A Galois Connection Calculus for Abstract Interpretation*

Patrick Cousot
CIMS**, NYU, USA pcousot@cims.nyu.edu

Radhia Cousot
CNRS Emeritus, ENS, France rcousot@ens.fr

Abstract We introduce a Galois connection calculus for language independent specification of abstract interpretations used in programming language semantics, formal verification, and static analysis. This Galois connection calculus and its type system are typed by abstract interpretation.

Categories and Subject Descriptors D.2.4 [*Software/Program Verification*]
General Terms Algorithms, Languages, Reliability, Security, Theory, Verification.
Keywords Abstract Interpretation, Galois connection, Static Analysis, Verification.

1. Galois connections in Abstract Interpretation

In *Abstract interpretation* [3, 4, 6, 7] concrete properties (for example (*e.g.*) of computations) are related to abstract properties (*e.g.* types). The abstract properties are always *sound* approximations of the concrete properties (abstract proofs/static analyzes are always correct in the concrete) and are sometimes *complete* (proofs/analyzes of abstract properties can all be done in the abstract only). *E.g.* types are sound but incomplete [2] while abstract semantics are usually complete [9]. The *concrete domain* $\langle\mathcal{C},\ \sqsubseteq\rangle$ and *abstract domain* $\langle\mathcal{A},\ \preccurlyeq\rangle$ of properties are posets (partial orders being interpreted as implication). When concrete properties all have a $\preccurlyeq$-most precise abstraction, the correspondence is a *Galois connection* (*GC*) $\langle\mathcal{C},\ \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle\mathcal{A},\ \preccurlyeq\rangle$ with *abstraction* $\alpha \in \mathcal{C} \mapsto \mathcal{A}$ and *concretization* $\gamma \in \mathcal{A} \mapsto \mathcal{C}$ satisfying $\forall P \in \mathcal{C} : \forall Q \in \mathcal{A} : \alpha(x) \preccurlyeq y \Leftrightarrow x \sqsubseteq \gamma(y)$ ($\Rightarrow$ expresses soundness and $\Leftarrow$ best abstraction). Each adjoint α/γ uniquely determines the other γ/α. A *Galois retraction* (or *insertion*) has α onto, so γ is one-to-one, and $\alpha \circ \gamma$ is the identity. *E.g.* the *interval abstraction* [3, 4] of the power set $\wp(C)$ of complete $\leq$-totally ordered sets $C \cup \{-\infty, \infty\}$ is $\mathcal{S}[\![\mathbb{I}[\langle C,\ \leq\rangle, -\infty, \infty]]\!] \triangleq \langle\wp(C), \subseteq\rangle \xleftrightarrow[\alpha^{\mathbb{I}}]{\gamma^{\mathbb{I}}} \langle\mathbb{I}(C\cup\{-\infty,\infty\},\leq), \Subset\rangle$ with $\alpha^{\mathbb{I}}(X) \triangleq [\min X, \max X]$, $\min\emptyset \triangleq \infty$, $\max\emptyset \triangleq -\infty$, $\gamma^{\mathbb{I}}([a,b]) \triangleq \{x \in C \mid a \leq x \leq b\}$, intervals $\mathcal{S}[\![\mathbb{I}(C \cup \{-\infty,\infty\}, \leq)]\!] \triangleq \{[a,b] \mid a \in C \cup \{-\infty\} \wedge b \in C \cup \{\infty\} \wedge a \leq b\} \cup \{[\infty, -\infty]\}$, and inclusion $[a,b] \Subset [c,d] \triangleq c \leq a \wedge b \leq d$. A *Galois isomorphism* $\langle\mathcal{C}, \subseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle\mathcal{A}, \preccurlyeq\rangle$ has both α and γ bijective. *E.g.* global and local invariants are isomorphic by the *right image abstraction* $\mathcal{S}[\![\curvearrowright[\mathbb{L},\mathcal{M}]]\!] \triangleq \langle\wp(\mathbb{L}\times\mathcal{M}), \subseteq\rangle \xleftrightarrow[\alpha^{\curvearrowright}]{\gamma^{\curvearrowright}} \langle\mathbb{L} \mapsto \wp(\mathcal{M}),\ \dot{\subseteq}\rangle$ with $\alpha^{\curvearrowright}(P) \triangleq \boldsymbol{\lambda}\,\ell \bullet \{m \mid \langle\ell,\ m\rangle \in P\}$, $\gamma^{\curvearrowright}(Q) \triangleq \{\langle\ell,\ m\rangle \mid m \in Q(\ell)\}$, and $\dot{\subseteq}$ is the pointwise extension of inclusion $\subseteq$.

2. Equivalent formalizations of *GC*-based Abstract Interpretation

GCs $\langle\mathcal{C}, \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle\mathcal{A}, \preccurlyeq\rangle$ are Galois retracts of/Galois isomorphic to numerous equivalent mathematical structures [6] such as *join-preserving maps* (α), *meet-preserving maps* (γ), *upper-closures* ($\gamma \circ \alpha$), *Moore families* ($\{\gamma(Q) \mid Q \in \mathcal{A}\}$), *Sierpiński topologies* [5] ($\{\neg\gamma(Q) \mid Q \in \mathcal{A}\}$ where $\neg$ is unique complementation in the concrete domain $\mathcal{C}$, if any), *principal downset families* ($\{\downarrow^{\sqsubseteq}\gamma(Q) \mid Q \in \mathcal{A}\}$ where $\downarrow^{\sqsubseteq}x \triangleq \{y \in \mathcal{C} \mid y \sqsubseteq x\}$), *maximal convex congruences* ($\{\{P \in \mathcal{C} \mid \alpha(P) = \alpha(\gamma(Q))\} \mid Q \in \mathcal{A}\}$, *soundness relations* (also called *abstraction relation*, *logical relation*, or *tensor product*, $\alpha \mathbin{⨾} \preccurlyeq = \{\langle P,\ Q\rangle \mid \alpha(P) \preccurlyeq Q\} = \{\langle P,\ Q\rangle \mid P \sqsubseteq \gamma(Q)\} = \sqsubseteq \mathbin{⨾} \gamma^{-1}$ where $f \equiv \{\langle x,\ f(x)\rangle \mid x \in \mathsf{dom}(f)\}$, $r \mathbin{⨾} r' = \{\langle x,\ z\rangle \mid \exists y : \langle x,\ y\rangle \in r \wedge \langle y,\ z\rangle \in r'\}$), and, for powersets $\mathcal{C} = \wp(C)$, $\mathcal{A} = \wp(A)$, *polarities* of relations ($\gamma(Q) = \{x \in C \mid \forall y \in Q : R(x,y)\}$ where $R = \{\langle x,\ y\rangle \mid x \in \gamma(\{y\})\}$).

3. Basic *GC* semantics

Basic *GCs* are primitive abstractions of properties. Classical examples are the *identity abstraction* $\mathcal{S}[\![\mathbb{1}[\langle\mathcal{C},\ \sqsubseteq\rangle]]\!] \triangleq \langle\mathcal{C},\ \sqsubseteq\rangle \xleftrightarrow[\boldsymbol{\lambda}\,P\bullet P]{\boldsymbol{\lambda}\,Q\bullet Q} \langle\mathcal{C},\ \sqsubseteq\rangle$, the *top abstraction* $\mathcal{S}[\![\top[\langle\mathcal{C},\ \sqsubseteq\rangle, \top]]\!] \triangleq \langle\mathcal{C},\ \sqsubseteq\rangle \xleftrightarrow[\boldsymbol{\lambda}\,P\bullet\top]{\boldsymbol{\lambda}\,Q\bullet\top} \langle\mathcal{C}, \sqsubseteq\rangle$, the *join abstraction* $\mathcal{S}[\![\cup[C]]\!] \triangleq \langle\wp(\wp(C)), \subseteq\rangle \xleftrightarrow[\alpha^{\wp}]{\gamma^{\wp}} \langle\wp(C), \subseteq\rangle$ with $\alpha^{\wp}(P) \triangleq \bigcup P$, $\gamma^{\wp}(Q) \triangleq \wp(Q)$, the *complement abstraction* $\mathcal{S}[\![\neg[C]]\!] \triangleq \langle\wp(C),\ \subseteq\rangle \xleftrightarrow[\neg]{\neg} \langle\wp(C),\ \supseteq\rangle$, the finite/infinite *sequence abstraction* $\mathcal{S}[\![\infty[C]]\!] \triangleq \langle\wp(C^{\infty}), \subseteq\rangle \xleftrightarrow[\alpha^{\infty}]{\gamma^{\infty}} \langle\wp(C), \subseteq\rangle$ with $\alpha^{\infty}(P) \triangleq \{\sigma_i \mid \sigma \in P \wedge i \in \mathsf{dom}(\sigma)\}$ and $\gamma^{\infty}(Q) \triangleq \{\sigma \in C^{\infty} \mid \forall i \in \mathsf{dom}(\sigma) : \sigma_i \in Q\}$, the *transformer abstraction* $\mathcal{S}[\![\rightsquigarrow[C_1, C_2]]\!] \triangleq \langle\wp(C_1\times C_2), \subseteq\rangle \xleftrightarrow[\alpha^{\rightsquigarrow}]{\gamma^{\rightsquigarrow}} \langle\wp(C_1) \xrightarrow{\cup} \wp(C_2),\ \dot{\subseteq}\rangle$ mapping relations to join-preserving transformers with $\alpha^{\rightsquigarrow}(R) \triangleq \boldsymbol{\lambda}\,X\bullet\{y \mid \exists x \in X : \langle x,\ y\rangle \in R\}$, $\gamma^{\rightsquigarrow}(g) \triangleq \{\langle x,\ y\rangle \mid y \in g(\{x\})\}$, the *function abstraction* $\mathcal{S}[\![\mapsto[C_1, C_2]]\!] \triangleq \langle\wp(C_1 \mapsto C_2),\ \subseteq\rangle \xleftrightarrow[\alpha^{\mapsto}]{\gamma^{\mapsto}} \langle\wp(C_1) \mapsto \wp(C_2),\ \dot{\subseteq}\rangle$ with $\alpha^{\mapsto}(P) \triangleq \boldsymbol{\lambda}\,X\bullet\{f(x) \mid f \in P \wedge x \in X\}$, $\gamma^{\mapsto}(g) \triangleq \{f \in C_1 \mapsto C_2 \mid \forall X \in \wp(C_1) : \forall x \in X : f(x) \in g(X)\}$, the *cartesian abstraction* $\mathcal{S}[\![\times[I, C]]\!] \triangleq \langle\wp(I \mapsto C),\ \subseteq\rangle \xleftrightarrow[\alpha^{\times}]{\gamma^{\times}} \langle I \mapsto \wp(C),\ \dot{\subseteq}\rangle$ with $\alpha^{\times}(X) \triangleq \boldsymbol{\lambda}\,i \in I\bullet\{x \in C \mid \exists f \in I \mapsto C : f[i \leftarrow x] \in X\}$, $\gamma^{\times}(Y) \triangleq \{f \mid \forall i \in I : f(i) \in Y(i)\}$, and the pointwise extension $\dot{\subseteq}$ of $\subseteq$ to I, *etc.*

4. Galois connector semantics

Galois connectors build a *GC* from *GCs* provided as parameters. Unary Galois connectors include the *reduction connector* $\mathcal{S}[\![\mathsf{R}[\langle\mathcal{C},\ \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle\mathcal{A},\ \preccurlyeq\rangle]]\!] \triangleq \langle\mathcal{C},\ \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle\{\alpha(P) \mid P \in \mathcal{C}\},\ \preccurlyeq\rangle$ and the *pointwise connector* $\mathcal{S}[\![X \rightarrow \langle C,\ \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle A,\ \preccurlyeq\rangle]\!] \triangleq \langle X \mapsto C,\ \dot{\sqsubseteq}\rangle \xleftrightarrow[\boldsymbol{\lambda}\,\rho\bullet\alpha\circ\rho]{\boldsymbol{\lambda}\,\overline{\rho}\bullet\gamma\circ\overline{\rho}} \langle X \mapsto A,\ \dot{\preccurlyeq}\rangle$ for the pointwise orderings $\dot{\sqsubseteq}$ and $\dot{\preccurlyeq}$. Binary Galois connectors include the *composition connector* $\mathcal{S}[\![\langle\mathcal{C}, \subseteq\rangle \xleftrightarrow[\alpha_1]{\gamma_1} \langle\mathcal{A}_1, \Subset\rangle \mathbin{⨾} \langle\mathcal{A}_2, \sqsubseteq\rangle \xleftrightarrow[\alpha_2]{\gamma_2} \langle\mathcal{A}_3, \preccurlyeq\rangle]\!] \triangleq (\!|\langle\mathcal{A}_1, \Subset\rangle = \langle\mathcal{A}_2, \sqsubseteq\rangle \mathrel{?} \langle\mathcal{C},\ \subseteq\rangle \xleftrightarrow[\alpha_2\circ\alpha_1]{\gamma_1\circ\gamma_2} \langle\mathcal{A}_3,\ \preccurlyeq\rangle \mathrel{:} \Omega|\!)$ (where Ω is a static error), the *product connector* $\mathcal{S}[\![\langle\mathcal{C}_1,\ \subseteq\rangle \xleftrightarrow[\alpha_1]{\gamma_1} \langle\mathcal{A}_1,\ \sqsubseteq\rangle \circledast \langle\mathcal{C}_2,\ \Subset\rangle \xleftrightarrow[\alpha_2]{\gamma_2} \langle\mathcal{A}_2,\ \preccurlyeq\rangle]\!] \triangleq \langle\mathcal{C}_1 \times \mathcal{C}_2,\ \subseteq \times \Subset\rangle \xleftrightarrow[\alpha_1\times\alpha_2]{\gamma_1\times\gamma_2} \langle\mathcal{A}_1 \times \mathcal{A}_2,\ \sqsubseteq \times \preccurlyeq\rangle$ (generalizing to tuples), the higher-order *functional connector* $\mathcal{S}[\![\langle\mathcal{C}_1,\ \subseteq\rangle \xleftrightarrow[\alpha_1]{\gamma_1} \langle\mathcal{A}_1,\ \sqsubseteq\rangle \Longrightarrow \langle\mathcal{C}_2,\ \preccurlyeq\rangle \xleftrightarrow[\alpha_2]{\gamma_2} \langle\mathcal{A}_2,\ \leqslant\rangle]\!] \triangleq \langle\mathcal{C}_1 \xrightarrow{\nearrow} \mathcal{C}_2,\ \dot{\preccurlyeq}\rangle \xleftrightarrow[\boldsymbol{\lambda}\,f\bullet\alpha_2\circ f\circ\gamma_1]{\boldsymbol{\lambda}\,g\bullet\gamma_2\circ g\circ\alpha_1} \langle\mathcal{A}_1 \xrightarrow{\nearrow} \mathcal{A}_2,\ \dot{\leqslant}\rangle$ for increasing maps and pointwise orderings $\dot{\sqsubseteq}$ and $\dot{\leqslant}$.

5. Galois connection calculus

The *GC* calculus $\mathbb{G}$ (to specify verifiers/analyzers compositionally) is $\mathtt{x}, \ldots \in \mathbb{X}$ for program variables, $\ell, \ldots \in \mathbb{L}$ for labels, $e \in \mathbb{E}$ for elements $e ::= \mathsf{true} \mid 1 \mid \infty \mid \mathtt{x} \mid \ell \mid -e \mid \ldots$, $s \in \mathbb{S}$ for sets $s ::= \mathbb{B} \mid \mathbb{Z} \mid \mathbb{X} \mid \mathbb{L} \mid \{e\} \mid [e, e] \mid \mathbb{I}(s, o) \mid s^{\infty} \mid s \cup s \mid s \mapsto s \mid s \times s \mid \wp(s) \mid \ldots$, $o \in \mathbb{O}$ for partial orders $o ::= \Rightarrow \mid \Leftrightarrow \mid \leq \mid \subseteq \mid \Subset \mid = \mid o^{-1} \mid o_1 \times o_2 \mid \dot{o} \mid \ddot{o} \mid \ldots$, $p \in \mathbb{P}$ for posets $p ::= \langle s,\ o\rangle$, and $g \in \mathbb{G}$ for *GCs* $g ::= \mathbb{1}[p] \mid \top[p, e] \mid \mathbb{I}[p, e, e] \mid \curvearrowright[s, s] \mid \cup[s] \mid \neg[s] \mid \infty[s] \mid \rightsquigarrow[s, s] \mid \mapsto[s, s] \mid \times[s, s] \mid \ldots \mid \mathsf{R}[g] \mid s \rightarrow g \mid g \mathbin{⨾} g \mid g \circledast g \mid g \Longrightarrow g \mid \ldots$. The semantics of interval sets is $\mathcal{S}[\![\mathbb{I}(C, \preccurlyeq)]\!] \triangleq (\!|\preccurlyeq \subseteq C \times C \mathrel{?} \{[a, b]_{\preccurlyeq} \mid a, b \in C\} \mathrel{:} \omega|\!)$ where ω is a dynamic error (maybe not detectable by typing).

---

* See the auxiliary materials. ** Work supported in part by the CMACS NSF award 0926166.

POPL '14, January 22–24, 2014, San Diego, CA, USA. Copyright is held by the owner/author(s).
ACM 978-1-4503-2544-8/14/01. http://dx.doi.org/10.1145/2535838.2537850

6. Abstraction Papers in semantics, verification, and static analysis can be understood by extracting the semantic domain and *GC* which are used. For the interval example [3, 4, p. 247], the semantic domain $\mathcal{S} \triangleq \wp(\Sigma^\infty)$ is that of (nonempty) sets of nonempty finite or infinite sequences of states in $\Sigma \triangleq \mathbb{L} \times \mathcal{M}$ made of a control state in $\mathbb{L}$ and a memory state in $\mathcal{M} \triangleq \mathbb{X} \mapsto \mathcal{V}$ mapping variables $\mathbb{X}$ to a complete total order $\langle \mathcal{V},\ \leq \rangle$ (*e.g.* $\langle \mathbb{Z}, \leqslant \rangle$ or $\langle [\mathtt{minint}, \mathtt{maxint}],\ \leqslant \rangle$). The *static* (or *collecting*) *semantics* is the *reachability abstraction* of program properties in $\wp(\mathcal{S})$ that is $G^* \triangleq \cup[\Sigma^\infty] \fatsemi \infty[\Sigma] \fatsemi \curvearrowright[\mathbb{L}, \mathcal{M}]$ with abstract domain $\langle \mathbb{L} \mapsto \wp(\mathcal{M}),\ \dot{\subseteq} \rangle$. The *reduced interval cartesian reachability abstraction* is $G^{\mathfrak{I}^*} \triangleq \mathsf{R}[G^* \fatsemi (\mathbb{L} \rightarrowtriangle (\times[\mathbb{X}, \mathcal{V}] \fatsemi (\mathbb{X} \rightarrowtriangle \mathbb{I}[\langle \mathcal{V},\ \leq \rangle, -\infty, \infty])))]$ that is the abstraction $\langle \wp(\wp((\mathbb{L} \times (\mathbb{X} \mapsto \mathcal{V}))^\infty)),\ \subseteq \rangle \xrightleftharpoons[\alpha]{\gamma} \langle \mathbb{L} \mapsto \mathbb{X} \mapsto \mathbb{I}(\mathcal{V} \cup \{-\infty, \infty\}),\ \ddot{\sqsubseteq} \rangle$ where $\alpha(P) \triangleq \boldsymbol{\lambda}\, \ell \bullet \mathsf{smash}(\boldsymbol{\lambda}\, \mathtt{x} \bullet \alpha^{\mathbb{I}}(\alpha^{\times}((\alpha^{\curvearrowright}(\alpha^{\infty}(\alpha^{\wp}(P))))(\ell))(\mathtt{x})))$ and $\mathsf{smash}(\boldsymbol{\lambda}\, \mathtt{x} \in \mathbb{X} \bullet [a_{\mathtt{x}}, b_{\mathtt{x}}])$ reduces to $\boldsymbol{\lambda}\, \mathtt{x} \in \mathbb{X} \bullet [\infty, -\infty]$ when some $[a_{\mathtt{x}}, b_{\mathtt{x}}]$ is the empty interval $[\infty, -\infty]$ else to $\boldsymbol{\lambda}\, \mathtt{x} {\in} \mathbb{X} \bullet [a_{\mathtt{x}}, b_{\mathtt{x}}]$.

7. Typing As usual with syntactic definitions, *GC* expression semantics may be undefined (*i.e.* Ω or ω). This can be fixed for Ω by a type system that is an Abstract Interpretation of the properties $\wp(\mathfrak{Gc})$ of the semantics $\mathcal{S}\llbracket g \rrbracket \in \mathfrak{Gc}$ of expressions $g \in \mathbb{G}$ belonging to the class $\mathfrak{Gc} \triangleq \{\langle \mathcal{C}, \sqsubseteq \rangle \xrightleftharpoons[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq \rangle \mid \mathcal{C}, \mathcal{A}$ are sets $\wedge \sqsubseteq \in \wp(\mathcal{C} \times \mathcal{C}) \wedge \preccurlyeq \in \wp(\mathcal{A} \times \mathcal{A})\} \cup \{\Omega, \omega\}$. Typing is formalized by a *GC* [2] $\langle \wp(\mathfrak{Gc}),\ \subseteq \rangle \xrightleftharpoons[\alpha^{\mathfrak{T}}]{\gamma^{\mathfrak{T}}} \langle \mathfrak{T}_{/\cong},\ \trianglelefteq \rangle$ where the preorder on types is $\mathsf{T} \trianglelefteq \mathsf{T}' \triangleq \gamma^{\mathfrak{T}}(\mathsf{T}) \subseteq \gamma^{\mathfrak{T}}(\mathsf{T}')$ so that types $\mathfrak{T}_{/\cong}$ are considered up to the equivalence $\cong$ for this preorder $\trianglelefteq$ ($\cong$ is $=$ when $\gamma^{\mathfrak{T}}$ is injective). In absence of a $\trianglelefteq$-most precise *i.e.* principal type, hence of a best abstraction $\alpha^{\mathfrak{T}}$, as *e.g.* in [15] for the polyhedral abstraction, only one of α or γ is used [7]. A *GC* expression $g \in \mathbb{G}$ has sound types $\mathsf{T} \in \mathfrak{T}$ such that $\{\mathcal{S}\llbracket g \rrbracket\} \subseteq \gamma^{\mathfrak{T}}(\mathsf{T})$ *i.e.* $\mathcal{S}\llbracket g \rrbracket \in \gamma^{\mathfrak{T}}(\mathsf{T})$ or $\rho^{\mathfrak{Gc}}(\mathcal{S}\llbracket g \rrbracket, \mathscr{T}\llbracket g \rrbracket)$ for the soundness relation $\rho^{\mathfrak{Gc}}(S, T) \triangleq S \in \gamma^{\mathfrak{T}}(T)$. For *GCs*, this is equivalent to $\alpha^{\mathfrak{T}}(\{\mathcal{S}\llbracket g \rrbracket\}) \trianglelefteq \mathsf{T}$, where $\{\mathcal{S}\llbracket g \rrbracket\}$ is the strongest property (collecting semantics) of g and $\alpha^{\mathfrak{T}}(\{\mathcal{S}\llbracket g \rrbracket\})$ is the best abstraction of g. The type soundness proof is by induction on the structure of the *GC* expressions as in [2] (instead of operational subject reduction *i.e.* induction on program computation steps).

8. Types For elements $\mathsf{E} \in \mathfrak{E}$, $\mathsf{E} ::= \mathtt{var} \mid \mathtt{lab} \mid \mathtt{bool} \mid \mathtt{int} \mid \mathtt{err}$ with $\gamma^{\mathfrak{E}}(\mathtt{int}) \triangleq \mathbb{Z} \cup \{-\infty, \infty\}$, $\gamma^{\mathfrak{E}}(\mathtt{err}) \triangleq \mathcal{S}(\mathbb{E}) \cup \{\Omega, \omega\}$.

For sets $\mathsf{S} \in \mathfrak{S}$, $\mathsf{S} ::= \mathtt{P}\ \mathsf{E} \mid \mathtt{P}\ \mathsf{S} \mid \mathtt{seq}\ \mathsf{S} \mid \mathsf{S} \ast\!\!\longleftrightarrow \mathsf{S} \mid \mathsf{S} \ast \mathsf{S} \mid \mathtt{err}$ with $\gamma^{\mathfrak{S}}(\mathtt{P}\ \mathsf{E}) \triangleq \wp(\gamma^{\mathfrak{E}}(\mathsf{E}))$, $\gamma^{\mathfrak{S}}(\mathtt{P}\ \mathsf{S}) \triangleq \wp(\gamma^{\mathfrak{S}}(\mathsf{S}))$, $\gamma^{\mathfrak{S}}(\mathtt{seq}\ \mathsf{S}) \triangleq \{X^\infty \mid X \in \gamma^{\mathfrak{S}}(\mathsf{S})\}$, $\gamma^{\mathfrak{S}}(\mathsf{S}_1 \ast\!\!\longleftrightarrow \mathsf{S}_2) \triangleq \{X \mapsto Y \mid X \in \gamma^{\mathfrak{S}}(\mathsf{S}_1) \wedge Y \in \gamma^{\mathfrak{S}}(\mathsf{S}_2)\}$, $\gamma^{\mathfrak{S}}(\mathsf{S}_1 \ast \mathsf{S}_2) \triangleq \{X \times Y \mid X \in \gamma^{\mathfrak{S}}(\mathsf{S}_1) \wedge Y \in \gamma^{\mathfrak{S}}(\mathsf{S}_2)\}$, $\gamma^{\mathfrak{S}}(\mathtt{err}) \triangleq \mathcal{S}(\mathbb{S}) \cup \{\Omega, \omega\}$.

For partial orders $\mathsf{O} \in \mathfrak{O}$, $\mathsf{O} ::= \Rightarrow \mid \Leftrightarrow \mid \leq \mid \subseteq \mid = \mid \mathsf{O}^{-1} \mid \mathsf{O} {\star} \mathsf{O} \mid \dot{\mathsf{O}} \mid \ldots \mid \mathtt{err}$ with $\gamma^{\mathfrak{O}}(\mathsf{O}) \triangleq \{\mathsf{O}\}$, $\mathsf{O} \in \{\Rightarrow, \Leftrightarrow, \leq, \subseteq, =\}$, $\Rightarrow \triangleq \{\langle \mathsf{false},\ \mathsf{false} \rangle, \langle \mathsf{true},\ \mathsf{true} \rangle\}$, *etc.*

For posets $\mathsf{P} \in \mathfrak{P}$, $\mathsf{P} ::= \mathsf{S} \circledast \mathsf{O} \mid \mathtt{err}$ with componentwise concretization $\gamma^{\mathfrak{P}}(\mathsf{S} \circledast \mathsf{O}) \triangleq \gamma^{\mathfrak{S}}(\mathsf{S}) \times \gamma^{\mathfrak{O}}(\mathsf{O})$.

For *GCs*, $\mathsf{T} \in \mathfrak{T}$, $\mathsf{T} ::= \mathsf{P} \leftrightarrows \mathsf{P} \mid \mathsf{S} \ast\!\!\rightarrowtriangle \mathsf{T} \mid \mathtt{err}$ with $\gamma^{\mathfrak{T}}(\mathsf{P} \leftrightarrows \mathsf{P}') \triangleq \{P \xrightleftharpoons[\alpha]{\gamma} P' \mid P \in \gamma^{\mathfrak{P}}(\mathsf{P}) \wedge P' \in \gamma^{\mathfrak{P}}(\mathsf{P}')\}$ and $\gamma^{\mathfrak{T}}(\mathsf{S} \ast\!\!\rightarrowtriangle \mathsf{T}) \triangleq \{\langle X \mapsto \mathcal{C},\ \dot{\sqsubseteq} \rangle \xrightleftharpoons[\alpha']{\gamma'} \langle X \mapsto \mathcal{A},\ \dot{\preccurlyeq} \rangle \mid X \in \gamma^{\mathfrak{S}}(\mathsf{S}) \wedge \langle \mathcal{C},\ \sqsubseteq \rangle \xrightleftharpoons[\alpha]{\gamma} \langle \mathcal{A},\ \preccurlyeq \rangle \in \gamma^{\mathfrak{T}}(\mathsf{T})\}$.

9. Type inference The type inference algorithm is $\mathscr{E}\llbracket \mathsf{true} \rrbracket \triangleq \mathtt{bool}, \ldots, \mathscr{E}\llbracket -e \rrbracket \triangleq \llparenthesis \mathscr{E}\llbracket e \rrbracket = \mathtt{bool} \vee \mathscr{E}\llbracket e \rrbracket = \mathtt{int} \mathrel{?} \mathscr{E}\llbracket e \rrbracket \mathrel{:} \mathtt{err} \rrparenthesis$.

For sets $\mathscr{S}\llbracket \mathbb{B} \rrbracket \triangleq \mathtt{P}\ \mathtt{bool}, \ldots, \mathscr{S}\llbracket \{e\} \rrbracket \triangleq \llparenthesis \mathscr{E}\llbracket e \rrbracket \neq \mathtt{err} \mathrel{?} \mathtt{P}\ \mathscr{E}\llbracket e \rrbracket \mathrel{:} \mathtt{err} \rrparenthesis, \ldots, \mathscr{S}\llbracket s_1 \cup s_2 \rrbracket \triangleq \llparenthesis \mathtt{err} \neq \mathscr{S}\llbracket s_1 \rrbracket \cong \mathscr{S}\llbracket s_2 \rrbracket \neq \mathtt{err} \mathrel{?} \mathscr{S}\llbracket s_1 \rrbracket \mathrel{:} \mathtt{err} \rrparenthesis$ (note the approximation that s_1 and s_2 must have equivalent types as for alternatives of conditionals in functional languages). Ignoring error propagation, $\mathscr{S}\llbracket s^\infty \rrbracket \triangleq \mathtt{seq}\ \mathscr{S}\llbracket s \rrbracket$, $\mathscr{S}\llbracket s_1 \mapsto s_2 \rrbracket \triangleq \mathscr{S}\llbracket s_1 \rrbracket \ast\!\!\longleftrightarrow \mathscr{S}\llbracket s_2 \rrbracket$, $\mathscr{S}\llbracket s_1 \times s_2 \rrbracket \triangleq \mathscr{S}\llbracket s_1 \rrbracket \ast \mathscr{S}\llbracket s_2 \rrbracket$, $\mathscr{S}\llbracket \wp(s) \rrbracket \triangleq \mathtt{P}\ \mathscr{S}\llbracket s \rrbracket$.

For orders and posets, $\mathscr{O}\llbracket o \rrbracket \triangleq o$, $o \in \{\Rightarrow, \Leftrightarrow, \leq, \subseteq, =\}$, $\mathscr{O}\llbracket \dot{\sqsubseteq} \rrbracket \triangleq \subseteq, \ldots, \mathscr{O}\llbracket \ddot{o} \rrbracket \triangleq ((\mathscr{O}\llbracket \dot{o} \rrbracket))$, and $\mathscr{P}\llbracket \langle s,\ o \rangle \rrbracket \triangleq \mathscr{S}\llbracket s \rrbracket \circledast \mathscr{O}\llbracket o \rrbracket$.

For *GCs*, $\mathscr{T}\llbracket \mathbb{1}[p] \rrbracket \triangleq \mathscr{P}\llbracket p \rrbracket \leftrightarrows \mathscr{P}\llbracket p \rrbracket$, $\mathscr{T}\llbracket \curvearrowright[s_{\mathbb{L}}, s_{\mathcal{M}}] \rrbracket \triangleq \mathtt{P}(\mathscr{S}\llbracket s_{\mathbb{L}} \rrbracket \ast \mathscr{S}\llbracket s_{\mathcal{M}} \rrbracket) \circledast \subseteq \leftrightarrows \mathscr{S}\llbracket s_{\mathbb{L}} \rrbracket \ast\!\!\longleftrightarrow \mathtt{P}\ \mathscr{S}\llbracket s_{\mathcal{M}} \rrbracket \circledast \dot{\subseteq}$, $\mathscr{T}\llbracket \cup[s] \rrbracket \triangleq \mathtt{P}\ (\mathtt{P}\ \mathscr{S}\llbracket s \rrbracket) \circledast \subseteq \leftrightarrows \mathtt{P}\ \mathscr{S}\llbracket s \rrbracket \circledast \subseteq$, $\mathscr{T}\llbracket \neg[s] \rrbracket \triangleq \mathtt{P}\ \mathscr{S}\llbracket s \rrbracket \circledast \subseteq \leftrightarrows \mathtt{P}\ \mathscr{S}\llbracket s \rrbracket \circledast \subseteq^{-1}$, $\mathscr{T}\llbracket \infty[s] \rrbracket \triangleq \mathtt{P}\ (\mathtt{seq}\ \mathscr{S}\llbracket s \rrbracket) \circledast \subseteq \leftrightarrows \mathtt{P}\ \mathscr{S}\llbracket s \rrbracket \circledast \subseteq$, $\mathscr{T}\llbracket \rightsquigarrow[s_1, s_2] \rrbracket \triangleq \mathtt{P}\ (\mathscr{S}\llbracket s_1 \rrbracket \ast \mathscr{S}\llbracket s_2 \rrbracket) \circledast \subseteq \leftrightarrows \mathtt{P}\ \mathscr{S}\llbracket s_1 \rrbracket \ast\!\!\longleftrightarrow \mathtt{P}\ \mathscr{S}\llbracket s_2 \rrbracket \circledast \dot{\subseteq}$, $\mathscr{T}\llbracket \mapsto[s_1, s_2] \rrbracket \triangleq \mathtt{P}\ (\mathscr{S}\llbracket s_1 \rrbracket \ast\!\!\longleftrightarrow \mathscr{S}\llbracket s_2 \rrbracket) \circledast \subseteq \leftrightarrows \mathtt{P}\ \mathscr{S}\llbracket s_1 \rrbracket \ast\!\!\longleftrightarrow \mathtt{P}\ \mathscr{S}\llbracket s_2 \rrbracket \circledast \dot{\subseteq}$, $\mathscr{T}\llbracket \times[s_1, s_2] \rrbracket \triangleq \mathtt{P}\ (\mathscr{S}\llbracket s_1 \rrbracket \ast\!\!\longleftrightarrow \mathscr{S}\llbracket s_2 \rrbracket) \circledast \subseteq \leftrightarrows \mathscr{S}\llbracket s_1 \rrbracket \ast\!\!\longleftrightarrow \mathtt{P}\ \mathscr{S}\llbracket s_2 \rrbracket \circledast \dot{\subseteq}$, $\mathscr{T}\llbracket \mathsf{R}[g] \rrbracket \triangleq \mathscr{T}\llbracket g \rrbracket$, $\mathscr{T}\llbracket s \rightarrowtriangle g \rrbracket \triangleq \mathscr{S}\llbracket s \rrbracket \ast\!\!\rightarrowtriangle \mathscr{T}\llbracket g \rrbracket, \ldots$

Examples of type errors are $\mathscr{T}\llbracket \top[p, e] \rrbracket \triangleq \llparenthesis \mathscr{E}\llbracket e \rrbracket \neq \mathtt{err} \wedge \exists \mathsf{S} \in \mathfrak{S}, \mathsf{O} \in \mathfrak{O} : \mathscr{P}\llbracket p \rrbracket = \mathsf{S} \circledast \mathsf{O} \wedge \mathscr{E}\llbracket e \rrbracket \Subset \mathsf{S} \mathrel{?} \mathscr{P}\llbracket p \rrbracket \leftrightarrows \mathscr{P}\llbracket p \rrbracket \mathrel{:} \mathtt{err} \rrparenthesis$ or $\mathscr{T}\llbracket \mathbb{I}[\langle s,\ o \rangle, b, t] \rrbracket \triangleq \llparenthesis \mathtt{err} \neq \mathscr{E}\llbracket b \rrbracket \Subset \mathscr{S}\llbracket s \rrbracket \neq \mathtt{err} \wedge \mathtt{err} \neq \mathscr{E}\llbracket t \rrbracket \Subset \mathscr{S}\llbracket s \rrbracket \mathrel{?} (\mathtt{P}\ \mathscr{S}\llbracket s \rrbracket \circledast \subseteq) \leftrightarrows (\mathtt{P}\ \mathscr{S}\llbracket s \rrbracket \circledast \subseteq) \mathrel{:} \mathtt{err} \rrparenthesis$ where $\Subset$ abstracts set membership $\in$ of top/botton elements to the abstracted set.

This functional presentation is equivalent to a rule-based system *e.g.* $\dfrac{g_1 \vdash \mathsf{P}_1 \leftrightarrows \mathsf{P}_2,\ g_2 \vdash \mathsf{P}_3 \leftrightarrows \mathsf{P}_4,\ \mathsf{P}_2 {\cong} \mathsf{P}_3}{g_1 {\fatsemi} g_2 \vdash \mathsf{P}_1 \leftrightarrows \mathsf{P}_4}$ (where $\mathtt{err}$ is not derivable), $\dfrac{g_1 \vdash \mathsf{S}_1 \circledast \mathsf{O}_1 \leftrightarrows \mathsf{S}_2 \circledast \mathsf{O}_2,\ g_2 \vdash \mathsf{S}_3 \circledast \mathsf{O}_3 \leftrightarrows \mathsf{S}_4 \circledast \mathsf{O}_4}{g_1 {\Longmapsto} g_2 \vdash \mathsf{S}_1 {\ast\!\!\longleftrightarrow} \mathsf{S}_3 \circledast \dot{\mathsf{O}}_3 \leftrightarrows \mathsf{S}_2 {\ast\!\!\longleftrightarrow} \mathsf{S}_4 \circledast \dot{\mathsf{O}}_4}$, *Id.* for $\divideontimes$.

