\mu : B \to \wp^{\downarrow}(A)$ are monotone and the following equivalence holds:

$$a \in \mu(b) \;\Leftrightarrow\; \eta(a) \leq_B b \qquad \text{(CGP-Corr)}$$

Hence, in (CGP-Corr) the partial order relation $\leq_B$ replaces the equality relation of (CGC-Corr). We also recall that since A is a poset, we have that $\langle \wp^{\downarrow}(A), \subseteq \rangle$ is a complete lattice. It turns out that CGPs have the following properties.

Lemma 3.3 (CGP properties). *Consider a CGP $\langle \eta, A, B, \mu \rangle$.*

(1) $\eta(a_1) = \eta(a_2) \;\Leftrightarrow\; \mu(\eta(a_1)) = \mu(\eta(a_2))$
(2) $\mu(b) = \varnothing \;\Leftrightarrow\; {\downarrow}b \cap \eta(A) = \varnothing$
(3) *If B is a complete lattice then $\langle \eta^{\vee}, \wp^{\downarrow}(A), B, \mu \rangle$ is a GC.*
(4) $\mu(B) = \mu(\eta^{\vee}(\wp^{\downarrow}(A)))$

Hence, let us remark that by moving from CGCs to CGPs, properties (1) and (2) of Lemma 3.1 are lost and replaced by the weaker properties (1) and (2) of Lemma 3.3. In particular, we lose the key property of CGCs, namely that $\{\mu(\eta(a))\}_{a \in A}$ is partition of the carrier concrete poset A. Let us see an example of this phenomenon.

Example 3.4. Consider $\mathbb{Z}$ with the discrete partial order, so that $\wp^{\downarrow}(\mathbb{Z}) = \wp(\mathbb{Z})$, and consider the following abstract domain B:

Let $\eta : \mathbb{Z} \to B$ be defined by $\eta(x) \triangleq$ **if** $x > 0$ **then** $+$ **else** $\top$ and $\mu : \mathbb{Z} \to \wp(\mathbb{Z})$ be defined by $\mu(+) \triangleq \mathbb{Z}_{>0}$ and $\mu(\top) \triangleq \mathbb{Z}$. It turns out that $\mathcal{C} = \langle \eta, \mathbb{Z}, B, \mu \rangle$ is not a CGC, because $1 \in \mu(\top)$ while $+ = \eta(1) \neq \top$. Instead, $+ = \eta(1) \leq_B \top$ holds, and indeed $\mathcal{C}$ turns out to be a CGP. Notice that here $\{\mu(\eta(z)) \mid z \in \mathbb{Z}\} = \{\mathbb{Z}_{>0}, \mathbb{Z}\}$ does not give rise to a partition of $\mathbb{Z}$. □

3.1 Comparing CGCs

In the following we will need to compare CGCs having a common concrete carrier set.

Definition 3.5 (Comparison of CGCs). Let $\mathcal{C}_1 = \langle \eta_1, A, B_1, \mu_1 \rangle$ and $\mathcal{C}_2 = \langle \eta_2, A, B_2, \mu_2 \rangle$ be CGCs. Then, $\mathcal{C}_1$ *more precise than* $\mathcal{C}_2$ (or, $\mathcal{C}_2$ *more abstract than* $\mathcal{C}_1$), denoted by $\mathcal{C}_1 \sqsubseteq \mathcal{C}_2$, when:

(1) $\mu_1 \circ \eta_1 \sqsubseteq \mu_2 \circ \eta_2$;
(2) $\eta_1(A) = B_1 \;\Rightarrow\; \eta_2(A) = B_2$.

Also, $\mathcal{C}_1$ and $\mathcal{C}_2$ are *isomorphic*, denoted by $\mathcal{C}_1 \cong \mathcal{C}_2$, when $\mathcal{C}_1 \sqsubseteq \mathcal{C}_2$ and $\mathcal{C}_2 \sqsubseteq \mathcal{C}_1$. □

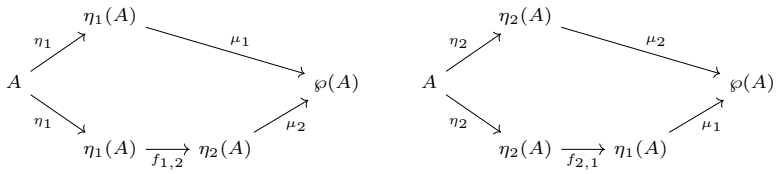
Condition (1) is analogous to GCs and formalizes the intuition that B_1 is a more precise abstract domain than B_2. However, this is not enough for CGCs, because, by Lemma 3.1 (2), if $\eta_2(A) \subsetneq B_2$ then there exists some $b_2 \notin \eta_2(A)$ such that $\mu_2(b_2) = \varnothing$, meaning that B_2 is able to represent the empty property, so that this must also hold for B_1. This is exactly stated by condition (2), which therefore allows us to provide the right comparison relation for CGCs. We also define a *nonempty comparison* relation $\sqsubseteq_\varnothing$ that does not take into account possible empty properties in $\mu(B_i)$: $\mathcal{C}_1 \sqsubseteq_\varnothing \mathcal{C}_2$ when just $\mu_1 \circ \eta_1 \sqsubseteq \mu_2 \circ \eta_2$ holds. In turn, we have nonempty isomorphism: $\mathcal{C}_1 \cong_\varnothing \mathcal{C}_2$ when $\mathcal{C}_1 \sqsubseteq_\varnothing \mathcal{C}_2$ and $\mathcal{C}_2 \sqsubseteq_\varnothing \mathcal{C}_1$.

Lemma 3.6.
(1) $\mathcal{C}_1 \cong \mathcal{C}_2$ *iff* $\mu_1(B_1) = \mu_2(B_2)$.
(2) $\mathcal{C}_1 \cong_\varnothing \mathcal{C}_2$ *iff* $\mu_1(B_1) \smallsetminus \{\varnothing\} = \mu_2(B_2) \smallsetminus \{\varnothing\}$.

Hence, the intuition of the isomorphism relation is the same of Galois connections, as defined in Section 2: two CGCs are isomorphic when they exactly represent the same abstraction of the concrete domain $\wp(A)$ up to a renaming of abstract values. This notion of isomorphism is also justified by the following result, where $f_{1,2}$ and $f_{2,1}$ play the role of renaming functions: $f_{1,2} : \eta_1(A) \to \eta_2(A)$ encodes abstract values in $\eta_1(A)$ as abstract values in $\eta_2(A)$, and conversely for $f_{2,1} : \eta_2(A) \to \eta_1(A)$, where $f_{1,2}$ and $f_{2,1}$ are one the inverse of the other and also commute with the concretizations μ_1 and μ_2.

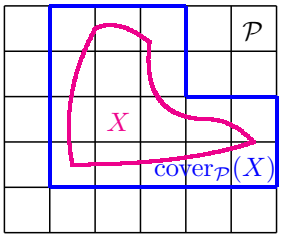
Lemma 3.7 (CGC Isomorphism). *Let* $\mathcal{C}_1 = \langle \eta_1, A, B_1, \mu_1 \rangle$ *and* $\mathcal{C}_2 = \langle \eta_2, A, B_2, \mu_2 \rangle$ *be CGCs. Then,* $\mathcal{C}_1 \cong_\varnothing \mathcal{C}_2$ *iff there exist* $f_{1,2} : \eta_1(A) \to \eta_2(A)$ *and* $f_{2,1} : \eta_2(A) \to \eta_1(A)$ *such that* $f_{1,2} \circ f_{2,1} = \mathrm{id} = f_{2,1} \circ f_{1,2}$, $\mu_1 \circ \eta_1 = \mu_2 \circ f_{1,2} \circ \eta_1$ *and* $\mu_2 \circ \eta_2 = \mu_1 \circ f_{2,1} \circ \eta_2$.

In particular, let us remark that Lemma 3.7 requires that the following two diagrams commute:



4 Partitioning Galois Connections

Partitioning Galois connections/insertions (PGCs/PGIs) have been introduced by Cousot and Cousot as particular examples of Galois connections in a number of articles, where they have been called elementwise set abstractions (or homomorphic abstractions): [7, Section 5], [8, Example 13] and [3, Example 6]. Given a partition $\mathcal{P}$ of a set A, the basic idea is that any subset $X \in \wp(A)$ is over-approximated by the unique minimal cover of X through blocks in $\mathcal{P}$, denoted by $\mathrm{cover}_\mathcal{P}(X)$ and depicted in the following picture:



The definition of PGCs given here has been studied and used in [21,22,23] for generalizing strong preservation of temporal logics in model checking. Let us consider a GC $\mathcal{G} = \langle \alpha, \wp(A)_{\subseteq}, D_{\leq}, \gamma \rangle$, where A is any unordered carrier set and D is a complete lattice. Let us remark that, as a consequence of the properties of GCs, D must necessarily be a complete lattice (rather than a mere poset). If $\mathrm{prt}(\mathcal{G}) \triangleq \{\gamma(\alpha(\{a\}))\}_{a \in A}$ then $\mathcal{G}$ is called a *partitioning Galois connection* when:

(1) $\mathrm{prt}(\mathcal{G})$ is a partition of A;
(2) γ is additive, i.e., γ preserves arbitrary lub's.

