Calculational Design of Hyperlogics by Abstract Interpretation

PATRICK COUSOT and JEFFERY WANG, CS, Courant Institute of Mathematical Studies, NYU, USA

We design various logics for proving hyper properties of iterative programs by application of abstract interpretation principles.

In part I, we design a generic, structural, fixpoint abstract interpreter parameterized by an algebraic abstract domain describing finite and infinite computations that can be instantiated for various operational, denotational, or relational program semantics. Considering semantics as program properties, we define a post algebraic transformer for execution properties (e.g. sets of traces) and a Post algebraic transformer for semantic (hyper) properties (e.g. sets of sets of traces), we provide corresponding calculuses as instances of the generic abstract interpreter, and we derive under and over approximation hyperlogics.

In part II, we define exact and approximate semantic abstractions, and show that they preserve the mathematical structure of the algebraic semantics, the collecting semantics post, the hyper collecting semantics Post, and the hyperlogics.

Since proofs by sound and complete hyperlogics require an exact characterization of the program semantics within the proof, we consider in part III abstractions of the (hyper) semantic properties that yield simplified proof rules. These abstractions include the join, the homomorphic, the elimination, the principal ideal, the order ideal, the frontier order ideal, and the chain limit algebraic abstractions, as well as their combinations, that lead to new algebraic generalizations of hyperlogics, including the $\forall\exists^*$, $\forall\forall^*$, and $\exists\forall^*$ hyperlogics.

CCS Concepts: • **Theory of computation → Logic and verification**.

Additional Key Words and Phrases: abstract interpretation, calculational design, completeness, correctness, hyperlogic, hyperproperty, incorrectness, nontermination, semantics, soundness, termination.

ACM Reference Format:
Patrick Cousot and Jeffery Wang. 2024. Calculational Design of Hyperlogics by Abstract Interpretation. 1, 1 (November 2024), 72 pages. https://doi.org/https://doi.org/10.1145/3704852

1 Introduction

Program (hyper) logics provide methods for reasoning about (sets of) program executions as defined by a semantics. For example, hyperproperties were defined by Michael Clarkson and Fred Schneider on execution traces [14] but more recent proposals consider relational logics. We aim at designing program (hyper) logics independently of a specific program semantics, and, more precisely, independently of the formal representation of program executions used by these semantics.

In part I, we recall elements of set and order theories (sect. 2) and then define a structural fixpoint *algebraic program semantics* (sect. 3.4) which is an abstract interpreter parameterized by an *algebraic abstract domain* (sect. 3.3) defined axiomatically. The abstract domain includes terminating and nonterminating executions and can be instantiated to various data and execution models such as the classic relational semantics (sect. 5) or the trace semantics corresponding to the original

Authors' Contact Information: Patrick Cousot, pcousot@cims.nyu.edu; Jeffery Wang, cw3736@nyu.edu, CS, Courant Institute of Mathematical Studies, NYU, New York, NY, USA.

ACM XXXX-XXXX/2024/11-ART
https://doi.org/https://doi.org/10.1145/3704852

definition of hyperproperties [14] (sect. 4 in the appendix) . Then in sect. 6, we define an *execution collecting semantics* (e.g. sets of traces i.e. trace properties) and introduce a sound and complete calculus post of execution properties. In sect. 7, we define a *semantic collecting semantics* (e.g. sets of sets of traces i.e. hyperproperties) and introduce a structural, fixpoint, sound, and complete calculus Post of semantics properties. In sect. 8, we define *upper and lower semantic logics* (e.g. a logic for trace hyperproperties) and derive over and under *sound and complete proof systems* by calculational design.

In part II, we define the abstraction of the structural algebraic program semantics (sect. 9) and show that it induces an abstraction of the algebraic execution collecting semantics (sect. 10), the algebraic semantic collecting semantics (sect. 11), and the algebraic upper and lower logics (sect. 12). Such abstractions preserve the mathematical structure of the algebraic semantic, collecting semantics, and logics in the abstract. This shows that the algebraic semantics, collecting semantics, and logics can be instantiated to any one in the *hierarchies of semantics* considered e.g. in [4, 18, 41].

Hyperlogics are under or over approximations of semantic properties that is sets of semantics. A program semantics satisfies a hyperproperty if and only if it appears *exactly* in the hyperproperty. It follows that proofs by semantic logics (for hyperproperties) require, for completeness, to describe the program semantics exactly in the proof. By analogy with Hoare logic, this would require the loop invariants to be the strongest, which is an extreme requirement.

This is why, in part III, we consider abstractions of semantic properties, which are less general, but otherwise offer adequate representations of semantic properties and/or allow for much simplified proof rules, closer to the tradition of classic program execution logics, and complete for well identified classes of *abstract semantic properties.* The classic *join abstraction* (sect. 13), *homomorphic abstraction* (sect. 14), and *intersection abstraction* (sect. 15) yield simplified proof rules for hyperlogics. The *principal ideal* (sect. 16), *order ideal* (sect. 17), *frontiers* (sect. 18), *chain limit* (sect. 19), *chain limit order ideal* (sect. 20) abstractions are more specific to hyperproperties. They are compared in sect. 23. These abstraction generalize known hyperlogics for the algebraic semantics and allow us to provide new sound and complete proof rules, including for $\forall\exists$ (sect. 19.2), $\forall\forall$ (sect. 20.2), and $\exists\forall$ (sect. 22) (hyper)properties.. This last case is based on conjunctive abstractions (i.e. conjunctions in logics or reduced products in static analysis) studied in sect. 22.1 of the appendix).

We finally briefly refer to the related works (already cited extensively in the text) in sect. 24 and summarize our contributions in the conclusion which also proposes future work (sect. 25).

Part I: Algebraic Semantics, Execution Properties, Semantic (Hyper) Properties, Calculi, and Logics

2 Elements of Set and Order Theories

2.1 Partially Ordered Sets

Definition 2.1 (Properties of posets). Let $\langle \mathbb{L}, \sqsubseteq\rangle$ be a poset with partially defined least upper bound (lub or join) $\sqcup$, greatest lower bound (glb or meet) $\sqcap$, infimum $\bot$, and supremum $\top$, if any. [31].

i. $\langle L, \sqsubseteq, \sqcup\rangle$ is a *join semilattice* when the least upper bound (lub, join) $\sqcup S$ exists for any nonempty finite subset $S \in \wp(L) \setminus \{\varnothing\}$ of L. If it exists, the infimum is $\bot = \sqcup\varnothing$. The dual is a *meet semilattice* with greatest lower bound (glb, meet) $\sqcap$ and supremum $\top = \sqcup L$, if it exists. A *lattice* is both a join and meet semilattice. By *limit* we mean either the join or the meet.

ii. A poset is *increasing chain complete* if and only if every nonempty increasing chain of L has a lub. It is *decreasing chain complete* if and only if every nonempty decreasing chain of L has a glb[1]. It is *chain complete* if both increasing and decreasing chain complete.

iii. A poset is a *complete lattice* if and only if any subset, including the empty set, has a lub (hence a glb and the infimum and supremum do exist).

Observe that (2.1.i) and (2.1.ii) are independent (i.e. none implies the other). We often use them simultaneously. For example, in a *increasing chain-complete join semilattice*, lubs exist for non-empty finite sets and non-empty increasing chains.

2.2 Ordinals

We let $\mathbb{O} = \{0, 1, 2, \ldots, \omega, \omega+1, \omega+2, \ldots, \omega\times 2, \omega\times 2+1, \omega\times 2+2, \ldots, \omega\times 3, \ldots, \omega\times\omega = \omega^2, \ldots, \omega^{\omega}, \ldots, \omega^{\omega^{\omega}}, \ldots, \omega^{\omega^{\cdot^{\cdot^{\omega}}}}\}^{\omega\text{ times}}, \ldots\}$ be the class of ordinals where ω is the first infinite limit ordinal [72]. $\langle\mathbb{O}, \leqslant\rangle$ extends the order on the naturals $\langle\mathbb{N}, \leqslant\rangle$ into the infinite. Ordinals yield typical examples of well-orderings (such that any two elements are comparable and any $<$-strictly decreasing chain is finite). Any well-ordering is order-isomorphic to an ordinal (called its rank e.g. ω for $\mathbb{N}$), [72, th. 13.10 & 13.11]. We use Von Neumann definition of ordinals [72, ch. 2] with $0 = \varnothing$, the successor is $\delta+1 = \delta\cup\{\delta\}$, $<$ is $\in$, $\lambda = \bigcup_{\beta<\lambda}\beta$ for infinite limit ordinals λ (which are not a successor ordinal such as ω, ω^2, etc), and the corresponding transfinite induction [72, Sec. 10], $P(0)$, $\forall\delta\in\mathbb{O}\mathrel{.}P(\delta)\Rightarrow P(\delta+1)$, and for all limit ordinals $\lambda\in\mathbb{O}$, $(\forall\beta<\lambda\mathrel{.}P(\beta))\Rightarrow P(\lambda)$ implies $\forall\delta\in\mathbb{O}\mathrel{.}P(\delta)$.

2.3 Functions on Partially Ordered Sets

Definition 2.2 (Properties of functions on posets). Let $\langle L, \sqsubseteq\rangle$ be a poset and $f\in L\rightarrow L$.

i. f is *increasing* (sometimes referred to as *monotone* or *isotone*) means that $\forall x, y\in L\mathrel{.}(x\sqsubseteq y)\Rightarrow(f(x)\sqsubseteq f(y))$. "Increasing" is order self-dual. *Decreasing* (or *antitone*) is $\forall x, y\in L\mathrel{.}(x\sqsubseteq y)\Rightarrow(f(y)\sqsubseteq f(x))$;

For example, a sequence $\langle X^{\delta}\in L, \delta<\lambda\rangle$ for ordinals $\delta, \lambda\in\mathbb{O}$ is an increasing chain means that $\forall\delta\leqslant\delta'<\lambda\mathrel{.}X^{\delta}\sqsubseteq X^{\delta'}$. A decreasing chain has $\forall\delta\leqslant\delta'<\lambda\mathrel{.}X^{\delta'}\sqsubseteq X^{\delta}$;

ii. Function f is *existing finite join-preserving* (also written *existing finite $\sqcup$-preserving*) if and only if for any non-empty finite set $S\in\wp_f(L)\setminus\{\varnothing\}$ such that $\sqcup S$ exists in L then $\sqcup f(S)$ exists in L and $f(\sqcup S) = \sqcup f(S)$ with $f(S) = \{f(x)\mid x\in S\}$, and dually for meets. f is *existing finite limit-preserving* if and only if it is both existing finite join and meet preserving. "Existing" can be omitted in a lattice;

iii. f is *upper-continuous* (or existing increasing chain join-preserving) if and only if for any non-empty increasing chain $S\in\wp_f(L)$ such that $\sqcup S$ exists in L, then $\sqcup f(S)$ exists in L such that $f(\sqcup S) = \sqcup f(S)$. The dual is *lower-continuous* for existing decreasing chain meet-preserving, and *continuous* means both lower and upper continuous. By Scott-Kleene theorem, continuity ensures that functions reach fixpoints iteratively at ω [20, th. 15.36]. This condition for *convergence at ω* is sufficient but not necessary e.g. [20, th. 15.21];

iv. f is *existing join-preserving* (also written *existing $\sqcup$-preserving*) if and only if for any non-empty set $S\in\wp(L)\setminus\{\varnothing\}$ such that $\sqcup S$ exists in L, then $\sqcup f(S)$ exists in L such that $f(\sqcup S) = \sqcup f(S)$, and dually for meets. f is *existing limit-preserving* if and only if it is both existing join and meet preserving. "Existing" can be omitted in a complete lattice;

v. The definitions 2.2.ii to 2.2.iv are extended to $f\in(L\times L)\rightarrow L$ by f has *left limit property* if and only if $\forall y\in L\mathrel{.}\boldsymbol{\lambda}x\bullet f(x,y)$ has that limit property and f has *right limit property* whenever

[1] We do not respectively use the classic *CPO* and *dual CPO* for which chains are usually restricted to be of length ω.

$\forall x \in L \,.\, \boldsymbol{\lambda} y \bullet f(x, y)$ has that limit property. f has that the limit property *in both parameters* if and only if f has both of the left and right limit properties;

vi. When extending the definitions 2.2.ii to 2.2.v to empty sets or chains, the function f is then said to be *lower strict*, dually *upper strict*, and *strict* for both cases.

Observe that 2.2.i $\Leftarrow$ 2.2.ii $\Leftarrow$ 2.2.iii $\Leftarrow$ 2.2.iv.

2.4 Fixpoints

Let $f \in \mathbb{L} \xrightarrow{\nearrow} \mathbb{L}$ be an increasing function on a poset $\langle \mathbb{L},\ \sqsubseteq\rangle$. There are essentially two classic characterizations of the least fixpoint $\mathsf{lfp}^{\sqsubseteq} f$ of f (we also use their order duals).

Proposition 2.3 (Fixpoint). $\mathsf{lfp}^{\sqsubseteq} f = \bigsqcap\{x \mid f(x) \sqsubseteq x\}$ *by* [81] *on complete lattices which also holds on increasing chain complete posets* [38].

Proposition 2.4 (Iteration to fixpoint). *If* $\langle \mathbb{L},\ \sqsubseteq,\ \bot,\ \sqcup\rangle$ *is a poset with infimum* $\bot$ *and partially defined join* $\sqcup$ *then the iterates* $\langle X^{\delta},\ \delta \in \mathbb{O}\rangle$ *of* f *are partially defined as* $X^{\delta+1} \triangleq f(X^{\delta})$*, and* $X^{\lambda} \triangleq \bigsqcup_{\beta<\lambda} X^{\beta}$ *for limit ordinals* λ *(hence* $X^0 = \bigsqcup \varnothing = \bot$ *for limit ordinal* 0*). They are well defined when* f *is increasing (hence when it is finite join preserving, upper-continuous or existing join-preserving) and* $\langle \mathbb{L},\ \sqsubseteq,\ \bot,\ \sqcup\rangle$ *is an increasing chain complete poset (hence when it is a complete lattice) in which case they form an increasing chain (i.e.* $\forall \beta < \delta \in \mathbb{O} \,.\, X^{\beta} \sqsubseteq X^{\delta}$*) ultimately stationary at the limit* $\exists \epsilon \,.\, \forall \beta \geqslant \epsilon \,.\, X^{\beta} = \mathsf{lfp}^{\sqsubseteq} f$ [23]*. In case* f *is upper-continuous (hence when preserving existing joins), the iterates are stationary at* $\epsilon = \omega$ *so that the iterates may be restricted to* $\mathbb{N}$ *and* $\mathsf{lfp}^{\sqsubseteq} f = \bigsqcup_{n\in\mathbb{N}} X^{n}$ [81, page 305].

2.5 Galois Connections, Retractions, and Isomorphisms

Galois connections are used throughout the paper either to formalize correspondances between transformers or to formalize exact or approximate abstractions. Formally, a Galois connection $\langle C,\ \sqsubseteq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle A,\ \preceq\rangle$ is a pair $\langle \alpha,\ \gamma\rangle$ of functions between posets $\langle C,\ \sqsubseteq\rangle$ and $\langle A,\ \preceq\rangle$ satisfying $\forall x \in C \,.\, \forall y \in A \,.\, \alpha(x) \preceq y \Leftrightarrow x \sqsubseteq \gamma(y)$. We use a double headed arrow $\twoheadrightarrow$ to indicate surjection in Galois retractions and $\mathrel{\substack{\twoheadleftarrow \\ \twoheadrightarrow}}$ for bijections. We use classic properties of Galois connections which proofs are found in [34].

2.6 Closures

We let $\mathbb{1}$ be the identity function. An upper closure operator ρ on $\mathbb{L}$ is increasing, extensive and idempotent so $\langle \mathbb{L},\ \sqsubseteq\rangle \xrightleftharpoons[\rho]{\mathbb{1}} \langle \rho(\mathbb{L}),\ \sqsubseteq\rangle$ where $\rho(X) \triangleq \{\rho(x) \mid x \in X\}$ is the post image (dually, a lower closure operator is reductive). It follows that ρ preserves existing arbitrary joins so if $\langle \mathbb{L},\ \sqsubseteq,\ \bot,\ \sqcup\rangle$ is an increasing chain complete poset (respectively complete lattice $\langle \mathbb{L},\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$) then $\langle \rho(\mathbb{L}),\ \sqsubseteq\rangle$ has the same structure with infimum $\rho(\bot)$, join $\boldsymbol{\lambda} X \bullet \rho(\sqcup X)$, meet $\sqcap$ and top $\top$, if any. In case of a complete lattice this is Morgan Ward's [83, th. 4.1]. If ρ_1 and ρ_2 are upper closures on $\mathbb{L}$ then $\rho_1 \circ \rho_2$ and $\rho_2 \circ \rho_1$ are upper closure operators on $\mathbb{L}$ if and only if ρ_1 and ρ_2 are commuting (i.e. $\rho_1 \circ \rho_2 = \rho_2 \circ \rho_1$) in which case $\rho_1 \circ \rho_2(\mathbb{L}) = \rho_2 \circ \rho_1(\mathbb{L}) = \rho_1(\mathbb{L}) \cap \rho_2(\mathbb{L})$ [76, p. 525].

3 Algebraic Semantics

We introduce the syntax and algebraic semantics of a simple iterative language based on an abstract domain that generalizes [20, Ch. 21] to include infinite program behaviors. The algebraic semantics is reminiscent of [12, 17, 37, 49, 50, 56, 57, 59, 60, 74] and others. Such algebraic semantics are a basis for studying a hierarchy of program properties independently of the data manipulated by programs.

3.1 Syntax

We consider an imperative language $\mathbb{S}$ with assignments, sequential composition, conditionals, and conditional iteration with breaks. The syntax is $\texttt{S} \in \mathbb{S} ::= \texttt{x = A} \mid \texttt{x = [}a\texttt{,}b\texttt{]} \mid \texttt{skip} \mid \texttt{S;S} \mid \texttt{if (B) S else S} \mid \texttt{while (B) S} \mid \texttt{break}$. $\texttt{A}$ is an arithmetic expression. The nondeterministic assignment $\texttt{x = [}a\texttt{, }b\texttt{]}$ with $a \in \mathbb{Z} \cup \{-\infty\}$ and $b \in \mathbb{Z} \cup \{\infty\}$, $-\infty - 1 = -\infty$, $\infty + 1 = \infty$ (or any, possibly unbounded, order isomorphic set). The Boolean expressions $\texttt{B}$ include the negation $\neg\texttt{B}$. A $\texttt{break}$ exits the closest enclosing loop (which existence is to be checked syntactically).

3.2 Structural Definitions

Let $\lhd$ be the "immediate strict syntactic component" well-founded partial order on statements $\mathbb{S}$ such that $\texttt{S}_1 \lhd \texttt{S}_1\texttt{;S}_2$, $\texttt{S}_2 \lhd \texttt{S}_1\texttt{;S}_2$, $\texttt{S}_1 \lhd \texttt{if (B) S}_1\texttt{ else S}_2$, $\texttt{S}_2 \lhd \texttt{if (B) S}_1\texttt{ else S}_2$, $\texttt{S} \lhd \texttt{while (B) S}$, and is otherwise false.

Given a nonempty set $\mathcal{V}$, the function $f \in \mathbb{S} \to \mathcal{V}$ has a structural definition if and only if $f(\texttt{S}) \in \mathcal{V}$ for basic commands (defined as minimal elements of $\lhd$) and, otherwise, is of the form $f(\texttt{S}) = F_{\texttt{S}}(\{\langle \texttt{S}', f(\texttt{S}')\rangle \mid \texttt{S}' \lhd \texttt{S}\})$ where $F_{\texttt{S}} \in \{\langle \texttt{S}', v'\rangle \mid \texttt{S}' \lhd \texttt{S} \wedge v' \in \mathcal{V}\} \to \mathcal{V}$ is a total function. Denotational semantics, Hoare logic, predicate transformers, and the abstract semantics of sect. 3.4 all have structural definitions (called "compositional" in denotational semantics).

3.3 Algebraic Computational Domain

We consider computational domains $\mathbb{D}^\sharp_+$ and $\mathbb{D}^\sharp_\infty$ to be abstract domains respectively abstracting the finite and infinite computations of statements and partially ordered by the respective computational orderings $\sqsubseteq^\sharp_+$ and $\sqsubseteq^\sharp_\infty$, as follows ($\fatsemi^\sharp$ is polymorphic).

$$\mathbb{D}^\sharp_+ \triangleq \langle \mathbb{L}^\sharp_+,\ \sqsubseteq^\sharp_+,\ \bot^\sharp_+,\ \sqcup^\sharp_+,\ \mathsf{init}^\sharp,\ \mathsf{assign}^\sharp[\![\mathsf{x}, \mathsf{A}]\!],\ \mathsf{rassign}^\sharp[\![\mathsf{x}, a, b]\!],\ \mathsf{test}^\sharp[\![\mathsf{B}]\!],\ \mathsf{break}^\sharp,\ \mathsf{skip}^\sharp,\ \fatsemi^\sharp\rangle \tag{1}$$

$$\mathbb{D}^\sharp_\infty \triangleq \langle \mathbb{L}^\sharp_\infty,\ \sqsubseteq^\sharp_\infty,\ \top^\sharp_\infty,\ \sqcap^\sharp_\infty,\ \fatsemi^\sharp\rangle \tag{2}$$

Example 3.1. Bi-inductive definitions [24] are used in [18] to define a trace semantics on states Σ which can be isomorphically decomposed into the domain of finite traces $\langle \mathbb{L}^\sharp_+, \sqsubseteq^\sharp_+, \bot^\sharp_+, \sqcup^\sharp_+\rangle = \langle \wp(\Sigma^*), \subseteq, \varnothing, \cup\rangle$ (where $\cup$ is the lub of increasing chains starting form $\varnothing$ for least fixpoints) and the domain of infinite traces $\langle \mathbb{L}^\sharp_\infty, \sqsubseteq^\sharp_\infty, \top^\sharp_\infty, \sqcap^\sharp_\infty\rangle = \langle \wp(\Sigma^\omega), \subseteq, \Sigma^\omega, \cap\rangle$ (where $\cap$ is the glb of decreasing chains starting form Σ^ω for greatest fixpoints), which abstractions yield a hierarchy of classic semantics, including Hoare logic.

Our objective in part I is to study hyperlogics abstracting away from a particular semantics thus allowing for multiple instantiations (such as traces in sect. 4) and, in part II, for multiple abstractions (which include Hoare logic).

A single domain $\mathbb{D}^\sharp \triangleq \mathbb{D}^\sharp_+ \cup \mathbb{D}^\sharp_\infty$ is used in denotational semantics [78, 80] but this is not always possible e.g. when $\mathbb{D}^\sharp_+ \cap \mathbb{D}^\sharp_\infty \neq \varnothing$. Moreover the separation into two different domains for finite and infinite executions allows e.g. for the use of input-output relations for finite behaviors and traces for infinite behaviors. (see also the discussion in remark 4.5 in the appendix.) ■

Definition 3.2 (Abstract domain well-definedness). We say that $\mathbb{D}^\sharp \triangleq \langle \mathbb{D}^\sharp_+, \mathbb{D}^\sharp_\infty\rangle$ is a well-defined chain-complete lattice (respectively complete lattice) with increasing (respectively finite limit-preserving, continuous, and existing limit-preserving) composition, if and only if

A. The finitary calculational domain $\langle \mathbb{L}^\sharp_+, \sqsubseteq^\sharp_+, \bot^\sharp_+, \sqcup^\sharp_+\rangle$ is an increasing chain-complete join semilattice with infimum, (respectively $\langle \mathbb{L}^\sharp_+, \sqsubseteq^\sharp_+, \bot^\sharp_+, \top^\sharp_+, \sqcup^\sharp_+, \sqcap^\sharp_+\rangle$ is a complete lattice);

B. $\mathsf{init}^\sharp, \mathsf{break}^\sharp, \mathsf{skip}^\sharp \in \mathbb{L}^\sharp_+$, $\mathsf{assign}^\sharp[\![\mathsf{x}, \mathsf{A}]\!]$, $\mathsf{rassign}^\sharp[\![\mathsf{x}, a, b]\!]$, $\mathsf{test}^\sharp[\![\mathsf{B}]\!] \in \mathbb{L}^\sharp_+$ are well-defined in $\mathbb{L}^\sharp_+$;

C. The infinitary calculational domain $\langle \mathbb{L}^\sharp_\infty, \sqsubseteq^\sharp_\infty, \top^\sharp_\infty, \sqcup^\sharp_\infty, \sqcap^\sharp_\infty\rangle$ is a decreasing chain-complete join lattice with supremum (respectively $\langle \mathbb{L}^\sharp_\infty, \sqsubseteq^\sharp_\infty, \bot^\sharp_\infty, \top^\sharp_\infty, \sqcup^\sharp_\infty, \sqcap^\sharp_\infty\rangle$ is a complete lattice);

D. The sequential composition $\fatsemi^\sharp \in \big(\mathbb{L}^\sharp_+ \times \mathbb{L}^\sharp_+ \to \mathbb{L}^\sharp_+\big) \cup \big(((\mathbb{L}^\sharp_+ \times \mathbb{L}^\sharp_\infty) \cup (\mathbb{L}^\sharp_\infty \times \mathbb{L}^\sharp_+) \cup (\mathbb{L}^\sharp_\infty \times \mathbb{L}^\sharp_\infty)) \to \mathbb{L}^\sharp_\infty\big)$ is associative and satisfies the following conditions (where $\langle \mathbb{L}^\sharp_x, \sqsubseteq^\sharp_x, \bot^\sharp_x, \top^\sharp_x, \sqcup^\sharp_x, \sqcap^\sharp_x \rangle$, $x \in \{+, \infty\}$ designates $\langle \mathbb{L}^\sharp_+, \sqsubseteq^\sharp_+, \bot^\sharp_+, \top^\sharp_+, \sqcup^\sharp_+, \sqcap^\sharp_+ \rangle$ when $x = +$ and $\langle \mathbb{L}^\sharp_\infty, \sqsubseteq^\sharp_\infty, \bot^\sharp_\infty, \top^\sharp_\infty, \sqcup^\sharp_\infty, \sqcap^\sharp_\infty \rangle$ when $x = \infty$).

   a. $\forall S \in \mathbb{L}^\sharp_+ \,.\, S \fatsemi^\sharp \mathsf{init}^\sharp = \mathsf{init}^\sharp \fatsemi^\sharp S = S$;

   b. $\forall S \in \mathbb{L}^\sharp_+ \,.\, S \fatsemi^\sharp \bot^\sharp_+ = \bot^\sharp_+$ and $\forall S \in \mathbb{L}^\sharp_x \,.\, \bot^\sharp_+ \fatsemi^\sharp S = \bot^\sharp_+$ (same for $\mathbb{L}^\sharp_\infty$ when $\bot^\sharp_\infty$ exists);

   c. $\forall S \in \mathbb{L}^\sharp_\infty \,.\, \forall S' \in \mathbb{L}^\sharp_x \,.\, S \fatsemi^\sharp S' = S$;

   d. In its left, right, or both parameters, the sequential composition $\fatsemi^\sharp$ is either

      i. increasing for $\sqsubseteq^\sharp_+$ and/or $\sqsubseteq^\sharp_\infty$;

      ii. finite join preserving for $\sqcup^\sharp_+$ and/or $\sqcup^\sharp_\infty$;

      iii. in addition to 3.2.D.d.ii, is lower continuous for $\sqcap^\sharp_+$ and/or $\sqcap^\sharp_\infty$ and/or upper continuous for $\sqcup^\sharp_+$ and/or $\sqcup^\sharp_\infty$;

      iv. existing arbitrary $\sqcup^\sharp_+$-preserving and/or existing arbitrary $\sqcap^\sharp_\infty$-preserving.

Remark 3.3. In case $\mathbb{L}^\sharp_+ \cap \mathbb{L}^\sharp_\infty = \varnothing$, we can define $\mathbb{L}^\sharp \triangleq \mathbb{L}^\sharp_+ \cup \mathbb{L}^\sharp_\infty$ with $X^+ \triangleq X \cap \mathbb{L}^\sharp_+$, $X^\infty \triangleq X \cap \mathbb{L}^\sharp_\infty$, and $X \sqsubseteq^\sharp Y \triangleq X^+ \sqsubseteq^\sharp_+ Y^+ \wedge X^\infty \sqsubseteq^\sharp_\infty Y^\infty$ which corresponds to the bi-inductive definitions [24] mentioned in example 3.1. ■

Remark 3.4. Hypotheses 3.2.B, 3.2.D.d.i and 3.2.D.d.ii determine the precision of the semantic of basic commands, composition, choices, conditionals, and iteration in the algebraic semantics. These hypotheses as well as 3.2.D.d.iii and 3.2.D.d.iv determine whether fixpoint iterations should be infinite or transfinite (see proposition 2.4). ■

3.4 Definition of the Algebraic Semantics

The algebraic semantics of statements $\mathtt{S} \in \mathbb{S}$ is an abstract property of executions. The basic commands S are assignment, random assignment, `break` out of the immediately enclosing loop, and `skip`, with the following $\llbracket \mathtt{S} \rrbracket^\sharp_e$ and break $\llbracket \mathtt{S} \rrbracket^\sharp_b$ finite/ending/terminating semantics in $\mathbb{L}^\sharp_+$ as well as infinite/nonterminating $\llbracket \mathtt{S} \rrbracket^\sharp_\bot$ abstract semantics in $\mathbb{L}^\sharp_\infty$.

3.4.1 Basic Statements.

$$\begin{array}{llllllllll}
\llbracket \mathtt{x\ =\ A} \rrbracket^\sharp_e & \triangleq & \mathsf{assign}^\sharp\llbracket \mathtt{x}, \mathtt{A} \rrbracket & \llbracket \mathtt{x\ =\ A} \rrbracket^\sharp_b & \triangleq & \bot^\sharp_+ & \llbracket \mathtt{x\ =\ A} \rrbracket^\sharp_\bot & \triangleq & \bot^\sharp_\infty & \\
\llbracket \mathtt{x\ =\ [}a\mathtt{,}\ b\mathtt{]} \rrbracket^\sharp_e & \triangleq & \mathsf{rassign}^\sharp\llbracket \mathtt{x}, a, b \rrbracket & \llbracket \mathtt{x\ =\ [}a\mathtt{,}\ b\mathtt{]} \rrbracket^\sharp_b & \triangleq & \bot^\sharp_+ & \llbracket \mathtt{x\ =\ [}a\mathtt{,}\ b\mathtt{]} \rrbracket^\sharp_\bot & \triangleq & \bot^\sharp_\infty & \\
\llbracket \mathtt{break} \rrbracket^\sharp_e & \triangleq & \bot^\sharp_+ & \llbracket \mathtt{break} \rrbracket^\sharp_b & \triangleq & \mathsf{break}^\sharp & \llbracket \mathtt{break} \rrbracket^\sharp_\bot & \triangleq & \bot^\sharp_\infty & (3) \\
\llbracket \mathtt{skip} \rrbracket^\sharp_e & \triangleq & \mathsf{skip}^\sharp & \llbracket \mathtt{skip} \rrbracket^\sharp_b & \triangleq & \bot^\sharp_+ & \llbracket \mathtt{skip} \rrbracket^\sharp_\bot & \triangleq & \bot^\sharp_\infty & \\
\llbracket \mathtt{B} \rrbracket^\sharp_e & \triangleq & \mathsf{test}^\sharp\llbracket \mathtt{B} \rrbracket & \llbracket \mathtt{B} \rrbracket^\sharp_b & \triangleq & \bot^\sharp_+ & \llbracket \mathtt{B} \rrbracket^\sharp_\bot & \triangleq & \bot^\sharp_\infty &
\end{array}$$

For the assignment `x = A`, the abstract semantics $\mathsf{assign}^\sharp\llbracket \mathtt{x}, \mathtt{A} \rrbracket$ is specified by the abstract domain, and so, is well-defined by 3.2.B. $\llbracket \mathtt{x\ =\ A} \rrbracket^\sharp_b = \bot^\sharp_+$ because the assignment cannot break. $\llbracket \mathtt{x\ =\ A} \rrbracket^\sharp_\bot = \bot^\sharp_\infty$ since the assignment always terminates. The algebraic semantics of the other primitives is similar, except for the `break` statement. $\llbracket \mathtt{break} \rrbracket^\sharp_e = \bot^\sharp_+$ since the `break` cannot continue in sequence. The semantics $\llbracket \mathtt{break} \rrbracket^\sharp_b$ of the `break` is given by the abstract domain primitive $\mathsf{break}^\sharp$ which is finite and well-defined. $\llbracket \mathtt{break} \rrbracket^\sharp_\bot = \bot^\sharp_\infty$ since a `break` always terminates.

3.4.2 Structural Statements. For the sequential composition and the conditional where $\llbracket \mathtt{B;S} \rrbracket^\sharp_x \triangleq \mathsf{test}^\sharp\llbracket \mathtt{B} \rrbracket \fatsemi^\sharp \llbracket \mathtt{S} \rrbracket^\sharp_x$, $x \in \{e, b, \bot\}$, we define

$$\begin{array}{lllllll}
\llbracket \mathtt{S}_1\mathtt{;S}_2 \rrbracket^\sharp_e & \triangleq & \llbracket \mathtt{S}_1 \rrbracket^\sharp_e \fatsemi^\sharp \llbracket \mathtt{S}_2 \rrbracket^\sharp_e & \llbracket \mathtt{if\ (B)\ S}_1\ \mathtt{else\ S}_2 \rrbracket^\sharp_e & \triangleq & \llbracket \mathtt{B;S}_1 \rrbracket^\sharp_e \sqcup^\sharp_+ \llbracket \neg\mathtt{B;S}_2 \rrbracket^\sharp_e & \\
\llbracket \mathtt{S}_1\mathtt{;S}_2 \rrbracket^\sharp_b & \triangleq & \llbracket \mathtt{S}_1 \rrbracket^\sharp_b \sqcup^\sharp_+ (\llbracket \mathtt{S}_1 \rrbracket^\sharp_e \fatsemi^\sharp \llbracket \mathtt{S}_2 \rrbracket^\sharp_b) & \llbracket \mathtt{if\ (B)\ S}_1\ \mathtt{else\ S}_2 \rrbracket^\sharp_b & \triangleq & \llbracket \mathtt{B;S}_1 \rrbracket^\sharp_b \sqcup^\sharp_+ \llbracket \neg\mathtt{B;S}_2 \rrbracket^\sharp_b & (4) \\
\llbracket \mathtt{S}_1\mathtt{;S}_2 \rrbracket^\sharp_\bot & \triangleq & \llbracket \mathtt{S}_1 \rrbracket^\sharp_\bot \sqcup^\sharp_\infty (\llbracket \mathtt{S}_1 \rrbracket^\sharp_e \fatsemi^\sharp \llbracket \mathtt{S}_2 \rrbracket^\sharp_\bot) & \llbracket \mathtt{if\ (B)\ S}_1\ \mathtt{else\ S}_2 \rrbracket^\sharp_\bot & \triangleq & \llbracket \mathtt{B;S}_1 \rrbracket^\sharp_\bot \sqcup^\sharp_\infty \llbracket \neg\mathtt{B;S}_2 \rrbracket^\sharp_\bot &
\end{array}$$

The semantics of the composition and conditional are well-defined by 3.2.D for $\fatsemi^\sharp$ and 3.2.A and 3.2.C which ensure the existence of the finite and infinite joins.

$\mathtt{S}_1\,;\mathtt{S}_2$ terminates if $\mathtt{S}_1$ terminates and is followed by $\mathtt{S}_2$ that terminates. $\mathtt{S}_1\,;\mathtt{S}_2$ breaks (resp. nonterminates) if either $\mathtt{S}_1$ breaks (resp. nonterminates) or $\mathtt{S}_1$ terminates and is followed by $\mathtt{S}_2$ that breaks (resp. nonterminates).

For a given execution of the conditional `if (B)` $\mathtt{S}_1$ `else` $\mathtt{S}_2$ only one branch is taken, so the semantics of the other one will be empty by definition (3) of $[\![\mathtt{B}]\!]^\sharp_e$ that should return $\bot^\sharp_+$[2] and 3.2.D.b.

Example 3.5. Assume that $\mathtt{S}_1$ never terminates in that $[\![\mathtt{S}_1]\!]^\sharp_\bot = \top^\sharp_\infty$ (sometimes named "chaos" modelling all possible nonterminating behaviors). Then, by (4), $[\![\mathtt{S}_1\,;\mathtt{S}_2]\!]^\sharp_\bot \triangleq [\![\mathtt{S}_1]\!]^\sharp_\bot \sqcup^\sharp_\infty ([\![\mathtt{S}_1]\!]^\sharp_e \fatsemi^\sharp [\![\mathtt{S}_2]\!]^\sharp_\bot) = \top^\sharp_\infty \sqcup^\sharp_\infty ([\![\mathtt{S}_1]\!]^\sharp_e \fatsemi^\sharp [\![\mathtt{S}_2]\!]^\sharp_\bot) = \top^\sharp_\infty$ meaning that $\mathtt{S}_1\,;\mathtt{S}_2$ never terminates either in chaos.

For the conditional, assume $\mathtt{B}$ is always true and $\mathtt{S}_1$ never terminates in that $[\![\mathtt{S}_1]\!]^\sharp_\bot = \top^\sharp_\infty$. Then the false branch is never taken so that $[\![\neg\mathtt{B}\,;\mathtt{S}_2]\!]^\sharp_\bot = \bot^\sharp_\infty$. It follows, by (4), that $[\![\mathtt{if\ (B)\ S_1\ else\ S_2}]\!]^\sharp_\bot \triangleq [\![\mathtt{B}\,;\mathtt{S}_1]\!]^\sharp_\bot \sqcup^\sharp_\infty [\![\neg\mathtt{B}\,;\mathtt{S}_2]\!]^\sharp_\bot = \top^\sharp_\infty \sqcup^\sharp_\infty \bot^\sharp_\infty = \top^\sharp_\infty$ so that the conditional `if (B)` $\mathtt{S}_1$ `else` $\mathtt{S}_2$ never terminates. ■

3.4.3 *Iteration.*

For iteration `while (B) S`, we define the transformers

$$\begin{array}{llll}
\text{backward} & \overleftarrow{F}^\sharp_e & \triangleq & \boldsymbol{\lambda} X \in \mathbb{L}^\sharp_+ \bullet \mathsf{init}^\sharp \sqcup^\sharp_+ ([\![\mathtt{B}\,;\mathtt{S}]\!]^\sharp_e \fatsemi^\sharp X) \qquad (5)\\
\text{forward} & \vec{F}^\sharp_e & \triangleq & \boldsymbol{\lambda} X \in \mathbb{L}^\sharp_+ \bullet \mathsf{init}^\sharp \sqcup^\sharp_+ (X \fatsemi^\sharp [\![\mathtt{B}\,;\mathtt{S}]\!]^\sharp_e) \qquad (6)\\
\text{infinite} & F^\sharp_\bot & \triangleq & \boldsymbol{\lambda} X \in \mathbb{L}^\sharp_\infty \bullet [\![\mathtt{B}\,;\mathtt{S}]\!]^\sharp_e \fatsemi^\sharp X \qquad (7)
\end{array}$$

Lemma 3.6 (Finite fixpoints well-definedness). *If $\mathbb{D}^\sharp_+$ is a well-defined increasing chain complete join semilattice and $\fatsemi^\sharp$ left satisfies any one of the 3.2.D.d.i, 3.2.D.d.ii, 3.2.D.d.iii, or 3.2.D.d.iv properties for $\mathbb{D}^\sharp_+$ then $\overleftarrow{F}^\sharp_e$ satisfy the same property and its least fixpoint deso exist (and similarly for $\vec{F}^\sharp_e$ when $\fatsemi^\sharp$ right satisfies any one of the properties listed in 3.2.D.d).*

Proof of lemma 3.6. By definition (5), $\overleftarrow{F}^\sharp_e$ is the composition of constants $\mathsf{init}^\sharp$ and $[\![\mathtt{B}\,;\mathtt{S}]\!]^\sharp_e\fatsemi^\sharp$, the lub $\sqcup^\sharp_+$ in a join semilattice (which satisfies all properties of definition 2.2), and sequential composition $\fatsemi^\sharp$. Therefore, depending on which property 3.2.D.d.i, 3.2.D.d.ii, 3.2.D.d.iii, or 3.2.D.d.iv does satisfy, $\overleftarrow{F}^\sharp_e$ satisfies the same property. It follows by 3.2.A that the iterates of $\overleftarrow{F}^\sharp_e$ do exist, so that, by proposition 2.4, $\mathsf{lfp}^{\sqsubseteq^\sharp_+}\ \overleftarrow{F}^\sharp_e$ does exists. The same way $\mathsf{lfp}^{\sqsubseteq^\sharp_+}\ \vec{F}^\sharp_e$ does exist by (6). □

Let us show that $\mathsf{lfp}^{\sqsubseteq^\sharp_+}\ \overleftarrow{F}^\sharp_e = \mathsf{lfp}^{\sqsubseteq^\sharp_+}\ \vec{F}^\sharp_e$ inductively defines the set of finite executions reaching the entry of the iteration `while(B) S` after zero or more terminating body iterations. To see that, we define

the powers $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ of $X \in \mathbb{L}^\sharp_+$ are $X^0 \triangleq \mathsf{init}^\sharp$, $X^{\delta+1} \triangleq X \fatsemi^\sharp X^\delta$ for successor ordinals, and $X^\lambda \triangleq \bigsqcup^\sharp_{+\,\beta<\lambda} X^\beta$ for limit ordinals. (8)

We now characterize the executions of iterations in terms of the fixpoints of the execution transformers 5—6. We show that $\mathsf{lfp}^{\sqsubseteq^\sharp_+}\ \overleftarrow{F}^\sharp_e = \mathsf{lfp}^{\sqsubseteq^\sharp_+}\ \vec{F}^\sharp_e$ inductively characterize 0 or more finite iterations of the loop body for which the loop condition holds and the loop body terminates.

Lemma 3.7 (Commutativity). *If $\mathbb{D}^\sharp_+$ is a well-defined complete lattice (resp. increasing chain-complete poset) with right existing $\sqcup^\sharp_+$-preserving (resp. right upper continuous) composition $\fatsemi^\sharp$ and $X \in \mathbb{L}^\sharp_+$ then $\forall \delta \in \mathbb{O}\ .\ X \fatsemi^\sharp X^\delta = X^\delta \fatsemi^\sharp X$ (resp. if $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ is an increasing chain).*

Proof of lemma 3.7. The proof is by transfinite induction on δ.

[2] unless the semantics of Boolean expressions is to be very exotic.

- For $\delta = 0$, we have $X \fatsemi^\sharp X^0 = X \fatsemi^\sharp \mathsf{init}^\sharp = \mathsf{init}^\sharp \fatsemi^\sharp X = X^0 \fatsemi^\sharp X$ by definition 3.2.D.a and definition (8) of the powers.
- If $X \fatsemi^\sharp X^\delta = X^\delta \fatsemi^\sharp X$ by induction hypothesis, then $X \fatsemi^\sharp X^{\delta+1} = X \fatsemi^\sharp (X \fatsemi^\sharp X^\delta) = X \fatsemi^\sharp (X^\delta \fatsemi^\sharp X)$ $= (X \fatsemi^\sharp X^\delta) \fatsemi^\sharp X = X^{\delta+1} \fatsemi^\sharp X$ by def. (8) of the iterates, induction hypothesis, associativity 3.2.D, and (8).
- If λ is a limit ordinal and $\forall \beta < \lambda \,.\, X \fatsemi^\sharp X^\beta = X^\beta \fatsemi^\sharp X$ by induction hypothesis, then $X \fatsemi^\sharp X^\lambda =$ $X \fatsemi^\sharp (\bigsqcup^\sharp_{+\,\beta<\lambda} X^\beta) = \bigsqcup^\sharp_{+\,\beta<\lambda}(X \fatsemi^\sharp X^\beta) = \bigsqcup^\sharp_{+\,\beta<\lambda} X^{\beta+1}$ by (8), right existing $\sqcup^\sharp_+$-preserving $\fatsemi^\sharp$ 3.2.D.d.iv (resp. right upper continuity when $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ is an increasing chain 3.2.D.d.iii). □

Lemma 3.8 (Finite body iterations). *If $\mathbb{D}^\sharp_+$ is a well-defined increasing chain-complete join semilattice with right upper continuous composition $\fatsemi^\sharp$ then* $\mathsf{lfp}^{\sqsubseteq^\sharp_+}\ \overleftarrow{F}^\sharp_e = \bigsqcup^\sharp_{+\,\delta\in\mathbb{O}} (\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\delta$.

Proof of lemma 3.8. By lemma 3.6, if $\mathbb{D}^\sharp_+$ is a well-defined incraesing chain-complete join semilattice with right upper continuous composition then $\overleftarrow{F}^\sharp_e$ in (6) is upper continuous hence increasing since continuous functions are increasing and the composition of increasing functions is increasing. It follows, by proposition 2.4, that the least fixpoint $\mathsf{lfp}^{\sqsubseteq^\sharp_+}\ \overleftarrow{F}^\sharp_e$ exists and is the limit of the increasing iterates $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ of $\overleftarrow{F}^\sharp_e$ from the infimum $\bot^\sharp_+$ (which exists in a chain-complete lattice).

Let us prove that $X^\delta = \bigsqcup^\sharp_{+\,\beta<\delta}(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\beta$ by transfinite induction on δ.

- For $\delta = 0$, we have $X^0 = \bot^\sharp_+ = \bigsqcup^\sharp_+ \varnothing = \bigsqcup^\sharp_{+\,\beta<0}(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\beta$ by definition of the iterates and the infimum.
- Assume by induction hypothesis that $X^\delta = \bigsqcup^\sharp_{+\,\beta<\delta}(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\beta$. Then $X^{\delta+1} = \overleftarrow{F}^\sharp_e(X^\delta) = \mathsf{init}^\sharp \sqcup^\sharp_+$ $(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e \fatsemi^\sharp X^\delta) = \mathsf{init}^\sharp \sqcup^\sharp_+ (\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e \fatsemi^\sharp (\bigsqcup^\sharp_{+\,\beta<\delta}(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\beta)) = \mathsf{init}^\sharp \sqcup^\sharp_+ \bigsqcup^\sharp_{+\,\beta<\delta}((\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e \fatsemi^\sharp \llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\beta) =$ $(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^0 \sqcup^\sharp_+ \bigsqcup^\sharp_{+\,\beta<\delta}(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^{\beta+1}) = \bigsqcup^\sharp_{+\,\beta<\delta+1}(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\beta$ by definition of iterates, definition (5) of $\overleftarrow{F}^\sharp_e$, induction hypothesis, definition 3.2.D.d, definition of the powers, grouping terms in the join.
- Assume that λ is a limit ordinal and that, by induction hypothesis, $\forall \delta < \lambda \,.\, X^\delta = \bigsqcup^\sharp_{+\,\beta<\delta}(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\beta$. Then we have $X^\lambda = \bigsqcup^\sharp_{+\,\delta<\lambda} X^\delta = \bigsqcup^\sharp_{+\,\delta<\lambda} \bigsqcup^\sharp_{+\,\beta<\delta}(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\beta = \bigsqcup^\sharp_{+\,\beta<\lambda}(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\beta$ by definition of the iterates, induction hypothesis, and definition of the join $\sqcup^\sharp_+$ (which exists since the iterates are increasing.