For example $\mathscr{T}\llbracket G^{\mathfrak{I}^*} \rrbracket = \mathtt{P}\ (\mathtt{P}\ (\mathtt{seq}(\mathtt{P}\ \mathtt{lab} \ast (\mathtt{P}\ \mathtt{var} \ast\!\!\longleftrightarrow \mathtt{P}\ \mathtt{int})))) \circledast \subseteq \leftrightarrows (\mathtt{P}\ \mathtt{lab} \ast\!\!\longleftrightarrow \mathtt{P}\ \mathtt{var} \ast\!\!\longleftrightarrow \mathtt{P}\ \mathtt{P}\ \mathtt{int} \circledast \ddot{\subseteq})$ *i.e.* sets of sets of sequences of states are abstracted to a map of labels to variables to sets of integers (which includes intervals), ordered pointwise.

10. Type soundness Typable expressions $g \in \mathbb{G}$ (for which $\mathscr{T}\llbracket g \rrbracket \neq \mathtt{err}$) cannot go wrong since then $\mathcal{S}\llbracket g \rrbracket \in \gamma^{\mathfrak{T}}(\mathscr{T}\llbracket g \rrbracket) \cup \{\omega\}$ and $\Omega \notin \gamma^{\mathfrak{T}}(\mathscr{T}\llbracket g \rrbracket)$. However, dynamic errors ($\mathcal{S}\llbracket g \rrbracket = \omega$) cannot be excluded (*e.g.* $\mathtt{int}$ does not prevent overflows).

11. Principal type Arbitrary concrete properties in $\wp(\mathfrak{Gc})$ may have no best abstraction (*e.g.* $\emptyset$ so we add the empty type $\varnothing$). Yet, by considering only semantic properties $P = \{\mathcal{S}\llbracket g_i \rrbracket \mid i \in \Delta\}$ of *GC* expressions, the principal type is $\alpha^{\mathfrak{T}}(\emptyset) \triangleq \varnothing$, $\alpha^{\mathfrak{T}}(P) \triangleq [\mathsf{T}]_{\cong}$ when $\forall i \in \Delta \neq \emptyset : \mathscr{T}\llbracket g_i \rrbracket \cong \mathsf{T}$ else $\alpha^{\mathfrak{T}}(P) \triangleq \mathtt{err}$ so $\langle \wp(\{\mathcal{S}\llbracket g \rrbracket \mid g \in \mathbb{G}\}),\ \subseteq \rangle \xrightleftharpoons[\alpha^{\mathfrak{T}}]{\gamma^{\mathfrak{T}}} \langle (\mathfrak{T} \cup \{\varnothing\})_{/\cong},\ \trianglelefteq \rangle$ ($\alpha^{\mathfrak{T}}$ onto).

12. Types of types Types $\mathcal{T} \triangleq \{\mathfrak{E}, \mathfrak{S}, \mathfrak{O}, \mathfrak{P}, \mathfrak{T}\}$ have properties $\mathcal{P} \triangleq \wp(\bigcup \mathcal{T})$ can be abstracted to types of types $\overline{\mathfrak{T}} ::= \overline{\varnothing} \mid \overline{\mathfrak{E}} \mid \overline{\mathfrak{S}} \mid \overline{\mathfrak{O}} \mid \overline{\mathfrak{P}} \mid \overline{\mathfrak{T}} \mid \overline{\mathtt{err}}$ by $\alpha^{\overline{\mathfrak{T}}}(P) \triangleq \llparenthesis P = \emptyset \mathrel{?} \overline{\varnothing} \parallel P \subseteq \mathsf{T}, \mathsf{T} \in \mathcal{T} \mathrel{?} \overline{\mathsf{T}} \mathrel{:} \overline{\mathtt{err}} \rrparenthesis$.

13. Static analyzers In static analyzers [1, 12, 14] *GCs* specify abstract domains modules and Galois connectors their combinations by functors. For scalability, rapid convergence acceleration of infinite fixpoint computations by widening/narrowing abstracting induction and/or their duals for co-induction [3–5] is effective and more precise than finite abstractions [8].

Acknowledgments We warmly thank the ACM SIGPLAN Awards Committee for awarding us the 2013 Programming Languages Achievement Award and the programming languages community for its support.

References

[1] B. Blanchet, P. Cousot, R. Cousot, J. Feret, L. Mauborgne, A. Miné, D. Monniaux, and X. Rival. A static analyzer for large safety-critical software. *PLDI'03*, 196–207.

[2] P. Cousot. Types as abstract interpretations. *POPL'97*, 316–331.

[3] P. Cousot and R. Cousot. Static determination of dynamic properties of programs. *Proc. 2nd Int. Symp. on Programming*, 106–130, Paris, 1976. Dunod.

[4] P. Cousot and R. Cousot. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. *POPL'77*, 238–252.

[5] P. Cousot and R. Cousot. Static determination of dynamic properties of recursive procedures. *IFIP Conf. on Formal Description of Programming Concepts, St-Andrews, N.B., CN*, 237–277. North-Holland Pub. Co., 1977.

[6] P. Cousot and R. Cousot. Systematic design of program analysis frameworks. *POPL'79*, 269–282.

[7] P. Cousot and R. Cousot. Abstract interpretation frameworks. *J. Logic and Comp.*, 2(4):511–547, 1992.

[8] P. Cousot and R. Cousot. Comparing the Galois connection and widening/narrowing approaches to abstract interpretation. *PLILP'92*, LNCS 631, 269–295.

[9] P. Cousot and R. Cousot. Inductive definitions, semantics and abstract interpretation. *POPL'92*, 83–94.

[10] P. Cousot and R. Cousot. Temporal abstract interpretation. *POPL'00*, 12–25.

[11] P. Cousot and R. Cousot. Systematic design of program transformation frameworks by abstract interpretation. *POPL'02*, 178–190.

[12] P. Cousot and R. Cousot. An abstract interpretation-based framework for software watermarking. *POPL'04*, 173–185.

[13] P. Cousot and R. Cousot. An abstract interpretation framework for termination. *POPL'12*, 245–258.

[14] P. Cousot, R. Cousot, and F. Logozzo. A parametric segmentation functor for fully automatic and scalable array content analysis. *POPL'11*, 105–118.

[15] P. Cousot and N. Halbwachs. Automatic discovery of linear restraints among variables of a program. *POPL'78*, 84–96.

A Galois Connection Calculus for Abstract Interpretation (Auxiliary Materials)

Patrick Cousot
CIMS [*], NYU, USA
pcousot@cims.nyu.edu

Radhia Cousot
CNRS Emeritus, ENS, France
rcousot@ens.fr

Abstract We introduce a Galois connection calculus for language independent specification of abstract interpretations used in programming language semantics, formal verification, and static analysis. This Galois connection calculus and its type system are typed by abstract interpretation.

Categories and Subject Descriptors D.2.4 [*Software/Program Verification*]

General Terms Algorithms, Languages, Reliability, Security, Theory, Verification.

Keywords Abstract Interpretation, Galois connection, Static Analysis, Verification.

1. Galois connections in Abstract Interpretation In *Abstract interpretation* [3, 4, 6, 7] concrete properties (for example (*e.g.*) of computations) are related to abstract properties (*e.g.* types). The abstract properties are always *sound* approximations of the concrete properties (abstract proofs/static analyzes are always correct in the concrete) and are sometimes *complete* (proofs/analyzes of abstract properties can all be done in the abstract only). *E.g.* types are sound but incomplete [2] while abstract semantics are usually complete [9]. The *concrete domain* $\langle \mathcal{C},\ \sqsubseteq\rangle$ and *abstract domain* $\langle \mathcal{A},\ \preccurlyeq\rangle$ of properties are posets (partial orders being interpreted as implication). When concrete properties all have a $\preccurlyeq$-most precise abstraction, the correspondence is a *Galois connection* (*GC*) $\langle \mathcal{C},\ \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{A},\ \preccurlyeq\rangle$ with *abstraction* $\alpha \in \mathcal{C} \mapsto \mathcal{A}$ and *concretization* $\gamma \in \mathcal{A} \mapsto \mathcal{C}$ satisfying $\forall P \in \mathcal{C} : \forall Q \in \mathcal{A} : \alpha(x) \preccurlyeq y \Leftrightarrow x \sqsubseteq \gamma(y)$ ($\Rightarrow$ expresses soundness and $\Leftarrow$ best abstraction). Each adjoint α/γ uniquely determines the other γ/α. A *Galois retraction* (or *insertion*) has α onto, so γ is one-to-one, and $\alpha \circ \gamma$ is the identity. A *Galois isomorphism* $\langle \mathcal{C},\ \subseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{A},\ \preccurlyeq\rangle$ has both α and γ one-to-one onto.

2. *GC* calculus syntax The *GC* calculus can describes complex *GCs* between posets representing concrete and abstract properties of the semantics of programs.

2.1 Syntax of program variables

$\mathtt{x}, \ldots \in \mathbb{X}$

2.2 Syntax of labels

$\ell, \ldots \in \mathbb{L}$

2.3 Syntax of ur-elements

The ur-elements are objects (concrete or abstract) which are not a set, but that may be elements of sets.

$e \in \mathbb{E}$
$e ::= \mathsf{true} \mid 1 \mid \infty \mid \mathtt{x} \mid \ell \mid -e \mid \ldots$

2.4 Syntax of sets

$s \in \mathbb{S}$
$s ::= \mathbb{B} \mid \mathbb{Z} \mid \mathbb{X} \mid \mathbb{L} \mid \{e\} \mid [e, e] \mid \mathbb{I}(s, o) \mid s^{\infty} \mid s \cup s \mid s \mapsto s \mid s \times s \mid \wp(s) \mid \ldots$

Sets are the sets of Booleans, integers, variables, labels, singletons, intervals, the set of all intervals of a poset $\langle s,\ o\rangle$, sets of finite or infinite sequences, unions of sets, sets of functions, of pairs, power sets, *etc.*

2.5 Syntax of partial orders

$o \in \mathbb{O}$
$o ::= \Rightarrow \mid \Leftrightarrow \mid \leq \mid \subseteq \mid \underline{\subseteq}^{+} \mid = \mid o^{-1} \mid o_1 \times o_2 \mid \dot{o} \mid \ddot{o} \mid \ldots$

Orders are implication, equivalence on Booleans, the natural order of integers, inclusion, interval inclusion, equality, the inverse of an order, the pairwise/component by component order, the pointwise order, the double pointwise order, *etc.*

2.6 Syntax of posets

$p \in \mathbb{P}$
$p ::= \langle s,\ o\rangle$

A poset is a set equipped with a partial order.

2.7 Syntax of *GCs*

$g \in \mathbb{G}$
$g ::= \mathbb{1}[p] \mid \top[p, e] \mid \mathbb{I}[p, e, e] \mid \curvearrowright[s, s] \mid \cup[s] \mid \neg[s] \mid \infty[s] \mid \rightsquigarrow[s, s] \mid \mapsto[s, s] \mid \times[s, s] \mid \ldots \mid \mathsf{R}[g] \mid s \multimap g \mid g \circ g \mid g \circledast g \mid g \Longmapsto g \mid \ldots$

Basic *GCs* include the identity abstraction $\mathbb{1}[p]$, the top/most abstract abstraction $\top[p, e]$, the interval abstraction $\mathbb{I}[p, e, e]$, the right-image abstraction $\curvearrowright[s, s]$, the join abstraction $\cup[s]$, the negation abstraction $\neg[s]$, the sequence abstraction $\infty[s]$, the transformer abstraction $\rightsquigarrow[s, s]$, the function abstraction $\mapsto[s, s]$, the cartesian abstraction $\times[s, s]$, *etc.*.

The Galois connectors include the reduction $\mathsf{R}[g]$, the pointwise extension $s \multimap g$, the composition $g \circ g$, the componentwise composition $g \circledast g$, the function extension $g \Longmapsto g$ at higher-order, *etc.*

3. *GC* calculus semantics The *GC* calculus semantics defines which *GC* is defined by the expressions of the *GC* calculus. Since some *GC* expressions may be ill-defined, the semantics may return a static error Ω (expected to be detectable by sound type systems) or dynamic errors ω (expected no to be detectable by some sound type systems).

---

[*] Work supported in part by CMACS, NSF Expedition in Computing award 0926166.

POPL '14, January 22–24, 2014, San Diego, CA, USA.
Copyright is held by the owner/author(s).
ACM 978-1-4503-2544-8/14/01.
http://dx.doi.org/10.1145/2535838.2537850

3.1 Semantics of ur-elements

The semantics $\mathcal{S}[\![e]\!]$ of an ur-element e is its value. $\mathcal{O}[\![e]\!]$ is the poset to which this value $\mathcal{S}[\![e]\!]$ belongs.

- $\mathcal{S}[\![\mathrm{x}]\!] \triangleq \mathrm{x}$
  $\mathcal{O}[\![\mathrm{x}]\!] \triangleq \langle \mathbb{X},\ = \rangle$
- $\mathcal{S}[\![\ell]\!] \triangleq \ell$
  $\mathcal{O}[\![\ell]\!] \triangleq \langle \mathbb{L},\ = \rangle$
- $\mathcal{S}[\![\mathsf{true}]\!] \triangleq \mathsf{true}$
  $\mathcal{O}[\![\mathsf{true}]\!] \triangleq \langle \mathbb{B},\ \Rightarrow \rangle$
- $\mathcal{S}[\![1]\!] \triangleq 1$
  $\mathcal{O}[\![1]\!] \triangleq \langle \mathbb{Z} \cup \{-\infty, \infty\},\ \leq \rangle$
- $\mathcal{S}[\![\infty]\!] \triangleq \infty$
  $\mathcal{O}[\![\infty]\!] \triangleq \langle \mathbb{Z} \cup \{-\infty, \infty\},\ \leq \rangle$
- $\mathcal{S}[\![-e]\!] \triangleq \llparenthesis \mathcal{S}[\![e]\!] \in \mathbb{B} \;?\; \neg\mathcal{S}[\![e]\!] \parallel \mathcal{S}[\![e]\!] \in \mathbb{Z} \cup \{-\infty, \infty\} \;?\; -\mathcal{S}[\![e]\!] \fatsemi \Omega \rrparenthesis$
  $\mathcal{O}[\![-e]\!] \triangleq \llparenthesis \mathcal{S}[\![e]\!] \in \mathbb{B} \vee \mathcal{S}[\![e]\!] \in \mathbb{Z} \cup \{-\infty, \infty\} \;?\; \mathcal{O}[\![e]\!] \fatsemi \Omega \rrparenthesis$
- Notice that errors on the semantics $\mathcal{S}[\![e]\!]$ of elements $e \in \mathbb{E}$ are all static *i.e.* Ω.

3.2 Errors

Errors can either be static (Ω) or dynamic (ω). Static errors are expected to be all captured by a static analysis *e.g.* by typing rules. An example is the addition of an integer and a list of booleans. Dynamic errors are those for which static analyses may fail *e.g.* arithmetic overflow which is undecidable. The combination $\mathbf{error}(x, y)$ of errors $x \in \{\omega, \Omega\}$ or $y \in \{\omega, \Omega\}$ is defined so as to give priority to static errors (and to ignore non-erroneous cases).

$\mathbf{error}(x, y)$		x		
		ω	Ω	$\notin \{\omega, \Omega\}$
y	ω	ω	Ω	ω
	Ω	Ω	Ω	Ω
	$\notin \{\omega, \Omega\}$	ω	Ω	——

3.3 Semantics of sets

The semantics $\mathcal{S}[\![s]\!]$ of set expressions $s \in \mathbb{S}$ is the set denoted by that expression.

- $\mathcal{S}[\![\mathbb{X}]\!] \triangleq \mathbb{X}$
- $\mathcal{S}[\![\mathbb{L}]\!] \triangleq \mathbb{L}$
- $\mathcal{S}[\![\mathbb{B}]\!] \triangleq \mathbb{B}$
- $\mathcal{S}[\![\mathbb{Z}]\!] \triangleq \mathbb{Z}$
- $\mathcal{S}[\![\{e\}]\!] \triangleq \llparenthesis \mathcal{S}[\![e]\!] \neq \Omega \;?\; \{\mathcal{S}[\![e]\!]\} \fatsemi \Omega \rrparenthesis$
- $\mathcal{S}[\![[e_1, e_2]]\!] \triangleq \llparenthesis \mathcal{O}[\![e_1]\!] = \mathcal{O}[\![e_2]\!] = \langle S,\ o\rangle \;?\; \{v \in S \mid \langle \mathcal{S}[\![e_1]\!],\ v\rangle \in o \wedge \langle v,\ \mathcal{S}[\![e_2]\!]\rangle \in 0\} \fatsemi \Omega \rrparenthesis$
- $\Im(S, \leqslant) \triangleq \{[v_1, v_2]_{\leqslant} \mid v_1, v_2 \in S\}$, intervals of S for $\leqslant$ where $[v_1, v_2]_{\leqslant} \triangleq \{v \in S \mid v_1 \leqslant v \wedge v \leqslant v_2\}$ so $\Im(S, \leqslant) \subseteq \wp(S)$ hence $\Im(S, \leqslant) \in \wp(\wp(S))$
- $\mathcal{S}[\![\mathbb{I}(s, o)]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \notin \{\omega, \Omega\} \;?\; \llparenthesis \mathcal{S}[\![o]\!] \subseteq \mathcal{S}[\![s]\!] \times \mathcal{S}[\![s]\!] \;?\; \Im(\mathcal{S}[\![s]\!], \mathcal{S}[\![o]\!]) \fatsemi \omega \rrparenthesis \fatsemi \mathcal{S}[\![s]\!] \rrparenthesis$
- $\mathcal{S}[\![s^\infty]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \notin \{\omega, \Omega\} \;?\; \mathcal{S}[\![s]\!]^\infty \fatsemi \mathcal{S}[\![s]\!] \rrparenthesis$
- $\mathcal{S}[\![s_1 \cup s_2]\!] \triangleq \llparenthesis \mathcal{S}[\![s_1]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![s_2]\!] \notin \{\omega, \Omega\} \;?\; \mathcal{S}[\![s_1]\!] \cup \mathcal{S}[\![s_2]\!] \fatsemi \mathbf{error}(\mathcal{S}[\![s_1]\!], \mathcal{S}[\![s_2]\!]) \rrparenthesis$
  where $X^\infty \triangleq X^+ \cup X^\omega$, $X^n \triangleq [0, n] \mapsto X$, $n \in \mathbb{N}$ ($\mathsf{dom}(\sigma) = [0, n]$ when $\sigma \in X^n$, $n \in \mathbb{N}$), $X^+ \triangleq \bigcup_{n \in \mathbb{N}} X^n$, and $X^\omega \triangleq \mathbb{N} \mapsto X$ ($\mathsf{dom}(\sigma) = \mathbb{N}$ when $\sigma \in X^\omega$)
- $\mathcal{S}[\![s_1 \mapsto s_2]\!] \triangleq \llparenthesis \mathcal{S}[\![s_1]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![s_2]\!] \notin \{\omega, \Omega\} \;?\; \mathcal{S}[\![s_1]\!] \mapsto \mathcal{S}[\![s_2]\!] \fatsemi \mathbf{error}(\mathcal{S}[\![s_1]\!], \mathcal{S}[\![s_2]\!]) \rrparenthesis$
- $\mathcal{S}[\![s_1 \times s_2]\!] \triangleq \llparenthesis \mathcal{S}[\![s_1]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![s_2]\!] \notin \{\omega, \Omega\} \;?\; \mathcal{S}[\![s_1]\!] \times \mathcal{S}[\![s_2]\!] \fatsemi \mathbf{error}(\mathcal{S}[\![s_1]\!], \mathcal{S}[\![s_2]\!]) \rrparenthesis$
- $\mathcal{S}[\![\wp(s)]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \notin \{\omega, \Omega\} \;?\; \wp(\mathcal{S}[\![s]\!]) \fatsemi \mathcal{S}[\![s]\!] \rrparenthesis$

3.4 Semantics of partial orders

The semantics $\mathcal{S}[\![o]\!]$ of partial order expressions $o \in \mathbb{O}$ is the partial order denoted by that expression. The fact that partial orders are always well-defined *i.e.* $\mathcal{S}[\![o]\!] \notin \{\Omega, \omega\}$ follows from the calculus syntax.

- $\mathcal{S}[\![\Rightarrow]\!] \triangleq \Rightarrow \triangleq \{\langle \mathsf{false},\ \mathsf{false}\rangle, \langle \mathsf{false},\ \mathsf{true}\rangle, \langle \mathsf{true},\ \mathsf{true}\rangle\}$ [1]
- $\mathcal{S}[\![\Leftrightarrow]\!] \triangleq \Leftrightarrow \triangleq \{\langle \mathsf{false},\ \mathsf{false}\rangle, \langle \mathsf{true},\ \mathsf{true}\rangle\}$
- $\mathcal{S}[\![\leq]\!] \triangleq \leq \triangleq \{\langle x,\ y\rangle \mid x, y \in \mathbb{Z} \cup \{-\infty, \infty\} \wedge x \leqslant y\}$
- $\mathcal{S}[\![\subseteq]\!] \triangleq \subseteq \triangleq \{\langle X,\ Y\rangle \mid \forall x \in X : x \in Y\}$ [2]
- $\mathcal{S}[\![\supseteq]\!] \triangleq \mathcal{S}[\![\subseteq]\!] = \subseteq$
- $\mathcal{S}[\![=]\!] \triangleq = \triangleq \mathcal{S}[\![\subseteq]\!] \cap \mathcal{S}[\![\subseteq^{-1}]\!]$
- $\mathcal{S}[\![o^{-1}]\!] \triangleq (\mathcal{S}[\![o]\!])^{-1}$ where $R^{-1} \triangleq \{\langle y,\ x\rangle \mid \langle x,\ y\rangle \in R\}$
- $\mathcal{S}[\![o_1 \times o_2]\!] \triangleq \mathcal{S}[\![o_1]\!] \times \mathcal{S}[\![o_2]\!]$ where $R_1 \times R_2 \triangleq \{\langle\langle x,\ x'\rangle,\ \langle y,\ y'\rangle\rangle \mid \langle x,\ y\rangle \in R_1 \wedge \langle x',\ y'\rangle \in R_2\}$
- $\mathcal{S}[\![\dot{o}]\!] \triangleq (\dot{\mathcal{S}[\![o]\!]})$ where $\dot{R} \triangleq \{\langle f,\ g\rangle \mid \forall x \in \mathsf{dom}(f) : x \in \mathsf{dom}(g) \wedge \langle f(x),\ g(x)\rangle \in R\}$
- $\mathcal{S}[\![\ddot{o}]\!] \triangleq (\dot{\mathcal{S}[\![\dot{o}]\!]})$

3.5 Semantics of posets

The semantics $\mathcal{S}[\![p]\!]$ of poset expressions $p \in \mathbb{P}$ is the poset denoted by that expression.

- $\mathcal{S}[\![\langle s,\ o\rangle]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![o]\!] \notin \{\omega, \Omega\} \;?\; \langle \mathcal{S}[\![s]\!],\ \mathcal{S}[\![o]\!]\rangle \fatsemi \mathbf{error}(\mathcal{S}[\![s]\!], \mathcal{S}[\![o]\!]) \rrparenthesis$

3.6 Semantics of *GCs*

The semantics $\mathcal{S}[\![g]\!]$ of *GCs* $g \in \mathbb{G}$ is the *GC* between posets denoted by that expression.

- $\mathcal{S}[\![\mathbb{1}[p]]\!] \triangleq \llparenthesis \mathcal{S}[\![p]\!] \notin \{\omega, \Omega\} \;?\; \mathcal{S}[\![p]\!] \underset{\boldsymbol{\lambda} P \bullet P}{\overset{\boldsymbol{\lambda} Q \bullet Q}{\leftrightarrows}} \mathcal{S}[\![p]\!] \fatsemi \mathcal{S}[\![p]\!] \rrparenthesis$
- $\mathcal{S}[\![\top[p, e]]\!] \triangleq \llparenthesis \exists S, \leqslant : \mathcal{S}[\![p]\!] = \langle S,\ \leqslant\rangle \;?\; \llparenthesis \mathcal{S}[\![e]\!] \in S \setminus \{\omega\} \;?\; \llparenthesis \forall x \in S : x \leqslant \mathcal{S}[\![e]\!] \;?\; \mathcal{S}[\![p]\!] \underset{\boldsymbol{\lambda} P \bullet \mathcal{S}[\![e]\!]}{\overset{\boldsymbol{\lambda} Q \bullet \mathcal{S}[\![e]\!]}{\leftrightarrows}} \mathcal{S}[\![p]\!] \fatsemi \omega \rrparenthesis \fatsemi \omega \rrparenthesis \fatsemi \mathbf{error}(\mathcal{S}[\![p]\!], \mathcal{S}[\![e]\!]) \rrparenthesis$
- $\mathcal{S}[\![\mathbb{I}[\langle s,\ o\rangle, e_1, e_2]]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![e_1]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![e_2]\!] \notin \{\omega, \Omega\} \;?\; \llparenthesis \mathcal{S}[\![o]\!] \subseteq (\mathcal{S}[\![s]\!] \cup \{\mathcal{S}[\![e_1]\!], \mathcal{S}[\![e_2]\!]\}) \times (\mathcal{S}[\![s]\!] \cup \{\mathcal{S}[\![e_1]\!], \mathcal{S}[\![e_2]\!]\}) \wedge \forall x \in \mathcal{S}[\![s]\!] : \langle \mathcal{S}[\![e_1]\!], x\rangle \in \mathcal{S}[\![o]\!] \wedge \langle x, \mathcal{S}[\![e_2]\!]\rangle \in \mathcal{S}[\![o]\!] \;?\; \langle \wp(\mathcal{S}[\![s]\!]), \subseteq\rangle \underset{\alpha^{\mathbb{I}}}{\overset{\gamma^{\mathbb{I}}}{\leftrightarrows}} \langle \Im(\mathcal{S}[\![s]\!] \cup \{\mathcal{S}[\![e_1]\!], \mathcal{S}[\![e_2]\!]\}, \mathcal{S}[\![o]\!]), \subseteq\rangle \fatsemi \omega \rrparenthesis \fatsemi \mathbf{error}(\mathcal{S}[\![s]\!], \mathbf{error}(\mathcal{S}[\![e_1]\!], \mathcal{S}[\![e_2]\!])) \rrparenthesis$ where
  - $\Im(S, \leqslant) \triangleq \{[v_1, v_2] \mid v_1, v_2 \in S\}$, intervals of S for $\leqslant$ where $[v_1, v_2] \triangleq \{v \in S \mid v_1 \leqslant v \wedge v \leqslant v_2\}$

[1] we use the same mathematical symbol for the syntax and semantics of partial orders in the *GC* calculus, which one is meant should be clear from the context.

[2] The use of proper classes can be avoided by assuming that all sets such as X and Y are taken in a universe of sets such as a Grothendieck universe or the Zermelo/von Neumann hierarchy of sets.

- $\alpha^{\mathbb{I}}(X) \triangleq [\min_{\mathcal{S}[\![o]\!]} X, \max_{\mathcal{S}[\![o]\!]} X], \min_{\mathcal{S}[\![o]\!]} \emptyset \triangleq \mathcal{S}[\![e_2]\!], \max_{\mathcal{S}[\![o]\!]} \emptyset \triangleq \mathcal{S}[\![e_1]\!]$, and
- $\gamma^{\mathbb{I}}([a, b]) \triangleq \{x \in \mathcal{S}[\![s]\!] \mid \langle a,\ x\rangle \in \mathcal{S}[\![o]\!] \wedge \langle x,\ b\rangle \in \mathcal{S}[\![o]\!]\}$

- $\mathcal{S}[\![\frown[s_{\mathbb{L}}, s_{\mathcal{M}}]]\!] \triangleq (\!|\mathcal{S}[\![s_{\mathbb{L}}]\!] \notin \{\Omega, \omega\} \wedge \mathcal{S}[\![s_{\mathcal{M}}]\!] \notin \{\Omega, \omega\}\ ?\ \langle\wp(\mathcal{S}[\![s_{\mathbb{L}}]\!] \times \mathcal{S}[\![s_{\mathcal{M}}]\!]),\ \subseteq\rangle \xleftrightarrow[\alpha^{\frown}]{\gamma^{\frown}} \langle\mathcal{S}[\![s_{\mathbb{L}}]\!] \mapsto \wp(\mathcal{S}[\![s_{\mathcal{M}}]\!]),\ \dot{\subseteq}\rangle : \mathtt{error}(\mathcal{S}[\![s_{\mathbb{L}}]\!], \mathcal{S}[\![s_{\mathcal{M}}]\!])|\!)$ where
  - $\alpha^{\frown} \triangleq \boldsymbol{\lambda} P \bullet \boldsymbol{\lambda} \ell \bullet \{m \mid \langle\ell,\ m\rangle \in P\}$
  - $\gamma^{\frown} \triangleq \boldsymbol{\lambda} Q \bullet \{\langle\ell,\ m\rangle \mid m \in Q(\ell)\}$
  - $\dot{\subseteq}$ is the pointwise extension of inclusion $\subseteq$ that is $f\ \dot{\subseteq}\ g \Leftrightarrow \forall x \in \mathsf{dom} f : x \in \mathsf{dom}(g) \wedge f(x) \subseteq g(x)$.

- $\mathcal{S}[\![\cup[s]]\!] \triangleq (\!|\mathcal{S}[\![s]\!] \notin \{\omega, \Omega\}\ ?\ \langle\wp(\wp(\mathcal{S}[\![s]\!])),\ \subseteq\rangle \xleftrightarrow[\alpha^{\wp}]{\gamma^{\wp}} \langle\wp(\mathcal{S}[\![s]\!]),\ \subseteq\rangle : \mathcal{S}[\![s]\!]|\!)$ with
  - $\alpha^{\wp} \triangleq \boldsymbol{\lambda} P \in \wp(\wp(\mathcal{S}[\![s]\!])) \bullet \bigcup P$
  - $\gamma^{\wp} \triangleq \boldsymbol{\lambda} Q \in \wp(\mathcal{S}[\![s]\!]) \bullet \wp(Q))$

- $\mathcal{S}[\![\neg[s]]\!] \triangleq (\!|\mathcal{S}[\![s]\!] \notin \{\omega, \Omega\}\ ?\ \langle\wp(\mathcal{S}[\![s]\!]),\ \subseteq\rangle \xleftrightarrow[\neg]{\neg} \langle\wp(\mathcal{S}[\![s]\!]),\ \supseteq\rangle : \mathcal{S}[\![s]\!]|\!)$,

- $\mathcal{S}[\![\infty[s]]\!] \triangleq (\!|\mathcal{S}[\![s]\!] \notin \{\omega, \Omega\}\ ?\ \langle\wp(\mathcal{S}[\![s]\!]^{\infty}),\ \subseteq\rangle \xleftrightarrow[\alpha^{\infty}]{\gamma^{\infty}} \langle\wp(\mathcal{S}[\![s]\!]),\ \subseteq\rangle : \mathcal{S}[\![s]\!]|\!)$ with
  - $\alpha^{\infty} \triangleq \boldsymbol{\lambda} P \in \wp(\mathcal{S}[\![s]\!]^{\infty}) \bullet \{\sigma_i \in \mathcal{S}[\![s]\!] \mid \sigma \in P \wedge i \in \mathsf{dom}(\sigma)\}$
  - $\gamma^{\infty} \triangleq \boldsymbol{\lambda} Q \in \wp(\mathcal{S}[\![s]\!]) \bullet \{\sigma \in \mathcal{S}[\![s]\!]^{\infty} \mid \forall i \in \mathsf{dom}(\sigma) : \sigma_i \in Q\}$

- $\mathcal{S}[\![\rightsquigarrow[s_1, s_2]]\!] \triangleq (\!|\mathcal{S}[\![s_1]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![s_1]\!] \notin \{\omega, \Omega\}\ ?\ \langle\wp(\mathcal{S}[\![s_1]\!] \times \mathcal{S}[\![s_2]\!]),\ \subseteq\rangle \xleftrightarrow[\alpha^{\rightsquigarrow}]{\gamma^{\rightsquigarrow}} \langle\wp(\mathcal{S}[\![s_1]\!]) \xrightarrow{\cup} \wp(\mathcal{S}[\![s_2]\!]),\ \dot{\subseteq}\rangle : \mathtt{error}(\mathcal{S}[\![s_1]\!], \mathcal{S}[\![s_2]\!])|\!)$ mapping relations to join-preserving set transformers with
  - $\alpha^{\rightsquigarrow} \triangleq \boldsymbol{\lambda} R \in \wp(\mathcal{S}[\![s_1]\!] \times \mathcal{S}[\![s_2]\!]) \bullet \boldsymbol{\lambda} X \in \wp(\mathcal{S}[\![s_1]\!]) \bullet \{y \mid \exists x \in X : \langle x,\ y\rangle \in R\}$
  - $\gamma^{\rightsquigarrow} \triangleq \boldsymbol{\lambda} g \in \wp(\mathcal{S}[\![s_1]\!]) \xrightarrow{\cup} \wp(\mathcal{S}[\![s_2]\!]) \bullet \{\langle x,\ y\rangle \mid y \in g(\{x\})\}$

- $\mathcal{S}[\![\mapsto[s_1, s_2]]\!] \triangleq (\!|\mathcal{S}[\![s_1]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![s_2]\!] \notin \{\omega, \Omega\}\ ?\ \langle\wp(\mathcal{S}[\![s_1]\!] \mapsto \mathcal{S}[\![s_2]\!]),\ \subseteq\rangle \xleftrightarrow[\alpha^{\mapsto}]{\gamma^{\mapsto}} \langle\wp(\mathcal{S}[\![s_1]\!]) \mapsto \wp(\mathcal{S}[\![s_2]\!]),\ \dot{\subseteq}\rangle : \mathtt{error}(\mathcal{S}[\![s_1]\!], \mathcal{S}[\![s_2]\!])|\!)$ with
  - $\alpha^{\mapsto} \triangleq \boldsymbol{\lambda} P \in \wp(\mathcal{S}[\![s_1]\!] \mapsto \mathcal{S}[\![s_2]\!]) \bullet \boldsymbol{\lambda} X \in \wp(\mathcal{S}[\![s_1]\!]) \bullet \{f(x) \mid f \in P \wedge x \in X\}$
  - $\gamma^{\mapsto} \triangleq \boldsymbol{\lambda} g \in \wp(\mathcal{S}[\![s_1]\!]) \mapsto \wp(\mathcal{S}[\![s_2]\!]) \bullet \{f \in \mathcal{S}[\![s_1]\!] \mapsto \mathcal{S}[\![s_2]\!] \mid \forall X \in \wp(\mathcal{S}[\![s_1]\!]) : \forall x \in X : f(x) \in g(X)\}$,

- $\mathcal{S}[\![\times[s_1, s_2]]\!] \triangleq (\!|\mathcal{S}[\![s_1]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![s_2]\!] \notin \{\omega, \Omega\}\ ?\ \langle\wp(\mathcal{S}[\![s_1]\!] \mapsto \mathcal{S}[\![s_2]\!]),\ \subseteq\rangle \xleftrightarrow[\alpha^{\times}]{\gamma^{\times}} \langle\mathcal{S}[\![s_1]\!] \mapsto \wp(\mathcal{S}[\![s_2]\!]),\ \dot{\subseteq}\rangle : \mathtt{error}(\mathcal{S}[\![s_1]\!], \mathcal{S}[\![s_2]\!])|\!)$ with
  - $\alpha^{\times}(X) \triangleq \boldsymbol{\lambda} i \in \mathcal{S}[\![s_1]\!] \bullet \{x \in \mathcal{S}[\![s_2]\!] \mid \exists f \in \mathcal{S}[\![s_1]\!] \mapsto \mathcal{S}[\![s_2]\!] : f[i \leftarrow x] \in X\}$
  - $\gamma^{\times}(Y) \triangleq \{f \in \mathcal{S}[\![s_1]\!] \mapsto \mathcal{S}[\![s_2]\!] \mid \forall i \in \mathcal{S}[\![s_1]\!] : f(i) \in Y(i)\}$, and
  - $\dot{\subseteq}$ is the the pointwise extension of $\subseteq$ to $\mathcal{S}[\![s_1]\!]$

- $\mathcal{S}[\![\mathsf{R}[g]]\!] \triangleq (\!|\mathcal{S}[\![g]\!] = \langle\mathcal{C},\ \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle\mathcal{A},\ \leqslant\rangle\ ?\ \langle\mathcal{C},\ \sqsubseteq\rangle \xrightarrow[\alpha]{\gamma} \langle\{\alpha(P) \mid P \in \mathcal{C}\},\ \leqslant\rangle : (\!|\mathcal{S}[\![g]\!] = \omega\ ?\ \omega : \Omega|\!)|\!)$

- $\mathcal{S}[\![s \twoheadrightarrow g]\!] \triangleq (\!|\mathcal{S}[\![s]\!] = X \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![g]\!] = \langle\mathcal{C},\ \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle\mathcal{A},\ \leqslant\rangle\ ?\ \langle X \mapsto \mathcal{C},\ \dot{\sqsubseteq}\rangle \xleftrightarrow[\boldsymbol{\lambda}\rho \bullet \alpha \circ \rho]{\boldsymbol{\lambda}\overline{\rho} \bullet \gamma \circ \overline{\rho}} \langle X \mapsto \mathcal{A},\ \dot{\leqslant}\rangle : \mathtt{error}(\mathcal{S}[\![s]\!], (\!|\mathcal{S}[\![g]\!] = \omega\ ?\ \omega : \Omega|\!))|\!)$ for the pointwise orderings $\dot{\sqsubseteq}$ and $\dot{\leqslant}$.