The main property of a PGC is that any abstract value $d \in D$ represents a union of blocks of the partition $\mathrm{prt}(\mathcal{G})$, namely $\gamma(d) = \cup_{a \in \gamma(d)} \gamma(\alpha(\{a\}))$, and, vice versa, for any set of blocks $\{\gamma(\alpha(\{a\}))\}_{a \in S}$ of the partition $\mathrm{prt}(\mathcal{G})$, for some $S \subseteq A$, there exists $d \in A$ such that $\gamma(d) = \cup_{a \in S} \gamma(\alpha(\{a\}))$. In other terms, the abstract domain D is a representation of all the possible unions of blocks in $\mathrm{prt}(\mathcal{G})$. Alternatively, instead of representing all the possible unions of blocks of a partition, one could equivalently represent no union of blocks at all. This means that the above condition (2), requiring the additivity of the concretization map γ, could be replaced by:

(2′) if $x, y \in D$ and x, y are uncomparable then $\gamma(x \vee_D y) = A$.

In this case, if $\alpha(\{a_1\})$ and $\alpha(\{a_2\})$ represent in D two different blocks then their lub represents no information at all, that is, $\gamma(\alpha(\{a_1, a_2\})) = A$.

Example 4.1. Consider the Sign abstract lattice for sign analysis as depicted in Section 1 and encoded by the GI $\mathcal{S} = \langle \alpha, \wp(\mathbb{Z}), \mathrm{Sign}, \gamma \rangle$, where abstraction and concretization maps are defined as usual. It turns out that $\mathcal{S}$ is a PGC (more precisely, a PGI), where the partition of $\mathbb{Z}$ is given by $\mathrm{prt}(\mathcal{S}) = \{\gamma(\alpha(\{z\})) \subseteq \mathbb{Z} \mid z \in \mathbb{Z}\} = \{\mathbb{Z}_{<0}, \mathbb{Z}_{=0}, \mathbb{Z}_{>0}\}$. □

It turns out that the notion of CGC is equivalent to that of PGC. This equivalence is formalized by two transforms $\mathbb{T}_{\mathrm{PGC}}$ and $\mathbb{T}_{\mathrm{CGC}}$ such that: (1) any CGC $\mathcal{C}$ can be transformed into a PGC $\mathbb{T}_{\mathrm{PGC}}(\mathcal{C})$; (2) any PGC $\mathcal{G}$ can be transformed into a CGC $\mathbb{T}_{\mathrm{CGC}}(\mathcal{G})$; (3) these transforms are one the inverse of the other up to (nonempty) isomorphism, i.e., $\mathbb{T}_{\mathrm{CGC}}(\mathbb{T}_{\mathrm{PGC}}(\mathcal{C})) \cong_{\varnothing} \mathcal{C}$ and $\mathbb{T}_{\mathrm{PGC}}(\mathbb{T}_{\mathrm{CGC}}(\mathcal{G})) \cong \mathcal{G}$.

Theorem 4.2 (CGC-PGC Equivalence).
(1) *If* $\mathcal{C} = \langle \eta, A, B, \mu \rangle$ *is a CGC then* $\mathbb{T}_{\mathrm{PGC}}(\mathcal{C}) \triangleq \langle \eta^{\diamond}, \wp(A)_{\subseteq}, \wp(B)_{\subseteq}, \mu^{*} \rangle$ *is a PGC.*
(2) *If* $\mathcal{G} = \langle \alpha, \wp(A)_{\subseteq}, D_{\leq}, \gamma \rangle$ *is a PGC then* $\mathbb{T}_{\mathrm{CGC}}(\mathcal{G}) \triangleq \langle \alpha^{\{\}}, A, \{\alpha(\{a\}) \mid a \in A\}, \gamma \rangle$ *is a CGC.*
(3) *The transforms* $\mathbb{T}_{\mathrm{PGC}}$ *and* $\mathbb{T}_{\mathrm{CGC}}$ *are one the inverse of the other, up to nonempty isomorphism.*

Let us remark that in Theorem 4.2, according to the definitions in Section 2:

(1) In the PGC $\mathbb{T}_{\text{PGC}}(\mathcal{C}) = \langle \eta^{\diamond}, \wp(A)_{\subseteq}, \wp(B)_{\subseteq}, \mu^{*} \rangle$, we have that for any $X \in \wp(A)$ and $Y \in \wp(B)$: $\eta^{\diamond}(X) = \{\eta(x) \mid x \in X\} \in \wp(B)$ and $\mu^{*}(Y) = \cup_{y \in Y} \mu(y) \in \wp(A)$.
(2) In the CGC $\mathbb{T}_{\text{CGC}}(\mathcal{G}) = \langle \alpha^{\{\}}, A, \{\alpha(\{a\}) \mid a \in A\}, \gamma \rangle$, we have that: $\alpha^{\{\}} : A \to \{\alpha(\{a\}) \mid a \in A\}$ and $\gamma : \{\alpha(\{a\}) \mid a \in A\} \to \wp(A)$, where $\alpha^{\{\}}(a) = \alpha(\{a\})$ and $\gamma(\alpha(\{a\})) \in \wp(A)$.

Example 4.3. Let us consider the PGC $\mathcal{S} = \langle \alpha, \wp(\mathbb{Z}), \mathrm{Sign}, \gamma \rangle$ of Example 4.1. Then, $\mathbb{T}_{\text{CGC}}(\mathcal{S})$ provides a CGC which is nonempty isomorphic to the CGC $\mathcal{C} = \langle \eta, \mathbb{Z}, B, \mu \rangle$ of Example 3.2: indeed, these two CGCs only differ for the element $\bot \in B$ whose meaning is $\varnothing = \mu(\bot)$. Conversely, $\mathbb{T}_{\text{PGC}}(\mathcal{C})$ is a PGC which is isomorphic to $\mathcal{S}$. In fact, the abstract domain of $\mathbb{T}_{\text{PGC}}(\mathcal{C})$ is $\wp(B)$, so that, since B includes the "useless" value $\bot$, we obtain a PGC rather than a PGI, because its concretization map μ^{*} is not injective, e.g., $\mu^{*}(\{\bot, +\}) = \mu^{*}(\{\bot\})$. □

Furthermore, it turns out that the transforms of Theorem 4.2 preserve the relative precision relations between CGCs/PGCs as follows.

Corollary 4.4. *If $\mathcal{C}_1$ and $\mathcal{C}_2$ are CGCs then $\mathcal{C}_1 \sqsubseteq_{\varnothing} \mathcal{C}_2$ iff $\mathbb{T}_{\text{PGC}}(\mathcal{C}_1) \sqsubseteq \mathbb{T}_{\text{PGC}}(\mathcal{C}_2)$. If $\mathcal{G}_1$ and $\mathcal{G}_2$ are PGCs then $\mathcal{G}_1 \sqsubseteq \mathcal{G}_2$ iff $\mathbb{T}_{\text{CGC}}(\mathcal{G}_1) \sqsubseteq_{\varnothing} \mathbb{T}_{\text{CGC}}(\mathcal{G}_2)$.*

As a consequence, one can define the lattice of all CGCs having a common concrete carrier set, ordered w.r.t. their relative precision up to nonempty isomorphism $\sqsubseteq_{\varnothing}$, which turns out to be order-theoretically isomorphic to the standard lattice of partitioning abstract domains [23, Theorem 3.2].

Let us mention that [10] also puts forward a notion of *Kleisli* Galois connection (KGC) between posets, which relies on a "monadic" notion of abstraction/concretization maps. Actually, this class of constructive abstract domains is shown to be equivalent to CGCs (cf. [10, Section 6]), where this isomorphism includes the notions of soundness and optimality for abstract functions. Hence, we do not need to replicate our isomorphism between KGCs and PGCs, which comes as a consequence.