We conclude by proposition 2.4 that $\mathsf{lfp}^{\sqsubseteq^\sharp_+}\ \overleftarrow{F}^\sharp_e = \bigsqcup^\sharp_{+\,\delta\in\mathbb{O}} (\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\delta$. □

Lemma 3.9 (Forward versus backward). *If $\mathbb{D}^\sharp$ is a well-defined increasing chain-complete join semilattice with right upper continuous sequential composition $\fatsemi^\sharp$ then* $\mathsf{lfp}^{\sqsubseteq^\sharp_+}\ \overleftarrow{F}^\sharp_e = \mathsf{lfp}^{\sqsubseteq^\sharp_+}\ \vec{F}^\sharp_e$.

Proof of lemma 3.9. The proof is similar to that of lemma 3.8. Let $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ be the iterates of $\vec{F}^\sharp_e$. For the basis, $X^0 = \bot^\sharp_+$. For the successor induction step, $X^{\delta+1} = \vec{F}^\sharp_e(X^\delta) = \mathsf{init}^\sharp \sqcup^\sharp_+$ $(X^\delta \fatsemi^\sharp \llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e) = \mathsf{init}^\sharp \sqcup^\sharp_+ ((\bigsqcup^\sharp_{+\,\beta<\delta}(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\beta) \fatsemi^\sharp \llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e) = \mathsf{init}^\sharp \sqcup^\sharp_+ \bigsqcup^\sharp_{+\,\beta<\delta}((\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\beta \fatsemi^\sharp \llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e) =$ $\mathsf{init}^\sharp \sqcup^\sharp_+ \bigsqcup^\sharp_{+\,\beta<\delta}((\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e \fatsemi^\sharp \llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\beta) = (\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^0 \sqcup^\sharp_+ \bigsqcup^\sharp_{+\,\beta<\delta}(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^{\beta+1}) \bigsqcup^\sharp_{+\,\beta<\delta+1}(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\beta$ by definition of iterates, definition (6) of $\vec{F}^\sharp_e$, induction hypothesis, definition 3.2.D.d, lemma 3.7, definition of the powers, grouping terms in the join. For the limit induction step, $X^\lambda = \bigsqcup^\sharp_{+\,\delta<\lambda} X^\delta =$ $\bigsqcup^\sharp_{+\,\delta<\lambda} \bigsqcup^\sharp_{+\,\beta<\delta}(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\beta = \bigsqcup^\sharp_{+\,\beta<\lambda}(\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\beta$ by definition of the iterates, induction hypothesis, and definition of the join. We conclude that $\mathsf{lfp}^{\sqsubseteq^\sharp_+}\ \overleftarrow{F}^\sharp_e = \bigsqcup^\sharp_{+\,\delta\in\mathbb{O}} (\llbracket \mathtt{B}\,;\mathtt{S}\rrbracket^\sharp_e)^\delta = \mathsf{lfp}^{\sqsubseteq^\sharp_+}\ \overleftarrow{F}^\sharp_e$ by proposition 2.4 and lemma 3.8. □

Example 3.10. Assume that the test `B` of the iteration `while (B) S` is always false, that is $\mathsf{test}^\sharp \llbracket \mathtt{B} \rrbracket =$ $\bot^\sharp_\infty$. Then, by (5), (6), (3.2.D.b), and def. lub, $\overleftarrow{F}^\sharp_e = \vec{F}^\sharp_e = \boldsymbol{\lambda} X \in \mathbb{L}^\sharp_+ \bullet \mathsf{init}^\sharp$. It follows that $\mathsf{lfp}^{\sqsubseteq^\sharp_+}\ \overleftarrow{F}^\sharp_e =$

$\mathsf{lfp}^{\sqsubseteq^\sharp_+}\,\vec{F}^\sharp_e = \mathsf{init}^\sharp$ meaning that the loop is never entered. The semantics of the loop after 0 or more iterations is therefore that after 0 iterations. ■

Lemma 3.11 (Infinite fixpoint well-definedness). *If $\mathbb{D}^\sharp_\infty$ is a well-defined decreasing chain complete poset and $\fatsemi^\sharp$ right satisfies any one of the 3.2.D.d.i, 3.2.D.d.ii, 3.2.D.d.iii, or 3.2.D.d.iv properties for $\mathbb{D}^\sharp_\infty$ then $F^\sharp_\bot$ satisfies the same property and* $\mathsf{gfp}^{\sqsubseteq^\sharp_\infty}\,F^\sharp_\bot$ *does exist.*

Proof of lemma 3.11. If $\fatsemi^\sharp$ satisfies any one of the 3.2.D.d.i, 3.2.D.d.ii, 3.2.D.d.iii, or 3.2.D.d.iv properties for $\mathbb{D}^\sharp_\infty$ then, by (7), $F^\sharp_\bot = \boldsymbol{\lambda} X \in \mathbb{L}^\sharp_\infty \bullet \llbracket \mathtt{B;S} \rrbracket^\sharp_e \fatsemi^\sharp X$ satisfies the same property since $\llbracket \mathtt{B;S} \rrbracket^\sharp_e$ is constant. By the dual of proposition 2.4, $\mathsf{gfp}^{\sqsubseteq^\sharp_\infty}\,F^\sharp_\bot$ exists in a decreasing chain complete poset. □

We now show that $\mathsf{gfp}^{\sqsubseteq^\sharp_\infty}\,F^\sharp_\bot$ coinductively characterizes the infinite executions of the iteration `while (B) S` after infinitely many terminating iterations of the body `S` with condition `B` always true.

Lemma 3.12 (Infinite body iterations). *If $\mathbb{D}^\sharp$ is a well-defined decreasing chain-complete poset and $\fatsemi^\sharp$ is right increasing for $\sqsubseteq^\sharp_\infty$ in 3.2.D.d.i then* $\mathsf{gfp}^{\sqsubseteq^\sharp_\infty}\,F^\sharp_\bot = \bigsqcap^\sharp_{\infty\,\delta\in\mathbb{O}}((\llbracket \mathtt{B;S} \rrbracket^\sharp_e)^\delta \fatsemi^\sharp \top^\sharp_\infty)$.

Proof of lemma 3.12. $\fatsemi^\sharp$ is increasing for $\sqsubseteq^\sharp_\infty$ so that, by lemma 3.11, $F^\sharp_\bot$ is is increasing for $\sqsubseteq^\sharp_\infty$. Since $\mathbb{D}^\sharp$ is a decreasing chain-complete poset, the iterates $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ of $F^\sharp_\bot$ from the supremum $\top^\sharp_\infty$ are well-defined, so that, by the dual of proposition 2.4, $\mathsf{gfp}^{\sqsubseteq^\sharp_\infty}\,F^\sharp_\bot$ exists and is the limit of these iterates. These iterates are $X^0 = \top^\sharp_\infty$, $X^1 = F^\sharp_\bot(X^0) = \llbracket \mathtt{B;S} \rrbracket^\sharp_e \fatsemi^\sharp \top^\sharp_\infty$. Assume that $X^\delta = (\llbracket \mathtt{B;S} \rrbracket^\sharp_e)^\delta \fatsemi^\sharp \top^\sharp_\infty$ by induction hypothesis so that $X^{\delta+1} = \llbracket \mathtt{B;S} \rrbracket^\sharp_e \fatsemi^\sharp X^\delta = \llbracket \mathtt{B;S} \rrbracket^\sharp_e \fatsemi^\sharp (\llbracket \mathtt{B;S} \rrbracket^\sharp_e)^\delta \fatsemi^\sharp \top^\sharp_\infty = (\llbracket \mathtt{B;S} \rrbracket^\sharp_e)^{(\delta+1)-1} \fatsemi^\sharp \top^\sharp_\infty$ by associativity, def. (8) of the powers, and def. of the iterates in prop. 2.4. $X^{\delta+1}$ is of the form of the recurrence hypothesis proving that it holds for all iterates. Passing to the limit, we have $\mathsf{gfp}^{\subseteq}\,F^\sharp_\bot = \bigsqcap^\sharp_{\infty\,\delta\in\mathbb{O}} X^\delta = \bigsqcap^\sharp_{\infty\,\delta\in\mathbb{O}}((\llbracket \mathtt{B;S} \rrbracket^\sharp_e)^\delta \fatsemi^\sharp \top^\sharp_\infty)$. □

The abstract semantics of iteration is defined as

$$\llbracket \mathtt{while\ (B)\ S} \rrbracket^\sharp_e \triangleq (\mathsf{lfp}^{\sqsubseteq^\sharp_+}\,\overleftarrow{F}^\sharp_e) \fatsemi^\sharp (\llbracket \neg\mathtt{B} \rrbracket^\sharp_e \sqcup^\sharp_e \llbracket \mathtt{B;S} \rrbracket^\sharp_b) \qquad \llbracket \mathtt{while\ (B)\ S} \rrbracket^\sharp_b \triangleq \bot^\sharp_+ \tag{9}$$

$$\llbracket \mathtt{while\ (B)\ S} \rrbracket^\sharp_{bi} \triangleq (\mathsf{lfp}^{\sqsubseteq^\sharp_+}\,\overleftarrow{F}^\sharp_e) \fatsemi^\sharp \llbracket \mathtt{B;S} \rrbracket^\sharp_\bot \qquad \llbracket \mathtt{while\ (B)\ S} \rrbracket^\sharp_{li} \triangleq \mathsf{gfp}^{\sqsubseteq^\sharp_\infty}\,F^\sharp_\bot \tag{10}$$

$$\llbracket \mathtt{while\ (B)\ S} \rrbracket^\sharp_\bot \triangleq \llbracket \mathtt{while\ (B)\ S} \rrbracket^\sharp_{bi} \sqcup^\sharp_\infty \llbracket \mathtt{while\ (B)\ S} \rrbracket^\sharp_{li} \tag{11}$$

The least fixpoint $\mathsf{lfp}^{\sqsubseteq^\sharp_+}\,\overleftarrow{F}^\sharp_e$ defines executions reaching the loop entry point after zero or finitely many iterations. Then (9) defines the finite executions of the loop when, after 0 or more iterations, the iteration condition `B` is false, or a break is executed in the body which exists the loop. By (9) the `break` is from the closest enclosing loop (which existence must be checked syntactically). The loop nontermination in (11) can happen either because, after zero or finitely many iterations, the next execution of the iteration body never terminates (10), or results in (10) from infinitely many finite iterations, as defined by the greatest fixpoint $\mathsf{gfp}^{\sqsubseteq^\sharp_\infty}\,F^\sharp_\bot$, and obtained as the limit of iterations of $F^\sharp_\bot$ from $\top^\sharp_\infty$. These fixpoints in (9) and (10) do exist by lemmas 3.6 and 3.11.

Theorem 3.13. *If $\mathbb{D}^\sharp$ is well-defined then for all* $\mathtt{S} \in \mathbb{S}$, $\llbracket \mathtt{S} \rrbracket^\sharp_e$, $\llbracket \mathtt{S} \rrbracket^\sharp_b$, *and* $\llbracket \mathtt{S} \rrbracket^\sharp_\bot$ *are well-defined.*

Proof of theorem 3.13. The proof is by structural induction, observing that all operators hence their compositions are well-defined, including $\sqcup^\sharp_+$, $\sqcup^\sharp_\infty$, and $\fatsemi^\sharp$. Lemmas 3.6 and 3.11 show that the transformers $\overleftarrow{F}^\sharp_e$, $\vec{F}^\sharp_e$, $F^\sharp_\bot$ are increasingso that their fixpoints do exist. □

3.5 Algebraic Abstract Semantic Domain and Abstract Semantics

The components of the abstract semantics can be recorded in a triple with named components, ordered componentwise by $\sqsubseteq^\sharp$, as follows

$$\begin{array}{rcl}\mathbb{L}^\sharp & \triangleq & (e : \mathbb{L}^\sharp_+ \times \bot : \mathbb{L}^\sharp_\infty \times br : \mathbb{L}^\sharp_+) \\ [\![\mathsf{S}]\!]^\sharp & \triangleq & \langle e : [\![\mathsf{S}]\!]^\sharp_e,\ \bot : [\![\mathsf{S}]\!]^\sharp_\bot,\ br : [\![\mathsf{S}]\!]^\sharp_b\rangle\end{array} \tag{12}$$

If $T = \langle e : F,\ \bot : I,\ br : B\rangle \in \mathbb{L}^\sharp$, then we select the individual components of the Cartesian product T using the field selectors e, br, and $\bot$, as follows

$$T_+ = F, \quad T_\infty = I, \quad \text{and} \quad T_{br} = B. \tag{13}$$

By convention,

The shorthand F denotes $\langle e : F,\ \bot : \bot^\sharp_\infty,\ br : \bot^\sharp_+\rangle$ and similarly for other unique nonempty components. (14)

The abstract semantics $[\![\mathsf{S}]\!]^\sharp \in \mathbb{L}^\sharp$ records three components $[\![\mathsf{S}]\!]^\sharp_e$, $[\![\mathsf{S}]\!]^\sharp_\bot$, and $[\![\mathsf{S}]\!]^\sharp_b$ of the definition of the algebraic semantics of statements S in sect. 3.4.

Lemma 3.14. *If $\mathbb{D}^\sharp$ is a well-defined chain-complete join semilattice (respectively complete lattice) with sequential composition $\fatsemi^\sharp$ satisfying any one of the hypotheses 3.2.D.d then $\langle \mathbb{L}^\sharp,\ \sqsubseteq^\sharp\rangle$ has the same structure, componentwise.*

Proof of lemma 3.14. Lemma 3.14 follows from the fact that the Cartesian product of complete lattices (respectively, a chain-complete join semilattice) is a complete lattice [31, p. 33] (resp., is a chain-complete join semilattice [31, p. 55]). □

All semantic definitions are extended componentwise. For $\fatsemi^\sharp \ \in\ \mathbb{L}^\sharp \times \mathbb{L}^\sharp \to \mathbb{L}^\sharp$, we define

$$\langle ok{:}\langle e{:}F_1, \bot{:}I_1\rangle, b{:}B_1\rangle \fatsemi^\sharp \langle ok{:}\langle e{:}F_2, \bot{:}I_2\rangle, b{:}B_2\rangle \triangleq \langle ok{:}\langle e{:}F_1 \fatsemi^\sharp F_2, \bot{:}I_1 \sqcup^\sharp_\infty (F_1 \fatsemi^\sharp I_2)\rangle, b{:}B_1 \sqcup^\sharp_+ (F_1 \fatsemi^\sharp B_2)\rangle$$

so that, by (4), $[\![\mathsf{S}_1\,;\mathsf{S}_2]\!]^\sharp = [\![\mathsf{S}_1]\!]^\sharp \fatsemi^\sharp [\![\mathsf{S}_2]\!]^\sharp$. (15)

Remark 3.15. The semantic domain of our algebraic semantics is much more refined than traditional ones such as [57] where, the computational and logical ordering are subset inclusion and, following the denotational semantics [80] approach, "Nontermination has to be represented by a fictitious "state at infinity" that can be "reached" only by a non-terminating program. Also, if the fictitious state is in the image of a state, then that image is universal." [56]. This can be achieved by instantiation e.g. to a trace semantics followed by an abstraction (mapping infinite traces to the "fictitious "state at infinity"").

Moreover, we do not specify the algebraic semantics by "laws" (or axioms) but in structural fixpoint form, which is known to be equivalent, according to the generalization [25] of Peter Aczel correspondance [2] between deductive/proof systems and fixpoint definitions. The "laws" for basic statements are the definitions (3). The other "laws" for structured statements and iteration are theorems following from the definition 3.2 of an abstract domain and fixpoint induction principles [19] following from propositions 2.3 and 2.4. ■

All semantics in [4, 18, 41] can be instantiated to the algebraic abstract semantics of sect. 3.5. There are obviously others, such as symbolic execution [61] (extended to infinite behaviors). For semantics defined by transformations such as compilation, the transformation is an instance of the algebraic abstract semantics, but the semantics of the transformed program is not, because of a different syntax, although it can certainly be also defined in an algebraic style.

The original definition of hyperproperties [14] was relative to a trace (or path) semantics $[\![\mathsf{S}]\!]^\pi$ which, as shown in the appendix , is an instance of the algebraic abstract semantics $[\![\mathsf{S}]\!]^\sharp$ where the domain $\mathbb{D}^\sharp_+$ is the complete lattice $\mathbb{D}^\pi_+$ of sets of finite traces and the domain $\mathbb{D}^\sharp_\infty$ is the complete lattice $\mathbb{D}^\pi_\infty$ of sets of infinite traces where traces account for the successive values taken by variables during execution, as recorded in states. All operators preserve arbitrary joins. For lower continuity, see counterexample 4.1 for infinite traces and the following lower continuity proof for finite traces.

4 Trace Semantics

4.1 The Trace Semantics Domain

4.1.1 States. States $\sigma \in \Sigma \triangleq \mathbb{X} \to \mathbb{V}$ (also called environments) map variables $\mathsf{x} \in \mathbb{X}$ to their values $\sigma(\mathsf{x})$ in $\mathbb{V}$ including integers, $\mathbb{Z} \subseteq \mathbb{V}$.

4.1.2 Finite Traces. We let $\pi = \pi_0\pi_1 \ldots \pi_{n-1} \in \Sigma^n \triangleq [0, n[\; \to \Sigma$ be the nonempty finite traces of length $|\pi| = n$, $n \geqslant 1$ over states $\pi_i \in \Sigma$, $i \in [0, n[$, $\Sigma^+ \triangleq \bigcup_{n \geqslant 1} \Sigma^n$. The empty trace ϵ is in $\Sigma^0 = \{\epsilon\}$. $\Sigma^* \triangleq \Sigma^+ \cup \Sigma^0$ is the set of possibly empty traces. A set of finite traces defines a property of finite executions in extension.

$$\langle \mathbb{L}^\pi_+, \sqsubseteq^\pi_+, \bot^\pi_+, \top^\pi_+, \sqcup^\pi_+, \sqcap^\pi_+ \rangle \quad \triangleq \quad \langle \wp(\Sigma^+), \subseteq, \varnothing, \Sigma^+, \cup, \cap \rangle \tag{16}$$

4.1.3 Infinite Traces. The infinite traces $\pi = \pi_0\pi_1 \ldots \pi_n \ldots \in \Sigma^\infty \triangleq [0, \infty[\; \to \Sigma$ have length $|\pi| = \infty$ over states $\pi_i \in \Sigma$, $i \in [0, \infty[$. We let $\Sigma^{+\infty} \triangleq \Sigma^+ \cup \Sigma^\infty$ and $\Sigma^{*\infty} \triangleq \Sigma^* \cup \Sigma^\infty$.

A trace $\sigma\pi \in \Sigma^{+\infty}$ has first state $\sigma \in \Sigma$. A trace of the form $\pi\sigma$ is necessarily finite with last state σ and $\pi \in \Sigma^*$. If $0 \leqslant i \leqslant j < n$ and $\pi \in \Sigma^n$ then $\pi_{[i,j]} \triangleq \pi_i\pi_{i+1} \ldots \pi_j$ is the subtrace of π stating at i and ending at j. A set of infinite traces defines a property of nonterminating executions in extension.

$$\langle \mathbb{L}^\pi_\infty, \sqsubseteq^\pi_\infty, \bot^\pi_\infty, \top^\pi_\infty, \sqcap^\sharp_\infty, \sqcup^\sharp_\infty \rangle \quad \triangleq \quad \langle \wp(\Sigma^\infty), \subseteq, \varnothing, \Sigma^\infty, \cap, \cup \rangle \tag{17}$$

Notice that $\mathsf{gfp}^{\sqsubseteq^\pi_\infty} F^\pi_\bot = \mathsf{gfp}^{\subseteq} F^\pi_\bot$ so that infinite execution traces are defined co-inductively.

4.1.4 Traces Operators.

$$\begin{array}{rcl@{\qquad}rcl}
\mathsf{init}^\pi & \triangleq & \Sigma^1 & \mathsf{test}^\pi[\![\mathsf{B}]\!] & \triangleq & \{\sigma \mid \sigma \in \mathcal{B}[\![\mathsf{B}]\!]\} \\
\mathsf{assign}^\pi[\![\mathsf{x}, \mathsf{A}]\!] & \triangleq & \{\sigma\sigma[\mathsf{x} \leftarrow \mathcal{A}[\![\mathsf{A}]\!]\sigma] \in \Sigma^2 \mid \sigma \in \Sigma\} & \mathsf{break}^\pi & \triangleq & \{\sigma\,\mathsf{break\text{-}to}(\sigma) \mid \sigma \in \Sigma\} \\
\mathsf{rassign}^\pi[\![\mathsf{x}, a, b]\!] & \triangleq & \{\sigma\sigma[\mathsf{x} \leftarrow i] \in \Sigma^2 \mid a - 1 < i < b + 1\} & \mathsf{skip}^\pi & \triangleq & \{\sigma\sigma \mid \sigma \in \Sigma\}
\end{array} \tag{18}$$

See [20, page 43] for a definition of break-to (exiting the enclosing loop with variables unchanged). We deliberately leave unspecified the syntax and semantics of arithmetic expressions $\mathcal{A}[\![\mathsf{A}]\!] \in \Sigma \to \mathbb{V}$ and Boolean expressions $\mathcal{B}[\![\mathsf{B}]\!] \in \wp(\Sigma) \simeq \Sigma \to \{\mathsf{true}, \mathsf{false}\}$. The only assumption on expressions is the absence of side effects.

We let $\fatsemi^\pi$ be the concatenation of sets of traces $T \in \wp(\Sigma^{*\infty})$ and $T' \in \wp(\Sigma^{*\infty})$ such that

$$T \fatsemi^\pi T' \quad \triangleq \quad \{\pi' \in T' \mid \epsilon \in T\} \cup \{\pi \in T \mid \epsilon \in T'\} \cup (T \cap \Sigma^\infty) \cup \{\pi\sigma\pi' \mid \pi\sigma \in T \wedge \sigma\pi' \in T'\}$$

The powers of a set $T \in \wp(\Sigma^{*\infty})$ of traces are $\{\epsilon\}^n = \{\epsilon\}$ and otherwise $T^0 = \Sigma^1$and $T^{n+1} = T^n \fatsemi T = T \fatsemi T^n$ for all $n \geqslant 0$. We denote $T^\infty \in \wp(\Sigma^\infty)$ the set of infinite traces obtained by concatenation of traces of T. Notice that $\fatsemi$ is right increasing but not right lower continuous on infinite traces $\wp(\Sigma^\infty)$.

Counter example 4.1. Let $r = \{\sigma_1, \sigma_1\sigma_2, \ldots, \sigma_1 \ldots \sigma_n, \ldots\}$ be the prefix closure of the infinite trace $\sigma_1\sigma_2\sigma_3 \ldots$. Define $X_i = \{\sigma_i\sigma_{i+1}\sigma_{i+2} \ldots, \sigma_{i+1}\sigma_{i+2} \ldots, \sigma_{i+2} \ldots, \ldots\}$ be the suffix closure of the infinite trace $\sigma_i\sigma_{i+1}\sigma_{i+2}\sigma_{i+3} \ldots$ so that $\langle X_i,\ i \in \mathbb{N}\rangle$ is a decreasing chain. Then $r \fatsemi^\pi \bigcap_{i \in \mathbb{N}} X_i = r \fatsemi^\pi \varnothing = \varnothing$, while $\bigcap_{i \in \mathbb{N}}(r \fatsemi^\pi X_i) = \bigcap_{i \in \mathbb{N}}\{\sigma_1\sigma_2\sigma_3 \ldots\} = \{\sigma_1\sigma_2\sigma_3 \ldots\}$. ■

However, $\fatsemi$ is right lower continuous on finite traces $\wp(\Sigma^+)$.

Proof of right lower continuity of $\fatsemi$ for finite traces. Let $\langle X^i \in \wp(\Sigma^+),\ i \in \mathbb{N}\rangle$ be a $\subseteq$-decreasing chain of sets of finite traces. We must prove that $r \fatsemi^\pi (\bigcap_{i \in \mathbb{N}} X^i) = \bigcap_{i \in \mathbb{N}}(r \fatsemi^\pi X^i)$. The inclusion $\subseteq$ is trivial. Conversely, let $\pi \in \bigcap_{i \in \mathbb{N}}(r \fatsemi^\pi X^i) \subseteq \wp(\Sigma^+)$ then there exists $\bar{\pi}_0 \in X^0$, $\bar{\pi}_1 \in X^1$, ..., $\bar{\pi}_i \in X^i$, ... and π_0, π_1, ..., π_i, ... $\in r$ such that $\bar{\pi}_0 \leqslant_s \bar{\pi}_1 \leqslant_s \ldots \leqslant_s \bar{\pi}_i \leqslant_s \ldots$ and $\pi = \pi_0 {}^\frown \bar{\pi}_0 = \pi_1 {}^\frown \bar{\pi}_1 = \ldots = \pi_i {}^\frown \bar{\pi}_i = \ldots$ where $\leqslant_s$ is the suffix ordering on traces and ${}^\frown$ is trace concatenation. The length of the $\langle \bar{\pi}_i,\ i \in \mathbb{N}\rangle$ is ultimately stationary at some $k \in \mathbb{N}$. This means that there exists $\bar{\pi}_k$ such that $\forall i \in \mathbb{N} \mathrel{.} \bar{\pi}_k \in X^i$. As a result, $\pi = \pi_k \frown \bar{\pi}_k \in r \fatsemi^{\pi} \ (\bigcap_{i\in\mathbb{N}} X_i)$. □

4.2 Structural Trace Semantics

$\mathsf{lfp}^{\sqsubseteq^{\pi}_{+}} F^{\pi}_{e} = \mathsf{lfp}^{\subseteq} F^{\pi}_{e}$ is the set of finite traces reaching the entry of the iteration `while (B) S` after zero or more terminating body iterations .

Lemma 4.2. $\mathsf{lfp}^{\subseteq} F^{\pi}_{e} = \bigcup_{n\in\mathbb{N}}(\llbracket \mathsf{B} \fatsemi^{\pi} \mathsf{S}\rrbracket^{\pi}_{e})^{n}$.

Proof of lemma 4.2. An instance of lemma 3.8 for $\mathbb{D}^{\pi}_{+}$. □

$\mathsf{gfp}^{\sqsubseteq^{\pi}_{\infty}} F^{\pi}_{\bot} = \mathsf{gfp}^{\subseteq} F^{\pi}_{\bot}$ is the set of infinite traces of the iteration `while (B) S` after infinitely many terminating body iterations .

Lemma 4.3. $\mathsf{gfp}^{\subseteq} F^{\pi}_{\bot} = (\llbracket \mathsf{B} \fatsemi^{\pi} \mathsf{S}\rrbracket^{\pi}_{e})^{\infty}$.

Proof of lemma 4.3. An instance of lemma 3.12 for $\mathbb{D}^{\pi}_{\infty}$. Moreover, $\bigsqcap^{\sharp}_{\infty\, n\in\mathbb{N}}((\llbracket \mathsf{B}\,;\mathsf{S}\rrbracket^{\sharp}_{e})^{n} \fatsemi^{\sharp} \bot^{\sharp}_{\infty})$ becomes $\bigcap_{n\in\mathbb{N}}((\llbracket \mathsf{B}\,;\mathsf{S}\rrbracket^{\pi}_{e})^{n} \fatsemi^{\pi} \Sigma^{\infty}) = (\llbracket \mathsf{B} \fatsemi^{\pi} \mathsf{S}\rrbracket^{\pi}_{e})^{\infty}$ since all traces in $(\llbracket \mathsf{B} \fatsemi^{\pi} \mathsf{S}\rrbracket^{\pi}_{e})^{\infty}$ belong to $(\llbracket \mathsf{B} \fatsemi^{\pi} \mathsf{S}\rrbracket^{\pi}_{e})^{n} \fatsemi^{\pi} \Sigma^{\infty}$, $n \geqslant 0$ while any trace not of that form must be $\pi\pi'\pi''$ with $\pi \in (\llbracket \mathsf{B} \fatsemi^{\pi} \mathsf{S}\rrbracket^{\pi}_{e})^{n}$, $\pi' \notin \llbracket \mathsf{B} \fatsemi^{\pi} \mathsf{S}\rrbracket^{\pi}_{e}$, and $\pi'' \in \Sigma^{\infty}$ for some $n \in \mathbb{N}$ and so does not belong to X^{n+2} hence not to the intersection. □

Example 4.4. Consider $\mathsf{S} \triangleq$ `while (x!=2) if (x==1) then break else x=x+2`. It's trace semantics is

$$\begin{array}{lcl}
\llbracket \mathsf{S}\rrbracket^{\pi}_{e} & = & \{\mathsf{x}:-2k;\mathsf{x}:-2k+2;\ldots;\mathsf{x}:0;\mathsf{x}:2 \mid k \geqslant -1\} \cup \{\mathsf{x}:-2k+1;\mathsf{x}:-2k+3;\ldots;\mathsf{x}:1 \mid k \geqslant 0\}\\
\llbracket \mathsf{S}\rrbracket^{\pi}_{b} & = & \varnothing \\
\llbracket \mathsf{S}\rrbracket^{\pi}_{\bot} & = & \{\mathsf{x}:n;\ldots;\mathsf{x}:n+2k;\ldots \mid n > 2\}\ .
\end{array} \tag{19}$$
■

Proof of (19). We have $\llbracket$`(x!=2)` $\fatsemi^{\pi}$ `if (x==1) then break else x=x+2`$\rrbracket = \langle ok : \{\mathsf{x}:n;\mathsf{x}:n+2 \mid n \notin \{1,2\}\},\ br : \{\mathsf{x}:1\}\rangle$ so that $F^{\pi}_{e}(X) = \{\mathsf{x}:n \mid n \in \mathbb{Z}\} \cup \{\mathsf{x}:n;\mathsf{x}:n+2;\pi \mid n \notin \{1,2\} \wedge \mathsf{x}:n+2;\pi \in X^{+}\}$ for the finite traces reaching the loop head.

The iterates are ${F^{\pi}_{e}}^{0} = \varnothing$, ${F^{\pi}_{e}}^{1} = \{\mathsf{x}:n \mid n \in \mathbb{Z}\}$, ${F^{\pi}_{e}}^{2} = \{\mathsf{x}:n \mid n \in \mathbb{Z}\} \cup \{\mathsf{x}:n;\mathsf{x}:n+2 \mid n \notin \{1,2\}\}$, ${F^{\pi}_{e}}^{3} = \{\mathsf{x}:n \mid n \in \mathbb{Z}\} \cup \{\mathsf{x}:n;\mathsf{x}:n+2 \mid n \notin \{1,2\}\} \cup \{\mathsf{x}:n;\mathsf{x}:n+2;\mathsf{x}:n+4 \mid n \notin \{-1,0,1,2\}\}$, so that ${F^{\pi}_{e}}^{k} = \{\mathsf{x}:n \mid n \in \mathbb{Z}\} \cup \bigcup_{j=1}^{k-1}\{\mathsf{x}:n;\ldots;\mathsf{x}:n+2j;\mid n \notin [3-2j,2]\}$ by induction hypothesis. For the induction step

$$\begin{array}{ll}
& {F^{\pi}_{e}}^{k+1}\\
= & F^{\pi}_{e}({F^{\pi}_{e}}^{k})\\
= & \{\mathsf{x}:n \mid n \in \mathbb{Z}\} \cup \{\mathsf{x}:n;\mathsf{x}:n+2;\pi \mid n \notin \{1,2\} \wedge \mathsf{x}:n+2;\pi \in {F^{\pi}_{e}}^{k}\} \hfill \lbag \text{def. } F^{\pi}_{e} \rbag\\
= & \{\mathsf{x}:n \mid n \in \mathbb{Z}\} \cup \{\mathsf{x}:n;\mathsf{x}:n+2;\pi \mid n \notin \{1,2\} \wedge \mathsf{x}:n+2;\pi \in \{\mathsf{x}:n \mid n \in \mathbb{Z}\} \cup \displaystyle\bigcup_{j=1}^{k-1}\{\mathsf{x}:n;\ldots;\mathsf{x}:\\
& n+2j \mid n \notin [3-2j,2]\}\} \hfill \lbag \text{induction hypothesis} \rbag\\
= & \{\mathsf{x}:n \mid n \in \mathbb{Z}\} \cup \{\mathsf{x}:n;\mathsf{x}:n+2;\pi \mid n \notin \{1,2\} \wedge \mathsf{x}:n+2;\pi \in \{\mathsf{x}:n \mid n \in \mathbb{Z}\}\} \cup \displaystyle\bigcup_{j=1}^{k-1}\{\mathsf{x}:n;\mathsf{x}:n+2;\pi \mid\\
& \mathsf{x}:n+2;\pi \in \{\mathsf{x}:n;\ldots;\mathsf{x}:n+2j \mid n \notin [3-2j,2]\}\} \hfill \lbag \text{def. } \cup \rbag\\
= & \{\mathsf{x}:n \mid n \in \mathbb{Z}\} \cup \{\mathsf{x}:n;\mathsf{x}:n+2 \mid n \notin \{1,2\}\} \cup \displaystyle\bigcup_{j=1}^{k-1}\{\mathsf{x}:n;\mathsf{x}:n+2;\pi \mid \mathsf{x}:n+2;\pi \in \{\mathsf{x}:n+2;\ldots;\mathsf{x}:\\
& n+2+2j \mid n+2 \notin [3-2j,2]\}\} \hfill \lbag \text{simplification and renaming} \rbag\\
= & \{\mathsf{x}:n \mid n \in \mathbb{Z}\} \cup \{\mathsf{x}:n;\mathsf{x}:n+2 \mid n \notin \{1,2\}\} \cup \displaystyle\bigcup_{j=1}^{k-1}\{\mathsf{x}:n;\mathsf{x}:n+2;\mathsf{x}:n+4;\ldots;\mathsf{x}:n+2(j+1) \mid n \notin\\
& [1-2j,0]\}
\end{array}$$

$$\wr\text{def. } \in \int$$

$$= \{\mathsf{x}:n \mid n\in\mathbb{Z}\} \cup \{\mathsf{x}:n;\mathsf{x}:n+2 \mid n\notin\{1,2\}\} \cup \bigcup_{j'=2}^{k}\{\mathsf{x}:n;\mathsf{x}:n+2;\mathsf{x}:n+4;\ldots;\mathsf{x}:n+2j' \mid n\notin [1-2(j'-1),0]\}$$

$$\wr\text{def. } j=j'-1 \text{ so } j'=j+1\int$$

$$= \{\mathsf{x}:n \mid n\in\mathbb{Z}\} \cup \bigcup_{j'=1}^{k}\{\mathsf{x}:n;\mathsf{x}:n+2;\ldots;\mathsf{x}:n+2j' \mid n\notin [3-2j',2]\}$$

$$\wr\text{incorporating the term } \{\mathsf{x}:n;\mathsf{x}:n+2 \mid n\notin\{1,2\}\} \text{ in the join for } j'=1\int$$

This shows that all iterates of F_e^{π} have the form ${F_e^{\pi}}^{k}$. Since F_e^{π} preserves joins, we have, by Tarski's fixpoint iteration theorem [81, page 305], that

$$\begin{aligned}
&\mathsf{lfp}^{\subseteq} F_e^{\pi}\\
=\ &\bigcup_{k\in\mathbb{N}} {F_e^{\pi}}^{k}\\
=\ &\bigcup_{k\in\mathbb{N}}\Big(\{\mathsf{x}:n \mid n\in\mathbb{Z}\} \cup \bigcup_{j=1}^{k-1}\{\mathsf{x}:n;\ldots;\mathsf{x}:n+2j;\mid n\notin[3-2j,2]\}\Big)\\
=\ &\{\mathsf{x}:n \mid n\in\mathbb{Z}\} \cup \bigcup_{j\geqslant 1}\{\mathsf{x}:n;\ldots;\mathsf{x}:n+2j;\mid n\notin[3-2j,2]\}\\
=\ &\bigcup_{j\in\mathbb{N}}\{\mathsf{x}:n;\ldots;\mathsf{x}:n+2j;\mid n\notin[3-2j,2]\}
\end{aligned}$$

$\wr$since for $j=0$, we have $n\notin[3-2j,2]$ which is $n\notin[3,2]$ that is $n\notin\varnothing$ or $n\in\mathbb{Z}$ with $\mathsf{x}:n;\ldots;\mathsf{x}:n+2j=\mathsf{x}:n;\ldots;\mathsf{x}:n=\mathsf{x}:n$$\int$

For the infinite traces, we have

$$\begin{aligned}
&F^{\perp}(X), \quad X\in\wp(\Sigma^{+\infty})\\
=\ &[\![\mathsf{B} \mathbin{\fatsemi}^{\pi} \mathsf{S}]\!]_e^{\pi} \mathbin{\fatsemi}^{\pi} X^{\infty}\\
=\ &\{\mathsf{x}:n;\mathsf{x}:n+2;\pi \mid n\notin\{1,2\} \land \mathsf{x}:n+2;\pi\in X^{\infty}\}
\end{aligned}$$

The iterates of $F^{\perp}$ are ${F^{\perp}}^{0}=\Sigma^{\infty}$, ${F^{\perp}}^{1}=\{\mathsf{x}:n;\mathsf{x}:n+2;\pi \mid n\notin\{1,2\}\land\mathsf{x}:n+2;\pi\in\Sigma^{\infty}\}=\{\mathsf{x}:n;\mathsf{x}:n+2;\pi \mid n\notin\{1,2\}\land\pi\in\Sigma^{\infty}\}$, ${F^{\perp}}^{2}=\{\mathsf{x}:n;\mathsf{x}:n+2;\pi \mid n\notin\{1,2\}\land\mathsf{x}:n+2;\pi\in\{\mathsf{x}:n;\mathsf{x}:n+2;\pi \mid n\notin\{1,2\}\land\pi\in\Sigma^{\infty}\}\}=\{\mathsf{x}:n;\mathsf{x}:n+2;\pi \mid n\notin\{1,2\}\land\mathsf{x}:n+2;\pi\in\{\mathsf{x}:n+2;\mathsf{x}:n+4;\pi' \mid n+2\notin\{1,2\}\land\pi'\in\Sigma^{\infty}\}\}=\{\mathsf{x}:n;\mathsf{x}:n+2;\mathsf{x}:n+4;\pi' \mid n\notin\{-1,0,1,2\}\land\pi'\in\Sigma^{\infty}\}$ which leads to the induction hypothesis ${F^{\perp}}^{k}=\{\mathsf{x}:n;\ldots;\mathsf{x}:n+2k;\pi \mid n\notin[3-2k,2]\land\pi\in\Sigma^{\infty}\}$. For the induction step,

$$\begin{aligned}
&{F^{\perp}}^{k+1}\\
=\ &F^{\perp}({F^{\perp}}^{k})\\
=\ &\{\mathsf{x}:n;\mathsf{x}:n+2;\pi \mid n\notin\{1,2\}\land\mathsf{x}:n+2;\pi\in\{\mathsf{x}:n;\ldots;\mathsf{x}:n+2k;\pi \mid n\notin[3-2k,2]\land\pi\in\Sigma^{\infty}\}\}\\
=\ &\{\mathsf{x}:n;\mathsf{x}:n+2;\pi \mid n\notin\{1,2\}\land\mathsf{x}:n+2;\pi\in\{\mathsf{x}:n+2;\ldots;\mathsf{x}:n+2+2k;\pi' \mid n+2\notin[1-2k,0]\land\pi'\in\\
&\Sigma^{\infty}\}\}\\
=\ &\{\mathsf{x}:n;\mathsf{x}:n+2;\ldots;\mathsf{x}:n+2+2k;\pi' \mid n\notin\{1,2\}\land n\notin[1-2k,0]\land\pi'\in\Sigma^{\infty}\}\\
=\ &\{\mathsf{x}:n;\ldots;\mathsf{x}:n+2(k+1);\pi' \mid n\notin[3-2(k+1),2]\land\pi'\in\Sigma^{\infty}\}
\end{aligned}$$

This shows that all iterates of $F^{\perp}$ have the form ${F^{\perp}}^{k}$. Since $F^{\perp}$ preserves meets, we have, by the dual of Tarski's fixpoint iteration theorem [81, page 305], that

$$\begin{aligned}
&\mathsf{gfp}^{\subseteq} F^{\perp}\\
=\ &\bigcap_{k\in\mathbb{N}} {F^{\perp}}^{k}
\end{aligned}$$

$$= \bigcap_{k\in\mathbb{N}} \{\texttt{x} : n;\ldots;\texttt{x} : n+2k;\pi \mid n \notin [3-2k,2] \wedge \pi \in \Sigma^{\infty}\}$$
$$= \{\texttt{x} : n;\ldots;\texttt{x} : n+2k;\ldots \mid n > 2\}$$

since all infinite traces of the form $\texttt{x} : n;\ldots;\texttt{x} : n+2k;\ldots$ with $n > 2$ belong to all iterates $F^{\perp^k}$ hence to their intersection while, conversely, all other traces start with $\texttt{x} : n;\ldots$ and $n \leqslant 2$ so do not belong to the $F^{\perp^k}$, $k \geqslant 1$ so don't belong to their intersection, or else, start with $n > 2$, but have the form $\texttt{x} : n;\ldots;\texttt{x} : n+2k+1;\ldots$ and so do not belong to $F^{\perp^k}$, hence to the intersection.

The trace semantics of $\texttt{S} \triangleq \texttt{while (x!=2) if (x==1) then break else x=x+2}$ is therefore

— $\llbracket\texttt{S}\rrbracket^{\pi}_{e}$

$\triangleq\ \mathsf{lfp}^{\subseteq}\, F^{\pi}_{e} \fatsemi^{\pi} (\llbracket\neg\texttt{(x!=2)}\ \rrbracket \cup \llbracket\texttt{(x!=2)} \fatsemi^{\pi} \texttt{if (x==1) then break else x=x+2}\rrbracket^{\pi}_{b})$ ⟅by (9)⟆

$=\ \mathsf{lfp}^{\subseteq}\, F^{\pi}_{e} \fatsemi^{\pi} (\{\texttt{x} : 2;\texttt{x} : 2\} \cup \{\texttt{x} : 1\})$

⟅$\llbracket\neg\texttt{(x!=2)}\rrbracket = \{\texttt{x} : 2;\texttt{x} : 2\}$ and $\llbracket\texttt{(x!=2)} \fatsemi^{\pi} \texttt{if (x==1) then break else x=x+2}\rrbracket = \langle ok : \{\texttt{x} : n;\texttt{x} : n+2 \mid n \notin \{1,2\}\},\ br : \{\texttt{x} : 1\}\rangle$⟆

$$= \bigcup_{j\in\mathbb{N}} \{\texttt{x} : n;\ldots;\texttt{x} : n+2j; \mid n \notin [3-2j,2]\} \fatsemi^{\pi} (\{\texttt{x} : 2;\texttt{x} : 2, \texttt{x} : 1\})$$
$$= \{\texttt{x} : -2k;\texttt{x} : -2k+2;\ldots;\texttt{x} : 0;\texttt{x} : 2 \mid k \geqslant -1\} \cup \{\texttt{x} : -2k+1;\texttt{x} : -2k+3;\ldots;\texttt{x} : 1 \mid k \geqslant 0\}$$

since, by definition of $\fatsemi^{\pi}$, we have only two possible cases.

- Either $n+2j = 2$, $j \in \mathbb{N}$, $n \notin [3-2j,2]$ so $n = -2k$ with $j = 1+k \geqslant 0$ that is $k \geqslant -1$ which implies $n \notin [3-2j,2] = [3-(2-n),2] = [n+1,2]$;
- Or $n+2j = 1$, $j \in \mathbb{N}$, $n \notin [3-2j,2]$ so $n = -2k+1$ with $j = k \geqslant 0$ which implies $n \notin [3-2j,2]$ since $n = -2k+1 < 3-2k$.

— $\llbracket\texttt{S}\rrbracket^{\pi}_{b}\ \ \triangleq\ \ \varnothing$ ⟅by (18)⟆

— $\llbracket\texttt{S}\rrbracket^{\pi}_{\perp}$

$\triangleq\ \mathsf{lfp}^{\subseteq}\, F^{\pi}_{e} \fatsemi^{\pi} \llbracket\texttt{(x!=2)} \fatsemi^{\pi} \texttt{if (x==1) then break else x=x+2}\rrbracket^{\pi}_{\perp} \cup \mathsf{gfp}^{\subseteq}\, F^{\pi}_{\perp}$ ⟅by (11)⟆

$= \mathsf{gfp}^{\subseteq}\, F^{\pi}_{\perp}$ ⟅$\texttt{(x!=2)} \fatsemi^{\pi} \texttt{if (x==1) then break else x=x+2}$ always terminates⟆

$= \{\texttt{x} : n;\ldots;\texttt{x} : n+2k;\ldots \mid n > 2\}$ □

Remark 4.5. We follow [24] by using least fixpoints for finite traces and greatest fixpoints for infinite traces. We could, equivalently, definite finite traces by a greatest fixpoint as in [64], since the least and greatest fixpoints are equal $\mathsf{lfp}^{\subseteq}\, F^{\pi}_{e} = \mathsf{gfp}^{\subseteq}\, F^{\pi}_{e}$, which would look more uniform. However, the induction principles for least and greatest fixpoints are not the same. This would require proofs relative to finite executions to be done coinductively instead of the usual inductive reasonings by induction on the length of traces. A related problem is that the abstraction theorems for least and greatest fixpoints are not the same [20, Chapter 18]. The abstraction of a least fixpoint is, in general, more precise than that of a greatest one. So if finite traces had been defined by a greatest fixpoint, it would be necessary to prove that it is equal to the least fixpoint before applying the appropriate abstractions. Then the greatest fixpoint characterization of the finite traces becomes useless. Least and greatest fixpoints can also be merged using the bi-inductive order of [24] (which abstractions yield Egli-Milner and Scott order [18]). ■

4.3 Bi-inductive Trace Semantics

The trace semantics instantiation of (12) is

$$\llbracket\texttt{S}\rrbracket^{\pi}\ \ \triangleq\ \ \langle e : \llbracket\texttt{S}\rrbracket^{\pi}_{e},\ \perp : \llbracket\texttt{S}\rrbracket^{\pi}_{\perp},\ br : \llbracket\texttt{S}\rrbracket^{\pi}_{b}\rangle \tag{20}$$

belonging to the Cartesian product : $(e : \wp(\Sigma^+) \times \bot : \wp(\Sigma^\infty) \times br : \wp(\Sigma^+))$ with named selectors e, $\bot$, and br. Since $\llbracket \mathsf{S}\rrbracket^\pi_e$ and $\llbracket \mathsf{S}\rrbracket^\pi_\bot$ are disjoint they can be put together as follows.

$$\llbracket \mathsf{S}\rrbracket^\pi \quad\triangleq\quad \langle ok : \llbracket \mathsf{S}\rrbracket^\pi_e \cup \llbracket \mathsf{S}\rrbracket^\pi_\bot,\ br : \llbracket \mathsf{S}\rrbracket^\pi_b\rangle \tag{21}$$

belonging to the Cartesian product $ok : \wp(\Sigma^{+\infty}) \times br : \wp(\Sigma^+)$ with named selectors ok and br. We can recover $\llbracket \mathsf{S}\rrbracket^\pi_e = (\llbracket \mathsf{S}\rrbracket^\pi_{ok}) \cap \Sigma^+$ and $\llbracket \mathsf{S}\rrbracket^\pi_\bot = (\llbracket \mathsf{S}\rrbracket^\pi_{ok}) \cap \Sigma^\infty$. Moreover, if $T = \langle ok : Q,\ br : B\rangle \in ok : \wp(\Sigma^{+\infty}) \times br : \wp(\Sigma^+)$, then we define the shorthands

$$T_{ok} = Q, \quad T_+ = Q \cap \Sigma^+, \quad T_\infty = Q \cap \Sigma^\infty, \quad\text{and}\quad T_{br} = B. \tag{22}$$

Then the pairwise order on $(e : \wp(\Sigma^+) \times \bot : \wp(\Sigma^\infty))$ becomes the computational ordering of [24, 26] defined on $\llbracket \mathsf{S}\rrbracket^\pi_e \cup \llbracket \mathsf{S}\rrbracket^\pi_\bot$ as $X \sqsubseteq Y \triangleq (X \cap \Sigma^+ \subseteq Y \cap \Sigma^+) \wedge (X \cap \Sigma^\infty \supseteq Y \cap \Sigma^\infty)$.