- $\mathcal{S}[\![g_1 \fatsemi g_2]\!] \triangleq (\!|\mathcal{S}[\![g_1]\!] = p_1 \xleftrightarrow[\alpha_1]{\gamma_1} p_2 \wedge \mathcal{S}[\![g_2]\!] = p_3 \xleftrightarrow[\alpha_2]{\gamma_2} p_4\ ?\ (\!|p_2 = p_3\ ?\ p_1 \xleftrightarrow[\alpha_2 \circ \alpha_1]{\gamma_1 \circ \gamma_2} p_4 : \omega|\!) : \mathtt{error}((\!|\mathcal{S}[\![g_1]\!] = \omega\ ?\ \omega : \Omega|\!), (\!|\mathcal{S}[\![g_2]\!] = \omega\ ?\ \omega : \Omega|\!))|\!)$,

- $\mathcal{S}[\![g_1 \circledast g_2]\!] \triangleq (\!|\mathcal{S}[\![g_1]\!] = \langle\mathcal{C}_1,\ \subseteq\rangle \xleftrightarrow[\alpha_1]{\gamma_1} \langle\mathcal{A}_1,\ \sqsubseteq\rangle \wedge \mathcal{S}[\![g_2]\!] = \langle\mathcal{C}_2,\ \Subset\rangle \xleftrightarrow[\alpha_2]{\gamma_2} \langle\mathcal{A}_2,\ \preceq\rangle\ ?\ \langle\mathcal{C}_1 \times \mathcal{C}_2,\ \subseteq \times \subseteq\rangle \xleftrightarrow[\alpha_1 \times \alpha_2]{\gamma_1 \times \gamma_2} \langle\mathcal{A}_1 \times \mathcal{A}_2,\ \sqsubseteq \times \preceq\rangle : \mathtt{error}((\!|\mathcal{S}[\![g_1]\!] = \omega\ ?\ \omega : \Omega|\!), (\!|\mathcal{S}[\![g_2]\!] = \omega\ ?\ \omega : \Omega|\!))|\!)$ (generalizing to tuples),

- $\mathcal{S}[\![g_1 \Longmapsto g_2]\!] \triangleq (\!|\mathcal{S}[\![g_1]\!] = \langle\mathcal{C}_1,\ \subseteq\rangle \xleftrightarrow[\alpha_1]{\gamma_1} \langle\mathcal{A}_1,\ \sqsubseteq\rangle \wedge \mathcal{S}[\![g_2]\!] = \langle\mathcal{C}_2,\ \preceq\rangle \xleftrightarrow[\alpha_2]{\gamma_2} \langle\mathcal{A}_2,\ \leqslant\rangle\ ?\ \langle\mathcal{C}_1 \xrightarrow{\nearrow} \mathcal{C}_2,\ \dot{\preceq}\rangle \xleftrightarrow[\boldsymbol{\lambda} f \bullet \alpha_2 \circ f \circ \gamma_1]{\boldsymbol{\lambda} g \bullet \gamma_2 \circ g \circ \alpha_1} \langle\mathcal{A}_1 \xrightarrow{\nearrow} \mathcal{A}_2,\ \dot{\leqslant}\rangle : \mathtt{error}((\!|\mathcal{S}[\![g_1]\!] = \omega\ ?\ \omega : \Omega|\!), (\!|\mathcal{S}[\![g_2]\!] = \omega\ ?\ \omega : \Omega|\!))|\!)$ for increasing maps and pointwise orderings $\dot{\sqsubseteq}$ and $\dot{\leqslant}$.

4. The POPL'77 abstraction

We express the abstraction that was used in the interval example of [3, 4, p. 247] in the *GC* calculus.

4.1 POPL'77 semantics and semantic properties

- $\mathbb{L}$ labels
- $\mathbb{X}$ variables
- $\langle\mathcal{V}, \leq\rangle$ (*e.g.* $\langle\mathbb{Z}, \leqslant\rangle$ complete partial order of values (*e.g.* $\langle\mathbb{Z}, \leqslant\rangle$ or $\langle[\mathtt{minint}, \mathtt{maxint}], \leqslant\rangle$)
- $\mathcal{M} \triangleq \mathbb{X} \mapsto \mathcal{V}$ memory states
- $\Sigma \triangleq \mathbb{L} \times \mathcal{M} = \mathbb{L} \times (\mathbb{X} \mapsto \mathcal{V})$ states
- Σ^{∞} program runs/executions, *i.e.* finite or infinite sequences of states
- $\mathcal{S} \triangleq \wp(\Sigma^{\infty})$ semantic domain
- $\wp(\mathcal{S})$ semantic properties (*i.e.* the sets of sets of finite or infinite state sequences $\wp(\wp((\mathbb{L} \times (\mathbb{X} \mapsto \mathbb{Z}))^{\infty})))$

4.2 POPL'77 reachability abstraction

The reachability abstraction collects states appearing along execution traces into local invariants on variables attached to program points designated by labels.

- G^*

$$\begin{aligned}
&\triangleq \cup[\Sigma^{\infty}] \fatsemi \infty[\Sigma] \fatsemi \frown[\mathbb{L}, \mathcal{M}] \\
&= \langle\wp(\wp(\Sigma^{\infty})), \subseteq\rangle \xleftrightarrow[\alpha^{\wp}]{\gamma^{\wp}} \langle\wp(\Sigma^{\infty}), \subseteq\rangle \fatsemi \langle\wp(\Sigma^{\infty}), \subseteq\rangle \xleftrightarrow[\alpha^{\infty}]{\gamma^{\infty}} \langle\wp(\Sigma),\ \subseteq\rangle \fatsemi \frown[\mathbb{L}, \mathcal{M}] \\
&= \langle\wp(\wp(\Sigma^{\infty})),\ \subseteq\rangle \xleftrightarrow[\alpha^{\infty} \circ \alpha^{\wp}]{\gamma^{\wp} \circ \gamma^{\infty}} \langle\wp(\Sigma),\ \subseteq\rangle \fatsemi \frown[\mathbb{L}, \mathcal{M}] \\
&= \langle\wp(\wp(\Sigma^{\infty})), \subseteq\rangle \xleftrightarrow[\alpha^{\infty} \circ \alpha^{\wp}]{\gamma^{\wp} \circ \gamma^{\infty}} \langle\wp(\mathbb{L} \times \mathcal{M}), \subseteq\rangle \fatsemi \langle\wp(\mathbb{L} \times \mathcal{M}), \subseteq\rangle \xleftrightarrow[\alpha^{\frown}]{\gamma^{\frown}} \langle\mathbb{L} \mapsto \wp(\mathcal{M}),\ \dot{\subseteq}\rangle \\
&= \langle\wp(\wp(\Sigma^{\infty})),\ \subseteq\rangle \xleftrightarrow[\alpha^{\frown} \circ \alpha^{\infty} \circ \alpha^{\wp}]{\gamma^{\wp} \circ \gamma^{\infty} \circ \gamma^{\frown}} \langle\mathbb{L} \mapsto \wp(\mathcal{M}),\ \dot{\subseteq}\rangle \\
&= \langle\wp(\wp((\mathbb{L} \times (\mathbb{X} \mapsto \mathcal{V}))^{\infty})),\ \subseteq\rangle \xleftrightarrow[\alpha^{\frown} \circ \alpha^{\infty} \circ \alpha^{\wp}]{\gamma^{\wp} \circ \gamma^{\infty} \circ \gamma^{\frown}} \langle\mathbb{L} \mapsto \wp(\mathbb{X} \mapsto \mathcal{V}),\ \dot{\subseteq}\rangle
\end{aligned}$$

4.3 POPL'77 interval cartesian abstraction

- $G^{\mathfrak{I}}$

$\triangleq \mathbb{L} \rightarrowtriangle (\times[\mathbb{X},\mathcal{V}] \fatsemi (\mathbb{X} \rightarrowtriangle \mathbb{I}[\langle\mathcal{V},\ \leq\rangle, -\infty, \infty]))$

$= \mathbb{L} \rightarrowtriangle (\times[\mathbb{X},\mathcal{V}] \fatsemi (\mathbb{X} \rightarrowtriangle \langle\wp(\mathcal{V}),\ \subseteq\rangle \overset{\gamma^{\mathbb{I}}}{\underset{\alpha^{\mathbb{I}}}{\leftrightarrows}} \langle\mathbb{I}(\mathcal{V} \cup \{-\infty,\infty\}, \leq),\ \underline{\oplus}\rangle))$

$= \mathbb{L} \rightarrowtriangle (\times[\mathbb{X},\mathcal{V}] \fatsemi \langle\mathbb{X} \mapsto \wp(\mathcal{V}),\ \dot{\subseteq}\rangle \overset{\boldsymbol{\lambda}\,\overline{\rho}\bullet\gamma^{\mathbb{I}}\circ\overline{\rho}}{\underset{\boldsymbol{\lambda}\,\rho\bullet\alpha^{\mathbb{I}}\circ\rho}{\leftrightarrows}} \langle\mathbb{X} \mapsto \mathbb{I}(\mathcal{V} \cup \{-\infty,\infty\}, \leq),\ \dot{\underline{\oplus}}\rangle)$

$= \mathbb{L} \rightarrowtriangle (\langle\wp(\mathbb{X} \mapsto \mathcal{V}),\ \subseteq\rangle \overset{\gamma^{\times}}{\underset{\alpha^{\times}}{\leftrightarrows}} \langle\mathbb{X} \mapsto \wp(\mathcal{V}),\ \dot{\subseteq}\rangle \fatsemi \langle\mathbb{X} \mapsto \wp(\mathcal{V}),\ \dot{\subseteq}\rangle \overset{\boldsymbol{\lambda}\,\overline{\rho}\bullet\gamma^{\mathbb{I}}\circ\overline{\rho}}{\underset{\boldsymbol{\lambda}\,\rho\bullet\alpha^{\mathbb{I}}\circ\rho}{\leftrightarrows}} \langle\mathbb{X} \mapsto \mathbb{I}(\mathcal{V} \cup \{-\infty,\infty\}, \leq),\ \dot{\underline{\oplus}}\rangle)$

$= \mathbb{L} \rightarrowtriangle (\langle\wp(\mathbb{X} \mapsto \mathcal{V}),\ \subseteq\rangle \overset{\boldsymbol{\lambda}\,\overline{\rho}\bullet\gamma^{\times}(\gamma^{\mathbb{I}}\circ\overline{\rho})}{\underset{\boldsymbol{\lambda}\,P\bullet\alpha^{\mathbb{I}}\circ(\alpha^{\times}(P))}{\leftrightarrows}} \langle\mathbb{X} \mapsto \mathbb{I}(\mathcal{V} \cup \{-\infty,\infty\}, \leq),\ \dot{\underline{\oplus}}\rangle)$

since

- $(\boldsymbol{\lambda}\,\rho\bullet\alpha^{\mathbb{I}} \circ \rho) \circ \alpha^{\times}$

$= \boldsymbol{\lambda}\,P\bullet(\boldsymbol{\lambda}\,\rho\bullet\alpha^{\mathbb{I}} \circ \rho)(\alpha^{\times}(P))$

$= \boldsymbol{\lambda}\,P\bullet\alpha^{\mathbb{I}} \circ (\alpha^{\times}(P))$

$= \boldsymbol{\lambda}\,P\bullet\ \boldsymbol{\lambda}\,\mathtt{x}\bullet\alpha^{\mathbb{I}} \circ (\alpha^{\times}(P))(\mathtt{x})$

$= \boldsymbol{\lambda}\,P\bullet\ \boldsymbol{\lambda}\,\mathtt{x}\bullet\alpha^{\mathbb{I}}((\alpha^{\times}(P))(\mathtt{x}))$

and

- $\gamma^{\times} \circ (\boldsymbol{\lambda}\,\overline{\rho}\bullet\gamma^{\mathbb{I}} \circ \overline{\rho})$

$= \boldsymbol{\lambda}\,\overline{\rho}\bullet\gamma^{\times}((\boldsymbol{\lambda}\,\overline{\rho}\bullet\gamma^{\mathbb{I}} \circ \overline{\rho})(\overline{\rho}))$

$= \boldsymbol{\lambda}\,\overline{\rho}\bullet\gamma^{\times}(\gamma^{\mathbb{I}} \circ \overline{\rho})$

so that

- $G^{\mathfrak{I}}$

$= \langle\mathbb{L} \mapsto \wp(\mathbb{X} \mapsto \mathcal{V}),\ \dot{\subseteq}\rangle \overset{\boldsymbol{\lambda}\,\overline{\rho}\bullet\ \boldsymbol{\lambda}\,\ell\bullet\gamma^{\times}(\boldsymbol{\lambda}\,\mathtt{x}\bullet(\gamma^{\mathbb{I}}(\overline{\rho}(\ell)(\mathtt{x}))))}{\underset{\boldsymbol{\lambda}\,\rho\bullet\ \boldsymbol{\lambda}\,\ell\bullet\ \boldsymbol{\lambda}\,\mathtt{x}\bullet\alpha^{\mathbb{I}}(\alpha^{\times}(\rho(\ell))(\mathtt{x}))}{\leftrightarrows}} \langle\mathbb{L} \mapsto \mathbb{X} \mapsto \mathbb{I}(\mathcal{V} \cup \{-\infty,\infty\}, \leq),\ \ddot{\underline{\oplus}}\rangle$

since

- $\boldsymbol{\lambda}\,\rho\bullet(\boldsymbol{\lambda}\,P\bullet\alpha^{\mathbb{I}} \circ (\alpha^{\times}(P))) \circ \rho$

$= \boldsymbol{\lambda}\,\rho\bullet\ \boldsymbol{\lambda}\,\ell\bullet((\boldsymbol{\lambda}\,P\bullet\alpha^{\mathbb{I}} \circ (\alpha^{\times}(P))) \circ \rho)(\ell)$

$= \boldsymbol{\lambda}\,\rho\bullet\ \boldsymbol{\lambda}\,\ell\bullet(\boldsymbol{\lambda}\,P\bullet\alpha^{\mathbb{I}} \circ (\alpha^{\times}(P)))(\rho(\ell))$

$= \boldsymbol{\lambda}\,\rho\bullet\ \boldsymbol{\lambda}\,\ell\bullet\alpha^{\mathbb{I}} \circ (\alpha^{\times}(\rho(\ell)))$

$= \boldsymbol{\lambda}\,\rho\bullet\ \boldsymbol{\lambda}\,\ell\bullet\ \boldsymbol{\lambda}\,\mathtt{x}\bullet(\alpha^{\mathbb{I}} \circ (\alpha^{\times}(\rho(\ell))))(\mathtt{x})$

$= \boldsymbol{\lambda}\,\rho\bullet\ \boldsymbol{\lambda}\,\ell\bullet\ \boldsymbol{\lambda}\,\mathtt{x}\bullet\alpha^{\mathbb{I}}(\alpha^{\times}(\rho(\ell))(\mathtt{x}))$

and

- $\boldsymbol{\lambda}\,\overline{\rho}\bullet(\boldsymbol{\lambda}\,\overline{\rho}'\bullet\gamma^{\times}(\gamma^{\mathbb{I}} \circ \overline{\rho}')) \circ \overline{\rho}$

$= \boldsymbol{\lambda}\,\overline{\rho}\bullet\ \boldsymbol{\lambda}\,\ell\bullet((\boldsymbol{\lambda}\,\overline{\rho}'\bullet\gamma^{\times}(\gamma^{\mathbb{I}} \circ \overline{\rho}')) \circ \overline{\rho})(\ell)$

$= \boldsymbol{\lambda}\,\overline{\rho}\bullet\ \boldsymbol{\lambda}\,\ell\bullet(\boldsymbol{\lambda}\,\overline{\rho}'\bullet\gamma^{\times}(\gamma^{\mathbb{I}} \circ \overline{\rho}'))(\overline{\rho}(\ell))$

$= \boldsymbol{\lambda}\,\overline{\rho}\bullet\ \boldsymbol{\lambda}\,\ell\bullet(\gamma^{\times}(\gamma^{\mathbb{I}} \circ (\overline{\rho}(\ell))))$

$= \boldsymbol{\lambda}\,\overline{\rho}\bullet\ \boldsymbol{\lambda}\,\ell\bullet(\gamma^{\times}(\boldsymbol{\lambda}\,\mathtt{x}\bullet(\gamma^{\mathbb{I}} \circ (\overline{\rho}(\ell)))(\mathtt{x}))$

$= \boldsymbol{\lambda}\,\overline{\rho}\bullet\ \boldsymbol{\lambda}\,\ell\bullet\gamma^{\times}(\boldsymbol{\lambda}\,\mathtt{x}\bullet(\gamma^{\mathbb{I}}(\overline{\rho}(\ell)(\mathtt{x})))$

4.4 POPL'77 reduced interval cartesian reachability abstraction

- $G^{\mathfrak{I}*}$

$\triangleq \mathsf{R}[G^{*} \fatsemi \mathbb{G}^{\mathfrak{I}}]$

$= \mathsf{R}[\langle\wp(\wp(\Sigma^{\infty})),\ \subseteq\rangle \overset{\gamma^{\wp}\circ\gamma^{\infty}\circ\gamma^{\curvearrowright}}{\underset{\alpha^{\curvearrowright}\circ\alpha^{\infty}\circ\alpha^{\wp}}{\leftrightarrows}} \langle\mathbb{L} \mapsto \wp(\mathbb{X} \mapsto \mathcal{V}),\ \dot{\subseteq}\rangle \fatsemi \langle\mathbb{L} \mapsto \wp(\mathbb{X} \mapsto \mathcal{V}),\ \dot{\subseteq}\rangle \overset{\boldsymbol{\lambda}\,\overline{\rho}\bullet\ \boldsymbol{\lambda}\,\ell\bullet\gamma^{\times}(\boldsymbol{\lambda}\,\mathtt{x}\bullet(\gamma^{\mathbb{I}}(\overline{\rho}(\ell)(\mathtt{x}))))}{\underset{\boldsymbol{\lambda}\,\rho\bullet\ \boldsymbol{\lambda}\,\ell\bullet\ \boldsymbol{\lambda}\,\mathtt{x}\bullet\alpha^{\mathbb{I}}(\alpha^{\times}(\rho(\ell))(\mathtt{x}))}{\leftrightarrows}} \langle\mathbb{L} \mapsto \mathbb{X} \mapsto \mathbb{I}(\mathcal{V} \cup \{-\infty,\infty\}, \leq),\ \ddot{\underline{\oplus}}\rangle]$

$= \mathsf{R}[\langle\wp(\wp(\Sigma^{\infty})), \subseteq\rangle \overset{\boldsymbol{\lambda}\,\overline{\rho}\bullet(\gamma^{\wp}\circ\gamma^{\infty}\circ\gamma^{\curvearrowright})(\boldsymbol{\lambda}\,\ell\bullet\gamma^{\times}(\boldsymbol{\lambda}\,\mathtt{x}\bullet(\gamma^{\mathbb{I}}(\overline{\rho}(\ell)(\mathtt{x})))))}{\underset{\boldsymbol{\lambda}\,P\bullet\ \boldsymbol{\lambda}\,\ell\bullet\ \boldsymbol{\lambda}\,\mathtt{x}\bullet\alpha^{\mathbb{I}}(\alpha^{\times}((\alpha^{\curvearrowright}(\alpha^{\infty}(\alpha^{\wp}(P))))(\ell))(\mathtt{x}))}{\leftrightarrows}} \langle\mathbb{L} \mapsto \mathbb{X} \mapsto \mathbb{I}(\mathcal{V} \cup \{-\infty,\infty\}, \leq),\ \ddot{\underline{\oplus}}\rangle]$

since

- $(\boldsymbol{\lambda}\,\rho\bullet\ \boldsymbol{\lambda}\,\ell\bullet\ \boldsymbol{\lambda}\,\mathtt{x}\bullet\alpha^{\mathbb{I}}(\alpha^{\times}(\rho(\ell))(\mathtt{x}))) \circ (\alpha^{\curvearrowright} \circ \alpha^{\infty} \circ \alpha^{\wp})$

$= \boldsymbol{\lambda}\,P\bullet(\boldsymbol{\lambda}\,\rho\bullet\ \boldsymbol{\lambda}\,\ell\bullet\ \boldsymbol{\lambda}\,\mathtt{x}\bullet\alpha^{\mathbb{I}}(\alpha^{\times}(\rho(\ell))(\mathtt{x})))((\alpha^{\curvearrowright} \circ \alpha^{\infty} \circ \alpha^{\wp})(P))$

$= \boldsymbol{\lambda}\,P\bullet\ \boldsymbol{\lambda}\,\ell\bullet\ \boldsymbol{\lambda}\,\mathtt{x}\bullet\alpha^{\mathbb{I}}(\alpha^{\times}(((\alpha^{\curvearrowright} \circ \alpha^{\infty} \circ \alpha^{\wp})(P))(\ell))(\mathtt{x}))$

$= \boldsymbol{\lambda}\,P\bullet\ \boldsymbol{\lambda}\,\ell\bullet\ \boldsymbol{\lambda}\,\mathtt{x}\bullet\alpha^{\mathbb{I}}(\alpha^{\times}(((\alpha^{\curvearrowright} \circ \alpha^{\infty} \circ \alpha^{\wp})(P))(\ell))(\mathtt{x}))$

$= \boldsymbol{\lambda}\,P\bullet\ \boldsymbol{\lambda}\,\ell\bullet\ \boldsymbol{\lambda}\,\mathtt{x}\bullet\alpha^{\mathbb{I}}(\alpha^{\times}((\alpha^{\curvearrowright}(\alpha^{\infty}(\alpha^{\wp}(P))))(\ell))(\mathtt{x}))$

and

- $(\gamma^{\wp} \circ \gamma^{\infty} \circ \gamma^{\curvearrowright}) \circ (\boldsymbol{\lambda}\,\overline{\rho}'\bullet\ \boldsymbol{\lambda}\,\ell\bullet\gamma^{\times}(\boldsymbol{\lambda}\,\mathtt{x}\bullet(\gamma^{\mathbb{I}}(\overline{\rho}'(\ell)(\mathtt{x})))))$

$= \boldsymbol{\lambda}\,\overline{\rho}\bullet(\gamma^{\wp} \circ \gamma^{\infty} \circ \gamma^{\curvearrowright})((\boldsymbol{\lambda}\,\overline{\rho}'\bullet\ \boldsymbol{\lambda}\,\ell\bullet\gamma^{\times}(\boldsymbol{\lambda}\,\mathtt{x}\bullet(\gamma^{\mathbb{I}}(\overline{\rho}'(\ell)(\mathtt{x})))))(\overline{\rho}))$

$= \boldsymbol{\lambda}\,\overline{\rho}\bullet(\gamma^{\wp} \circ \gamma^{\infty} \circ \gamma^{\curvearrowright})(\boldsymbol{\lambda}\,\ell\bullet\gamma^{\times}(\boldsymbol{\lambda}\,\mathtt{x}\bullet(\gamma^{\mathbb{I}}(\overline{\rho}(\ell)(\mathtt{x})))))$

so that

- $G^{\mathfrak{I}*}$

$= \langle\wp(\wp(\Sigma^{\infty})),\ \subseteq\rangle \overset{\gamma}{\underset{\alpha}{\leftrightarrows}} \langle\mathbb{L} \mapsto \mathbb{X} \mapsto \mathbb{I}(\mathcal{V} \cup \{-\infty,\infty\}, \leq),\ \ddot{\underline{\oplus}}\rangle$

where

- $\alpha \triangleq \boldsymbol{\lambda}\,P\bullet\ \boldsymbol{\lambda}\,\ell\bullet\mathsf{smash}(\boldsymbol{\lambda}\,\mathtt{x}\bullet\alpha^{\mathbb{I}}(\alpha^{\times}((\alpha^{\curvearrowright}(\alpha^{\infty}(\alpha^{\wp}(P))))(\ell))(\mathtt{x})))$
- $\gamma \triangleq \boldsymbol{\lambda}\,\overline{\rho}\bullet(\gamma^{\wp} \circ \gamma^{\infty} \circ \gamma^{\curvearrowright})(\boldsymbol{\lambda}\,\ell\bullet\gamma^{\times}(\boldsymbol{\lambda}\,\mathtt{x}\bullet(\gamma^{\mathbb{I}}(\overline{\rho}(\ell)(\mathtt{x})))))$
  and
- the reduction $\mathsf{smash}(\boldsymbol{\lambda}\,\mathtt{x} \in \mathbb{X}\bullet[a_{\mathtt{x}}, b_{\mathtt{x}}])$ is $\boldsymbol{\lambda}\,\mathtt{x} \in \mathbb{X}\bullet[\infty, -\infty]$ when some $[a_{\mathtt{x}}, b_{\mathtt{x}}]$ is the empty interval with $b_{\mathtt{x}} < a_{\mathtt{x}}$ and $\boldsymbol{\lambda}\,\mathtt{x} \in \mathbb{X}\bullet[a_{\mathtt{x}}, b_{\mathtt{x}}]$ otherwise.

In conclusion, the *static* (or *collecting*) *semantics* is the *reachability abstraction* of program properties in $\wp(\mathcal{S})$ that is $G^{*} \triangleq \cup[\Sigma^{\infty}] \fatsemi \infty[\Sigma] \fatsemi \curvearrowright[\mathbb{L}, \mathcal{M}]$ with abstract domain $\mathbb{L} \mapsto \wp(\mathbb{X} \mapsto \mathcal{V})$. The *reduced interval cartesian reachbility abstraction* is $\mathsf{R}[G^{*} \fatsemi (\mathbb{L} \rightarrowtriangle (\times[\mathbb{X},\mathcal{V}] \fatsemi (\mathbb{X} \rightarrowtriangle \mathbb{I}[\langle\mathcal{V},\ \leq\rangle, -\infty, \infty])))]$ that is the abstraction $\langle\wp(\wp((\mathbb{L} \times (\mathbb{X} \mapsto \mathcal{V}))^{\infty})),\ \subseteq\rangle \overset{\gamma}{\underset{\alpha}{\leftrightarrows}} \langle\mathbb{L} \mapsto \mathbb{X} \mapsto \mathbb{I}(\mathcal{V} \cup \{-\infty,\infty\}),\ \ddot{\underline{\oplus}}\rangle$ where

$$\alpha(P) \triangleq \boldsymbol{\lambda}\,\ell\bullet\mathsf{smash}(\boldsymbol{\lambda}\,\mathtt{x}\bullet\alpha^{\mathbb{I}}(\alpha^{\times}((\alpha^{\curvearrowright}(\alpha^{\infty}(\alpha^{\wp}(P))))(\ell))(\mathtt{x})))$$

and the reduction $\mathsf{smash}(\boldsymbol{\lambda}\,\mathtt{x} \in \mathbb{X}\bullet[a_{\mathtt{x}}, b_{\mathtt{x}}])$ is $\boldsymbol{\lambda}\,\mathtt{x} \in \mathbb{X}\bullet[\infty, -\infty]$ to the empty interval $[\infty, -\infty]$ when some $[a_{\mathtt{x}}, b_{\mathtt{x}}]$ is $[\infty, -\infty]$ and $\boldsymbol{\lambda}\,\mathtt{x} \in \mathbb{X}\bullet[a_{\mathtt{x}}, b_{\mathtt{x}}]$ otherwise.

5. Syntax of types The intuition for types is that a *GC* expression has type T if and only if the semantics of this expression belongs to the set described by type T. For example true has type **bool** which describes the set $\mathbb{B}$ of Booleans since $\mathsf{true} \in \mathbb{B}$.

5.1 Syntax of ur-element types

$\mathsf{E} \in \mathfrak{E}$

$\mathsf{E} ::= \texttt{var} \mid \texttt{lab} \mid \texttt{bool} \mid \texttt{int} \mid \texttt{err}$

5.2 Syntax of set types

$\mathsf{S} \in \mathfrak{S}$

$\mathsf{S} ::= \mathbf{P}\ \mathsf{E} \mid \mathbf{P}\ \mathsf{S} \mid \texttt{seq}\ \mathsf{S} \mid \mathsf{S} \twoheadrightarrow \mathsf{S} \mid \mathsf{S} * \mathsf{S} \mid \texttt{err}$

5.3 Syntax of partial order types

$\mathsf{O} \in \mathfrak{O}$
$\quad \mathsf{O} ::= \Rightarrow \mid \Leftrightarrow \mid \leq \mid \subseteq \mid = \mid \mathsf{O}^{-1} \mid \mathsf{O} \star \mathsf{O} \mid \dot{\mathsf{O}} \mid \ldots \mid \mathtt{err}$

5.4 Syntax of poset types

$\mathsf{P} \in \mathfrak{P}$
$\quad \mathsf{P} ::= \mathsf{S} \circledast \mathsf{O} \mid \mathtt{err}$

5.5 Syntax of *GC* types

$\mathsf{T} \in \mathfrak{T}$
$\quad \mathsf{T} ::= \mathsf{P} \leftrightarrows \mathsf{P} \mid \mathsf{S} \twoheadrightarrow \mathsf{T} \mid \mathtt{err}$

6. Semantics of types

A error type $\mathtt{err}$ denotes any possible value, including the static error (Ω *e.g.* captured by type systems) and the dynamic error (ω *e.g.* possibly captured by static analyzes more powerful than type systems). The error type $\mathtt{err}$ allows to conclude absolutely nothing on a value of that type, including this these value exists or is erroneous.

- $\gamma^{\mathfrak{U}}(\mathtt{err}) \triangleq \mathcal{S}(\mathbb{U}) \cup \{\omega, \Omega\}$ for all $\langle \mathbb{U}, \mathfrak{U}\rangle \in \{\langle \mathbb{E}, \mathfrak{E}\rangle, \langle \mathbb{S}, \mathfrak{S}\rangle, \langle \mathbb{O}, \mathfrak{O}\rangle, \langle \mathbb{P}, \mathfrak{P}\rangle, \langle \mathbb{G}, \mathfrak{T}\rangle\}$ where $\mathcal{S}(\mathbb{U}) \triangleq \{\mathcal{S}[\![u]\!] \mid u \in \mathbb{U}\}$.

6.1 Semantics of ur-element types

- $\gamma^{\mathfrak{E}}(\mathtt{bool}) \triangleq \mathbb{B}$
- $\gamma^{\mathfrak{E}}(\mathtt{int}) \triangleq \mathbb{Z} \cup \{-\infty, \infty\}$
- $\gamma^{\mathfrak{E}}(\mathtt{var}) \triangleq \mathbb{X}$
- $\gamma^{\mathfrak{E}}(\mathtt{lab}) \triangleq \mathbb{L}$
- Observe that $\gamma^{\mathfrak{E}}$ is injective ($\mathsf{E} \neq \mathsf{E}' \Rightarrow \gamma^{\mathfrak{E}}(\mathsf{E}) \neq \gamma^{\mathfrak{E}}(\mathsf{E}')$).

6.2 Semantics of set types

- $\gamma^{\mathfrak{S}}(\mathbf{P}\ \mathsf{E}) \triangleq \wp(\gamma^{\mathfrak{E}}(\mathsf{E}))$
- $\gamma^{\mathfrak{S}}(\mathbf{P}\ \mathsf{S}) \triangleq \wp(\gamma^{\mathfrak{S}}(\mathsf{S}))$
  It follows that $\{\wp(X) \mid X \in \gamma^{\mathfrak{S}}(\mathsf{S})\} \subseteq \gamma^{\mathfrak{S}}(\mathbf{P}\ \mathsf{S})$.
- $\gamma^{\mathfrak{S}}(\mathbf{seq}\ \mathsf{S}) \triangleq \{X^\infty \mid X \in \gamma^{\mathfrak{S}}(\mathsf{S})\}$ where X^∞ is the set of all finite or infinite sequences of elements of X
- $\gamma^{\mathfrak{S}}(\mathsf{S}_1 \twoheadrightarrow \mathsf{S}_2) \triangleq \{X \mapsto Y \mid X \in \gamma^{\mathfrak{S}}(\mathsf{S}_1) \wedge Y \in \gamma^{\mathfrak{S}}(\mathsf{S}_2)\}$
- $\gamma^{\mathfrak{S}}(\mathsf{S}_1 * \mathsf{S}_2) \triangleq \{X \times Y \mid X \in \gamma^{\mathfrak{S}}(\mathsf{S}_1) \wedge Y \in \gamma^{\mathfrak{S}}(\mathsf{S}_2)\}$
- $\forall \mathsf{S} \in \mathfrak{S} : \gamma^{\mathfrak{S}}(\mathsf{S})$ is $\subseteq$-downward closed meaning that $X \subseteq Y \in \gamma^{\mathfrak{S}}(\mathsf{S}) \Rightarrow X \in \gamma^{\mathfrak{S}}(\mathsf{S})$. The proof is by structural induction on S.
- Observe that $\gamma^{\mathfrak{S}}$ is injective (the proof is by structural induction where $\gamma^{\mathfrak{E}}$ is injective for the base case).

6.3 Semantics of partial order types

- $\gamma^{\mathfrak{O}}(\mathsf{O}) \triangleq \{\mathcal{S}[\![\mathsf{O}]\!]\}, \quad \mathsf{O} \in \{\Rightarrow, \Leftrightarrow, \leq, \subseteq, =\}$
- $\gamma^{\mathfrak{O}}(\mathsf{O}^{-1}) \triangleq \{R^{-1} \mid R \in \gamma^{\mathfrak{O}}(\mathsf{O})\}$
- $\gamma^{\mathfrak{O}}(\mathsf{O}_1 \star \mathsf{O}_2) \triangleq \gamma^{\mathfrak{O}}(\mathsf{O}_1) \times \gamma^{\mathfrak{O}}(\mathsf{O}_2) \triangleq \{R_1 \times R_2 \mid R_1 \in \gamma^{\mathfrak{O}}(\mathsf{O}_1) \wedge R_2 \in \gamma^{\mathfrak{O}}(\mathsf{O}_2)\}$
- $\gamma^{\mathfrak{O}}(\dot{\mathsf{O}}) \triangleq \{\dot{\leqslant} \mid \leqslant \in \gamma^{\mathfrak{O}}(\mathsf{O})\}$

Observe, by structural induction on O, that $\gamma^{\mathfrak{O}}(\mathsf{O})$ is always a singleton and $\gamma^{\mathfrak{O}}$ is injective.

6.4 Semantics of poset types

- $\gamma^{\mathfrak{P}}(\mathsf{S} \circledast \mathsf{O}) \triangleq \gamma^{\mathfrak{S}}(\mathsf{S}) \times \gamma^{\mathfrak{O}}(\mathsf{O})$
- $\gamma^{\mathfrak{P}}$ is injective.

6.5 Semantics of *GC* types

- $\gamma^{\mathfrak{T}}(\mathsf{P} \leftrightarrows \mathsf{P}') \triangleq \{P \xleftrightarrow[\alpha]{\gamma} P' \mid P \in \gamma^{\mathfrak{P}}(\mathsf{P}) \wedge P' \in \gamma^{\mathfrak{P}}(\mathsf{P}')\}$ [3].
- $\gamma^{\mathfrak{T}}(\mathsf{S} \twoheadrightarrow \mathsf{T}) \triangleq \{\langle X \mapsto \mathcal{C}, \dot{\sqsubseteq}\rangle \xleftrightarrow[\alpha']{\gamma'} \langle X \mapsto \mathcal{A}, \dot{\leqslant}\rangle \mid X \in \gamma^{\mathfrak{S}}(\mathsf{S}) \wedge \langle \mathcal{C}, \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{A}, \leqslant\rangle \in \gamma^{\mathfrak{T}}(\mathsf{T})\}$
- $\gamma^{\mathfrak{T}}$ is injective.

7. Type membership

Type membership $\Subset$ is the abstraction of set membership $\in$.