CGCs as Least Disjunctive Bases. Given a CGC $\mathcal{C} = \langle \eta, A, B, \mu \rangle$, Theorem 4.2 shows that $\mathbb{T}_{\text{PGC}}(\mathcal{C}) = \langle \eta^{\diamond}, \wp(A)_{\subseteq}, \wp(B)_{\subseteq}, \mu^{*} \rangle$ is a PGC. Let us observe here that $\{\{x\} \mid x \in B\}$ is the set of join-irreducible elements of the complete lattice $\langle \wp(B), \subseteq \rangle$. Recall that an element x of a complete lattice C is join-irreducible when, for any $S \subseteq C$, $x = \vee S \Rightarrow x \in S$, namely when any element $x \in C$ can never be represented as a lub of a subset $S \subseteq C$ not containing x. In abstract interpretation terms (see [11]), this observation means that the set $\{\{x\} \mid x \in B\}$ can be viewed as the so-called *least disjunctive basis* of the partitioning abstract domain $\wp(B)_{\subseteq}$. Least disjunctive bases have been introduced in [11] as an inverse operation to the well-known disjunctive completion of abstract domains [5]. Given an abstract domain D, its least disjunctive basis is defined to be the most abstract domain which has the same disjunctive completion as D. Hence, the least disjunctive basis of D reveals and therefore removes all the disjunctive information inside D by keeping only the information which cannot be reconstructed through logical disjunction. It turns out that a concrete domain which is a powerset,

as it is the case of $\wp(A)_{\subseteq}$ in the PGC $\mathbb{T}_{\text{PGC}}(\mathcal{C})$, satisfies the hypotheses of [11, Theorem 4.13], and this latter result ensures that the least disjuctive basis of any abstract domain D exists and is characterized as the closure under arbitrary meets of the join-irreducible elements of D. This result can be therefore applied to the abstract domain $\wp(B)_{\subseteq}$ of the PGC $\mathbb{T}_{\text{PGC}}(\mathcal{C})$, whose least disjunctive basis is given by the meet-closure of $\{\{x\} \mid x \in B\}$. We observe that this meet-closure of $\{\{x\} \mid x \in B\}$ simply adds $\varnothing$ and B. Hence, in this sense, the role of the abstract domain B in a CGC $\langle \eta, A, B, \mu \rangle$ can also be viewed as least disjunctive basis of a partitioning abstract domain.

Constructive Closure Operators. In abstract interpretation, abstract domains up to renaming of abstract values are encoded by closure operators on the concrete domain, which turn out to be fully isomorphic to Galois connections [5] and allow to reason on abstract domains independently of a specific representation of abstract values. Recall that a map $\rho : C \to C$ is a closure operator when ρ is monotone, idempotent and extensive (i.e., $x \leq_C \rho(x)$). Hence, the isomorphism between CGCs and PGCs given by Theorem 4.2 leads us to a notion of "constructive closure operator".

Given any concrete unordered carrier set A, a map $\varphi : A \to \wp(A)$ is a *constructive closure operator* (CCO) when the following condition holds:

$$x \in \varphi(y) \;\Leftrightarrow\; \varphi(x) = \varphi(y) \qquad \text{(CCO-Corr)}$$

CCOs turn out to be the right notion, since they do not rely on a specific representation of abstract values and are equivalent to CGCs, as shown by the following result.

Corollary 4.5 (CGC-CCO Equivalence).
(1) *If* $\mathcal{C} = \langle \eta, A, B, \mu \rangle$ *is a CGC then* $\mathbb{T}_{\text{CCO}}(\mathcal{C}) \triangleq \mu \circ \eta : A \to \wp(A)$ *is a CCO.*
(2) *If* $\varphi : A \to \wp(A)$ *is a CCO then* $\mathbb{T}_{\text{CGC}}(\varphi) \triangleq \langle \varphi, A, \{\varphi(a) \mid a \in A\}, \mathrm{id} \rangle$ *is a CGC.*
(3) *The transforms* $\mathbb{T}_{\text{CCO}}$ *and* $\mathbb{T}_{\text{CGC}}$ *are one the inverse of the other, up to nonempty isomorphism.*

Example 4.6. Consider the CGC $\mathcal{C} = \langle \eta, \mathbb{Z}, B, \mu \rangle$ of Example 3.2, where the unordered abstract domain is $B = \{-, 0, +, \bot\}$. The corresponding constructive closure operator $\mathbb{T}_{\text{CCO}}(\mathcal{C}) : \mathbb{Z} \to \wp(\mathbb{Z})$ is therefore trivially defined, by Corollary 4.5 (1), as follows:

$$\mathbb{T}_{\text{CCO}}(z) = \begin{cases} \mathbb{Z}_{<0} & \text{if } z < 0 \\ \{0\} & \text{if } z = 0 \\ \mathbb{Z}_{>0} & \text{if } z > 0 \end{cases}$$

Analogously to closure operators for standard Galois connections, this map $\mathbb{T}_{\text{CCO}}(\mathcal{C})$ allows us to encode the approximation of the constructive Galois connection $\mathcal{C}$ independently of the specific representation of the abstract domain B. □

4.1 Characterization of CGPs

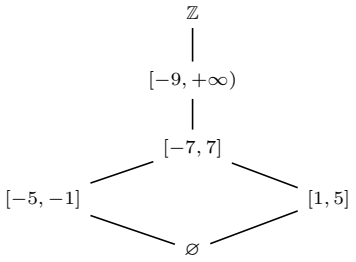
Let us now turn on CGPs. Can this class of constructive abstractions be characterized in terms of some subclass of Galois connections?

Consider a CGP $\langle \eta, A, B, \mu \rangle$, so that the concrete carrier set A is a poset, the abstract domain B is a poset, and the maps $\eta : A \to B$ and $\mu : B \to \wp^{\downarrow}(A)$ are monotone. Here, for our characterization, we additionally need that the abstract domain B is a complete lattice. Following the proof of Theorem 4.2, hence relying on the definition of two CGPs/GCs transforms, we show that the class of CGPs turns out to be isomorphic to the whole class of GCs of the concrete powerdomain $\wp^{\downarrow}(A)$.

Theorem 4.7 (CGP-GC Equivalence).
(1) *If* $\mathcal{C} = \langle \eta, A, B, \mu \rangle$ *is a CGP then* $\mathbb{T}_{\mathsf{GC}}(\mathcal{C}) \triangleq \langle \eta^{\vee}, \wp^{\downarrow}(A)_{\subseteq}, B, \mu \rangle$ *is a GC.*
(2) *If* $\mathcal{G} = \langle \alpha, \wp^{\downarrow}(A)_{\subseteq}, D_{\leq}, \gamma \rangle$ *is a GC then* $\mathbb{T}_{\mathsf{CGP}}(\mathcal{G}) \triangleq \langle \lambda a.\alpha(\downarrow\{a\}), A, D, \gamma \rangle$ *is a CGP.*
(3) *The transforms* $\mathbb{T}_{\mathsf{GC}}$ *and* $\mathbb{T}_{\mathsf{CGP}}$ *are one the inverse of the other, up to isomorphism.*

Otherwise stated, this result shows that the generalization from CGCs to CGPs, which takes care of concrete and abstract carrier sets which are posets, actually provides a constructive characterization of the whole class of Galois connections of the powerdomain $\wp^{\downarrow}(A)$.

Example 4.8. Consider the following lattice D of integer intervals ordered by subset inclusion:



This lattice D gives rise to a Galois insertion $\mathcal{G} = \langle \alpha, \wp(\mathbb{Z}), D, \gamma \rangle$ where $\mathbb{Z}$ is considered with the discrete order, γ is the identity and, for example, we have that $\alpha(\{2\}) = [1, 5]$, $\alpha(\{0\}) = \alpha(\{6\}) = [-7, 7]$, $\alpha(\{10\}) = [-9, +\infty)$, $\alpha(\{-10\}) = \mathbb{Z}$. Let us observe that γ is not additive, because $[-5, 5] = [-5, -1] \cup [1, 5] = \gamma([-5, -1]) \cup \gamma([1, 5]) \subsetneq \gamma([-5, -1] \vee_D [1, 5]) = [-7, 7]$. Hence, this Galois insertion is neither partitioning nor disjunctive.
By Theorem 4.7 (2), it turns out that $\mathbb{T}_{\mathsf{CGP}}(\mathcal{G}) = \langle \lambda z.\alpha(\{z\}), \mathbb{Z}, D, \gamma \rangle$ is a CGP, and this allows us to view D as a constructive abstract domain. Let us remark that this is true even if $\mathcal{G}$ is neither partitioning nor disjunctive.
Let us remark that Theorem 4.7 applies to infinite abstract domains as well. As a simple example, consider the complete lattice $E \triangleq \{[0, n] \mid n \in \mathbb{N}\} \cup \{\mathbb{N}\}$, ordered by subset inclusion, which is an infinite increasing chain of intervals of natural numbers. This complete lattice gives rise to a GI $\mathcal{E} = \langle \alpha, \wp(\mathbb{N}), E, \gamma \rangle$ where $\mathbb{N}$ is discretely ordered and γ is the identity. Here, Theorem 4.7 (2) yields a CGP $\mathbb{T}_{\mathsf{CGP}}(\mathcal{E}) = \langle \eta, \mathbb{N}, E, \mathrm{id} \rangle$ where $\eta(n) = [0, n]$. As a further infinite example, consider the well-known complete lattice of integer intervals Int, which is defined by a GI $\mathcal{I} = \langle \alpha_{\mathrm{Int}}, \wp(\mathbb{N}), \mathrm{Int}, \gamma_{\mathrm{Int}} \rangle$ where $\mathbb{N}$ is discretely ordered [4,5]. Here, Theorem 4.7 (2) yields a CGP $\mathbb{T}_{\mathsf{CGP}}(\mathcal{I}) = \langle \eta_{\mathrm{Int}}, \mathbb{N}, \mathrm{Int}, \gamma_{\mathrm{Int}} \rangle$ where $\eta_{\mathrm{Int}}(n) = [n, n]$. □

4.2 On the Meaning of the Isomorphisms

Theorem 4.2 provides an isomorphism between CGCs and partitioning GCs, while Theorem 4.7 yields an isomorphism between CGPs and standard GCs. In particular, Theorem 4.2 (2) shows how a partitioning GC $\mathcal{G}$ can be transformed into an equivalent CGC $\mathbb{T}_{\mathsf{CGC}}(\mathcal{G})$, while Theorem 4.7 (2) establishes how a standard GC $\mathcal{G}$ of a concrete powerdomain can be mapped to an equivalent CGP $\mathbb{T}_{\mathsf{CGP}}(\mathcal{G})$. It should be remarked that the transforms $\mathbb{T}_{\mathsf{CGC}}(\mathcal{G})$ and $\mathbb{T}_{\mathsf{CGP}}(\mathcal{G})$ are nonconstructive, meaning that their definitions rely on the abstraction map α which determines the input Galois connection $\mathcal{G}$. Nevertheless, these transforms are still useful since they provide a precise formal definition which can be used for manually designing a CGC out of a partitioning GC and a CGP out of any GC of a concrete powerdomain, in this latter case thus making possible to define a constructive abstract domain starting from any GC.

5 Soundness of Abstract Operations

Our next step is to transform a pair of sound abstract functions from CGCs to PGCs and vice versa, in order to show that the equivalence between CGCs and PGCs also include soundness of abstract functions. Analogously for optimality. For notational simplicity, we consider unary functions, but the whole approach can be straighforwardly generalized to generic n-ary functions (that indeed we will use in some examples).

Let $\mathcal{C} = \langle \eta, A, B, \mu \rangle$ be a CGC, $f : A \to A$ be a concrete function and $f_\sharp : B \to B$ be a corresponding abstract function. Darais and Van Horn [10] provide four equivalent soudness conditions for the pair $\langle f, f_\sharp \rangle$ w.r.t. $\mathcal{C}$, which are as follows:

$$x \in \mu(y) \,\&\, y' = \eta(f(x)) \;\Rightarrow\; y' = f_\sharp(y) \qquad \text{(CGC-Snd/}\eta\mu\text{)}$$
$$x \in \mu(y) \,\&\, x' = f(x) \;\Rightarrow\; x' \in \mu(f_\sharp(y)) \qquad \text{(CGC-Snd/}\mu\mu\text{)}$$
$$y = \eta(f(x)) \;\Rightarrow\; y = f_\sharp(\eta(x)) \qquad \text{(CGC-Snd/}\eta\eta\text{)}$$
$$x' = f(x) \;\Rightarrow\; x' \in \mu(f_\sharp(\eta(x))) \qquad \text{(CGC-Snd/}\mu\eta\text{)}$$

Given two CGCs $\mathcal{C}_i = \langle \eta_i, A, B_i, \mu_i \rangle$, $i = 1, 2$, a concrete function $f : A \to A$ and two corresponding abstract functions $f_i^\sharp : B_i \to B_i$, we extend the notion of CGC isomorphism (given in Section 3.1) to functions as follows: $\langle f, f_1^\sharp \rangle \cong \langle f, f_2^\sharp \rangle$ when (1) f_i is sound for f w.r.t. $\mathcal{C}_i$; (2) $\mu_1 \circ f_1^\sharp \circ \eta_1 = \mu_2 \circ f_2^\sharp \circ \eta_2$. This corresponds to require that the concrete projections of $f_1^\sharp$ and $f_2^\sharp$, which are of type $A \to \wp(A)$, coincide, so that $f_1^\sharp$ and $f_2^\sharp$ can be regarded as being isomorphic.

Let us first consider $\mathbb{T}_{\mathsf{PGC}}$ which transforms a CGC $\mathcal{C}$ into an equivalent partitioning Galois connection $\mathbb{T}_{\mathsf{PGC}}(\mathcal{C}) = \langle \eta^\diamond, \wp(A)_\subseteq, \wp(B)_\subseteq, \mu^* \rangle$. Here, the pair of functions $\langle f, f_\sharp \rangle$ w.r.t. $\mathcal{C}$ is transformed, through the powerset lifting $(\cdot)^\diamond$ of Section 2, into a pair of functions $\mathbb{T}_{\mathsf{PGC}}(\langle f, f_\sharp \rangle)$ w.r.t. $\mathbb{T}_{\mathsf{PGC}}(\mathcal{C})$, that is, $\mathbb{T}_{\mathsf{PGC}}(\langle f, f_\sharp \rangle) \triangleq \langle f^\diamond, f_\sharp^\diamond \rangle$, where $f^\diamond : \wp(A) \to \wp(A)$ and $f_\sharp^\diamond : \wp(B) \to \wp(B)$.

Conversely, let $\mathcal{G} = \langle \alpha, \wp(A)_\subseteq, D_\leq, \gamma \rangle$ be a PGC, so that the abstract domain D represents a partition $\mathrm{prt}(\mathcal{G})$ of A. Here, we need to consider concrete functions on the powerset $\wp(A)$ which are defined as powerset lifting of a mapping $g : A \to A$ on the unordered carrier set A, that is, $g^\diamond : \wp(A) \to \wp(A)$ will be our concrete function. On

the abstract side, a monotone abstract function $g_\sharp : D \to D$ is called *block-preserving* (w.r.t. blocks in $\mathrm{prt}(\mathcal{G})$) when $g_\sharp$ maps (abstract representations of) blocks to (abstract representations of) blocks, namely, when the following condition holds:

$$\forall a \in A. \exists a' \in A.\ g_\sharp(\alpha(\{a\})) = \alpha(\{a'\}).$$

Example 5.1. Consider the PGC (actually PGI) $\mathcal{S} = \langle \alpha, \wp(\mathbb{Z}), \mathrm{Sign}, \gamma \rangle$ of Example 4.1. Similarly to the examples in [10, Section 2], we consider the successor concrete function $succ : \mathbb{Z} \to \mathbb{Z}$ on the concrete carrier domain $\mathbb{Z}$, so that $succ^\diamond : \wp(\mathbb{Z}) \to \wp(\mathbb{Z})$. The corresponding best correct approximation $succ_{\mathrm{Sign}} \triangleq \alpha \circ succ^\diamond \circ \gamma$ is as follows:

$$succ_{\mathrm{Sign}} = \{\varnothing \mapsto \varnothing,\ {<}0 \mapsto {\leq}0,\ {=}0 \mapsto {>}0,\ {>}0 \mapsto {>}0,\ {\leq}0 \mapsto \mathbb{Z},\ {\neq}0 \mapsto \mathbb{Z},\ {\geq}0 \mapsto {>}0,\ \mathbb{Z} \mapsto \mathbb{Z}\}$$