Notice that the algebraic semantics can be instantiated to semantics of probabilistic and quantum programs. In this cases the hyperlogics developed in this paper, which differentiate between computational and approximation orders, apply to probabilistic programs [33, 79] and to quantum programs [39, 84, 85]

5 Structural Fixpoint Natural Relational Semantics

The structural fixpoint natural relational semantics of [21, sect. II.1] is an instance of the algebraic semantics of sect. 3. Given states Σ, $\bot \notin \Sigma$ denoting nontermination, and $\Sigma_\bot \triangleq \Sigma \cup \{\bot\}$, the finitary domain $\mathbb{L}^\varrho_+ \triangleq \langle \wp(\Sigma\times\Sigma), \subseteq\rangle$ in 3.2.A and the infinitary domain $\mathbb{L}^\varrho_\infty \triangleq \langle \wp(\Sigma\times\{\bot\}), \subseteq\rangle$ in 3.2.C are both complete lattices for set inclusion $\subseteq$ so $\bot^\varrho_+ = \varnothing$. We let $\mathbb{1}$ be the identity function. The primitives 3.2.B are well-defined.

$$\begin{array}{rcl@{\qquad}rcl}
\mathsf{assign}^\varrho\llbracket \mathsf{x}, \mathsf{A}\rrbracket & \triangleq & \{\langle \sigma,\ \sigma[\mathsf{x} \leftarrow \mathcal{A}\llbracket \mathsf{A}\rrbracket\sigma]\rangle \mid \sigma \in \Sigma\} & \mathsf{init}^\varrho & \triangleq & \mathbb{1}\\
\mathsf{rassign}^\varrho\llbracket \mathsf{x}, a, b\rrbracket & \triangleq & \{\langle \sigma,\ \sigma[\mathsf{x} \leftarrow i]\rangle \mid \sigma \in \Sigma \wedge a - 1 < i < b + 1\} & \mathsf{break}^\varrho & \triangleq & \mathbb{1}\\
\mathsf{test}^\varrho\llbracket \mathsf{B}\rrbracket & \triangleq & \{\langle \sigma,\ \sigma\rangle \mid \sigma \in \mathcal{B}\llbracket \mathsf{B}\rrbracket\} & \mathsf{skip}^\varrho & \triangleq & \mathbb{1}\\
r \fatsemi^\varrho r' & \triangleq & \multicolumn{4}{l}{\{\langle x,\ \bot\rangle \mid \langle x,\ \bot\rangle \in r\} \cup \{\langle x,\ y\rangle \mid \exists z \in \Sigma \,.\, \langle x,\ z\rangle \in r \wedge \langle z,\ y\rangle \in r'\}}
\end{array} \tag{23}$$

$\fatsemi^\varrho$ left preserves arbitrary joins $\cup$ on $\wp(\Sigma \times \Sigma_\bot)$. $\fatsemi^\varrho$ right preserves non empty joins $\cup$ on $\wp(\Sigma \times \Sigma_\bot)$. $\fatsemi^\varrho$ is right increasing (but not necessarily lower continuous for the finitary and infinitary domains). (24)

Proof of (24).

— Let $\langle X_i,\ i \in \Delta\rangle$ be a possibly empty family of elements of $\wp(\Sigma \times \Sigma_\bot)$.

$$\begin{aligned}
&(\bigcup_{i\in\Delta} X_i) \fatsemi^\varrho r'\\
=\ & ((\bigcup_{i\in\Delta} X_i \cap \wp(\Sigma \times \Sigma)) \cup (\bigcup_{i\in\Delta} X_i \cap \wp(\Sigma \times \{\bot\}))) \fatsemi^\varrho r' && \lbag\text{def. } \wp(\Sigma \times \Sigma_\bot)\rbag\\
=\ & \{\langle x,\ \bot\rangle \mid \langle x,\ \bot\rangle \in (\bigcup_{i\in\Delta} X_i \cap \wp(\Sigma \times \{\bot\}))\} \cup \{\langle x,\ y\rangle \mid \exists z \in \Sigma \,.\, \langle x,\ z\rangle \in (\bigcup_{i\in\Delta} X_i \cap \wp(\Sigma \times \Sigma)) \wedge \langle z,\\
& y\rangle \in r'\} \qquad \lbag\text{def. } \fatsemi^\varrho,\ \forall x \in \Sigma \,.\, \langle x,\ \bot\rangle \notin \Sigma \times \Sigma, \text{ and } \forall z \in \Sigma \,.\, \langle x,\ z\rangle \notin \Sigma \times \{\bot\} \text{ since } \bot \notin \Sigma\rbag\\
=\ & \bigcup_{i\in\Delta}(\{\langle x,\ \bot\rangle \mid \langle x,\ \bot\rangle \in (X_i \cap \wp(\Sigma \times \{\bot\}))\} \cup \{\langle x,\ y\rangle \mid \exists z \in \Sigma \,.\, \langle x,\ z\rangle \in (X_i \cap \wp(\Sigma \times \Sigma)) \wedge \langle z,\ y\rangle \in r'\})\\
& && \lbag\text{def. } \cup\rbag\\
=\ & \bigcup_{i\in\Delta}(\{\langle x,\ \bot\rangle \mid \langle x,\ \bot\rangle \in (X_i \cap \wp(\Sigma \times \Sigma)) \cup (X_i \cap \wp(\Sigma \times \{\bot\}))\} \cup \{\langle x,\ y\rangle \mid \exists z \in \Sigma \,.\, \langle x,\ z\rangle \in\\
& (X_i \cap \wp(\Sigma \times \Sigma)) \cup (\bigcup_{i\in\Delta} X_i \cap \wp(\Sigma \times \{\bot\})) \wedge \langle z,\ y\rangle \in r'\}) && \lbag\bot \notin \Sigma\rbag\\
=\ & \bigcup_{i\in\Delta}(\{\langle x,\ \bot\rangle \mid \langle x,\ \bot\rangle \in X_i\} \cup \{\langle x,\ y\rangle \mid \exists z \in \Sigma \,.\, \langle x,\ z\rangle \in X_i \wedge \langle z,\ y\rangle \in r'\}) && \lbag\text{def. } \wp(\Sigma \times \Sigma_\bot)\rbag\\
=\ & \bigcup_{i\in\Delta}(X_i \fatsemi^\varrho r') && \lbag\text{def. } \fatsemi^\varrho\text{, Q.E.D.}\rbag
\end{aligned}$$

Notice that if $\Delta = \varnothing$ then $\varnothing \fatsemi^{\varrho} r' = \varnothing$.

— Let $\langle X_i,\ i \in \Delta\rangle$ be a nonempty family of elements of $\wp(\Sigma \times \Sigma_\bot) \setminus \{\varnothing\}$.

$$\begin{aligned}
& r \fatsemi^{\varrho} (\bigcup_{i\in\Delta} X_i) \\
= {} & \{\langle x,\ \bot\rangle \mid \langle x,\ \bot\rangle \in r\} \cup \{\langle x,\ y\rangle \mid \exists z \in \Sigma \mathrel{.} \langle x,\ z\rangle \in r \wedge \langle z,\ y\rangle \in (\bigcup_{i\in\Delta} X_i)\} && \lbag \text{def. } \fatsemi^{\varrho} \rbag \\
= {} & \bigcup_{i\in\Delta}(\{\langle x,\ \bot\rangle \mid \langle x,\ \bot\rangle \in r\} \cup \{\langle x,\ y\rangle \mid \exists z \in \Sigma \mathrel{.} \langle x,\ z\rangle \in r \wedge \langle z,\ y\rangle \in X_i\}) && \lbag \text{def. } \cup \rbag \\
= {} & \bigcup_{i\in\Delta}(r \fatsemi^{\varrho} X_i) && \lbag \text{def. } \fatsemi^{\varrho}\text{, Q.E.D.} \rbag
\end{aligned}$$

If $\Delta = \varnothing$ then $r \fatsemi^{\varrho} (\bigcup_{i\in\Delta} X_i) = r \fatsemi^{\varrho} \varnothing = \{\langle x,\ \bot\rangle \mid \langle x,\ \bot\rangle \in r\}$ which, in general is not empty, while $\bigcup_{i\in\Delta}(r \fatsemi^{\varrho} X_i) = \varnothing$.

— The following counter example shows that if $\langle X^i \in \wp(\Sigma \times \Sigma),\ i \in \mathbb{N}\rangle$ is a decreasing chain and $r \in \wp(\Sigma \times \Sigma)$, we may have $r \fatsemi^{\varrho} (\bigcap_{i\in\mathbb{N}} X^i) \neq \bigcap_{i\in\mathbb{N}}(r \fatsemi^{\varrho} X^i)$.

Take $r \triangleq \{\bar{\sigma}\} \times \Sigma$ and $X^i = \{\langle \sigma_j,\ \bar{\sigma}\rangle \mid j \geqslant i\}$ (that is $X^0 = \{\langle \sigma_0,\ \bar{\sigma}\rangle, \langle \sigma_1,\ \bar{\sigma}\rangle, \langle \sigma_2,\ \bar{\sigma}\rangle, \ldots\}$, $X^1 = \{\langle \sigma_1,\ \bar{\sigma}\rangle, \langle \sigma_2,\ \bar{\sigma}\rangle, \ldots\}$, $X^2 = \{\langle \sigma_2,\ \bar{\sigma}\rangle, \ldots\}$, etc). Then $r \fatsemi^{\varrho} (\bigcap_{i\in\mathbb{N}} X^i) = r \fatsemi^{\varrho} \varnothing = \varnothing$ while $\bigcap_{i\in\mathbb{N}}(r \fatsemi^{\varrho} X^i) = \bigcap_{i\in\mathbb{N}}\{\langle \bar{\sigma},\ \bar{\sigma}\rangle\} = \{\langle \bar{\sigma},\ \bar{\sigma}\rangle\}$. □

Example 5.1. Define $\mathsf{S}_1 \triangleq$ `while (y!=0) y=y-1;` with relational semantics

$$[\![\mathsf{S}_1]\!]^{\varrho} \quad = \quad \langle e : \{\langle \sigma,\ \sigma[\mathsf{y} \leftarrow 0]\rangle \mid \sigma(\mathsf{y}) \geqslant 0\},\ \bot : \{\langle \sigma,\ \bot\rangle \mid \sigma(\mathsf{y}) < 0\},\ br : \varnothing\rangle$$

meaning that S_1 terminates with $\mathsf{y} = 0$ when y is initially positive and otherwise does not terminate.

Define $\mathsf{S}_2 \triangleq$ `y=[-oo,oo]; S`$_1$ with relational semantics

$$[\![\mathsf{S}_2]\!]^{\varrho} \quad = \quad \langle e : \{\langle \sigma,\ \sigma[\mathsf{y} \leftarrow 0]\rangle \mid \sigma \in \Sigma\},\ \bot : \{\langle \sigma,\ \bot\rangle \mid \sigma \in \Sigma\},\ br : \varnothing\rangle$$

meaning that either S_2 terminates with `y=0` or does not terminate . ■

Proof of example 5.1.

$$\begin{aligned}
— & [\![\texttt{y!=0;y=y-1;}]\!]^{\varrho}_{e} \\
= {} & [\![\texttt{y!=0}]\!]^{\varrho}_{e} \fatsemi^{\varrho} [\![\texttt{y=y-1;}]\!]^{\varrho}_{e} && \lbag (4) \rbag \\
= {} & \{\langle \sigma,\ \sigma\rangle \mid \sigma(\mathsf{y}) \neq 0\} \fatsemi^{\varrho} \{\langle \sigma,\ \sigma[\mathsf{y} \leftarrow \sigma(\mathsf{y}) - 1]\rangle \mid \sigma \in \Sigma\} && \lbag (3) \text{ and } (23) \rbag \\
= {} & \{\langle \sigma,\ \sigma[\mathsf{y} \leftarrow \sigma(\mathsf{y}) - 1]\rangle \mid \sigma(\mathsf{y}) \neq 0\} && \lbag \text{def. (23) of } \fatsemi^{\varrho} \rbag
\end{aligned}$$

$$\begin{aligned}
— & \overleftarrow{F}^{\varrho}_{e} && \lbag \text{for } \mathsf{S}_1 = \texttt{while (y!=0) y=y-1;} \rbag \\
\triangleq {} & \boldsymbol{\lambda} X \in \wp(\Sigma \times \Sigma) \bullet \mathsf{init}^{\varrho} \sqcup^{\varrho}_{+} ([\![\texttt{y!=0;y=y-1;}]\!]^{\varrho}_{e} \fatsemi^{\varrho} X) && \lbag (5) \rbag \\
= {} & \boldsymbol{\lambda} X \in \wp(\Sigma \times \Sigma) \bullet \{\langle \sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup (\{\langle \sigma,\ \sigma[\mathsf{y} \leftarrow \sigma(\mathsf{y}) - 1]\rangle \mid \sigma(\mathsf{y}) \neq 0\} \fatsemi^{\varrho} X) && \lbag (23) \rbag \\
= {} & \boldsymbol{\lambda} X \in \wp(\Sigma \times \Sigma) \bullet \{\langle \sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \{\langle \sigma,\ \sigma'\rangle \mid \sigma(\mathsf{y}) \neq 0 \wedge \langle \sigma[\mathsf{y} \leftarrow \sigma(\mathsf{y}) - 1],\ \sigma'\rangle \in X\} && \lbag (23) \rbag
\end{aligned}$$

— By (24) and (5), $\overleftarrow{F}^{\varrho}_{e}$ for $\mathsf{S}_1 =$ `while (y!=0) y=y-1;` preserves nonempty joins $\cup$ so that the infinite iterates $\langle X^i,\ i \leqslant \omega\rangle$ of $\mathsf{lfp}^{\subseteq}\ \overleftarrow{F}^{\varrho}_{e}$ are as follows

$$\begin{aligned}
X^0 = {} & \varnothing \\
X^1 = {} & \{\langle \sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \\
X^2 = {} & \{\langle \sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \{\langle \sigma,\ \sigma'\rangle \mid \sigma(\mathsf{y}) \neq 0 \wedge \langle \sigma[\mathsf{y} \leftarrow \sigma(\mathsf{y}) - 1],\ \sigma'\rangle \in X^1\} && \lbag \text{def. iterates} \rbag \\
= {} & \{\langle \sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \{\langle \sigma,\ \sigma[\mathsf{y} \leftarrow \sigma(\mathsf{y}) - 1]\rangle \mid \sigma(\mathsf{y}) \neq 0\} && \lbag \text{def. } X^1 \rbag \\
X^3 = {} & \{\langle \sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \{\langle \sigma,\ \sigma'\rangle \mid \sigma(\mathsf{y}) \neq 0 \wedge \langle \sigma[\mathsf{y} \leftarrow \sigma(\mathsf{y}) - 1],\ \sigma'\rangle \in X^2\} && \lbag \text{def. iterates} \rbag
\end{aligned}$$

$$= \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \cup \{\langle\sigma,\,\sigma'\rangle \mid \sigma(\mathrm{y}) \neq 0 \wedge \langle\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1],\,\sigma'\rangle \in (\{\langle\sigma',\,\sigma'\rangle \mid \sigma'\in\Sigma\} \cup \{\langle\sigma',\,\sigma'[\mathrm{y}\leftarrow\sigma'(\mathrm{y})-1]\rangle \mid \sigma'(\mathrm{y})\neq 0\})\} \qquad \llparenthesis\text{def. } X^2\rrparenthesis$$

$$= \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \cup \{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1]\rangle \mid \sigma(\mathrm{y})\neq 0\} \cup \{\langle\sigma,\,\sigma''\rangle \mid \sigma(\mathrm{y})\neq 0 \wedge \langle\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1],\,\sigma''\rangle \in \{\langle\sigma',\,\sigma'[\mathrm{y}\leftarrow\sigma'(\mathrm{y})-1]\rangle \mid \sigma'(\mathrm{y})\neq 0\}\} \qquad \llparenthesis\text{def. } \cup\rrparenthesis$$

$$= \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \cup \{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1]\rangle \mid \sigma(\mathrm{y})\neq 0\} \cup \{\langle\sigma,\,\sigma''\rangle \mid \sigma(\mathrm{y})\neq 0 \wedge \langle\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1],\,\sigma''\rangle \in \{\langle\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1],\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1][\mathrm{y}\leftarrow\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1](\mathrm{y})-1]\rangle \mid \sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1](\mathrm{y})\neq 0\}\} \qquad \llparenthesis\text{def. } \in\rrparenthesis$$

$$= \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \cup \{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1]\rangle \mid \sigma(\mathrm{y})\neq 0\} \cup \{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1][\mathrm{y}\leftarrow\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1](\mathrm{y})-1]\rangle \mid \sigma(\mathrm{y})\neq 0 \wedge \sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1](\mathrm{y})\neq 0\} \qquad \llparenthesis\text{def. } \in\rrparenthesis$$

$$= \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \cup \{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1]\rangle \mid \sigma(\mathrm{y})\neq 0\} \cup \{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-2]\rangle \mid \sigma(\mathrm{y})\neq 0 \wedge \sigma(\mathrm{y})\neq 1\} \qquad \llparenthesis\text{simplification}\rrparenthesis$$

$$X^n = \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \cup \bigcup_{i=1}^{n-1}\{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-i]\rangle \mid \bigwedge_{j=0}^{i-1}\sigma(\mathrm{y})\neq j\} \qquad \llparenthesis\text{induction hypothesis}\rrparenthesis$$

$$X^{n+1} = \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \cup \{\langle\sigma,\,\sigma'\rangle \mid \sigma(\mathrm{y})\neq 0 \wedge \langle\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1],\,\sigma'\rangle \in X^n\} \qquad \llparenthesis\text{def. iterates}\rrparenthesis$$

$$= \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \cup \{\langle\sigma,\,\sigma'\rangle \mid \sigma(\mathrm{y})\neq 0 \wedge \langle\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1],\,\sigma'\rangle \in (\{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \cup \bigcup_{i=1}^{n-1}\{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-i]\rangle \mid \bigwedge_{j=0}^{i-1}\sigma(\mathrm{y})\neq j\})\} \qquad \llparenthesis\text{def. } X^n\rrparenthesis$$

$$= \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \cup \{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1]\rangle \mid \sigma(\mathrm{y})\neq 0\} \cup \{\langle\sigma,\,\sigma'\rangle \mid \sigma(\mathrm{y})\neq 0 \wedge \langle\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1],\,\sigma'\rangle \in \bigcup_{i=1}^{n-1}\{\langle\sigma'',\,\sigma''[\mathrm{y}\leftarrow\sigma''(\mathrm{y})-i]\rangle \mid \bigwedge_{j=0}^{i-1}\sigma''(\mathrm{y})\neq j\}\} \qquad \llparenthesis\text{def. } \cup\text{, renaming}\rrparenthesis$$

$$= \{\langle\sigma,\sigma\rangle \mid \sigma\in\Sigma\} \cup \{\langle\sigma,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1]\rangle \mid \sigma(\mathrm{y})\neq 0\} \cup \bigcup_{i=1}^{n-1}\{\langle\sigma,\sigma'\rangle \mid \sigma(\mathrm{y})\neq 0 \wedge \langle\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1],\,\sigma'\rangle \in \{\langle\sigma'',\,\sigma''[\mathrm{y}\leftarrow\sigma''(\mathrm{y})-i]\rangle \mid \bigwedge_{j=0}^{i-1}\sigma''(\mathrm{y})\neq j\}\} \qquad \llparenthesis\text{def. } \cup\rrparenthesis$$

$$= \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \cup \{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1]\rangle \mid \sigma(\mathrm{y})\neq 0\} \cup \bigcup_{i=1}^{n-1}\{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-(i+1)]\rangle \mid \sigma(\mathrm{y})\neq 0 \wedge \bigwedge_{j=0}^{i-1}\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1](\mathrm{y})\neq j\}$$

$$\llparenthesis\text{def. } \in \text{ so } \sigma'' = \sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1] \text{ and } \sigma' = \sigma''[\mathrm{y}\leftarrow\sigma''(\mathrm{y})-i] = \sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1][\mathrm{y}\leftarrow\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1](\mathrm{y})-i] = \sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-(i+1)]\rrparenthesis$$

$$= \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \cup \{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1]\rangle \mid \sigma(\mathrm{y})\neq 0\} \cup \bigcup_{i=1}^{n-1}\{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-(i+1)]\rangle \mid \sigma(\mathrm{y})\neq 0 \wedge \bigwedge_{j=0}^{i-1}\sigma(\mathrm{y})\neq j+1\} \qquad \llparenthesis\text{simplification}\rrparenthesis$$

$$= \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \cup \{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1]\rangle \mid \sigma(\mathrm{y})\neq 0\} \cup \bigcup_{i=1}^{n-1}\{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-(i+1)]\rangle \mid \bigwedge_{j=0}^{i}\sigma(\mathrm{y})\neq j\}$$

$$\llparenthesis\text{change of dummy variable and incorporation of } \sigma(\mathrm{y})\neq 0 \text{ in the conjunction for } j=0\rrparenthesis$$

$$= \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \ \cup \bigcup_{i=0}^{n-1}\{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-(i+1)]\rangle \mid \bigwedge_{j=0}^{i}\sigma(\mathrm{y})\neq j\}\}$$

$$\llparenthesis\text{incorporation of } \{\langle\sigma,\,\sigma[\mathrm{y}\leftarrow\sigma(\mathrm{y})-1]\rangle \mid \sigma(\mathrm{y})\neq 0\} \text{ in the union for } i=0\rrparenthesis$$

$$= \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \;\cup \bigcup_{i=1}^{(n+1)-1} \{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow\sigma(\mathtt{y})-i]\rangle \mid \bigwedge_{j=0}^{i-1}\sigma(\mathtt{y})\neq j\}$$

⟅change of dummy variables⟆

— By recurrence, $X^n = \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\}\cup\bigcup_{i=1}^{n-1}\{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow\sigma(\mathtt{y})-i]\rangle \mid \bigwedge_{j=0}^{i-1}\sigma(\mathtt{y})\neq j\}$, so that the least fixpoint of $\overleftarrow{F}_e^{\varrho}$ for $\mathtt{S}_1 = \mathtt{while\ \ (y!=0)\ \ y=y-1;}$ is

$$\begin{aligned}
&\mathsf{lfp}^{\subseteq}\,\overleftarrow{F}_e^{\varrho}\\
= {}& \bigcup_{n\in\mathbb{N}} X^n && \text{⟅def. iterates⟆}\\
= {}& \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \;\cup \bigcup_{n\in\mathbb{N}}\bigcup_{i=1}^{n}\{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow\sigma(\mathtt{y})-i]\rangle \mid \bigwedge_{j=0}^{i-1}\sigma(\mathtt{y})\neq j\}\\
= {}& \{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \;\cup \bigcup_{i>0}\{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow\sigma(\mathtt{y})-i]\rangle \mid \sigma(\mathtt{y})\notin[0,i-1]\}
\end{aligned}$$

— It follows that for $\mathtt{S}_1 \triangleq \mathtt{while\ \ (y!=0)\ \ y=y-1;}$, we have

$$\begin{aligned}
&\llbracket\mathtt{S}_1\rrbracket_e^{\varrho}\\
= {}& \mathsf{lfp}^{\subseteq}\,\overleftarrow{F}_e^{\varrho}\,\fatsemi^{\varrho}\,(\llbracket\neg\mathtt{B}\rrbracket_e^{\varrho}\cup\llbracket\mathtt{B;S}\rrbracket_b^{\varrho}) && \text{⟅by (9) with } \mathtt{B} = \mathtt{(y!=0)},\ \neg\mathtt{B} = \mathtt{(y=0)}\text{, and } \mathtt{S} = \mathtt{y=y-1;}\text{⟆}\\
= {}& (\{\langle\sigma,\,\sigma\rangle \mid \sigma\in\Sigma\} \;\cup\bigcup_{i>0}\{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow\sigma(\mathtt{y})-i]\rangle \mid \sigma(\mathtt{y})\notin[0,i-1]\})\,\fatsemi^{\varrho}\,(\{\langle\sigma,\,\sigma\rangle \mid \sigma(\mathtt{y})=0\}\cup\varnothing)\\
= {}& \{\langle\sigma,\,\sigma\rangle \mid \sigma(\mathtt{y})=0\} \;\cup\bigcup_{i>0}\{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow\sigma(\mathtt{y})-i]\rangle \mid \sigma(\mathtt{y})\notin[0,i-1]\wedge\sigma[\mathtt{y}\leftarrow\sigma(\mathtt{y})-i](\mathtt{y})=0\} && \text{⟅(23)⟆}\\
= {}& \{\langle\sigma,\,\sigma\rangle \mid \sigma(\mathtt{y})=0\} \;\cup\bigcup_{i>0}\{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow\sigma(\mathtt{y})-i]\rangle \mid \sigma(\mathtt{y})\notin[0,i-1]\wedge\sigma(\mathtt{y})=i\}\\
& && \text{⟅function application⟆}\\
= {}& \{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow 0]\rangle \mid \sigma(\mathtt{y})=0\} \;\cup\bigcup_{i>0}\{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow 0]\rangle \mid \sigma(\mathtt{y})=i\}\\
& && \text{⟅substitution } \sigma(\mathtt{y})=i\text{⟆}\\
= {}& \{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow 0]\rangle \mid \sigma(\mathtt{y})\geqslant 0\} && \text{⟅joining cases⟆}
\end{aligned}$$

— It follows that for $\mathtt{S}_2 = \mathtt{y=[-oo,oo];\ \ S}_1$, we have

$$\begin{aligned}
&\llbracket\mathtt{S}_2\rrbracket_e^{\varrho}\\
= {}& \llbracket\mathtt{y=[-oo,oo];}\rrbracket_e^{\varrho}\,\fatsemi^{\varrho}\,\llbracket\mathtt{S}_1\rrbracket_e^{\varrho} && \text{⟅(4)⟆}\\
= {}& \{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow n]\rangle \mid n\in\mathbb{N}\}\,\fatsemi^{\varrho}\,\{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow 0]\rangle \mid \sigma(\mathtt{y})\geqslant 0\} && \text{⟅(3) and as previously shown⟆}\\
= {}& \{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow n][\mathtt{y}\leftarrow 0]\rangle \mid n\in\mathbb{N}\wedge\sigma[\mathtt{y}\leftarrow n](\mathtt{y})\geqslant 0\} && \text{⟅(23)⟆}\\
= {}& \{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow 0]\rangle \mid \sigma\in\Sigma\} && \text{⟅simplification⟆}
\end{aligned}$$

— By (7), we have

$$\begin{aligned}
&F_{\perp}^{\varrho} && \text{⟅for } \mathtt{S}_1 = \mathtt{while\ \ (y!=0)\ \ y=y-1;}\text{⟆}\\
= {}& \boldsymbol{\lambda} X\in\mathbb{L}_{\infty}^{\varrho}\bullet\llbracket\mathtt{y!=0;y=y-1;}\rrbracket_e^{\varrho}\,\fatsemi^{\varrho}\,X\\
= {}& \boldsymbol{\lambda} X\in\wp(\Sigma\times\{\perp\})\bullet\{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow\sigma(\mathtt{y})-1]\rangle \mid \sigma(\mathtt{y})\neq 0\}\,\fatsemi^{\varrho}\,X\\
= {}& \{\langle x,\,y\rangle \mid \exists z\in\Sigma\;.\;\langle x,\,z\rangle\in\{\langle\sigma,\,\sigma[\mathtt{y}\leftarrow\sigma(\mathtt{y})-1]\rangle \mid \sigma(\mathtt{y})\neq 0\}\wedge\langle z,\,y\rangle\in X\} && \text{⟅(23)⟆}\\
= {}& \{\langle\sigma,\,y\rangle \mid \sigma(\mathtt{y})\neq 0\wedge\langle\sigma[\mathtt{y}\leftarrow\sigma(\mathtt{y})-1],\,y\rangle\in X\} && \text{⟅def. }\in\text{⟆}\\
= {}& \{\langle\sigma,\,\perp\rangle \mid \sigma(\mathtt{y})\neq 0\wedge\langle\sigma[\mathtt{y}\leftarrow\sigma(\mathtt{y})-1],\,\perp\rangle\in X\} && \text{⟅}X\in\wp(\Sigma\times\{\perp\})\text{⟆}
\end{aligned}$$

— By (24) and (5), $F^{\varrho}_{\perp}$ for $\texttt{S}_1$ = `while (y!=0) y=y-1;` converges at ω so that the infinite iterates $\langle X^i,\ i \leqslant \omega\rangle$ of $\llbracket \texttt{S}_1 \rrbracket^{\varrho}_{li} = \mathsf{gfp}^{\subseteq}\, F^{\varrho}_{\perp}$ are as follows

$$
\begin{array}{lll}
X^0 = & \Sigma \times \{\perp\} & \\
X^1 = & \{\langle\sigma,\ \perp\rangle \mid \sigma(\texttt{y}) \neq 0 \wedge \langle\sigma[\texttt{y} \leftarrow \sigma(\texttt{y}) - 1],\ \perp\rangle \in \Sigma \times \{\perp\}\} & \lbag \text{def. iterates} \rbag\\
 = & \{\langle\sigma,\ \perp\rangle \mid \sigma(\texttt{y}) \neq 0\} & \lbag \text{simplification} \rbag\\
X^2 = & \{\langle\sigma,\ \perp\rangle \mid \sigma(\texttt{y}) \neq 0 \wedge \langle\sigma[\texttt{y} \leftarrow \sigma(\texttt{y}) - 1],\ \perp\rangle \in \{\langle\sigma',\ \perp\rangle \mid \sigma'(\texttt{y}) \neq 0\}\} & \lbag \text{def. iterates} \rbag\\
 = & \{\langle\sigma,\ \perp\rangle \mid \sigma(\texttt{y}) \neq 0 \wedge \sigma[\texttt{y} \leftarrow \sigma(\texttt{y}) - 1](\texttt{y}) \neq 0\} & \lbag \text{def. } \in \rbag\\
 = & \{\langle\sigma,\ \perp\rangle \mid \sigma(\texttt{y}) \neq 0 \wedge \sigma(\texttt{y}) \neq 1\} & \lbag \text{function application} \rbag\\
X^n = & \{\langle\sigma,\ \perp\rangle \mid \displaystyle\bigwedge_{i=0}^{n-1} \sigma(\texttt{y}) \neq i\} & \lbag \text{induction hypothesis} \rbag\\
X^{n+1} = & \{\langle\sigma,\ \perp\rangle \mid \sigma(\texttt{y}) \neq 0 \wedge \langle\sigma[\texttt{y} \leftarrow \sigma(\texttt{y}) - 1],\ \perp\rangle \in \{\langle\sigma,\ \perp\rangle \mid \displaystyle\bigwedge_{i=0}^{n-1} \sigma(\texttt{y}) \neq i\}\} & \lbag \text{def. iterates} \rbag\\
\phantom{X^{n+1}} = & \{\langle\sigma,\ \perp\rangle \mid \sigma(\texttt{y}) \neq 0 \wedge \displaystyle\bigwedge_{i=0}^{n-1} \sigma[\texttt{y} \leftarrow \sigma(\texttt{y}) - 1](\texttt{y}) \neq i\} & \lbag \text{def. } \in \rbag\\
\phantom{X^{n+1}} = & \{\langle\sigma,\ \perp\rangle \mid \sigma(\texttt{y}) \neq 0 \wedge \displaystyle\bigwedge_{i=0}^{n-1} \sigma(\texttt{y}) \neq i + 1\} & \lbag \text{function application} \rbag\\
\phantom{X^{n+1}} = & \{\langle\sigma,\ \perp\rangle \mid \sigma(\texttt{y}) \neq 0 \wedge \displaystyle\bigwedge_{j=1}^{n} \sigma(\texttt{y}) \neq j\} & \lbag \text{change of dummy variables } j = i + 1 \rbag\\
\phantom{X^{n+1}} = & \{\langle\sigma,\ \perp\rangle \mid \displaystyle\bigwedge_{i=0}^{(n+1)-1} \sigma(\texttt{y}) \neq i\} & \lbag \text{grouping terms and renaming} \rbag
\end{array}
$$

— By recurrence, $X^n = \{\langle\sigma,\ \perp\rangle \mid \bigwedge_{i=0}^{n-1} \sigma(\texttt{y}) \neq i\}$, so that, by convergence at ω, the greatest fixpoint is

$$
\begin{array}{lll}
& \llbracket \texttt{S}_1 \rrbracket^{\varrho}_{li} \ = \ \mathsf{gfp}^{\subseteq}\, F^{\varrho}_{\perp} & \\
= & \displaystyle\bigcap_{n\in\mathbb{N}} X^n & \lbag \text{def. iterates} \rbag\\
= & \displaystyle\bigcap_{n\in\mathbb{N}} \{\langle\sigma,\ \perp\rangle \mid \bigwedge_{i=0}^{n-1} \sigma(\texttt{y}) \neq i\} & \\
= & \{\langle\sigma,\ \perp\rangle \mid \sigma(\texttt{y}) < 0\} & \lbag \Sigma = \{\mathsf{x}, \mathsf{y}\} \to \mathbb{Z} \rbag
\end{array}
$$

— Obviously $\llbracket \texttt{(y!=0); y=y-1;} \rrbracket^{\varrho}_{\perp} = \varnothing$ since the body always terminates, so that, by (10), we have $\llbracket \texttt{while (y!=0) y=y-1;} \rrbracket^{\varrho}_{bi} \triangleq \mathsf{lfp}^{\sqsubseteq^{\varrho}_{+}}\, \overleftarrow{F}^{\varrho}_{e} \fatsemi^{\varrho} \llbracket \texttt{(y!=0); y=y-1;} \rrbracket^{\varrho}_{\perp} = \mathsf{lfp}^{\subseteq}\, \overleftarrow{F}^{\varrho}_{e} \fatsemi^{\varrho} \varnothing = \varnothing$. By (11), we have $\llbracket \texttt{while (y!=0) y=y-1;} \rrbracket^{\varrho}_{\perp} \triangleq \llbracket \texttt{while (y!=0) y=y-1;} \rrbracket^{\varrho}_{bi} \cup \llbracket \texttt{while (y!=0) y=y-1;} \rrbracket^{\varrho}_{li} = \{\langle\sigma, \perp\rangle \mid \sigma(\texttt{y}) < 0\}$.

— It follows that

$$
\begin{array}{lll}
& \llbracket \texttt{S}_2 \rrbracket^{\varrho}_{\perp} & \\
= & \llbracket \texttt{y=[-oo,oo]; S}_1 \rrbracket^{\varrho}_{\perp} & \\
= & \llbracket \texttt{y=[-oo,oo];} \rrbracket^{\varrho}_{\perp} \cup (\llbracket \texttt{y=[-oo,oo];} \rrbracket^{\varrho}_{e} \fatsemi^{\varrho} \llbracket \texttt{S}_1 \rrbracket^{\varrho}_{\perp}) & \lbag (4) \rbag\\
= & \varnothing \cup (\{\langle\sigma,\ \sigma[\texttt{y} \leftarrow i]\rangle \mid \sigma \in \Sigma \wedge i \in \mathbb{N}\} \fatsemi^{\varrho} \{\langle\sigma,\ \perp\rangle \mid \sigma(\texttt{y}) < 0\}) & \lbag (4), (3) \text{ and } (23) \rbag\\
= & \{\langle x,\ \perp\rangle \mid \langle x,\ \perp\rangle \in \{\langle\sigma,\ \sigma[\texttt{y} \leftarrow i]\rangle \mid \sigma \in \Sigma \wedge i \in \mathbb{N}\}\} \cup \{\langle x,\ y\rangle \mid \exists z \in \Sigma \mathrel{.} \langle x,\ z\rangle \in \{\langle\sigma,\ \sigma[\texttt{y} \leftarrow i]\rangle \mid \sigma \in & \\
& \Sigma \wedge i \in \mathbb{N}\} \wedge \langle z,\ y\rangle \in \{\langle\sigma',\ \perp\rangle \mid \sigma'(\texttt{y}) < 0\}\} & \lbag (23) \rbag\\
= & \{\langle\sigma,\ \perp\rangle \mid \exists i \mathrel{.} \sigma \in \Sigma \wedge i \in \mathbb{N} \wedge \sigma[\texttt{y} \leftarrow i](\texttt{y}) < 0\} & \lbag \text{def. } \in \rbag
\end{array}
$$

$= \{\langle\sigma,\ \bot\rangle \mid \exists i \,.\, \sigma \in \Sigma \wedge i \in \mathbb{N} \wedge i < 0\}$ ⟅function application⟆

$= \{\langle\sigma,\ \bot\rangle \mid \sigma \in \Sigma\}$ ⟅simplification⟆

— By (12) and (10), we get $[\![\mathtt{S}_1]\!]^{\varrho} = \langle e : \{\langle\sigma,\ \sigma[\mathtt{y} \leftarrow 0]\rangle \mid \sigma(\mathtt{y}) \geqslant 0\},\ \bot : \{\langle\sigma,\ \bot\rangle \mid \sigma(\mathtt{y}) < 0\},\ br : \varnothing\rangle$ and $[\![\mathtt{S}_2]\!]^{\varrho} \triangleq \langle e : \{\langle\sigma,\ \sigma[\mathtt{y} \leftarrow 0]\rangle \mid \sigma \in \Sigma\},\ \bot : \{\langle\sigma,\ \bot\rangle \mid \sigma \in \Sigma\},\ br : \varnothing\rangle$. □

Example 5.2. Define $\mathtt{S}_3 \triangleq$ `while (x!=0) {` $\mathtt{S}_2$ `x=x-1; }` with relational semantics

$$[\![\mathtt{S}_3]\!]^{\sharp} = \langle e : \{\langle\sigma,\ \sigma\rangle \mid \sigma(\mathtt{x}) = 0\} \cup \{\langle\sigma,\ \sigma[\mathtt{y} \leftarrow 0][\mathtt{x} \leftarrow 0]\rangle \mid \sigma(\mathtt{x}) > 0\},\ \bot : \{\langle\sigma,\ \bot\rangle \mid \sigma(\mathtt{x}) \neq 0\},\ br : \varnothing\rangle$$

meaning that $\mathtt{S}_3$ terminates because either the loop is not entered or it is entered with $\mathtt{x} > 0$ and $\mathtt{S}_2$ terminates at each iteration setting y to 0. $\mathtt{S}_3$ does not terminate when the loop is entered and either its body does not terminate or $\mathtt{x} < 0$.

Define $\mathtt{S}_4 \triangleq$ `x=[-oo,oo];` $\mathtt{S}_3$ with relational semantics

$$[\![\mathtt{S}_4]\!]^{\sharp} = \langle e : \{\langle\sigma,\ \sigma[\mathtt{x} \leftarrow 0]\rangle \mid \sigma \in \Sigma\} \cup \{\langle\sigma,\ \sigma[\mathtt{y} \leftarrow 0][\mathtt{x} \leftarrow 0]\rangle \mid \sigma \in \Sigma\},\ \bot : \{\langle\sigma,\ \bot\rangle \mid \sigma \in \Sigma\},\ br : \varnothing\rangle$$

meaning either termination with x=0 (when x is randomly assigned 0) or with x=0 and y=0 (when x is randomly assigned a positive number while x is randomly assigned a positive number or zero) or nontermination (when x is randomly assigned a negative number or x is randomly assigned a positive number and y are randomly assigned a negative number). . In this example, the fixpoint iterations are infinite but would be transfinite for a transition semantics (corresponding to the lexicographic ordering for the nested loops) [18]. ■

Proof of example 5.2.

— $[\![$`x!=0;` $\mathtt{S}_2$ `x=x-1;`$]\!]^{\varrho}_{e}$

$= [\![$`x!=0`$]\!]^{\varrho}_{e} \fatsemi^{\varrho} [\![\mathtt{S}_2]\!]^{\varrho}_{e} \fatsemi^{\varrho} [\![$`x=x-1;`$]\!]^{\varrho}_{e}$ ⟅(4)⟆

$= \{\langle\sigma,\ \sigma\rangle \mid \sigma(\mathtt{x}) \neq 0\} \fatsemi^{\varrho} \{\langle\sigma,\ \sigma[\mathtt{y} \leftarrow 0]\rangle \mid \sigma \in \Sigma\} \fatsemi^{\varrho} \{\langle\sigma,\ \sigma[\mathtt{x} \leftarrow \sigma(\mathtt{x}) - 1]\rangle \mid \sigma \in \Sigma\}$ ⟅(3) and (23)⟆

$= \{\langle\sigma,\ \sigma[\mathtt{y} \leftarrow 0][\mathtt{x} \leftarrow \sigma[\mathtt{y} \leftarrow 0](\mathtt{x}) - 1]\rangle \mid \sigma(\mathtt{x}) \neq 0\}$ ⟅def. (23) of $\fatsemi^{\varrho}$⟆

$= \{\langle\sigma,\ \sigma[\mathtt{y} \leftarrow 0][\mathtt{x} \leftarrow \sigma(\mathtt{x}) - 1]\rangle \mid \sigma(\mathtt{x}) \neq 0\}$ ⟅$\mathtt{x} \neq \mathtt{y}$⟆

— $\vec{F}^{\varrho}_{e}$ ⟅for $\mathtt{S}_3$ = `while (x!=0) {` $\mathtt{S}_2$ `x=x-1; }`⟆

$\triangleq \boldsymbol{\lambda} X \in \wp(\Sigma \times \Sigma) \bullet \mathsf{init}^{\varrho} \sqcup^{\varrho}_{+} ([\![$`x!=0;` $\mathtt{S}_2$ `x=x-1;`$]\!]^{\varrho}_{e} \fatsemi^{\varrho} X)$ ⟅(5)⟆

$= \boldsymbol{\lambda} X \in \wp(\Sigma \times \Sigma) \bullet \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup (\{\langle\sigma,\ \sigma[\mathtt{y} \leftarrow 0][\mathtt{x} \leftarrow \sigma(\mathtt{x}) - 1]\rangle \mid \sigma(\mathtt{x}) \neq 0\} \fatsemi^{\varrho} X)$ ⟅(23)⟆

$= \boldsymbol{\lambda} X \in \wp(\Sigma \times \Sigma) \bullet \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \{\langle\sigma,\ \sigma'\rangle \mid \sigma(\mathtt{x}) \neq 0 \wedge \langle\sigma[\mathtt{y} \leftarrow 0][\mathtt{x} \leftarrow \sigma(\mathtt{x}) - 1],\ \sigma'\rangle \in X\}$⟅(23)⟆

— By (24) and (5), $\vec{F}^{\varrho}_{e}$ for $\mathtt{S}_3$ = `while (x!=0) {` $\mathtt{S}_2$ `x=x-1; }` preserves nonempty joins $\cup$ so that the infinite iterates $\langle X^{i},\ i \leqslant \omega\rangle$ of $\mathsf{lfp}^{\subseteq}\ \vec{F}^{\varrho}_{e}$ are as follows

$X^{0} = \varnothing$

$X^{1} = \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\}$

$X^{2} = \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \{\langle\sigma,\ \sigma'\rangle \mid \sigma(\mathtt{x}) \neq 0 \wedge \langle\sigma[\mathtt{y} \leftarrow 0][\mathtt{x} \leftarrow \sigma(\mathtt{x}) - 1],\ \sigma'\rangle \in X^{1}\}$ ⟅def. iterates⟆

$\quad = \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \{\langle\sigma,\ \sigma[\mathtt{y} \leftarrow 0][\mathtt{x} \leftarrow \sigma(\mathtt{x}) - 1]\rangle \mid \sigma(\mathtt{x}) \neq 0\}$ ⟅def. X^{1}⟆

$X^{n} = \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \bigcup_{i=1}^{n-1} \{\langle\sigma,\ \sigma[\mathtt{y} \leftarrow 0][\mathtt{x} \leftarrow \sigma(\mathtt{x}) - i]\rangle \mid \bigwedge_{j=0}^{i-1} \sigma(\mathtt{x}) \neq j\}$ ⟅induction hypothesis⟆

$X^{n+1} = \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \{\langle\sigma,\ \sigma'\rangle \mid \sigma(\mathtt{x}) \neq 0 \wedge \langle\sigma[\mathtt{y} \leftarrow 0][\mathtt{x} \leftarrow \sigma(\mathtt{x}) - 1],\ \sigma'\rangle \in X^{n}\}$ ⟅def. iterates⟆

$$= \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \{\langle\sigma,\ \sigma'\rangle \mid \sigma(\mathsf{x}) \neq 0 \wedge \langle\sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1],\ \sigma'\rangle \in (\{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \bigcup_{i=1}^{n-1}\{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - i]\rangle \mid \bigwedge_{j=0}^{i-1}\sigma(\mathsf{x}) \neq j\})\} \qquad \text{⟅def. } X^n\text{⟆}$$

$$= \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \{\langle\sigma,\ \sigma'\rangle \mid \sigma(\mathsf{x}) \neq 0 \wedge \langle\sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1],\ \sigma'\rangle \in \{\langle\sigma'',\ \sigma''\rangle \mid \sigma'' \in \Sigma\}\} \cup \bigcup_{i=1}^{n-1}\{\langle\sigma,\ \sigma'\rangle \mid \sigma(\mathsf{x}) \neq 0 \wedge \langle\sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1],\ \sigma'\rangle \in \{\langle\sigma'',\ \sigma''[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma''(\mathsf{x}) - i]\rangle \mid \bigwedge_{j=0}^{i-1}\sigma''(\mathsf{x}) \neq j\}\} \qquad \text{⟅def. } \in \text{ and } \cup\text{, renaming⟆}$$

$$= \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1]\rangle \mid \sigma(\mathsf{x}) \neq 0\} \cup \bigcup_{i=1}^{n-1}\{\langle\sigma,\ \sigma'\rangle \mid \exists\sigma''\ .\ \sigma'' = \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1] \wedge \sigma''[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma''(\mathsf{x}) - i] = \sigma' \wedge \bigwedge_{j=0}^{i-1}\sigma''(\mathsf{x}) \neq j)\} \qquad \text{⟅def. } \in\text{⟆}$$

$$= \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1]\rangle \mid \sigma(\mathsf{x}) \neq 0\} \cup \bigcup_{i=1}^{n-1}\{\langle\sigma,\ \sigma'\rangle \mid \exists\sigma''\ .\ \sigma'' = \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1] \wedge \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - (i+1)] = \sigma' \wedge \bigwedge_{j=0}^{i-1}\sigma(\mathsf{x}) \neq (j+1))\}$$

$$\text{⟅function application with } \sigma''(\mathsf{x}) = \sigma(\mathsf{x}) - 1 \text{ and } \sigma''[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - (i+1)] = \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - (i+1)]\text{⟆}$$

$$= \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1]\rangle \mid \sigma(\mathsf{x}) \neq 0\} \cup \bigcup_{i=1}^{n-1}\{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - (i+1)]\rangle \mid \bigwedge_{j=0}^{i-1}\sigma(\mathsf{x}) \neq (j+1)j)\} \qquad \text{⟅simplification⟆}$$

$$= \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1]\rangle \mid \sigma(\mathsf{x}) \neq 0\} \cup \bigcup_{i'=2}^{n}\{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - i']\rangle \mid \bigwedge_{j=0}^{i'-2}\sigma(\mathsf{x}) \neq (j+1))\} \qquad \text{⟅change of variable } i' = i + 1\text{⟆}$$

$$= \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1]\rangle \mid \sigma(\mathsf{x}) \neq 0\} \cup \bigcup_{i'=2}^{n}\{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - i']\rangle \mid \bigwedge_{j'=1}^{i'-1}\sigma(\mathsf{x}) \neq j')\} \qquad \text{⟅change of variable } j' = j + 1\text{⟆}$$

$$= \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \bigcup_{i=1}^{(n+1)-1}\{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - i]\rangle \mid \bigwedge_{j=0}^{i-1}\sigma(\mathsf{x}) \neq j\})\} \qquad \text{⟅grouping terms for } i = 1\text{⟆}$$

which is the induction hypothesis for $n + 1$.