- $\mathsf{E} \Subset \mathsf{S} \Rightarrow \forall e \in \gamma^{\mathfrak{E}}(\mathsf{E}) : \exists s \in \gamma^{\mathfrak{S}}(\mathsf{S}) : e \in s$
- $\mathsf{S}_1 \Subset \mathsf{S}_2 \Rightarrow \forall s_1 \in \gamma^{\mathfrak{S}}(\mathsf{S}_1) : \exists s_2 \in \gamma^{\mathfrak{S}}(\mathsf{S}_2) : s_1 \in s_2$

so that

- $\mathsf{E} \Subset \mathbf{P}\ \mathsf{E}$
  For example $\mathtt{bool} \Subset \mathbf{P}\ \mathtt{bool}$ since $\forall b \in \gamma^{\mathfrak{E}}(\mathtt{bool}) = \mathbb{B}$: $\exists B \in \{\emptyset, \{\mathsf{true}\}, \{\mathsf{false}\}, \mathbb{B}\} = \wp(\mathbb{B}) = \wp(\gamma^{\mathfrak{E}}(\mathtt{bool})) = \gamma^{\mathfrak{S}}(\mathbf{P}\ \mathtt{bool})$: $b \in B$.
- $\mathsf{S} \Subset \mathbf{P}\ \mathsf{S}$

Observe that if $\mathsf{E} \not\Subset \mathsf{S}$ (*e.g.* $\mathtt{bool} \not\Subset \mathbf{P}\ \mathtt{int}$) then $\exists e \in \gamma^{\mathfrak{E}}(\mathsf{E}) : \forall s \in \gamma^{\mathfrak{S}}(\mathsf{S}) : e \notin s$ so e of type S belongs to none of the sets s of type S (*e.g.* true belongs to no set of integers).

8. Type preorder

- $\mathsf{T}_1 \trianglelefteq \mathsf{T}_2 \triangleq \gamma^{\mathfrak{T}}(\mathsf{T}_1) \subseteq \gamma^{\mathfrak{T}}(\mathsf{T}_2)$ and similarly for $\mathfrak{S}$, $\mathfrak{O}$, $\mathfrak{P}$, specifically $\mathsf{E}_1 \trianglelefteq \mathsf{E}_2 \triangleq \mathsf{E}_1 = \mathsf{E}_2$ for $\mathfrak{E}$.

The situation would be different if *e.g.* basic types where enriched by intervals *e.g.* as in the PASCAL language, in which case $\trianglelefteq$ would be interval inclusion.

The relation $\trianglelefteq$ is reflexive $\mathsf{T} \trianglelefteq \mathsf{T}$, transitive $\mathsf{T}_1 \trianglelefteq \mathsf{T}_2 \wedge \mathsf{T}_2 \trianglelefteq \mathsf{T}_3 \Rightarrow \mathsf{T}_1 \trianglelefteq \mathsf{T}_3$ and $\mathtt{err}$ is the supremum (top element). To ensure the existence of a best abstraction of the empty set (*i.e.* false property), it may be useful to add a type infimum (bottom element) $\varnothing$ such that $\gamma^{\mathfrak{E}}(\varnothing) \triangleq \emptyset$. It follows from the definition of $\trianglelefteq$ that

- $\mathsf{E} \trianglelefteq \mathsf{E}' \Rightarrow \mathbf{P}\ \mathsf{E} \trianglelefteq \mathbf{P}\ \mathsf{E}'$
- $\mathsf{S} \trianglelefteq \mathsf{S}' \Rightarrow \mathbf{P}\ \mathsf{S} \trianglelefteq \mathbf{P}\ \mathsf{S}'$
- $\mathsf{S} \trianglelefteq \mathsf{S}' \Rightarrow \mathbf{seq}\ \mathsf{S} \trianglelefteq \mathbf{seq}\ \mathsf{S}'$
- $\mathsf{S}_1 \trianglelefteq \mathsf{S}'_1 \wedge \mathsf{S}_2 \trianglelefteq \mathsf{S}'_2 \Rightarrow \mathsf{S}_1 \twoheadrightarrow \mathsf{S}_2 \trianglelefteq \mathsf{S}'_1 \twoheadrightarrow \mathsf{S}'_2$
- $\mathsf{S}_1 \trianglelefteq \mathsf{S}'_1 \wedge \mathsf{S}_2 \trianglelefteq \mathsf{S}'_2 \Rightarrow \mathsf{S}_1 * \mathsf{S}_2 \trianglelefteq \mathsf{S}'_1 * \mathsf{S}'_2$
- $\Leftrightarrow \trianglelefteq \Rightarrow, = \trianglelefteq \leq, = \trianglelefteq \subseteq, = \trianglelefteq \Subset$
- $\mathsf{O} \trianglelefteq \mathsf{O}' \Rightarrow \mathsf{O}^{-1} \trianglelefteq \mathsf{O}'^{-1}$
- $\mathsf{O}_1 \trianglelefteq \mathsf{O}'_1 \wedge \mathsf{O}_2 \trianglelefteq \mathsf{O}'_2 \Rightarrow \mathsf{O}_1 \star \mathsf{O}_2 \trianglelefteq \mathsf{O}'_1 \star \mathsf{O}'_2$
- $\mathsf{O} \trianglelefteq \mathsf{O}' \Rightarrow \dot{\mathsf{O}} \trianglelefteq \dot{\mathsf{O}}'$
- $\mathsf{S} \trianglelefteq \mathsf{S}' \wedge \mathsf{O} \trianglelefteq \mathsf{O}' \Rightarrow \mathsf{S} \circledast \mathsf{O} \trianglelefteq \mathsf{S}' \circledast \mathsf{O}'$
- $\mathsf{P}_1 \trianglelefteq \mathsf{P}'_1 \wedge \mathsf{P}_2 \trianglelefteq \mathsf{P}'_2 \Rightarrow \mathsf{P}_1 \leftrightarrows \mathsf{P}_2 \trianglelefteq \mathsf{P}'_1 \leftrightarrows \mathsf{P}'_2$
- $\mathsf{S} \trianglelefteq \mathsf{S}' \wedge \mathsf{T} \trianglelefteq \mathsf{T}' \Rightarrow \mathsf{S} \twoheadrightarrow \mathsf{T} \trianglelefteq \mathsf{S}' \twoheadrightarrow \mathsf{T}'$

9. Type equivalence

- $\mathsf{T}_1 \cong \mathsf{T}_2 \triangleq \mathsf{T}_1 \trianglelefteq \mathsf{T}_2 \wedge \mathsf{T}_2 \trianglelefteq \mathsf{T}_1 = \gamma^{\mathfrak{S}}(\mathsf{T}_1) = \gamma^{\mathfrak{S}}(\mathsf{T}_2)$

It follows that we have the rule $\mathsf{X} \trianglelefteq \mathsf{Y} \wedge \mathsf{Y} \trianglelefteq \mathsf{X} \Rightarrow \mathsf{X} \cong \mathsf{Y}$ and so $(\mathsf{O}^{-1})^{-1} \cong \mathsf{O}$, $\ddot{\mathsf{O}} \cong \dot{\mathsf{O}}$, *etc.*

[3] By the *GC* notation $\langle C, \preceq\rangle \xleftrightarrow[\alpha]{\gamma} \langle A, \sqsubseteq\rangle, \forall x \in C : \forall y \in A : \alpha(x) \sqsubseteq y \Leftrightarrow x \preceq \gamma(y)$.

10. Type inference algorithm We provide the type inference algorithm and prove its soundness. The classical theory of types, which proceeds by subject reduction, that is by induction on the computation steps of an operational semantics, is not helpful since the *GC* calculus does not describe computations. However Abstract Interpretation is not bound to a specific kind of language, semantics (*e.g.* denotational semantics in [2]), and form of induction (*e.g.* no subject reduction in [2]). So soundness is proved by structural induction on the syntax of types.

The type inference algorithm is

- $\mathscr{E}[\![\mathsf{true}]\!] = \mathscr{E}[\![\mathsf{false}]\!] \triangleq \mathtt{bool}$
- $\mathscr{E}[\![0]\!] = \mathscr{E}[\![1]\!] = \ldots = \mathscr{E}[\![\infty]\!] \triangleq \mathtt{int}$,
- $\mathscr{E}[\![\mathrm{x}]\!] = \mathscr{E}[\![\mathrm{y}]\!] = \ldots \triangleq \mathtt{var}$
- $\mathscr{E}[\![\ell]\!] = \ldots \triangleq \mathtt{lab}$
- $\mathscr{E}[\![-e]\!] \triangleq \llparenthesis \mathscr{E}[\![e]\!] = \mathtt{bool} \vee \mathscr{E}[\![e]\!] = \mathtt{int} \mathrel{?} \mathscr{E}[\![e]\!] \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathcal{S}[\![\mathbb{B}]\!] \triangleq \mathbf{P}\ \mathtt{bool}$
- $\mathcal{S}[\![\mathbb{Z}]\!] \triangleq \mathbf{P}\ \mathtt{int}$
- $\mathcal{S}[\![\mathbb{X}]\!] \triangleq \mathbf{P}\ \mathtt{var}$
- $\mathcal{S}[\![\mathbb{L}]\!] \triangleq \mathbf{P}\ \mathtt{lab}$
- $\mathcal{S}[\![\{e\}]\!] \triangleq \llparenthesis \mathscr{E}[\![e]\!] \neq \mathtt{err} \mathrel{?} \mathbf{P}\ \mathscr{E}[\![e]\!] \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathcal{S}[\![[e_1, e_2]]\!] \triangleq \llparenthesis \mathscr{E}[\![e_1]\!] \cong \mathscr{E}[\![e_2]\!] \neq \mathtt{err} \mathrel{?} \mathbf{P}\ \mathscr{E}[\![e_1]\!] \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathcal{S}[\![\mathbb{I}(s, o)]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \neq \mathtt{err} \mathrel{?} \mathbf{P}\ \mathcal{S}[\![s]\!] \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathcal{S}[\![s^\infty]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \neq \mathtt{err} \mathrel{?} \mathtt{seq}\ \mathcal{S}[\![s]\!] \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathcal{S}[\![s_1 \cup s_2]\!] \triangleq \llparenthesis \mathtt{err} \neq \mathcal{S}[\![s_1]\!] \cong \mathcal{S}[\![s_2]\!] \neq \mathtt{err} \mathrel{?} \mathcal{S}[\![s_1]\!] \mathrel{:} \mathtt{err} \rrparenthesis$ (note the approximation that s_1 and s_2 must be of the same type as is the case for alternatives of conditionals in functional languages)
- $\mathcal{S}[\![s_1 \mapsto s_2]\!] \triangleq \llparenthesis \mathcal{S}[\![s_1]\!] \neq \mathtt{err} \wedge \mathcal{S}[\![s_2]\!] \neq \mathtt{err} \mathrel{?} \mathcal{S}[\![s_1]\!] \mathrel{\ast\!\!\to} \mathcal{S}[\![s_2]\!] \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathcal{S}[\![s_1 \times s_2]\!] \triangleq \llparenthesis \mathcal{S}[\![s_1]\!] \neq \mathtt{err} \wedge \mathcal{S}[\![s_2]\!] \neq \mathtt{err} \mathrel{?} \mathcal{S}[\![s_1]\!] * \mathcal{S}[\![s_2]\!] \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathcal{S}[\![\wp(s)]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \neq \mathtt{err} \mathrel{?} \mathbf{P}\ \mathcal{S}[\![s]\!] \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathscr{O}[\![o]\!] \triangleq o, \quad o \in \{\Rightarrow, \Leftrightarrow, \leq, \subseteq, =\}$
- $\mathscr{O}[\![\stackrel{\pm}{\subseteq}]\!] \triangleq \subseteq$
- $\mathscr{O}[\![o^{-1}]\!] \triangleq (\mathscr{O}[\![o]\!])^{-1}$
- $\mathscr{O}[\![o_1 \times o_2]\!] \triangleq \mathscr{O}[\![o_1]\!] * \mathscr{O}[\![o_2]\!]$
- $\mathscr{O}[\![\dot{o}]\!] \triangleq (\dot{\mathscr{O}[\![o]\!]})$
- $\mathscr{O}[\![\ddot{o}]\!] \triangleq ((\ddot{\mathscr{O}[\![o]\!]}))$
- $\mathscr{P}[\![\langle s,\ o\rangle]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \neq \mathtt{err} \wedge \mathscr{O}[\![o]\!] \neq \mathtt{err} \mathrel{?} \mathcal{S}[\![s]\!] \circledast \mathscr{O}[\![o]\!] \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathscr{T}[\![\mathbb{1}[p]]\!] \triangleq \llparenthesis \mathscr{P}[\![p]\!] \neq \mathtt{err} \mathrel{?} \mathscr{P}[\![p]\!] \leftrightarrows \mathscr{P}[\![p]\!] \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathscr{T}[\![\top[p, e]]\!] \triangleq \llparenthesis \mathscr{E}[\![e]\!] \neq \mathtt{err} \wedge \exists \mathsf{S} \in \mathfrak{S}, \mathsf{O} \in \mathfrak{O} : \mathscr{P}[\![p]\!] = \mathsf{S} \circledast \mathsf{O} \wedge \mathscr{E}[\![e]\!] \Subset \mathsf{S} \mathrel{?} \mathscr{P}[\![p]\!] \leftrightarrows \mathscr{P}[\![p]\!] \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathscr{T}[\![\mathbb{I}[\langle s,\ o\rangle, b, t]]\!] \triangleq \llparenthesis \mathtt{err} \neq \mathscr{E}[\![b]\!] \Subset \mathcal{S}[\![s]\!] \neq \mathtt{err} \wedge \mathtt{err} \neq \mathscr{E}[\![t]\!] \Subset \mathcal{S}[\![s]\!] \mathrel{?} (\mathbf{P}\ \mathcal{S}[\![s]\!] \circledast \subseteq) \leftrightarrows (\mathbf{P}\ \mathcal{S}[\![s]\!] \circledast \subseteq) \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathscr{T}[\![\curvearrowright[s_{\mathbb{L}}, s_{\mathcal{M}}]]\!] \triangleq \llparenthesis \mathcal{S}[\![s_{\mathbb{L}}]\!] \neq \mathtt{err} \wedge \mathcal{S}[\![s_{\mathcal{M}}]\!] \neq \mathtt{err} \mathrel{?} \mathbf{P}\ (\mathcal{S}[\![s_{\mathbb{L}}]\!] * \mathcal{S}[\![s_{\mathcal{M}}]\!]) \circledast \subseteq \leftrightarrows \mathcal{S}[\![s_{\mathbb{L}}]\!] \mathrel{\ast\!\!\to} \mathbf{P}\ \mathcal{S}[\![s_{\mathcal{M}}]\!] \circledast \dot{\subseteq} \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathscr{T}[\![\cup[s]]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \neq \mathtt{err} \mathrel{?} \mathbf{P}\ (\mathbf{P}\ \mathcal{S}[\![s]\!]) \circledast \subseteq \leftrightarrows \mathbf{P}\ \mathcal{S}[\![s]\!] \circledast \subseteq \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathscr{T}[\![\neg[s]]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \neq \mathtt{err} \mathrel{?} \mathbf{P}\ \mathcal{S}[\![s]\!] \circledast \subseteq \leftrightarrows \mathbf{P}\ \mathcal{S}[\![s]\!] \circledast \subseteq^{-1} \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathscr{T}[\![\infty[s]]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \neq \mathtt{err} \mathrel{?} \mathbf{P}\ (\mathtt{seq}\ \mathcal{S}[\![s]\!]) \circledast \subseteq \leftrightarrows \mathbf{P}\ \mathcal{S}[\![s]\!] \circledast \subseteq \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathscr{T}[\![\rightsquigarrow[s_1, s_2]]\!] \triangleq \llparenthesis \mathcal{S}[\![s_1]\!] \neq \mathtt{err} \wedge \mathcal{S}[\![s_2]\!] \neq \mathtt{err} \mathrel{?} \mathbf{P}(\mathcal{S}[\![s_1]\!] * \mathcal{S}[\![s_2]\!]) \circledast \subseteq \leftrightarrows \mathbf{P}\ \mathcal{S}[\![s_1]\!] \mathrel{\ast\!\!\to} \mathbf{P}\ \mathcal{S}[\![s_2]\!] \circledast \dot{\subseteq} \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathscr{T}[\![\mapsto[s_1, s_2]]\!] \triangleq \llparenthesis \mathcal{S}[\![s_1]\!] \neq \mathtt{err} \wedge \mathcal{S}[\![s_2]\!] \neq \mathtt{err} \mathrel{?} \mathbf{P}(\mathcal{S}[\![s_1]\!] \mathrel{\ast\!\!\to} \mathcal{S}[\![s_2]\!]) \circledast \subseteq \leftrightarrows \mathbf{P}\ \mathcal{S}[\![s_1]\!] \mathrel{\ast\!\!\to} \mathbf{P}\ \mathcal{S}[\![s_2]\!] \circledast \dot{\subseteq} \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathscr{T}[\![\times[s_1, s_2]]\!] \triangleq \llparenthesis \mathcal{S}[\![s_1]\!] \neq \mathtt{err} \wedge \mathcal{S}[\![s_2]\!] \neq \mathtt{err} \mathrel{?} \mathbf{P}(\mathcal{S}[\![s_1]\!] \mathrel{\ast\!\!\to} \mathcal{S}[\![s_2]\!]) \circledast \subseteq \leftrightarrows \mathcal{S}[\![s_1]\!] \mathrel{\ast\!\!\to} \mathbf{P}\ \mathcal{S}[\![s_2]\!] \circledast \dot{\subseteq} \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathscr{T}[\![\mathsf{R}[g]]\!] \triangleq \mathscr{T}[\![g]\!]$
- $\mathscr{T}[\![s \multimap g]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \neq \mathtt{err} \wedge \mathscr{T}[\![g]\!] \neq \mathtt{err} \mathrel{?} \mathcal{S}[\![s]\!] \mathrel{\ast\!\!\to} \mathscr{T}[\![g]\!] \mathrel{:} \mathtt{err} \rrparenthesis$

  For brevity, we write $\mathscr{T}[\![s \multimap g]\!] \triangleq \mathcal{S}[\![s]\!] \multimap \mathscr{T}[\![g]\!]$ by defining $\mathsf{S} \multimap \mathsf{T} \triangleq \llparenthesis \mathsf{S} \neq \mathtt{err} \wedge \mathsf{T} \neq \mathtt{err} \mathrel{?} \mathsf{S} \mathrel{\ast\!\!\to} \mathsf{T} \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathscr{T}[\![g_1 \fatsemi g_2]\!] \triangleq \llparenthesis \mathscr{T}[\![g_1]\!] = \mathsf{P}_1 \leftrightarrows \mathsf{P}_2 \wedge \mathscr{T}[\![g_2]\!] = \mathsf{P}_3 \leftrightarrows \mathsf{P}_4 \wedge \mathsf{P}_2 \cong \mathsf{P}_3 \mathrel{?} \mathsf{P}_1 \leftrightarrows \mathsf{P}_4 \mathrel{:} \mathtt{err} \rrparenthesis$

  For brevity, we write $\mathscr{T}[\![g_1 \fatsemi g_2]\!] = \mathscr{T}[\![g_1]\!] \fatsemi \mathscr{T}[\![g_2]\!]$ by defining $\mathsf{T}_1 \fatsemi \mathsf{T}_2 \triangleq \llparenthesis \mathsf{T}_1 = \mathsf{P}_1 \leftrightarrows \mathsf{P}_2 \wedge \mathsf{T}_2 = \mathsf{P}_3 \leftrightarrows \mathsf{P}_4 \wedge \mathsf{P}_2 \cong \mathsf{P}_3 \mathrel{?} \mathsf{P}_1 \leftrightarrows \mathsf{P}_4 \mathrel{:} \mathtt{err} \rrparenthesis$.
- $\mathscr{T}[\![g_1 \circledast g_2]\!] \triangleq \llparenthesis \mathscr{T}[\![g_1]\!] = \mathsf{S}_1 \circledast \mathsf{O}_1 \leftrightarrows \mathsf{S}_2 \circledast \mathsf{O}_2 \wedge \mathscr{T}[\![g_2]\!] = \mathsf{S}_3 \circledast \mathsf{O}_3 \leftrightarrows \mathsf{S}_4 \circledast \mathsf{O}_4 \mathrel{?} \mathsf{S}_1 * \mathsf{S}_2 \circledast \mathsf{O}_1 \star \mathsf{O}_2 \leftrightarrows \mathsf{S}_3 * \mathsf{S}_4 \circledast \mathsf{O}_3 \star \mathsf{O}_4 \mathrel{:} \mathtt{err} \rrparenthesis$
- $\mathscr{T}[\![g_1 \Longrightarrow g_2]\!] \triangleq \llparenthesis \mathscr{T}[\![g_1]\!] = \mathsf{S}_1 \circledast \mathsf{O}_1 \leftrightarrows \mathsf{S}_2 \circledast \mathsf{O}_2 \wedge \mathscr{T}[\![g_2]\!] = \mathsf{S}_3 \circledast \mathsf{O}_3 \leftrightarrows \mathsf{S}_4 \circledast \mathsf{O}_4 \mathrel{?} \mathsf{S}_1 \mathrel{\ast\!\!\to} \mathsf{S}_3 \circledast \dot{\mathsf{O}}_3 \leftrightarrows \mathsf{S}_2 \mathrel{\ast\!\!\to} \mathsf{S}_4 \circledast \dot{\mathsf{O}}_4 \mathrel{:} \mathtt{err} \rrparenthesis$

For example the type of the *GC* expression describing the interval example of [3, 4, p. 247] is

$$
\begin{aligned}
& \mathscr{T}[\![\cup[(\mathbb{L} \times (\mathbb{X} \mapsto \mathbb{Z}))^\infty] \fatsemi \infty[\mathbb{L} \times (\mathbb{X} \mapsto \mathbb{Z})] \fatsemi \curvearrowright[\mathbb{L}, \mathbb{X} \mapsto \mathbb{Z}] \fatsemi \mathbb{L} \multimap (\times[\mathbb{X}, \mathbb{Z}] \fatsemi (\mathbb{X} \multimap \mathbb{I}[\langle \mathbb{Z},\ \leq\rangle, -\infty, \infty]))]\!] \\
= \ & \mathscr{T}[\![\cup[(\mathbb{L} \times (\mathbb{X} \mapsto \mathbb{Z}))^\infty] \fatsemi \infty[\mathbb{L} \times (\mathbb{X} \mapsto \mathbb{Z})] \fatsemi \curvearrowright[\mathbb{L}, \mathbb{X} \mapsto \mathbb{Z}] \fatsemi \mathbb{L} \multimap (\times[\mathbb{X}, \mathbb{Z}]\!] \fatsemi (\mathbf{P}\ \mathtt{var} \multimap (\mathbf{P}\ \mathbf{P}\ \mathtt{int} \circledast \subseteq) \leftrightarrows (\mathbf{P}\ \mathbf{P}\ \mathtt{int} \circledast \subseteq))) \\
= \ & \mathscr{T}[\![\cup[(\mathbb{L} \times (\mathbb{X} \mapsto \mathbb{Z}))^\infty] \fatsemi \infty[\mathbb{L} \times (\mathbb{X} \mapsto \mathbb{Z})] \fatsemi \curvearrowright[\mathbb{L}, \mathbb{X} \mapsto \mathbb{Z}]]\!] \fatsemi \mathbf{P}\ \mathtt{lab} \multimap ((\mathbf{P}(\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{int}) \circledast \subseteq) \leftrightarrows (\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathbf{P}\ \mathtt{int} \circledast \dot{\subseteq}) \fatsemi (\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathbf{P}\ \mathtt{int} \circledast \dot{\subseteq}) \leftrightarrows (\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathbf{P}\ \mathtt{int} \circledast \dot{\subseteq})) \\
= \ & \mathscr{T}[\![\cup[(\mathbb{L} \times (\mathbb{X} \mapsto \mathbb{Z}))^\infty] \fatsemi \infty[\mathbb{L} \times (\mathbb{X} \mapsto \mathbb{Z})] \fatsemi \curvearrowright[\mathbb{L}, \mathbb{X} \mapsto \mathbb{Z}]]\!] \fatsemi \mathbf{P}\ \mathtt{lab} \multimap ((\mathbf{P}(\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{int}) \circledast \subseteq) \leftrightarrows (\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathbf{P}\ \mathtt{int} \circledast \dot{\subseteq})) \\
= \ & \mathscr{T}[\![\cup[(\mathbb{L} \times (\mathbb{X} \mapsto \mathbb{Z}))^\infty] \fatsemi \infty[\mathbb{L} \times (\mathbb{X} \mapsto \mathbb{Z})]]\!] \fatsemi \mathbf{P}\ (\mathbf{P}\ \mathtt{lab} * (\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{int})) \circledast \subseteq \leftrightarrows \mathbf{P}\ \mathtt{lab} \mathrel{\ast\!\!\to} \mathbf{P}\ (\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{int}) \circledast \dot{\subseteq} \fatsemi ((\mathbf{P}\ \mathtt{lab} \mathrel{\ast\!\!\to} \mathbf{P}(\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{int}) \circledast \dot{\subseteq}) \leftrightarrows (\mathbf{P}\ \mathtt{lab} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathbf{P}\ \mathtt{int} \circledast \ddot{\subseteq})) \\
= \ & \mathscr{T}[\![\cup[(\mathbb{L} \times (\mathbb{X} \mapsto \mathbb{Z}))^\infty]]\!] \fatsemi \mathbf{P}\ (\mathtt{seq}\ (\mathbf{P}\ \mathtt{lab} * (\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{int}))) \circledast \subseteq \leftrightarrows \mathbf{P}\ (\mathbf{P}\ \mathtt{lab} * (\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{int})) \circledast \subseteq \fatsemi \mathbf{P}\ (\mathbf{P}\ \mathtt{lab} * (\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{int})) \circledast \subseteq \leftrightarrows (\mathbf{P}\ \mathtt{lab} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathbf{P}\ \mathtt{int} \circledast \ddot{\subseteq}) \\
= \ & \mathbf{P}\ (\mathbf{P}\ (\mathtt{seq}\ (\mathbf{P}\ \mathtt{lab} * (\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{int})))) \circledast \subseteq \leftrightarrows \mathbf{P}\ (\mathtt{seq}\ (\mathbf{P}\ \mathtt{lab} * (\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{int}))) \circledast \subseteq \fatsemi \mathbf{P}\ (\mathtt{seq}\ (\mathbf{P}\ \mathtt{lab} * (\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{int}))) \circledast \subseteq \leftrightarrows (\mathbf{P}\ \mathtt{lab} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathbf{P}\ \mathtt{int} \circledast \ddot{\subseteq}) \\
= \ & \mathbf{P}\ (\mathbf{P}\ (\mathtt{seq}\ (\mathbf{P}\ \mathtt{lab} * (\mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{int})))) \circledast \subseteq \leftrightarrows (\mathbf{P}\ \mathtt{lab} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathtt{var} \mathrel{\ast\!\!\to} \mathbf{P}\ \mathbf{P}\ \mathtt{int} \circledast \ddot{\subseteq})
\end{aligned}
$$

Intuitively, sets of sets of sequences of states are abstracted by a map of labels to variables to intervals *i.e.* sets of integers (the difference as abstracted away by the type abstraction).

10.1 Soundness of the type inference algorithm

$\forall \mathsf{T} \in \mathfrak{T} \setminus \{\mathtt{err}\} : \Omega \notin \gamma^{\mathfrak{T}}(\mathsf{T})$ so the soundness of type inference is $\llparenthesis \mathscr{T}[\![g]\!] \neq \mathtt{err} \mathrel{?} \mathcal{S}[\![g]\!] \in \gamma^{\mathfrak{T}}(\mathscr{T}[\![g]\!]) \cup \{\omega\} \rrparenthesis$ *i.e.* "typepable expressions cannot go wrong (*i.e.* return Ω but may return a runtime error ω)". There is no soundness requirement to prove in case of static type error $\mathcal{T}[\![g]\!] = \texttt{err}$ since untypble expressions are rejected. There is also nothing to prove when the semantics returns a dynamic error ω since types say nothing on possible dynamic errors (*e.g.* the type $\texttt{int}$ does no prevent overflows).

For example,

$$
\begin{aligned}
&\mathcal{S}[\![\mathbb{I}(\mathbb{Z}, \leq)]\!] \\
\triangleq\ & (\!| \mathcal{S}[\![\mathbb{Z}]\!] = S \notin \{\omega, \Omega\} \ ?\ (\!| \mathcal{S}[\![\leq]\!] \subseteq S \times S \ ?\ \{\{v \in S \mid \langle v_1,\ v\rangle \in \mathcal{S}[\![\leq]\!] \wedge \langle v,\ v_2\rangle \in \mathcal{S}[\![\leq]\!]\} \mid v_1, v_2 \in S\} \ ⁏\ \omega |\!) \ ⁏\ \mathcal{S}[\![\mathbb{Z}]\!] |\!) \\
=\ & (\!| \mathcal{S}[\![\leq]\!] \subseteq \mathbb{Z} \times \mathbb{Z} \ ?\ \{\{v \in \mathbb{Z} \mid \langle v_1,\ v\rangle \in \mathcal{S}[\![\leq]\!] \wedge \langle v,\ v_2\rangle \in \mathcal{S}[\![\leq]\!]\} \mid v_1, v_2 \in \mathbb{Z}\} \ ⁏\ \omega |\!) \\
=\ & \{\{v \in \mathbb{Z} \mid \langle v_1,\ v\rangle \in \mathcal{S}[\![\leq]\!] \wedge \langle v,\ v_2\rangle \in \mathcal{S}[\![\leq]\!]\} \mid v_1, v_2 \in \mathbb{Z}\} \\
=\ & \{\{v \in \mathbb{Z} \mid v_1 \leq v \langle v,\ \leq\rangle v_2\} \mid v_1, v_2 \in \mathbb{Z}\} \\
=\ & \{[v_1, v_2] \mid v_1, v_2 \in \mathbb{Z}\} \\
\in\ & \{\wp(X) \mid X \in \wp(\mathbb{Z} \cup \{-\infty, \infty\})\} \\
=\ & \{\wp(X) \mid X \in \wp(\gamma^{\mathfrak{E}}(\texttt{int}))\} \\
=\ & \{\wp(X) \mid X \in \gamma^{\mathfrak{S}}(\texttt{P int})\} \\
\subseteq\ & \gamma^{\mathfrak{S}}(\texttt{P P int}) \\
=\ & \gamma^{\mathfrak{S}}(\texttt{P}\ \mathcal{S}[\![\mathbb{Z}]\!]) \\
\subseteq\ & \gamma^{\mathfrak{S}}(\texttt{P}\ \mathcal{S}[\![\mathbb{Z}]\!]) \cup \{\omega\}
\end{aligned}
$$

10.2 Soundness of element type inference

- $\mathscr{E}[\![\mathsf{true}]\!] = \mathscr{E}[\![\mathsf{false}]\!] \triangleq \texttt{bool}$
  $\mathcal{S}[\![\mathsf{true}]\!] = \mathsf{true} \in \mathbb{B} = \gamma^{\mathfrak{E}}(\texttt{bool}) = \gamma^{\mathfrak{E}}(\mathscr{E}[\![\mathsf{true}]\!])$, *etc.*
- $\mathscr{E}[\![0]\!] = \mathscr{E}[\![1]\!] = \ldots = \mathscr{E}[\![\infty]\!] \triangleq \texttt{int}$,
  $\mathcal{S}[\![0]\!] = 0 \in \mathbb{Z} \cup \{-\infty, \infty\} = \gamma^{\mathfrak{E}}(\texttt{int}) = \gamma^{\mathfrak{E}}(\mathscr{E}[\![0]\!])$, *etc.*
- $\mathscr{E}[\![\mathrm{x}]\!] = \mathscr{E}[\![\mathrm{y}]\!] = \ldots \triangleq \texttt{var}$
  $\mathcal{S}[\![\mathrm{x}]\!] = \mathrm{x} \in \mathbb{X} = \gamma^{\mathfrak{E}}(\texttt{var}) = \gamma^{\mathfrak{E}}(\mathscr{E}[\![\mathrm{x}]\!])$, *etc.*
- $\mathscr{E}[\![\ell]\!] = \ldots \triangleq \texttt{lab}$
  $\mathcal{S}[\![\ell]\!] = \ell \in \mathbb{L} = \gamma^{\mathfrak{E}}(\texttt{lab}) = \gamma^{\mathfrak{E}}(\mathscr{E}[\![\ell]\!])$,
- $\mathscr{E}[\![-e]\!] = (\!| \mathscr{E}[\![e]\!] = \texttt{bool} \vee \mathscr{E}[\![e]\!] = \texttt{int} \ ?\ \mathscr{E}[\![e]\!] \ ⁏\ \texttt{err} |\!)$
  - if $\mathscr{E}[\![e]\!] = \texttt{bool}$ then $\mathcal{S}[\![e]\!] \in \gamma^{\mathfrak{E}}(\mathscr{E}[\![e]\!]) = \gamma^{\mathfrak{E}}(\texttt{bool}) = \mathbb{B}$ by structural induction hypothesis so $\mathcal{S}[\![-e]\!] = \neg\mathcal{S}[\![e]\!] \in \mathbb{B} = \gamma^{\mathfrak{E}}(\texttt{bool}) = \gamma^{\mathfrak{E}}(\mathscr{E}[\![-e]\!])$
  - else if $\mathscr{E}[\![e]\!] = \texttt{int}$, *Id.*
  - else $\mathscr{E}[\![e]\!] = \texttt{err}$, no requirement to prove.
- Observe that when $\mathcal{O}[\![e]\!] \neq \Omega$, $\mathcal{O}[\![e]\!]$ has been defined in Sect. 3.1 to be a poset of the form $\mathcal{O}[\![e]\!] = \langle \gamma^{\mathfrak{E}}(\mathscr{E}[\![e]\!]),\ o\rangle$

10.3 Soundness of set type inference

- $\mathbb{S}[\![\mathbb{B}]\!] \triangleq \texttt{P bool}$
  $\mathcal{S}[\![\mathbb{B}]\!] = \mathbb{B} \in \wp(\mathbb{B}) = \wp(\gamma^{\mathfrak{E}}(\texttt{bool})) = \gamma^{\mathfrak{S}}(\texttt{P bool}) = \gamma^{\mathfrak{S}}(\mathbb{S}[\![\mathbb{B}]\!])$ *QED.*
- $\mathbb{S}[\![\mathbb{Z}]\!] \triangleq \texttt{P int}$
  Id.
- $\mathbb{S}[\![\mathbb{X}]\!] \triangleq \texttt{P var}$
  Id.
- $\mathbb{S}[\![\mathbb{L}]\!] \triangleq \texttt{P lab}$
  Id.
- $\mathbb{S}[\![\{e\}]\!] \triangleq (\!| \mathscr{E}[\![e]\!] \neq \texttt{err} \ ?\ \texttt{P}\ \mathscr{E}[\![e]\!] \ ⁏\ \texttt{err} |\!)$

  By structural induction hypothesis, $\mathcal{S}[\![e]\!] \in \gamma^{\mathfrak{E}}(\mathscr{E}[\![e]\!])$ so $\forall \mathsf{E} \in \mathfrak{E} \setminus \{\texttt{err}\} : \Omega \notin \gamma^{\mathfrak{E}}(\mathsf{E})$ and $\mathscr{E}[\![e]\!] \neq \texttt{err}$ imply that $\mathcal{S}[\![e]\!] \neq \Omega$ so $\mathcal{S}[\![\{e\}]\!] = (\!| \mathcal{S}[\![e]\!] \neq \Omega \ ?\ \{\mathcal{S}[\![e]\!]\} \ ⁏\ \Omega |\!) = \{\mathcal{S}[\![e]\!]\} \in \wp(\gamma^{\mathfrak{E}}(\mathscr{E}[\![e]\!])) = \gamma^{\mathfrak{S}}(\texttt{P}\ \mathscr{E}[\![e]\!]) = \gamma^{\mathfrak{S}}(\mathbb{S}[\![\{e\}]\!])$
- $\mathbb{S}[\![[e_1, e_2]]\!] \triangleq (\!| \mathscr{E}[\![e_1]\!] \cong \mathscr{E}[\![e_2]\!] \neq \texttt{err} \ ?\ \texttt{P}\ \mathscr{E}[\![e_1]\!] \ ⁏\ \texttt{err} |\!)$

  No requirement has to be proved when $\mathbb{S}[\![[e_1, e_2]]\!] = \texttt{err}$. Otherwise $\mathscr{E}[\![e_1]\!] \cong \mathscr{E}[\![e_2]\!] \neq \texttt{err}$ and $\mathbb{S}[\![[e_1, e_2]]\!] = \texttt{P}\ \mathscr{E}[\![e_1]\!]$, in which case we must prove that $\mathcal{S}[\![[e_1, e_2]]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![[e_1, e_2]]\!])$.