Then, $succ_{\mathrm{Sign}}$ is not block-preserving because $succ_{\mathrm{Sign}}(\alpha(\{-1\})) = {\leq}0$ and there exists no $z \in \mathbb{Z}$ such that $\alpha(\{z\}) = {\leq}0$.
As a further example, consider the concrete square function $sq : \mathbb{Z} \to \mathbb{Z}$, namely, $sq(z) = z^2$, its powerset lifting $sq^\diamond : \wp(\mathbb{Z}) \to \wp(\mathbb{Z})$, and, in turn, its corresponding best correct approximation $sq_{\mathrm{Sign}} \triangleq \alpha \circ sq^\diamond \circ \gamma$:

$$sq_{\mathrm{Sign}} = \{\varnothing \mapsto \varnothing,\ {<}0 \mapsto {>}0,\ {=}0 \mapsto {=}0,\ {>}0 \mapsto {>}0,\ {\leq}0 \mapsto {\geq}0,\ {\neq}0 \mapsto {>}0,\ {\geq}0 \mapsto {\geq}0,\ \mathbb{Z} \mapsto {\geq}0\}$$

Here, it turns out that sq_{Sign} is instead block-preserving. □

Lemma 5.2. *If $\mathcal{G}$ is a PGI, $\langle g^\diamond, g_\sharp \rangle$ is sound and $g_\sharp$ is block-preserving then, for any $a \in A$, $g_\sharp(\alpha(\{a\})) = \alpha(\{g(a)\})$ and $g^\diamond(\gamma(\alpha(\{a\}))) \subseteq \gamma(\alpha(\{g(a)\}))$.*

In order to transform a sound pair of functions $\langle g^\diamond, g_\sharp \rangle$ w.r.t. $\mathcal{G}$, where $g_\sharp$ is assumed to be block-preserving, into a pair of functions for $\mathbb{T}_{\mathrm{CGC}}(\mathcal{G}) = \langle \alpha^{\{\}}, A, \{\alpha(\{a\}) \mid a \in A\}, \gamma \rangle$, we consider:

(i) the concrete carrier function $g : A \to A$
(ii) the restriction $g^r_\sharp$ of the abstract function $g_\sharp$ to abstract representations of blocks, as determined by Lemma 5.2, namely, $g^r_\sharp : \{\alpha(\{a\}) \mid a \in A\} \to \{\alpha(\{a\}) \mid a \in A\}$, with $g^r_\sharp(\alpha(\{a\})) \triangleq \alpha(\{g(a)\})$.

This transform of pair of functions from PGCs to CGCs is denoted by $\mathbb{T}_{\mathrm{CGC}}(\langle g^\diamond, g_\sharp \rangle) \triangleq \langle g, g^r_\sharp \rangle$. It allows us to extend our correspondance between CGCs and PGCs in order to include soundness as follows.

Theorem 5.3.
(1) *Let $\mathcal{C} = \langle \eta, A, B, \mu \rangle$ be a CGC, $f : A \to A$ and $f_\sharp : B \to B$. Then, $\langle f, f_\sharp \rangle$ is sound iff $\mathbb{T}_{\mathrm{PGC}}(\langle f, f_\sharp \rangle)$ is sound w.r.t. $\mathbb{T}_{\mathrm{PGC}}(\mathcal{C})$.*
(2) *Let $\mathcal{G} = \langle \alpha, \wp(A)_\subseteq, D_\leq, \gamma \rangle$ be a PGC, $g^\diamond : \wp(A) \to \wp(A)$, for some $g : A \to A$, and $g_\sharp : D \to D$ be monotone and block-preserving. Then, $\langle g^\diamond, g_\sharp \rangle$ is sound iff $\mathbb{T}_{\mathrm{CGC}}(\langle g^\diamond, g_\sharp \rangle)$ is sound w.r.t. $\mathbb{T}_{\mathrm{CGC}}(\mathcal{G})$.*
(3) *If $\langle f, f_\sharp \rangle$ is sound then $\mathbb{T}_{\mathrm{CGC}}(\mathbb{T}_{\mathrm{PGC}}(\langle f, f_\sharp \rangle)) \cong \langle f, f_\sharp \rangle$. If $\langle g^\diamond, g_\sharp \rangle$ is sound and $g_\sharp$ is block-preserving and additive then $\mathbb{T}_{\mathrm{PGC}}(\mathbb{T}_{\mathrm{CGC}}(\langle g^\diamond, g_\sharp \rangle)) \cong \langle g^\diamond, g_\sharp \rangle$.*

Example 5.4. Consider Example 5.1, where the best correct approximation $sq_{\mathrm{Sign}} : \mathrm{Sign} \to \mathrm{Sign}$ of the concrete square operation $sq^{\diamond} : \wp(\mathbb{Z}) \to \wp(\mathbb{Z})$ is (monotone and) block-preserving. Indeed, the set of (abstract) blocks is $B = \{\alpha(\{z\}) \mid z \in \mathbb{Z}\} = \{<0, =0, >0\}$ and sq_{Sign} maps blocks to blocks. Here, we have that $\mathbb{T}_{\mathrm{CGC}}(\mathcal{S}) = \langle \eta, \mathbb{Z}, B, \mu \rangle$ and $\mathbb{T}_{\mathrm{CGC}}(\langle sq^{\diamond}, sq_{\mathcal{S}} \rangle) = \langle sq, sq^{r}_{\mathcal{S}} \rangle$ where $sq : \mathbb{Z} \to \mathbb{Z}$ and the restriction $sq^{r}_{\mathcal{S}} : B \to B$ is such that $sq^{r}_{\mathcal{S}}(\alpha(\{z\})) = \alpha(\{sq(z)\})$, namely:

$$sq^{r}_{\mathcal{S}} = \{<0 \mapsto >0,\ =0 \mapsto =0,\ >0 \mapsto >0\}$$ □

5.1 Completeness

As observed in [10], the above four equivalent soundness conditions (CGC-Snd) for CGCs lead to four non-equivalent conditions of completeness for abstract functions, where $\Leftrightarrow$ replaces $\Rightarrow$:

$$x \in \mu(y)\ \&\ y' = \eta(f(x)) \ \Leftrightarrow\ y' = f_{\sharp}(y) \qquad \text{(CGC-Cmp/}\eta\mu\text{)}$$
$$x \in \mu(y)\ \&\ x' = f(x) \ \Leftrightarrow\ x' \in \mu(f_{\sharp}(y)) \qquad \text{(CGC-Cmp/}\mu\mu\text{)}$$
$$y = \eta(f(x)) \ \Leftrightarrow\ y = f_{\sharp}(\eta(x)) \qquad \text{(CGC-Cmp/}\eta\eta\text{)}$$
$$x' = f(x) \ \Leftrightarrow\ x' \in \mu(f_{\sharp}(\eta(x))) \qquad \text{(CGC-Cmp/}\mu\eta\text{)}$$

It turns out that these completeness conditions for a pair $\langle f, f_{\sharp} \rangle$ can be equivalently stated using the standard optimality/completeness/precision conditions for Galois connections, as recalled in Section 2, for the transformed pair $\mathbb{T}_{\mathrm{PGC}}(\langle f, f_{\sharp} \rangle)$.

Lemma 5.5.
(1) $\langle f, f_{\sharp} \rangle$ *satisfies* (CGC-Cmp/$\eta\mu$) *iff* $\mathbb{T}_{\mathrm{PGC}}(\langle f, f_{\sharp} \rangle)$ *is optimal w.r.t.* $\mathbb{T}_{\mathrm{PGC}}(\mathcal{C})$.
(2) $\langle f, f_{\sharp} \rangle$ *satisfies* (CGC-Cmp/$\mu\mu$) *iff* $\mathbb{T}_{\mathrm{PGC}}(\langle f, f_{\sharp} \rangle)$ *is forward complete w.r.t.* $\mathbb{T}_{\mathrm{PGC}}(\mathcal{C})$.
(3) $\langle f, f_{\sharp} \rangle$ *satisfies* (CGC-Cmp/$\eta\eta$) *iff* $\mathbb{T}_{\mathrm{PGC}}(\langle f, f_{\sharp} \rangle)$ *is backward complete w.r.t.* $\mathbb{T}_{\mathrm{PGC}}(\mathcal{C})$.
(4) $\langle f, f_{\sharp} \rangle$ *satisfies* (CGC-Cmp/$\mu\eta$) *iff* $\mathbb{T}_{\mathrm{PGC}}(\langle f, f_{\sharp} \rangle)$ *is precise w.r.t.* $\mathbb{T}_{\mathrm{PGC}}(\mathcal{C})$.