— By recurrence, $X^n = \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \bigcup_{i=1}^{n-1}\{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - i]\rangle \mid \bigwedge_{j=0}^{i-1}\sigma(\mathsf{x}) \neq j\}$, so that the least fixpoint of $\overleftarrow{F}_e^{\varrho}$ for S_3 = `while (x!=0) {` S_2 `x=x-1; }` is

$$\mathsf{lfp}^{\subseteq}\,\overleftarrow{F}_e^{\varrho} \qquad \text{⟅for } \mathsf{S}_3 = \texttt{while (x!=0) \{ } \mathsf{S}_2 \texttt{ x=x-1; \}}\text{⟆}$$

$$= \bigcup_{n\in\mathbb{N}} X^n \qquad \text{⟅def. iterates⟆}$$

$$= \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \bigcup_{n\in\mathbb{N}}\bigcup_{i=1}^{n-1}\{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - i]\rangle \mid \bigwedge_{j=0}^{i-1}\sigma(\mathsf{x}) \neq j\} \qquad \text{⟅def. } \cup\text{⟆}$$

$$= \{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \bigcup_{i>0}\{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - i]\rangle \mid \sigma(\mathsf{x}) \notin [0, i-1]\}$$

— It follows that for $\mathsf{S}_3 \triangleq \texttt{while (x!=0) \{ }\mathsf{S}_2\texttt{ x=x-1; \}}$, we have

$\llbracket \mathsf{S}_3 \rrbracket_e^{\varrho}$

$= \mathsf{lfp}^{\subseteq}\, \overleftarrow{F}_e^{\varrho} \fatsemi^{\varrho} (\llbracket \neg\mathsf{B} \rrbracket_e^{\varrho} \cup \llbracket \mathsf{B}\,;\mathsf{S} \rrbracket_b^{\varrho})$ ≀by (9) with $\mathsf{B} = \texttt{(x!=0)}$, $\neg\mathsf{B} = \texttt{(x=0)}$, and $\mathsf{S} = \mathsf{S}_2\ \texttt{x=x-1;}$⟆

$= (\{\langle\sigma, \sigma\rangle \mid \sigma \in \Sigma\} \cup \bigcup_{i>0} \{\langle\sigma, \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - i]\rangle \mid \sigma(\mathsf{x}) \notin [0, i-1]\}) \fatsemi^{\varrho} (\{\langle\sigma, \sigma\rangle \mid \sigma(\mathsf{x}) = 0\} \cup \varnothing)$

$= (\{\langle\sigma, \sigma\rangle \mid \sigma \in \Sigma\} \fatsemi^{\varrho} \{\langle\sigma, \sigma\rangle \mid \sigma(\mathsf{x}) = 0\}) \cup (\bigcup_{i>0} \{\langle\sigma, \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - i]\rangle \mid \sigma(\mathsf{x}) \notin [0, i-1]\} \fatsemi^{\varrho}$
$(\{\langle\sigma, \sigma\rangle \mid \sigma(\mathsf{x}) = 0\}))$ ≀by (24), $\fatsemi^{\varrho}$ left preserves joins⟆

$= \{\langle\sigma, \sigma\rangle \mid \sigma(\mathsf{x}) = 0\} \cup (\bigcup_{i>0} \{\langle\sigma, \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - i]\rangle \mid \sigma(\mathsf{x}) \notin [0, i-1] \wedge \sigma(\mathsf{x}) - i = 0\})$
≀def. (23) of $\fatsemi^{\varrho}$⟆

$= \{\langle\sigma, \sigma\rangle \mid \sigma(\mathsf{x}) = 0\} \cup \{\langle\sigma, \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow 0]\rangle \mid \sigma(\mathsf{x}) > 0\}$ ≀simplification⟆

— Then, for $\mathsf{S}_4 = \texttt{x=[-oo,oo]; }\mathsf{S}_3$, we have

$\llbracket \mathsf{S}_4 \rrbracket_e^{\varrho}$

$= \llbracket \texttt{x=[-oo,oo];} \rrbracket_e^{\varrho} \fatsemi^{\varrho} \llbracket \mathsf{S}_3 \rrbracket_e^{\varrho}$ ≀(4)⟆

$= \{\langle\sigma, \sigma[\mathsf{x} \leftarrow n]\rangle \mid n \in \mathbb{N}\} \fatsemi^{\varrho} (\{\langle\sigma, \sigma\rangle \mid \sigma(\mathsf{x}) = 0\} \cup \{\langle\sigma, \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow 0]\rangle \mid \sigma(\mathsf{x}) > 0\})$
≀(3) and as previously shown⟆

$= \{\langle\sigma, \sigma[\mathsf{x} \leftarrow n]\rangle \mid n \in \mathbb{N}\} \fatsemi^{\varrho} \{\langle\sigma, \sigma\rangle \mid \sigma(\mathsf{x}) = 0\} \cup \{\langle\sigma, \sigma[\mathsf{x} \leftarrow n]\rangle \mid n \in \mathbb{N}\} \fatsemi^{\varrho} \{\langle\sigma, \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow 0]\rangle \mid$
$\sigma(\mathsf{x}) > 0\}$ ≀by (24), $\fatsemi^{\varrho}$ left preserves joins⟆

$= \{\langle\sigma, \sigma[\mathsf{x} \leftarrow n]\rangle \mid \sigma[\mathsf{x} \leftarrow n](\mathsf{x}) = 0\} \cup \{\langle\sigma, \sigma[\mathsf{x} \leftarrow n][\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow 0]\rangle \mid \sigma[\mathsf{x} \leftarrow n](\mathsf{x}) > 0\}$
≀def. (23) of $\fatsemi^{\varrho}$⟆

$= \{\langle\sigma, \sigma[\mathsf{x} \leftarrow n]\rangle \mid n = 0\} \cup \{\langle\sigma, \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow 0]\rangle \mid n > 0\}$ ≀function application⟆

$= \{\langle\sigma, \sigma[\mathsf{x} \leftarrow 0]\rangle \mid \sigma \in \Sigma\} \cup \{\langle\sigma, \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow 0]\rangle \mid \sigma \in \Sigma\}$ ≀simplification⟆

— The iteration $\mathsf{S}_3 = \texttt{while (x!=0) \{ }\mathsf{S}_2\texttt{ x=x-1; \}}$ may iterate for ever. To show this, we have, by (7), that

$F_{\perp}^{\varrho}$ ≀for $\mathsf{S}_3 = \texttt{while (x!=0) \{ }\mathsf{S}_2\texttt{ x=x-1; \}}$⟆

$= \boldsymbol{\lambda} X \in \mathbb{L}_{\infty}^{\varrho} \bullet \llbracket \texttt{x!=0;}\mathsf{S}_2\texttt{ x=x-1;} \rrbracket_e^{\varrho} \fatsemi^{\varrho} X$

$= \boldsymbol{\lambda} X \in \mathbb{L}_{\infty}^{\varrho} \bullet \{\langle\sigma, \sigma\rangle \mid \sigma(\mathsf{x}) \neq 0\} \fatsemi^{\varrho} \{\langle\sigma, \sigma[\mathsf{y} \leftarrow 0]\rangle \mid \sigma \in \Sigma\} \fatsemi^{\varrho} \{\langle\sigma, \sigma[\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1]\rangle \mid \sigma \in \Sigma\} \fatsemi^{\varrho} X$
≀(4), (3), def. $\llbracket \mathsf{S}_2 \rrbracket_e^{\varrho}$ in ex. 5.1⟆

$= \boldsymbol{\lambda} X \in \mathbb{L}_{\infty}^{\varrho} \bullet \{\langle\sigma, \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma[\mathsf{y} \leftarrow 0](\mathsf{x}) - 1]\rangle \mid \sigma(\mathsf{x}) \neq 0\} \fatsemi^{\varrho} X$ ≀def. (23) of $\fatsemi^{\varrho}$⟆

$= \boldsymbol{\lambda} X \in \mathbb{L}_{\infty}^{\varrho} \bullet \{\langle\sigma, \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1]\rangle \mid \sigma(\mathsf{x}) \neq 0\} \fatsemi^{\varrho} X$ ≀simplification since $\mathsf{x} \neq \mathsf{y}$⟆

— By (24) and (5), $F_{\perp}^{\varrho}$ for $\mathsf{S}_3 = \texttt{while (x!=0) \{ }\mathsf{S}_2\texttt{ x=x-1; \}}$ converges at ω so that the infinite iterates $\langle X^i,\ i \leqslant \omega\rangle$ of $\llbracket \mathsf{S}_3 \rrbracket_{li}^{\varrho} = \mathsf{gfp}^{\subseteq}\, F_{\perp}^{\varrho}$ are as follows

$X^0 = \Sigma \times \{\perp\}$

$X^1 = \{\langle\sigma, \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1]\rangle \mid \sigma(\mathsf{x}) \neq 0\} \fatsemi^{\varrho} X^0$ ≀def. iterates and $F_{\perp}^{\varrho}$⟆

$\quad = \{\langle\sigma, \perp\rangle \mid \sigma(\mathsf{x}) \neq 0\}$ ≀def. (23) of $\fatsemi^{\varrho}$ and X^0⟆

$X^2 = \{\langle\sigma, \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1]\rangle \mid \sigma(\mathsf{x}) \neq 0\} \fatsemi^{\varrho} X^1$ ≀def. iterates and $F_{\perp}^{\varrho}$⟆

$\quad = \{\langle\sigma, \perp\rangle \mid \sigma(\mathsf{x}) \neq 0 \wedge \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1](\mathsf{x}) \neq 0\}$ ≀def. (23) of $\fatsemi^{\varrho}$ and X^1⟆

$\quad = \{\langle\sigma, \perp\rangle \mid \sigma(\mathsf{x}) \neq 0 \wedge \sigma(\mathsf{x}) \neq 1\}$ ≀function application and simplification⟆

$$
\begin{aligned}
X^{n} &= \{\langle\sigma,\ \bot\rangle \mid \bigwedge_{i=0}^{n-1} \sigma(\mathsf{x}) \neq i\} && \lbag\text{induction hypothesis}\rbag \\
X^{n+1} &= \{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1]\rangle \mid \sigma(\mathsf{x}) \neq 0\} \fatsemi^{\varrho} X^{n} && \lbag\text{def. iterates and } F^{\varrho}_{\bot}\rbag \\
&= \{\langle\sigma,\ \bot\rangle \mid \sigma(\mathsf{x}) \neq 0 \wedge \bigwedge_{i=0}^{n-1} \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - 1](\mathsf{x}) \neq i\} && \lbag\text{def. (23) of } \fatsemi^{\varrho} \text{ and } X^{n}\rbag \\
&= \{\langle\sigma,\ \bot\rangle \mid \bigwedge_{i=0}^{(n+1)-1} \sigma(\mathsf{x}) \neq i\} && \lbag\text{simplification}\rbag
\end{aligned}
$$

— By recurrence, $X^{n} = \{\langle\sigma,\ \bot\rangle \mid \bigwedge_{i=0}^{n-1} \sigma(\mathsf{x}) \neq i\}$, so that, by convergence at ω, the greatest fixpoint is

$$
\begin{aligned}
&\llbracket \mathsf{S}_3 \rrbracket^{\varrho}_{li} \ = \ \mathsf{gfp}^{\subseteq} F^{\varrho}_{\bot} \\
=\ & \bigcap_{n\in\mathbb{N}} X^{n} && \lbag\text{def. iterates}\rbag \\
=\ & \bigcap_{n\in\mathbb{N}} \{\langle\sigma,\ \bot\rangle \mid \bigwedge_{i=0}^{n-1} \sigma(\mathsf{x}) \neq i\} \\
=\ & \{\langle\sigma,\ \bot\rangle \mid \sigma(\mathsf{x}) < 0\} && \lbag\Sigma = \{\mathsf{x},\mathsf{y}\} \rightarrow \mathbb{Z}\rbag
\end{aligned}
$$

— The iteration S_3 = `while (x!=0) {` S_2 `x=x-1; }` may also not terminate because of the non-termination of S_2 in its body. The loop body S_2 `x=x-1;` may not terminate, as follows.

$$
\begin{aligned}
&\llbracket \mathsf{S}_2\ \ \mathtt{x=x-1;} \rrbracket^{\varrho}_{\bot} \\
=\ & \llbracket \mathsf{S}_2 \rrbracket^{\varrho}_{\bot} \cup (\llbracket \mathsf{S}_2 \rrbracket^{\varrho}_{e} \fatsemi^{\varrho} \llbracket \mathtt{x=x-1;} \rrbracket^{\varrho}_{\bot}) && \lbag(4)\rbag \\
=\ & \llbracket \mathsf{S}_2 \rrbracket^{\varrho}_{\bot} && \lbag\text{def. (23) of } \fatsemi^{\varrho} \text{ and (3) so that } \llbracket \mathtt{x=x-1;} \rrbracket^{\varrho}_{\bot} = \emptyset\rbag \\
=\ & \{\langle\sigma,\ \bot\rangle \mid \sigma \in \Sigma\} && \lbag\text{by example 5.1}\rbag
\end{aligned}
$$

This implies that

$$
\begin{aligned}
&\llbracket \mathtt{x!=0;}\ \ \mathsf{S}_2\ \ \mathtt{x=x-1;} \rrbracket^{\varrho}_{\bot} \\
=\ & \{\langle x,\ \bot\rangle \mid \langle x,\ \bot\rangle \in \llbracket \mathtt{x!=0;} \rrbracket^{\varrho}_{\bot}\} \cup \{\langle x,\ y\rangle \mid \exists z \in \Sigma\ .\ \langle x,\ z\rangle \in \llbracket \mathtt{x!=0;} \rrbracket^{\varrho}_{e} \wedge \langle z,\ y\rangle \in \llbracket \mathsf{S}_2\ \ \mathtt{x=x-1;} \rrbracket^{\varrho}_{\bot}\} \\
& && \lbag\text{(4) and def. of (23)}\rbag \\
=\ & \{\langle\sigma,\ \bot\rangle \mid \sigma(\mathsf{x}) \neq 0\} && \lbag(3)\rbag
\end{aligned}
$$

It follows that

$$
\begin{aligned}
&\llbracket \mathsf{S}_3 \rrbracket^{\sharp}_{bi} \\
\triangleq\ & (\mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\ \overleftarrow{F}^{\sharp}_{e}) \fatsemi^{\sharp} \llbracket \mathsf{B};\mathsf{S} \rrbracket_{\bot} && \lbag\text{(10) with } \mathsf{B} = \mathtt{x!=0} \text{ and } \mathsf{S} = \mathsf{S}_2\ \ \mathtt{x=x-1;}\rbag \\
=\ & (\{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \cup \bigcup_{i>0} \{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - i]\rangle \mid \sigma(\mathsf{x}) \notin [0, i-1]\}) \fatsemi^{\sharp} \{\langle\sigma,\ \bot\rangle \mid \sigma(\mathsf{x}) \neq 0\} \\
& && \lbag\text{previous evaluation of } \mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\ \overleftarrow{F}^{\sharp}_{e} \text{ and } \llbracket \mathtt{x!=0;}\ \ \mathsf{S}_2\ \ \mathtt{x=x-1;} \rrbracket^{\varrho}_{\bot}\rbag \\
=\ & (\{\langle\sigma,\ \sigma\rangle \mid \sigma \in \Sigma\} \fatsemi^{\sharp} \{\langle\sigma,\ \bot\rangle \mid \sigma(\mathsf{x}) \neq 0\}) \cup \bigcup_{i>0} (\{\langle\sigma,\ \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - i]\rangle \mid \sigma(\mathsf{x}) \notin [0, i-1]\} \fatsemi^{\sharp} \\
& \{\langle\sigma,\ \bot\rangle \mid \sigma(\mathsf{x}) \neq 0\}) && \lbag\fatsemi^{\varrho} \text{ left preserves joins } \cup \text{ on } \wp(\Sigma \times \Sigma_{\bot})\rbag \\
=\ & \{\langle\sigma,\ \bot\rangle \mid \sigma(\mathsf{x}) \neq 0\} \cup \bigcup_{i>0} (\{\langle\sigma,\ \bot\rangle \mid \sigma(\mathsf{x}) \notin [0, i-1] \wedge \sigma[\mathsf{y} \leftarrow 0][\mathsf{x} \leftarrow \sigma(\mathsf{x}) - i](\mathsf{x}) \neq 0\}) \\
& && \lbag\text{def. (23) of } \fatsemi^{\varrho}\rbag \\
=\ & \{\langle\sigma,\ \bot\rangle \mid \sigma(\mathsf{x}) \neq 0\} \cup \bigcup_{i>0} (\{\langle\sigma,\ \bot\rangle \mid \sigma(\mathsf{x}) \notin [0, i-1] \wedge \sigma(\mathsf{x}) \neq i\}) && \lbag\text{function application}\rbag \\
=\ & \{\langle\sigma,\ \bot\rangle \mid \sigma(\mathsf{x}) \neq 0\} && \lbag\text{simplification}\rbag
\end{aligned}
$$

— The nonterminating behavior $\llbracket \mathsf{S}_3 \rrbracket^\sharp_\bot$ of the iteration S_3 = `while (x!=0) { S`$_2$` x=x-1; }` is defined, by (11), to be either due to the nontermination $\llbracket \mathsf{S}_3 \rrbracket^\sharp_{bi}$ of its body or infinite iteration $\llbracket \mathsf{S}_3 \rrbracket^\sharp_{li}$.

$$
\begin{array}{ll@{\qquad}r}
& \llbracket \mathsf{S}_3 \rrbracket^\sharp_\bot & \\
\triangleq & \llbracket \mathsf{S}_3 \rrbracket^\sharp_{bi} \cup \llbracket \mathsf{S}_3 \rrbracket^\sharp_{li} & \lbag (11) \text{ and } \sqcup^\sharp_\infty = \cup \rbag \\
= & \{\langle \sigma,\ \bot \rangle \mid \sigma(\mathtt{x}) \neq 0\} \cup \{\langle \sigma,\ \bot \rangle \mid \sigma(\mathtt{x}) < 0\} & \lbag \text{as previously shown} \rbag \\
= & \{\langle \sigma,\ \bot \rangle \mid \sigma(\mathtt{x}) \neq 0\} & \lbag \text{simplification} \rbag
\end{array}
$$

— The nonterminating behavior $\llbracket \mathsf{S}_4 \rrbracket^\sharp_\bot$ of the iteration $\mathsf{S}_4 = \triangleq$ `x=[-oo,oo];` S_3 is now

$$
\begin{array}{ll@{\qquad}r}
& \llbracket \mathsf{S}_4 \rrbracket^\sharp_\bot & \\
= & \llbracket \mathtt{x=[-oo,oo];} \rrbracket^\sharp_\bot \cup (\llbracket \mathtt{x=[-oo,oo];} \rrbracket^\sharp_e \fatsemi^\sharp \llbracket \mathsf{S}_3 \rrbracket^\sharp_\bot) & \lbag (4) \rbag \\
= & \{\langle \sigma,\ \sigma[\mathtt{x} \leftarrow n] \rangle \mid n \in \mathbb{N}\} \fatsemi^\sharp \{\langle \sigma,\ \bot \rangle \mid \sigma(\mathtt{x}) \neq 0\} & \lbag (3) \rbag \\
= & \{\langle x,\ y \rangle \mid \exists z \in \Sigma \mathrel{.} \langle x,\ z \rangle \in \{\langle \sigma,\ \sigma[\mathtt{x} \leftarrow n] \rangle \mid n \in \mathbb{N}\} \wedge \langle z,\ y \rangle \in \{\langle \sigma',\ \bot \rangle \mid \sigma'(\mathtt{x}) \neq 0\}\} & \lbag \text{def. (23) of } \fatsemi^\varrho \rbag \\
= & \{\langle \sigma,\ \bot \rangle \mid \exists n \in \mathbb{N} \mathrel{.} \sigma[\mathtt{x} \leftarrow n](\mathtt{x}) \neq 0\} & \lbag z = \sigma[\mathtt{x} \leftarrow n] \rbag \\
= & \{\langle \sigma,\ \bot \rangle \mid \sigma \in \Sigma\} & \lbag \text{simplification} \rbag
\end{array}
$$

Grouping all cases together according to (12), we get $\llbracket \mathsf{S}_3 \rrbracket^\sharp = \langle e : \llbracket \mathsf{S}_3 \rrbracket^\sharp_e,\ \bot : \llbracket \mathsf{S}_3 \rrbracket^\sharp_\bot,\ br : \llbracket \mathsf{S}_3 \rrbracket^\sharp_b \rangle = \langle e : \{\langle \sigma,\ \sigma \rangle \mid \sigma(\mathtt{x}) = 0\} \cup \{\langle \sigma,\ \sigma[\mathtt{y} \leftarrow 0][\mathtt{x} \leftarrow 0] \rangle \mid \sigma(\mathtt{x}) > 0\},\ \bot : \{\langle \sigma,\ \bot \rangle \mid \sigma(\mathtt{x}) \neq 0\},\ br : \varnothing \rangle$ and $\llbracket \mathsf{S}_4 \rrbracket^\sharp = \langle e : \llbracket \mathsf{S}_4 \rrbracket^\sharp_e,\ \bot : \llbracket \mathsf{S}_4 \rrbracket^\sharp_\bot,\ br : \llbracket \mathsf{S}_4 \rrbracket^\sharp_b \rangle = \langle e : \{\langle \sigma,\ \sigma[\mathtt{x} \leftarrow 0] \rangle \mid \sigma \in \Sigma\} \cup \{\langle \sigma,\ \sigma[\mathtt{y} \leftarrow 0][\mathtt{x} \leftarrow 0] \rangle \mid \sigma \in \Sigma\},$ $\bot : \{\langle \sigma,\ \bot \rangle \mid \sigma \in \Sigma\},\ br : \varnothing \rangle$, proving example 5.2. □

6 Algebraic Program Execution Properties

6.1 Algebraic Execution Properties

Traditionally, logics involve two formal languages, one to express programs and another one to express properties of the program executions. The syntax and semantics of these programming and logic languages are considered to be different. Therefore, in addition to the program syntax and semantics, this traditional approach requires to define the syntax and semantics of the logic expressing program properties.

A semantics $\llbracket \mathsf{S} \rrbracket^\sharp \in \mathbb{L}^\sharp$ in (12) is an abstraction of a property of the executions of the statement S. Therefore $\mathbb{L}^\sharp$ will be the domain of execution properties whether used to describe the semantics or logic properties of programs executions. This will avoid us the necessary traditional distinction between programs semantics and program properties.

This idea follows [52–54]'s slogan that "Programs are predicates" and define properties of program executions as programs (which semantics is already defined). It is also found in Dexter Kozen's Kleene algebra with tests [62, 63, 82]. Therefore, from an abstract point of view, program execution specification and verification need nothing more than programs and an associated calculus $\mathsf{post}^\sharp$ on programs.

6.2 The Algebraic Program Execution Property Transformer

Let us define the transformer $\mathsf{post}^\sharp \in \mathbb{L}^\sharp \xrightarrow{\nearrow} \mathbb{L}^\sharp \xrightarrow{\nearrow} \mathbb{L}^\sharp$ such that

$$\mathsf{post}^\sharp(S)P \quad \triangleq \quad P \fatsemi^\sharp S \tag{25}$$

where S is a semantics in $\mathbb{L}^\sharp$ as defined by (12) and $\fatsemi^\sharp$ is defined by (15). If P is a precondition when at S then $\mathsf{post}^\sharp \llbracket \mathsf{S} \rrbracket^\sharp P$ is the postcondition after S (including when breaking out of S).

For example, using the shorthand (14), $\mathsf{post}^\sharp(S)\mathsf{init}^\sharp = S$ by 3.2.D.a and $\mathsf{post}^\sharp(S)P = P$ for all $P \in \mathbb{L}^\sharp_\infty$ by 3.2.D.c.

In definition (25) of "predicate transformers" the meaning of "predicates" about programs executions is abstracted away as programs specifying executions. Further abstractions will yield the classic understanding of "predicates", "abstract property", etc. The classic Galois connections post–$\widetilde{\mathsf{pre}}$ [20, (12.22)] and post–post^{-1} [20, (12.6)] are still valid with this different definition of post.

The following lemmas show that the post transformer inherits the properties of sequential composition. It applies e.g. to $\langle\mathbb{L}^{\sharp}_{+},\ \sqsubseteq^{\sharp}_{+}\rangle$ in 3.2.A, $\langle\mathbb{L}^{\sharp}_{\infty},\ \sqsubseteq^{\sharp}_{\infty}\rangle$ in 3.2.C, or $\langle\mathbb{L}^{\sharp},\ \sqsubseteq^{\sharp}\rangle$ in (12).

Lemma 6.1. *Let $\langle L, \sqsubseteq, \sqcup\rangle$ be a poset with partially defined join $\sqcup$. Let $\fatsemi$ be the sequential composition on L. If $\fatsemi$ left-satisfies any one of the properties of definition 2.2 or their dual then for all $S \in \mathbb{L}$, $\mathsf{post}(S)$ satisfies the same property.*

Proof of lemma 6.1. Let $\langle P_i,\ i \in \Delta\rangle$ be a family of elements of L such that $\Delta = \{0, 1\}$ with $P_0 \sqsubseteq P_1$ for the left-increasingness hypothesis (def. 2.2.i), Δ is finite for the existing finite $\sqcup$ left preserving hypothesis (def. 2.2.ii), $\Delta \in \mathbb{O}$ and $\langle P_i,\ i \in \Delta\rangle$ is an increasing chain for the left upper-continuity hypothesis (def. 2.2.iii), Δ is an arbitrary set for the existing join left preservation property (def. 2.2.iv), possibly empty in case of left strictness (def. 2.2.vi). The proof is similar in all of these cases, as follows

$$\begin{array}{ll}
\quad \mathsf{post}(S)(\bigsqcup_{i\in\Delta} P_i) & \\
\Leftrightarrow\ (\bigsqcup_{i\in\Delta} P_i) \fatsemi S & \text{⟅def. (25) of post⟆} \\
\Leftrightarrow\ \bigsqcup_{i\in\Delta}(P_i \fatsemi S) & \text{⟅by the left preservation hypothesis for } \fatsemi\text{⟆} \\
\Leftrightarrow\ \bigsqcup_{i\in\Delta} \mathsf{post}(S)P_i & \text{⟅def. (25) of post⟆} \quad \square
\end{array}$$

The following Galois connection shows the equivalence of forward/deductive and backward/abductive reasonings on the program semantics.

Lemma 6.2. *If $\langle L, \sqsubseteq, \sqcup\rangle$ is a poset and the sequential composition $\fatsemi$ is existing $\sqcup$ left preserving then we have the Galois connection*

$$\forall S \in \mathbb{L}\ .\ \langle\mathbb{L},\ \sqsubseteq\rangle \mathrel{\underset{\mathsf{post}(S)}{\overset{\widetilde{\mathsf{pre}}(S)}{\leftrightarrows}}} \langle\mathbb{L},\ \sqsubseteq\rangle \quad \textit{where} \quad \widetilde{\mathsf{pre}}(S)Q \triangleq \bigsqcup\{P \in \mathbb{L} \mid \mathsf{post}(S)P \sqsubseteq Q\}\big). \qquad (26)$$

Proof of lemma 26. By lemma 6.1, $\mathsf{post}(S)$ preserves existing joins. It is the therefore the lower adjoint of a Galois connection [20, exercise 11.39]. $\widetilde{\mathsf{pre}}(S)$ is its unique upper adjoint [20, exercise 11.39]. □

Lemma 6.3. *Let $\langle L, \sqsubseteq, \sqcup\rangle$ be a poset with partially defined join $\sqcup$. Let $\fatsemi$ be the sequential composition on L. If $\fatsemi$ right-satisfies any one of the properties of definition 2.2 or their dual then* post *satisfies the same property.*

Proof of lemma 6.3. Let $\langle P_i,\ i \in \Delta\rangle$ be a family of elements of L such that $\Delta = \{0, 1\}$ with $P_0 \sqsubseteq P_1$ for the right-increasingness hypothesis (def. 2.2.i), Δ is finite for the existing finite $\sqcup$ right preserving hypothesis (def. 2.2.ii), $\Delta \in \mathbb{O}$ and $\langle P_i,\ i \in \Delta\rangle$ is an increasing chain for the right upper-continuity hypothesis (def. 2.2.iii), Δ is an arbitrary set for the existing join right preservation property (def. 2.2.iv), possibly empty in case of right strictness (def. 2.2.vi). The proof is similar in all of these cases, as follows

$$\begin{array}{ll}
\quad \mathsf{post}(\bigsqcup_{i\in\Delta} S_i) & \\
= \boldsymbol{\lambda} P \bullet \mathsf{post}(\bigsqcup_{i\in\Delta} S_i)P & \text{⟅function application⟆} \\
= \boldsymbol{\lambda} P \bullet P \fatsemi (\bigsqcup_{i\in\Delta} S_i) & \text{⟅def. (25) of post⟆} \\
= \boldsymbol{\lambda} P \bullet \bigsqcup_{i\in\Delta}(P \fatsemi S_i) & \text{⟅by the right preservation hypothesis for } \fatsemi\text{⟆}
\end{array}$$

$= \boldsymbol{\lambda} P \bullet \bigsqcup_{i\in\Delta} \text{post}(S_i)P$ $\qquad\wr\text{def. (25) of post}\int$

$= \bigsqcup_{i\in\Delta} \text{post}(S_i)$ $\qquad\wr\text{pointwise def. of }\bigsqcup\int$ □

The following Galois connection formalizes Dijkstra's program inversion [36].

Lemma 6.4. *If $\langle L, \sqsubseteq, \sqcup\rangle$ is a poset and the sequential composition $\fatsemi$ is existing $\sqcup$ right preserving then we have the following Galois connection ($\mathbb{L} \xrightarrow{\sqcup} \mathbb{L}$ is the set of existing join preserving operators on $\mathbb{L}$ and $\dot{\sqsubseteq}$ is the pointwise extension of $\sqsubseteq$)*

$$\langle \mathbb{L}, \sqsubseteq\rangle \underset{\text{post}}{\overset{\text{post}^{-1}}{\leftrightarrows}} \langle \mathbb{L} \xrightarrow{\sqcup} \mathbb{L}, \dot{\sqsubseteq}\rangle \quad \textit{where} \quad \text{post}^{-1}(T) = \bigsqcup\{S \in \mathbb{L} \mid \text{post}(S) \mathrel{\dot{\sqsubseteq}} T\}. \tag{27}$$

Proof of lemma 6.4. By lemma 6.3, post preserves existing joins. It is the therefore the lower adjoint of a Galois connection [20, exercise 11.39]. post is its unique upper adjoint [20, exercise 11.39]. □

6.3 A Calculus of Algebraic Program Execution Properties

We derive the sound and complete $\text{post}^\sharp$ calculus by calculational design, as follows.

Theorem 6.5 (Program execution property calculus). *If $\mathbb{D}^\sharp$ is a well-defined increasing and decreasing chain-complete join semilattice with right upper continuous sequential composition $\fatsemi^\sharp$ then*

$$\begin{aligned}
\text{post}^\sharp\llbracket\texttt{x = A}\rrbracket^\sharp P &= \langle e : P_+ \fatsemi^\sharp \text{assign}^\sharp\llbracket\texttt{x},\texttt{A}\rrbracket,\ \bot : P_\infty,\ br : P_{br}\rangle && (28)\\
\text{post}^\sharp\llbracket\texttt{x = [}a\texttt{, }b\texttt{]}\rrbracket^\sharp P &= \langle e : P_+ \fatsemi^\sharp \text{rassign}^\sharp\llbracket\texttt{x}, a, b\rrbracket,\ \bot : P_\infty,\ br : P_{br}\rangle && (29)\\
\text{post}^\sharp\llbracket\texttt{skip}\rrbracket^\sharp P &= \langle e : P_+ \fatsemi^\sharp \text{skip}^\sharp,\ \bot : P_\infty,\ br : P_{br}\rangle && (30)\\
\text{post}^\sharp\llbracket\texttt{B}\rrbracket^\sharp P &= \langle e : P_+ \fatsemi^\sharp \text{test}^\sharp\llbracket\texttt{B}\rrbracket,\ \bot : P_\infty,\ br : P_{br}\rangle && (31)\\
\text{post}^\sharp\llbracket\texttt{break}\rrbracket^\sharp P &= \langle e : \bot^\sharp_+,\ \bot : P_\infty,\ br : P_{br} \sqcup^\sharp_+ (P_e \fatsemi^\sharp \text{break}^\sharp)\rangle && (32)\\
\text{post}^\sharp\llbracket\texttt{S}_1\texttt{;S}_2\rrbracket^\sharp P &= \text{post}^\sharp\llbracket\texttt{S}_2\rrbracket^\sharp(\text{post}^\sharp\llbracket\texttt{S}_1\rrbracket^\sharp P) && (33)\\
\text{post}^\sharp\llbracket\texttt{if (B) S}_1\texttt{ else S}_2\rrbracket^\sharp P &= \text{post}^\sharp\llbracket\texttt{B;S}_1\rrbracket^\sharp P \sqcup^\sharp \text{post}^\sharp\llbracket\neg\texttt{B;S}_2\rrbracket^\sharp P && (34)\\
\vec{F}^\sharp_{pe} &\triangleq \boldsymbol{\lambda} P \bullet \boldsymbol{\lambda} X \bullet \text{post}^\sharp(\text{init}^\sharp)P \sqcup^\sharp_+ \text{post}^\sharp(\llbracket\texttt{B;S}\rrbracket^\sharp_e)(X) && (35)\\
F^\sharp_{p\bot} &\triangleq \boldsymbol{\lambda} X \bullet \text{post}^\sharp(X)(\llbracket\texttt{B;S}\rrbracket^\sharp_e) && (36)\\
\text{post}^\sharp\llbracket\texttt{while (B) S}\rrbracket^\sharp P &= \langle ok : \langle e : \text{post}^\sharp(\llbracket\neg\texttt{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket\texttt{B;S}\rrbracket^\sharp_b)(\text{lfp}^{\sqsubseteq^\sharp_+}(\vec{F}^\sharp_{pe}(P))), && (37)\\
&\qquad\qquad \bot : \text{post}^\sharp(\llbracket\texttt{B;S}\rrbracket^\sharp_\bot)(\text{lfp}^{\sqsubseteq^\sharp_+}(\vec{F}^\sharp_{pe}(P))) \sqcup^\sharp_\infty\\
&\qquad\qquad\qquad\qquad \text{post}^\sharp(\text{gfp}^{\sqsubseteq^\sharp_\infty} F^\sharp_{p\bot})P\ \rangle,\\
&\quad br : P_{br}\rangle
\end{aligned}$$

is sound and complete.

To prove theorem 6.5, we need preliminary lemmas.

Lemma 6.6. *If $\mathbb{D}^\sharp_+$ is a well-defined increasing chain-complete join semilattice with sequential composition $\fatsemi^\sharp$ that is existing $\sqcup$ right preserving and upper continuous in both arguments then* $\text{post}^\sharp(\text{lfp}^{\sqsubseteq^\sharp_+} \vec{F}^\sharp_e)P = \text{lfp}^{\sqsubseteq^\sharp_+}(\vec{F}^\sharp_{pe}(P))$.

Proof of 6.6. By lemma 3.6, $\vec{F}^\sharp_e$ is increasing so that the transfinite iterates $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ of $\vec{F}^\sharp_e$ from $\bot^\sharp_+$ from an increasing chain which is ultimately stationary at rank ϵ so that $\text{lfp}^{\sqsubseteq^\sharp_+} \vec{F}^\sharp_e = X^\epsilon$ [23].

– We have $\text{post}^\sharp(X^0) = \text{post}^\sharp(\bot^\sharp_+) = \boldsymbol{\lambda} P \bullet P \fatsemi^\sharp \bot^\sharp_+ = \boldsymbol{\lambda} P \bullet \bot^\sharp_+$ by def. (25) of $\text{post}^\sharp$ and $\forall S \in \mathbb{L}^\sharp_+ \,.\, S \fatsemi^\sharp \bot^\sharp_+ = \bot^\sharp_+$ in definition 3.2.D.a.

– Let us prove commutation of $\vec{F}^\sharp_e$ and $\boldsymbol{\lambda} P \bullet \vec{F}^\sharp_{pe}(P)$ for the abstraction $\text{post}^\sharp$ of the iterates.

$$\begin{aligned}
&\text{post}^\sharp(\vec{F}^\sharp_e(X^\delta))\\
={}& \boldsymbol{\lambda} P \bullet \text{post}^\sharp(\vec{F}^\sharp_e(X^\delta))P && \wr\text{def. function application}\int\\
={}& \boldsymbol{\lambda} P \bullet \text{post}^\sharp(\text{init}^\sharp \sqcup^\sharp_+ (X^\delta \fatsemi^\sharp \llbracket \mathtt{B;S} \rrbracket^\sharp_e))P && \wr\text{def. (6) of } \vec{F}^\sharp_e\int\\
={}& \boldsymbol{\lambda} P \bullet \text{post}^\sharp(\text{init}^\sharp)P \sqcup^\sharp_+ \text{post}^\sharp(\llbracket \mathtt{B;S} \rrbracket^\sharp_e)(\text{post}^\sharp(X^\delta)P)\\
& && \wr\text{post}^\sharp \text{ is existing join preserving by hypothesis on } \fatsemi^\sharp \text{ and lemma 6.1}\int\\
={}& \boldsymbol{\lambda} P \bullet \vec{F}^\sharp_{pe}(P)(\text{post}^\sharp(X^\delta)) && \wr\text{def. (35) of } \vec{F}^\sharp_{pe}\int
\end{aligned}$$

We conclude by continuity and [20, th. 18.26]. □

Note that if $\text{post}^\sharp$ is simply increasing, we have an over approximation.

Lemma 6.7. *If $\mathbb{D}^\sharp$ is well-defined decreasing chain-complete lattice and the sequential composition $\fatsemi^\sharp$ is right lower continuous then* $\text{post}^\sharp(\text{gfp}^{\sqsubseteq^\sharp_\infty} F^\sharp_\bot) = \text{post}^\sharp(\text{gfp}^{\sqsubseteq^\sharp_\infty} F^\sharp_{p\bot})$.

Proof of (6.7). Let us prove commutation for the iterates $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ of $\text{gfp}^{\sqsubseteq^\sharp_\infty} F^\sharp_\bot$.

$$\begin{aligned}
&\text{post}^\sharp(F^\sharp_\bot(X^\delta))\\
={}& \boldsymbol{\lambda} P \bullet \text{post}^\sharp(F^\sharp_\bot(X^\delta))P && \wr\text{function application}\int\\
={}& \boldsymbol{\lambda} P \bullet \text{post}^\sharp(\llbracket \mathtt{B;S} \rrbracket^\sharp_e \fatsemi^\sharp X^\delta)P && \wr\text{def. (7) of } F^\sharp_\bot\int\\
={}& \boldsymbol{\lambda} P \bullet P \fatsemi^\sharp (\llbracket \mathtt{B;S} \rrbracket^\sharp_e \fatsemi^\sharp X^\delta) && \wr\text{def. (25) of } \text{post}^\sharp\int\\
={}& \boldsymbol{\lambda} P \bullet (P \fatsemi^\sharp \llbracket \mathtt{B;S} \rrbracket^\sharp_e) \fatsemi^\sharp X^\delta && \wr \fatsemi^\sharp \text{ associative by definition 3.2.D}\int\\
={}& \boldsymbol{\lambda} P \bullet \text{post}^\sharp(X^\delta)(P \fatsemi^\sharp \llbracket \mathtt{B;S} \rrbracket^\sharp_e) && \wr\text{def. (25) of } \text{post}^\sharp\int\\
={}& \boldsymbol{\lambda} P \bullet \text{post}^\sharp(X^\delta)(\text{post}^\sharp(\llbracket \mathtt{B;S} \rrbracket^\sharp_e)P) && \wr\text{def. (25) of } \text{post}^\sharp\int\\
={}& \boldsymbol{\lambda} P \bullet F^\sharp_{p\bot}(\text{post}^\sharp(X^\delta))P && \wr\text{def. (36) of } F^\sharp_{p\bot}\int\\
={}& F^\sharp_{p\bot}(\text{post}^\sharp(X^\delta)) && \wr\text{function application}\int
\end{aligned}$$

By hypothesis, the sequential composition $\fatsemi^\sharp$ is right lower continuous, so that by lemma 6.4, $\text{post}^\sharp$ is lower continuous. By commutativity, we conclude by the dual of [20, th. 18.26]. □

Proof of theorem 6.5. The proof is by structural induction on the statement syntax.

$$\begin{aligned}
—\ &\text{post}^\sharp\llbracket \mathtt{x\ =\ A} \rrbracket^\sharp P\\
={}& P \fatsemi^\sharp \llbracket \mathtt{x\ =\ A} \rrbracket^\sharp && \wr\text{def. (25) of } \text{post}^\sharp\int\\
={}& P \fatsemi^\sharp \langle e : \text{assign}^\sharp\llbracket \mathtt{x,A} \rrbracket,\ \bot : \bot^\sharp_\infty,\ br : \bot^\sharp_+\rangle && \wr\text{(12) and (3)}\int\\
={}& \langle e : P_+ \fatsemi^\sharp \text{assign}^\sharp\llbracket \mathtt{x,A} \rrbracket,\ \bot : P_\infty \sqcup^\sharp_\infty (P_+ \fatsemi^\sharp \bot^\sharp_\infty),\ br : P_{br} \sqcup^\sharp_+ (P_+ \fatsemi^\sharp \bot^\sharp_+)\rangle && \wr\text{def. (15) of } \fatsemi^\sharp\int\\
={}& \langle e : P_+ \fatsemi^\sharp \text{assign}^\sharp\llbracket \mathtt{x,A} \rrbracket,\ \bot : P_\infty \sqcup^\sharp_\infty \bot^\sharp_\infty,\ br : P_{br} \sqcup^\sharp_+ \bot^\sharp_+\rangle\\
& && \wr \bot^\sharp_\infty \text{ and } \bot^\sharp_+ \text{ absorbent for } \fatsemi^\sharp \text{ by definition 3.2.D.c }\int\\
={}& \langle e : P_+ \fatsemi^\sharp \text{assign}^\sharp\llbracket \mathtt{x,A} \rrbracket,\ \bot : P_\infty,\ br : P_{br}\rangle && \wr\text{def. lub}\int
\end{aligned}$$

— The $\text{post}^\sharp$ transformers (29) for $\mathtt{x\ =\ [}a\mathtt{,\ }b\mathtt{]}$, (30) for $\mathtt{x\ =\ skip}$, and (31) for $\mathtt{B}$ are similar.

$$\begin{aligned}
—\ &\text{post}^\sharp\llbracket \mathtt{break} \rrbracket^\sharp P\\
={}& P \fatsemi^\sharp \llbracket \mathtt{break} \rrbracket^\sharp && \wr\text{def. (25) of } \text{post}^\sharp\int\\
={}& P \fatsemi^\sharp \langle e : \bot^\sharp_+,\ \bot : \bot^\sharp_\infty,\ br : \text{break}^\sharp\rangle && \wr\text{(12) and (3)}\int
\end{aligned}$$

$= \langle e: P_{+} \fatsemi^{\sharp} \bot^{\sharp}_{+},\ \bot: P_{\infty} \fatsemi^{\sharp} \bot^{\sharp}_{\infty},\ br: P_{br} \sqcup^{\sharp}_{+} (P_{e} \fatsemi^{\sharp} \mathsf{break}^{\sharp})\rangle$ ⟅def. (15) of $\fatsemi^{\sharp}$⟆

$= \langle e: \bot^{\sharp}_{+},\ \bot: P_{\infty},\ br: P_{br} \sqcup^{\sharp}_{+} (P_{e} \fatsemi^{\sharp} \mathsf{break}^{\sharp})\rangle$ ⟅definitions 3.2.D.c and 3.2.D.a⟆

— $\mathsf{post}^{\sharp}\llbracket \mathtt{S}_1\,\mathtt{;}\,\mathtt{S}_2 \rrbracket^{\sharp} P$

$= P \fatsemi^{\sharp} (\llbracket \mathtt{S}_1\,\mathtt{;}\,\mathtt{S}_2 \rrbracket^{\sharp})$ ⟅def. (25) of $\mathsf{post}^{\sharp}$⟆

$= P \fatsemi^{\sharp} (\llbracket \mathtt{S}_1 \rrbracket^{\sharp} \fatsemi^{\sharp} \llbracket \mathtt{S}_2 \rrbracket^{\sharp})$ ⟅def. (15) of $\fatsemi^{\sharp}$⟆

$= (P \fatsemi^{\sharp} \llbracket \mathtt{S}_1 \rrbracket^{\sharp}) \fatsemi^{\sharp} \llbracket \mathtt{S}_2 \rrbracket^{\sharp}$ ⟅$\fatsemi^{\sharp}$ associative by definition 3.23.2.D⟆

$= \mathsf{post}^{\sharp}\llbracket \mathtt{S}_2 \rrbracket^{\sharp}(P \fatsemi^{\sharp} \llbracket \mathtt{S}_1 \rrbracket^{\sharp})$ ⟅def. (25) of $\mathsf{post}^{\sharp}\llbracket \mathtt{S}_2 \rrbracket^{\sharp} Q \triangleq Q \fatsemi^{\sharp} \llbracket \mathtt{S}_2 \rrbracket^{\sharp}$⟆

$= \mathsf{post}^{\sharp}\llbracket \mathtt{S}_2 \rrbracket^{\sharp}(\mathsf{post}^{\sharp}\llbracket \mathtt{S}_1 \rrbracket^{\sharp} P)$ ⟅def. (25) of $\mathsf{post}^{\sharp}\llbracket \mathtt{S}_1 \rrbracket^{\sharp} P \triangleq P \fatsemi^{\sharp} \llbracket \mathtt{S}_1 \rrbracket^{\sharp}$⟆

— $\mathsf{post}^{\sharp}\llbracket \mathtt{if\ (B)\ S}_1\ \mathtt{else\ S}_2 \rrbracket^{\sharp} P$

$= P \fatsemi^{\sharp} \llbracket \mathtt{if\ (B)\ S}_1\ \mathtt{else\ S}_2 \rrbracket^{\sharp}$ ⟅def. (25) of $\mathsf{post}^{\sharp}$⟆

$= P \fatsemi^{\sharp} (\llbracket \mathtt{B;S}_1 \rrbracket^{\sharp} \sqcup^{\sharp} \llbracket \neg\mathtt{B;S}_2 \rrbracket^{\sharp})$ ⟅(4) and (12)⟆

$= (P \fatsemi^{\sharp} \llbracket \mathtt{B;S}_1 \rrbracket^{\sharp}) \sqcup^{\sharp} (P \fatsemi^{\sharp} \llbracket \neg\mathtt{B;S}_2 \rrbracket^{\sharp})$
⟅binary (hence finite) join preservation is definition 3.2.D.d, lemma 6.2, and (12)⟆

$= \mathsf{post}^{\sharp}\llbracket \mathtt{B;S}_1 \rrbracket^{\sharp} P \sqcup^{\sharp} \mathsf{post}^{\sharp}\llbracket \neg\mathtt{B;S}_2 \rrbracket^{\sharp} P$ ⟅def. (25) of $\mathsf{post}^{\sharp}$⟆

— For $\mathsf{post}^{\sharp}\llbracket \mathtt{while\ (B)\ S} \rrbracket^{\sharp} P$, we proceed by cases.