  $\mathscr{E}[\![e_1]\!] \cong \mathscr{E}[\![e_2]\!]$ implies $\gamma^{\mathfrak{E}}(\mathscr{E}[\![e_1]\!]) = \gamma^{\mathfrak{E}}(\mathscr{E}[\![e_2]\!])$ (and reciprocally). But $\gamma^{\mathfrak{E}}$ is injective so $\mathscr{E}[\![e_1]\!] = \mathscr{E}[\![e_2]\!] \neq \texttt{err}$. Morover, $\forall \mathsf{E} \in \mathfrak{E} \setminus \{\texttt{err}\} : \Omega \notin \gamma^{\mathfrak{E}}(\mathsf{E})$ and $\mathscr{E}[\![e_i]\!] \neq \texttt{err}$ imply that $\Omega \notin \gamma^{\mathfrak{E}}(\mathscr{E}[\![e_i]\!])$, $i = 1, 2$. By structural induction hypothesis, $\mathcal{S}[\![e_i]\!] \in \gamma^{\mathfrak{E}}(\mathscr{E}[\![e_i]\!])$, $i = 1, 2$, so that $\mathcal{S}[\![e_i]\!] \neq \Omega$.
  - In case $\mathcal{O}[\![e_1]\!] = \mathcal{O}[\![e_2]\!] = \langle S,\ o\rangle$, $\mathcal{O}[\![e_i]\!] \neq \Omega$ so $\mathcal{O}[\![e_i]\!] = \langle \gamma^{\mathfrak{E}}(\mathscr{E}[\![e_i]\!]),\ o_i\rangle$ implies that $S = \gamma^{\mathfrak{E}}(\mathscr{E}[\![e_i]\!])$. It follows that $\mathcal{S}[\![[e_1, e_2]]\!] \triangleq (\!| \mathcal{O}[\![e_1]\!] = \mathcal{O}[\![e_2]\!] = \langle S,\ o\rangle \ ?\ \{v \in S \mid \langle \mathcal{S}[\![e_1]\!],\ v\rangle \in o \wedge \langle v,\ \mathcal{S}[\![e_2]\!]\rangle \in 0\} \ ⁏\ \Omega |\!) = \{v \in \gamma^{\mathfrak{E}}(\mathscr{E}[\![e_1]\!]) \mid \langle \mathcal{S}[\![e_1]\!],\ v\rangle \in o \wedge \langle v,\ \mathcal{S}[\![e_2]\!]\rangle \in 0\} \in \wp(\gamma^{\mathfrak{E}}(\mathscr{E}[\![e_1]\!])) \triangleq \gamma^{\mathfrak{S}}(\texttt{P}\ \mathscr{E}[\![e_1]\!]) = \gamma^{\mathfrak{S}}(\mathbb{S}[\![[e_1, e_2]]\!])$, *QED.*
  - In case $\mathcal{O}[\![e_1]\!] = \langle S_1,\ o_1\rangle \neq \mathcal{O}[\![e_2]\!] = \langle S_2,\ o_2\rangle$, we have $\mathcal{O}[\![e_i]\!] \neq \Omega$ so $\mathcal{O}[\![e_i]\!] = \langle \gamma^{\mathfrak{E}}(\mathscr{E}[\![e_i]\!]),\ o_i\rangle$. Therefore $\mathscr{E}[\![e_1]\!] = \mathscr{E}[\![e_2]\!]$ implies $S_1 = S_2$. It follows that $o_1 \neq o_2$, which is in contradiction with the definition of $\mathcal{O}$ in Sect. 3.1. By reductio ad absurdum, this case is impossible.
  - The last possible case is $\mathcal{O}[\![e_1]\!] = \Omega$ or $\mathcal{O}[\![e_2]\!] = \Omega$. By def. of $\mathcal{O}$ in Sect. 3.1, one of e_1 or e_2 is of the form $e_i = -e'_i$ with $\mathcal{S}[\![e'_i]\!] \notin \mathbb{B} \wedge \mathcal{S}[\![e'_i]\!] \notin \mathbb{Z} \cup \{-\infty, \infty\}$, which implies that $\mathcal{S}[\![e_i]\!] = \Omega$, a contradiction. By reductio ad absurdum, this case is also impossible.

  In conclusion, $\mathcal{S}[\![[e_1, e_2]]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![[e_1, e_2]]\!])$. *QED.*
- $\mathbb{S}[\![\mathbb{I}(s, o)]\!] \triangleq (\!| \mathbb{S}[\![s]\!] \neq \texttt{err} \ ?\ \texttt{P}\ \mathbb{S}[\![s]\!] \ ⁏\ \texttt{err} |\!)$

  In case $\mathbb{S}[\![\mathbb{I}(s, o)]\!] \neq \texttt{err}$, $\mathbb{S}[\![s]\!] \neq \texttt{err}$ so, by structural induction hypothesis, $\mathcal{S}[\![s]\!] \in (\gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!]) \cup \{\omega\}) \setminus \{\Omega\}$.
  - In case, $\mathcal{S}[\![s]\!] = \omega$, we have $\mathcal{S}[\![\mathbb{I}(s, o)]\!] \triangleq (\!| \mathcal{S}[\![s]\!] = S \notin \{\omega, \Omega\} \ ?\ (\!| \mathcal{S}[\![o]\!] \subseteq S \times S \ ?\ \{\{v \in S \mid \langle v_1,\ v\rangle \in \mathcal{S}[\![o]\!] \wedge \langle v,\ v_2\rangle \in \mathcal{S}[\![o]\!]\} \mid v_1, v_2 \in S\} \ ⁏\ \omega |\!) \ ⁏\ \mathcal{S}[\![s]\!] |\!) = \mathcal{S}[\![s]\!] = \omega$ in which case $\mathcal{S}[\![\mathbb{I}(s, o)]\!] \in \{\omega\}$
  - Otherwise, in case $\mathcal{S}[\![s]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!])$ and $\mathcal{S}[\![o]\!] \nsubseteq S \times S$, $\mathcal{S}[\![\mathbb{I}(s, o)]\!] \triangleq \mathcal{S}[\![\mathbb{I}(s, o)]\!] \triangleq (\!| \mathcal{S}[\![s]\!] = S \notin \{\omega, \Omega\} \ ?\ (\!| \mathcal{S}[\![o]\!] \subseteq S \times S \ ?\ \{\{v \in S \mid \langle v_1,\ v\rangle \in \mathcal{S}[\![o]\!] \wedge \langle v,\ v_2\rangle \in \mathcal{S}[\![o]\!]\} \mid v_1, v_2 \in S\} \ ⁏\ \omega |\!) \ ⁏\ \mathcal{S}[\![s]\!] |\!) = \omega$ so $\mathcal{S}[\![\mathbb{I}(s, o)]\!] \in \{\omega\}$
  - Otherwise $\mathcal{S}[\![s]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!])$ and $\mathcal{S}[\![o]\!] \subseteq S \times S$ and so $\mathcal{S}[\![\mathbb{I}(s, o)]\!] \triangleq (\!| \mathcal{S}[\![s]\!] = S \notin \{\omega, \Omega\} \ ?\ (\!| \mathcal{S}[\![o]\!] \subseteq S \times S \ ?\ \{\{v \in S \mid \langle v_1,\ v\rangle \in \mathcal{S}[\![o]\!] \wedge \langle v,\ v_2\rangle \in \mathcal{S}[\![o]\!]\} \mid v_1, v_2 \in S\} \ ⁏\ \omega |\!) \ ⁏\ \mathcal{S}[\![s]\!] |\!) = \{\{v \in \mathcal{S}[\![s]\!] \mid \langle v_1,\ v\rangle \in \mathcal{S}[\![o]\!] \wedge \langle v,\ v_2\rangle \in \mathcal{S}[\![o]\!]\} \mid v_1, v_2 \in \mathcal{S}[\![s]\!]\} \in \{\wp(X) \mid X \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!])\} \subseteq \gamma^{\mathfrak{S}}(\texttt{P}\ \mathbb{S}[\![s]\!])$
  - In all cases, we have $\mathcal{S}[\![\mathbb{I}(s, o)]\!] \in \gamma^{\mathfrak{S}}(\texttt{P}\ \mathbb{S}[\![s]\!]) \cup \{\omega\}$. *QED.*
- $\mathbb{S}[\![s^{\infty}]\!] \triangleq (\!| \mathbb{S}[\![s]\!] \neq \texttt{err} \ ?\ \texttt{seq}\ \mathbb{S}[\![s]\!] \ ⁏\ \texttt{err} |\!)$

  In case $\mathbb{S}[\![s^{\infty}]\!] \neq \texttt{err}$, $\mathbb{S}[\![s]\!] \neq \texttt{err}$ so, by structural induction hypothesis, $\mathcal{S}[\![s]\!] \in (\gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!]) \cup \{\omega\}) \setminus \{\Omega\}$.

- The case $\mathcal{S}[\![s]\!] = \Omega$ is impossible since $\mathbb{S}[\![s^\infty]\!] \neq \texttt{err}$
- In case $\mathcal{S}[\![s]\!] = \omega$, $\mathcal{S}[\![s^\infty]\!] \triangleq (\!|\mathcal{S}[\![s]\!] \notin \{\omega, \Omega\} \mathrel{?} \mathcal{S}[\![s]\!]^\infty \mathrel{⨟} \mathcal{S}[\![s]\!]|\!) = \omega \in \{\omega\}$
- Otherwise, $\mathcal{S}[\![s]\!] \notin \{\omega, \Omega\}$ so $\mathcal{S}[\![s]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!])$ and $\mathcal{S}[\![s^\infty]\!] \triangleq (\!|\mathcal{S}[\![s]\!] \notin \{\omega, \Omega\} \mathrel{?} \mathcal{S}[\![s]\!]^\infty \mathrel{⨟} \mathcal{S}[\![s]\!]|\!) = \mathcal{S}[\![s]\!]^\infty \in \{X^\infty \mid X \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!])\} \triangleq \gamma^{\mathfrak{S}}(\texttt{seq}\,\mathbb{S}[\![s]\!]) = \gamma^{\mathfrak{S}}(\mathbb{S}[\![s^\infty]\!])$.

We conclude that $\mathbb{S}[\![s^\infty]\!] \neq \Omega$ implies that $\mathcal{S}[\![s^\infty]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s^\infty]\!]) \cup \{\omega\}$. *QED.*

- $\mathbb{S}[\![s_1 \cup s_2]\!] \triangleq (\!|\texttt{err} \neq \mathbb{S}[\![s_1]\!] \cong \mathbb{S}[\![s_2]\!] \neq \texttt{err} \mathrel{?} \mathbb{S}[\![s_1]\!] \mathrel{⨟} \texttt{err}|\!)$

In case $\mathbb{S}[\![s_1 \cup s_2]\!] \neq \texttt{err}$, we have $\mathbb{S}[\![s_1]\!] \neq \texttt{err}$ and $\mathbb{S}[\![s_2]\!] \neq \texttt{err}$ so $\mathbb{S}[\![s_1 \cup s_2]\!] = \mathbb{S}[\![s_1]\!]$ and, by structural induction hypothesis, $\mathcal{S}[\![s_1]\!] \in (\gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1]\!]) \cup \{\omega\}) \setminus \{\Omega\} = (\gamma^{\mathfrak{S}}(\mathbb{S}[\![s_2]\!]) \cup \{\omega\}) \setminus \{\Omega\} \ni \mathcal{S}[\![s_2]\!]$.

- In case $\mathcal{S}[\![s_1]\!] \in \{\omega, \Omega\} \vee \mathcal{S}[\![s_2]\!] \in \{\omega, \Omega\}$, we have $\mathcal{S}[\![s_1]\!] = \omega \vee \mathcal{S}[\![s_2]\!] = \omega$ so $\mathcal{S}[\![s_1 \cup s_2]\!] \triangleq (\!|\mathcal{S}[\![s_1]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![s_2]\!] \notin \{\omega, \Omega\} \mathrel{?} \mathcal{S}[\![s_1]\!] \cup \mathcal{S}[\![s_2]\!] \mathrel{⨟} \texttt{error}(\mathcal{S}[\![s_1]\!], \mathcal{S}[\![s_2]\!])|\!) = \texttt{error}(\mathcal{S}[\![s_1]\!], \mathcal{S}[\![s_2]\!]) = \omega \in \{\omega\}$
- Otherwise, $\mathcal{S}[\![s_1]\!] \neq \omega \wedge \mathcal{S}[\![s_2]\!] \neq \omega$ so $\mathcal{S}[\![s_1 \cup s_2]\!] \triangleq (\!|\mathcal{S}[\![s_1]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![s_2]\!] \notin \{\omega, \Omega\} \mathrel{?} \mathcal{S}[\![s_1]\!] \cup \mathcal{S}[\![s_2]\!] \mathrel{⨟} \texttt{error}(\mathcal{S}[\![s_1]\!], \mathcal{S}[\![s_2]\!])|\!) = \mathcal{S}[\![s_1]\!] \cup \mathcal{S}[\![s_2]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1]\!]) \cup \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_2]\!]) = \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1]\!]) = \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1 \cup s_2]\!])$
- In both cases, $\mathcal{S}[\![s_1 \cup s_2]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1 \cup s_2]\!]) \cup \{\omega\}$. *QED.*

- $\mathbb{S}[\![s_1 \mapsto s_2]\!] \triangleq (\!|\mathbb{S}[\![s_1]\!] \neq \texttt{err} \wedge \mathbb{S}[\![s_2]\!] \neq \texttt{err} \mathrel{?} \mathbb{S}[\![s_1]\!] \twoheadleftarrow\!\!\!\rightarrow \mathbb{S}[\![s_2]\!] \mathrel{⨟} \texttt{err}|\!)$

In case $\mathbb{S}[\![s_1 \mapsto s_2]\!] \neq \texttt{err}$, we have $\mathbb{S}[\![s_1]\!] \neq \texttt{err}$ and $\mathbb{S}[\![s_2]\!] \neq \texttt{err}$ so $\mathbb{S}[\![s_1 \mapsto s_2]\!] = \mathbb{S}[\![s_1]\!] \twoheadleftarrow\!\!\!\rightarrow \mathbb{S}[\![s_2]\!]$ and, by structural induction hypothesis, $\mathcal{S}[\![s_1]\!] \in (\gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1]\!]) \cup \{\omega\}) \setminus \{\Omega\}$ and $\mathcal{S}[\![s_2]\!] \in (\gamma^{\mathfrak{S}}(\mathbb{S}[\![s_2]\!]) \cup \{\omega\}) \setminus \{\Omega\}$.

- If $\mathcal{S}[\![s_1]\!] \in \{\omega, \Omega\}$ or $\mathcal{S}[\![s_2]\!] \in \{\omega, \Omega\}$ then $\mathcal{S}[\![s_1]\!] = \omega$ or $\mathcal{S}[\![s_2]\!] = \omega$ in which case $\mathcal{S}[\![s_1 \mapsto s_2]\!] \triangleq (\!|\mathcal{S}[\![s_1]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![s_2]\!] \notin \{\omega, \Omega\} \mathrel{?} \mathcal{S}[\![s_1]\!] \mapsto \mathcal{S}[\![s_2]\!] \mathrel{⨟} \texttt{error}(\mathcal{S}[\![s_1]\!], \mathcal{S}[\![s_2]\!])|\!) = \texttt{error}(\mathcal{S}[\![s_1]\!], \mathcal{S}[\![s_2]\!]) = \omega \in \{\omega\}$
- Otherwise $\mathcal{S}[\![s_1]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1]\!])$, $\mathcal{S}[\![s_2]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_2]\!])$, and $\mathcal{S}[\![s_1 \mapsto s_2]\!] \triangleq (\!|\mathcal{S}[\![s_1]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![s_2]\!] \notin \{\omega, \Omega\} \mathrel{?} \mathcal{S}[\![s_1]\!] \mapsto \mathcal{S}[\![s_2]\!] \mathrel{⨟} \texttt{error}(\mathcal{S}[\![s_1]\!], \mathcal{S}[\![s_2]\!])|\!) = \mathcal{S}[\![s_1]\!] \mapsto \mathcal{S}[\![s_2]\!] \in \{X \mapsto Y \mid X \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1]\!]) \wedge Y \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_2]\!])\} \triangleq \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1]\!] \twoheadleftarrow\!\!\!\rightarrow \mathbb{S}[\![s_2]\!]) \triangleq \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1 \mapsto s_2]\!])$.
- Grouping both cases together, we have $\mathcal{S}[\![s_1 \mapsto s_2]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1 \mapsto s_2]\!]) \cup \{\omega\}$.

- $\mathbb{S}[\![s_1 \times s_2]\!] \triangleq (\!|\mathbb{S}[\![s_1]\!] \neq \texttt{err} \wedge \mathbb{S}[\![s_2]\!] \neq \texttt{err} \mathrel{?} \mathbb{S}[\![s_1]\!] * \mathbb{S}[\![s_2]\!] \mathrel{⨟} \texttt{err}|\!)$

In case $\mathbb{S}[\![s_1 \times s_2]\!] \neq \texttt{err}$, we have $\mathbb{S}[\![s_1]\!] \neq \texttt{err}$ and $\mathbb{S}[\![s_2]\!] \neq \texttt{err}$ so $\mathbb{S}[\![s_1 \times s_2]\!] = \mathbb{S}[\![s_1]\!] * \mathbb{S}[\![s_2]\!]$ and, by structural induction hypothesis, $\mathcal{S}[\![s_1]\!] \in (\gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1]\!]) \cup \{\omega\}) \setminus \{\Omega\}$ and $\mathcal{S}[\![s_2]\!] \in (\gamma^{\mathfrak{S}}(\mathbb{S}[\![s_2]\!]) \cup \{\omega\}) \setminus \{\Omega\}$.

- If $\mathcal{S}[\![s_1]\!] \in \{\omega, \Omega\}$ or $\mathcal{S}[\![s_2]\!] \in \{\omega, \Omega\}$ then $\mathcal{S}[\![s_1]\!] = \omega$ or $\mathcal{S}[\![s_2]\!] = \omega$ in which case $\mathcal{S}[\![s_1 \times s_2]\!] \triangleq \mathcal{S}[\![s_1 \times s_2]\!] \triangleq (\!|\mathcal{S}[\![s_1]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![s_2]\!] \notin \{\omega, \Omega\} \mathrel{?} \mathcal{S}[\![s_1]\!] \times \mathcal{S}[\![s_2]\!] \mathrel{⨟} \texttt{error}(\mathcal{S}[\![s_1]\!], \mathcal{S}[\![s_2]\!])|\!) = \texttt{error}(\mathcal{S}[\![s_1]\!], \mathcal{S}[\![s_2]\!]) = \omega \in \{\omega\}$
- Otherwise $\mathcal{S}[\![s_1]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1]\!])$, $\mathcal{S}[\![s_2]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_2]\!])$, and $\mathcal{S}[\![s_1 \times s_2]\!] \triangleq \mathcal{S}[\![s_1 \times s_2]\!] \triangleq (\!|\mathcal{S}[\![s_1]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![s_2]\!] \notin \{\omega, \Omega\} \mathrel{?} \mathcal{S}[\![s_1]\!] \times \mathcal{S}[\![s_2]\!] \mathrel{⨟} \texttt{error}(\mathcal{S}[\![s_1]\!], \mathcal{S}[\![s_2]\!])|\!) = \mathcal{S}[\![s_1]\!] \times \mathcal{S}[\![s_2]\!] \in \{X \times Y \mid X \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1]\!]) \wedge Y \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_2]\!])\} \triangleq \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1]\!] * \mathbb{S}[\![s_2]\!]) \triangleq \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1 \times s_2]\!])$.
- Grouping both cases together, we have $\mathcal{S}[\![s_1 \times s_2]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s_1 \times s_2]\!]) \cup \{\omega\}$.

- $\mathbb{S}[\![\wp(s)]\!] \triangleq (\!|\mathbb{S}[\![s]\!] \neq \texttt{err} \mathrel{?} \texttt{P}\ \mathbb{S}[\![s]\!] \mathrel{⨟} \texttt{err}|\!)$

In case $\mathbb{S}[\![\wp(s)]\!] \neq \texttt{err}$, we have $\mathbb{S}[\![s]\!] \neq \texttt{err}$, $\mathbb{S}[\![\wp(s)]\!] = \texttt{P}\ \mathbb{S}[\![s]\!]$ and, by structural induction hypothesis, $\mathcal{S}[\![s]\!] \in (\gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!]) \cup \{\omega\}) \setminus \{\Omega\}$.

- If $\mathcal{S}[\![s]\!] \in \{\omega, \Omega\}$ then $\mathcal{S}[\![s]\!] = \omega$ in which case $\mathcal{S}[\![\wp(s)]\!] \triangleq (\!|\mathcal{S}[\![s]\!] \notin \{\omega, \Omega\} \mathrel{?} \wp(\mathcal{S}[\![s]\!]) \mathrel{⨟} \mathcal{S}[\![s]\!]|\!) = \mathcal{S}[\![s]\!] = \omega \in \{\omega\}$
- Otherwise $\mathcal{S}[\![s]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!])$ and $\mathcal{S}[\![\wp(s)]\!] \triangleq (\!|\mathcal{S}[\![s]\!] \notin \{\omega, \Omega\} \mathrel{?} \wp(\mathcal{S}[\![s]\!]) \mathrel{⨟} \mathcal{S}[\![s]\!]|\!) = \wp(\mathcal{S}[\![s]\!]) \in \{\wp(X) \mid X \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!])\} \subseteq \gamma^{\mathfrak{S}}(\texttt{P}\ \mathbb{S}[\![s]\!]) \triangleq \gamma^{\mathfrak{S}}(\mathbb{S}[\![\wp(s)]\!])$.
- In both cases, we have $\mathcal{S}[\![\wp(s)]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![\wp(s)]\!]) \cup \{\omega\}$.

- $\mathbb{S}[\![x]\!] \triangleq \texttt{err}$, otherwise (nothing to prove).

10.4 Partial order type inference

- $\mathbb{O}[\![o]\!] \triangleq o, \quad o \in \{\Rightarrow, \Leftrightarrow, \leq, \subseteq, =\}$
- $\mathbb{O}[\![\underline{\subseteq}]\!] \triangleq \subseteq$
- $\mathbb{O}[\![o^{-1}]\!] \triangleq (\mathbb{O}[\![o]\!])^{-1}$
- $\mathbb{O}[\![o_1 \times o_2]\!] \triangleq \mathbb{O}[\![o_1]\!] * \mathbb{O}[\![o_2]\!]$
- $\mathbb{O}[\![\dot{o}]\!] \triangleq (\mathbb{O}[\![\dot{o}]\!])$
- $\mathbb{O}[\![\ddot{o}]\!] \triangleq ((\mathbb{O}[\![\dot{o}]\!]))$

Since $\mathbb{O}[\![o]\!] \neq \texttt{err}$, soundness is $\mathcal{S}[\![o]\!] \in \gamma^{\mathfrak{O}}(\mathbb{O}[\![o]\!])$ (which implies $\mathcal{S}[\![o]\!] \in \gamma^{\mathfrak{O}}(\mathbb{O}[\![o]\!]) \cup \{\omega\}$). By the definition of $\gamma^{\mathfrak{O}}$ in Sec. 6.3, we have $\gamma^{\mathfrak{O}}(\mathsf{O}) \triangleq \{\mathcal{S}[\![\mathsf{O}]\!]\}$ for all $\mathsf{O} \in \mathfrak{O}$ (up to the isomorphism between partial order types and the semantics of partial orders, up to the use of $*$ for the type of pairs $\times$ and $\subseteq$ for interval inclusion $\underline{\subseteq}$) and therefore $\mathcal{S}[\![o]\!] \in \{\mathcal{S}[\![o]\!]\} = \gamma^{\mathfrak{O}}(o) = \gamma^{\mathfrak{O}}(\mathbb{O}[\![o]\!])$.

- $\mathbb{O}[\![x]\!] \triangleq \Omega$, otherwise (nothing to prove).

10.5 Poset type inference

- $\mathbb{P}[\![\langle s,\ o\rangle]\!] \triangleq (\!|\mathbb{S}[\![s]\!] \neq \texttt{err} \wedge \mathbb{O}[\![o]\!] \neq \texttt{err} \mathrel{?} \mathbb{S}[\![s]\!] \circledast \mathbb{O}[\![o]\!] \mathrel{⨟} \texttt{err}|\!)$

If $\mathbb{P}[\![\langle s,\ o\rangle]\!] \neq \texttt{err}$ then $\mathbb{S}[\![s]\!] \neq \texttt{err}$ and $\mathbb{O}[\![o]\!] \neq \texttt{err}$ so by, structural induction hypothesis, $\mathcal{S}[\![s]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!]) \cup \{\omega\}$ and $\mathcal{S}[\![o]\!] \in \gamma^{\mathfrak{O}}(\mathbb{O}[\![o]\!]) \cup \{\omega\}$. There is nothing to prove in case of a dynamic error ω so, in the remaining case, $\mathcal{S}[\![\langle s,\ o\rangle]\!] \triangleq (\!|\mathcal{S}[\![s]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![o]\!] \notin \{\omega, \Omega\} \mathrel{?} \langle \mathcal{S}[\![s]\!], \mathcal{S}[\![o]\!]\rangle \mathrel{⨟} \texttt{error}(\mathcal{S}[\![s]\!], \mathcal{S}[\![o]\!])|\!) = \langle \mathcal{S}[\![s]\!],\ \mathcal{S}[\![o]\!]\rangle \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!]) \times \gamma^{\mathfrak{O}}(\mathbb{O}[\![o]\!]) \triangleq \gamma^{\mathfrak{P}}(\mathbb{S}[\![s]\!] \circledast \mathbb{O}[\![o]\!]) \triangleq \gamma^{\mathfrak{P}}(\mathbb{P}[\![\langle s,\ o\rangle]\!])$

10.6 Galois connection type inference

- $\mathbb{T}[\![\mathbb{1}[p]]\!] \triangleq (\!|\mathbb{P}[\![p]\!] \neq \texttt{err} \mathrel{?} \mathbb{P}[\![p]\!] \leftrightarrows \mathbb{P}[\![p]\!] \mathrel{⨟} \texttt{err}|\!)$

The soundness proof must be done in the case when $\mathbb{T}[\![\mathbb{1}[p]]\!] \neq \texttt{err}$ which implies $\mathbb{P}[\![p]\!] \neq \texttt{err}$ and so $\mathbb{T}[\![\mathbb{1}[p]]\!] = \mathbb{P}[\![p]\!] \leftrightarrows \mathbb{P}[\![p]\!]$. By structural induction hypothesis, $\mathcal{S}[\![p]\!] \in \gamma^{\mathfrak{P}}(\mathbb{P}[\![p]\!]) \cup \{\omega\}$.

- If $\mathcal{S}[\![p]\!] = \omega$ then $\mathcal{S}[\![\mathbb{1}[p]]\!] = \llparenthesis \mathcal{S}[\![p]\!] \notin \{\omega, \Omega\} \mathrel{?} \mathcal{S}[\![p]\!] \xrightleftharpoons[\boldsymbol{\lambda} P \bullet P]{\boldsymbol{\lambda} Q \bullet Q} \mathcal{S}[\![p]\!] ⨾ \mathcal{S}[\![p]\!] \rrparenthesis = \mathcal{S}[\![p]\!] = \omega \in \{\omega\}$
- Otherwise $\mathcal{S}[\![p]\!] \notin \{\omega, \Omega\}$. By the syntactic definition of p in Sec. 2.6, p is of the form $p = \langle s,\ o\rangle$. s and o are syntactic components of p, itself a syntactic component of $\mathbb{1}[p]$, so, by structural induction hypothesis, $\mathcal{S}[\![s]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!]) \cup \{\omega\}$ and $\mathcal{S}[\![o]\!] \in \gamma^{\mathfrak{O}}(\mathbb{O}[\![o]\!]) \cup \{\omega\}$. But $\mathcal{S}[\![p]\!] = \mathcal{S}[\![\langle s,\ o\rangle]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![o]\!] \notin \{\omega, \Omega\} \mathrel{?} \langle \mathcal{S}[\![s]\!],\ \mathcal{S}[\![o]\!]\rangle ⨾ \mathbf{error}(\mathcal{S}[\![s]\!], \mathcal{S}[\![o]\!]) \rrparenthesis$ so $\mathcal{S}[\![s]\!] \in \{\omega\}$ or $\mathcal{S}[\![o]\!] \in \{\omega\}$ would yield a contradiction so $\mathcal{S}[\![s]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!])$ and $\mathcal{S}[\![o]\!] \in \gamma^{\mathfrak{O}}(\mathbb{O}[\![o]\!])$. It follows that

$$
\begin{aligned}
& \mathcal{S}[\![\mathbb{1}[p]]\!] \\
\triangleq\ & \llparenthesis \mathcal{S}[\![p]\!] \notin \{\omega, \Omega\} \mathrel{?} \mathcal{S}[\![p]\!] \xrightleftharpoons[\boldsymbol{\lambda} P \bullet P]{\boldsymbol{\lambda} Q \bullet Q} \mathcal{S}[\![p]\!] ⨾ \mathcal{S}[\![p]\!] \rrparenthesis \\
=\ & \mathcal{S}[\![p]\!] \xrightleftharpoons[\boldsymbol{\lambda} P \bullet P]{\boldsymbol{\lambda} Q \bullet Q} \mathcal{S}[\![p]\!] && \wr \text{case } \mathcal{S}[\![p]\!] \notin \{\omega, \Omega\} \wr \\
=\ & \mathcal{S}[\![\langle s,\ o\rangle]\!] \xrightleftharpoons[\boldsymbol{\lambda} P \bullet P]{\boldsymbol{\lambda} Q \bullet Q} \mathcal{S}[\![\langle s,\ o\rangle]\!] && \wr p = \langle s,\ o\rangle \wr \\
\triangleq\ & \llparenthesis \mathcal{S}[\![s]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![o]\!] \notin \{\omega, \Omega\} \mathrel{?} \langle \mathcal{S}[\![s]\!],\ \mathcal{S}[\![o]\!]\rangle ⨾ \mathbf{error}(\mathcal{S}[\![s]\!], \mathcal{S}[\![o]\!]) \rrparenthesis \xrightleftharpoons[\boldsymbol{\lambda} P \bullet P]{\boldsymbol{\lambda} Q \bullet Q} \llparenthesis \mathcal{S}[\![s]\!] \notin \{\omega, \Omega\} \wedge \\
& \mathcal{S}[\![o]\!] \notin \{\omega, \Omega\} \mathrel{?} \langle \mathcal{S}[\![s]\!],\ \mathcal{S}[\![o]\!]\rangle ⨾ \mathbf{error}(\mathcal{S}[\![s]\!], \mathcal{S}[\![o]\!]) \rrparenthesis \\
=\ & \langle \mathcal{S}[\![s]\!],\ \mathcal{S}[\![o]\!]\rangle \xrightleftharpoons[\boldsymbol{\lambda} P \bullet P]{\boldsymbol{\lambda} Q \bullet Q} \langle \mathcal{S}[\![s]\!],\ \mathcal{S}[\![o]\!]\rangle \\
\in\ & \{\langle C,\ \preceq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle A,\ \sqsubseteq\rangle \mid C \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!]) \wedge \preceq \in \gamma^{\mathfrak{O}}(\mathbb{O}[\![o]\!]) \wedge \\
& A \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!]) \wedge \sqsubseteq \in \gamma^{\mathfrak{O}}(\mathbb{O}[\![o]\!])\} \\
\triangleq\ & \gamma^{\mathfrak{T}}(\mathbb{S}[\![s]\!] \circledast \mathbb{O}[\![o]\!] \leftrightarrows \mathbb{S}[\![s]\!] \circledast \mathbb{O}[\![o]\!]) \\
=\ & \gamma^{\mathfrak{T}}(\mathscr{P}[\![\langle s,\ o\rangle]\!] \leftrightarrows \mathscr{P}[\![\langle s,\ o\rangle]\!]) \\
=\ & \gamma^{\mathfrak{T}}(\mathscr{P}[\![p]\!] \leftrightarrows \mathscr{P}[\![p]\!]) && \wr p = \langle s,\ o\rangle \wr \\
\subseteq\ & \gamma^{\mathfrak{T}}(\mathscr{P}[\![p]\!] \leftrightarrows \mathscr{P}[\![p]\!]) \cup \{\omega\} \\
=\ & \gamma^{\mathfrak{T}}(\mathscr{T}[\![\mathbb{1}[p]]\!]) \cup \{\omega\} && \textit{QED.}
\end{aligned}
$$

- $\mathscr{T}[\![\top[p, e]]\!] \triangleq \llparenthesis \mathscr{E}[\![e]\!] \neq \mathbf{err} \wedge \exists \mathsf{S} \in \mathfrak{S}, \mathsf{O} \in \mathfrak{O} : \mathscr{P}[\![p]\!] = \mathsf{S} \circledast \mathsf{O} \wedge \mathscr{E}[\![e]\!] \Subset \mathsf{S} \mathrel{?} \mathscr{P}[\![p]\!] \leftrightarrows \mathscr{P}[\![p]\!] ⨾ \mathbf{err} \rrparenthesis$

The soundness proof must be done in the case when $\mathscr{T}[\![\top[p, e]]\!] \neq \mathbf{err}$ which implies $\mathscr{E}[\![e]\!] \neq \mathbf{err} \wedge \exists \mathsf{S} \in \mathfrak{S}, \mathsf{O} \in \mathfrak{O} : \mathscr{P}[\![p]\!] = \mathsf{S} \circledast \mathsf{O} \wedge \mathscr{E}[\![e]\!] \Subset \mathsf{S}$.
Since $p = \langle s,\ o\rangle$ and $\mathscr{P}[\![\langle s,\ o\rangle]\!] \triangleq \llparenthesis \mathbb{S}[\![s]\!] \neq \mathbf{err} \wedge \mathbb{O}[\![o]\!] \neq \mathbf{err} \mathrel{?} \mathbb{S}[\![s]\!] \circledast \mathbb{O}[\![o]\!] ⨾ \mathbf{err} \rrparenthesis$ we have $\mathscr{E}[\![e]\!] \neq \mathbf{err}$, $\mathsf{S} = \mathbb{S}[\![s]\!] \neq \mathbf{err}$, $\mathsf{O} = \mathbb{O}[\![o]\!] \neq \mathbf{err}$, $\mathscr{E}[\![e]\!] \Subset \mathsf{S} = \mathbb{S}[\![s]\!]$, and $\mathscr{T}[\![\top[p, e]]\!] = \mathscr{P}[\![p]\!] \leftrightarrows \mathscr{P}[\![p]\!]$.

By structural induction hypothesis, $\mathcal{S}[\![e]\!] \in \gamma^{\mathfrak{E}}(\mathscr{E}[\![e]\!]) \not\ni \Omega$, $\mathcal{S}[\![s]\!] \in (\gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!]) \cup \{\omega\}) \not\ni \Omega$, $\mathcal{S}[\![o]\!] \in (\gamma^{\mathfrak{O}}(\mathbb{O}[\![o]\!]) \cup \{\omega\}) \not\ni \Omega$, and $\mathcal{S}[\![p]\!] \in (\gamma^{\mathfrak{P}}(\mathscr{P}[\![p]\!]) \cup \{\omega\}) \not\ni \Omega$

- If $\mathcal{S}[\![s]\!] = \omega$, $\mathcal{S}[\![o]\!] = \omega$, or $\mathcal{S}[\![p]\!] = \omega$ then $\mathcal{S}[\![\top[p, e]]\!] = \llparenthesis \exists S, \leqslant\ : \mathcal{S}[\![p]\!] = \langle S,\ \leqslant\rangle \mathrel{?} \llparenthesis \mathcal{S}[\![e]\!] \in S \setminus \{\omega\} \mathrel{?} \llparenthesis \forall x \in S : x \leqslant \mathcal{S}[\![e]\!] \mathrel{?} \mathcal{S}[\![p]\!] \xrightleftharpoons[\boldsymbol{\lambda} P \bullet \mathcal{S}[\![e]\!]]{\boldsymbol{\lambda} Q \bullet \mathcal{S}[\![e]\!]} \mathcal{S}[\![p]\!] ⨾ \omega \rrparenthesis ⨾ \omega \rrparenthesis ⨾ \mathbf{error}(\mathcal{S}[\![p]\!], \mathcal{S}[\![e]\!]) \rrparenthesis = \omega \in \{\omega\}$
- Otherwise $\mathcal{S}[\![p]\!] \notin \{\omega, \Omega\}$ so $\mathcal{S}[\![p]\!] \in \gamma^{\mathfrak{P}}(\mathscr{P}[\![p]\!])$. We have $\mathcal{S}[\![p]\!] = \mathcal{S}[\![\langle s,\ o\rangle]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![o]\!] \notin \{\omega, \Omega\} \mathrel{?} \langle \mathcal{S}[\![s]\!],\ \mathcal{S}[\![o]\!]\rangle ⨾ \mathbf{error}(\mathcal{S}[\![s]\!], \mathcal{S}[\![o]\!]) \rrparenthesis$ so $\mathcal{S}[\![s]\!] \in \{\omega, \Omega\}$ or $\mathcal{S}[\![o]\!] \in \{\omega, \Omega\}$ would imply the contradiction $\mathcal{S}[\![p]\!] \in \{\omega, \Omega\}$ so $\mathcal{S}[\![s]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!])$, $\mathcal{S}[\![o]\!] \in \gamma^{\mathfrak{O}}(\mathbb{O}[\![o]\!])$, and $\mathcal{S}[\![p]\!] = \langle \mathcal{S}[\![s]\!], \mathcal{S}[\![o]\!]\rangle \in \gamma^{\mathfrak{P}}(\mathscr{P}[\![p]\!])$.