Example 5.6. Consider Example 5.4, namely the CGC $\mathcal{C} = \langle \eta, \mathbb{Z}, B, \mu \rangle$, with $B = \{<0,\ =0,\ >0\}$, the concrete square operation $sq : \mathbb{Z} \to \mathbb{Z}$ and the corresponding abstract square operation $sq_{\sharp} : B \to B$

$$sq_{\sharp} = \{<0 \mapsto >0,\ =0 \mapsto =0,\ >0 \mapsto >0\}$$

It turns out that $\langle sq, sq_{\sharp} \rangle$ satisfies (CGC-Cmp/$\eta\mu$), (CGC-Cmp/$\mu\mu$) and (CGC-Cmp/$\eta\eta$) but not (CGC-Cmp/$\mu\eta$). This can be easily checked on the transformed pair of functions $\mathbb{T}_{\mathrm{PGC}}(\langle sq, sq_{\sharp} \rangle) = \langle sq^{\diamond}, sq^{\diamond}_{\sharp} \rangle$ by resorting to Lemma 5.5: in fact, we have that $sq^{\diamond}_{\sharp} : \wp(B) \to \wp(B)$ is clearly both backward and forward complete (and therefore optimal) for $sq^{\diamond} : \wp(\mathbb{Z}) \to \wp(\mathbb{Z})$, while it is not precise, because $sq^{\diamond} \neq \gamma \circ sq^{\diamond}_{\sharp} \circ \alpha$. □

6 Purely Partitioning Galois Connections

Drawing on the above results, we define a novel class of constructive abstract domains, which we call purely constructive Galois connections (PCGCs). The idea is that PCGCs

generalize CGCs as follows. We have shown that CGCs may be viewed as representing a partition of the concrete carrier domain A through an abstract domain B. We proved that this view of a CGC as a partition also implicitly represents all the possible unions of its blocks. The goal here is to generalize this approach by allowing to choose which unions of blocks to consider in the abstract domain B. Hence, B may be defined as a partition P of A together with an explicit selection of unions of blocks of P, where this selection may range from none to all.

A *purely constructive Galois connection* (PCGC) $\langle \eta, A, B, \mu \rangle$ consists of a concrete unordered carrier set A and of an abstract ordered domain $\langle B, \leq \rangle$ which is required to be a poset, together with two maps $\eta : A \to B$ and $\mu : B \to \wp(A)$ which satify the following two conditions:

$$a \in \mu(\eta(a')) \;\Leftrightarrow\; \eta(a) = \eta(a') \qquad \text{(PCGC-Corr}_1\text{)}$$
$$a \in \mu(b) \;\Leftrightarrow\; \eta(a) \leq b \qquad \text{(PCGC-Corr}_2\text{)}$$

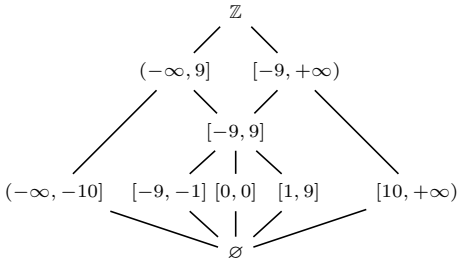
Thus, (PCGC-Corr$_2$) coincides with (CGP-Corr), while the condition (PCGC-Corr$_1$) amounts to (CGC-Corr) restricted to abstract values ranging in $\eta(A)$. PCGCs have the following properties.

Lemma 6.1 (PCGC properties). *Consider a PCGC $\langle \eta, A, B_{\leq}, \mu \rangle$.*
(1) $\eta(a_1) = \eta(a_2) \;\Leftrightarrow\; \mu(\eta(a_1)) = \mu(\eta(a_2)) \;\Leftrightarrow\; \mu(\eta(a_1)) \cap \mu(\eta(a_2)) \neq \varnothing$
(2) $\mu(b) = \varnothing \;\Rightarrow\; b \notin \eta(A)$*, while the viceversa does not hold.*
(3) *If B is a complete lattice then $\langle \eta^{\vee}, \wp(A)_{\subseteq}, B_{\leq}, \mu \rangle$ is a GC.*

In particular, let us remark that:

- by Lemma 6.1 (1), which is the same property of Lemma 3.1 (1) for CGCs, we have that $\{\mu(\eta(a))\}_{a \in A}$ still a partition of A;
- by Lemma 6.1 (2), differently from CGCs (cf. Lemma 3.1 (2)), if $b \notin \eta(A)$ it may happen that $\mu(b) \neq \varnothing$;
- by Lemma 6.1 (3), analogously to CGPs, $\eta^{\vee}$ and μ give rise to a GC, analogously to what happens for CGPs (cf. Lemma 3.3 (3)).

Example 6.2. Consider the following finite lattice B of integer intervals ordered by subset inclusion:

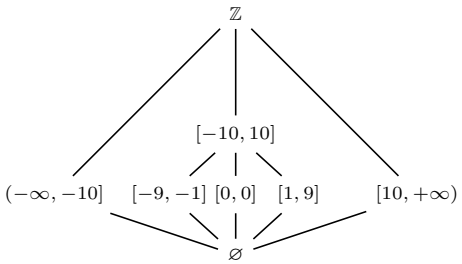


Let $\eta : \mathbb{Z} \to B$ be defined as follows:

$$\eta(x) \triangleq \begin{cases} (-\infty, -10] & \text{if } x \in (-\infty, -10] \\ [-9, -1] & \text{if } x \in [-9, -1] \\ [0, 0] & \text{if } x = 0 \\ [1, 9] & \text{if } x \in [1, 9] \\ [10, +\infty) & \text{if } x \in [10, +\infty) \end{cases}$$

while $\mu : B \to \wp(\mathbb{Z})$ is simply defined as the identity map. Then, it is simple to check that $\mathcal{P} = \langle \eta, \mathbb{Z}, B, \mu \rangle$ is a PCGC. It turns out that $\mathcal{P}$ is not a CGC: in fact, $0 \in \mu([-9, 9])$ while $\eta(0) = [0, 0] \neq [-9, 9]$, thus (CGC-Corr) does not hold. Also, if $\mathbb{Z}$ is considered as a poset w.r.t. the discrete order then $\wp^{\downarrow}(\mathbb{Z}) = \wp(\mathbb{Z})$ and η and μ are monotone functions, so that, since (PCGC-Corr$_2$) holds, $\mathcal{P}$ turns out to be a CGP as well.

Consider now the following lattice B':

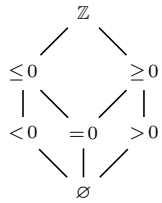


In this case, we have that $\langle \eta, \mathbb{Z}, B', \mu \rangle$ is not a PCGC, because $10 \in \mu([-10, 10])$ but $\eta(10) = [10, +\infty) \not\subseteq [-10, 10]$, so that (PCGC-Corr$_2$) does not hold. The intuition is that while B' still includes a subset which gives rise to a partition of $\mathbb{Z}$, the whole lattice B' cannot be coeherently seen as a partition representation, because $[-10, 10] \in B'$ is not the union (i.e., lub) of the blocks $[-9, -1]$, $[0, 0]$ and $[1, 9]$.

Finally, consider the CGC $\mathcal{C} = \langle \eta, \mathbb{Z}, B, \mu \rangle$ defined in Example 3.4. Then, $\mathcal{C}$ is not a PCGC because $1 \in \mu(\eta(0)) = \mathbb{Z}$ but $+ = \eta(1) \neq \eta(0) = \top$, that is, (PCGC-Corr$_1$) does not hold. □

Similarly to Theorems 4.2 and 4.7, let us now characterize PCGCs as a class of Galois connections. Recall that a GC $\mathcal{G} = \langle \alpha, \wp(A)_{\subseteq}, D_{\leq}, \gamma \rangle$ is a PGC when $\mathrm{prt}(\mathcal{G})$ is a partition of A and γ is additive. By dropping this latter requirement of additivity for γ, we define $\mathcal{G}$ to be a *purely partitioning* Galois connection (PPGC) just when $\mathrm{prt}(\mathcal{G})$ is a partition of A. The terminology "purely partitioning" hints at the property (which is not hard to check) that the disjunctive completion of D indeed yields a partitioning Galois connection.

Example 6.3. Consider the following abstract domain $\mathrm{Sign}^{\neq} \triangleq \mathrm{Sign} \setminus \{\neq 0\}$, already mentioned in Section 1:



Then, $\mathcal{S}^{\neq} = \langle \alpha, \wp(\mathbb{Z}), \mathrm{Sign}^{\neq}, \gamma \rangle$ is not a PCG because γ is not additive (in fact: $\gamma(<0) \cup \gamma(>0) \neq \gamma(<0 \ \vee \ >0) = \gamma(\mathbb{Z})$). However, $\mathrm{prt}(\mathcal{S}^{\neq}) = \{\mathbb{Z}_{<0}, \{0\}, \mathbb{Z}_{>0}\}$ still is a partition of $\mathbb{Z}$, so that $\mathcal{S}^{\neq}$ is a PPCG. □

It turns out that this class of GCs precisely characterize PCGCs as follows.