– $\mathsf{post}^{\sharp}\llbracket \mathtt{while\ (B)\ S} \rrbracket^{\sharp}_{e} P$

$= \mathsf{post}^{\sharp}(\mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\ \overleftarrow{F}^{\sharp}_{e} \fatsemi^{\sharp} (\llbracket \neg\mathtt{B} \rrbracket^{\sharp}_{e} \sqcup^{\sharp}_{e} \llbracket \mathtt{B;S} \rrbracket^{\sharp}_{b})P)$ ⟅(9)⟆

$= \mathsf{post}^{\sharp}(\llbracket \neg\mathtt{B} \rrbracket^{\sharp}_{e} \sqcup^{\sharp}_{e} \llbracket \mathtt{B;S} \rrbracket^{\sharp}_{b})(\mathsf{post}^{\sharp}(\mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\ \overleftarrow{F}^{\sharp}_{e}\fatsemi^{\sharp})P)$ ⟅(33)⟆

$= \mathsf{post}^{\sharp}(\llbracket \neg\mathtt{B} \rrbracket^{\sharp}_{e} \sqcup^{\sharp}_{e} \llbracket \mathtt{B;S} \rrbracket^{\sharp}_{b})(\mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\ (\vec{F}^{\sharp}_{pe}(P)))$ ⟅lemma 6.6⟆ (38)

– Similarly, for case (10), we get
$\mathsf{post}^{\sharp}\llbracket \mathtt{while\ (B)\ S} \rrbracket^{\sharp}_{bi} P$

$= \mathsf{post}^{\sharp}(\llbracket \mathtt{B;S} \rrbracket^{\sharp}_{\bot})(\mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\ (\vec{F}^{\sharp}_{pe}(P)))$

– $\mathsf{post}^{\sharp}\llbracket \mathtt{while\ (B)\ S} \rrbracket^{\sharp}_{b} P$

$= P \fatsemi^{\sharp} \llbracket \mathtt{while\ (B)\ S} \rrbracket^{\sharp}_{b}$ ⟅def. (25) of $\mathsf{post}^{\sharp}$⟆

$= P \fatsemi^{\sharp} \bot^{\sharp}_{+}$ ⟅(9)⟆

$= \bot^{\sharp}_{+}$ ⟅$\bot^{\sharp}_{+}$ absorbent for $\fatsemi^{\sharp}$ in definition 3.2.D.a⟆

– $\mathsf{post}^{\sharp}\llbracket \mathtt{while\ (B)\ S} \rrbracket^{\sharp}_{li}$

$= \mathsf{post}^{\sharp}(\mathsf{gfp}^{\sqsubseteq^{\sharp}_{\infty}}\ F^{\sharp}_{\bot})$ ⟅(10)⟆

$= \mathsf{post}^{\sharp}(\mathsf{gfp}^{\sqsubseteq^{\sharp}_{\infty}}\ F^{\sharp}_{p\bot})$ ⟅lemma 6.7⟆ (39)

– $\mathsf{post}^{\sharp}(\llbracket \mathtt{while\ (B)\ S} \rrbracket^{\sharp}_{\bot})$

$= \mathsf{post}^{\sharp}(\llbracket \mathtt{while\ (B)\ S} \rrbracket^{\sharp}_{bi} \sqcup^{\sharp}_{\infty} \llbracket \mathtt{while\ (B)\ S} \rrbracket^{\sharp}_{li})$ ⟅(11)⟆

$= \mathsf{post}^{\sharp}(\llbracket \mathtt{while\ (B)\ S} \rrbracket^{\sharp}_{bi}) \sqcup^{\sharp}_{\infty} \mathsf{post}^{\sharp}(\llbracket \mathtt{while\ (B)\ S} \rrbracket^{\sharp}_{li})$ ⟅binary (hence finite) join preservation and (6.2)⟆

$= \boldsymbol{\lambda} P \bullet \mathsf{post}^{\sharp}(\llbracket \mathtt{while\ (B)\ S} \rrbracket^{\sharp}_{bi})P \sqcup^{\sharp}_{\infty} \mathsf{post}^{\sharp}(\llbracket \mathtt{while\ (B)\ S} \rrbracket^{\sharp}_{li})P$ ⟅pointwise def. $\sqcap_{\infty}$⟆

$$= \boldsymbol{\lambda} P \bullet \mathsf{post}^\sharp(\llbracket\texttt{B;S}\rrbracket^\sharp_\bot)(\mathsf{lfp}^{\sqsubseteq^\sharp_+}\,\vec{F}^\sharp_{pe}(P)) \sqcup^\sharp_\infty \mathsf{post}^\sharp(\mathsf{gfp}^{\sqsubseteq^\sharp_\infty}\,F^\sharp_{p\bot})P \qquad \wr\text{as proved in (38) and (39)}\int$$

– Grouping all cases together, we get

$$\mathsf{post}^\sharp\llbracket\texttt{while (B) S}\rrbracket^\sharp P$$

$$= P \fatsemi^\sharp \llbracket\texttt{while (B) S}\rrbracket^\sharp \qquad \wr\text{def. (25) of }\mathsf{post}^\sharp\int$$

$$= P \fatsemi^\sharp \langle e : \llbracket\texttt{while (B) S}\rrbracket^\sharp_e,\ \bot : \llbracket\texttt{while (B) S}\rrbracket^\sharp_\bot,\ br : \llbracket\texttt{while (B) S}\rrbracket^\sharp_b\rangle \qquad \wr(12)\int$$

$$= \langle e : P^+_{ok} \fatsemi^\sharp \llbracket\texttt{while (B) S}\rrbracket^\sharp_e,\ \bot : P^\infty_{ok} \sqcup^\sharp_\infty P^+_{ok} \fatsemi^\sharp \llbracket\texttt{while (B) S}\rrbracket^\sharp_\bot,\ br : P_{br} \sqcup^\sharp_+ P^+_{ok} \fatsemi^\sharp \llbracket\texttt{while (B) S}\rrbracket^\sharp_b\rangle$$
$$\wr\text{def. (15) of }\fatsemi^\sharp\int$$

$$= \langle e : \mathsf{post}^\sharp\llbracket\texttt{while (B) S}\rrbracket^\sharp_e P,\ \bot : \mathsf{post}^\sharp\llbracket\texttt{while (B) S}\rrbracket^\sharp_\bot P,\ br : P_{br}\rangle$$
$$\wr\text{def. (25) of }\mathsf{post}^\sharp,\ \llbracket\texttt{while (B) S}\rrbracket^\sharp_b \triangleq \bot^\sharp_+ \text{ by (9), } P^+_{ok} \fatsemi^\sharp \bot^\sharp_+ = \bot^\sharp_+ \text{ by 3.2.D.b, and } \bot^\sharp_+ \text{ infimum by 3.2.A}\int$$

$$= \langle e : \mathsf{post}^\sharp(\llbracket\neg\texttt{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket\texttt{B;S}\rrbracket^\sharp_b)(\mathsf{lfp}^{\sqsubseteq^\sharp_+}\,\vec{F}^\sharp_{pe}(P)),\quad \bot : \mathsf{post}^\sharp(\llbracket\texttt{B;S}\rrbracket^\sharp_\bot)(\mathsf{lfp}^{\sqsubseteq^\sharp_+}\,\vec{F}^\sharp_{pe}(P)) \sqcap^\sharp_\infty$$
$$\mathsf{post}^\sharp(\mathsf{gfp}^{\sqsubseteq^\sharp_\infty}\,F^\sharp_{p\bot})P,\ br : P_{br}\rangle \qquad \wr\text{as previously proved for each case, proving (37).}\int \qquad \square$$

Remark 6.8. By defining the appropriate primitives, the post program execution calculus (28) — (37) of theorem 6.5 is an instance of the generic abstract semantics (12). ■

Example 6.9 (Finitary powerset deterministic calculational domain). In [5], the while language is deterministic and has no breaks so the random assignment and breaks have to be eliminated in (3). The denotational semantics is $\llbracket\texttt{S}\rrbracket \in (\Sigma\times\Sigma)_\bot \to (\Sigma\times\Sigma)_\bot$ where $(\Sigma\times\Sigma)_\bot$ is the domain of relations between states extended by $\bot$ to denote nontermination with Scott flat ordering $\sqsubseteq$.

Anticipating on the abstractions of part II, this is an abstraction [18, sect. 8.2] of the trace semantics of sect. 4. Then a semantic abstraction 9.1 gets rid of nontermination [18, sect. 8.1.6] and another one [18, sect. 9.1] abstracts relations to transformers to yield the collecting semantics [5, p. 876].

Skipping these abstractions of the trace semantics, we can directly instantiate the generic abstract semantics of sect. 3 to a finitary relational semantics such as $\llbracket S\rrbracket^e$ in [21]. Then $\mathsf{post}^\sharp$ in (25) becomes $\mathsf{post}^\sharp(S)P = \{\langle\sigma,\ \sigma''\rangle \mid \exists\sigma' \in \Sigma\ .\ \langle\sigma,\ \sigma'\rangle \in P \wedge \langle\sigma',\ \sigma''\rangle \in S\}$, which is a specification of the collecting semantics postulated in [5, p. 876]. $\mathsf{post}^\sharp(S)$ preserves arbitrary unions so, in absence of breaks and ignoring nontermination, together with $\llbracket\texttt{B}\rrbracket^\sharp_e \circ \llbracket\texttt{B}\rrbracket^\sharp_e = \llbracket\texttt{B}\rrbracket^\sharp_e$, $\llbracket\texttt{B}\rrbracket^\sharp_e \circ \llbracket\neg\texttt{B}\rrbracket^\sharp_e = \varnothing$, and$\llbracket\texttt{skip}\rrbracket^\sharp_e = \mathsf{init}^\sharp$ by 3.2.D.a, (37) in theorem 6.5 simplifies to

$$\mathsf{post}^\sharp\llbracket\texttt{while (B) S}\rrbracket^\sharp P \quad = \quad \mathsf{post}^\sharp(\llbracket\neg\texttt{B}\rrbracket^\sharp_e)(\mathsf{lfp}^{\subseteq}\,\boldsymbol{\lambda} X \bullet P \cup \mathsf{post}^\sharp(\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e)(X)$$

which is precisely the data-independent abstraction of the collecting semantics of [5, p. 876]. ■

6.4 Algebraic Logics of Program Execution Properties

By defining $\overline{\{}\,P\,\overline{\}}\,\texttt{S}\,\overline{\{}\,Q\,\overline{\}} \triangleq (\langle P,\ Q\rangle \in \overset{\blacktriangle}{\alpha}(\llbracket\texttt{S}\rrbracket^\sharp))$ with $\overset{\blacktriangle}{\alpha}(S) \triangleq \{\langle P,\ Q\rangle \mid \mathsf{post}^\sharp(S)P \sqsubseteq^\sharp Q\}$ and dually $\underline{\{}\,P\,\underline{\}}\,\texttt{S}\,\underline{\{}\,Q\,\underline{\}} \triangleq (\langle P,\ Q\rangle \in \overset{\blacktriangledown}{\alpha}(\llbracket\texttt{S}\rrbracket^\sharp))$ with $\overset{\blacktriangledown}{\alpha}(S) \triangleq \{\langle P,\ Q\rangle \mid Q \sqsubseteq^\sharp \mathsf{post}^\sharp(S)P\}$, we respectively get the abstract version [20, chapter 26] of Hoare logic [55] and that of reverse/incorrectness logic [32, 75] (extended to loops breaks and nontermination [21, 65]). This is now classic and will be used but not be further detailled.

7 A Calculus of Algebraic Program Semantic (Hyper) Properties

We now study proof methods for semantic properties, that is properties of the semantics, that we define in extension. This is called hyperproperties when the semantics is a set of traces [13, 14], and by extension, for their abstractions, in particular to relational semantics.

7.1 Algebraic Semantic (Hyper) Properties

Defined in extension, program semantic properties are in $\wp(\mathbb{L}^\sharp)$.

Example 7.1 (Algebraic noninterference). Noninterference [46], can be generalized to semantic (hyper) properties of algebraic semantics, as follows. The precondition $R_i \in \wp(\mathbb{L}^\sharp_+ \times \mathbb{L}^\sharp_+)$ is a relation between prelude executions extended to $\mathbb{L}^\sharp$ by (14). The postcondition $R_f \in \wp(\mathbb{L}^\sharp \times \mathbb{L}^\sharp)$ is a relation between terminated or infinite executions. Then algebraic noninterference is $\mathsf{ANI} \triangleq \{\mathcal{P} \in \wp(\mathbb{L}^\sharp) \mid \forall S_1, S_2 \in \mathcal{P} \mathrel{.} \forall P_1, P_2 \in \mathbb{L}^\sharp_+ \mathrel{.} \langle P_1,\ P_2\rangle \in R_i \implies \langle \mathsf{post}^\sharp(S_1)P_1,\ \mathsf{post}^\sharp(S_2)P_2\rangle \in R_f\}$. An instance is algebraic abstract noninterference $\mathsf{AANI} \triangleq \{\mathcal{P} \in \wp(\mathbb{L}^\sharp) \mid \forall S_1, S_2 \in \mathcal{P} \mathrel{.} \forall P_1, P_2 \in \mathbb{L}^\sharp_+ \mathrel{.} \alpha_1(P_1) = \alpha_1(P_2) \implies \alpha_2(\mathsf{post}^\sharp(S_1)P_1) = \alpha_2(\mathsf{post}^\sharp(S_2)P_2)\}$ for abstractions $\alpha_1 \in \mathbb{L}^\sharp \to A_1$ and $\alpha_2 \in \mathbb{L}^\sharp \to A_2$ with special case $\alpha_1 = \alpha_2$ to characterize abstract domain completeness in abstract interpretation [42, 43, 68]. After [14], the generalized algebraic noninterference is $\mathsf{GANI} \triangleq \{\mathcal{P} \in \wp(\mathbb{L}^\sharp) \mid \forall S_1, S_2 \in \mathcal{P} \mathrel{.} \exists \bar{S} \in \mathcal{P} \mathrel{.} \forall P_1, P_2 \in \mathbb{L}^\sharp_+ \mathrel{.} \forall \bar{P} \in \bar{S} \mathrel{.} \langle \bar{P},\ P_1\rangle \in R_i \implies \langle \mathsf{post}^\sharp(S_1)\bar{P},\ \mathsf{post}^\sharp(S_2)P_2\rangle \in R_f\}$. ■

7.2 The Algebraic Program Semantic (Hyper) Properties Transformer

When considering semantic properties in extension, the traditional view of transformers is that they now belong to $\wp(\mathbb{L}^\sharp) \to \wp(\mathbb{L}^\sharp)$ with

$$\begin{array}{rcl} \mathsf{Post}^\sharp & \in & \mathbb{L}^\sharp \to \wp(\mathbb{L}^\sharp) \xrightarrow{\nearrow} \wp(\mathbb{L}^\sharp) \\ \mathsf{Post}^\sharp(S)\mathcal{P} & \triangleq & \{\mathsf{post}^\sharp(S)P \mid P \in \mathcal{P}\} \end{array} \tag{40}$$

[5, 29, 30, 67] are all instances of this definition. The advantage is that logical implication is the traditional $\subseteq$. But the classic structural definition (see sect. 3.2) of the transformer $\mathsf{Post}^\sharp$ fails (unless restrictions are placed on the considered hyperproperties). For the conditional

$$\begin{array}{ll@{\qquad}l}
& \mathsf{Post}^\sharp\llbracket\texttt{if (B) S}_1\texttt{ else S}_2\rrbracket^\sharp\mathcal{P} & \\
= & \{\mathsf{post}^\sharp\llbracket\texttt{if (B) S}_1\texttt{ else S}_2\rrbracket^\sharp P \mid P \in \mathcal{P}\} & ⟅\text{def. (40) of } \mathsf{Post}^\sharp(S)⟆ \\
= & \{\mathsf{post}^\sharp\llbracket\texttt{B;S}_1\rrbracket^\sharp P \sqcup^\sharp \mathsf{post}^\sharp\llbracket\neg\texttt{B;S}_2\rrbracket^\sharp P \mid P \in \mathcal{P}\} & ⟅(34)⟆ \qquad (41) \\
\subseteq & \{\mathsf{post}^\sharp\llbracket\texttt{B;S}_1\rrbracket^\sharp P_1 \sqcup^\sharp \mathsf{post}^\sharp\llbracket\neg\texttt{B;S}_2\rrbracket^\sharp P_2 \mid P_1 \in \mathcal{P} \wedge P_2 \in \mathcal{P}\} & ⟅\text{def. } \subseteq⟆ \qquad (42) \\
= & \{Q_1 \sqcup^\sharp Q_2 \mid Q_1 \in \{\mathsf{post}^\sharp\llbracket\texttt{B;S}_1\rrbracket^\sharp P_1 \mid P_1 \in \mathcal{P}\} \wedge Q_2 \in \{\mathsf{post}^\sharp\llbracket\neg\texttt{B;S}_2\rrbracket^\sharp P_2 \mid P_2 \in \mathcal{P}\}\} & ⟅\text{def. } \in⟆ \\
= & \{Q_1 \sqcup^\sharp Q_2 \mid Q_1 \in \mathsf{Post}^\sharp\llbracket\texttt{B;S}_1\rrbracket^\sharp\mathcal{P} \wedge Q_2 \in \mathsf{Post}^\sharp\llbracket\neg\texttt{B;S}_2\rrbracket^\sharp\mathcal{P}\} & ⟅\text{def. (40) of } \mathsf{Post}^\sharp(S)⟆
\end{array}$$

The problem is that in (41) the two possible executions of the conditional are tight together, whereas, by necessity of traditional independent structural induction on both branches of the conditional, this link is lost in (42). So the hypercollecting semantics of [5, p. 877] is incomplete (the inclusion (42) may be strict).

A solution to preserve structurality is to observe that

$$\{\mathsf{post}^\sharp(S)P\} \quad = \quad \mathsf{Post}^\sharp(S)\{P\} \tag{43}$$

so that the calculation goes on at (41)

$$\begin{array}{ll@{\qquad}l}
= & \{Q_1 \sqcup^\sharp Q_2 \mid Q_1 \in \{\mathsf{post}^\sharp\llbracket\texttt{B;S}_1\rrbracket^\sharp P\} \wedge Q_2 \in \{\mathsf{post}^\sharp\llbracket\neg\texttt{B;S}_2\rrbracket^\sharp P\} \wedge P \in \mathcal{P}\} & ⟅\text{def. singleton and } \in⟆ \\
= & \{Q_1 \sqcup^\sharp Q_2 \mid Q_1 \in \mathsf{Post}^\sharp\llbracket\texttt{B;S}_1\rrbracket^\sharp\{P\} \wedge Q_2 \in \mathsf{Post}^\sharp\llbracket\neg\texttt{B;S}_2\rrbracket^\sharp\{P\} \wedge P \in \mathcal{P}\} & ⟅\text{def. (40) of } \mathsf{Post}^\sharp(S)⟆
\end{array}$$

so that $\mathsf{Post}^\sharp\llbracket\texttt{if (B) S}_1\texttt{ else S}_2\rrbracket^\sharp$ is exactly defined structurally as a function of the components $\mathsf{Post}^\sharp\llbracket\texttt{B;S}_1\rrbracket^\sharp$ and $\mathsf{Post}^\sharp\llbracket\neg\texttt{B;S}_2\rrbracket^\sharp$.

Of course, this element wise reasoning may be considered inelegant. Its necessity becomes more clear when considering the trace semantics of sect. 4. When reasoning on paths e.g. in an iteration statement, the same paths must be considered consistently at each iteration. This requirement may be lifted after abstraction, for example with invariants which forget about computation history.

For backward reasonings, we define Pre such that for all $S \in \mathbb{L}^\sharp$, we have

$$\mathsf{Pre}(S)\mathcal{Q} \quad \triangleq \quad \{P \mid \mathsf{post}^\sharp(S)P \in \mathcal{Q}\} \quad (44) \qquad\qquad \langle \wp(\mathbb{L}^\sharp),\ \subseteq\rangle \xleftarrow[\mathsf{Post}^\sharp(S)]{\mathsf{Pre}(S)} \langle \wp(\mathbb{L}^\sharp),\ \subseteq\rangle \quad (45)$$

Proof of (45).

$$\begin{aligned}
& \mathsf{Post}^\sharp(S)\mathcal{P} \subseteq \mathcal{Q} \\
\Leftrightarrow\ & \{\mathsf{post}^\sharp(S)P \mid P \in \mathcal{P}\} \subseteq \mathcal{Q} && \wr\text{def. (40) of } \mathsf{Post}^\sharp \int \\
\Leftrightarrow\ & \forall P \in \mathcal{P}\ .\ \mathsf{post}^\sharp(S)P \in \mathcal{Q} && \wr\text{def. } \subseteq \int \\
\Leftrightarrow\ & \mathcal{P} \subseteq \{P \mid \mathsf{post}^\sharp(S)P \in \mathcal{Q}\} && \wr\text{def. } \subseteq \int \\
\Leftrightarrow\ & \mathcal{P} \subseteq \mathsf{Pre}(S)\mathcal{Q} && \wr\text{def. 45) of Pre} \int \qquad \square
\end{aligned}$$

If $\mathbb{D}^\sharp$ is a well-defined chain-complete lattice with right finite $\boxed{x}$ preservation composition $\fatsemi^\sharp$ then we have ($\boxed{x}$, $x \in \{+, \infty\}$, stands for $\sqcup^\sharp_+$ in definition 3.2.A when $x = +$ and for $\sqcup^\sharp_\infty$ in definition 3.2.C when $x = \infty$)

$$\begin{aligned}
&& \mathsf{Post}^\sharp(S_1 \boxed{x} S_2)\mathcal{P} &= (\mathsf{Post}^\sharp(S_1) \boxed{x} \mathsf{Post}^\sharp(S_2))\mathcal{P} & (46)\\
\text{where} && (S_1 \boxed{x} S_2)\mathcal{P} &\triangleq \{Q_1 \boxed{x} Q_2 \mid Q_1 \in S_1\{P\} \wedge Q_2 \in S_2\{P\} \wedge P \in \mathcal{P}\}
\end{aligned}$$

Proof of (46).

$$\begin{aligned}
& \mathsf{Post}^\sharp(S_1 \boxed{x} S_2)\mathcal{P} \\
=\ & \{\mathsf{post}^\sharp(S_1 \boxed{x} S_2)P \mid P \in \mathcal{P}\} && \wr(43)\int \\
=\ & \{P \fatsemi^\sharp (S_1 \boxed{x} S_2) \mid P \in \mathcal{P}\} && \wr\text{def. (25) of } \mathsf{post}^\sharp \int \\
=\ & \{(P \fatsemi^\sharp S_1) \boxed{x} (P \fatsemi^\sharp S_2) \mid P \in \mathcal{P}\} && \wr\text{right finite } \boxed{x} \text{ preservation in definition 3.2.D.d} \int \\
=\ & \{\mathsf{post}^\sharp(S_1)P \boxed{x} \mathsf{post}^\sharp(S_2)P \mid P \in \mathcal{P}\} && \wr\text{def. (25) of } \mathsf{post}^\sharp \int \\
=\ & \{Q_1 \boxed{x} Q_2 \mid Q_1 \in \{\mathsf{post}^\sharp(S_1)P\} \wedge Q_2 \in \{\mathsf{post}^\sharp(S_2)P\} \wedge P \in \mathcal{P}\} && \wr\text{def. } \in \text{ and singleton} \int \\
=\ & \{Q_1 \boxed{x} Q_2 \mid Q_1 \in \mathsf{Post}^\sharp(S_1)\{P\} \wedge Q_2 \in \mathsf{Post}^\sharp(S_2)\{P\} \wedge P \in \mathcal{P}\} && \wr(43)\int \\
=\ & \mathsf{Post}^\sharp(S_1) \boxed{x} \mathsf{Post}^\sharp(S_2)\mathcal{P} && \wr\text{def. } \boxed{x} \text{ in (46)} \int \qquad \square
\end{aligned}$$

Remark 7.2. Contrary to join preservation lemma 6.1 for post, Post may not preserve existing joins and meets so that, in general, $\bigsqcup_{i\in\Delta} \mathsf{Post}^\sharp(S_i) \neq \mathsf{Post}^\sharp(\bigsqcup_{i\in\Delta} S_i)$ and dually. For example, let $\mathcal{P}$ be a semantic property. By (40), $\bigsqcup^\sharp_{+\,n\in\mathbb{N}} \mathsf{Post}^\sharp((\llbracket \mathsf{B} \fatsemi \mathsf{S}\rrbracket^\sharp)^n)\mathcal{P} = \bigsqcup^\sharp_{+\,n\in\mathbb{N}} \{\mathsf{post}^\sharp((\llbracket \mathsf{B} \fatsemi \mathsf{S}\rrbracket^\sharp)^n)P \mid P \in \mathcal{P}\}$ is the set of finite executions, for every precondition $P \in \mathcal{P}$, reaching the entry of the iteration `while(B) S` after exactly n terminating body iterations, for all $n \in \mathbb{N}$. On the contrary $\mathsf{Post}^\sharp(\bigsqcup^\sharp_{+\,n\in\mathbb{N}}(\llbracket \mathsf{B} \fatsemi \mathsf{S}\rrbracket^\sharp)^n)\mathcal{P} = \{\mathsf{post}^\sharp(\bigsqcup^\sharp_{+\,n\in\mathbb{N}}(\llbracket \mathsf{B} \fatsemi \mathsf{S}\rrbracket^\sharp)^n)P \mid P \in \mathcal{P}\} = \{\bigsqcup^\sharp_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp((\llbracket \mathsf{B} \fatsemi \mathsf{S}\rrbracket^\sharp)^n)P \mid P \in \mathcal{P}\}$ is the set of finite executions, for every precondition $P \in \mathcal{P}$, reaching the entry of the iteration `while(B) S` after any number of terminating body iterations. ■

7.3 A Calculus of Algebraic Semantic (Hyper) Properties

In the calculational design of the $\mathsf{Post}^\sharp$, we will need the following trivial proposition.

Proposition 7.3 (Singleton fixpoint). *There is an obvious isomorphism between a poset $\langle L, \sqsubseteq, \bot, \sqcup\rangle$ and its singletons $\langle \breve{L}, \breve{\sqsubseteq}, \breve{\bot}, \breve{\sqcup}\rangle$ with $\breve{L} \triangleq \{\{x\} \mid x \in L\}$, $\{x\}\breve{\sqsubseteq}\{y\} \triangleq x \sqsubseteq y$, $\breve{\bot} \triangleq \{\bot\}$, $\{x\}\breve{\sqcup}\{y\} \triangleq \{x \sqcup y\}$, so that, for a increasing chain complete poset we have $\{\mathsf{lfp}^{\sqsubseteq} F\} = \{\bigsqcup_{\delta\in\mathbb{O}} F^\delta\} = \breve{\bigsqcup}_{\delta\in\mathbb{O}}\{F^\delta\} = \mathsf{lfp}^{\breve{\sqsubseteq}} \breve{F}$*

where $\langle F^{\delta},\ \delta \in \mathbb{O}\rangle$ *are the transfinite iterates of* F *from* $\bot$ *and* $\breve{F}(\{x\}) \triangleq \{F(x)\}$. *Dually for greatest fixpoints.*

We derive the sound and complete $\mathsf{Post}^\sharp$ calculus by calculational design, as follows.

Theorem 7.4 (Program semantic (hyper) property calculus). *If* $\mathbb{D}^\sharp$ *is a well-defined increasing and decreasing chain-complete join semilattice with right upper continuous sequential composition* $\fatsemi^\sharp$ *then*

$$\mathsf{Post}^\sharp\llbracket \mathtt{x = A}\rrbracket^\sharp\mathcal{P} = \{\langle e: P_+ \fatsemi^\sharp \mathsf{assign}^\sharp\llbracket \mathsf{x}, \mathsf{A}\rrbracket,\ \bot: P_\infty,\ br: P_{br}\rangle \mid P \in \mathcal{P}\} \tag{47}$$

$$\mathsf{Post}^\sharp\llbracket \mathtt{x = [}a\mathtt{,}\ b\mathtt{]}\rrbracket^\sharp\mathcal{P} = \{\langle e: P_+ \fatsemi^\sharp \mathsf{rassign}^\sharp\llbracket \mathsf{x}, a, b\rrbracket,\ \bot: P_\infty,\ br: P_{br}\rangle \mid P \in \mathcal{P}\} \tag{48}$$

$$\mathsf{Post}^\sharp\llbracket \mathtt{skip}\rrbracket\mathcal{P} = \{\langle e: P_+ \fatsemi^\sharp \mathsf{skip}^\sharp,\ \bot: P_\infty,\ br: P_{br}\rangle \mid P \in \mathcal{P}\} \tag{49}$$

$$\mathsf{Post}^\sharp\llbracket \mathtt{B}\rrbracket^\sharp\mathcal{P} = \{\langle e: P_+ \fatsemi^\sharp \mathsf{test}^\sharp\llbracket \mathsf{B}\rrbracket,\ \bot: P_\infty,\ br: P_{br}\rangle \mid P \in \mathcal{P}\} \tag{50}$$

$$\mathsf{Post}^\sharp\llbracket \mathtt{break}\rrbracket^\sharp\mathcal{P} = \{\langle e: \bot^\sharp_+,\ \bot: P_\infty,\ br: P_{br} \sqcup^\sharp_+ (P_e \fatsemi^\sharp \mathsf{break}^\sharp)\rangle \mid P \in \mathcal{P}\} \tag{51}$$

$$\mathsf{Post}^\sharp\llbracket \mathtt{S}_1\mathtt{;S}_2\rrbracket^\sharp\mathcal{P} = \mathsf{Post}^\sharp\llbracket \mathtt{S}_2\rrbracket^\sharp(\mathsf{Post}^\sharp\llbracket \mathtt{S}_1\rrbracket^\sharp\mathcal{P}) \tag{52}$$

$$\mathsf{Post}^\sharp\llbracket \mathtt{if(B)\ S}_1\ \mathtt{else\ S}_2\rrbracket^\sharp\mathcal{P} = (\mathsf{Post}^\sharp\llbracket \mathtt{B;S}_1\rrbracket^\sharp \sqcup^\sharp \mathsf{Post}^\sharp\llbracket \neg\mathtt{B;S}_2\rrbracket^\sharp)\mathcal{P} \tag{53}$$

$$\breve{\vec{F}}{}^\sharp_{pe} \triangleq \boldsymbol{\lambda} P \bullet \boldsymbol{\lambda} X \bullet \mathsf{Post}^\sharp(\mathsf{init}^\sharp)\{P\}\ \breve{\sqcup}^\sharp_+\ \mathsf{Post}^\sharp(\llbracket \mathtt{B;S}\rrbracket^\sharp_e)(X) \tag{54}$$

$$\breve{F}{}^\sharp_{p\bot} \triangleq \boldsymbol{\lambda} X \bullet \bigcup\{\mathsf{Post}^\sharp(S)(\llbracket \mathtt{B;S}\rrbracket^\sharp_e) \mid S \in X\} \tag{55}$$

$$\begin{aligned}\mathsf{Post}^\sharp\llbracket \mathtt{while(B)\ S}\rrbracket^\sharp\mathcal{P} = \{\langle & e: Q_e,\ \bot: Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b},\ br: P_{br}\rangle \mid \\ & Q_e \in \mathsf{Post}^\sharp(\llbracket \neg\mathtt{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket \mathtt{B;S}\rrbracket^\sharp_b)(\mathsf{lfp}^{\breve{\sqsubseteq}^\sharp_+}\ \breve{\vec{F}}{}^\sharp_{pe}(P)) \wedge \\ & Q_{\bot\ell} \in \mathsf{Post}^\sharp(\llbracket \mathtt{B;S}\rrbracket^\sharp_\bot)(\mathsf{lfp}^{\breve{\sqsubseteq}^\sharp_+}\ (\breve{\vec{F}}{}^\sharp_{pe}(P))) \wedge \\ & \exists Q_{\bot b}\ .\ Q_{\bot b} \in \mathsf{Post}^\sharp(Q_{p\bot})\{P\} \wedge Q_{p\bot} \in \mathsf{gfp}^{\breve{\sqsubseteq}^\sharp_\infty}\ \breve{F}{}^\sharp_{p\bot} \wedge P \in \mathcal{P}\}\end{aligned} \tag{56}$$

(*where* $S_1 \boxtimes S_2$ *is defined in* (46)) *is sound and complete.*

Proof of theorem 7.4.

We need two preliminary results.

$$\begin{aligned}
&— \breve{\vec{F}}{}^\sharp_{pe}(P)\{X\} \\
&= \mathsf{Post}^\sharp(\mathsf{init}^\sharp)\{P\}\ \breve{\sqcup}^\sharp_+\ \mathsf{Post}^\sharp(\llbracket \mathtt{B;S}\rrbracket^\sharp_e)\{X\} && \text{ℓ(54)∫} \\
&= \{\mathsf{post}^\sharp(\mathsf{init}^\sharp)P' \mid P' \in \{P\}\}\ \breve{\sqcup}^\sharp_+\ \{\mathsf{post}^\sharp(\llbracket \mathtt{B;S}\rrbracket^\sharp_e)X\} && \text{ℓ(40) and (43)∫} \\
&= \{\mathsf{post}^\sharp(\mathsf{init}^\sharp)P\}\ \breve{\sqcup}^\sharp_+\ \{\mathsf{post}^\sharp(\llbracket \mathtt{B;S}\rrbracket^\sharp_e)X\} && \text{ℓdef. }\in\text{∫} \\
&= \{\mathsf{post}^\sharp(\mathsf{init}^\sharp)P \sqcup^\sharp_+ \mathsf{post}^\sharp(\llbracket \mathtt{B;S}\rrbracket^\sharp_e)X\} && \text{ℓdef. }\breve{\sqcup}^\sharp_+\text{ in proposition 7.3∫} \\
&= \{\vec{F}{}^\sharp_{pe}(P)X\} && \text{ℓ(35)∫} \qquad (57)
\end{aligned}$$

$$\begin{aligned}
&— \breve{F}{}^\sharp_{p\bot}(\{X\}) \\
&= \bigcup\{\mathsf{Post}^\sharp(S)(\llbracket \mathtt{B;S}\rrbracket^\sharp_e) \mid S \in \{X\}\} && \text{ℓdef. (55) of }\breve{F}{}^\sharp_{p\bot}\text{∫} \\
&= \bigcup\{\mathsf{Post}^\sharp(X)(\llbracket \mathtt{B;S}\rrbracket^\sharp_e)\} && \text{ℓdef. }\in\text{∫} \\
&= \bigcup\{\{\mathsf{post}^\sharp(X)(\llbracket \mathtt{B;S}\rrbracket^\sharp_e)\}\} && \text{ℓ(43)∫} \\
&= \{\mathsf{post}^\sharp(X)(\llbracket \mathtt{B;S}\rrbracket^\sharp_e)\} && \text{ℓdef. }\bigcup\text{∫} \\
&= \{\vec{F}{}^\sharp_{p\bot}(X)\} && \text{ℓ(36)∫} \qquad (58)
\end{aligned}$$

The proof is by structural induction on the statement syntax.

— $\mathsf{Post}^\sharp\llbracket \mathtt{x\ =\ A}\rrbracket^\sharp\mathcal{P}$

$$\begin{aligned}
&= \{\mathsf{post}^\sharp\llbracket \mathtt{x\ =\ A}\rrbracket^\sharp P \mid P\in\mathcal{P}\} && \wr\text{def. (40) of }\mathsf{Post}^\sharp\int\\
&= \{P \fatsemi^\sharp \llbracket \mathtt{x\ =\ A}\rrbracket^\sharp \mid P\in\mathcal{P}\} && \wr\text{def. (40) of }\mathsf{post}^\sharp\int\\
&= \{P \fatsemi^\sharp \langle e:\mathsf{assign}^\sharp\llbracket \mathtt{x},\mathtt{A}\rrbracket,\ \bot:\bot^\sharp_\infty,\ br:P_{br}\rangle \mid P\in\mathcal{P}\} && \wr\text{(12) and (3)}\int\\
&= \{\langle e:P_+ \fatsemi^\sharp \mathsf{assign}^\sharp\llbracket \mathtt{x},\mathtt{A}\rrbracket,\ \bot:P_\infty \fatsemi^\sharp \bot^\sharp_\infty,\ br:P_{br}\rangle \mid P\in\mathcal{P}\} && \wr\text{def. (15) of }\fatsemi^\sharp\int\\
&= \{\langle e:P_+ \fatsemi^\sharp \mathsf{assign}^\sharp\llbracket \mathtt{x},\mathtt{A}\rrbracket,\ \bot:P_\infty \fatsemi^\sharp \bot^\sharp_\infty,\ br:P_{br}\rangle \mid P\in\mathcal{P}\}\\
& && \wr\bot^\sharp_+\text{ absorbent by definition 3.2.D.a}\int\\
&= \{\langle e:P_+ \fatsemi^\sharp \mathsf{assign}^\sharp\llbracket \mathtt{x},\mathtt{A}\rrbracket,\ \bot:P_\infty,\ br:P_{br}\rangle \mid P\in\mathcal{P}\} && \wr P_\infty\text{ absorbent by definition 3.2.D.c}\int
\end{aligned}$$

— The $\mathsf{Post}^\sharp$ characterizations (48) for `x = [`a`, `b`]`, (49) for `x = skip`, and (50) for `B` are similar.