  It follows that $\mathcal{S}[\![e]\!] \in S \setminus \{\omega\} = \mathcal{S}[\![s]\!]$ and therefore

$$
\begin{aligned}
& \mathcal{S}[\![\top[p, e]]\!] \\
\triangleq\ & \llparenthesis \exists S, \leqslant\ : \mathcal{S}[\![p]\!] = \langle S,\ \leqslant\rangle \mathrel{?} \llparenthesis \mathcal{S}[\![e]\!] \in S \setminus \{\omega\} \mathrel{?} \llparenthesis \forall x \in \\
& S : x \leqslant \mathcal{S}[\![e]\!] \mathrel{?} \mathcal{S}[\![p]\!] \xrightleftharpoons[\boldsymbol{\lambda} P \bullet \mathcal{S}[\![e]\!]]{\boldsymbol{\lambda} Q \bullet \mathcal{S}[\![e]\!]} \mathcal{S}[\![p]\!] ⨾ \omega \rrparenthesis ⨾ \omega \rrparenthesis ⨾ \\
& \mathbf{error}(\mathcal{S}[\![p]\!], \mathcal{S}[\![e]\!]) \rrparenthesis \\
=\ & \llparenthesis \forall x \in \mathcal{S}[\![s]\!] : x \leqslant \mathcal{S}[\![e]\!] \mathrel{?} \mathcal{S}[\![p]\!] \xrightleftharpoons[\boldsymbol{\lambda} P \bullet \mathcal{S}[\![e]\!]]{\boldsymbol{\lambda} Q \bullet \mathcal{S}[\![e]\!]} \mathcal{S}[\![p]\!] ⨾ \omega \rrparenthesis \\
& \qquad \wr \text{since } \mathcal{S}[\![p]\!] = \langle \mathcal{S}[\![s]\!],\ \mathcal{S}[\![o]\!]\rangle \text{ and } \mathcal{S}[\![e]\!] \in \mathcal{S}[\![s]\!] \wr \\
\in\ & \{\mathcal{S}[\![p]\!] \xrightleftharpoons[\boldsymbol{\lambda} P \bullet \mathcal{S}[\![e]\!]]{\boldsymbol{\lambda} Q \bullet \mathcal{S}[\![e]\!]} \mathcal{S}[\![p]\!]\} \cup \{\omega\} \\
\subseteq\ & \{P \xrightleftharpoons[\alpha]{\gamma} P' \mid P \in \gamma^{\mathfrak{P}}(\mathscr{P}[\![p]\!]) \wedge P' \in \gamma^{\mathfrak{P}}(\mathscr{P}[\![p]\!])\} \cup \{\omega\} \\
& \qquad \wr \text{since } \mathcal{S}[\![p]\!] \in \gamma^{\mathfrak{P}}(\mathscr{P}[\![p]\!]) \wr \\
=\ & \gamma^{\mathfrak{T}}(\mathscr{P}[\![p]\!] \leftrightarrows \mathscr{P}[\![p]\!]) \cup \{\omega\} \\
& \qquad \wr \text{by definition } \gamma^{\mathfrak{T}}(\mathsf{P} \leftrightarrows \mathsf{P}') \triangleq \{P \xrightleftharpoons[\alpha]{\gamma} P' \mid P \in \gamma^{\mathfrak{P}}(\mathsf{P}) \wedge P' \in \gamma^{\mathfrak{P}}(\mathsf{P}')\} \wr \\
=\ & \gamma^{\mathfrak{T}}(\mathscr{T}[\![\top[p, e]]\!]) \cup \{\omega\} && \textit{QED.}
\end{aligned}
$$

- $\mathscr{T}[\![\mathbb{I}[\langle s,\ o\rangle, b, t]]\!] \triangleq \llparenthesis \mathbf{err} \neq \mathscr{E}[\![b]\!] \Subset \mathbb{S}[\![s]\!] \neq \mathbf{err} \wedge \mathbf{err} \neq \mathscr{E}[\![t]\!] \Subset \mathbb{S}[\![s]\!] \mathrel{?} (\mathtt{P}\ \mathbb{S}[\![s]\!] \circledast \subseteq) \leftrightarrows (\mathtt{P}\ \mathbb{S}[\![s]\!] \circledast \subseteq) ⨾ \mathbf{err} \rrparenthesis$

For example, $\mathbb{I}[\langle \mathbb{Z},\ \leq\rangle, -\infty, \infty]$ denotes the *GC* $\langle \wp(\mathbb{Z}),\ \subseteq\rangle \xrightleftharpoons[\alpha^{\mathbb{I}}]{\gamma^{\mathbb{I}}} \langle \Im(\mathbb{Z} \cup \{-\infty, \infty\}, \leqslant),\ \subseteq\rangle$ where $\wp(\mathbb{Z}) \in \wp(\wp(\mathbb{Z} \cup \{-\infty, \infty\}))$ so $\wp(\mathbb{Z})$ has type $\mathtt{P}\ \mathbb{Z}$ and $\Im(\mathbb{Z} \cup \{-\infty, \infty\}, \leqslant) \subseteq \wp(\mathbb{Z} \cup \{-\infty, \infty\})$ so $\Im(\mathbb{Z} \cup \{-\infty, \infty\}, \leqslant) \in \wp(\wp(\mathbb{Z} \cup \{-\infty, \infty\}))$ hence $\Im(\mathbb{Z} \cup \{-\infty, \infty\}, \leqslant)$ has type $\mathtt{P}\ \mathbb{Z}$. It follows that $\mathscr{T}[\![\mathbb{I}[\langle \mathbb{Z},\ \leq\rangle, -\infty, \infty]]\!] = (\mathtt{P}\ \mathbb{Z} \circledast \subseteq) \leftrightarrows (\mathtt{P}\ \mathbb{Z} \circledast \subseteq)$.

For another example, $\mathbb{I}[\langle \wp(\mathbb{Z}),\ \subseteq\rangle, \emptyset, \mathbb{Z}]$ denotes the *GC* $\langle \wp(\wp(\mathbb{Z})),\ \subseteq\rangle \xrightleftharpoons[\alpha^{\mathbb{I}}]{\gamma^{\mathbb{I}}} \langle \Im(\wp(\mathbb{Z}) \cup \{\emptyset, \mathbb{Z}\}, \subseteq),\ \subseteq\rangle = \langle \Im(\wp(\mathbb{Z}), \subseteq),\ \subseteq\rangle$ where $\wp(\wp(\mathbb{Z})) \in \wp(\wp(\wp(\mathbb{Z})))$ and $\Im(\wp(\mathbb{Z}), \subseteq) \subseteq \wp(\wp(\mathbb{Z}))$ such that $\Im(\wp(\mathbb{Z}), \subseteq) \in \wp(\wp(\wp(\mathbb{Z})))$ have type $\mathtt{P}\ \mathtt{P}\ \mathbb{Z}$. It follows that $\mathscr{T}[\![\mathbb{I}[\langle \wp(\mathbb{Z}),\ \subseteq\rangle, \emptyset, \mathbb{Z}]]\!] = (\mathtt{P}\ \mathtt{P}\ \mathbb{Z} \circledast \subseteq) \leftrightarrows (\mathtt{P}\ \mathtt{P}\ \mathbb{Z} \circledast \subseteq)$

The soundness proof must be done in the case when $\mathscr{T}[\![\mathbb{I}[\langle s,\ o\rangle, b, t]]\!] \neq \mathbf{err}$ which implies $\mathbf{err} \neq \mathscr{E}[\![b]\!] \Subset \mathbb{S}[\![s]\!] \neq \mathbf{err}$ so $\mathcal{S}[\![b]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!]) \cup \{\omega\}$, $\mathbf{err} \neq \mathscr{E}[\![t]\!] \Subset \mathbb{S}[\![s]\!]$ so $\mathcal{S}[\![t]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!]) \cup \{\omega\}$, and $\mathscr{T}[\![\mathbb{I}[\langle s,\ o\rangle, b, t]]\!] \triangleq (\mathtt{P}\ \mathbb{S}[\![s]\!] \circledast \subseteq) \leftrightarrows (\mathtt{P}\ \mathbb{S}[\![s]\!] \circledast \subseteq)$.

- If $\mathcal{S}[\![\mathbb{I}[\langle s,\ o\rangle, b, t]]\!] = \omega$ then obviously $\mathcal{S}[\![\mathbb{I}[\langle s,\ o\rangle, b, t]]\!] \in \gamma^{\mathfrak{T}}(\mathscr{T}[\![\mathbb{I}[\langle s,\ o\rangle, b, t]]\!]) \cup \{\omega\}$.
- Otherwise $\mathcal{S}[\![\mathbb{I}[\langle s,\ o\rangle, b, t]]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![b]\!] \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![t]\!] \notin \{\omega, \Omega\} \mathrel{?} \llparenthesis \mathcal{S}[\![o]\!] \subseteq (\mathcal{S}[\![s]\!] \cup \{\mathcal{S}[\![b]\!], \mathcal{S}[\![t]\!]\}) \times (\mathcal{S}[\![s]\!] \cup \{\mathcal{S}[\![b]\!], \mathcal{S}[\![t]\!]\}) \wedge \forall x \in \mathcal{S}[\![s]\!] : \langle \mathcal{S}[\![b]\!],\ x\rangle \in \mathcal{S}[\![o]\!] \wedge \langle x,\ \mathcal{S}[\![t]\!]\rangle \in \mathcal{S}[\![o]\!] \mathrel{?} \langle \wp(\mathcal{S}[\![s]\!]),\ \subseteq\rangle \xrightleftharpoons[\alpha^{\mathbb{I}}]{\gamma^{\mathbb{I}}} \langle \Im(\mathcal{S}[\![s]\!] \cup \{\mathcal{S}[\![b]\!], \mathcal{S}[\![t]\!]\}, \mathcal{S}[\![o]\!]), \subseteq\rangle ⨾ \omega \rrparenthesis ⨾ \mathbf{error}(\mathcal{S}[\![s]\!], \mathbf{error}(\mathcal{S}[\![b]\!], \mathcal{S}[\![t]\!])) \rrparenthesis \neq \omega$ and so necessarily $\mathcal{S}[\![s]\!] \notin \{\omega, \Omega\}$, $\mathcal{S}[\![b]\!] \notin \{\omega, \Omega\}$, $\mathcal{S}[\![t]\!] \notin \{\omega, \Omega\}$, $\mathcal{S}[\![o]\!] \subseteq (\mathcal{S}[\![s]\!] \cup \{\mathcal{S}[\![b]\!], \mathcal{S}[\![t]\!]\}) \times (\mathcal{S}[\![s]\!] \cup \{\mathcal{S}[\![b]\!], \mathcal{S}[\![t]\!]\})$, $\forall x \in \mathcal{S}[\![s]\!] : \langle \mathcal{S}[\![b]\!],\ x\rangle \in \mathcal{S}[\![o]\!] \wedge \langle x,\ \mathcal{S}[\![t]\!]\rangle \in \mathcal{S}[\![o]\!]$, and $\mathcal{S}[\![\mathbb{I}[\langle s,\ o\rangle, b, t]]\!] \triangleq \langle \wp(\mathcal{S}[\![s]\!]),\ \subseteq\rangle \xrightleftharpoons[\alpha^{\mathbb{I}}]{\gamma^{\mathbb{I}}} \langle \Im(\mathcal{S}[\![s]\!] \cup \{\mathcal{S}[\![b]\!], \mathcal{S}[\![t]\!]\}, \mathcal{S}[\![o]\!]),\ \subseteq\rangle$. By structural induction, it follows that $\mathcal{S}[\![s]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!])$ so

$$
\begin{aligned}
& \langle \wp(\mathcal{S}[\![s]\!]),\ \subseteq\rangle \\
\in\ & \gamma^{\mathfrak{S}}(\mathtt{P}\ \mathbb{S}[\![s]\!]) \times \{\subseteq\} \\
& \qquad \wr \text{since } \mathcal{S}[\![s]\!] \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!]) \text{ so } \wp(\mathcal{S}[\![s]\!]) \in \{\wp(X) \mid X \in \gamma^{\mathfrak{S}}(\mathbb{S}[\![s]\!])\} \subseteq \gamma^{\mathfrak{S}}(\mathtt{P}\ \mathbb{S}[\![s]\!]) \text{ and } \subseteq \in \{\subseteq\} \wr \\
=\ & \gamma^{\mathfrak{S}}(\mathtt{P}\ \mathbb{S}[\![s]\!]) \times \gamma^{\mathfrak{O}}(\subseteq) \quad \wr \text{since } \gamma^{\mathfrak{O}}(\subseteq) \triangleq \{\mathcal{S}[\![\subseteq]\!]\} = \{\subseteq\} \wr \\
=\ & \gamma^{\mathfrak{P}}(\mathtt{P}\ \mathbb{S}[\![s]\!] \circledast \subseteq) \quad \wr \text{since } \gamma^{\mathfrak{P}}(\mathsf{S} \circledast \mathsf{O}) \triangleq \gamma^{\mathfrak{S}}(\mathsf{S}) \times \gamma^{\mathfrak{O}}(\mathsf{O}) \wr
\end{aligned}
$$

Moreover $\mathscr{E}[\![b]\!], \mathscr{E}[\![t]\!] \Subset \mathscr{S}[\![s]\!]$ implies $\mathcal{S}[\![b]\!], \mathcal{S}[\![t]\!] \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s]\!])$ and therefore $\mathcal{S}[\![s]\!] \cup \{\mathcal{S}[\![b]\!], \mathcal{S}[\![t]\!]\} \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s]\!])$ so

$$\begin{aligned}
&\langle \Im(\mathcal{S}[\![s]\!] \cup \{\mathcal{S}[\![b]\!], \mathcal{S}[\![t]\!]\}, \mathcal{S}[\![o]\!]),\ \subseteq\rangle \\
\in\ & \{\Im(X, \mathcal{S}[\![o]\!]) \mid X \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s]\!])\} \times \{\subseteq\} \\
&\qquad \wr\text{since } \mathcal{S}[\![s]\!] \cup \{\mathcal{S}[\![b]\!], \mathcal{S}[\![t]\!]\} \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s]\!])\wr \\
\subseteq\ & \{\wp(X) \mid X \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s]\!])\} \times \{\subseteq\} \\
&\qquad \wr\text{since } \Im(S, \leqslant) \subseteq \wp(S)\wr \\
\subseteq\ & \wp(\gamma^{\mathfrak{S}}(\mathscr{S}[\![s]\!])) \times \{\subseteq\} \\
&\qquad \wr\text{since } \{\wp(X) \mid X \in \gamma^{\mathfrak{S}}(\mathsf{S})\} \subseteq \gamma^{\mathfrak{S}}(\mathbf{P}\ \mathsf{S})\wr \\
=\ & \gamma^{\mathfrak{S}}(\mathbf{P}\ \mathscr{S}[\![s]\!]) \times \{\subseteq\} \qquad \wr\text{since } \gamma^{\mathfrak{S}}(\mathbf{P}\ \mathsf{S}) \triangleq \wp(\gamma^{\mathfrak{S}}(\mathsf{S}))\wr \\
=\ & \gamma^{\mathfrak{S}}(\mathbf{P}\ \mathscr{S}[\![s]\!]) \times \gamma^{\mathfrak{O}}(\subseteq) \quad \wr\text{since } \gamma^{\mathfrak{O}}(\subseteq) \triangleq \{\mathcal{S}[\![\subseteq]\!]\} = \{\subseteq\}\wr \\
=\ & \gamma^{\mathfrak{P}}(\mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq) \quad \wr\text{since } \gamma^{\mathfrak{P}}(\mathsf{S} \circledast \mathsf{O}) \triangleq \gamma^{\mathfrak{S}}(\mathsf{S}) \times \gamma^{\mathfrak{O}}(\mathsf{O})\wr
\end{aligned}$$

We conclude that

$$\begin{aligned}
&\mathcal{S}[\![\mathbb{I}[\langle s,\ o\rangle, b, t]]\!] \\
\triangleq\ & \langle \wp(\mathcal{S}[\![s]\!]),\ \subseteq\rangle \xleftarrow[\alpha^{\mathbb{I}}]{\gamma^{\mathbb{I}}} \langle \Im(\mathcal{S}[\![s]\!] \cup \{\mathcal{S}[\![b]\!], \mathcal{S}[\![t]\!]\}, \mathcal{S}[\![o]\!]),\ \subseteq\rangle \\
\in\ & \{P \xleftrightarrows[\alpha]{\gamma} P' \mid P \in \gamma^{\mathfrak{P}}(\mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq) \wedge P' \in \gamma^{\mathfrak{P}}(\mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq)\} \\
&\qquad \wr\text{since } \langle \wp(\mathcal{S}[\![s]\!]), \subseteq\rangle \in \gamma^{\mathfrak{P}}(\mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq) \text{ and } \langle \Im(\mathcal{S}[\![s]\!] \cup \\
&\qquad \{\mathcal{S}[\![b]\!], \mathcal{S}[\![t]\!]\}, \mathcal{S}[\![o]\!]),\ \subseteq\rangle \in \gamma^{\mathfrak{P}}(\mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq)\wr \\
\subseteq\ & \gamma^{\mathfrak{T}}((\mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq) \leftrightarrows (\mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq)) \cup \{\omega\} \\
&\qquad \wr\text{by definition } \gamma^{\mathfrak{T}}(\mathsf{P} \leftrightarrows \mathsf{P}') \triangleq \{P \xleftrightarrows[\alpha]{\gamma} P' \mid P \in \gamma^{\mathfrak{P}}(\mathsf{P}) \wedge P' \in \gamma^{\mathfrak{P}}(\mathsf{P}')\}\wr \\
=\ & \gamma^{\mathfrak{T}}(\mathscr{T}[\![\mathbb{I}[\langle s,\ o\rangle, b, t]]\!]) \cup \{\omega\} \qquad \textit{QED.}
\end{aligned}$$

- $\mathscr{T}[\![\curvearrowright[s_{\mathbb{L}}, s_{\mathcal{M}}]]\!] \triangleq \llparenthesis \mathscr{S}[\![s_{\mathbb{L}}]\!] \neq \texttt{err} \wedge \mathscr{S}[\![s_{\mathcal{M}}]\!] \neq \texttt{err} \mathrel{?} \mathbf{P}\ (\mathscr{S}[\![s_{\mathbb{L}}]\!] * \mathscr{S}[\![s_{\mathcal{M}}]\!]) \circledast \subseteq \leftrightarrows \mathscr{S}[\![s_{\mathbb{L}}]\!] \mathrel{*\!\!\longleftrightarrow} \mathbf{P}\ \mathscr{S}[\![s_{\mathcal{M}}]\!] \circledast \dot{\subseteq} \fatsemi \texttt{err}\rrparenthesis$

Assuming $\mathscr{T}[\![\curvearrowright[s_{\mathbb{L}}, s_{\mathcal{M}}]]\!] \neq \texttt{err}$ hence $\mathscr{S}[\![s_{\mathbb{L}}]\!] \neq \texttt{err}$ and $\mathscr{S}[\![s_{\mathcal{M}}]\!] \neq \texttt{err}$ so, by structural induction hypothesis, that $\mathcal{S}[\![s_{\mathbb{L}}]\!] \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s_{\mathbb{L}}]\!]) \cup \{\omega\}$ and $\mathcal{S}[\![s_{\mathcal{M}}]\!] \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s_{\mathcal{M}}]\!]) \cup \{\omega\}$, we must prove that $\mathcal{S}[\![\curvearrowright[s_{\mathbb{L}}, s_{\mathcal{M}}]]\!] \in \gamma^{\mathfrak{T}}(\mathscr{T}[\![\curvearrowright[s_{\mathbb{L}}, s_{\mathcal{M}}]]\!]) \cup \{\omega\}$. Observe that in case $\mathcal{S}[\![s_{\mathbb{L}}]\!] \neq \omega$ and $\mathcal{S}[\![s_{\mathcal{M}}]\!] \neq \omega$, we have

$$\begin{aligned}
&\wp(\mathcal{S}[\![s_{\mathbb{L}}]\!] \times \mathcal{S}[\![s_{\mathcal{M}}]\!]) \\
\in\ & \{\wp(X \times Y) \mid X \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s_{\mathbb{L}}]\!]) \wedge Y \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s_{\mathcal{M}}]\!])\} \\
&\qquad \wr\text{since } \mathcal{S}[\![s_{\mathbb{L}}]\!] \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s_{\mathbb{L}}]\!]) \text{ and } \mathcal{S}[\![s_{\mathcal{M}}]\!] \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s_{\mathcal{M}}]\!])\ \wr \\
=\ & \{\wp(X \times Y) \mid X \times Y \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s_{\mathbb{L}}]\!] * \mathscr{S}[\![s_{\mathcal{M}}]\!])\} \\
&\qquad \wr\text{since } \gamma^{\mathfrak{S}}(\mathsf{S}_1 * \mathsf{S}_2) \triangleq \{X \times Y \mid X \in \gamma^{\mathfrak{S}}(\mathsf{S}_1) \wedge Y \in \gamma^{\mathfrak{S}}(\mathsf{S}_2)\}\wr \\
\subseteq\ & \gamma^{\mathfrak{S}}(\mathbf{P}\ (\mathscr{S}[\![s_{\mathbb{L}}]\!] * \mathscr{S}[\![s_{\mathcal{M}}]\!])) \\
&\qquad \wr\{\wp(Z) \mid Z \in \gamma^{\mathfrak{S}}(\mathsf{S})\} \subseteq \gamma^{\mathfrak{S}}(\mathbf{P}\ \mathsf{S})\wr \quad .
\end{aligned}$$

and $\subseteq\ \in \{\subseteq\} = \{\mathcal{S}[\![\subseteq]\!]\} \triangleq \gamma^{\mathfrak{O}}(\subseteq)$ so $\langle \wp(\mathcal{S}[\![s_{\mathbb{L}}]\!] \times \mathcal{S}[\![s_{\mathcal{M}}]\!]), \subseteq\rangle \in \gamma^{\mathfrak{S}}(\mathbf{P}\ (\mathscr{S}[\![s_{\mathbb{L}}]\!] * \mathscr{S}[\![s_{\mathcal{M}}]\!])) \times \gamma^{\mathfrak{O}}(\subseteq) \triangleq \gamma^{\mathfrak{P}}(\mathbf{P}\ (\mathscr{S}[\![s_{\mathbb{L}}]\!] * \mathscr{S}[\![s_{\mathcal{M}}]\!]) \circledast \subseteq)$. Moreover

$$\begin{aligned}
&\mathcal{S}[\![s_{\mathbb{L}}]\!] \mapsto \wp(\mathcal{S}[\![s_{\mathcal{M}}]\!]) \\
\in\ & \{X \mapsto \wp(Y) \mid X \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s_{\mathbb{L}}]\!]) \wedge Y \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s_{\mathcal{M}}]\!])\} \\
&\qquad \wr\text{since } \mathcal{S}[\![s_{\mathbb{L}}]\!] \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s_{\mathbb{L}}]\!]) \text{ and } \mathcal{S}[\![s_{\mathcal{M}}]\!] \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s_{\mathcal{M}}]\!])\wr \\
=\ & \{X \mapsto Z \mid X \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s_{\mathbb{L}}]\!]) \wedge Z \in \gamma^{\mathfrak{S}}(\mathbf{P}\ \mathscr{S}[\![s_{\mathcal{M}}]\!])\} \\
&\qquad \wr\text{since } \gamma^{\mathfrak{S}}(\mathbf{P}\ \mathsf{S}) \triangleq \wp(\gamma^{\mathfrak{S}}(\mathsf{S}))\wr \\
=\ & \gamma^{\mathfrak{S}}(\mathscr{S}[\![s_{\mathbb{L}}]\!] \mathrel{*\!\!\longleftrightarrow} \mathbf{P}\ \mathscr{S}[\![s_{\mathcal{M}}]\!]) \\
&\qquad \wr\text{since } \gamma^{\mathfrak{S}}(\mathsf{S}_1 \mathrel{*\!\!\longleftrightarrow} \mathsf{S}_2) \triangleq \{X \mapsto Y \mid X \in \gamma^{\mathfrak{S}}(\mathsf{S}_1) \wedge Y \in \gamma^{\mathfrak{S}}(\mathsf{S}_2)\}\wr
\end{aligned}$$

and $\dot{\subseteq} \in \gamma^{\mathfrak{O}}(\dot{\subseteq})$ so $\langle \mathcal{S}[\![s_{\mathbb{L}}]\!] \mapsto \wp(\mathcal{S}[\![s_{\mathcal{M}}]\!]), \dot{\subseteq}\rangle \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s_{\mathbb{L}}]\!] \mathrel{*\!\!\longleftrightarrow} \mathbf{P}\ \mathscr{S}[\![s_{\mathcal{M}}]\!]) \times \gamma^{\mathfrak{O}}(\dot{\subseteq}) \triangleq \gamma^{\mathfrak{P}}(\mathscr{S}[\![s_{\mathbb{L}}]\!] \mathrel{*\!\!\longleftrightarrow} \mathbf{P}\ \mathscr{S}[\![s_{\mathcal{M}}]\!] \circledast \dot{\subseteq})$.
It follows that for the non-trivial case $\mathcal{S}[\![\curvearrowright[s_{\mathbb{L}}, s_{\mathcal{M}}]]\!] \neq \omega$, we have

$$\begin{aligned}
&\mathcal{S}[\![\curvearrowright[s_{\mathbb{L}}, s_{\mathcal{M}}]]\!] \\
=\ & \llparenthesis \mathcal{S}[\![s_{\mathbb{L}}]\!] \not\in \{\Omega, \omega\} \wedge \mathcal{S}[\![s_{\mathcal{M}}]\!] \not\in \{\Omega, \omega\} \mathrel{?} \langle \wp(\mathcal{S}[\![s_{\mathbb{L}}]\!] \times \\
& \mathcal{S}[\![s_{\mathcal{M}}]\!]),\ \subseteq\rangle \xleftrightarrows[\alpha^{\curvearrowright}]{\gamma^{\curvearrowright}} \langle \mathcal{S}[\![s_{\mathbb{L}}]\!] \mapsto \wp(\mathcal{S}[\![s_{\mathcal{M}}]\!]),\ \dot{\subseteq}\rangle \fatsemi \\
& \mathbf{error}(\mathcal{S}[\![s_{\mathbb{L}}]\!], \mathcal{S}[\![s_{\mathcal{M}}]\!])\rrparenthesis \\
=\ & \langle \wp(\mathcal{S}[\![s_{\mathbb{L}}]\!] \times \mathcal{S}[\![s_{\mathcal{M}}]\!]),\ \subseteq\rangle \xleftrightarrows[\alpha^{\curvearrowright}]{\gamma^{\curvearrowright}} \langle \mathcal{S}[\![s_{\mathbb{L}}]\!] \mapsto \wp(\mathcal{S}[\![s_{\mathcal{M}}]\!]), \\
& \dot{\subseteq}\rangle \\
\in\ & \{P \xleftrightarrows[\alpha]{\gamma} P' \mid P \in \gamma^{\mathfrak{P}}(\mathbf{P}\ (\mathscr{S}[\![s_{\mathbb{L}}]\!] * \mathscr{S}[\![s_{\mathcal{M}}]\!]) \circledast \subseteq) \wedge P' \in \\
& \gamma^{\mathfrak{P}}(\mathscr{S}[\![s_{\mathbb{L}}]\!] \mathrel{*\!\!\longleftrightarrow} \mathbf{P}\ \mathscr{S}[\![s_{\mathcal{M}}]\!] \circledast \dot{\subseteq})\} \\
&\qquad \wr\text{since } \langle \wp(\mathcal{S}[\![s_{\mathbb{L}}]\!] \times \mathcal{S}[\![s_{\mathcal{M}}]\!]),\ \subseteq\rangle \in \gamma^{\mathfrak{P}}(\mathbf{P}\ (\mathscr{S}[\![s_{\mathbb{L}}]\!] * \\
&\qquad \mathscr{S}[\![s_{\mathcal{M}}]\!]) \circledast \subseteq) \text{ and } \langle \mathcal{S}[\![s_{\mathbb{L}}]\!] \mapsto \wp(\mathcal{S}[\![s_{\mathcal{M}}]\!]),\ \dot{\subseteq}\rangle \in \\
&\qquad \gamma^{\mathfrak{P}}(\mathscr{S}[\![s_{\mathbb{L}}]\!] \mathrel{*\!\!\longleftrightarrow} \mathbf{P}\ \mathscr{S}[\![s_{\mathcal{M}}]\!] \circledast \dot{\subseteq})\ \wr \\
=\ & \gamma^{\mathfrak{T}}(\mathbf{P}\ (\mathscr{S}[\![s_{\mathbb{L}}]\!] * \mathscr{S}[\![s_{\mathcal{M}}]\!]) \circledast \subseteq \leftrightarrows \mathscr{S}[\![s_{\mathbb{L}}]\!] \mathrel{*\!\!\longleftrightarrow} \mathbf{P}\ \mathscr{S}[\![s_{\mathcal{M}}]\!] \circledast \dot{\subseteq}) \\
&\qquad \wr\text{since } \gamma^{\mathfrak{T}}(\mathsf{P} \leftrightarrows \mathsf{P}') \triangleq \{P \xleftrightarrows[\alpha]{\gamma} P' \mid P \in \gamma^{\mathfrak{P}}(\mathsf{P}) \wedge \\
&\qquad P' \in \gamma^{\mathfrak{P}}(\mathsf{P}')\}\wr \\
=\ & \gamma^{\mathfrak{T}}(\mathscr{T}[\![\curvearrowright[s_{\mathbb{L}}, s_{\mathcal{M}}]]\!]) \qquad \textit{QED.}
\end{aligned}$$

- $\mathscr{T}[\![\cup[s]]\!] \triangleq \llparenthesis \mathscr{S}[\![s]\!] \neq \texttt{err} \mathrel{?} \mathbf{P}\ (\mathbf{P}\ \mathscr{S}[\![s]\!]) \circledast \subseteq \leftrightarrows \mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq \fatsemi \texttt{err}\rrparenthesis$

Assuming $\mathscr{T}[\![\cup[s]]\!] \neq \texttt{err}$ hence $\mathscr{S}[\![s]\!] \neq \texttt{err}$ so, by structural induction hypothesis, that $\mathcal{S}[\![s]\!] \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s]\!]) \cup \{\omega\}$, we must prove that $\mathcal{S}[\![\cup[s]]\!] \in \gamma^{\mathfrak{T}}(\mathscr{T}[\![\cup[s]]\!]) \cup \{\omega\}$. For the non-trivial case $\mathcal{S}[\![\cup[s]]\!] \neq \omega$, we have

$$\begin{aligned}
&\mathcal{S}[\![\cup[s]]\!] \\
=\ & \llparenthesis \mathcal{S}[\![s]\!] \not\in \{\omega, \Omega\} \mathrel{?} \langle \wp(\wp(\mathcal{S}[\![s]\!])),\ \subseteq\rangle \xleftrightarrows[\alpha^{\wp}]{\gamma^{\wp}} \langle \wp(\mathcal{S}[\![s]\!]), \\
& \subseteq\rangle \fatsemi \mathcal{S}[\![s]\!]\rrparenthesis \\
=\ & \langle \wp(\wp(\mathcal{S}[\![s]\!])),\ \subseteq\rangle \xleftrightarrows[\alpha^{\wp}]{\gamma^{\wp}} \langle \wp(\mathcal{S}[\![s]\!]),\ \subseteq\rangle \\
\in\ & \{P \xleftrightarrows[\alpha]{\gamma} P' \mid P \in \gamma^{\mathfrak{P}}(\mathbf{P}\ (\mathbf{P}\ \mathscr{S}[\![s]\!]) \circledast \subseteq) \wedge P' \in \\
& \gamma^{\mathfrak{P}}(\mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq)\} \\
&\qquad \wr\text{since } \langle \wp(\wp(\mathcal{S}[\![s]\!])),\ \subseteq\rangle \in \gamma^{\mathfrak{P}}(\mathbf{P}\ (\mathbf{P}\ \mathscr{S}[\![s]\!]) \circledast \subseteq) \text{ and} \\
&\qquad \langle \wp(\mathcal{S}[\![s]\!]),\ \subseteq\rangle \in \gamma^{\mathfrak{P}}(\mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq)\wr \\
=\ & \gamma^{\mathfrak{T}}((\mathbf{P}\ (\mathbf{P}\ \mathscr{S}[\![s]\!]) \circledast \subseteq) \leftrightarrows (\mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq)) \\
&\qquad \wr\gamma^{\mathfrak{T}}(\mathsf{P} \leftrightarrows \mathsf{P}') \triangleq \{P \xleftrightarrows[\alpha]{\gamma} P' \mid P \in \gamma^{\mathfrak{P}}(\mathsf{P}) \wedge P' \in \\
&\qquad \gamma^{\mathfrak{P}}(\mathsf{P}')\}\wr \\
=\ & \gamma^{\mathfrak{T}}(\mathscr{T}[\![\cup[s]]\!]) \qquad \textit{QED.}
\end{aligned}$$

- $\mathscr{T}[\![\neg[s]]\!] \triangleq \llparenthesis \mathscr{S}[\![s]\!] \neq \texttt{err} \mathrel{?} \mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq \leftrightarrows \mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq^{-1} \fatsemi \texttt{err}\rrparenthesis$

In $\mathscr{T}[\![\neg[s]]\!] \neq \texttt{err}$ so $\mathscr{S}[\![s]\!] \neq \texttt{err}$, we have $\mathcal{S}[\![s]\!] \in \gamma^{\mathfrak{S}}(\mathscr{S}[\![s]\!]) \cup \{\omega\}$ by structural induction hypothesis. For the non-trivial case $\mathcal{S}[\![\neg[s]]\!] \neq \omega$ so $\mathcal{S}[\![s]\!] \neq \omega$ hence $\wp(\mathcal{S}[\![s]\!]) \in \gamma^{\mathfrak{S}}(\mathbf{P}\ \mathscr{S}[\![s]\!])$, we have

$$\begin{aligned}
&\mathcal{S}[\![\neg[s]]\!] \\
=\ & \llparenthesis \mathcal{S}[\![s]\!] \not\in \{\omega, \Omega\} \mathrel{?} \langle \wp(\mathcal{S}[\![s]\!]),\ \subseteq\rangle \xleftrightarrows[\neg]{\neg} \langle \wp(\mathcal{S}[\![s]\!]),\ \supseteq\rangle \fatsemi \\
& \mathcal{S}[\![s]\!]\rrparenthesis \\
=\ & \langle \wp(\mathcal{S}[\![s]\!]),\ \subseteq\rangle \xleftrightarrows[\neg]{\neg} \langle \wp(\mathcal{S}[\![s]\!]),\ \supseteq\rangle \\
\in\ & \{P \xleftrightarrows[\alpha]{\gamma} P' \mid P \in \gamma^{\mathfrak{P}}(\mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq) \wedge P' \in \\
& \gamma^{\mathfrak{P}}(\mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq^{-1})\} \\
&\qquad \wr\text{since } \wp(\mathcal{S}[\![s]\!]) \in \gamma^{\mathfrak{S}}(\mathbf{P}\ \mathscr{S}[\![s]\!]),\ \subseteq\ \in \gamma^{\mathfrak{O}}(\subseteq),\ \supseteq\ \in \\
&\qquad \gamma^{\mathfrak{O}}((\subseteq)^{-1}), \text{ and } \gamma^{\mathfrak{P}}(\mathsf{S} \circledast \mathsf{O}) \triangleq \gamma^{\mathfrak{S}}(\mathsf{S}) \times \gamma^{\mathfrak{O}}(\mathsf{O})\ \wr \\
=\ & \gamma^{\mathfrak{T}}(\mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq \leftrightarrows \mathbf{P}\ \mathscr{S}[\![s]\!] \circledast \subseteq^{-1}) \qquad \wr\text{def. } \gamma^{\mathfrak{T}}\wr
\end{aligned}$$

$= \;\gamma^{\mathfrak{T}}(\llparenthesis \mathcal{S}\llbracket s\rrbracket \neq \texttt{err} \;?\; \mathbf{P}\;\mathcal{S}\llbracket s\rrbracket \circledast \subseteq \leftrightarrows \mathbf{P}\;\mathcal{S}\llbracket s\rrbracket \circledast \subseteq^{-1} \mathbin{⸾} \texttt{err}\rrparenthesis)$
$\subseteq \;\gamma^{\mathfrak{T}}(\mathcal{T}\llbracket \neg[s]\rrbracket) \cup \{\omega\}$ *QED.*

- $\mathcal{T}\llbracket \infty[s]\rrbracket \triangleq \llparenthesis \mathcal{S}\llbracket s\rrbracket \neq \texttt{err} \;?\; \mathbf{P}\;(\texttt{seq}\,\mathcal{S}\llbracket s\rrbracket) \circledast \subseteq \leftrightarrows \mathbf{P}\;\mathcal{S}\llbracket s\rrbracket \circledast \subseteq \mathbin{⸾} \texttt{err}\rrparenthesis$