Theorem 6.4 (PCGC-PPGC Equivalence).
(1) *If $B_{\leq}$ is a complete lattice and $\mathcal{C} = \langle \eta, A, B_{\leq}, \mu \rangle$ is a PCGC then $\mathbb{T}_{\text{PPGC}}(\mathcal{C}) \triangleq \langle \eta^{\vee}, \wp(A)_{\subseteq}, B_{\leq}, \mu \rangle$ is a PPGC.*
(2) *If $\mathcal{G} = \langle \alpha, \wp(A)_{\subseteq}, D_{\leq}, \gamma \rangle$ is a PPGC then $\mathbb{T}_{\text{PCGC}}(\mathcal{G}) \triangleq \langle \alpha^{\{\}}, A, D_{\leq}, \gamma \rangle$ is a PCGC.*
(3) *The transforms $\mathbb{T}_{\text{PPGC}}$ and $\mathbb{T}_{\text{PCGC}}$ are one the inverse of the other, up to isomorphism.*

Example 6.5. Let us consider the PCGC $\mathcal{P}$ defined in Example 6.2. Then, $\mathbb{T}_{\text{PPGC}}(\mathcal{P}) = \langle \eta^{\vee}, \wp(\mathbb{Z})_{\subseteq}, B_{\leq}, \mathrm{id} \rangle$ is a purely partitioning GC where the corresponding partition of $\mathbb{Z}$ is

$$P = \{(-\infty, 10], [-9, -1], [0, 0], [1, 9], [10, +\infty)\}$$

and the abstraction map $\eta^{\vee}$ approximates a set of integers $X \in \wp(\mathbb{Z})$ by the least union of blocks of P which belongs to B: for example, $\eta^{\vee}(\{1, 10\}) = [-9, +\infty)$ and $\eta^{\vee}(\{0, 1\}) = [-9, 9]$. □

CGCs as PCGCs as CGPs. Let us show that any CGC is indeed a PCGC, which, in turn, is a CGP. Let $\langle \eta, A, B, \mu \rangle$ be a CGC. Firstly, it is enough to consider B as a poset for the discrete partial order $\leq_d$, since this makes $\langle \eta, A, B_{\leq_d}, \mu \rangle$ a PCGC. In fact: (1) $a \in \mu(\eta(a'))$ iff, by (CGC-Corr), $\eta(a) = \eta(a')$; (2) if $b \in \eta(A)$ then $b = \eta(a')$, for some a', so that, by (CGC-Corr), $a \in \mu(b) \Leftrightarrow \eta(a) = b$, while if $b \notin \eta(A)$, then, by Lemma 3.1 (2), $\mu(b) = \varnothing$. Secondly, any PCGC $\langle \eta, A, B_{\leq_B}, \mu \rangle$ can be viewed as a CGP simply by making the concrete unordered carrier set A a poset for the discrete order $\leq_d$, so that $\wp^{\downarrow}(A) = \wp(A)$, and $\eta : A \to B$ becomes trivially monotone as well as $\mu : B \to \wp(A)$: in fact, if $b_1 \leq_B b_2$ and $a \in \mu(b_1)$ then $\eta(a) \leq_B b_1 \leq_B b_2$, so that $a \in \mu(b_2)$, namely $\mu(b_1) \subseteq \mu(b_2)$.

6.1 Soundness of Abstract Operations

Let $\mathcal{C} = \langle \eta, A, B_{\leq}, \mu \rangle$ be a PCGC and $f : A \to A$ be a concrete function. By relying on Theorem 6.4 (1), we are able to define the best correct approximation of the lifted function $f^{\diamond} : \wp(A) \to \wp(A)$ w.r.t. the PPGC $\langle \eta^{\vee}, \wp(A)_{\subseteq}, B_{\leq}, \mu \rangle = \mathbb{T}_{\text{PPGC}}(\mathcal{C})$. This b.c.a. is denoted by $f_{\mathcal{C}} : B \to B$ and is therefore defined by $f_{\mathcal{C}} \triangleq \eta^{\vee} \circ f^{\diamond} \circ \mu$, so that:

$$f_{\mathcal{C}}(b) = \vee\{\eta(f(a)) \mid a \in \mu(b)\}.$$

Hence, given an abstract function $f_\sharp : B \to B$, this b.c.a. suggests to define $\langle f, f^\sharp \rangle$ to be sound for the PCGC $\mathcal{C}$ when $f_\sharp$ is less precise than the b.c.a., that is, when for any $b \in B$, $f_{\mathcal{C}}(b) \leq f_\sharp(b)$. It is easy to check that this latter condition turns out to be equivalent to the following definition: $\langle f, f^\sharp \rangle$ is sound w.r.t. $\mathcal{C}$ when

$$\eta(a) \leq b \;\Rightarrow\; \eta(f(a)) \leq f_\sharp(b) \qquad \text{(PCGC-Snd)}$$

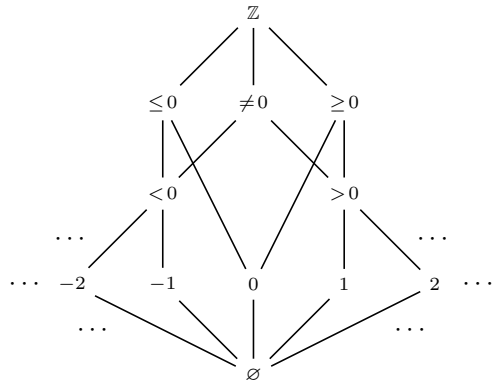
It is then easy to transform a sound pair of concrete/abstract functions $\langle f, f_\sharp \rangle$ for a PCGC $\mathcal{C}$ into a pair $\mathbb{T}_{\text{PPGC}}(\langle f, f_\sharp \rangle) \triangleq \langle f^\diamond, f_\sharp \rangle$ for the corresponding PPGC $\mathbb{T}_{\text{PPGC}}(\mathcal{C}) = \langle \eta^\vee, \wp(A)_\subseteq, B_\leq, \mu \rangle$. Conversely, if $\mathcal{D} = \langle \alpha, \wp(A)_\subseteq, D_\leq, \gamma \rangle$ is a PPGC and $\langle g^\diamond, g_\sharp \rangle$ is a sound pair for $\mathcal{D}$, where $g^\diamond : \wp(A) \to \wp(A)$ for some $g : A \to A$, then $\langle g^\diamond, g_\sharp \rangle$ is transformed into $\mathbb{T}_{\text{PCGC}}(\langle g^\diamond, g_\sharp \rangle) \triangleq \langle g, g_\sharp \rangle$ relatively to the PCGC $\mathbb{T}_{\text{PCGC}}(\mathcal{D})$. Hence, an equivalence result analogous to Theorem 5.3 can then be proved.

Theorem 6.6.
(1) *Let $\mathcal{C} = \langle \eta, A, B_\leq, \mu \rangle$ be a PCGC, with B complete lattice, $f : A \to A$ and $f_\sharp : B \to B$. Then, $\langle f, f_\sharp \rangle$ is sound iff $\mathbb{T}_{\text{PPGC}}(\langle f, f_\sharp \rangle)$ is sound w.r.t. $\mathbb{T}_{\text{PPGC}}(\mathcal{C})$.*
(2) *Let $\mathcal{D} = \langle \alpha, \wp(A)_\subseteq, D_\leq, \gamma \rangle$ be a PPGC, $g^\diamond : \wp(A) \to \wp(A)$, for some $g : A \to A$, and $g_\sharp : D \to D$. Then, $\langle g^\diamond, g_\sharp \rangle$ is sound iff $\mathbb{T}_{\text{PCGC}}(\langle g^\diamond, g_\sharp \rangle)$ is sound w.r.t. $\mathbb{T}_{\text{PCGC}}(\mathcal{D})$.*
(3) *The transforms $\mathbb{T}_{\text{PPGC}}$ and $\mathbb{T}_{\text{PCGC}}$ are one the inverse of the other.*

Since $f_\sharp$ is defined to be sound when $\eta^\vee \circ f^\diamond \circ \mu \sqsubseteq f_\sharp$ holds, it is then natural to define $f_\sharp$ to be optimal when $\eta^\vee \circ f^\diamond \circ \mu = f_\sharp$, backward complete when $\eta^\vee \circ f^\diamond = f_\sharp \circ \eta^\vee$ and forward complete when $f^\diamond \circ \mu = \mu \circ f_\sharp$. In particular, these definitions allow us to apply the abstraction refinement operators introduced in [14] for minimally refining the abstract domain B in order to obtain a backward/forward complete abstract function and the technique introduced in [12,13] for simplifying abstract domains while retaining the optimality of abstract operations.