— $\mathsf{Post}^\sharp\llbracket \mathtt{break}\rrbracket^\sharp\mathcal{P}$

$$\begin{aligned}
&= \{\mathsf{post}^\sharp\llbracket \mathtt{break}\rrbracket^\sharp P \mid P\in\mathcal{P}\} && \wr\text{def. (40) of }\mathsf{Post}^\sharp\int\\
&= \{P \fatsemi^\sharp \llbracket \mathtt{break}\rrbracket^\sharp \mid P\in\mathcal{P}\} && \wr\text{def. (40) of }\mathsf{post}^\sharp\int\\
&= \{P \fatsemi^\sharp \langle e:\bot^\sharp_+,\ \bot:\bot^\sharp_\infty,\ br:\mathsf{break}^\sharp\rangle \mid P\in\mathcal{P}\} && \wr\text{(12) and (3)}\int\\
&= \{\langle e:P_+ \fatsemi^\sharp \bot^\sharp_+,\ \bot:P_\infty \fatsemi^\sharp \bot^\sharp_\infty,\ br:P_{br}\sqcup^\sharp_+ (P_e \fatsemi^\sharp \mathsf{break}^\sharp)\rangle \mid P\in\mathcal{P}\} && \wr\text{def. (15) of }\fatsemi^\sharp\int\\
&= \{\langle e:\bot^\sharp_+,\ \bot:P_\infty,\ br:P_{br}\sqcup^\sharp_+ (P_e \fatsemi^\sharp \mathsf{break}^\sharp)\rangle \mid P\in\mathcal{P}\} && \wr\text{definitions 3.2.D.c and 3.2.D.a}\int
\end{aligned}$$

— $\mathsf{Post}^\sharp\llbracket \mathtt{S}_1\mathtt{;}\mathtt{S}_2\rrbracket^\sharp\mathcal{P}$

$$\begin{aligned}
&= \{\mathsf{post}^\sharp\llbracket \mathtt{S}_1\mathtt{;}\mathtt{S}_2\rrbracket^\sharp P \mid P\in\mathcal{P}\} && \wr\text{def. (40) of }\mathsf{Post}^\sharp\int\\
&= \{P \fatsemi^\sharp (\llbracket \mathtt{S}_1\mathtt{;}\mathtt{S}_2\rrbracket^\sharp) \mid P\in\mathcal{P}\} && \wr\text{def. (40) of }\mathsf{post}^\sharp\int\\
&= \{P \fatsemi^\sharp (\llbracket \mathtt{S}_1\rrbracket^\sharp \fatsemi^\sharp \llbracket \mathtt{S}_2\rrbracket^\sharp) \mid P\in\mathcal{P}\} && \wr\text{def. (15) of }\fatsemi^\sharp\int\\
&= \{(P \fatsemi^\sharp \llbracket \mathtt{S}_1\rrbracket^\sharp) \fatsemi^\sharp \llbracket \mathtt{S}_2\rrbracket^\sharp \mid P\in\mathcal{P}\} && \wr\fatsemi^\sharp\text{ associative by definition 3.23.2.D}\int\\
&= \{\mathsf{post}^\sharp\llbracket \mathtt{S}_2\rrbracket^\sharp(P \fatsemi^\sharp \llbracket \mathtt{S}_1\rrbracket^\sharp) \mid P\in\mathcal{P}\} && \wr\text{def. (40) of }\mathsf{post}^\sharp\llbracket \mathtt{S}_2\rrbracket^\sharp Q \triangleq Q \fatsemi^\sharp \llbracket \mathtt{S}_2\rrbracket^\sharp\int\\
&= \{\mathsf{post}^\sharp\llbracket \mathtt{S}_2\rrbracket^\sharp(\mathsf{post}^\sharp\llbracket \mathtt{S}_1\rrbracket^\sharp P) \mid P\in\mathcal{P}\} && \wr\text{def. (40) of }\mathsf{post}^\sharp\llbracket \mathtt{S}_1\rrbracket^\sharp P \triangleq P \fatsemi^\sharp \llbracket \mathtt{S}_1\rrbracket^\sharp\int\\
&= \{\mathsf{post}^\sharp\llbracket \mathtt{S}_2\rrbracket^\sharp Q \mid Q\in\{\mathsf{post}^\sharp\llbracket \mathtt{S}_1\rrbracket^\sharp P \mid P\in\mathcal{P}\}\} && \wr\text{def. }\in\int\\
&= \mathsf{Post}^\sharp\llbracket \mathtt{S}_2\rrbracket^\sharp(\mathsf{Post}^\sharp\llbracket \mathtt{S}_1\rrbracket^\sharp\mathcal{P}) && \wr\text{def. (40) of }\mathsf{Post}^\sharp\int
\end{aligned}$$

— $\mathsf{Post}^\sharp\llbracket \mathtt{if\ (B)\ S}_1\mathtt{\ else\ S}_2\rrbracket^\sharp\mathcal{P}$

$$\begin{aligned}
&= \{Q_1 \sqcup^\sharp Q_2 \mid Q_1\in\mathsf{Post}^\sharp\llbracket \mathtt{B;S}_1\rrbracket^\sharp\{P\} \wedge Q_2\in\mathsf{Post}^\sharp\llbracket \neg\mathtt{B;S}_2\rrbracket^\sharp\{P\} \wedge P\in\mathcal{P}\} && \wr\text{as shown above}\int\\
&= (\mathsf{Post}^\sharp\llbracket \mathtt{B;S}_1\rrbracket^\sharp \sqcup^\sharp \mathsf{Post}^\sharp\llbracket \neg\mathtt{B;S}_2\rrbracket^\sharp)\mathcal{P} && \wr\text{by def. (46) of }\sqcup^\sharp\int
\end{aligned}$$

— $\mathsf{Post}^\sharp\llbracket \mathtt{while\ (B)\ S}\rrbracket^\sharp\mathcal{P}$

$$\begin{aligned}
&= \{\mathsf{post}^\sharp\llbracket \mathtt{while\ (B)\ S}\rrbracket^\sharp P \mid P\in\mathcal{P}\} && \wr\text{def. (40) of }\mathsf{Post}^\sharp\int\\
&= \{\langle ok\ :\ \langle e:\mathsf{post}^\sharp(\llbracket \neg\mathtt{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket \mathtt{B;S}\rrbracket^\sharp_b)(\mathsf{lfp}^{\sqsubseteq^\sharp_+}(\vec{F}^\sharp_{pe}(P))),\ \bot\ :\ \mathsf{post}^\sharp(\llbracket \mathtt{B;S}\rrbracket^\sharp_\bot)(\mathsf{lfp}^{\sqsubseteq^\sharp_+}(\vec{F}^\sharp_{pe}(P))) \sqcup^\sharp_\infty\\
&\quad \mathsf{post}^\sharp(\mathsf{gfp}^{\sqsubseteq^\sharp_\infty} F^\sharp_{p\bot})P\rangle, br:P_{br}\rangle \mid P\in\mathcal{P}\} && \wr\text{(37)}\int\\
&= \{\langle e\ :\ Q_e,\ \bot\ :\ Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b},\ br\ :\ P_{br}\rangle \mid Q_e \in \{\mathsf{post}^\sharp(\llbracket \neg\mathtt{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket \mathtt{B;S}\rrbracket^\sharp_b)(\mathsf{lfp}^{\sqsubseteq^\sharp_+}(\vec{F}^\sharp_{pe}(P)))\} \wedge Q_{\bot\ell} \in\\
&\quad \{\mathsf{post}^\sharp(\llbracket \mathtt{B;S}\rrbracket^\sharp_\bot)(\mathsf{lfp}^{\sqsubseteq^\sharp_+}(\vec{F}^\sharp_{pe}(P)))\} \wedge \exists Q_{p\bot}\ .\ Q_{\bot b}\in\{\mathsf{post}^\sharp(Q_{p\bot})P\} \wedge Q_{p\bot}\in\{\mathsf{gfp}^{\sqsubseteq^\sharp_\infty} F^\sharp_{p\bot}\} \wedge P\in\mathcal{P}\}
\end{aligned}$$

$$\wr\text{def. singleton and } \in\int$$

$$= \{\langle e : Q_e,\ \bot : Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b},\ br : P_{br}\rangle \mid Q_e \in \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)\{\mathsf{lfp}^{\sqsubseteq^\sharp_+}(\vec{F}^\sharp_{pe}(P))\} \wedge Q_{\bot\ell} \in \mathsf{Post}^\sharp(\llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_\bot)\{\mathsf{lfp}^{\sqsubseteq^\sharp_+}(\vec{F}^\sharp_{pe}(P))\} \wedge \exists Q_{\bot b} \mathrel{.} Q_{\bot b} \in \mathsf{Post}^\sharp(Q_{p\bot})\{P\} \wedge Q_{p\bot} \in \{\mathsf{gfp}^{\sqsubseteq^\sharp_\infty} F^\sharp_{p\bot}\} \wedge P \in \mathcal{P}\}$$

$$\wr(43)\int$$

$$= \{\langle e : Q_e,\ \bot : Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b},\ br : P_{br}\rangle \mid Q_e \in \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)(\mathsf{lfp}^{\breve{\sqsubseteq}^\sharp_+}\breve{\vec{F}}^\sharp_{pe}(P)) \wedge Q_{\bot\ell} \in \mathsf{Post}^\sharp(\llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_\bot)(\mathsf{lfp}^{\breve{\sqsubseteq}^\sharp_+}\breve{\vec{F}}^\sharp_{pe}(P)) \wedge \exists Q_{\bot b} \mathrel{.} Q_{\bot b} \in \mathsf{Post}^\sharp(Q_{p\bot})\{P\} \wedge Q_{p\bot} \in \{\mathsf{gfp}^{\sqsubseteq^\sharp_\infty} F^\sharp_{p\bot}\} \wedge P \in \mathcal{P}\}$$

$$\wr\text{since } \{\mathsf{lfp}^{\sqsubseteq^\sharp_+}\vec{F}^\sharp_{pe}(P)\} = \mathsf{lfp}^{\breve{\sqsubseteq}^\sharp_+}\breve{\vec{F}}^\sharp_{pe}(P) \text{ by (57) and proposition 7.3}\int$$

$$= \{\langle e : Q_e,\ \bot : Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b},\ br : P_{br}\rangle \mid Q_e \in \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)(\mathsf{lfp}^{\breve{\sqsubseteq}^\sharp_+}\breve{\vec{F}}^\sharp_{pe}(P)) \wedge Q_{\bot\ell} \in \mathsf{Post}^\sharp(\llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_\bot)(\mathsf{lfp}^{\breve{\sqsubseteq}^\sharp_+}\breve{\vec{F}}^\sharp_{pe}(P)) \wedge \exists Q_{\bot b} \mathrel{.} Q_{\bot b} \in \mathsf{Post}^\sharp(Q_{p\bot})\{P\} \wedge Q_{p\bot} \in \mathsf{gfp}^{\breve{\sqsubseteq}^\sharp_\infty} \breve{F}^\sharp_{p\bot} \wedge P \in \mathcal{P}\}$$

$$\wr\text{since } \{\mathsf{gfp}^{\sqsubseteq^\sharp_\infty} F^\sharp_{p\bot}\} = \mathsf{gfp}^{\breve{\sqsubseteq}^\sharp_\infty} \breve{F}^\sharp_{p\bot} \text{ by (58) and proposition 7.3}\int \qquad \square$$

Example 7.5 (Finitary powerset calculational domain). Continuing example 6.9 ignoring `breaks` and nontermination, the hypercollecting semantics of [5, p. 877] is

$$\begin{array}{rl} & \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e)(\mathsf{lfp}^{\subseteq}\boldsymbol{\lambda} X \bullet \mathcal{P} \cup \mathsf{Post}^\sharp(\llbracket\mathtt{if\ (B)\ S\ else\ skip}\rrbracket^\sharp_e)(X)) \\ = & \{\mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e)(\mathsf{Post}^\sharp(\llbracket\mathtt{if\ (B)\ S\ else\ skip}\rrbracket^\sharp_e)^n\mathcal{P}) \mid n \in \mathbb{N}\} \\ = & \{\mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e)(\mathsf{Post}^\sharp(\llbracket\mathtt{if\ (B)\ S\ else\ skip}\rrbracket^\sharp_e)^n\{P\}) \mid n \in \mathbb{N} \wedge P \in \mathcal{P}\} \\ \neq & \bigcup\{\mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e)(\mathsf{lfp}^{\subseteq}\breve{\vec{F}}^\sharp_{pe}(P)) \mid P \in \mathcal{P}\} \end{array} \tag{59}$$

By remark 7.2, this is different from (56) (even when ignoring nontermination and `breaks`) so that [5, p. 877] is incomplete and cannot be used as a hypercollecting semantics for general hyperproperties, as further discussed in sect. 21. Moreover (59) is unsound, invalidating [5, th. 1]. This will be fixed by the weak hypercollecting semantics defined in (108). ■

8 Abstract Logic of Semantic (Hyper) Properties

8.1 Definition of the Upper and Lower Abstract Logics

The upper (respectively lower) logic $\overline{\mathsf{L}}^\sharp$ (resp. $\underline{\mathsf{L}}^\sharp$) maps the semantics S of a statement into a pair of a precondition and postcondition that is $\overline{\mathsf{L}}^\sharp, \underline{\mathsf{L}}^\sharp \in \mathbb{L}^\sharp \to (\wp(\mathbb{L}^\sharp) \times \wp(\mathbb{L}^\sharp))$ ordered pointwise by $\subseteq$ (the larger the precondition, the larger is the postcondition). We have

$$\overline{\mathsf{L}}^\sharp(S) \quad \triangleq \quad \{\langle\mathcal{P},\ \mathcal{Q}\rangle \mid \mathsf{Post}^\sharp(S)\mathcal{P} \subseteq \mathcal{Q}\} \tag{60}$$

where $\langle\mathcal{P},\ \mathcal{Q}\rangle \in \overline{\mathsf{L}}^\sharp\llbracket\mathsf{S}\rrbracket^\sharp$ is traditionally written $\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\ \mathsf{S}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}$. The $\subseteq$-dual holds for the lower abstract logic. As was the case in sect. 6.4 for execution properties, this is an abstraction $\overset{\blacktriangle}{\alpha}(\mathsf{P}) \triangleq \boldsymbol{\lambda} S \bullet \{\langle\mathcal{P},\ \mathcal{Q}\rangle \mid \mathsf{P}(S)\mathcal{P} \subseteq \mathcal{Q}\}$

$$\langle\mathbb{L}^\sharp \to \wp(\mathbb{L}^\sharp) \xrightarrow{\nearrow} \wp(\mathbb{L}^\sharp),\ \subseteq\rangle \underset{\overset{\blacktriangle}{\alpha}}{\overset{\overset{\blacktriangle}{\gamma}}{\leftrightarrows}} \langle\mathbb{L}^\sharp \to (\wp(\mathbb{L}^\sharp) \times \wp(\mathbb{L}^\sharp)),\ \subseteq\rangle \tag{61}$$

where $\overline{\mathsf{L}}^\sharp(S) = \overset{\blacktriangle}{\alpha}(\mathsf{Post}^\sharp)S$.

Defining the upper and lower logic triples

$$\begin{array}{rcccccc} \overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\ \mathsf{S}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}} & \triangleq & \langle\mathcal{P},\ \mathcal{Q}\rangle \in \overline{\mathsf{L}}^\sharp\llbracket\mathsf{S}\rrbracket^\sharp & = & \mathsf{Post}^\sharp\llbracket\mathsf{S}\rrbracket^\sharp\mathcal{P} \subseteq \mathcal{Q} & = & \forall P \in \mathcal{P} \mathrel{.} \mathsf{post}^\sharp\llbracket\mathsf{S}\rrbracket^\sharp P \in \mathcal{Q} \\ \underline{\{\!|}\,\mathcal{P}\,\underline{|\!\}}\ \mathsf{S}\ \underline{\{\!|}\,\mathcal{Q}\,\underline{|\!\}} & \triangleq & \langle\mathcal{P},\ \mathcal{Q}\rangle \in \underline{\mathsf{L}}^\sharp\llbracket\mathsf{S}\rrbracket^\sharp & = & \mathcal{Q} \subseteq \mathsf{Post}^\sharp\llbracket\mathsf{S}\rrbracket^\sharp\mathcal{P} & = & \forall Q \in \mathcal{Q} \mathrel{.} \exists P \in \mathcal{P} \mathrel{.} \mathsf{post}^\sharp\llbracket\mathsf{S}\rrbracket^\sharp P = Q \end{array} \tag{62}$$

(where for symmetry, we can write $\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}} \triangleq \forall P \in \mathcal{P}\,.\,\exists Q \in \mathcal{Q}\,.\,\mathrm{post}^\sharp(S)P = Q$.) We get generalizations of Hoare logic [55] and incorrectness logic [32, 75] from execution to semantic properties.

Example 8.1 (Finitary powerset nondeterministic calculational domain). In [29, 30], the relational semantics is identical to that of [5] in example 6.9 but for a nondeterministic language. Nontermination is abstracted away. The extended semantics [29, 30, Definition 4] is $\mathrm{post}^\sharp(S)P = \{\langle\sigma, \sigma''\rangle \mid \exists\sigma' \in \Sigma\,.\,\langle\sigma, \sigma'\rangle \in P \wedge \langle\sigma', \sigma''\rangle \in S\}$, the same as in example 6.9. Hyper-triples $\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}$ are defined in [29, 30, Definition 5] to be the powerset instance of (62), the same instance used in example 6.9. ■

The upper and lower abstract logics can always be expressed in terms of singleton (although the equivalent formula is not part of the logic).

Lemma 8.2.

$$\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}} \;\Leftrightarrow\; \forall P \in \mathcal{P}\,.\,\exists Q \in \mathcal{Q}\,.\,\overline{\{\!|}\,\{P\}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\{Q\}\,\overline{|\!\}} \qquad \text{(a)}$$

$$\underline{\{\!|}\,\mathcal{P}\,\underline{|\!\}}\,\mathsf{S}\,\underline{\{\!|}\,\mathcal{Q}\,\underline{|\!\}} \;\Leftrightarrow\; \forall Q \in \mathcal{Q}\,.\,\exists P \in \mathcal{P}\,.\,\underline{\{\!|}\,\{P\}\,\underline{|\!\}}\,\mathsf{S}\,\underline{\{\!|}\,\{Q\}\,\underline{|\!\}} \qquad \text{(b)}$$

Proof of lemma 8.2.

— $\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}$

$$\begin{aligned}
&= \mathrm{Post}^\sharp[\![\mathsf{S}]\!]^\sharp\mathcal{P} \subseteq \mathcal{Q} && \text{⟅def. (62) of the logic triples⟆}\\
&= \{\mathrm{post}^\sharp(S)P \mid P \in \mathcal{P}\} \subseteq \mathcal{Q} && \text{⟅def. (40) of Post}^\sharp\text{⟆}\\
&= \forall P \in \mathcal{P}\,.\,\mathrm{post}^\sharp(S)P \in \mathcal{Q} && \text{⟅def. }\subseteq\text{⟆}\\
&= \forall P \in \mathcal{P}\,.\,\exists Q \in \mathcal{Q}\,.\,\mathrm{post}^\sharp(S)P = Q && \text{⟅def. }\exists\text{⟆}\\
&= \forall P \in \mathcal{P}\,.\,\exists Q \in \mathcal{Q}\,.\,\{\mathrm{post}^\sharp(S)P\} \subseteq \{Q\} && \text{⟅def. }\subseteq\text{⟆}\\
&= \forall P \in \mathcal{P}\,.\,\exists Q \in \mathcal{Q}\,.\,\{\mathrm{post}^\sharp(S)P' \mid P' \in \{P\}\} \subseteq \{Q\} && \text{⟅def. }\in\text{⟆}\\
&= \forall P \in \mathcal{P}\,.\,\exists Q \in \mathcal{Q}\,.\,\mathrm{Post}^\sharp[\![\mathsf{S}]\!]^\sharp\{P\} \subseteq \{Q\} && \text{⟅def. (40) of Post}^\sharp\text{⟆}\\
&= \forall P \in \mathcal{P}\,.\,\exists Q \in \mathcal{Q}\,.\,\overline{\{\!|}\,\{P\}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\{Q\}\,\overline{|\!\}} && \text{⟅def. (62) of the logic triples⟆}
\end{aligned}$$

— (b) is the $\subseteq$-dual of (a). □

Corollary 8.3. $(\exists P \in \mathcal{P}\,.\,\underline{\{\!|}\,\{P\}\,\underline{|\!\}}\,\mathsf{S}\,\underline{\{\!|}\,\{Q\}\,\underline{|\!\}}) \Leftrightarrow \underline{\{\!|}\,\mathcal{P}\,\underline{|\!\}}\,\mathsf{S}\,\underline{\{\!|}\,\{Q\}\,\underline{|\!\}}$.

Proof of corollary 8.3.

$$\begin{aligned}
&\underline{\{\!|}\,\mathcal{P}\,\underline{|\!\}}\,\mathsf{S}\,\underline{\{\!|}\,\{Q\}\,\underline{|\!\}}\\
\Leftrightarrow\;& \forall Q' \in \{Q\}\,.\,\exists P \in \mathcal{P}\,.\,\underline{\{\!|}\,\{P\}\,\underline{|\!\}}\,\mathsf{S}\,\underline{\{\!|}\,\{Q'\}\,\underline{|\!\}} && \text{⟅lemma 8.2.b⟆}\\
\Leftrightarrow\;& \exists P \in \mathcal{P}\,.\,\underline{\{\!|}\,\{P\}\,\underline{|\!\}}\,\mathsf{S}\,\underline{\{\!|}\,\{Q\}\,\underline{|\!\}} && \text{⟅def. }\in\text{⟆}
\end{aligned}$$
□

For singletons, the two logics are equivalent.

Lemma 8.4. *For all* $P, Q \in \mathbb{L}^\sharp$, $\overline{\{\!|}\,\{P\}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\{Q\}\,\overline{|\!\}} = \underline{\{\!|}\,\{P\}\,\underline{|\!\}}\,\mathsf{S}\,\underline{\{\!|}\,\{Q\}\,\underline{|\!\}}$.

Proof of lemma 8.4.

$$\begin{aligned}
&\overline{\{\!|}\,\{P\}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\{Q\}\,\overline{|\!\}}\\
&= \mathrm{Post}^\sharp[\![\mathsf{S}]\!]^\sharp\{P\} \subseteq \{Q\} && \text{⟅def. (62) of logic triples⟆}\\
&= \{\mathrm{post}^\sharp(S)P' \mid P' \in \{P\}\} \subseteq \{Q\} && \text{⟅def. (40) of Post}^\sharp\text{⟆}\\
&= \{\mathrm{post}^\sharp(S)P\} \subseteq \{Q\} && \text{⟅def. }\in\text{⟆}\\
&= \mathrm{post}^\sharp(S)P = Q && \text{⟅def. }\subseteq\text{⟆}
\end{aligned}$$

$$
\begin{aligned}
&= \ \{Q\} \subseteq \{\mathrm{post}^\sharp(S)P\} && \wr\text{def. } \subseteq\int\\
&= \ \{Q\} \subseteq \{\mathrm{post}^\sharp(S)P' \mid P' \in \{P\}\} && \wr\text{def. } \in\int\\
&= \ \{Q\} \subseteq \mathsf{Post}^\sharp\llbracket \mathtt{S}\rrbracket^\sharp\{P\} && \wr\text{def. (40) of } \mathsf{Post}^\sharp\int\\
&= \ \underline{\{\!|}\,\{P\}\,\underline{|\!\}}\ \mathtt{S}\ \underline{\{\!|}\,\{Q\}\,\underline{|\!\}} && \wr\text{def. (62) of logic triples}\int \qquad \square
\end{aligned}
$$

8.2 The Proof Systems of the Upper and Lower Abstract Logics

Since the definition (47)—(56) of $\mathsf{Post}^\sharp\llbracket \mathtt{S}\rrbracket^\sharp$ by a Hilbert proof system is structural, it is the same for the logics. Following [21], this is obtained by Aczel correspondance between set-based fixpoints and proof rules [2]. For iteration fixpoint, over-approximation is provided by [21, th. II.3.4] generalizing Park fixpoint induction [77], whereas under-approximation can be handled by [21, th. II.3.6] generalizing Scott's induction or [21, th. II.3.8] generalizing Turing/Floyd variant functions.

Therefore the sound and complete Hilbert deductive system can be designed calculationally to be the following (where $\mathcal{P}, \mathcal{Q} \in \wp(\mathbb{L}^\sharp)$, $\bowtie$ and $\{\!|\,\mathcal{P}\,|\!\}\ \mathtt{S}\ \{\!|\,\mathcal{Q}\,|\!\}$ are respectively $\subseteq$ and $\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\ \mathtt{S}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}$ for the Upper Abstract Logic and $\supseteq$ and $\underline{\{\!|}\,\mathcal{P}\,\underline{|\!\}}\ \mathtt{S}\ \underline{\{\!|}\,\mathcal{Q}\,\underline{|\!\}}$ for the Lower Abstract Logic and the calculational design proving theorem 8.5 follows in sect. 8.3).

Theorem 8.5 (Upper abstract logic proof system). *If $\mathbb{D}^\sharp$ is a well-defined increasing and decreasing chain-complete join semilattice with right upper continuous sequential composition $\fatsemi^\sharp$ then*

$$\frac{\{\langle e : P_+ \fatsemi^\sharp \mathsf{assign}^\sharp\llbracket \mathsf{x}, \mathsf{A}\rrbracket,\ \bot : P_\infty,\ br : P_{br}\rangle \mid P \in \mathcal{P}\} \bowtie \mathcal{Q}}{\{\!|\,\mathcal{P}\,|\!\}\ \mathtt{x = A}\ \{\!|\,\mathcal{Q}\,|\!\}} \tag{63}$$

$$\frac{\{\langle e : P_+ \fatsemi^\sharp \mathsf{rassign}^\sharp\llbracket \mathsf{x}, a, b\rrbracket,\ \bot : P_\infty,\ br : P_{br}\rangle \mid P \in \mathcal{P}\} \bowtie \mathcal{Q}}{\{\!|\,\mathcal{P}\,|\!\}\ \mathtt{x = [}a\mathtt{,}\ b\mathtt{]}\ \{\!|\,\mathcal{Q}\,|\!\}} \tag{64}$$

$$\frac{\{\langle e : P_+ \fatsemi^\sharp \mathsf{skip}^\sharp,\ \bot : P_\infty,\ br : P_{br}\rangle \mid P \in \mathcal{P}\} \bowtie \mathcal{Q}}{\{\!|\,\mathcal{P}\,|\!\}\ \mathtt{skip}\ \{\!|\,\mathcal{Q}\,|\!\}} \tag{65}$$

$$\frac{\{\langle e : P_+ \fatsemi^\sharp \mathsf{test}^\sharp\llbracket \mathsf{B}\rrbracket,\ \bot : P_\infty,\ br : P_{br}\rangle \mid P \in \mathcal{P}\} \bowtie \mathcal{Q}}{\{\!|\,\mathcal{P}\,|\!\}\ \mathtt{B}\ \{\!|\,\mathcal{Q}\,|\!\}} \tag{66}$$

$$\frac{\{\langle e : \bot^\sharp_+,\ \bot : P_\infty,\ br : P_{br} \sqcup^\sharp_+ (P_e \fatsemi^\sharp \mathsf{break}^\sharp)\rangle \mid P \in \mathcal{P}\} \bowtie \mathcal{Q}}{\{\!|\,\mathcal{P}\,|\!\}\ \mathtt{break}\ \{\!|\,\mathcal{Q}\,|\!\}} \tag{67}$$

$$\frac{\{\!|\,\mathcal{P}\,|\!\}\ \mathtt{S}_1\ \{\!|\,\mathcal{Q}\,|\!\},\quad \{\!|\,\mathcal{Q}\,|\!\}\ \mathtt{S}_2\ \{\!|\,\mathcal{R}\,|\!\}}{\{\!|\,\mathcal{P}\,|\!\}\ \mathtt{S}_1\mathtt{;}\mathtt{S}_2\ \{\!|\,\mathcal{R}\,|\!\}} \tag{68}$$

$$\frac{\forall P \in \mathcal{P},\quad (\overline{\{\!|}\,\{P\}\,\overline{|\!\}}\ \mathtt{B;S}_1\ \overline{\{\!|}\,\{Q_1\}\,\overline{|\!\}} \wedge \overline{\{\!|}\,\{P\}\,\overline{|\!\}}\ \neg\mathtt{B;S}_2\ \overline{\{\!|}\,\{Q_2\}\,\overline{|\!\}}) \Rightarrow (Q_1 \sqcup^\sharp Q_2 \in \mathcal{Q})}{\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\ \mathtt{if\ (B)\ S_1\ else\ S_2}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}} \tag{69}$$

$$\frac{\begin{array}{c}\big(P_e = \mathsf{lfp}^{\sqsubseteq^\sharp_+}\,\vec{F}^\sharp_{pe}(P') \wedge\ \overline{\{\!|}\,\{P_e\}\,\overline{|\!\}}\ \neg\mathtt{B}\ \overline{\{\!|}\,\{Q_e\}\,\overline{|\!\}} \wedge\ \overline{\{\!|}\,\{P_e\}\,\overline{|\!\}}\ \mathtt{B;S}\ \overline{\{\!|}\,\{Q_b\}\,\overline{|\!\}} \wedge\\ \overline{\{\!|}\,\{P_e\}\,\overline{|\!\}}\ \mathtt{B;S}\ \overline{\{\!|}\,\{Q_{\bot\ell}\}\,\overline{|\!\}} \wedge\ Q_{\bot b} = \mathsf{gfp}^{\sqsubseteq^\sharp_\infty}\,F^\sharp_{p\bot} \wedge\ P' \in \mathcal{P}\big)\ \Rightarrow\\ \big(\langle e : Q_e \sqcup^\sharp_e Q_b,\ \bot : Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b},\ br : P_{br}\rangle \in \mathcal{Q}\big)\end{array}}{\overline{\{\!|}\,\mathcal{I}\,\overline{|\!\}}\ \mathtt{while\ (B)\ S}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}} \tag{70}$$

is sound and complete.

Remarkably in (69) and (70), we have to consider all possible over approximations, and in (70) P_e and $Q_{\bot b}$ must be exact fixpoints. This is because, for completeness and in full generality, hyperlogics cannot make any approximation of the program semantics defined by $\mathsf{post}^\sharp$ in (40) hence prohibiting approximations in (62).

Notice that no consequence rule is required for completeness, although they are sound.

$$\frac{\mathcal{P} \subseteq \mathcal{P}', \quad \overline{\{\!|}\,\mathcal{P}'\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\mathcal{Q}'\,\overline{|\!\}}, \quad \mathcal{Q}' \subseteq \mathcal{Q}}{\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}} \qquad \frac{\mathcal{P}' \subseteq \mathcal{P}, \quad \underline{\{\!|}\,\mathcal{P}'\,\underline{|\!\}}\,\mathsf{S}\,\underline{\{\!|}\,\mathcal{Q}'\,\underline{|\!\}}, \quad \mathcal{Q} \subseteq \mathcal{Q}'}{\underline{\{\!|}\,\mathcal{P}\,\underline{|\!\}}\,\mathsf{S}\,\underline{\{\!|}\,\mathcal{Q}\,\underline{|\!\}}} \tag{71}$$

Proof of (71).

$$\begin{aligned}
& \mathcal{P} \subseteq \mathcal{P}' \wedge \overline{\{\!|}\,\mathcal{P}'\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\mathcal{Q}'\,\overline{|\!\}} \wedge \mathcal{Q}' \subseteq \mathcal{Q} \\
\Rightarrow\ & \mathcal{P} \subseteq \mathcal{P}' \wedge \mathsf{Post}^\sharp[\![\mathsf{S}]\!]^\sharp\mathcal{P}' \subseteq \mathcal{Q}' \wedge \mathcal{Q}' \subseteq \mathcal{Q} && \wr\text{def. (62) of the logic triples}\int \\
\Rightarrow\ & \mathcal{P} \subseteq \mathcal{P}' \wedge \mathsf{Post}^\sharp[\![\mathsf{S}]\!]^\sharp\mathcal{P}' \subseteq \mathcal{Q} && \wr\subseteq\text{ transitive}\int \\
\Rightarrow\ & \mathsf{Post}^\sharp[\![\mathsf{S}]\!]^\sharp\mathcal{P} \subseteq \mathsf{Post}^\sharp[\![\mathsf{S}]\!]^\sharp\mathcal{P}' \wedge \mathsf{Post}^\sharp[\![\mathsf{S}]\!]^\sharp\mathcal{P}' \subseteq \mathcal{Q} && \wr\mathsf{Post}^\sharp[\![\mathsf{S}]\!]^\sharp\text{ increasing by (45)}\int \\
\Rightarrow\ & \mathsf{Post}^\sharp[\![\mathsf{S}]\!]^\sharp\mathcal{P} \subseteq \mathcal{Q} && \wr\subseteq\text{ transitive}\int \\
\Rightarrow\ & \overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}} && \wr\text{def. (62) of the logic triples}\int
\end{aligned}$$

The converse follows immediately by choosing $\mathcal{P} = \mathcal{P}'$ and $\mathcal{Q}' = \mathcal{Q}$ since $\subseteq$ is reflexive. The consequence rule for the lower abstract logic is $\subseteq$-dual. □

Example 8.6 (Choice). Let us define the choice $\mathsf{S}_1 + \mathsf{S}_2 \triangleq \texttt{c = [0,1]; if (c) }\mathsf{S}_1\texttt{ else }\mathsf{S}_2$ where auxiliary variable c does not appear in S_1 nor in S_2. The proof rule can be derived as follows

$$\begin{aligned}
& \overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}_1 + \mathsf{S}_2\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}} \\
\Leftrightarrow\ & \overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\texttt{c = [0,1]; if (c) }\mathsf{S}_1\texttt{ else }\mathsf{S}_2\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}} && \wr\text{def. choice }+\int \\
\Leftrightarrow\ & \exists\mathcal{R}\,.\,\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\texttt{c = [0,1]}\,\overline{\{\!|}\,\mathcal{R}\,\overline{|\!\}} \wedge \overline{\{\!|}\,\mathcal{R}\,\overline{|\!\}}\,\texttt{if (c) }\mathsf{S}_1\texttt{ else }\mathsf{S}_2\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}} && \wr\text{sequential composition (68)}\int \\
\Leftrightarrow\ & \exists\mathcal{R}\,.\,\{P \mathbin{\text{;}}^\sharp \mathsf{rassign}^\sharp[\![\mathsf{c},0,1]\!] \mid P \in \mathcal{P}\} \subseteq \mathcal{R} \wedge \overline{\{\!|}\,\mathcal{R}\,\overline{|\!\}}\,\texttt{if (c) }\mathsf{S}_1\texttt{ else }\mathsf{S}_2\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}} && \wr\text{(64)}\int \\
\Leftrightarrow\ & \overline{\{\!|}\,\{P \mathbin{\text{;}}^\sharp \mathsf{rassign}^\sharp[\![\mathsf{c},0,1]\!] \mid P \in \mathcal{P}\}\,\overline{|\!\}}\,\texttt{if (c) }\mathsf{S}_1\texttt{ else }\mathsf{S}_2\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}} \\
& && \wr\text{taking }\mathcal{R} = \{P \mathbin{\text{;}}^\sharp \mathsf{rassign}^\sharp[\![\mathsf{c},0,1]\!] \mid P \in \mathcal{P}\}\int \\
\Leftrightarrow\ & \forall P \in \{P' \mathbin{\text{;}}^\sharp \mathsf{rassign}^\sharp[\![\mathsf{c},0,1]\!] \mid P' \in \mathcal{P}\}, Q_1, Q_2\,.\,(\underline{\{\!|}\,\{P\}\,\underline{|\!\}}\,\mathsf{B};\mathsf{S}_1\,\underline{\{\!|}\,\{Q_1\}\,\underline{|\!\}} \wedge \underline{\{\!|}\,\{P\}\,\underline{|\!\}}\,\neg\mathsf{B};\mathsf{S}_2\,\underline{\{\!|}\,\{Q_2\}\,\underline{|\!\}}) \Rightarrow \\
& (Q_1 \sqcup^\sharp Q_2 \in \mathcal{Q}) && \wr\text{(69)}\int \\
\Leftrightarrow\ & \forall P \in \mathcal{P}, Q_1, Q_2\,.\,(\underline{\{\!|}\,\{P\}\,\underline{|\!\}}\,\mathsf{S}_1\,\underline{\{\!|}\,\{Q_1\}\,\underline{|\!\}} \wedge \underline{\{\!|}\,\{P\}\,\underline{|\!\}}\,\mathsf{S}_2\,\underline{\{\!|}\,\{Q_2\}\,\underline{|\!\}}) \Rightarrow (Q_1 \sqcup^\sharp Q_2 \in \mathcal{Q}) && (72) \\
& \quad \wr\text{assuming states where } \mathsf{c} \text{ is assigned 0 or 1, } \mathsf{B} \text{ is true for 0 and } \neg\mathsf{B} \text{ is true for 1 (or conversely)}\int
\end{aligned}$$

so that we get the sound and complete rule

$$\frac{\forall P \in \mathcal{P}, Q_1, Q_2\,.\,(\underline{\{\!|}\,\{P\}\,\underline{|\!\}}\,\mathsf{S}_1\,\underline{\{\!|}\,\{Q_1\}\,\underline{|\!\}} \wedge \underline{\{\!|}\,\{P\}\,\underline{|\!\}}\,\mathsf{S}_2\,\underline{\{\!|}\,\{Q_2\}\,\underline{|\!\}}) \Rightarrow (Q_1 \sqcup^\sharp Q_2 \in \mathcal{Q})}{\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}_1 + \mathsf{S}_2\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}} \tag{73}$$

Let us now consider the particular case $\mathsf{post}^\sharp(S)P = \{\langle\sigma, \sigma''\rangle \mid \exists\sigma' \in \Sigma\,.\,\langle\sigma, \sigma'\rangle \in P \wedge \langle\sigma', \sigma''\rangle \in S\}$ as in example 6.9 (but this time with unbounded nondeterminism) so that $\sqcup^\sharp$ is $\cup$ in (73). Then (73) is implied, but not conversely, by the proof rule

$$\frac{\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}_1\,\overline{\{\!|}\,\mathcal{Q}_1\,\overline{|\!\}}, \quad \overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}_2\,\overline{\{\!|}\,\mathcal{Q}_2\,\overline{|\!\}}}{\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}_1 + \mathsf{S}_2\,\overline{\{\!|}\,\{Q_1 \cup Q_2 \mid Q_1 \in \mathcal{Q}_1 \wedge Q_2 \in \mathcal{Q}_2\}\,\overline{|\!\}}} \quad (\mathit{Choice})$$

of [29], which is sound but incomplete. For completeness, [29, p. 207:9] has to introduce an (*Exist*) proof rule which amounts to the case by case analysis of rule (73). ■

Example 8.7 (Finitary powerset nondeterministic calculational domain). Continuing example 8.1, the iteration rule postulated in [29, 30, Fig. 2] is (70), ignoring nontermination and breaks, and applying proposition 2.4 to reason on the fixpoint iterates. ■

8.3 Calculational Design of the Proof System of the Upper Abstract Logic

Proof of (63) — (70). The proof of soundness and completeness is by structural induction. We show the calculational design for the iteration (70). The other cases are in the appendix.

— Proof of (63), (64), (65), and (66). The characterization (47) of $\mathsf{Post}^\sharp[\![\mathtt{x = A}]\!]^\sharp\mathcal{P}$ yields, by (62), the axiom (63) for $\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\;\mathtt{x = A}\;\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}$ (where the side condition is written as a premiss). The rule for $\underline{\{\!|}\,\mathcal{P}\,\underline{|\!\}}\;\mathtt{x = A}\;\underline{\{\!|}\,\mathcal{Q}\,\underline{|\!\}}$ is $\subseteq$-order dual. The rule (64) for $\mathtt{x = [}a\mathtt{,}\ b\mathtt{]}$, (65) for $\mathtt{x = skip}$, and (66) for $\mathtt{B}$ and their duals are similar.

— Proof of (67). The characterization (62) of $\mathsf{Post}^\sharp[\![\mathtt{break}]\!]^\sharp\mathcal{P}$ yields the axiom (67) for $\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\;\mathtt{break}\;\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}$ (where the side condition is written as a premiss). The rule for $\underline{\{\!|}\,\mathcal{P}\,\underline{|\!\}}\;\mathtt{break}\;\underline{\{\!|}\,\mathcal{Q}\,\underline{|\!\}}$ is $\subseteq$-order dual.

— Proof of (68). For sequential composition, we have

$\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\;\mathtt{S}_1\mathtt{;S}_2\;\overline{\{\!|}\,\mathcal{R}\,\overline{|\!\}}$

$\Leftrightarrow$ $\mathsf{Post}^\sharp[\![\mathtt{S}_1\mathtt{;S}_2]\!]^\sharp\mathcal{P}\subseteq\mathcal{R}$ ⟅def. (62) of the logic triples⟆

$\Leftrightarrow$ $\mathsf{Post}^\sharp[\![\mathtt{S}_2]\!]^\sharp(\mathsf{Post}^\sharp[\![\mathtt{S}_1]\!]^\sharp\mathcal{P})\subseteq\mathcal{R}$ ⟅(52)⟆

$\Leftrightarrow$ $\exists\mathcal{Q}\;.\;\mathsf{Post}^\sharp[\![\mathtt{S}_1]\!]^\sharp\mathcal{P}\subseteq\mathcal{Q}\wedge\mathsf{Post}^\sharp[\![\mathtt{S}_2]\!]^\sharp\mathcal{Q}\subseteq\mathcal{R}$

⟅(soundness, $\Rightarrow$) By (40), $\mathsf{Post}^\sharp[\![\mathtt{S}]\!]^\sharp$ is $\subseteq$-increasing so $\mathsf{Post}^\sharp[\![\mathtt{S}_1]\!]^\sharp\mathcal{P}\subseteq\mathcal{Q}$ implies $\mathsf{Post}^\sharp[\![\mathtt{S}_2]\!]^\sharp(\mathsf{Post}^\sharp[\![\mathtt{S}_1]\!]^\sharp\mathcal{P})\subseteq\mathsf{Post}^\sharp[\![\mathtt{S}_2]\!]^\sharp\mathcal{Q}$ and $\subseteq$ is transitive;
(completeness, $\Leftarrow$) take $\mathcal{Q}=\mathsf{Post}^\sharp[\![\mathtt{S}_1]\!]^\sharp\mathcal{P}$ and reflexivity⟆

$\Leftrightarrow$ $\exists\mathcal{Q}\;.\;\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\;\mathtt{S}_1\;\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}\wedge\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}\;\mathtt{S}_2\;\overline{\{\!|}\,\mathcal{R}\,\overline{|\!\}}$

⟅def. (62) of the logic triples and dually for under approximation⟆

— Proof of (69). For the conditional, we have

$\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\;\mathtt{if\ (B)\ S}_1\ \mathtt{else\ S}_2\;\overline{\{\!|}\,\mathcal{R}\,\overline{|\!\}}$

$\Leftrightarrow$ $\mathsf{Post}^\sharp[\![\mathtt{if\ (B)\ S}_1\ \mathtt{else\ S}_2]\!]^\sharp\mathcal{P}\subseteq\mathcal{R}$ ⟅def. (62) of the logic triples⟆

$\Leftrightarrow$ $(\mathsf{Post}^\sharp[\![\mathtt{B;S}_1]\!]^\sharp\sqcup^\sharp\mathsf{Post}^\sharp[\![\neg\mathtt{B;S}_2]\!]^\sharp)\mathcal{P}\subseteq\mathcal{R}$ ⟅(53)⟆

$\Leftrightarrow$ $\{Q_1\sqcup^\sharp Q_2\mid Q_1\in\mathsf{Post}^\sharp[\![\mathtt{B;S}_1]\!]^\sharp\{P\}\wedge Q_2\in\mathsf{Post}^\sharp[\![\neg\mathtt{B;S}_2]\!]^\sharp\{P\}\wedge P\in\mathcal{P}\}\subseteq\mathcal{R}$ ⟅def. (46) of $\sqcup^\sharp$⟆

$\Leftrightarrow$ $\forall P,Q_1,Q_2\;.\;(P\in\mathcal{P}\wedge Q_1\in\mathsf{Post}^\sharp[\![\mathtt{B;S}_1]\!]^\sharp\{P\}\wedge Q_2\in\mathsf{Post}^\sharp[\![\neg\mathtt{B;S}_2]\!]^\sharp\{P\})\Rightarrow(Q_1\sqcup^\sharp Q_2\in\mathcal{R})$

⟅def. $\subseteq$, $\wedge$ commutative⟆

$\Leftrightarrow$ $\forall P,Q_1,Q_2\;.\;(P\in\mathcal{P}\wedge\{Q_1\}\subseteq\mathsf{Post}^\sharp[\![\mathtt{B;S}_1]\!]^\sharp\{P\}\wedge\{Q_2\}\subseteq\mathsf{Post}^\sharp[\![\neg\mathtt{B;S}_2]\!]^\sharp\{P\})\Rightarrow(Q_1\sqcup^\sharp Q_2\in\mathcal{R})$

⟅def. $\subseteq$⟆

$\Leftrightarrow$ $\forall P,Q_1,Q_2\;.\;(P\in\mathcal{P}\wedge\underline{\{\!|}\,\{P\}\,\underline{|\!\}}\;\mathtt{B;S}_1\;\underline{\{\!|}\,\{Q_1\}\,\underline{|\!\}}\wedge\underline{\{\!|}\,\{P\}\,\underline{|\!\}}\;\neg\mathtt{B;S}_2\;\underline{\{\!|}\,\{Q_2\}\,\underline{|\!\}})\Rightarrow(Q_1\sqcup^\sharp Q_2\in\mathcal{R})$

⟅def. (62) of the lower abstract logic⟆

$\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\;\mathtt{while\ (B)\ S}\;\overline{\{\!|}\,\mathcal{R}\,\overline{|\!\}}$

$\Leftrightarrow$ $\mathsf{Post}^\sharp[\![\mathtt{while\ (B)\ S}]\!]^\sharp\mathcal{P}\subseteq\mathcal{R}$ ⟅def. (62) of the logic triples⟆

$\Leftrightarrow$ $\{\langle e:Q_e,\ \bot:Q_{\bot\ell}\sqcup^\sharp_\infty Q_{\bot b},\ br:P_{br}\rangle\mid Q_e\in\mathsf{Post}^\sharp([\![\neg\mathtt{B}]\!]^\sharp_e\sqcup^\sharp_e[\![\mathtt{B;S}]\!]^\sharp_b)(\mathsf{lfp}^{\breve{\sqsubseteq}^\sharp_+}\vec{\breve{F}}{}^\sharp_{pe}(P))\wedge Q_{\bot\ell}\in\mathsf{Post}^\sharp([\![\mathtt{B;S}]\!]^\sharp_\bot)(\mathsf{lfp}^{\breve{\sqsubseteq}^\sharp_+}\vec{\breve{F}}{}^\sharp_{pe}(P))\wedge\exists Q_{\bot b}\;.\;Q_{\bot b}\in\mathsf{Post}^\sharp(Q_{p\bot})\{P\}\wedge Q_{p\bot}\in\mathsf{gfp}^{\breve{\sqsubseteq}^\sharp_\infty}\breve{F}^\sharp_{p\bot}\wedge P\in\mathcal{P}\}\subseteq\mathcal{R}$

⟅(56)⟆

$\Leftrightarrow$ $\{\langle e:Q_e,\bot:Q_{\bot\ell}\sqcup^\sharp_\infty Q_{\bot b},br:P_{br}\rangle\mid\exists I_e\;.\;I_e\subseteq\mathsf{lfp}^{\breve{\sqsubseteq}^\sharp_+}\vec{\breve{F}}{}^\sharp_{pe}(P)\wedge Q_e\in\mathsf{Post}^\sharp([\![\neg\mathtt{B}]\!]^\sharp_e\sqcup^\sharp_e[\![\mathtt{B;S}]\!]^\sharp_b)I_e\wedge Q_{\bot\ell}\in\mathsf{Post}^\sharp([\![\mathtt{B;S}]\!]^\sharp_\bot)(I_e)\wedge\exists I_\bot\;.\;I_\bot\subseteq\mathsf{gfp}^{\breve{\sqsubseteq}^\sharp_\infty}\breve{F}^\sharp_{p\bot}\wedge Q_{\bot b}\in I_\bot\wedge P\in\mathcal{P}\}\subseteq\mathcal{R}$

≀(⇒) Take $I_e = \mathsf{lfp}^{\breve{\sqsubseteq}^{\sharp}_{+}}\, \breve{\vec{F}}^{\sharp}_{pe}(P)$, $I_\bot = \mathsf{gfp}^{\breve{\sqsubseteq}^{\sharp}_{\infty}}\, \breve{F}^{\sharp}_{p\bot}$, and $\subseteq$ reflexive
(⇐) by (45), $\mathsf{Post}^\sharp(S)$ is $\subseteq$-increasing⟆

$\Leftrightarrow \{\langle e: Q_e, \bot: Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b}, br: P_{br}\rangle \mid \exists P_e \mathrel{.} \{P_e\} = \mathsf{lfp}^{\breve{\sqsubseteq}^{\sharp}_{+}}\, \breve{\vec{F}}^{\sharp}_{pe}(P) \wedge Q_e \in \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)\{P_e\} \wedge Q_{\bot\ell} \in \mathsf{Post}^\sharp(\llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_\bot)\{P_e\} \wedge \exists P_\bot \mathrel{.} \{P_\bot\} = \mathsf{gfp}^{\breve{\sqsubseteq}^{\sharp}_{\infty}}\, \breve{F}^{\sharp}_{p\bot} \wedge Q_{\bot b} \in \{P_\bot\} \wedge P \in \mathcal{P}\} \subseteq \mathcal{R}$

≀If I_e is empty then $\mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)I_e$ is empty by (40), contrary to $Q_e \in \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)I_e$ proving that I_e cannot be empty. By (54), $\mathsf{lfp}^{\breve{\sqsubseteq}^{\sharp}_{+}}\, \breve{\vec{F}}^{\sharp}_{pe}(P)$ is a singleton, say $\{P_e\}$. For I_e to be non-empty and included in a singleton, it must be equal to that singleton so $I_e = \{P_e\}$. The reasoning is the same for $I_\bot = \{P_\bot\}$⟆

$\Leftrightarrow \{\langle e: Q_e, \bot: Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b}, br: P_{br}\rangle \mid \exists P_e \mathrel{.} \{P_e\} = \mathsf{lfp}^{\breve{\sqsubseteq}^{\sharp}_{+}}\, \breve{\vec{F}}^{\sharp}_{pe}(P) \wedge Q_e \in \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)\{P_e\} \wedge Q_{\bot\ell} \in \mathsf{Post}^\sharp(\llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_\bot)\{P_e\} \wedge \{Q_{\bot b}\} = \mathsf{gfp}^{\breve{\sqsubseteq}^{\sharp}_{\infty}}\, \breve{F}^{\sharp}_{p\bot} \wedge P \in \mathcal{P}\} \subseteq \mathcal{R}$

≀$Q_{\bot b} \in \{P_\bot\}$ if and only if $Q_{\bot b} = P_{\bot b}$⟆

$\Leftrightarrow \{\langle e: Q_e, \bot: Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b}, br: P_{br}\rangle \mid \exists P_e \mathrel{.} \{P_e\} = \{\mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\, \vec{F}^{\sharp}_{pe}(P)\} \wedge Q_e \in \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)\{P_e\} \wedge Q_{\bot\ell} \in \mathsf{Post}^\sharp(\llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_\bot)\{P_e\} \wedge \{Q_{\bot b}\} = \{\mathsf{gfp}^{\sqsubseteq^{\sharp}_{\infty}}\, F^{\sharp}_{p\bot}\} \wedge P \in \mathcal{P}\} \subseteq \mathcal{R}$

≀since $\mathsf{lfp}^{\breve{\sqsubseteq}^{\sharp}_{+}}\, \breve{\vec{F}}^{\sharp}_{pe}(P) = \{\mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\, \vec{F}^{\sharp}_{pe}(P)\}$ by (54), proposition 7.3, and $\mathsf{gfp}^{\breve{\sqsubseteq}^{\sharp}_{\infty}}\, (\breve{F}^{\sharp}_{p\bot}) = \{\mathsf{gfp}^{\sqsubseteq^{\sharp}_{\infty}}\, F^{\sharp}_{p\bot}\}$ by (36) and proposition 7.3⟆

$\Leftrightarrow \{\langle e: Q_e, \bot: Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b}, br: P_{br}\rangle \mid \exists P_e \mathrel{.} P_e = \mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\, \vec{F}^{\sharp}_{pe}(P) \wedge Q_e \in \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)\{P_e\} \wedge Q_{\bot\ell} \in \mathsf{Post}^\sharp(\llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_\bot)\{P_e\} \wedge Q_{\bot b} = \mathsf{gfp}^{\sqsubseteq^{\sharp}_{\infty}}\, F^{\sharp}_{p\bot} \wedge P \in \mathcal{P}\} \subseteq \mathcal{R}$ ≀def. set equality⟆

$\Leftrightarrow \{\langle e: Q_e, \bot: Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b}, br: P_{br}\rangle \mid \exists P_e \mathrel{.} P_e = \mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\, \vec{F}^{\sharp}_{pe}(P) \wedge \{Q_e\} \subseteq \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)\{P_e\} \wedge \{Q_{\bot\ell}\} \subseteq \mathsf{Post}^\sharp(\llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_\bot)\{P_e\} \wedge Q_{\bot b} = \mathsf{gfp}^{\sqsubseteq^{\sharp}_{\infty}}\, F^{\sharp}_{p\bot} \wedge P \in \mathcal{P}\} \subseteq \mathcal{R}$ ≀def. $\in$ and $\subseteq$⟆