In the non-trivial case $\mathcal{T}\llbracket \infty[s]\rrbracket \neq \texttt{err}$ (so $\mathcal{S}\llbracket s\rrbracket \neq \texttt{err}$) and $\mathcal{S}\llbracket s\rrbracket \neq \omega$, we have $\mathcal{S}\llbracket s^{\infty}\rrbracket \triangleq \llparenthesis \mathcal{S}\llbracket s\rrbracket \notin \{\omega,\Omega\} \;?\; \mathcal{S}\llbracket s\rrbracket^{\infty} \mathbin{⸾} \mathcal{S}\llbracket s\rrbracket\rrparenthesis = \mathcal{S}\llbracket s\rrbracket^{\infty}$. By structural induction hypothesis, $\mathcal{S}\llbracket s\rrbracket \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s\rrbracket)$ so $\wp(\mathcal{S}\llbracket s\rrbracket) \in \gamma^{\mathfrak{S}}(\mathbf{P}\;\mathcal{S}\llbracket s\rrbracket)$ hence $\langle \wp(\mathcal{S}\llbracket s\rrbracket),\, \subseteq\rangle \in \gamma^{\mathfrak{P}}(\mathbf{P}\;\mathcal{S}\llbracket s\rrbracket \circledast \subseteq)$. Similarly $\mathcal{S}\llbracket s\rrbracket \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s\rrbracket)$ implies that $\mathcal{S}\llbracket s\rrbracket^{\infty} \in \{X^{\infty} \mid X \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s\rrbracket)\} \triangleq \gamma^{\mathfrak{S}}(\texttt{seq}\;\mathcal{S}\llbracket s\rrbracket)$ so $\wp(\mathcal{S}\llbracket s\rrbracket^{\infty}) \in \gamma^{\mathfrak{S}}(\mathbf{P}(\texttt{seq}\;\mathcal{S}\llbracket s\rrbracket))$ hence $\langle \wp(\mathcal{S}\llbracket s\rrbracket^{\infty}),\, \subseteq\rangle \in \gamma^{\mathfrak{P}}((\mathbf{P}(\texttt{seq}\,\mathcal{S}\llbracket s\rrbracket)) \circledast \subseteq)$. We conclude that

$\mathcal{S}\llbracket \infty[s]\rrbracket$
$\triangleq \llparenthesis \mathcal{S}\llbracket s\rrbracket \notin \{\omega,\Omega\} \;?\; \langle \wp(\mathcal{S}\llbracket s\rrbracket^{\infty}),\, \subseteq\rangle \underset{\alpha^{\infty}}{\overset{\gamma^{\infty}}{\leftrightarrows}} \langle \wp(\mathcal{S}\llbracket s\rrbracket),\, \subseteq\rangle \mathbin{⸾} \mathcal{S}\llbracket s\rrbracket\rrparenthesis$
$= \langle \wp(\mathcal{S}\llbracket s\rrbracket^{\infty}),\, \subseteq\rangle \underset{\alpha^{\infty}}{\overset{\gamma^{\infty}}{\leftrightarrows}} \langle \wp(\mathcal{S}\llbracket s\rrbracket),\, \subseteq\rangle$
$\in \{P \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} P' \mid P \in \gamma^{\mathfrak{P}}(\mathbf{P}\;(\texttt{seq}\,\mathcal{S}\llbracket s\rrbracket) \circledast \subseteq) \wedge P' \in \gamma^{\mathfrak{P}}(\mathbf{P}\;\mathcal{S}\llbracket s\rrbracket \circledast \subseteq)\}$
$\triangleq \gamma^{\mathfrak{T}}(\mathbf{P}\;(\texttt{seq}\,\mathcal{S}\llbracket s\rrbracket) \circledast \subseteq \leftrightarrows \mathbf{P}\;\mathcal{S}\llbracket s\rrbracket \circledast \subseteq)$
$= \gamma^{\mathfrak{T}}(\llparenthesis \mathcal{S}\llbracket s\rrbracket \neq \texttt{err} \;?\; \mathbf{P}\;(\texttt{seq}\,\mathcal{S}\llbracket s\rrbracket) \circledast \subseteq \leftrightarrows \mathbf{P}\;\mathcal{S}\llbracket s\rrbracket \circledast \subseteq \mathbin{⸾} \texttt{err}\rrparenthesis)$
$\triangleq \gamma^{\mathfrak{T}}(\mathcal{T}\llbracket \infty[s]\rrbracket)$ *QED.*

- $\mathcal{T}\llbracket \rightsquigarrow[s_1,s_2]\rrbracket \triangleq \llparenthesis \mathcal{S}\llbracket s_1\rrbracket \neq \texttt{err} \wedge \mathcal{S}\llbracket s_2\rrbracket \neq \texttt{err} \;?\; \mathbf{P}(\mathcal{S}\llbracket s_1\rrbracket * \mathcal{S}\llbracket s_2\rrbracket) \circledast \subseteq \leftrightarrows \mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket \circledast \dot{\subseteq} \mathbin{⸾} \texttt{err}\rrparenthesis$

In the non-trivial case $\mathcal{T}\llbracket \rightsquigarrow[s_1,s_2]\rrbracket \neq \texttt{err}$, $\mathcal{S}\llbracket s_1\rrbracket \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_1\rrbracket)$, and $\mathcal{S}\llbracket s_2\rrbracket \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_2\rrbracket)$, we have $\mathcal{S}\llbracket s_1\rrbracket \times \mathcal{S}\llbracket s_2\rrbracket \in \{\langle X, Y\rangle \mid X \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_1\rrbracket) \wedge Y \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_2\rrbracket)\} \triangleq \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_1\rrbracket * \mathcal{S}\llbracket s_2\rrbracket)$ and so $\wp(\mathcal{S}\llbracket s_1\rrbracket \times \mathcal{S}\llbracket s_2\rrbracket) \in \gamma^{\mathfrak{S}}(\mathbf{P}\;(\mathcal{S}\llbracket s_1\rrbracket * \mathcal{S}\llbracket s_2\rrbracket))$. Similarly, $\wp(\mathcal{S}\llbracket s_1\rrbracket) \in \gamma^{\mathfrak{S}}(\mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket)$ and $\wp(\mathcal{S}\llbracket s_2\rrbracket) \in \gamma^{\mathfrak{S}}(\mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket)$ so $\wp(\mathcal{S}\llbracket s_1\rrbracket) \xrightarrow{\cup} \wp(\mathcal{S}\llbracket s_2\rrbracket) \in \{X \mapsto Y \mid X \in \gamma^{\mathfrak{S}}(\mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket) \wedge Y \in \gamma^{\mathfrak{S}}(\mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket)\} \triangleq \gamma^{\mathfrak{S}}(\mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket)$. It follows that

$\mathcal{S}\llbracket \rightsquigarrow[s_1,s_2]\rrbracket$
$\triangleq \llparenthesis \mathcal{S}\llbracket s_1\rrbracket \notin \{\omega,\Omega\} \wedge \mathcal{S}\llbracket s_1\rrbracket \notin \{\omega,\Omega\} \;?\; \langle \wp(\mathcal{S}\llbracket s_1\rrbracket \times \mathcal{S}\llbracket s_2\rrbracket),\, \subseteq\rangle \underset{\alpha^{\rightsquigarrow}}{\overset{\gamma^{\rightsquigarrow}}{\leftrightarrows}} \langle \wp(\mathcal{S}\llbracket s_1\rrbracket) \xrightarrow{\cup} \wp(\mathcal{S}\llbracket s_2\rrbracket),\, \dot{\subseteq}\rangle \mathbin{⸾} \texttt{error}(\mathcal{S}\llbracket s_1\rrbracket, \mathcal{S}\llbracket s_2\rrbracket)\rrparenthesis$
$= \langle \wp(\mathcal{S}\llbracket s_1\rrbracket \times \mathcal{S}\llbracket s_2\rrbracket),\, \subseteq\rangle \underset{\alpha^{\rightsquigarrow}}{\overset{\gamma^{\rightsquigarrow}}{\leftrightarrows}} \langle \wp(\mathcal{S}\llbracket s_1\rrbracket) \xrightarrow{\cup} \wp(\mathcal{S}\llbracket s_2\rrbracket),\, \dot{\subseteq}\rangle$
$\in \{P \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} P' \mid P \in \gamma^{\mathfrak{P}}(\mathbf{P}(\mathcal{S}\llbracket s_1\rrbracket * \mathcal{S}\llbracket s_2\rrbracket) \circledast \subseteq) \wedge P' \in \gamma^{\mathfrak{P}}(\mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket)\}$
$= \gamma^{\mathfrak{T}}(\mathbf{P}(\mathcal{S}\llbracket s_1\rrbracket * \mathcal{S}\llbracket s_2\rrbracket) \circledast \subseteq \leftrightarrows \mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket \circledast \dot{\subseteq})$
$= \gamma^{\mathfrak{T}}(\llparenthesis \mathcal{S}\llbracket s_1\rrbracket \neq \texttt{err} \wedge \mathcal{S}\llbracket s_2\rrbracket \neq \texttt{err} \;?\; \mathbf{P}(\mathcal{S}\llbracket s_1\rrbracket * \mathcal{S}\llbracket s_2\rrbracket) \circledast \subseteq \leftrightarrows \mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket \circledast \dot{\subseteq} \mathbin{⸾} \texttt{err}\rrparenthesis)$
$\subseteq \gamma^{\mathfrak{T}}(\mathcal{T}\llbracket \rightsquigarrow[s_1,s_2]\rrbracket) \cup \{\omega\}$ *QED.*

- $\mathcal{T}\llbracket \mapsto[s_1,s_2]\rrbracket \triangleq \llparenthesis \mathcal{S}\llbracket s_1\rrbracket \neq \texttt{err} \wedge \mathcal{S}\llbracket s_2\rrbracket \neq \texttt{err} \;?\; \mathbf{P}(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathcal{S}\llbracket s_2\rrbracket) \circledast \subseteq \leftrightarrows \mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket \circledast \dot{\subseteq} \mathbin{⸾} \texttt{err}\rrparenthesis$

In the non-trivial case $\mathcal{T}\llbracket \mapsto[s_1,s_2]\rrbracket \neq \texttt{err}$, $\mathcal{S}\llbracket s_1\rrbracket \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_1\rrbracket)$, and $\mathcal{S}\llbracket s_2\rrbracket \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_2\rrbracket)$, we have $\mathcal{S}\llbracket s_1\rrbracket \mapsto \mathcal{S}\llbracket s_2\rrbracket \in \{X \mapsto Y \mid X \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_1\rrbracket) \wedge Y \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_2\rrbracket)\} \triangleq \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathcal{S}\llbracket s_2\rrbracket)$ so $\wp(\mathcal{S}\llbracket s_1\rrbracket \mapsto \mathcal{S}\llbracket s_2\rrbracket) \in \gamma^{\mathfrak{S}}(\mathbf{P}\;(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathcal{S}\llbracket s_2\rrbracket))$. Moreover $\wp(\mathcal{S}\llbracket s_1\rrbracket) \in \gamma^{\mathfrak{S}}(\mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket)$ and $\wp(\mathcal{S}\llbracket s_2\rrbracket) \in \gamma^{\mathfrak{S}}(\mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket)$ imply that $\wp(\mathcal{S}\llbracket s_1\rrbracket) \mapsto \wp(\mathcal{S}\llbracket s_2\rrbracket) \in \{X \mapsto Y \mid X \in \gamma^{\mathfrak{S}}(\mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket) \wedge Y \in \gamma^{\mathfrak{S}}(\mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket)\} \triangleq \gamma^{\mathfrak{S}}((\mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket) \twoheadrightarrow (\mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket))$. It follows that

$\mathcal{S}\llbracket \mapsto[s_1,s_2]\rrbracket$
$\triangleq \llparenthesis \mathcal{S}\llbracket s_1\rrbracket \notin \{\omega,\Omega\} \wedge \mathcal{S}\llbracket s_2\rrbracket \notin \{\omega,\Omega\} \;?\; \langle \wp(\mathcal{S}\llbracket s_1\rrbracket \mapsto \mathcal{S}\llbracket s_2\rrbracket),\, \subseteq\rangle \underset{\alpha^{\mapsto}}{\overset{\gamma^{\mapsto}}{\leftrightarrows}} \langle \wp(\mathcal{S}\llbracket s_1\rrbracket) \mapsto \wp(\mathcal{S}\llbracket s_2\rrbracket),\, \dot{\subseteq}\rangle \mathbin{⸾} \texttt{error}(\mathcal{S}\llbracket s_1\rrbracket, \mathcal{S}\llbracket s_2\rrbracket)\rrparenthesis$
$= \langle \wp(\mathcal{S}\llbracket s_1\rrbracket \mapsto \mathcal{S}\llbracket s_2\rrbracket),\, \subseteq\rangle \underset{\alpha^{\mapsto}}{\overset{\gamma^{\mapsto}}{\leftrightarrows}} \langle \wp(\mathcal{S}\llbracket s_1\rrbracket) \mapsto \wp(\mathcal{S}\llbracket s_2\rrbracket),\, \dot{\subseteq}\rangle$
$\in \{P \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} P' \mid P \in \gamma^{\mathfrak{P}}(\mathbf{P}(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathcal{S}\llbracket s_2\rrbracket) \circledast \subseteq) \wedge P' \in \gamma^{\mathfrak{P}}(\mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket \circledast \dot{\subseteq})\}$
$= \gamma^{\mathfrak{T}}(\mathbf{P}(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathcal{S}\llbracket s_2\rrbracket) \circledast \subseteq \leftrightarrows \mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket \circledast \dot{\subseteq})$
$= \gamma^{\mathfrak{T}}(\llparenthesis \mathcal{S}\llbracket s_1\rrbracket \neq \texttt{err} \wedge \mathcal{S}\llbracket s_2\rrbracket \neq \texttt{err} \;?\; \mathbf{P}(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathcal{S}\llbracket s_2\rrbracket) \circledast \subseteq \leftrightarrows \mathbf{P}\;\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket \circledast \dot{\subseteq} \mathbin{⸾} \texttt{err}\rrparenthesis)$
$\subseteq \gamma^{\mathfrak{T}}(\mathcal{T}\llbracket \mapsto[s_1,s_2]\rrbracket) \cup \{\omega\}$ *QED.*

- $\mathcal{T}\llbracket \times[s_1,s_2]\rrbracket \triangleq \llparenthesis \mathcal{S}\llbracket s_1\rrbracket \neq \texttt{err} \wedge \mathcal{S}\llbracket s_2\rrbracket \neq \texttt{err} \;?\; \mathbf{P}(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathcal{S}\llbracket s_2\rrbracket) \circledast \subseteq \leftrightarrows \mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket \circledast \dot{\subseteq} \mathbin{⸾} \texttt{err}\rrparenthesis$

In the only non-trivial case $\mathcal{T}\llbracket \times[s_1,s_2]\rrbracket \neq \texttt{err}$, $\mathcal{S}\llbracket s_1\rrbracket, \mathcal{S}\llbracket s_2\rrbracket \notin \{\omega,\Omega\}$, we have $\mathcal{S}\llbracket s_i\rrbracket \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_i\rrbracket)$, $i = 1,2$ by structural induction hypothesis. It follows that $\mathcal{S}\llbracket s_1\rrbracket \mapsto \mathcal{S}\llbracket s_2\rrbracket \in \{X \mapsto Y \mid X \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_1\rrbracket) \wedge Y \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_2\rrbracket)\} \triangleq \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathcal{S}\llbracket s_2\rrbracket)$ so $\wp(\mathcal{S}\llbracket s_1\rrbracket \mapsto \mathcal{S}\llbracket s_2\rrbracket) \in \gamma^{\mathfrak{S}}(\mathbf{P}\;(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathcal{S}\llbracket s_2\rrbracket))$ hence $\langle \wp(\mathcal{S}\llbracket s_1\rrbracket \mapsto \mathcal{S}\llbracket s_2\rrbracket),\, \subseteq\rangle \in \gamma^{\mathfrak{P}}(\mathbf{P}(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathcal{S}\llbracket s_2\rrbracket) \circledast \subseteq)$. Moreover $\mathcal{S}\llbracket s_2\rrbracket \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_2\rrbracket)$ implies $\wp(\mathcal{S}\llbracket s_2\rrbracket) \in \gamma^{\mathfrak{S}}(\mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket)$ so $\mathcal{S}\llbracket s_1\rrbracket \mapsto \wp(\mathcal{S}\llbracket s_2\rrbracket) \in \{X \mapsto Y \mid X \in \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_1\rrbracket) \wedge Y \in \gamma^{\mathfrak{S}}(\mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket)\} \triangleq \gamma^{\mathfrak{S}}(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket)$ hence $\langle \mathcal{S}\llbracket s_1\rrbracket \mapsto \wp(\mathcal{S}\llbracket s_2\rrbracket),\, \subseteq\rangle \in \gamma^{\mathfrak{P}}(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket \circledast \subseteq)$. We conclude that

$\mathcal{S}\llbracket \times[s_1,s_2]\rrbracket$
$\triangleq \llparenthesis \mathcal{S}\llbracket s_1\rrbracket \notin \{\omega,\Omega\} \wedge \mathcal{S}\llbracket s_2\rrbracket \notin \{\omega,\Omega\} \;?\; \langle \wp(\mathcal{S}\llbracket s_1\rrbracket \mapsto \mathcal{S}\llbracket s_2\rrbracket),\, \subseteq\rangle \underset{\alpha^{\times}}{\overset{\gamma^{\times}}{\leftrightarrows}} \langle \mathcal{S}\llbracket s_1\rrbracket \mapsto \wp(\mathcal{S}\llbracket s_2\rrbracket),\, \dot{\subseteq}\rangle \mathbin{⸾} \texttt{error}(\mathcal{S}\llbracket s_1\rrbracket, \mathcal{S}\llbracket s_2\rrbracket)\rrparenthesis$
$= \langle \wp(\mathcal{S}\llbracket s_1\rrbracket \mapsto \mathcal{S}\llbracket s_2\rrbracket),\, \subseteq\rangle \underset{\alpha^{\times}}{\overset{\gamma^{\times}}{\leftrightarrows}} \langle \mathcal{S}\llbracket s_1\rrbracket \mapsto \wp(\mathcal{S}\llbracket s_2\rrbracket),\, \dot{\subseteq}\rangle$
$\in \{P \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} P' \mid P \in \gamma^{\mathfrak{P}}(\mathbf{P}(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathcal{S}\llbracket s_2\rrbracket) \circledast \subseteq) \wedge P' \in \gamma^{\mathfrak{P}}(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket \circledast \dot{\subseteq})\}$
$\triangleq \gamma^{\mathfrak{T}}(\mathbf{P}(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathcal{S}\llbracket s_2\rrbracket) \circledast \subseteq \leftrightarrows \mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket \circledast \dot{\subseteq})$
$= \gamma^{\mathfrak{T}}(\llparenthesis \mathcal{S}\llbracket s_1\rrbracket \neq \texttt{err} \wedge \mathcal{S}\llbracket s_2\rrbracket \neq \texttt{err} \;?\; \mathbf{P}(\mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathcal{S}\llbracket s_2\rrbracket) \circledast \subseteq \leftrightarrows \mathcal{S}\llbracket s_1\rrbracket \twoheadrightarrow \mathbf{P}\;\mathcal{S}\llbracket s_2\rrbracket \circledast \dot{\subseteq} \mathbin{⸾} \texttt{err}\rrparenthesis)$
$\triangleq \gamma^{\mathfrak{T}}(\mathcal{T}\llbracket \times[s_1,s_2]\rrbracket)$ *QED.*

- $\mathcal{T}\llbracket \mathsf{R}[g]\rrbracket \triangleq \mathcal{T}\llbracket g\rrbracket$

In case $\mathcal{T}\llbracket \mathsf{R}[g]\rrbracket \neq \texttt{err}$ and $\mathcal{S}\llbracket \mathsf{R}[g]\rrbracket \notin \{\omega,\Omega\}$, we have

$\mathcal{S}\llbracket \mathsf{R}[g]\rrbracket$
$\triangleq \llparenthesis \mathcal{S}\llbracket g\rrbracket = \langle \mathcal{C},\, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A},\, \leqslant\rangle \;?\; \langle \mathcal{C},\, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \{\alpha(P) \mid P \in \mathcal{C}\},\, \leqslant\rangle \mathbin{⸾} \llparenthesis \mathcal{S}\llbracket g\rrbracket = \omega \;?\; \omega \mathbin{⸾} \Omega\rrparenthesis\rrparenthesis$
$= \langle \mathcal{C},\, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \{\alpha(P) \mid P \in \mathcal{C}\},\, \leqslant\rangle$

By structural induction hypothesis, $\mathcal{S}\llbracket g\rrbracket = \langle \mathcal{C},\, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A},\, \leqslant\rangle \in \gamma^{\mathfrak{T}}(\mathcal{T}\llbracket g\rrbracket)$ so $\mathcal{T}\llbracket g\rrbracket = \mathsf{P} \leftrightarrows \mathsf{P}'$ with $\langle \mathcal{C},\, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A},\, \leqslant\rangle \in \gamma^{\mathfrak{T}}(\mathsf{P} \leftrightarrows \mathsf{P}') = \{P \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} P' \mid P \in \gamma^{\mathfrak{P}}(\mathsf{P}) \wedge P' \in \gamma^{\mathfrak{P}}(\mathsf{P}')\}$. Necessarily, $P' = \mathsf{S}' \circledast \mathsf{O}'$ with $\langle \mathcal{A},\, \leqslant\rangle \in \gamma^{\mathfrak{P}}(\mathsf{P}') = \gamma^{\mathfrak{S}}(\mathsf{S}') \times$

$\gamma^{\mathfrak{O}}(\mathsf{O}')$ so $\mathcal{A} \in \gamma^{\mathfrak{S}}(\mathsf{S}')$. But $\{\alpha(P) \mid P \in \mathcal{C}\} \subseteq \mathcal{A}$ and $\gamma^{\mathfrak{S}}(\mathsf{S}')$ is $\subseteq$-downward closed so $\{\alpha(P) \mid P \in \mathcal{C}\} \in \gamma^{\mathfrak{S}}(\mathsf{S}')$ and $\langle\{\alpha(P) \mid P \in \mathcal{C}\},\ \leqslant\rangle \in \gamma^{\mathfrak{S}}(\mathsf{S}') \times \gamma^{\mathfrak{O}}(\mathsf{O}') = \gamma^{\mathfrak{P}}(\mathsf{P}')$. It follows that

$$
\begin{aligned}
& \langle\mathcal{C},\ \sqsubseteq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle\{\alpha(P) \mid P \in \mathcal{C}\},\ \leqslant\rangle \\
\in\ & \{P \xrightleftharpoons[\alpha]{\gamma} P' \mid P \in \gamma^{\mathfrak{P}}(\mathsf{P}) \wedge P' \in \gamma^{\mathfrak{P}}(\mathsf{P}')\} \\
\triangleq\ & \gamma^{\mathfrak{T}}(\mathsf{P} \leftrightarrows \mathsf{P}') \\
\triangleq\ & \gamma^{\mathfrak{T}}(\mathcal{T}[\![\mathsf{R}[g]]\!]) \qquad \textit{QED.}
\end{aligned}
$$

- $\mathcal{T}[\![s \rightarrowtriangle g]\!] \triangleq \llparenthesis \mathcal{S}[\![s]\!] \neq \texttt{err} \wedge \mathcal{T}[\![g]\!] \neq \texttt{err} \mathrel{?} \mathcal{S}[\![s]\!] \mathrel{\ast\!\!\!\leftrightarrowtriangle} \mathcal{T}[\![g]\!] \mathrel{:} \texttt{err} \rrparenthesis$

In the non trivial case $\mathcal{T}[\![s \rightarrowtriangle g]\!] \neq \texttt{err}$, $\mathcal{S}[\![s]\!] \notin \{\omega, \Omega\}$, and $\mathcal{S}[\![g]\!] = \langle\mathcal{C},\ \sqsubseteq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle\mathcal{A},\ \leqslant\rangle \not\ni \{\omega, \Omega\}$, we have $\mathcal{S}[\![s]\!] \in \gamma^{\mathfrak{S}}(\mathcal{S}[\![s]\!])$ and $\langle\mathcal{C},\ \sqsubseteq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle\mathcal{A},\ \leqslant\rangle \in \gamma^{\mathfrak{T}}(\mathcal{T}[\![g]\!])$ by structural induction hypothesis, so that we conclude that

$$
\begin{aligned}
& \mathcal{S}[\![s \rightarrowtriangle g]\!] \\
\triangleq\ & \llparenthesis \mathcal{S}[\![s]\!] = X \notin \{\omega, \Omega\} \wedge \mathcal{S}[\![g]\!] = \langle\mathcal{C},\ \sqsubseteq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle\mathcal{A},\ \leqslant\rangle \mathrel{?} \langle X \mapsto \mathcal{C},\ \dot{\sqsubseteq}\rangle \xrightleftharpoons[\boldsymbol{\lambda}\,\rho \bullet \alpha\circ\rho]{\boldsymbol{\lambda}\,\overline{\rho} \bullet \gamma\circ\overline{\rho}} \langle X \mapsto \mathcal{A},\ \dot{\leqslant}\rangle \mathrel{:} \\
& \quad \mathbf{error}(\mathcal{S}[\![s]\!], \llparenthesis \mathcal{S}[\![g]\!] = \omega \mathrel{?} \omega \mathrel{:} \Omega \rrparenthesis)\rrparenthesis \\
=\ & \langle\mathcal{S}[\![s]\!] \mapsto \mathcal{C},\ \dot{\sqsubseteq}\rangle \xrightleftharpoons[\boldsymbol{\lambda}\,\rho \bullet \alpha\circ\rho]{\boldsymbol{\lambda}\,\overline{\rho} \bullet \gamma\circ\overline{\rho}} \langle\mathcal{S}[\![s]\!] \mapsto \mathcal{A},\ \dot{\leqslant}\rangle \\
\in\ & \{\langle X \mapsto \mathcal{C},\ \dot{\sqsubseteq}\rangle \xrightleftharpoons[\alpha']{\gamma'} \langle X \mapsto \mathcal{A},\ \dot{\leqslant}\rangle \mid X \in \gamma^{\mathfrak{S}}(\mathcal{S}[\![s]\!]) \wedge \langle\mathcal{C}, \\
& \quad \sqsubseteq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle\mathcal{A},\ \leqslant\rangle \in \gamma^{\mathfrak{T}}(\mathcal{T}[\![g]\!])\} \\
\triangleq\ & \gamma^{\mathfrak{T}}(\mathcal{S}[\![s]\!] \mathrel{\ast\!\!\!\leftrightarrowtriangle} \mathcal{T}[\![g]\!]) \\
\triangleq\ & \gamma^{\mathfrak{T}}(\mathcal{T}[\![s \rightarrowtriangle g]\!]) \qquad \textit{QED.}
\end{aligned}
$$

- $\mathcal{T}[\![g_1 \fatsemi g_2]\!] \triangleq \llparenthesis \mathcal{T}[\![g_1]\!] = \mathsf{P}_1 \leftrightarrows \mathsf{P}_2 \wedge \mathcal{T}[\![g_2]\!] = \mathsf{P}_3 \leftrightarrows \mathsf{P}_4 \wedge \mathsf{P}_2 \cong \mathsf{P}_3 \mathrel{?} \mathsf{P}_1 \leftrightarrows \mathsf{P}_4 \mathrel{:} \texttt{err} \rrparenthesis$

In case $\mathcal{T}[\![g_1 \fatsemi g_2]\!] \neq \texttt{err}$ and $\mathcal{S}[\![g_1]\!], \mathcal{S}[\![g_2]\!] \notin \{\Omega, \omega\}$, we have, by structural induction hypothesis, that $\mathcal{S}[\![g_1]\!] = p_1 \xrightleftharpoons[\alpha_1]{\gamma_1} p_2 \in \gamma^{\mathfrak{T}}(\mathcal{T}[\![g_1]\!]) = \gamma^{\mathfrak{T}}(\mathsf{P}_1 \leftrightarrows \mathsf{P}_2) = \{P_1 \xrightleftharpoons[\alpha_1]{\gamma_1} P_2 \mid P_1 \in \gamma^{\mathfrak{P}}(\mathsf{P}_1) \wedge P_2 \in \gamma^{\mathfrak{P}}(\mathsf{P}_2)\}$ so $p_1 \in \gamma^{\mathfrak{P}}(\mathsf{P}_1)$ and $\mathcal{S}[\![g_2]\!] = p_3 \xrightleftharpoons[\alpha_2]{\gamma_2} p_4 \in \gamma^{\mathfrak{T}}(\mathcal{T}[\![g_2]\!]) = \gamma^{\mathfrak{T}}(\mathsf{P}_3 \leftrightarrows \mathsf{P}_4) = \{P_3 \xrightleftharpoons[\alpha_2]{\gamma_2} P_4 \mid P_3 \in \gamma^{\mathfrak{P}}(\mathsf{P}_3) \wedge P_4 \in \gamma^{\mathfrak{P}}(\mathsf{P}_4)\}$ so $p_4 \in \gamma^{\mathfrak{P}}(\mathsf{P}_4)$. Moreover $\mathsf{P}_4 \cong \mathsf{P}_4$ so $p_2 \in \gamma^{\mathfrak{P}}(\mathsf{P}_2) = \gamma^{\mathfrak{P}}(\mathsf{P}_3) \ni p_3$. Nevertheless this type requirement is too weak to ensure that $p_2 = p_3$. When $p_2 \neq p_3$, the semantics returns a dynamic error ω allowed by the type system. Otherwise $p_2 = p_3$, in which case

$$
\begin{aligned}
& \mathcal{S}[\![g_1 \fatsemi g_2]\!] \\
\triangleq\ & \llparenthesis \mathcal{S}[\![g_1]\!] = p_1 \xrightleftharpoons[\alpha_1]{\gamma_1} p_2 \wedge \mathcal{S}[\![g_2]\!] = p_3 \xrightleftharpoons[\alpha_2]{\gamma_2} p_4 \mathrel{?} \llparenthesis p_2 = \\
& \quad p_3 \mathrel{?} p_1 \xrightleftharpoons[\alpha_2\circ\alpha_1]{\gamma_1\circ\gamma_2} p_4 \mathrel{:} \omega \rrparenthesis \mathrel{:} \mathbf{error}(\llparenthesis \mathcal{S}[\![g_1]\!] = \omega \mathrel{?} \omega \mathrel{:} \\
& \quad \Omega \rrparenthesis, \llparenthesis \mathcal{S}[\![g_2]\!] = \omega \mathrel{?} \omega \mathrel{:} \Omega \rrparenthesis)\rrparenthesis \\
=\ & p_1 \xrightleftharpoons[\alpha_2\circ\alpha_1]{\gamma_1\circ\gamma_2} p_4 \qquad \wr\text{in the non-trivial case}\wr \\
\in\ & \{P_1 \xrightleftharpoons[\alpha]{\gamma} P_4 \mid P_1 \in \gamma^{\mathfrak{P}}(\mathsf{P}_1) \wedge P_4 \in \gamma^{\mathfrak{P}}(\mathsf{P}_4)\} \\
& \qquad \wr\text{since } p_1 \in \gamma^{\mathfrak{P}}(\mathsf{P}_1) \text{ and } p_4 \in \gamma^{\mathfrak{P}}(\mathsf{P}_4)\wr \\
\triangleq\ & \gamma^{\mathfrak{T}}(\mathsf{P}_1 \leftrightarrows \mathsf{P}_4) \\
\triangleq\ & \gamma^{\mathfrak{T}}(\mathcal{T}[\![g_1 \fatsemi g_2]\!]) \qquad \textit{QED.}
\end{aligned}
$$

- $\mathcal{T}[\![g_1 \divideontimes g_2]\!] \triangleq \llparenthesis \mathcal{T}[\![g_1]\!] = \mathsf{S}_1 \circledast \mathsf{O}_1 \leftrightarrows \mathsf{S}_2 \circledast \mathsf{O}_2 \wedge \mathcal{T}[\![g_2]\!] = \mathsf{S}_3 \circledast \mathsf{O}_3 \leftrightarrows \mathsf{S}_4 \circledast \mathsf{O}_4 \mathrel{?} \mathsf{S}_1 \ast \mathsf{S}_2 \circledast \mathsf{O}_1 \star \mathsf{O}_2 \leftrightarrows \mathsf{S}_3 \ast \mathsf{S}_4 \circledast \mathsf{O}_3 \star \mathsf{O}_4 \mathrel{:} \texttt{err} \rrparenthesis$

In case $\mathcal{T}[\![g_1 \divideontimes g_2]\!] \neq \texttt{err}$, $\mathcal{S}[\![g_1]\!] = \langle\mathcal{C}_1,\ \subseteq\rangle \xrightleftharpoons[\alpha_1]{\gamma_1} \langle\mathcal{A}_1,\ \sqsubseteq\rangle \neq \omega$, and $\mathcal{S}[\![g_2]\!] = \langle\mathcal{C}_2,\ \Subset\rangle \xrightleftharpoons[\alpha_2]{\gamma_2} \langle\mathcal{A}_2,\ \preceq\rangle \neq \omega$, we have $\langle\mathcal{C}_1,\ \subseteq\rangle \in \gamma^{\mathfrak{P}}(\mathsf{S}_1 \circledast \mathsf{O}_1)$, $\langle\mathcal{A}_1,\ \sqsubseteq\rangle \in \gamma^{\mathfrak{P}}(\mathsf{S}_2 \circledast \mathsf{O}_2)$, $\langle\mathcal{C}_2,\ \Subset\rangle \in \gamma^{\mathfrak{P}}(\mathsf{S}_3 \circledast \mathsf{O}_3)$, and $\langle\mathcal{A}_2, \preceq\rangle \in \gamma^{\mathfrak{P}}(\mathsf{S}_4 \circledast \mathsf{O}_4)$, by structural induction hypothesis.