6.2 An Example of PCGC

Consider the following infinite complete lattice $\langle B, \leq \rangle$.



B is intended to be an abstract domain which includes both constant and sign information of an integer variable. Indeed B can be defined as the well-known reduced product [5] of the standard constant propagation domain [19] and of the abstraction Sign in Example 4.1. For example, for a while program such as:

$$x := 2; y := 2; \ \textbf{while}\ x < 9\ \textbf{do}\ x := x * y;$$

a standard analysis with this abstract domain B allows us to derive the loop invariant $\{x > 0,\ y = 2\}$.

It turns out that the abstraction B can be constructively defined. This definition of B relies on $\eta : \mathbb{Z} \to B$ and $\mu : B \to \wp(\mathbb{Z})$ which are essentially defined as identity functions. It should be clear that B is a purely partitioning domain, while it is not a fully partitioning domain, and therefore B cannot be equivalently defined by a constructive Galois connection. In fact, $\mathcal{C} = \langle \eta, \mathbb{Z}, B, \mu \rangle$ is not a CGC, because $1 \in \mu(>0)$ while $1 = \eta(1) \not> 0$, so that (CGC-Corr) does not hold. Instead, $\mathcal{C}$ turns out to be a PCGC.

Consider the concrete binary integer multiplication $\otimes : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. By following Theorem 6.6 (1), we define a corresponding abstract multiplication $\otimes_\sharp : B \times B \to B$ as follows:

$$\otimes_\sharp(b_1, b_2) \triangleq \eta^\vee(\otimes^\diamond(\mu(b_1), \mu(b_2))$$

This means that $\otimes_\sharp$ is defined as best correct approximation of the powerset lifting $\otimes^\diamond : \wp(\mathbb{Z}) \times \wp(\mathbb{Z}) \to \wp(\mathbb{Z})$ w.r.t. the PPGC $\langle \eta^\vee, \wp(\mathbb{Z})_\subseteq, B_\leq, \mu \rangle = \mathbb{T}_{\text{PPGC}}(\mathcal{C})$, i.e., $\otimes_\sharp = \eta^\vee \circ \otimes^\diamond \circ \mu$. For instance, we have that $\otimes_\sharp(2, <0) = <0$ and $\otimes_\sharp(-2, \leq 0) = \geq 0$. Then, since $\langle \otimes^\diamond, \otimes_\sharp \rangle$ is sound, by construction, for $\mathbb{T}_{\text{PPGC}}(\mathcal{C})$, we have that $\langle \otimes, \otimes_\sharp \rangle$ is sound for $\mathcal{C}$. Furthermore, as expected, it turns out that $\otimes_\sharp$ is backward complete for $\mathcal{C}$, meaning that for any $X, Y \in \wp(\mathbb{Z})$, $\vee_B\{x \otimes y \mid x \in X, y \in Y\} = \otimes_\sharp(\vee_B X, \vee_B Y)$. For instance, we have that:

$$\vee_B\,(\otimes^\diamond(\{2,4\},\{-1,0\})) = \vee_B\{0,-2,-4\} = \leq 0\ = \\ \otimes_\sharp\,(>0,\leq 0) = \otimes_\sharp(\vee_B\{2,4\}, \vee_B\{-1,0\}).$$

7 Conclusion

This paper showed that constructive Galois connections, proposed by Darais and Van Horn [10] as a way to define domains to be used in a mechanized and calculational approach to abstract interpretation, are mathematically isomorphic to an already known class of Galois connections which formalize partitions of an unordered set as an abstract domain. Building on that, we defined a novel class of constructive abstract domains, called purely constructive Galois connections. We showed that this class of abstract domains permits to represent a set partition in a flexible way while preserving a constructive approach to Galois connections.

References

1. S. Blazy, V. Laporte, A. Maroneze, D. Pichardie. Formal verification of a C value analysis based on abstract interpretation. In *Proc. of the 20th International Static Analysis Symposium (SAS'13)*, Springer LNCS 7935, pp. 324-344, 2013.

2. P. Cousot. The calculational design of a generic abstract interpreter. In M. Broy and R. Steinbrüggen, eds, *Calculational System Design*, NATO ASI Series F. IOS Press, Amsterdam, 1999.
3. P. Cousot. Constructive design of a hierarchy of semantics of a transition system by abstract interpretation. *Theor. Comput. Sci.*, 277(1-2):47–103, 2002.
4. P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Proc. 4th ACM POPL*, pp. 238-252, 1977.
5. P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Proc. 6th ACM POPL*, pp. 269-282, 1979.
6. P. Cousot and R. Cousot. Abstract interpretation frameworks. *J. Logic and Computation*, 2(4):511-547, 1992.
7. P. Cousot and R. Cousot. Higher-order abstract interpretation (and application to comportment analysis generalizing strictness, termination, projection and PER analysis of functional languages) (Invited Paper). In *Proc. of the IEEE Int. Conf. on Computer Languages (ICCL'94)*, pp. 95-112. IEEE Computer Society Press, 1994.
8. P. Cousot and R. Cousot. Abstract interpretation of algebraic polynomial systems. In *Proceedings of the 6th International Conference on Algebraic Methodology and Software Technology (AMAST'97)*, LNCS 1349, pp. 138-154, 1997.
9. P. Cousot and N. Halbwachs. Automatic discovery of linear restraints among variables of a program. In *Proc. 5th ACM POPL*, pp. 84-97, 1978.
10. D. Darais and D. Van Horn. Constructive Galois connections: taming the Galois connection framework for mechanized metatheory. In *Proceedings of the 21st ACM Intern. Conf. on Functional Programming (ICFP'16)*. ACM, pp. 311-324, 2016.
11. R. Giacobazzi and F. Ranzato. Optimal domains for disjunctive abstract interpretation. *Sci. Comp. Program.*, 32:177-210, 1998.
12. R. Giacobazzi and F. Ranzato. Example-guided abstraction simplification. In *Proc. 37th Intern. Colloq. on Automata, Languages and Programming (ICALP'10)*, LNCS 6199, pp. 211-222, Springer, 2010.
13. R. Giacobazzi and F. Ranzato. Correctness kernels of abstract interpretations. *Information and Computation*, 237:187-203, 2014.
14. R. Giacobazzi, F. Ranzato and F. Scozzari. Making abstract interpretations complete. *J. ACM*, 47(2):361-416, 2000.
15. J.H. Jourdan. *Verasco: a Formally Verified C Static Analyzer*. PhD thesis, Université Paris Diderot (Paris 7), France, 2016.
16. J.H. Jourdan, V. Laporte, S. Blazy, X. Leroy, D. Pichardie. A formally-verified C static analyzer. In *Proc. 42nd ACM POPL*, pp. 247-259, 2015.
17. J. Midtgaard and T. Jensen. A calculational approach to control-flow analysis by abstract interpretation. In *Proc. 15th Intern. Static Analysis Symposium (SAS'08)*, LNCS 5079, pp. 347-362, Springer, 2008.
18. D. Monniaux. *Réalisation Mécanisée d'Interpréteurs Abstraits*. Rapport de DEA, Université Paris VII, France, 1998. In French.
19. F. Nielson, H.R. Nielson, C. Hankin. *Principles of Program Analysis*. Springer-Verlag, 1999.
20. D. Pichardie. *Interprétation Abstraite en Logique Intuitionniste: Extraction d'Analyseurs Java Certifiés*. PhD thesis, Université de Rennes, France, 2005. In French.
21. F. Ranzato and F. Tapparo. Strong preservation as completeness in abstract interpretation. In *Proc. 13th European Symposium on Programming (ESOP'04)*, LNCS. 2986, pp. 18–32, Springer, 2004.
22. F. Ranzato and F. Tapparo. An abstract interpretation-based refinement algorithm for strong preservation. In *Proc. 11th Intern. Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'05)*, LNCS 3440, pp. 140–156, Springer, 2005.

23. F. Ranzato and F. Tapparo. Generalized strong preservation by abstract interpretation. *J. Logic and Computation*, 17(1):157-197, 2007.
24. P.F. Silva and J.N. Oliveira. 'Galculator': Functional prototype of a Galois-connection based proof assistant. In *Proc. 10th International ACM Conference on Principles and Practice of Declarative Programming (PPDP'08)*, pp. 44-55, ACM, 2008.