$\Leftrightarrow \{\langle e: Q_e, \bot: Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b}, br: P_{br}\rangle \mid \exists P_e \mathrel{.} P_e = \mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\, \vec{F}^{\sharp}_{pe}(P) \wedge \{Q_e\} \subseteq \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)\{P_e\} \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\mathsf{B};\mathsf{S}\,\underline{\{\!|}\,\{Q_{\bot\ell}\}\,\underline{|\!\}} \wedge Q_{\bot b} = \mathsf{gfp}^{\sqsubseteq^{\sharp}_{\infty}}\, F^{\sharp}_{p\bot} \wedge P \in \mathcal{P}\} \subseteq \mathcal{R}$

≀def. (62) of $\underline{\{\!|}\,\mathcal{P}\,\underline{|\!\}}\,\mathsf{S}\,\underline{\{\!|}\,\mathcal{Q}\,\underline{|\!\}} \triangleq (\mathcal{Q} \subseteq \mathsf{Post}^\sharp\llbracket\mathsf{S}\rrbracket^\sharp\mathcal{P})$⟆

$\Leftrightarrow \{\langle e: Q_e, \bot: Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b}, br: P_{br}\rangle \mid \exists P_e \mathrel{.} P_e = \mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\, \vec{F}^{\sharp}_{pe}(P) \wedge \{Q_e\} \subseteq \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e)\{P_e\} \sqcup^\sharp_e \mathsf{Post}^\sharp(\llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)\{P_e\} \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\mathsf{B};\mathsf{S}\,\underline{\{\!|}\,\{Q_{\bot\ell}\}\,\underline{|\!\}} \wedge Q_{\bot b} = \mathsf{gfp}^{\sqsubseteq^{\sharp}_{\infty}}\, F^{\sharp}_{p\bot} \wedge P \in \mathcal{P}\} \subseteq \mathcal{R}$ ≀(46)⟆

$\Leftrightarrow \{\langle e: Q'_e, \bot: Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b}, br: P_{br}\rangle \mid \exists P_e \mathrel{.} P_e = \mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\, \vec{F}^{\sharp}_{pe}(P) \wedge \{Q'_e\} \subseteq \{Q_e \sqcup^\sharp_e Q_b \mid \{Q_e\} \subseteq \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e)\{P\} \wedge \{Q_b\} \subseteq \mathsf{Post}^\sharp(\llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)\{P\} \wedge P \in \{P_e\}\} \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\mathsf{B};\mathsf{S}\,\underline{\{\!|}\,\{Q_{\bot\ell}\}\,\underline{|\!\}} \wedge Q_{\bot b} = \mathsf{gfp}^{\sqsubseteq^{\sharp}_{\infty}}\, F^{\sharp}_{p\bot} \wedge P \in \mathcal{P}\} \subseteq \mathcal{R}$ ≀def. (46) of $\sqcup^\sharp_e$⟆

$\Leftrightarrow \{\langle e: Q'_e, \bot: Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b}, br: P_{br}\rangle \mid \exists P_e \mathrel{.} P_e = \mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\, \vec{F}^{\sharp}_{pe}(P') \wedge \exists Q_e, Q_b, P \mathrel{.} Q'_e = Q_e \sqcup^\sharp_e Q_b \wedge \{Q_e\} \subseteq \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e)\{P\} \wedge \{Q_b\} \subseteq \mathsf{Post}^\sharp(\llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)\{P\} \wedge P \in \{P_e\} \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\mathsf{B};\mathsf{S}\,\underline{\{\!|}\,\{Q_{\bot\ell}\}\,\underline{|\!\}} \wedge Q_{\bot b} = \mathsf{gfp}^{\sqsubseteq^{\sharp}_{\infty}}\, F^{\sharp}_{p\bot} \wedge P' \in \mathcal{P}\} \subseteq \mathcal{R}$ ≀def. singleton and $\subseteq$, renaming⟆

$\Leftrightarrow \{\langle e: Q_e \sqcup^\sharp_e Q_b, \bot: Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b}, br: P_{br}\rangle \mid \exists P_e \mathrel{.} P_e = \mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\, \vec{F}^{\sharp}_{pe}(P') \wedge \exists P \mathrel{.} \{Q_e\} \subseteq \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e)\{P\} \wedge \{Q_b\} \subseteq \mathsf{Post}^\sharp(\llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)\{P\} \wedge P \in \{P_e\} \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\mathsf{B};\mathsf{S}\,\underline{\{\!|}\,\{Q_{\bot\ell}\}\,\underline{|\!\}} \wedge Q_{\bot b} = \mathsf{gfp}^{\sqsubseteq^{\sharp}_{\infty}}\, F^{\sharp}_{p\bot} \wedge P' \in \mathcal{P}\} \subseteq \mathcal{R}$ ≀replacing Q'_e by its value⟆

$\Leftrightarrow \{\langle e: Q_e \sqcup^\sharp_e Q_b, \bot: Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b}, br: P_{br}\rangle \mid \exists P_e \mathrel{.} P_e = \mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\, \vec{F}^{\sharp}_{pe}(P') \wedge \{Q_e\} \subseteq \mathsf{Post}^\sharp(\llbracket\neg\mathsf{B}\rrbracket^\sharp_e)\{P_e\} \wedge \{Q_b\} \subseteq \mathsf{Post}^\sharp(\llbracket\mathsf{B};\mathsf{S}\rrbracket^\sharp_b)\{P_e\} \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\mathsf{B};\mathsf{S}\,\underline{\{\!|}\,\{Q_{\bot\ell}\}\,\underline{|\!\}} \wedge Q_{\bot b} = \mathsf{gfp}^{\sqsubseteq^{\sharp}_{\infty}}\, F^{\sharp}_{p\bot} \wedge P' \in \mathcal{P}\} \subseteq \mathcal{R}$

≀corollary 8.3⟆

$\Leftrightarrow \{\langle e: Q_e \sqcup^\sharp_e Q_b, \bot: Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b}, br: P_{br}\rangle \mid \exists P_e \mathrel{.} P_e = \mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\, \vec{F}^{\sharp}_{pe}(P') \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\neg\mathsf{B}\,\underline{\{\!|}\,\{Q_e\}\,\underline{|\!\}} \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\mathsf{B};\mathsf{S}\,\underline{\{\!|}\,\{Q_b\}\,\underline{|\!\}} \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\mathsf{B};\mathsf{S}\,\underline{\{\!|}\,\{Q_{\bot\ell}\}\,\underline{|\!\}} \wedge Q_{\bot b} = \mathsf{gfp}^{\sqsubseteq^{\sharp}_{\infty}}\, F^{\sharp}_{p\bot} \wedge P' \in \mathcal{P}\} \subseteq \mathcal{R}$

$$\wr\text{def. (62) of } \underline{\{\!|}\,\mathcal{P}\,\underline{|\!\}}\,\texttt{S}\,\underline{\{\!|}\,\mathcal{Q}\,\underline{|\!\}} \triangleq (\mathcal{Q} \subseteq \mathsf{Post}^\sharp[\![\texttt{S}]\!]^\sharp\mathcal{P})\int$$

$$\Leftrightarrow\ (P_e = \mathsf{lfp}^{\sqsubseteq^\sharp_+}\,\vec{F}^\sharp_{pe}(P') \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\neg\texttt{B}\,\underline{\{\!|}\,\{Q_e\}\,\underline{|\!\}} \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\texttt{B;S}\,\underline{\{\!|}\,\{Q_b\}\,\underline{|\!\}} \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\texttt{B;S}\,\underline{\{\!|}\,\{Q_{\perp\ell}\}\,\underline{|\!\}} \wedge Q_{\perp b} = \mathsf{gfp}^{\sqsubseteq^\sharp_\infty}\,F^\sharp_{p\perp} \wedge P' \in \mathcal{P}) \Rightarrow \langle e : Q_e \sqcup^\sharp_e Q_b,\ \perp : Q_{\perp\ell} \sqcup^\sharp_\infty Q_{\perp b},\ br : P_{br}\rangle \in \mathcal{R} \qquad \wr\text{def. } \subseteq\int$$

$$\Leftrightarrow\ (P_e = \mathsf{lfp}^{\sqsubseteq^\sharp_+}\,\vec{F}^\sharp_{pe}(P') \wedge \overline{\{\!|}\,\{P_e\}\,\overline{|\!\}}\,\neg\texttt{B}\,\overline{\{\!|}\,\{Q_e\}\,\overline{|\!\}} \wedge \overline{\{\!|}\,\{P_e\}\,\overline{|\!\}}\,\texttt{B;S}\,\overline{\{\!|}\,\{Q_b\}\,\overline{|\!\}} \wedge \overline{\{\!|}\,\{P_e\}\,\overline{|\!\}}\,\texttt{B;S}\,\overline{\{\!|}\,\{Q_{\perp\ell}\}\,\overline{|\!\}} \wedge Q_{\perp b} = \mathsf{gfp}^{\sqsubseteq^\sharp_\infty}\,F^\sharp_{p\perp} \wedge P' \in \mathcal{P}) \Rightarrow \langle e : Q_e \sqcup^\sharp_e Q_b,\ \perp : Q_{\perp\ell} \sqcup^\sharp_\infty Q_{\perp b},\ br : P_{br}\rangle \in \mathcal{R} \qquad \wr\text{lemma 8.4}\int \qquad \square$$

Propositions 2.3 and 2.4 can be used to characterize the fixpoints of increasing functions in (70).

8.4 Calculational Design of the Proof System of the Lower Abstract Logic

Apart from (63)—(68), the sound and complete induction rules for the lower abstract logic are constructed by calculational design as follows.

Theorem 8.8 (Lower abstract logic proof system). *If $\mathbb{D}^\sharp$ is a well-defined increasing and decreasing chain-complete join semilattice with right upper continuous sequential composition $\fatsemi^\sharp$ then*

$$\frac{\forall Q \in \mathcal{Q}\ .\ \exists P \in \mathcal{P}, Q_1, Q_2\ .\ \underline{\{\!|}\,\{P\}\,\underline{|\!\}}\,\texttt{B;S}_1\,\underline{\{\!|}\,\{Q_1\}\,\underline{|\!\}} \wedge \underline{\{\!|}\,\{P\}\,\underline{|\!\}}\,\neg\texttt{B;S}_2\,\underline{\{\!|}\,\{Q_2\}\,\underline{|\!\}} \wedge Q = Q_1 \sqcup^\sharp Q_2}{\underline{\{\!|}\,\mathcal{P}\,\underline{|\!\}}\,\texttt{if (B) S}_1\texttt{ else S}_2\,\underline{\{\!|}\,\mathcal{Q}\,\underline{|\!\}}} \tag{74}$$

$$\frac{\begin{array}{c}\forall\langle e : Q'_e,\ \perp : Q'_\perp,\ br : Q'_{br}\rangle \in \mathcal{Q}\ .\ \exists Q_e, Q_b, Q_{\perp\ell}, Q_{\perp b}, P_e\ .\ Q'_e = Q_e \sqcup^\sharp_e Q_b \wedge Q'_\perp = \\ Q_{\perp\ell} \sqcup^\sharp_\infty Q_{\perp b} \wedge Q'_{br} = P'_{br} \wedge P_e = \mathsf{lfp}^{\sqsubseteq^\sharp_+}\,\vec{F}^\sharp_{pe}(P') \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\neg\texttt{B}\,\underline{\{\!|}\,\{Q_e\}\,\underline{|\!\}} \wedge \\ \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\texttt{B;S}\,\underline{\{\!|}\,\{Q_b\}\,\underline{|\!\}} \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\texttt{B;S}\,\underline{\{\!|}\,\{Q_{\perp\ell}\}\,\underline{|\!\}} \wedge Q_{\perp b} = \mathsf{gfp}^{\sqsubseteq^\sharp_\infty}\,F^\sharp_{p\perp} \wedge P' \in \mathcal{P}\end{array}}{\underline{\{\!|}\,\mathcal{P}\,\underline{|\!\}}\,\texttt{while (B) S}\,\underline{\{\!|}\,\mathcal{Q}\,\underline{|\!\}}} \tag{75}$$

Proof of theorem 8.8.

— $\underline{\{\!|}\,\mathcal{P}\,\underline{|\!\}}\,\texttt{if (B) S}_1\texttt{ else S}_2\,\underline{\{\!|}\,\mathcal{Q}\,\underline{|\!\}}$

$\Leftrightarrow\ \mathcal{Q} \subseteq \mathsf{Post}^\sharp[\![\texttt{if (B) S}_1\texttt{ else S}_2]\!]^\sharp\mathcal{P}$ $\qquad\wr$def. (62) of the logic triples$\int$

$\Leftrightarrow\ \mathcal{Q} \subseteq (\mathsf{Post}^\sharp[\![\texttt{B;S}_1]\!]^\sharp \sqcup^\sharp \mathsf{Post}^\sharp[\![\neg\texttt{B;S}_2]\!]^\sharp)\mathcal{P}$ $\qquad\wr$(53)$\int$

$\Leftrightarrow\ \mathcal{Q} \subseteq \{Q_1 \sqcup^\sharp Q_2 \mid Q_1 \in \mathsf{Post}^\sharp[\![\texttt{B;S}_1]\!]^\sharp\{P\} \wedge Q_2 \in \mathsf{Post}^\sharp[\![\neg\texttt{B;S}_2]\!]^\sharp\{P\} \wedge P \in \mathcal{P}\}$ $\qquad\wr$def. (46) of $\sqcup^\sharp$ $\int$

$\Leftrightarrow\ \forall Q \in \mathcal{Q}\ .\ \exists Q_1, Q_2, P\ .\ Q_1 \in \mathsf{Post}^\sharp[\![\texttt{B;S}_1]\!]^\sharp\{P\} \wedge Q_2 \in \mathsf{Post}^\sharp[\![\neg\texttt{B;S}_2]\!]^\sharp\{P\} \wedge P \in \mathcal{P} \wedge Q = Q_1 \sqcup^\sharp Q_2$ $\qquad\wr$def. $\subseteq\int$

$\Leftrightarrow\ \forall Q \in \mathcal{Q}\ .\ \exists Q_1, Q_2, P\ .\ \{Q_1\} \subseteq \mathsf{Post}^\sharp[\![\texttt{B;S}_1]\!]^\sharp\{P\} \wedge \{Q_2\} \subseteq \mathsf{Post}^\sharp[\![\neg\texttt{B;S}_2]\!]^\sharp\{P\} \wedge P \in \mathcal{P} \wedge Q = Q_1 \sqcup^\sharp Q_2$ $\qquad\wr$def. $\subseteq$ for singleton$\int$

$\Leftrightarrow\ \forall Q \in \mathcal{Q}\ .\ \exists Q_1, Q_2, P\ .\ \underline{\{\!|}\,\{P\}\,\underline{|\!\}}\,\texttt{B;S}_1\,\underline{\{\!|}\,\{Q_1\}\,\underline{|\!\}} \wedge \underline{\{\!|}\,\{P\}\,\underline{|\!\}}\,\neg\texttt{B;S}_2\,\underline{\{\!|}\,\{Q_2\}\,\underline{|\!\}} \wedge P \in \mathcal{P} \wedge Q = Q_1 \sqcup^\sharp Q_2$ $\qquad\wr$def. (62) of the logic triples$\int$

— $\underline{\{\!|}\,\mathcal{P}\,\underline{|\!\}}\,\texttt{while (B) S}\,\underline{\{\!|}\,\mathcal{Q}\,\underline{|\!\}}$

$\Leftrightarrow\ \mathcal{Q} \subseteq \mathsf{Post}^\sharp[\![\texttt{while (B) S}]\!]^\sharp\mathcal{P}$ $\qquad\wr$def. (62) of the logic triples$\int$

$\Leftrightarrow\ \mathcal{Q} \subseteq \{\langle e : Q_e,\ \perp : Q_{\perp\ell} \sqcup^\sharp_\infty Q_{\perp b},\ br : P_{br}\rangle \mid Q_e \in \mathsf{Post}^\sharp([\![\neg\texttt{B}]\!]^\sharp_e \sqcup^\sharp_e [\![\texttt{B;S}]\!]^\sharp_b)(\mathsf{lfp}^{\breve{\sqsubseteq}^\sharp_+}\,\breve{\vec{F}}^\sharp_{pe}(P)) \wedge Q_{\perp\ell} \in \mathsf{Post}^\sharp([\![\texttt{B;S}]\!]^\sharp_\perp)(\mathsf{lfp}^{\breve{\sqsubseteq}^\sharp_+}\,\breve{\vec{F}}^\sharp_{pe}(P)) \wedge Q_{\perp b} \in \mathsf{gfp}^{\breve{\sqsubseteq}^\sharp_\infty}\,(\breve{F}^\sharp_{p\perp}) \wedge P \in \mathcal{P}\}$ $\qquad\wr$(56)$\int$

$\Leftrightarrow\ \mathcal{Q} \subseteq \{\langle e : Q_e \sqcup^\sharp_e Q_b,\ \perp : Q_{\perp\ell} \sqcup^\sharp_\infty Q_{\perp b},\ br : P_{br}\rangle \mid \exists P_e\ .\ P_e = \mathsf{lfp}^{\sqsubseteq^\sharp_+}\,\vec{F}^\sharp_{pe}(P') \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\neg\texttt{B}\,\underline{\{\!|}\,\{Q_e\}\,\underline{|\!\}} \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\texttt{B;S}\,\underline{\{\!|}\,\{Q_b\}\,\underline{|\!\}} \wedge \underline{\{\!|}\,\{P_e\}\,\underline{|\!\}}\,\texttt{B;S}\,\underline{\{\!|}\,\{Q_{\perp\ell}\}\,\underline{|\!\}} \wedge Q_{\perp b} = \mathsf{gfp}^{\sqsubseteq^\sharp_\infty}\,F^\sharp_{p\perp} \wedge P' \in \mathcal{P}\}$

$\wr$following the same development as for the previous proof of (70)$\int$

$$\Leftrightarrow \forall\langle e:Q'_e, \bot:Q'_\bot, br:Q'_{br}\rangle \in \mathcal{Q} \mathrel{.} \exists Q_e, Q_b, Q_{\bot\ell}, Q_{\bot b}, P_e \mathrel{.} Q'_e = Q_e \sqcup^\sharp_e Q_b \wedge Q'_\bot = Q_{\bot\ell} \sqcup^\sharp_\infty Q_{\bot b} \wedge Q'_{br} = P'_{br} \wedge P_e = \mathsf{lfp}^{\sqsubseteq^\sharp_+}\vec{F}^\sharp_{pe}(P') \wedge \underline{\{\!\!|}\,\{P_e\}\,\underline{|\!\!\}}\,\neg\mathsf{B}\,\underline{\{\!\!|}\,\{Q_e\}\,\underline{|\!\!\}} \wedge \underline{\{\!\!|}\,\{P_e\}\,\underline{|\!\!\}}\,\mathsf{B};\mathsf{S}\,\underline{\{\!\!|}\,\{Q_b\}\,\underline{|\!\!\}} \wedge \underline{\{\!\!|}\,\{P_e\}\,\underline{|\!\!\}}\,\mathsf{B};\mathsf{S}\,\underline{\{\!\!|}\,\{Q_{\bot\ell}\}\,\underline{|\!\!\}} \wedge Q_{\bot b} = \mathsf{gfp}^{\sqsubseteq^\sharp_\infty} F^\sharp_{p\bot} \wedge P' \in \mathcal{P} \qquad \text{(def. }\subseteq\text{)} \qquad \square$$

Part II: Abstraction of Semantics, Execution Properties, Semantic (Hyper) Properties, Calculi, and Logics

Since hyperlogics deal with properties of semantics, there are four levels at which an abstraction can be applied.

(1) The first level is that of the program semantics considered in appendix sect. 9 and illustrated by the relational semantics in example 9.4 abstracting the trace semantics of sect. 4. This abstraction is common in transformational logics [21] such as Hoare logic [55] but also in hyperlogics [29, 30]; (76)

(2) The second level is that of program properties of sect. 6.1;

(3) The third level is that of program hyperproperties of sect. 7;

(4) The fourth level is that of the abstract logics of sect. 8.

Because logics are required to be sound and complete, abstractions should be exact so that any proof of abstract properties in the concrete should be doable in the abstract. This relies on Galois retractions in sect. 2.5. The main result is that the abstraction of a logic of semantic (hyper) properties of sect. 8 is a a logic of semantic (hyper) properties.

9 Abstraction of the Abstract Semantics

We show that the abstraction of an instance of the abstract semantics is itself an instance of the abstract semantics.

Definition 9.1 (Semantic abstraction). We say that $\bar{\mathbb{D}}^\sharp \triangleq \langle\bar{\mathbb{D}}^\sharp_+,\ \bar{\mathbb{D}}^\sharp_\infty\rangle$ is an exact (respectively approximate) abstraction of an abstract domain $\mathbb{D}^\sharp \triangleq \langle\mathbb{D}^\sharp_+,\ \mathbb{D}^\sharp_\infty\rangle$ if and only if

A. There exists a Galois retraction $\langle\mathbb{L}^\sharp_+,\ \sqsubseteq^\sharp_+\rangle \underset{\alpha_+}{\overset{\gamma_+}{\leftrightarrows}} \langle\bar{\mathbb{L}}^\sharp_+,\ \bar{\sqsubseteq}^\sharp_+\rangle$;

B. $\alpha_+(\mathsf{init}^\sharp) = \overline{\mathsf{init}}^\sharp$, $\alpha_+ \circ \mathsf{assign}^\sharp[\![\mathsf{x},\mathsf{A}]\!] = \overline{\mathsf{assign}}^\sharp[\![\mathsf{x},\mathsf{A}]\!] \circ \alpha_+$, $\alpha_+ \circ \mathsf{rassign}^\sharp[\![\mathsf{x},a,b]\!] = \overline{\mathsf{rassign}}^\sharp[\![\mathsf{x},a,b]\!] \circ \alpha_+$, $\alpha_+ \circ \mathsf{test}^\sharp[\![\mathsf{B}]\!] = \overline{\mathsf{test}}^\sharp[\![\mathsf{B}]\!] \circ \alpha_+$, $\alpha_+(\mathsf{break}^\sharp) = \overline{\mathsf{break}}^\sharp$, and $\alpha_+(\mathsf{skip}^\sharp) = \overline{\mathsf{skip}}^\sharp$;

C. There exists a Galois retraction $\langle\mathbb{L}^\sharp_\infty,\ \sqsupseteq^\sharp_\infty\rangle \underset{\alpha_\infty}{\overset{\gamma_\infty}{\leftrightarrows}} \langle\bar{\mathbb{L}}^\sharp_\infty,\ \bar{\sqsupseteq}^\sharp_\infty\rangle$ (i.e. α_∞ preserves existing $\sqcap^\sharp_\infty$);

D. For $S \in \mathbb{L}^\sharp_+$, $\alpha_+(S \mathbin{\fatsemi^\sharp} S') = \alpha_+(S) \mathbin{\bar{\fatsemi}^\sharp} \alpha_+(S')$ when $S' \in \mathbb{L}^\sharp_+$ and $\alpha_\infty(S \mathbin{\fatsemi^\sharp} S') = \alpha_\infty(S) \mathbin{\bar{\fatsemi}^\sharp} \alpha_\infty(S')$ when $S' \in \mathbb{L}^\sharp_\infty$.

(respectively "$\bar{\sqsubseteq}^\sharp_+$" or "$\bar{\sqsupseteq}^\sharp_\infty$" instead of "=" and $\leftrightarrows$ instead of $\underset{}{\overset{}{\leftrightarrows}}$ for approximate abstractions);

Following (12), the abstraction of the semantic domain and semantics are

$$\begin{array}{rcl} \bar{\mathbb{L}}^\sharp & \triangleq & (e:\bar{\mathbb{L}}^\sharp_+ \times \bot:\bar{\mathbb{L}}^\sharp_\infty \times br:\bar{\mathbb{L}}^\sharp_+) \\ \alpha(\langle e:S_+,\ \bot:S_\infty,\ br:S_{br}\rangle) & \triangleq & \langle e:\alpha_+(S_+),\ \bot:\alpha_\infty(S_\infty),\ br:\alpha_+(S_{br})\rangle \end{array} \tag{77}$$

are well-defined such that

$$\langle\mathbb{L}^\sharp,\ \sqsubseteq^\sharp\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle\bar{\mathbb{L}}^\sharp,\ \bar{\sqsubseteq}^\sharp\rangle. \tag{78}$$

Lemma 9.2. *An exact abstraction $\bar{\mathbb{D}}^\sharp \triangleq \langle \bar{\mathbb{D}}^\sharp_+, \bar{\mathbb{D}}^\sharp_\infty \rangle$ of a well-defined concrete domain $\mathbb{D}^\sharp \triangleq \langle \mathbb{D}^\sharp_+, \mathbb{D}^\sharp_\infty \rangle$ satisfying any one of the hypotheses 3.2.D.a to 3.2.D.d.i to 3.2.D.d.iv of definition 3.2 is a well-defined abstract domain of the same nature.*

Proof of lemma 9.2. Lemma 9.2 follows from the fact that in Galois connections the abstraction preserves existing joins [20, lemma 11.38]. and in Galois retractions $\alpha \circ \gamma$ is the identity [20, exercise 11.50]. □

Theorem 9.3. *If $\bar{\mathbb{D}}^\sharp$ is an exact (respectively approximate) abstraction of $\mathbb{D}^\sharp$ then $\forall \mathsf{S} \in \mathbb{S} \,.\, \bar{[\![\mathsf{S}]\!]}^\sharp = \alpha([\![\mathsf{S}]\!]^\sharp)$ (respectively "$\bar{\sqsubseteq}^\sharp$" instead of "$=$" for approximate abstractions).*

Proof of theorem 9.3. The proof of theorem 9.3 is an easy generalization of that of theorem 27.8 and corollary 27.20 of [20]. □

Example 9.4 (Relational semantics). The relational semantics $[\![\mathsf{S}]\!]^\varrho$ of [21] is the following abstraction of the trace semantics $[\![\mathsf{S}]\!]^\pi$.

$$\alpha_+(S) \;\triangleq\; \{\langle\sigma,\, \sigma'\rangle \mid \exists \pi \,.\, \sigma\pi\sigma' \in S \cap \Sigma^+\} \qquad\qquad \alpha_\infty(S) \;\triangleq\; \{\langle\sigma,\, \bot\rangle \mid \exists \pi \,.\, \sigma\pi \in S \cap \Sigma^\infty\}$$

It follows, by theorem 9.3, that $\forall \mathsf{S} \in \mathbb{S} \,.\, [\![\mathsf{S}]\!]^\varrho = \alpha([\![\mathsf{S}]\!]^\pi)$ and by a classic calculational design, we would get the relational semantics of [21, sect. I.1] (recalled in sect. 5 as a specific instance of the algebraic semantics of sect. 3). ■

10 Induced Abstraction of the Execution Transformer

We have defined properties of program executions as program semantics in $\mathbb{L}^\sharp$ (12). This formalizes the observation that program semantics specify exactly the properties of all possible executions of any program of the language. An abstraction (77) of the semantics in definition 9.1 induces an execution transformer $\overline{\mathsf{post}}^\sharp \in \bar{\mathbb{L}}^\sharp \xrightarrow{\nearrow} \bar{\mathbb{L}}^\sharp \xrightarrow{\nearrow} \bar{\mathbb{L}}^\sharp$ (25) for this abstract semantics

$$\begin{array}{rcl} \bar{\alpha}(\mathsf{p}) & \triangleq & \boldsymbol{\lambda}\bar{S} \bullet \boldsymbol{\lambda}\bar{P} \bullet \alpha(\mathsf{p}(\gamma(\bar{S}))\gamma(\bar{P})) \\ \overline{\mathsf{post}}^\sharp(\bar{S})\bar{P} & \triangleq & \bar{\alpha}(\mathsf{post}^\sharp)(\bar{S})\bar{P} \;\;=\;\; \alpha(\mathsf{post}^\sharp(\gamma(\bar{S}))\gamma(\bar{P})) \;\;=\;\; \bar{P} \mathbin{\bar{\fatsemi}^\sharp} \bar{S} \end{array} \tag{79}$$

Proof of (79).

$$\begin{array}{ll} & \alpha(\mathsf{post}^\sharp(\gamma(\bar{S}))\gamma(\bar{P})) \\ = & \alpha(\gamma(\bar{P}) \mathbin{\fatsemi^\sharp} \gamma(\bar{S})) \hfill \text{(def. (25) of post}^\sharp\text{)} \\ = & \alpha(\gamma(\bar{P})) \mathbin{\bar{\fatsemi}^\sharp} \alpha(\gamma(\bar{S})) \hfill \text{(case 9.1.D of definition 9.1 applied component wise)} \\ = & \bar{P} \mathbin{\bar{\fatsemi}^\sharp} \bar{S} \hfill \text{(component wise Galois retraction)} \end{array}$$ □

Notice that defining $\bar{\gamma}(\bar{\mathsf{p}}) \triangleq \boldsymbol{\lambda} S \bullet \boldsymbol{\lambda} P \bullet \gamma(\bar{\mathsf{p}}(\alpha(S))\alpha(P))$, we have a Galois retraction

$$\langle \mathbb{L}^\sharp \xrightarrow{\nearrow} \mathbb{L}^\sharp \xrightarrow{\nearrow} \mathbb{L}^\sharp,\, \sqsubseteq^\sharp \rangle \; \underset{\bar{\alpha}}{\overset{\bar{\gamma}}{\leftrightarrows}} \; \langle \bar{\mathbb{L}}^\sharp \xrightarrow{\nearrow} \bar{\mathbb{L}}^\sharp \xrightarrow{\nearrow} \bar{\mathbb{L}}^\sharp,\, \bar{\sqsubseteq}^\sharp \rangle \tag{80}$$

Proof of (80). By [20, th. 11.78], we have a Galois connection. The retraction follows from

$$\begin{array}{ll} & \bar{\alpha}(\bar{\gamma}(\bar{\mathsf{p}})) \\ = & \boldsymbol{\lambda}\bar{S} \bullet \boldsymbol{\lambda}\bar{P} \bullet \alpha(\bar{\gamma}(\bar{\mathsf{p}})(\gamma(\bar{S}))\gamma(\bar{P})) \hfill \text{(def. (79) of } \bar{\alpha}\text{)} \\ = & \boldsymbol{\lambda}\bar{S} \bullet \boldsymbol{\lambda}\bar{P} \bullet \alpha(\gamma(\bar{\mathsf{p}}(\alpha(\gamma(\bar{S})))\alpha(\gamma(\bar{P})))) \hfill \text{(def. } \bar{\gamma}(\bar{\mathsf{p}}) \triangleq \boldsymbol{\lambda} S \bullet \boldsymbol{\lambda} P \bullet \gamma(\bar{\mathsf{p}}(\alpha(S))\alpha(P))\text{)} \\ = & \boldsymbol{\lambda}\bar{S} \bullet \boldsymbol{\lambda}\bar{P} \bullet \bar{\mathsf{p}}(\bar{S})\bar{P} \hfill \text{(Galois retraction (78) and [20, exercise 11.50])} \\ = & \bar{\mathsf{p}} \hfill \text{(def. lambda-notation and [20, exercise 11.50])} \end{array}$$ □

such that $\overline{\mathrm{post}}^\sharp = \bar{\alpha}(\mathrm{post})$ in (79). Observe that if an abstraction $\bar{\mathbb{D}}^\sharp \triangleq \langle \bar{\mathbb{D}}^\sharp_+,\ \bar{\mathbb{D}}^\sharp_\infty \rangle$ of an abstract domain $\mathbb{D}^\sharp \triangleq \langle \mathbb{D}^\sharp_+,\ \mathbb{D}^\sharp_\infty \rangle$ is commuting (82) then

$$\alpha(\mathrm{post}^\sharp(\gamma(\bar{S}))P) \quad = \quad \overline{\mathrm{post}}^\sharp(\bar{S})(\alpha(P)) \tag{81}$$

Proof of (81).

$$\begin{aligned}
& \alpha(\mathrm{post}^\sharp(\gamma(\bar{S}))P) \\
= \ & \alpha(P \fatsemi^\sharp \gamma(\bar{S})) && \text{⟅def. (25) of } \mathrm{post}^\sharp\text{⟆} \\
= \ & \alpha(P) \mathbin{\bar{\fatsemi}^\sharp} \bar{S} && \text{⟅commutation (82)⟆} \\
= \ & \overline{\mathrm{post}}^\sharp(\bar{S})(\alpha(P)) && \text{⟅characterization (79) of } \overline{\mathrm{post}}^\sharp\text{⟆} \quad \square
\end{aligned}$$

Lemma 10.1 (Commutation). *If the abstraction* $\bar{\mathbb{D}}^\sharp \triangleq \langle \bar{\mathbb{D}}^\sharp_+,\ \bar{\mathbb{D}}^\sharp_\infty \rangle$ *of an abstract domain* $\mathbb{D}^\sharp \triangleq \langle \mathbb{D}^\sharp_+,\ \mathbb{D}^\sharp_\infty \rangle$ *is exact then*

$$\alpha(P \fatsemi^\sharp \gamma(\bar{S})) \quad = \quad \alpha(P) \mathbin{\bar{\fatsemi}^\sharp} \bar{S} \qquad \textit{and} \qquad \alpha(\mathrm{post}(\gamma(\bar{S}))P) \quad = \quad \overline{\mathrm{post}}(\bar{S})(\alpha(P)) \tag{82}$$

Lemma 10.1 shows that doing the computation in the concrete and then abstracting is equivalent to doing the computation in the abstract. Relative to the abstraction, no information is lost.

Proof of lemma 10.1.

$$\begin{aligned}
— \ & \alpha(P \fatsemi^\sharp \gamma(\bar{S})) \\
= \ & \alpha(P) \mathbin{\bar{\fatsemi}^\sharp} \alpha(\gamma(\bar{S})) && \text{⟅commutation 9.1.D⟆} \\
= \ & \alpha(P) \mathbin{\bar{\fatsemi}^\sharp} \bar{S} && \text{⟅Galois retraction (78). Q.E.D.⟆}
\end{aligned}$$

$$\begin{aligned}
— \ & \alpha(\mathrm{post}(\gamma(\bar{S}))P) \\
= \ & \alpha(P \fatsemi^\sharp (\gamma(\bar{S}))) && \text{⟅def. (25) of } \mathrm{post}^\sharp\text{⟆} \\
= \ & \alpha(P) \mathbin{\bar{\fatsemi}^\sharp} \bar{S} && \text{⟅as previously shown⟆} \\
= \ & \overline{\mathrm{post}}(\bar{S})(\alpha(P)) && \text{⟅(79⟆} \quad \square
\end{aligned}$$

□

Moreover, instead of deriving the Galois connection (80) from that (78), we can start directly from an abstraction of post given by (80). The abstract semantics is then $\bar{S} = \overline{\mathrm{post}}^\sharp(\bar{S})$skip proving the equivalence of (76.1) and (76.2).

11 Induced Abstraction of the Semantic Transformer

The semantics transformer $\overline{\mathrm{Post}}^\sharp \in \bar{\mathbb{L}}^\sharp \to \wp(\bar{\mathbb{L}}^\sharp) \to \wp(\bar{\mathbb{L}}^\sharp)$ for this abstract semantics is

$$\bar{\alpha}(\mathsf{P}) \quad \triangleq \quad \boldsymbol{\lambda} \bar{S} \bullet \boldsymbol{\lambda} \bar{\mathcal{P}} \bullet \{\alpha(R) \mid R \in \mathsf{P}(\gamma(\bar{S}))(\{\gamma(\bar{P}) \mid \bar{P} \in \bar{\mathcal{P}}\})\} \tag{83}$$

$$\overline{\mathrm{Post}}^\sharp(\bar{S})\bar{\mathcal{P}} \quad \triangleq \quad \bar{\alpha}(\mathrm{Post}^\sharp)(\bar{S})\bar{\mathcal{P}} \quad = \quad \{\overline{\mathrm{post}}^\sharp(\bar{S})\bar{P} \mid \bar{P} \in \bar{\mathcal{P}}\} \tag{84}$$

Proof of (84).

$$\begin{aligned}
& \overline{\mathrm{Post}}^\sharp(\bar{S})\bar{\mathcal{P}} \\
\triangleq \ & \bar{\alpha}(\mathrm{Post}^\sharp)(\bar{S})\bar{\mathcal{P}} && \text{⟅def. (84) of } \overline{\mathrm{Post}}^\sharp\text{⟆} \\
= \ & \{\alpha(R) \mid R \in \mathrm{Post}^\sharp(\gamma(\bar{S}))(\{\gamma(\bar{P}) \mid \bar{P} \in \bar{\mathcal{P}}\})\} && \text{⟅def. (83) of } \bar{\alpha}\text{⟆} \\
= \ & \{\alpha(R) \mid R \in \{\mathrm{post}^\sharp(\gamma(\bar{S}))P \mid P \in (\{\gamma(\bar{P}) \mid \bar{P} \in \bar{\mathcal{P}}\})\}\} && \text{⟅def. (40) of } \mathrm{Post}^\sharp\text{⟆} \\
= \ & \{\alpha(\mathrm{post}^\sharp(\gamma(\bar{S}))(\gamma(\bar{P}))) \mid \bar{P} \in \bar{\mathcal{P}}\} && \text{⟅def. } \in\text{⟆} \\
= \ & \{\overline{\mathrm{post}}^\sharp(\bar{S})\bar{P} \mid \bar{P} \in \bar{\mathcal{P}}\} && \text{⟅(79)⟆} \quad \square
\end{aligned}$$

Example 11.1 (Transformers for the relational semantics). For the relational semantics of example 9.4, the composition is $S \,\bar{\fatsemi}^{\varrho}\, S' = (S \cap (\Sigma \times \{\bot\})) \cup (S \cap (\Sigma \times \Sigma) \circ S')$ (intuitively $\mathsf{S}_1\,;\mathsf{S}_2$ does not terminate if S_1 does not terminate or S_1 terminates but S_2 doesn't and terminates if both S_1 and S_2 terminate with the composition of their effects). Then $\overline{\mathsf{Post}}^{\varrho}[\![\mathsf{S}]\!]^{\varrho}\mathcal{P} = \{P \,\bar{\fatsemi}^{\varrho}\, [\![\mathsf{S}]\!]^{\varrho} \mid P \in \mathcal{P}\}$ so that if $\mathcal{P}$ is a precondition relating the initial states of the command S to those of the program then $\overline{\mathsf{Post}}^{\varrho}[\![\mathsf{S}]\!]^{\varrho}$ relates the final states of the command S or nontermination to the initial states of the program. ■

We have the Galois retraction

$$\langle \mathbb{L}^\sharp \to \wp(\mathbb{L}^\sharp) \xrightarrow{\nearrow} \wp(\mathbb{L}^\sharp),\ \subseteq\rangle \underset{\bar{\bar{\alpha}}}{\overset{\bar{\bar{\gamma}}}{\leftrightarrows}} \langle \bar{\mathbb{L}}^\sharp \to \wp(\bar{\mathbb{L}}^\sharp) \xrightarrow{\nearrow} \wp(\bar{\mathbb{L}}^\sharp),\ \subseteq\rangle \tag{85}$$

Proof of (85). $\bar{\bar{\alpha}}$ preserves arbitrary point wise union $\cup$. □

Observe that instead of deriving (85) from (80), it is equivalent to start from a Galois retraction (85) since we can recover post from Post by (43).

12 Induced Abstraction of the Abstract Logics

Writing $f(X) \triangleq \{f(x) \mid x \in X\}$, the abstract logic $\overline{\mathsf{L}}^\sharp \in \bar{\mathbb{L}}^\sharp \to (\wp(\bar{\mathbb{L}}^\sharp) \times \wp(\bar{\mathbb{L}}^\sharp))$ is

$$\bar{\bar{\bar{\alpha}}}(\mathsf{L}) \triangleq \boldsymbol{\lambda}\bar{S} \bullet \{\langle\bar{\mathcal{P}},\ \bar{\mathcal{Q}}\rangle \mid \alpha(\textstyle\bigcap\{\mathcal{Q} \mid \langle\gamma(\bar{\mathcal{P}}),\ \mathcal{Q}\rangle \in \mathsf{L}(\gamma(\bar{S}))\}) \subseteq \bar{\mathcal{Q}}\} \tag{86}$$

$$\overline{\overline{\mathsf{L}}}^\sharp(\bar{S}) \triangleq \bar{\bar{\bar{\alpha}}}(\overline{\mathsf{L}}^\sharp)(\bar{S}) \qquad\qquad \underline{\overline{\mathsf{L}}}^\sharp(\bar{S}) \triangleq \bar{\bar{\bar{\alpha}}}(\underline{\mathsf{L}}^\sharp)(\bar{S}) \tag{87}$$

Theorem 12.1. *If $\bar{\mathbb{D}}^\sharp$ is an exact abstraction of $\mathbb{D}^\sharp$ then $\overline{\overline{L}}^\sharp(\bar{S}) = \{\langle\bar{\mathcal{P}},\ \bar{\mathcal{Q}}\rangle \mid \overline{\mathsf{Post}}^\sharp(\bar{S})\bar{\mathcal{P}} \subseteq \bar{\mathcal{Q}}\}$ (and $\underline{\overline{L}}^\sharp(\bar{S}) = \{\langle\bar{\mathcal{P}},\ \bar{\mathcal{Q}}\rangle \mid \bar{\mathcal{Q}} \subseteq \overline{\mathsf{Post}}^\sharp(\bar{S})\bar{\mathcal{P}}\}$).*

Proof of theorem 12.1.

$$\begin{aligned}
&\overline{\overline{\mathsf{L}}}^\sharp(\bar{S}) = \bar{\bar{\bar{\alpha}}}(\overline{\mathsf{L}}^\sharp)(\bar{S}) && \text{⟅(87)⟆}\\
={}& \{\langle\bar{\mathcal{P}},\ \bar{\mathcal{Q}}\rangle \mid \alpha(\textstyle\bigcap\{\mathcal{Q} \mid \langle\gamma(\bar{\mathcal{P}}),\ \mathcal{Q}\rangle \in \mathsf{L}(\gamma(\bar{S}))\}) \subseteq \bar{\mathcal{Q}}\} && \text{⟅(86)⟆}\\
={}& \{\langle\bar{\mathcal{P}},\ \bar{\mathcal{Q}}\rangle \mid \alpha(\textstyle\bigcap\{\mathcal{Q} \mid \langle\gamma(\bar{\mathcal{P}}),\ \mathcal{Q}\rangle \in \{\langle\mathcal{P},\ \mathcal{Q}\rangle \mid \mathsf{Post}^\sharp(\gamma(\bar{S}))\mathcal{P} \subseteq \mathcal{Q}\}\}) \subseteq \bar{\mathcal{Q}}\} && \text{⟅def. (60) of } \overline{\mathsf{L}}^\sharp\text{⟆}\\
={}& \{\langle\bar{\mathcal{P}},\ \bar{\mathcal{Q}}\rangle \mid \alpha(\textstyle\bigcap\{\mathcal{Q} \mid \mathsf{Post}^\sharp(\gamma(\bar{S}))\gamma(\bar{\mathcal{P}}) \subseteq \mathcal{Q}\}) \subseteq \bar{\mathcal{Q}}\} && \text{⟅def. } \in\text{⟆}\\
={}& \{\langle\bar{\mathcal{P}},\ \bar{\mathcal{Q}}\rangle \mid \alpha(\{\mathsf{Post}^\sharp(\gamma(\bar{S}))\gamma(\bar{\mathcal{P}})\}) \subseteq \bar{\mathcal{Q}}\} && \text{⟅def. } \textstyle\bigcap \text{ and } \subseteq\text{⟆}\\
={}& \{\langle\bar{\mathcal{P}},\ \bar{\mathcal{Q}}\rangle \mid \alpha(\{\mathsf{post}^\sharp(\gamma(\bar{S}))P \mid P \in \gamma(\bar{\mathcal{P}})\}) \subseteq \bar{\mathcal{Q}}\} && \text{⟅def. (40) of } \mathsf{Post}^\sharp\text{⟆}\\
={}& \{\langle\bar{\mathcal{P}},\ \bar{\mathcal{Q}}\rangle \mid \{\alpha(\mathsf{post}^\sharp(\gamma(\bar{S}))P) \mid P \in \gamma(\bar{\mathcal{P}})\} \subseteq \bar{\mathcal{Q}}\} && \text{⟅def. image⟆}\\
={}& \{\langle\bar{\mathcal{P}},\ \bar{\mathcal{Q}}\rangle \mid \forall \bar{P} \in \bar{\mathcal{P}}\ .\ \alpha(\mathsf{post}^\sharp(\gamma(\bar{S}))\gamma(\bar{P})) \in \bar{\mathcal{Q}}\} && \text{⟅def. } \subseteq\text{⟆}\\
={}& \{\langle\bar{\mathcal{P}},\ \bar{\mathcal{Q}}\rangle \mid \forall \bar{P} \in \bar{\mathcal{P}}\ .\ \overline{\mathsf{post}}^\sharp(\bar{S})\bar{P} \in \bar{\mathcal{Q}}\} && \text{⟅def. (79) of } \overline{\mathsf{post}}^\sharp\text{⟆}\\
={}& \{\langle\bar{\mathcal{P}},\ \bar{\mathcal{Q}}\rangle \mid \{\overline{\mathsf{post}}^\sharp(\bar{S})\bar{P} \mid \bar{P} \in \bar{\mathcal{P}}\} \subseteq \bar{\mathcal{Q}}\} && \text{⟅def. } \subseteq\text{⟆}\\
={}& \{\langle\bar{\mathcal{P}},\ \bar{\mathcal{Q}}\rangle \mid \overline{\mathsf{Post}}^\sharp(\bar{S})\bar{\mathcal{P}} \subseteq \bar{\mathcal{Q}}\} && \text{⟅def. (84) of } \overline{\mathsf{Post}}^\sharp\text{⟆}
\end{aligned}$$

The proof for $\underline{\overline{\mathsf{L}}}^\sharp$ is $\subseteq$-dual. □

It follows from theorem 12.1 that the logic proof system of theorem 8.5 is applicable to the upper abstract logic $\overline{\overline{\mathsf{L}}}^\sharp(\bar{S})$ (and dually theorem 8.8 for the lower abstract logic).

In conclusion of this part II, although the abstractions of the semantics, post, Post, and logics have been shown to be equally expressible for exact abstractions, they do not really solve the problem of the complexity of the resulting logic (although hyperproperties may be simpler). The logics still have to handle exactly the (abstract) semantics occurring in the (hyper) properties. So our proposed proof system has rules (63)—(70) plus simplified rules applicable to less general classes of properties defined by the abstractions studied in the following part III.

Part III: Abstractions for Semantic (Hyper) Logics

The problem with (hyper) logics studied in part I (and their abstractions in part II) is that for a program to satisfy a semantic (hyper) property, its semantics must exactly occur in this (hyper) property and therefore the proof must exactly characterize the program semantics. So, contrary to Hoare logic or its dual, (hyper) proof rules cannot make over or under approximations of the program semantics in semantic properties. In this part III, we study abstractions of semantic properties that yield simpler sound and complete proof rules for the less general semantic (hyper) properties defined by the abstraction. Such abstractions can also provide representations of abstract semantic (hyper) properties[3].