It follows that $\mathcal{C}_1 \in \gamma^{\mathfrak{S}}(\mathsf{S}_1)$, $\mathcal{C}_2 \in \gamma^{\mathfrak{S}}(\mathsf{S}_2)$, $\subseteq\ \in \gamma^{\mathfrak{O}}(\mathsf{O}_1)$, $\Subset\ \in \gamma^{\mathfrak{O}}(\mathsf{O}_2)$, and therefore $\langle\mathcal{C}_1 \times \mathcal{C}_2,\ \subseteq \times \Subset\rangle \in (\{X \times Y \mid X \in \gamma^{\mathfrak{S}}(\mathsf{S}_1) \wedge Y \in \gamma^{\mathfrak{S}}(\mathsf{S}_2)\}) \times (\gamma^{\mathfrak{O}}(\mathsf{O}_1) \times \gamma^{\mathfrak{O}}(\mathsf{O}_2)) = \gamma^{\mathfrak{S}}(\mathsf{S}_1 \ast \mathsf{S}_2) \times \gamma^{\mathfrak{O}}(\mathsf{O}_1 \star \mathsf{O}_2) = \gamma^{\mathfrak{P}}(\mathsf{S}_1 \ast \mathsf{S}_2 \circledast \mathsf{O}_1 \star \mathsf{O}_2)$ and similarly $\langle\mathcal{A}_1 \times \mathcal{A}_2,\ \sqsubseteq \times \preceq\rangle \in \gamma^{\mathfrak{P}}(\mathsf{S}_3 \ast \mathsf{S}_4 \circledast \mathsf{O}_3 \star \mathsf{O}_4)$

We conclude that

$$
\begin{aligned}
& \mathcal{S}[\![g_1 \divideontimes g_2]\!] \\
\triangleq\ & \langle\mathcal{C}_1 \times \mathcal{C}_2,\ \subseteq \times \Subset\rangle \xrightleftharpoons[\alpha_1\times\alpha_2]{\gamma_1\times\gamma_2} \langle\mathcal{A}_1 \times \mathcal{A}_2,\ \sqsubseteq \times \preceq\rangle \\
\in\ & \{P \xrightleftharpoons[\alpha]{\gamma} P' \mid P \in \gamma^{\mathfrak{P}}(\mathsf{S}_1 \ast \mathsf{S}_2 \circledast \mathsf{O}_1 \star \mathsf{O}_2) \wedge P' \in \\
& \quad \gamma^{\mathfrak{P}}(\mathsf{S}_3 \ast \mathsf{S}_4 \circledast \mathsf{O}_3 \star \mathsf{O}_4)\} \\
\triangleq\ & \gamma^{\mathfrak{T}}(\mathcal{T}[\![\mathsf{S}_1 \ast \mathsf{S}_2 \circledast \mathsf{O}_1 \star \mathsf{O}_2 \leftrightarrows \mathsf{S}_3 \ast \mathsf{S}_4 \circledast \mathsf{O}_3 \star \mathsf{O}_4]\!]) \\
\triangleq\ & \gamma^{\mathfrak{T}}(\mathcal{T}[\![g_1 \divideontimes g_2]\!]) \qquad \textit{QED.}
\end{aligned}
$$

- $\mathcal{T}[\![g_1 \Longrightarrow g_2]\!] \triangleq \llparenthesis \mathcal{T}[\![g_1]\!] = \mathsf{S}_1 \circledast \mathsf{O}_1 \leftrightarrows \mathsf{S}_2 \circledast \mathsf{O}_2 \wedge \mathcal{T}[\![g_2]\!] = \mathsf{S}_3 \circledast \mathsf{O}_3 \leftrightarrows \mathsf{S}_4 \circledast \mathsf{O}_4 \mathrel{?} \mathsf{S}_1 \mathrel{\ast\!\!\!\leftrightarrow} \mathsf{S}_3 \circledast \dot{\mathsf{O}}_3 \leftrightarrows \mathsf{S}_2 \mathrel{\ast\!\!\!\leftrightarrow} \mathsf{S}_4 \circledast \dot{\mathsf{O}}_4 \mathrel{:} \texttt{err} \rrparenthesis$

$\mathcal{T}[\![g_1 \Longrightarrow g_2]\!] \neq \texttt{err}$, $\mathcal{S}[\![g_1]\!] = \langle\mathcal{C}_1,\ \subseteq\rangle \xrightleftharpoons[\alpha_1]{\gamma_1} \langle\mathcal{A}_1,\ \sqsubseteq\rangle \neq \omega$ so $\mathcal{C}_1 \in \gamma^{\mathfrak{S}}(\mathsf{S}_1)$, $\subseteq\ \in \gamma^{\mathfrak{O}}(\mathsf{O}_1)$, $\mathcal{A}_1 \in \gamma^{\mathfrak{S}}(\mathsf{S}_2)$, $\sqsubseteq\ \in \gamma^{\mathfrak{O}}(\mathsf{O}_2)$ by structural induction hypothesis, and similarly for $\mathcal{S}[\![g_2]\!] = \langle\mathcal{C}_2,\ \preceq\rangle \xrightleftharpoons[\alpha_2]{\gamma_2} \langle\mathcal{A}_2,\ \leqslant\rangle \neq \omega$ where $\preceq\ \in \gamma^{\mathfrak{O}}(\mathsf{O}_3)$ so $\dot{\preceq}\ \in \gamma^{\mathfrak{O}}(\dot{\mathsf{O}}_3)$ and $\leqslant\ \in \gamma^{\mathfrak{O}}(\mathsf{O}_4)$ so $\dot{\leqslant}\ \in \gamma^{\mathfrak{O}}(\dot{\mathsf{O}}_4)$. It follows that $\mathcal{C}_1 \xrightarrow{\nearrow} \mathcal{C}_2 \in \{X \mapsto Y \mid X \in \gamma^{\mathfrak{S}}(\mathsf{S}_1) \wedge Y \in \gamma^{\mathfrak{S}}(\mathsf{S}_3)\} \triangleq \gamma^{\mathfrak{S}}(\mathsf{S}_1 \mathrel{\ast\!\!\!\leftrightarrow} \mathsf{S}_3)$ and similarly $\mathcal{A}_1 \xrightarrow{\nearrow} \mathcal{A}_2 \in \gamma^{\mathfrak{S}}(\mathsf{S}_2 \mathrel{\ast\!\!\!\leftrightarrow} \mathsf{S}_4)$. We conclude that

$$
\begin{aligned}
& \mathcal{S}[\![g_1 \Longrightarrow g_2]\!] \\
\triangleq\ & \langle\mathcal{C}_1 \xrightarrow{\nearrow} \mathcal{C}_2,\ \dot{\preceq}\rangle \xrightleftharpoons[\boldsymbol{\lambda}\,f \bullet \alpha_2\circ f\circ\gamma_1]{\boldsymbol{\lambda}\,g \bullet \gamma_2\circ g\circ\alpha_1} \langle\mathcal{A}_1 \xrightarrow{\nearrow} \mathcal{A}_2,\ \dot{\leqslant}\rangle \\
=\ & \{\langle S,\ O\rangle \xrightleftharpoons[\alpha]{\gamma} \langle S',\ O'\rangle \mid S \in \gamma^{\mathfrak{S}}(\mathsf{S}_1 \mathrel{\ast\!\!\!\leftrightarrow} \mathsf{S}_3) \wedge O \in \\
& \quad \gamma^{\mathfrak{O}}(\dot{\mathsf{O}}_3) \wedge S' \in \gamma^{\mathfrak{S}}(\mathsf{S}_2 \mathrel{\ast\!\!\!\leftrightarrow} \mathsf{S}_4) \wedge O' \in \gamma^{\mathfrak{O}}(\dot{\mathsf{O}}_4)\} \\
=\ & \{P \xrightleftharpoons[\alpha]{\gamma} P' \mid P \in \gamma^{\mathfrak{P}}(\mathsf{S}_1 \mathrel{\ast\!\!\!\leftrightarrow} \mathsf{S}_3 \circledast \dot{\mathsf{O}}_3) \wedge P' \in \\
& \quad \gamma^{\mathfrak{P}}(\mathsf{S}_2 \mathrel{\ast\!\!\!\leftrightarrow} \mathsf{S}_4 \circledast \dot{\mathsf{O}}_4)\} \\
\triangleq\ & \gamma^{\mathfrak{T}}(\mathsf{S}_1 \mathrel{\ast\!\!\!\leftrightarrow} \mathsf{S}_3 \circledast \dot{\mathsf{O}}_3 \leftrightarrows \mathsf{S}_2 \mathrel{\ast\!\!\!\leftrightarrow} \mathsf{S}_4 \circledast \dot{\mathsf{O}}_4) \\
\triangleq\ & \gamma^{\mathfrak{T}}(\mathcal{T}[\![g_1 \Longrightarrow g_2]\!]) \qquad \textit{QED.}
\end{aligned}
$$

11. Rule-based typing deduction system Abstract interpretations can always be presented by a suitable generalization of rule-based deduction systems [4].

We write $x \vdash \mathsf{T}$ to mean that $\mathcal{E}[\![x]\!]/\mathcal{S}[\![x]\!]/\mathcal{O}[\![x]\!]/\mathcal{P}[\![x]\!]/\mathcal{T}[\![x]\!] = \mathsf{T}$ (with discrimination on the syntax of x). The rule-based typing deduction system can only derive $x \vdash \mathsf{T}$ when $\mathcal{E}[\![x]\!]/\mathcal{S}[\![x]\!]/\mathcal{O}[\![x]\!]/\mathcal{P}[\![x]\!]/\mathcal{T}[\![x]\!] \neq \texttt{err}$. So an expression which is not typable by the type system is understood to have type $\texttt{err}$. Otherwise stated, $\texttt{err}$ encodes untypable.

[4] Patrick Cousot, Radhia Cousot: Compositional and Inductive Semantic Definitions in Fixpoint, Equational, Constraint, Closure-condition, Rule-based and Game-Theoretic Form. CAV 1995: 293–308.

11.1 Elements

$\mathsf{true} \vdash \mathtt{bool}$ $\quad \mathsf{false} \vdash \mathtt{bool}$ $\quad 0 \vdash \mathtt{int}$ $\quad 1 \vdash \mathtt{int}$ $\quad \infty \vdash \mathtt{int}$

$\mathrm{x} \vdash \mathtt{var}$ $\quad \mathrm{y} \vdash \mathtt{var}$ $\quad \ell \vdash \mathtt{lab}$ $\quad \dfrac{e \vdash \mathtt{bool}}{-e \vdash \mathtt{bool}}$ $\quad \dfrac{e \vdash \mathtt{int}}{-e \vdash \mathtt{int}}$

11.2 Sets

$\mathbb{B} \vdash \mathbf{P}\ \mathtt{bool}$ $\quad \mathbb{Z} \vdash \mathbf{P}\ \mathtt{int}$ $\quad \mathbb{X} \vdash \mathbf{P}\ \mathtt{var}$

$\mathbb{L} \vdash \mathbf{P}\ \mathtt{lab}$ $\quad \dfrac{e \vdash \mathsf{E}}{\{e\} \vdash \mathbf{P}\ \mathsf{E}}$ $\quad \dfrac{e_1 \vdash \mathsf{E}_1, \quad e_2 \vdash \mathsf{E}_2, \quad \mathsf{E}_1 \cong \mathsf{E}_2}{[e_1, e_2] \vdash \mathbf{P}\ \mathsf{E}_1}$

$\dfrac{s \vdash \mathsf{S}}{\mathbb{I}(s, o) \vdash \mathbf{P}\ \mathsf{S}}$ $\quad \dfrac{s \vdash \mathsf{S}}{s^{\infty} \vdash \mathbf{seq}\ \mathsf{S}}$ $\quad \dfrac{s_1 \vdash \mathsf{S}_1, \quad s_2 \vdash \mathsf{S}_2, \quad \mathsf{S}_1 \cong \mathsf{S}_2}{s_1 \cup s_2 \vdash \mathsf{S}_1}$

$\dfrac{s_1 \vdash \mathsf{S}_1, \quad s_2 \vdash \mathsf{S}_2}{s_1 \mapsto s_2 \vdash \mathsf{S}_1 \ast\!\!\leftrightarrow \mathsf{S}_2}$ $\quad \dfrac{s_1 \vdash \mathsf{S}_1, \quad s_2 \vdash \mathsf{S}_2}{s_1 \times s_2 \vdash \mathsf{S}_1 \ast \mathsf{S}_2}$ $\quad \dfrac{s \vdash \mathsf{S}}{\wp(s) \vdash \mathbf{P}\ \mathsf{S}}$

11.3 Partial orders and posets

$o \vdash o, \quad o \in \{\Rightarrow, \Leftrightarrow, \leq, \subseteq, =\}$ $\quad \underline{\in} \vdash \subseteq$ $\quad \dfrac{o \vdash \mathsf{O}}{o^{-1} \vdash (\mathsf{O})^{-1}}$

$\dfrac{o_1 \vdash \mathsf{O}_1, \quad o_2 \vdash \mathsf{O}_2}{o_1 \times o_2 \vdash \mathsf{O}_1 \ast \mathsf{O}_2}$ $\quad \dfrac{o \vdash \mathsf{O}}{\dot{o} \vdash (\dot{\mathsf{O}})}$ $\quad \dfrac{o \vdash \mathsf{O}}{\ddot{o} \vdash ((\dot{\dot{\mathsf{O}}}))}$ $\quad \dfrac{s \vdash \mathsf{S}, \quad o \vdash \mathsf{o}'}{\langle s, o \rangle \vdash \mathsf{S} \circledast o'}$

11.4 Galois connections

$\dfrac{p \vdash \mathsf{P},}{\mathbb{1}[p] \vdash \mathsf{P} \leftrightarrows \mathsf{P}}$ $\quad \dfrac{e \vdash \mathsf{E}, \quad p \vdash \mathsf{S} \circledast \mathsf{O}, \quad \mathsf{E} \Subset \mathsf{S}}{\top[p, e] \vdash \mathsf{S} \circledast \mathsf{O} \leftrightarrows \mathsf{S} \circledast \mathsf{O}}$

$\dfrac{s \vdash \mathsf{S}, \quad b \vdash \mathsf{E}_b, \quad t \vdash \mathsf{E}_t, \quad \mathsf{E}_b \Subset \mathsf{S}, \quad \mathsf{E}_t \Subset \mathsf{S}}{\mathbb{I}[\langle s, o \rangle, b, t] \vdash (\mathbf{P}\ \mathsf{S} \circledast \subseteq) \leftrightarrows (\mathbf{P}\ \mathsf{S} \circledast \subseteq)}$

$\dfrac{s_{\mathbb{L}} \vdash \mathsf{S}_{\mathbb{L}}, \quad s_{\mathcal{M}} \vdash \mathsf{S}_{\mathcal{M}}}{\curvearrowright[s_{\mathbb{L}}, s_{\mathcal{M}}] \vdash \mathbf{P}\ (\mathsf{S}_{\mathbb{L}} \ast \mathsf{S}_{\mathcal{M}}) \circledast \subseteq \ \leftrightarrows\ \mathsf{S}_{\mathbb{L}} \ast\!\!\leftrightarrow \mathbf{P}\ \mathsf{S}_{\mathcal{M}} \circledast \dot{\subseteq}}$

$\dfrac{s \vdash \mathsf{S}}{\bigcup[s] \vdash \mathbf{P}\ (\mathbf{P}\ \mathsf{S}) \circledast \subseteq \ \leftrightarrows\ \mathbf{P}\ \mathsf{S} \circledast \subseteq}$ $\quad \dfrac{s \vdash \mathsf{S}}{\neg[s] \vdash \mathbf{P}\ \mathsf{S} \circledast \subseteq \ \leftrightarrows\ \mathbf{P}\ \mathsf{S} \circledast \subseteq^{-1}}$

$\dfrac{s \vdash \mathsf{S}}{\infty[s] \vdash \mathbf{P}\ (\mathbf{seq}\ \mathsf{S}) \circledast \subseteq \ \leftrightarrows\ \mathbf{P}\ \mathsf{S} \circledast \subseteq}$

$\dfrac{s_1 \vdash \mathsf{S}_1, \quad s_2 \vdash \mathsf{S}_2}{\rightsquigarrow[s_1, s_2] \vdash \mathbf{P}(\mathsf{S}_1 \ast \mathsf{S}_2) \circledast \subseteq \ \leftrightarrows\ \mathbf{P}\ \mathsf{S}_1 \ast\!\!\leftrightarrow \mathbf{P}\ \mathsf{S}_2 \circledast \dot{\subseteq}}$

$\dfrac{s_1 \vdash \mathsf{S}_1, \quad s_2 \vdash \mathsf{S}_2}{\mapsto[s_1, s_2] \vdash \mathbf{P}(\mathsf{S}_1 \ast\!\!\leftrightarrow \mathsf{S}_2) \circledast \subseteq \ \leftrightarrows\ \mathbf{P}\ \mathsf{S}_1 \ast\!\!\leftrightarrow \mathbf{P}\ \mathsf{S}_2 \circledast \dot{\subseteq}}$

$\dfrac{s_1 \vdash \mathsf{S}_1, \quad s_2 \vdash \mathsf{S}_2}{\times[s_1, s_2] \vdash \mathbf{P}(\mathsf{S}_1 \ast\!\!\leftrightarrow \mathsf{S}_2) \circledast \subseteq \ \leftrightarrows\ \mathsf{S}_1 \ast\!\!\leftrightarrow \mathbf{P}\ \mathsf{S}_2 \circledast \dot{\subseteq}}$

$\dfrac{g \vdash \mathsf{T}}{\mathsf{R}[g] \vdash \mathsf{T}}$ $\quad \dfrac{s \vdash \mathsf{S}, \quad g \vdash \mathsf{T}}{s \multimap g \vdash \mathsf{S} \ast\!\!\multimap \mathsf{T}}$

$\dfrac{g_1 \vdash \mathsf{P}_1 \leftrightarrows \mathsf{P}_2, \quad g_2 \vdash \mathsf{P}_3 \leftrightarrows \mathsf{P}_4, \quad \mathsf{P}_2 \cong \mathsf{P}_3}{g_1 \mathbin{;} g_2 \vdash \mathsf{P}_1 \leftrightarrows \mathsf{P}_4}$

$\dfrac{g_1 \vdash \mathsf{S}_1 \circledast \mathsf{O}_1 \leftrightarrows \mathsf{S}_2 \circledast \mathsf{O}_2, \quad g_2 \vdash \mathsf{S}_3 \circledast \mathsf{O}_3 \leftrightarrows \mathsf{S}_4 \circledast \mathsf{O}_4}{g_1 \ast g_2 \vdash \mathsf{S}_1 \ast \mathsf{S}_2 \circledast \mathsf{O}_1 \star \mathsf{O}_2 \leftrightarrows \mathsf{S}_3 \ast \mathsf{S}_4 \circledast \mathsf{O}_3 \star \mathsf{O}_4}$

$\dfrac{g_1 \vdash \mathsf{S}_1 \circledast \mathsf{O}_1 \leftrightarrows \mathsf{S}_2 \circledast \mathsf{O}_2, \quad g_2 \vdash \mathsf{S}_3 \circledast \mathsf{O}_3 \leftrightarrows \mathsf{S}_4 \circledast \mathsf{O}_4}{g_1 \Longmapsto g_2 \vdash \mathsf{S}_1 \ast\!\!\leftrightarrow \mathsf{S}_3 \circledast \dot{\mathsf{O}_3} \leftrightarrows \mathsf{S}_2 \ast\!\!\leftrightarrow \mathsf{S}_4 \circledast \dot{\mathsf{O}_4}}$

12. Principal type As usual for syntactic abstractions like types, there is in general no best abstraction of an arbitrary set[5]. For example there is no best regular expression to describe as precisely as possible a non-regular language. There is no best set type for an empty set. As shown in [2], the problem is solved for typing both by restricting types (*e.g.* no disjunctive type in ML which requires to tag the alternatives) and the programming language (*e.g.* alternatives of conditionals in ML cannot return objects of different types). The same is true for the *GC* calculus, in that there is a best abstraction for the properties of semantic objects generated by the language, although none exists in general.

[5] Patrick Cousot, Radhia Cousot: Formal Language, Grammar and Set-Constraint-Based Program Analysis by Abstract Interpretation. FPCA 1995: 170–181

12.1 Best abstraction of ur-element properties

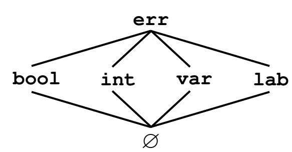
The ur-element properties are $\mathcal{P}^{\mathfrak{e}} \triangleq \wp(\{\mathcal{S}[\![e]\!] \mid e \in \mathbb{E}\})$. Define

- $\alpha^{\mathfrak{e}}(\emptyset) \triangleq \varnothing$[6], and otherwise
- $\alpha^{\mathfrak{e}}(P) \triangleq \mathtt{bool}$, when $\emptyset \neq P \subseteq \mathbb{B}$;
- $\alpha^{\mathfrak{e}}(P) \triangleq \mathtt{int}$, when $\emptyset \neq P \subseteq \mathbb{Z} \cup \{-\infty, \infty\}$;
- $\alpha^{\mathfrak{e}}(P) \triangleq \mathtt{var}$, when $\emptyset \neq P \subseteq \mathbb{X}$;
- $\alpha^{\mathfrak{e}}(P) \triangleq \mathtt{lab}$, when $\emptyset \neq P \subseteq \mathbb{L}$;
- $\alpha^{\mathfrak{e}}(P) \triangleq \mathtt{err}$, otherwise.

We have defined

- $\gamma^{\mathfrak{e}}(\varnothing) \triangleq \emptyset$;
- $\gamma^{\mathfrak{e}}(\mathtt{bool}) \triangleq \mathbb{B}$;
- $\gamma^{\mathfrak{e}}(\mathtt{int}) \triangleq \mathbb{Z} \cup \{-\infty, \infty\}$;
- $\gamma^{\mathfrak{e}}(\mathtt{var}) \triangleq \mathbb{X}$;
- $\gamma^{\mathfrak{e}}(\mathtt{lab}) \triangleq \mathbb{L}$;
- $\gamma^{\mathfrak{e}}(\mathtt{err}) \triangleq \{\mathcal{S}[\![e]\!] \mid e \in \mathbb{E}\}$.

We extend $\trianglelefteq$ to $\varnothing \trianglelefteq \varnothing \trianglelefteq \mathsf{E}$ for all $\mathsf{E} \in \mathfrak{E}$ so that we have the following lattice of element types.



It follows that

$$
\begin{array}{ll}
& \alpha^{\mathfrak{e}}(P) \trianglelefteq \mathsf{E} \\
\Leftrightarrow & \alpha^{\mathfrak{e}}(P) = \mathsf{E} \qquad \qquad \wr \text{def. } \trianglelefteq \text{ on } \mathfrak{E} \wr \\
\Leftrightarrow & P \subseteq \gamma^{\mathfrak{e}}(\mathsf{E}) \qquad \qquad \wr \text{def. } \alpha^{\mathfrak{e}} \text{ and } \gamma^{\mathfrak{e}} \wr
\end{array}
$$

and so $\langle \mathcal{P}^{\mathfrak{e}}, \subseteq \rangle \xrightleftharpoons[\alpha^{\mathfrak{e}}]{\gamma^{\mathfrak{e}}} \langle \mathfrak{E} \cup \{\varnothing\}, \trianglelefteq \rangle$. Moreover $\gamma^{\mathfrak{e}}$ is injective so $\langle \mathcal{P}^{\mathfrak{e}}, \subseteq \rangle \xrightleftharpoons[\alpha^{\mathfrak{e}}]{\gamma^{\mathfrak{e}}} \langle \mathfrak{E} \cup \{\varnothing\}, \trianglelefteq \rangle$. We conclude that any ur-element semantic property $P \in \mathcal{P}^{\mathfrak{e}}$ now has a $\trianglelefteq$-best abstraction in $\mathfrak{E} \cup \{\varnothing\}$ which is their principal type $\alpha^{\mathfrak{e}}(P)$.

12.2 Best abstraction of set properties

The set semantic properties are $\mathcal{P}^{\mathfrak{S}} \triangleq \wp(\{\mathcal{S}[\![s]\!] \mid s \in \mathbb{S}\})$ *i.e.* the properties of those mathematical sets describable by the formal language $\mathbb{S}$ such as $\wp(\emptyset)$ which best abstraction is $\mathbf{P}\ \varnothing$, $\{\{\mathsf{true}\}, \mathbb{B}\}$ which best abstraction is $\mathbf{P}\ \mathbb{B}$ and $\{\{1\}, \mathbb{B}\}$ which best abstraction is $\mathtt{err}$.

If $P \in \mathcal{P}^{\mathfrak{S}}$ then either $P = \emptyset$ and $\alpha^{\mathfrak{S}}(\emptyset) \triangleq \varnothing$ else $P = \{\mathcal{S}[\![s_i]\!] \mid i \in \Delta \wedge \forall i \in \Delta : s_i \in \mathbb{S}\}, \Delta \neq \emptyset$. Then consider $\mathsf{S}_i \triangleq \mathbb{S}[\![s_i]\!]$, $i \in \Delta$. If $\forall i, j \in \Delta : \mathsf{S}_i \cong \mathsf{S}_j$ then $\alpha^{\mathfrak{S}}(P) = [\mathsf{S}_i]_{\cong}$ for some $i \in \Delta$ which choice is irrelevant. Else $\exists i, j \in \Delta : \mathsf{S}_i \ncong \mathsf{S}_j$, in which case $\alpha^{\mathfrak{S}}(P) = \mathtt{err}$.

Observe that $\alpha^{\mathfrak{S}}$ is increasing, sound since $\alpha^{\mathfrak{S}}(P) \trianglelefteq \mathsf{S} \Rightarrow P \subseteq \gamma^{\mathfrak{S}}(\mathsf{S})$, and the best abstraction since $P \subseteq \gamma^{\mathfrak{S}}(\mathsf{S}) \Rightarrow \alpha^{\mathfrak{S}}(P) \trianglelefteq \mathsf{S}$.

It follows that $\langle \mathcal{P}^{\mathfrak{S}}, \subseteq \rangle \xrightleftharpoons[\alpha^{\mathfrak{S}}]{\gamma^{\mathfrak{S}}} \langle (\mathfrak{S} \cup \{\varnothing\})_{/\cong}, \trianglelefteq \rangle$ where $\trianglelefteq$ is naturally expended to equivalence classes since $\alpha^{\mathfrak{S}}$ is onto/$\gamma^{\mathfrak{S}}$ injective.

[6] By analogy with a programming language, $\emptyset$ would be the false invariant so that $\varnothing$ would be the type of unreachable code.

12.3 Best abstraction of partial order and poset properties

The partial order properties are $\mathcal{P}^{\mathfrak{O}} \triangleq \wp(\{\mathcal{S}[\![o]\!] \mid o \in \mathbb{O}\})$. Define $\alpha^{\mathfrak{O}}(P) \triangleq \llparenthesis P = \emptyset \mathrel{?} \varnothing \parallel \exists \mathsf{O} \in \mathfrak{O} : \forall o \in \mathbb{O} : \mathcal{S}[\![o]\!] \in P \Rightarrow \mathscr{O}[\![o]\!] \cong \mathsf{O} \mathrel{?} [\mathsf{O}]_{\cong} \mathrel{:} \mathtt{err} \rrparenthesis$. Then $\langle \mathcal{P}^{\mathfrak{O}}, \subseteq\rangle \underset{\alpha^{\mathfrak{O}}}{\overset{\gamma^{\mathfrak{O}}}{\leftrightarrows}} \langle (\mathfrak{O} \cup \{\varnothing\})_{/\cong}, \trianglelefteq\rangle$.

Similarly, poset properties are $\mathcal{P}^{\mathfrak{P}} \triangleq \wp(\{\mathcal{S}[\![p]\!] \mid p \in \mathbb{P}\})$. Define $\alpha^{\mathfrak{P}}(P) \triangleq \llparenthesis P = \emptyset \mathrel{?} \varnothing \parallel \exists \mathsf{P} : \forall \mathcal{S}[\![o]\!] \in P : \mathscr{P}[\![p]\!] \cong \mathsf{P} \mathrel{?} [\mathsf{P}]_{\cong} \mathrel{:} \mathtt{err} \rrparenthesis$. Then $\langle \mathcal{P}^{\mathfrak{P}}, \subseteq\rangle \underset{\alpha^{\mathfrak{P}}}{\overset{\gamma^{\mathfrak{P}}}{\leftrightarrows}} \langle (\mathfrak{P} \cup \{\varnothing\})_{/\cong}, \trianglelefteq\rangle$.

12.4 Best abstraction of *GC* properties

Finally, the semantic properties $P = \{\mathcal{S}[\![g_i]\!] \mid i \in \Delta\}$ of *GC* expressions, the principal type is $\alpha^{\mathfrak{T}}(\emptyset) \triangleq \varnothing$, $\alpha^{\mathfrak{T}}(P) \triangleq [\mathsf{T}]_{\cong}$ when $\forall i \in \Delta \neq \emptyset : \mathscr{T}[\![g_i]\!] \cong \mathsf{T}$ else $\alpha^{\mathfrak{T}}(P) \triangleq \mathtt{err}$ so $\langle \wp(\{\mathcal{S}[\![g]\!] \mid g \in \mathbb{G}\}), \subseteq\rangle \underset{\alpha^{\mathfrak{T}}}{\overset{\gamma^{\mathfrak{T}}}{\leftrightarrows}} \langle (\mathfrak{T} \cup \{\varnothing\})_{/\cong}, \trianglelefteq\rangle$ since $\alpha^{\mathfrak{T}}$ is onto.

13. Types of types To add one more level of abstraction, we can consider types of types.

Types $\mathcal{T} \triangleq \{\mathfrak{E}, \mathfrak{S}, \mathfrak{O}, \mathfrak{P}, \mathfrak{T}\}$ have properties which are sets of types *i.e.* $\mathcal{P} \triangleq \wp(\mathfrak{E} \cup \mathfrak{S} \cup \mathfrak{O} \cup \mathfrak{P} \cup \mathfrak{T}) = \wp(\bigcup \mathcal{T})$ abstracted by types of types $\overline{\mathfrak{T}} ::= \overline{\varnothing} \mid \overline{\mathfrak{E}} \mid \overline{\mathfrak{S}} \mid \overline{\mathfrak{O}} \mid \overline{\mathfrak{P}} \mid \overline{\mathfrak{T}} \mid \overline{\mathtt{err}}$.

The abstraction is $\alpha^{\overline{\mathfrak{T}}}(P) \triangleq \llparenthesis P = \emptyset \mathrel{?} \overline{\varnothing} \parallel P \subseteq \mathsf{T}, \mathsf{T} \in \{\mathfrak{E}, \mathfrak{S}, \mathfrak{O}, \mathfrak{P}, \mathfrak{T}\} \mathrel{?} \overline{\mathsf{T}} \mathrel{:} \overline{\mathtt{err}} \rrparenthesis$.

The concretization is $\gamma^{\overline{\mathfrak{T}}}(\overline{\mathsf{T}}) \triangleq \llparenthesis \overline{\mathsf{T}} = \overline{\varnothing} \mathrel{?} \emptyset \parallel \overline{\mathsf{T}} \in \{\overline{\mathfrak{E}}, \overline{\mathfrak{S}}, \overline{\mathfrak{O}}, \overline{\mathfrak{P}}, \overline{\mathfrak{T}}\} \mathrel{?} \mathsf{T} \mathrel{:} \mathfrak{E} \cup \mathfrak{S} \cup \mathfrak{O} \cup \mathfrak{P} \cup \mathfrak{T} \rrparenthesis$ so $\gamma^{\overline{\mathfrak{T}}}(\overline{\mathtt{err}}) = \mathfrak{E} \cup \mathfrak{S} \cup \mathfrak{O} \cup \mathfrak{P} \cup \mathfrak{T}$.

Defining $\overline{\mathsf{T}} \mathrel{\overline{\trianglelefteq}} \overline{\mathsf{T}}' \triangleq \gamma^{\overline{\mathfrak{T}}}(\overline{\mathsf{T}}) \subseteq \gamma^{\overline{\mathfrak{T}}}(\overline{\mathsf{T}}')$, we get the flat partial order $\overline{\varnothing} \mathrel{\overline{\trianglelefteq}} \overline{\varnothing} \mathrel{\overline{\trianglelefteq}} \overline{\mathsf{T}} \mathrel{\overline{\trianglelefteq}} \overline{\mathsf{T}} \mathrel{\overline{\trianglelefteq}} \overline{\mathtt{err}} \mathrel{\overline{\trianglelefteq}} \overline{\mathtt{err}}$ for all $\mathsf{T} \in \{\mathfrak{E}, \mathfrak{S}, \mathfrak{O}, \mathfrak{P}, \mathfrak{T}\}$.

The abstraction is $\langle \mathcal{P}, \subseteq\rangle \underset{\alpha^{\overline{\mathfrak{T}}}}{\overset{\gamma^{\overline{\mathfrak{T}}}}{\leftrightarrows}} \langle \overline{\mathfrak{T}}, \overline{\trianglelefteq}\rangle$ where $\alpha^{\overline{\mathfrak{T}}}(\mathcal{P})$ is the principal type of type of the type property $\mathcal{P}$.

Define the type inference $\overline{\mathscr{T}}[\![\mathsf{T}]\!] \triangleq \alpha^{\overline{\mathfrak{T}}}(\{\mathsf{T}\})$ for all $\mathsf{T} \in \bigcup \mathcal{T}$. The typing rules for the meta-language that we have used to define $\mathscr{T}$ include traditional rules $\mathscr{T}^{\mathbb{B}}$ for Boolean expressions as well as

- $\overline{\mathscr{T}}[\![\mathtt{bool}]\!] = \overline{\mathscr{T}}[\![\mathtt{int}]\!] = \overline{\mathscr{T}}[\![\mathtt{var}]\!] = \overline{\mathscr{T}}[\![\mathtt{lab}]\!] \triangleq \overline{\mathfrak{E}}$
- $\overline{\mathscr{T}}[\![\mathtt{P}\ X]\!] \triangleq \llparenthesis \overline{\mathscr{T}}[\![X]\!] = \mathfrak{E} \vee \overline{\mathscr{T}}[\![X]\!] = \mathfrak{S} \mathrel{?} \mathfrak{S} \mathrel{:} \overline{\mathtt{err}} \rrparenthesis$
- $\overline{\mathscr{T}}[\![\subseteq]\!] \triangleq \overline{\mathfrak{O}}$
- $\overline{\mathscr{T}}[\![(X)^{-1}]\!] \triangleq \llparenthesis \overline{\mathscr{T}}[\![X]\!] = \overline{\mathfrak{O}} \mathrel{?} \overline{\mathfrak{O}} \mathrel{:} \overline{\mathtt{err}} \rrparenthesis$
- $\overline{\mathscr{T}}[\![X_1 \circledast X_2]\!] \triangleq \llparenthesis \overline{\mathscr{T}}[\![X_1]\!] = \overline{\mathfrak{S}} \wedge \overline{\mathscr{T}}[\![X_2]\!] = \overline{\mathfrak{O}} \mathrel{?} \overline{\mathfrak{P}} \mathrel{:} \overline{\mathtt{err}} \rrparenthesis$
- $\overline{\mathscr{T}}[\![X_1 \leftrightarrows X_2]\!] \triangleq \llparenthesis \overline{\mathscr{T}}[\![X_1]\!] = \overline{\mathscr{T}}[\![X_2]\!] = \overline{\mathfrak{P}} \mathrel{?} \overline{\mathfrak{T}} \mathrel{:} \overline{\mathtt{err}} \rrparenthesis$
- $\overline{\mathscr{T}}[\![X_1 \mathbin{;} X_2]\!] \triangleq \llparenthesis \overline{\mathscr{T}}[\![X_1]\!] = \overline{\mathscr{T}}[\![X_2]\!] = \overline{\mathfrak{T}} \mathrel{?} \overline{\mathfrak{T}} \mathrel{:} \overline{\mathtt{err}} \rrparenthesis$
- $\overline{\mathscr{T}}[\![\llparenthesis X_1 \mathrel{?} X_2 \mathrel{:} X_3 \rrparenthesis]\!] \triangleq \llparenthesis \mathscr{T}^{\mathbb{B}}[\![X_1]\!] = \mathtt{bool} \wedge (\overline{\mathscr{T}}[\![X_2]\!] = \overline{\mathscr{T}}[\![X_3]\!] \vee X_3 = \mathtt{err}) \mathrel{?} \overline{\mathscr{T}}[\![X_2]\!] \mathrel{:} \overline{\mathtt{err}} \rrparenthesis$
- *etc.*

Well-typing of types requires that $\overline{\mathscr{T}}[\![\mathsf{T}]\!] \neq \overline{\mathtt{err}}$. In particular, for all $g \in \mathbb{G}$, $\overline{\mathscr{T}}[\![\mathscr{T}[\![g]\!]]\!] \neq \overline{\mathtt{err}}$ so that $\mathscr{T}[\![g]\!]$ is well-defined that is "well-types types cannot go wrong".

Notice that the typing of types rules correspond to the routine informal verification of mathematical texts by checking that operators take their arguments and return their results in their domains of definition.

14. Abstraction of induction by widening/narrowing In static analyzers [1, 12, 14] *GCs* specify abstract domains modules and Galois connectors their combinations by functors. For scalability and precision, rapid convergence acceleration of infinite fixpoint computations by widening/narrowing abstracting induction and/or their duals for co-induction [3–5] is more precise than finite abstractions [8].

This can be illustrated for recursive definitions of sets such as $\mathbf{lfp}^{\subseteq}\, \boldsymbol{\lambda} S \bullet \{\emptyset\} \cup \wp(S) = \{\emptyset\} \cup \wp(\{\emptyset\}) \cup \wp(\{\emptyset\} \cup \wp(\{\emptyset\})) \cup \ldots\} = \{\emptyset\} \cup \{\emptyset, \{\emptyset\}\} \cup \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\} \cup \ldots\} = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}, \ldots\}$ which can be typed by introducing recursive/fixpoint type definitions such as $\mathbf{lfp}^{\trianglelefteq}\, \boldsymbol{\lambda} \mathsf{S} \bullet \mathtt{P}\, \varnothing \cup \mathtt{P}\, \mathsf{S}$.

This requires a widening, such as the trivial one considered in ML typing, hidden in the type inference rules, and requiring that all actual arguments in recursive calls have the same type [2] .

References

[1] B. Blanchet, P. Cousot, R. Cousot, J. Feret, L. Mauborgne, A. Miné, D. Monniaux, and X. Rival. A static analyzer for large safety-critical software. *PLDI*, 196–207. 2003.

[2] P. Cousot. Types as abstract interpretations. *POPL*, 316–331. 1997.

[3] P. Cousot and R. Cousot. Static determination of dynamic properties of programs. *Proc. 2nd Int. Symp. on Programming*, 106–130, Paris, 1976. Dunod.

[4] P. Cousot and R. Cousot. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. *POPL*, 238–252. 1977.

[5] P. Cousot and R. Cousot. Static determination of dynamic properties of recursive procedures. *IFIP Conf. on Formal Description of Programming Concepts, St-Andrews, N.B., CN*, 237–277. North-Holland Pub. Co., 1977.

[6] P. Cousot and R. Cousot. Systematic design of program analysis frameworks. *POPL*, 269–282. 1979.

[7] P. Cousot and R. Cousot. Abstract interpretation frameworks. *J. Logic and Comp.*, 2(4):511–547, 1992.

[8] P. Cousot and R. Cousot. Comparing the Galois connection and widening/narrowing approaches to abstract interpretation. *PLILP*, LNCS 631, 269–295. 1992.

[9] P. Cousot and R. Cousot. Inductive definitions, semantics and abstract interpretation. *POPL*, 83–94. 1992.

[10] P. Cousot and R. Cousot. Temporal abstract interpretation. *POPL*, 12–25. 2000.

[11] P. Cousot and R. Cousot. Systematic design of program transformation frameworks by abstract interpretation. *POPL*, 178–190. 2002.

[12] P. Cousot and R. Cousot. An abstract interpretation-based framework for software watermarking. *POPL*, 173–185. 2004.

[13] P. Cousot and R. Cousot. An abstract interpretation framework for termination. *POPL*, 245–258. 2012.

[14] P. Cousot, R. Cousot, and F. Logozzo. A parametric segmentation functor for fully automatic and scalable array content analysis. *POPL*, 105–118. 2011.

[15] P. Cousot and N. Halbwachs. Automatic discovery of linear restraints among variables of a program. *POPL*, 84–96. 1978.