13 Semantic to Execution Property Abstraction

13.1 Join Abstraction

13.1.1 Definition of the Join Abstraction. In a complete lattice, the abstraction $\alpha_\sqcup(\mathcal{P}) \triangleq \bigsqcup\mathcal{P}$ and $\gamma_\sqcup(Q) \triangleq \{P \mid P \sqsubseteq Q\}$ yields a Galois retraction.

$$\langle\wp(\mathbb{L}),\ \subseteq\rangle \underset{\alpha_\sqcup}{\overset{\gamma_\sqcup}{\leftrightarrows}} \langle\mathbb{L},\ \sqsubseteq\rangle \qquad \text{and so} \qquad \langle\wp(\mathbb{L}),\ \subseteq\rangle \underset{\gamma_\sqcup \circ \alpha_\sqcup}{\overset{\mathbb{1}}{\leftrightarrows}} \langle\gamma_\sqcup \circ \alpha_\sqcup(\wp(\mathbb{L})),\ \subseteq\rangle \tag{88}$$

Proof of (88).

$$\begin{aligned}
& \alpha_\sqcup(\mathcal{P}) \sqsubseteq Q \\
\Leftrightarrow\ & \textstyle\bigsqcup\mathcal{P} \sqsubseteq Q && \text{(def. } \alpha_\sqcup\text{)} \\
\Leftrightarrow\ & \forall P \in \mathcal{P}\ .\ P \sqsubseteq Q && \text{(def. least upper bound)} \\
\Leftrightarrow\ & \mathcal{P} \subseteq \{P \mid P \sqsubseteq Q\} && \text{(def. } \subseteq\text{)} \\
\Leftrightarrow\ & \mathcal{P} \subseteq \gamma_\sqcup(Q) && \text{(def. } \gamma_\sqcup\text{)}
\end{aligned}$$

It follows that $\gamma_\sqcup \circ \alpha_\sqcup$ is an upper closure operator hence the second Galois retraction. □

The properties in $\gamma_\sqcup \circ \alpha_\sqcup(\wp(\mathbb{L}))$ are called execution properties as opposed to semantic (hyper) properties in $\wp(\mathbb{L})$. If the abstract domains $\mathbb{D}^\sharp$ of definition 3.2 or their abstractions by definition 9.1 are complete lattices, this abstraction approximates abstracts semantic properties in $\wp(\mathbb{L}^\sharp)$ into executions in $\mathbb{L}^\sharp$.

Example 13.1 (Trace property abstraction). The trace hyperproperties in $\wp(\wp(\Sigma^{+\infty}))$ can be abstracted to trace properties in $\wp(\Sigma^{+\infty})$ by $\langle\wp(\wp(\Sigma^{+\infty}),\ \subseteq\rangle \underset{\alpha_\cup}{\overset{\gamma_\cup}{\leftrightarrows}} \langle\wp(\Sigma^{+\infty})),\ \subseteq\rangle$ with $\alpha_\cup(P) = \bigcup P$ and $\gamma_\cup(Q) = \wp(Q)$ as done e.g. in [27, section 5, p. 246] which is the starting point of [21] to recover Hoare logic and its variants. $\gamma_\cup(P)$ is called the lift of trace property $P \in \wp(\Sigma^{+\infty})$ in [14, page 1162]. ■

Example 13.2 (Hyperlogic to execution logic abstraction). Applied to $\mathrm{Post}^\sharp(S)$ in (40) this join abstraction yields $\mathrm{post}^\sharp(S)$ in (25), so that the hyperproperty calculus of theorem 7.4 is abstracted into the execution property calculus of theorem 6.5 and therefore the hyperlogic of theorem 8.5 is abstracted in the classic program logic of execution properties (as considered in [21], after appropriate generalization to the algebraic semantics of section 3). ■

[3] Another example is the possible representation of semantic properties satisfying the decreasing chain condition by join irreducibles [11, theorem 4.8].

13.1.2 Proof Rule Simplification. By correspondence (88), the abstract logical ordering (abstracting the implication $\subseteq$) is also the computational ordering in lemma 3.14 whereas, in general, for the generic algebraic abstract semantics the computational ordering $\sqsubseteq^\sharp$ and the logical ordering and $\subseteq$ are not directly related, which is at the origin of complications in proofs. Therefore, the `while` rule (70) can be simplified since fixpoints can be over approximated (or under approximated) hence handled by fixpoint induction such as Park induction [21, theorem II.3.1] or Scott-Kleene induction [21, theorem II.3.6].

14 Homomorphic Semantic Abstraction

Given an execution property abstraction $\alpha \in \mathbb{L}^\sharp \to \mathbb{A}$, it can be extended elementwise to $\langle \wp(\mathbb{L}^\sharp), \subseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \wp(\mathbb{A}), \subseteq\rangle$ by $\alpha(\mathcal{P}) \triangleq \{\alpha(P) \mid P \in \mathcal{P}\}$ and $\gamma(\mathcal{Q}) \triangleq \{P \mid \alpha(P) \in \mathcal{Q}\}$.

Example 14.1 (Partial hypercorrectness). Partial hypercorrectness consists in ignoring one component $\mathbb{D}^\sharp_+$ or $\mathbb{D}^\sharp_\infty$ of the abstract domain and preserving only the other, that is $\alpha^+(\langle e : P_+,\ \bot : P_\infty,\ br : P_b\rangle) \triangleq \langle ok : P_+,\ br : P_b\rangle$ or $\alpha^\infty(\langle e : P_+,\ \bot : P_\infty,\ br : P_b\rangle) \triangleq P_\infty$ in (12). This execution property abstraction α is extended to semantic properties by the homomorphic abstraction $\alpha(\mathcal{P}) \triangleq \{\alpha(P) \mid P \in \mathcal{P}\}$. This yields a Galois retraction $\langle \wp(\mathbb{L}^\sharp), \subseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \alpha(\wp(\mathbb{L}^\sharp)), \subseteq\rangle$ hence a closure $\langle \wp(\mathbb{L}^\sharp), \subseteq\rangle \underset{\gamma\circ\alpha}{\overset{\mathbb{1}}{\leftrightarrows}} \langle \gamma \circ \alpha(\wp(\mathbb{L}^\sharp)), \subseteq\rangle$. This is an extension of partial correctness or termination to semantic (hyper) properties. The `while` rule (70) can be simplified by ignoring one of the two fixpoints. However, the other fixpoint must still be calculated exactly. ■

Example 14.2 (Trace safety hyperproperties). The safety abstraction α by prefix and limit abstraction of trace properties [27, section 6.1] can be applied to the trace semantic (hyper) properties of section 4 so that $\alpha(\wp(ok : \wp(\Sigma^{+\infty}) \times br : \wp(\Sigma^+)))$ yields safety semantic (hyper) properties of [14]. This consists in replacing each semantics in the semantic property by its safety approximation by prefixes (in $\mathbb{L}^\sharp_+$) and limits (in $\mathbb{L}^\sharp_\infty$). ■

Example 14.3 (Algebraic safety hyperproperties). The trace safety hyperproperties of example 14.2 can be generalized to the algebraic semantics by requiring that, under the hypotheses of lemmas 3.8 and 3.11, algebraic safety properties $\mathcal{P}$ do satisfy that $[\![\mathsf{S}_1\,;\mathsf{S}_2]\!]^\sharp \in \mathcal{P}$ implies $[\![\mathsf{S}_1]\!]^\sharp_e \cup [\![\mathsf{S}_1]\!]^\sharp_{br} \in \mathcal{P}$ (prefix closure), that $\forall \delta \in \mathbb{O}\ .\ ([\![\mathsf{B}\,;\mathsf{S}]\!]^\sharp_e)^\delta \in \mathcal{P}$ implies $\mathsf{lfp}^{\sqsubseteq^\sharp_+}\ \overleftarrow{F}^\sharp_e \in \mathcal{P}$ (limit closure for finite executions), and that $\forall \delta \in \mathbb{O}\ .\ (([\![\mathsf{B}\,;\mathsf{S}]\!]^\sharp_e)^\delta \mathbin{⨾^\sharp} \top^\sharp_\infty) \in \mathcal{P}$ implies $\mathsf{gfp}^{\sqsubseteq^\sharp_\infty}\ F^\sharp_\bot \in \mathcal{P}$ (limit closure for infinite executions). Then $\alpha_{\mathsf{safety}}(\mathcal{P}) \triangleq \{\alpha_{\mathsf{safety}}(P) \mid P \in \mathcal{P}\}$ thus generalizing the classic definition of safety property $\alpha_{\mathsf{safety}}(P) = P$ as prefix closed and limit closed sets of traces [21, Definition 14.11]. Then the proof rule (70) can be simplified since the passage to the limit need not be checked since it is guaranteed by the safety hypothesis. ■

15 Execution Property Elimination

Given a set $\mathbb{I} \in \wp(\wp(\mathbb{L}^\sharp))$ of semantic properties of interest, the Galois retraction

$$\langle \wp(\mathbb{L}^\sharp), \subseteq\rangle \underset{\lambda\mathcal{P}\bullet\mathcal{P}\cap\mathbb{I}}{\overset{\lambda\mathcal{Q}\bullet\mathcal{Q}\cup\mathbb{I}}{\leftrightarrows}} \langle \mathbb{I}, \subseteq\rangle$$

[20, exercise 11.5] eliminates the semantics of no interest. We have used this abstraction $\lambda\mathcal{P}\bullet\mathcal{P} \cap \mathbb{I}$ implicitly in examples 6.9 and 7.5 when saying that we ignored nontermination. The logics of section 8.2 are simplified by intersection with $\mathbb{I}$ but this still requires the restricted fixpoints in the `while` rules (70) and (75) to be computed exactly, which, mechanically, does not scale up.

Example 15.1 (k-semantic properties). If $\mathbb{L} = \wp(L)$ is a powerset (which is the case for the trace semantics of section 4.3), $\mathbb{I} \triangleq \{\mathcal{P} \in \wp(\wp(L)) \mid |\mathcal{P}| \leqslant k\}$, $k \geqslant 1$, where $|S|$ is the cardinality of set S, restricts the trace properties to be considered in the semantic properties to those of cardinality at most k. An instance of this abstraction is the k-hypersafety of [14, page 1170]. ■

16 Principal Order Ideal Abstraction

16.1 Definition of the Principal Order Ideal Abstraction

Subject to the existence of the least upper bound, the principal ideal abstraction is

$$\alpha^{\curlywedge}(\mathcal{P}) \quad \triangleq \quad \{P \mid P \sqsubseteq \bigsqcup \mathcal{P}\} \tag{89}$$

Lemma 16.1. *$\alpha^{\curlywedge}$ is an upper closure operator and $\langle \alpha^{\curlywedge}(\wp(\mathbb{L})),\ \subseteq,\ \{\bot\},\ \mathbb{L},\ \boldsymbol{\lambda} X \bullet \alpha^{\curlywedge}(\cup X),\ \cap \rangle$ is a complete lattice.*

Proof of lemma 16.1. By definition, $\alpha^{\curlywedge}$ is increasing and extensive. For idempotence, we have

$$\begin{array}{lll}
 & \alpha^{\curlywedge}(\alpha^{\curlywedge}(\mathcal{P})) & \\
= & \alpha^{\curlywedge}(\{P \mid P \sqsubseteq \bigsqcup \mathcal{P}\}) & \wr\text{def. (89) of } \alpha^{\curlywedge}\int \\
= & \{P \mid P \sqsubseteq \bigsqcup \{P' \mid P' \sqsubseteq \bigsqcup \mathcal{P}\}\} & \wr\text{def. (89) of } \alpha^{\curlywedge}\int \\
= & \{P \mid P \sqsubseteq \bigsqcup \mathcal{P}\} & \wr\text{def. lub } \bigsqcup\int \\
= & \alpha^{\curlywedge}(\mathcal{P}) & \wr\text{def. (89) of } \alpha^{\curlywedge}\int
\end{array}$$

By Morgan Ward's [83, theorem 4.1], $\langle \alpha^{\curlywedge}(\wp(\mathbb{L})),\ \subseteq,\ \{\bot\},\ \mathbb{L},\ \boldsymbol{\lambda} X \bullet \alpha^{\curlywedge}(\cup X),\ \cap \rangle$ is a complete lattice. □

16.2 Proof Rule Simplification

If $\langle \mathbb{L},\ \sqsubseteq \rangle$ is a complete lattice and the composition preserves arbitrary existing limits in definition 3.2.D.d then proofs in the upper abstract semantic logic can be based on the classic upper abstract execution property logic of section 6.4 for principal ideal closed properties and their dual .

$$\frac{\overline{\{}\bigsqcup \mathcal{P}\overline{\}}\ \mathsf{S}\ \overline{\{}\bigsqcup \mathcal{Q}\overline{\}}}{\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\ \mathsf{S}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}},\quad \alpha^{\curlywedge}(\mathcal{Q}) = \mathcal{Q} \qquad\qquad \frac{\forall P \in \mathcal{P}\ .\ \underline{\{}P\underline{\}}\ \mathsf{S}\ \underline{\{}\bigsqcap \mathcal{Q}\underline{\}}}{\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\ \mathsf{S}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}},\quad \alpha^{\curlyvee}(\mathcal{Q}) = \mathcal{Q} \tag{90}$$

Soundness and completeness proof of rule (90).

$$\begin{array}{lll}
- & \overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\ \mathsf{S}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}} & \\
\Leftrightarrow & \mathsf{Post}^{\sharp}(S)\mathcal{P} \subseteq \mathcal{Q} & \wr\text{def. (60) of } \overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\ \mathsf{S}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}\int \\
\Leftrightarrow & \{\mathsf{post}^{\sharp}(S)P \mid P \in \mathcal{P}\} \subseteq \mathcal{Q} & \wr\text{def. (40) of } \mathsf{Post}^{\sharp}\int \\
\Leftrightarrow & \{\mathsf{post}^{\sharp}(S)P \mid P \in \mathcal{P}\} \subseteq \{P' \mid P' \sqsubseteq \bigsqcup \mathcal{Q}\} & \wr\text{hypothesis } \alpha^{\curlywedge}(\mathcal{Q}) = \mathcal{Q} \text{ and def. (89) of } \alpha^{\curlywedge}\int \\
\Leftrightarrow & \forall P \in \mathcal{P}\ .\ \mathsf{post}^{\sharp}(S)P \sqsubseteq \bigsqcup \mathcal{Q} & \wr\text{def. } \subseteq\int \\
\Leftrightarrow & \bigsqcup_{P \in \mathcal{P}} \mathsf{post}^{\sharp}(S)P \sqsubseteq \bigsqcup \mathcal{Q} & \wr\text{def. lub } \sqcup\int \\
\Leftrightarrow & \mathsf{post}^{\sharp}(S)\Big(\bigsqcup_{P \in \mathcal{P}} P\Big) \sqsubseteq \bigsqcup \mathcal{Q} & \\
 & \multicolumn{2}{l}{\quad\wr\text{by hypothesis, the composition preserves arbitrary existing limits in definition 3.2.D.d and (26)}\int} \\
\Leftrightarrow & \mathsf{post}^{\sharp}[\![\mathsf{S}]\!]^{\sharp}(\bigsqcup \mathcal{P}) \sqsubseteq^{\sharp} \bigsqcup \mathcal{Q} & \wr\text{def. } \bigsqcup\int \\
= & \overline{\{}\bigsqcup \mathcal{P}\overline{\}}\ \mathsf{S}\ \overline{\{}\bigsqcup \mathcal{Q}\overline{\}} & \wr\text{def. } \overline{\{}\,P\,\overline{\}}\ \mathsf{S}\ \overline{\{}\,Q\,\overline{\}} \text{ in section 6.4}\int
\end{array}$$

$$\begin{array}{lll}
- & \overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\ \mathsf{S}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}} & \\
\Leftrightarrow & \mathsf{Post}^{\sharp}(S)\mathcal{P} \subseteq \mathcal{Q} & \wr\text{def. (60) of } \overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\ \mathsf{S}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}\int
\end{array}$$

$$
\begin{aligned}
&\Leftrightarrow\ \{\mathrm{post}^{\sharp}(S)P \mid P \in \mathcal{P}\} \subseteq \mathcal{Q} && \wr\text{def. (40) of } \mathrm{Post}^{\sharp}\int\\
&\Leftrightarrow\ \{\mathrm{post}^{\sharp}(S)P \mid P \in \mathcal{P}\} \subseteq \{P' \mid \textstyle\bigsqcap \mathcal{Q} \sqsubseteq P'\} && \wr\text{hypothesis } \alpha^{\curlyvee}(\mathcal{Q}) = \mathcal{Q} \text{ and dual def. (89) of } \alpha^{\curlyvee}\int\\
&\Leftrightarrow\ \forall P \in \mathcal{P}\,.\ \mathrm{post}^{\sharp}(S)P \in \{P' \mid \textstyle\bigsqcap \mathcal{Q} \sqsubseteq P'\} && \wr\text{def. } \subseteq\int\\
&\Leftrightarrow\ \forall P \in \mathcal{P}\,.\ \textstyle\bigsqcap \mathcal{Q} \sqsubseteq \mathrm{post}^{\sharp}(S)P && \wr\text{def. } \in\int\\
&\Leftrightarrow\ \forall P \in \mathcal{P}\,.\ \underline{\{}P\underline{\}}\,\mathtt{S}\,\underline{\{}\textstyle\bigsqcap \mathcal{Q}\underline{\}} && \wr\text{def. } \underline{\{}\,P\,\underline{\}}\,\mathtt{S}\,\underline{\{}\,Q\,\underline{\}} \text{ in section 6.4}\int \qquad \square
\end{aligned}
$$

Example 16.2 (Proof reduction for principal ideal hyperproperties). Consider the instantiation for the natural relational semantics in section 5 with no break. Define the assertional execution post-condition $Q_1 \triangleq \{\sigma \in \Sigma \mid \sigma(x) \leq 10\}$ with relational equivalent $Q_2 \triangleq \Sigma \times Q_1$ and hyperproperty $\mathcal{Q} \triangleq \alpha^{\curlywedge}(Q_2) = \alpha^{\curlywedge}(\Sigma\times\{\sigma \in \Sigma \mid \sigma(x) \leq 10\})$ and similarly $\mathcal{P} \triangleq \{(\Sigma\times\{\sigma \in \Sigma \mid\ \sigma(x) = n\}) \mid n \in \mathbb{N} \wedge n > 10\}$. To prove the following hyperlogic triple $\overline{\{\!\!\{}\,\mathcal{P}\,\overline{\}\!\!\}}\,\texttt{while(x>10) x=x-1}\,\overline{\{\!\!\{}\,\mathcal{Q}\,\overline{\}\!\!\}}$, it is equivalent to prove the following.

$$
\begin{aligned}
&\overline{\{\!\!\{}\,\mathcal{P}\,\overline{\}\!\!\}}\,\texttt{while(x>10) x=x-1}\,\overline{\{\!\!\{}\,\mathcal{Q}\,\overline{\}\!\!\}}\\
\Leftrightarrow\ &\overline{\{}\,\textstyle\bigcup \mathcal{P}\,\overline{\}}\,\texttt{while(x>10) x=x-1}\,\overline{\{}\,\textstyle\bigcup \mathcal{Q}\,\overline{\}} && \wr\text{By rule of (90)}\int\\
\Leftrightarrow\ &\overline{\{}\,\Sigma \times \{\sigma \in \Sigma \mid \sigma(x) > 10\}\,\overline{\}}\,\texttt{while(x>10) x=x-1}\,\overline{\{}\,\Sigma \times \{\sigma \in \Sigma \mid \sigma(x) \leq 10\}\,\overline{\}}
\end{aligned}
$$

Then one can use the over-approximation logic with termination proof in [22]. ■

17 Order Ideal Abstraction

17.1 Definition of the Order Ideal Abstraction

The order ideal abstraction on $\langle \wp(\mathbb{L}),\ \subseteq\rangle$ is

$$
\alpha^{\sqsubseteq}(\mathcal{P}) \quad \triangleq \quad \{P' \in \mathbb{L} \mid \exists P \in \mathcal{P}\,.\ P' \sqsubseteq P\} \qquad \langle \wp(\mathbb{L}),\ \subseteq\rangle \underset{\alpha^{\sqsubseteq}}{\overset{\mathbb{1}}{\leftrightarrows}} \langle \alpha^{\sqsubseteq}(\wp(\mathbb{L})),\ \subseteq\rangle \tag{91}
$$

$\alpha^{\sqsubseteq}$ is an upper closure operator and $\langle \alpha^{\sqsubseteq}(\wp(\mathbb{L})),\ \subseteq,\ \varnothing,\ \mathbb{L},\ \boldsymbol{\lambda} X \bullet \alpha^{\sqsubseteq}(\cup X),\ \cap\rangle$ is a complete lattice [83, theorem 4.1]. The order filter abstraction $\alpha^{\sqsupseteq}$ is defined dually. Note that $\alpha^{\curlywedge}(\mathcal{P}) = \alpha^{\sqsubseteq}(\{\bigsqcup \mathcal{P}\})$. As observed by [66, page 239] for subset-closed hyperproperties, all execution properties are order-ideal closed for trace properties (where $\sqsubseteq$ is $\subseteq$), but not conversely, citing observational determinism [86] as a counterexample.

17.2 Proof Rule Simplification

The main interest of the order ideal/filter abstraction is the substantial simplification of the `while` rules (70) and (75). To show this consider properties in $\alpha^{\sqsupseteq^{\sharp}}(\wp(\mathbb{L}^{\sharp})$ where $\sqsupseteq^{\sharp}$ is defined component wise on $\mathbb{L}^{\sharp}$ in (12) with $\sqsupseteq^{\sharp}_{+}$ on the exit and break components and $\sqsubseteq^{\sharp}_{\infty}$ on the infinite component. We abstract $\mathrm{Post}^{\sharp}$ in (40) to $\mathrm{Post}^{\sqsupseteq^{\sharp}} \in \mathbb{L}^{\sharp} \rightarrow \alpha^{\sqsupseteq^{\sharp}}(\wp(\mathbb{L}^{\sharp})) \stackrel{\nearrow}{\longrightarrow} \alpha^{\sqsupseteq^{\sharp}}(\wp(\mathbb{L}^{\sharp}))$ by $(\mathcal{P} \in \alpha^{\sqsupseteq^{\sharp}}(\wp(\mathbb{L}^{\sharp})))$

$$
\begin{aligned}
\mathrm{Post}^{\sqsupseteq^{\sharp}}(S)\mathcal{P} \triangleq\ \alpha^{\sqsupseteq^{\sharp}}(\mathrm{Post}^{\sharp}(S)\mathcal{P}) \quad &= \quad \{P' \in \mathbb{L}^{\sharp} \mid \exists P \in \mathrm{Post}^{\sharp}(S)\mathcal{P}\,.\ P' \sqsupseteq^{\sharp} P\} && \wr\text{def. (91) of } \alpha^{\sqsupseteq^{\sharp}}\int\\
&= \ \{P' \in \mathbb{L}^{\sharp} \mid \exists P \in \{\mathrm{post}^{\sharp}(S)P \mid P \in \mathcal{P}\}\,.\ P \sqsubseteq^{\sharp} P'\} && \wr\text{def. (40) of Post and inversion of } \sqsupseteq^{\sharp}\int\\
&= \ \{P' \in \mathbb{L}^{\sharp} \mid \exists P \in \mathcal{P}\,.\ \mathrm{post}^{\sharp}(S)P \in \mathcal{P} \sqsubseteq^{\sharp} P'\} && \wr\text{def. } \in\int
\end{aligned}
$$

The consequence is that the `while` loop verification condition (70) simplifies to $\mathsf{lfp}^{\sqsubseteq^{\sharp}_{+}}\ \vec{F}^{\sharp}_{pe}(P') \sqsubseteq^{\sharp}_{+} P_e$ and $\mathsf{gfp}^{\sqsubseteq^{\sharp}_{\infty}}\ F^{\sharp}_{p\bot} \sqsubseteq^{\sharp}_{\infty} Q_{\bot b}$ which can respectively be handled by Park induction [21, theorem II.3.1] and greatest fixpoint over apppoximation by transfinite iterates using the dual of [21, theorem II.3.6] as is the case, for classic execution properties, in Hoare logic and termination proofs. The reasoning is dual for (75).

Example 17.1 (Proof reduction for the order ideal abstraction: bounded nondeterminism). Let us consider proofs of programs with bounded nondeterminism, assuming that the value of variables could only be integers. Consider the instantiation of relational natural semantics in section 5 with no break and no nontermination where $\mathbb{V} = \mathbb{Z}$. Let $|S|$ be the cardinality of a set S and consider the semantic (hyper) property $\mathcal{F} \triangleq \wp_{\mathsf{fin}}(\mathbb{L}) \triangleq \{P \in \wp(\mathbb{L}) \mid |P| \in \mathbb{N}\}$ to be the set of finite execution semantics i.e. programs satisfying $\mathcal{F}$ cannot have infinitely many different executions although $\mathbb{L}$ has an infinite cardinality.

Now, suppose we want prove that $\overline{\{\!|}\,\mathcal{F}\,\overline{|\!\}}\;\mathtt{S}\;\overline{\{\!|}\,\mathcal{F}\,\overline{|\!\}}$, where $\mathtt{S} \triangleq$ `x = [0, ∞]; while(x>0) x=x-1`. Since $\mathcal{F}$ is an order ideal abstraction (subset-closed), we need to find a function $\mathcal{I} \in \mathcal{F} \rightarrow \mathcal{F}$ such that for arbitrary $P \in \mathcal{P}$, we have $\mathsf{post}[\![\mathtt{S}]\!] \subseteq \mathcal{I}(P)$, and, at the same time, the image of $\mathcal{I}$ is a subset of $\mathcal{F}$. Let m and n to be any integer such that $m < 0 < n$, we can set this $\mathcal{I}$ to be

$$\mathcal{I} = \boldsymbol{\lambda} P \bullet \{\langle\sigma,\ \sigma'\rangle \in \Sigma \times \Sigma \mid m < \sigma'(x) \leq n \wedge \exists\langle\sigma_1,\ \sigma_1'\rangle \in P\ .\ (\sigma_1 = \sigma \wedge \forall v \in \mathbb{V}\ .\ v \neq x \Rightarrow \sigma_1'(x) = \sigma'(x))\}$$

We notice that this program component eventually assigns the value 0 to x while keeping the value of the other variables unchanged. As a result, for arbitrary $P \in \mathcal{P}$

$$\begin{array}{rcl}\mathsf{post}[\![\mathtt{S}]\!](P) & = & \{\langle\sigma,\ \sigma'\rangle \in \Sigma \times \Sigma \mid\ \sigma'(x) = 0 \wedge \exists\langle\sigma_1,\ \sigma_1'\rangle \in P\ .\ (\sigma_1 = \sigma \wedge \forall v \in \mathbb{V}\ .\ v \neq x \Rightarrow \\ & & \qquad \sigma_1'(x) = \sigma'(x))\} \subseteq \mathcal{I}(P)\end{array}$$

For the cardinality of $\mathcal{I}(P)$, we let the sequence $\langle X^i,\ n < i \leq m\rangle$ such that $X^i = \{\langle\sigma,\ \sigma'\rangle \in \Sigma \times \Sigma \mid \sigma'(x) = i \wedge \exists\langle\sigma_1,\ \sigma_1'\rangle \in P\ .\ (\sigma_1 = \sigma \wedge \forall v \in \mathbb{V}\ .\ v \neq x \Rightarrow \sigma_1'(x) = \sigma'(x))\}$. The cardinality of X^i in this case will be smaller than that of P, meaning $|X^i| \in \mathbb{N}$. Thus, the finite union of X^i, $\bigcup\limits_{m<i\leq n} X^i$ also has finite cardinality. ■

18 Frontiers Abstractions

Another solution to represent order ideal abstractions as proposed by [66, proposition 1] is to consider the maximal elements of the order ideal closed semantic (hyper) property only. Unfortunately, this is not the same abstraction.

Counter example 18.1. Consider the hyperproperty $\mathcal{F} \triangleq \wp_{\mathsf{fin}}(\mathbb{L}) \triangleq \{P \in \wp(\mathbb{L}) \mid |P| \in \mathbb{N}\}$ in example 17.1 i.e. programs satisfying $\mathcal{F}$ cannot have infinitely many different executions although $\mathbb{L}$ has an infinite cardinality. Then the order ideal abstraction is $\alpha^{\sqsubseteq}(\mathcal{F}) = \mathcal{F}$ which has no maximal elements so the maximal elements abstraction of this order ideal abstraction $\alpha^{\sqsubseteq}(\mathcal{F}) = \mathcal{F}$ is the empty set which is definitely different from this order ideal abstraction $\alpha^{\sqsubseteq}(\mathcal{F}) = \mathcal{F}$. ■

Let us study this abstraction in more detail.

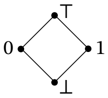
18.1 Lower Frontier Abstraction

The lower frontier abstraction abstracts a subset of a poset to its mimimal elements

$$\alpha^{\underline{F}}(\mathcal{P}) \quad \triangleq \quad \{P \in \mathcal{P} \mid \forall P' \in \mathcal{P}\ .\ P' \sqsubseteq P \Rightarrow P' = P\} \tag{92}$$

$\alpha^{\underline{F}}$ is reductive and idempotent by not necessarily increasing (and so does not necessarily preserve existing joins) hence may not be the lower adjoint of a Galois connection.

Counter example 18.2. Consider the complete lattice $\{\bot, 0, 1, \top\}$ with $\bot \sqsubseteq \bot \sqsubseteq 0 \sqsubseteq 0 \sqsubseteq \top \sqsubseteq \top$ and $\bot \sqsubseteq 1 \sqsubseteq 1 \sqsubseteq \top$. We have $\mathcal{P}_1 = \{\top\} \subseteq \{0, 1, \top\} = \mathcal{P}_2$ but $\alpha^{\underline{F}}(\mathcal{P}_1) = \{\top\} \nsubseteq \{0, 1\} = \alpha^{\underline{F}}(\mathcal{P}_2)$ proving that $\alpha^{\overline{F}}$ is not increasing hence does not preserve existing joins hence is not the lower adjoint of a Galois connection. By duality, neither is $\alpha^{\overline{F}}$. ■



18.2 Frontier Order Ideal Abstraction

The frontier order ideal abstraction

$$\alpha^{\sqsupseteq\underline{F}} \quad \triangleq \quad \alpha^{\sqsupseteq} \circ \alpha^{\underline{F}} \tag{93}$$

closes the frontier by its over approximations, as shown by the following

Lemma 18.3. $\alpha^{\sqsupseteq\underline{F}}(\mathcal{P}) = \{P \in \mathbb{L} \mid \exists F \in \alpha^{\underline{F}}(\mathcal{P}) \,.\, F \sqsubseteq P\} = \{P \in \mathbb{L} \mid \exists F \in \mathcal{P} \,.\, \forall P' \in \mathcal{P} \,.\, P' \sqsubseteq F \Rightarrow P' = F \wedge F \sqsubseteq P\}$.

Proof of lemma 18.3.

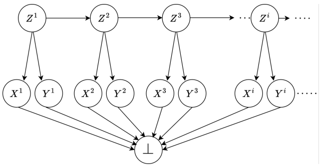
$$
\begin{array}{rll}
& \alpha^{\sqsupseteq} \circ \alpha^{\underline{F}}(\mathcal{P}) & \\
= & \{P \in \mathbb{L} \mid \exists F \in \alpha^{\underline{F}}(\mathcal{P}) \,.\, F \sqsubseteq P\} & \text{(def. function composition } \circ \text{ and (91) of the dual } \alpha^{\sqsubseteq}\text{)} \\
= & \{P \in \mathbb{L} \mid \exists F \in \{P \in \mathcal{P} \mid \forall P' \in \mathcal{P} \,.\, P' \sqsubseteq P \Rightarrow P' = P\} \,.\, F \sqsubseteq P\} & \text{(def. (92) of } \alpha^{\underline{F}}\text{)} \\
= & \{P \in \mathbb{L} \mid \exists F \in \mathcal{P} \,.\, \forall P' \in \mathcal{P} \,.\, P' \sqsubseteq F \Rightarrow P' = F \wedge F \sqsubseteq P\} & \text{(def. } \in\text{)} \quad \square
\end{array}
$$

Observe that $\alpha^{\sqsupseteq\underline{F}}$ is idempotent but not necessarily increasing or extensive.

Counter example 18.4. Consider $\mathbb{L} = \{\langle a,\, n\rangle \mid n \in \mathbb{N}\} \cup \{\langle b,\, m\rangle \mid m \in \mathbb{N}\}$ with $\langle x,\, n\rangle \sqsubseteq \langle y,\, m\rangle \triangleq x = y \wedge n \geqslant m$ be two incomparable infinite decreasing chains. $\mathbb{L} \nsubseteq \alpha^{\sqsupseteq\underline{F}}(\mathbb{L}) = \varnothing$. Take $\mathcal{P} = \{\langle a,\, n\rangle \mid n \in \mathbb{N}\} \cup \{\langle b,\, 0\rangle\}$ so that $\mathcal{P} \subseteq \mathbb{L}$ but $\alpha^{\sqsupseteq\underline{F}}(\mathcal{P}) = \{\langle b,\, m\rangle \mid m \in \mathbb{N}\} \nsubseteq \alpha^{\sqsupseteq\underline{F}}(\mathbb{L}) = \varnothing$. ■

$\alpha^{\sqsupseteq\underline{F}}(\wp(\mathbb{L}))$ is not closed by intersection.

Counter example 18.5. Consider the lattice on the right. Let $\mathcal{P}_1 = \{Z^i \mid i \in \mathbb{N}_*\} \cup \{X^i \mid i \in \mathbb{N}_*\}$ with frontier $\mathcal{F}_1 = \{X^i \mid i \in \mathbb{N}_*\}$ and $\mathcal{P}_2 = \{Z^i \mid i \in \mathbb{N}_*\} \cup \{Y^i \mid i \in \mathbb{N}_*\}$ with frontier $\mathcal{F}_2 = \{Y^i \mid i \in \mathbb{N}_*\}$. There is no largest set smaller than $\mathcal{P}_1$ and $\mathcal{P}_2$ with an existing frontier. ■



Lemma 18.6. *$\langle \alpha^{\sqsupseteq\underline{F}}(\wp(\mathbb{L})),\, \subseteq,\, \varnothing,\, \mathbb{L},\, \cup\rangle$ is a join semilattice.*

Proof of lemma 18.6. Given $\mathcal{P}_1, \mathcal{P}_2 \in \alpha^{\sqsupseteq\underline{F}}(\wp(\mathbb{L}))$, we have to prove that $\mathcal{P}_1 \cup \mathcal{P}_2 \in \alpha^{\sqsupseteq\underline{F}}(\wp(\mathbb{L}))$ that is the existence of a frontier $\mathcal{F} \in \alpha^{\underline{F}}(\wp(\mathbb{L}))$ such that $\mathcal{P}_1 \cup \mathcal{P}_2 = \alpha^{\sqsupseteq}(\mathcal{F})$. Let $\mathcal{F}_1$, $\mathcal{F}_2$ be the frontiers such that $\mathcal{P}_1 = \alpha^{\sqsupseteq}(\mathcal{F}_1)$ and $\mathcal{P}_2 = \alpha^{\sqsupseteq}(\mathcal{F}_2)$. Define the frontier

$$\mathcal{F} \quad \triangleq \quad \alpha^{\underline{F}}(\mathcal{F}_1 \cup \mathcal{F}_2) \quad = \quad \{P \in \mathcal{F}_1 \cup \mathcal{F}_2 \mid \forall P' \in \mathcal{F}_1 \cup \mathcal{F}_2 \,.\, P' \sqsubseteq P \Rightarrow P' = P\} \tag{94}$$

— To prove $\mathcal{P}_1 \cup \mathcal{P}_2 \subseteq \alpha^{\sqsupseteq}(\mathcal{F})$, given any $X \in \mathcal{P}_1 \cup \mathcal{P}_2$, let us show the existence of $F \in \mathcal{F}$ such that $X \in \alpha^{\sqsupseteq}(P)$ that is $F \sqsubseteq X$. There are two cases.

(1) If $X \in \mathcal{P}_1$ and $X \notin \mathcal{P}_2$ then $\exists F_1 \in \mathcal{F}_1 \,.\, F_1 \sqsubseteq X$ and $\forall F_2 \in \mathcal{F}_2 \,.\, F_2 \nsqsubseteq X$ so taking $P = F_1$ in (94), we have $P = F_1 \in \mathcal{F}_1 \cup \mathcal{F}_2$ and $\forall P' \in \mathcal{F}_1 \cup \mathcal{F}_2$, if $P' \sqsubseteq P = F_1$ then $P' \sqsubseteq X$ by transitivity so $P' \notin \mathcal{F}_2$ proving $P' \in \mathcal{F}_1$ and so $P' = F_1 = P$ by $F_1 \in \alpha^{\underline{F}}(\mathcal{F}_1)$;
(2) The case $X \notin \mathcal{P}_1$ and $X \in \mathcal{P}_2$ is symmetric;
(3) Otherwise $X \in \mathcal{P}_1 \cap \mathcal{P}_2$. In that case $\exists F_1 \in \mathcal{F}_1 \,.\, F_1 \sqsubseteq X$. Let $\mathcal{M} = \mathcal{F}_2 \cap \alpha^{\sqsupseteq}(X)$. There are two subcases.
   (a) $\forall F_2 \in \mathcal{M} \,.\, F_2 \not\sqsubset F_1$. This is similar to case 1;
   (b) $\exists F_2 \in \mathcal{M} \,.\, F_2 \sqsubset F_1$. No element F_1' of $\mathcal{F}_1 \setminus \{F_1\}$ is comparable to F_2 since otherwise $F_1' \sqsubseteq F_2 \sqsubset F_1$ would contradict that F_1 is in the frontier of $\mathcal{P}_1$. Therefore, taking $P = F_2$, we have $P = F_2 \in \mathcal{F}_1 \cup \mathcal{F}_2$ and if $P' \in \mathcal{F}_1 \cup \mathcal{F}_2$ then $P' \in \mathcal{F}_2$ is impossible so $P' \in \mathcal{F}_1$ so $P' = F_1 = P$ by $F_1 \in \alpha^{\underline{F}}(\mathcal{F}_1)$;

— Conversely, to prove $\mathcal{P}_1 \cup \mathcal{P}_2 \supseteq \alpha^{\sqsupseteq}(\mathcal{F})$, assume $X \in \alpha^{\sqsupseteq}(\mathcal{F})$ so that there exists $F \in \alpha^{\underline{F}}(\mathcal{F}_1 \cup \mathcal{F}_2)$ such that $F \sqsubseteq X$. By (94), either $F \in \mathcal{F}_1$ and $X \in \mathcal{P}_1$ or $F \in \mathcal{F}_2$ and $X \in \mathcal{P}_2$ proving $X \in \mathcal{P}_1 \cup \mathcal{P}_2$. □

18.3 A Frontier Characterization of the Order Ideal Abstraction

Lemma 18.7. *There is a Galois isomorphism $\langle \alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L})), \subseteq\rangle \mathrel{\substack{\xleftarrow{\;\alpha^{\sqsubseteq}\;} \\ \xrightarrow[\;\alpha^{\overline{F}}\;]{}}} \langle \alpha^{\overline{F}}(\wp(\mathbb{L})), \preceq^{\overline{F}}\rangle$ and $\langle \alpha^{\overline{F}}(\wp(\mathbb{L})), \preceq^{\overline{F}},\, \curlyvee^{\overline{F}}\rangle$ is a join semi lattice with $P \preceq^{\overline{F}} Q \triangleq (\alpha^{\sqsubseteq}(P) \subseteq \alpha^{\sqsubseteq}(Q))$ and $P \curlyvee^{\overline{F}} Q \triangleq \alpha^{\overline{F}}(\alpha^{\sqsubseteq}(P) \cup \alpha^{\sqsubseteq}(Q))$.*

Proof of lemma 18.7. — We first show that $\alpha^{\overline{F}} \circ \alpha^{\sqsubseteq} \circ \alpha^{\overline{F}} = \alpha^{\overline{F}}$. Consider $\mathcal{P} \in \alpha^{\overline{F}}(\wp(\mathbb{L}))$. Then

$$\begin{aligned}
& \alpha^{\overline{F}} \circ \alpha^{\sqsubseteq}(\mathcal{P}) \\
= {} & \{P \in \alpha^{\sqsubseteq}(\mathcal{P}) \mid \forall P' \in \alpha^{\sqsubseteq}(\mathcal{P}) \mathrel{.} P \sqsubseteq P' \Rightarrow P = P'\} && \wr\text{By def. (92) of } \alpha^{\overline{F}}\int \\
= {} & \{P \in \{P' \in \mathbb{L} \mid \exists F \in \mathcal{P} \mathrel{.} P' \sqsubseteq F\} \mid \forall P' \in \{P' \in \mathbb{L} \mid \exists F' \in \mathcal{P} \mathrel{.} P' \sqsubseteq F'\} \mathrel{.} P \sqsubseteq P' \Rightarrow P = P'\} \\
& && \wr\text{by def. (91) of } \alpha^{\sqsubseteq}\int \\
= {} & \{P \mid \exists F \in \mathcal{P} \mathrel{.} P \sqsubseteq F \wedge \forall P' \in \{P' \in \mathbb{L} \mid \exists F' \in \mathcal{P} \mathrel{.} P' \sqsubseteq F'\} \mathrel{.} P \sqsubseteq P' \Rightarrow P = P'\} && \wr\text{def. } \in\int \\
= {} & \{P \mid \exists F \in \mathcal{P} \mathrel{.} P \sqsubseteq F \wedge \forall P' \in \mathbb{L} \mathrel{.} (\exists F' \in \mathcal{P} \mathrel{.} P' \sqsubseteq F') \Rightarrow (P \sqsubseteq P' \Rightarrow P = P')\} && \wr\text{def. } \in\int \\
= {} & \{P \in \mathbb{L} \mid \exists F \in \mathcal{P} \mathrel{.} P \sqsubseteq F \wedge \forall P' \in \mathbb{L} \mathrel{.} (\exists F' \in \mathcal{P} \mathrel{.} P \sqsubseteq P' \sqsubseteq F') \Rightarrow P = P'\} && \wr\text{def. } \Rightarrow \text{ and transitivity}\int \\
= {} & \{P \in \mathbb{L} \mid P \in \mathcal{P}\}
\end{aligned}$$

$\wr$($\subseteq$) Let $P' = F$, so that $\exists F' \in \mathcal{P} \mathrel{.} P \sqsubseteq P' \sqsubseteq F'$ holds by choosing $F' = F$ which implies $P = P' = F \in \mathcal{P}$ so $P \in \mathcal{P}$;

($\supseteq$) Let $P \in \mathcal{P}$ and choose $F = P$ so that $P \sqsubseteq F$. Consider any $P' \in \mathbb{L}$. Then, by choosing $F' = P'$, $(\exists F' \in \mathcal{P} \mathrel{.} P \sqsubseteq P' \sqsubseteq F')$ if and only if $P \sqsubseteq P'$. But $P = F \in \mathcal{P}$ and $\mathcal{P} \in \alpha^{\overline{F}}(\wp(\mathbb{L}))$ is a frontier so $P = P'$$\int$

$$\begin{aligned}
= {} & \mathcal{P} && \wr\text{def. set in extension}\int
\end{aligned}$$

— If $\mathcal{P} \in \alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L}))$ then there exists $\mathcal{P}' \in \wp(\mathbb{L}))$ such that $\mathcal{P} = \alpha^{\sqsubseteq\overline{F}}(\mathcal{P}')$ and then

$$\begin{aligned}
& \alpha^{\sqsubseteq} \circ \alpha^{\overline{F}}(\mathcal{P}) \\
= {} & \alpha^{\sqsubseteq} \circ \alpha^{\overline{F}} \circ \alpha^{\sqsubseteq\overline{F}}(\mathcal{P}') && \wr\mathcal{P} = \alpha^{\sqsubseteq\overline{F}}(\mathcal{P}')\int \\
= {} & \alpha^{\sqsubseteq} \circ \alpha^{\overline{F}} \circ \alpha^{\sqsubseteq} \circ \alpha^{\overline{F}}(\mathcal{P}') && \wr\text{dual def. (93) of } \alpha^{\sqsubseteq\overline{F}}\int \\
= {} & \alpha^{\sqsubseteq} \circ \alpha^{\overline{F}}(\mathcal{P}') && \wr\text{since } \alpha^{\overline{F}} \circ \alpha^{\sqsubseteq} \circ \alpha^{\overline{F}} = \alpha^{\overline{F}}\int \\
= {} & \alpha^{\sqsubseteq\overline{F}}(\mathcal{P}') && \wr\text{dual def. (93) of } \alpha^{\sqsubseteq\overline{F}}\int \\
= {} & \mathcal{P} && \wr\text{by definition } \mathcal{P} = \alpha^{\sqsubseteq\overline{F}}(\mathcal{P}')\int
\end{aligned}$$

— If $\mathcal{Q} \in \alpha^{\overline{F}}(\wp(\mathbb{L}))$ then there exists $\mathcal{Q}' \in \wp(\mathbb{L}))$ such that $\mathcal{Q} = \alpha^{\overline{F}}(\mathcal{Q}')$ and then

$$\begin{aligned}
& \alpha^{\overline{F}} \circ \alpha^{\sqsubseteq}(\mathcal{Q}) \\
= {} & \alpha^{\overline{F}} \circ \alpha^{\sqsubseteq} \circ \alpha^{\overline{F}}(\mathcal{Q}') && \wr\mathcal{Q} = \alpha^{\overline{F}}(\mathcal{Q}')\int \\
= {} & \alpha^{\overline{F}}(\mathcal{Q}') && \wr\text{since } \alpha^{\overline{F}} \circ \alpha^{\sqsubseteq} \circ \alpha^{\overline{F}} = \alpha^{\overline{F}}\int \\
= {} & \mathcal{Q} && \wr\mathcal{Q} = \alpha^{\overline{F}}(\mathcal{Q}')\int
\end{aligned}$$

— It follows that there is a bijection $\alpha^{\overline{F}}$ with inverse $\alpha^{\sqsubseteq}$ between $\alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L}))$ and $\alpha^{\overline{F}}(\wp(\mathbb{L}))$.

— Defining $P \preceq^{\overline{F}} Q \triangleq (\alpha^{\sqsubseteq}(P) \subseteq \alpha^{\sqsubseteq}(Q))$ this yields the Galois retraction $\langle \alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L})),\ \subseteq\rangle \mathrel{\underset{\alpha^{\overline{F}}}{\overset{\alpha^{\sqsubseteq}}{\leftrightarrows}}} \langle \alpha^{\overline{F}}(\wp(\mathbb{L})),\ \preceq^{\overline{F}}\rangle$. By the dual of lemma 18.6, $\langle \alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L})),\ \subseteq,\ \varnothing,\ \mathbb{L},\ \cup\rangle$ is a join semilattice. Therefore the finite joins are preserved by the Galois connection so that $\langle \alpha^{\overline{F}}(\wp(\mathbb{L})),\ \preceq^{\overline{F}},\ \curlyvee^{\overline{F}}\rangle$ is a join semilattice with $P \preceq^{\overline{F}} Q \triangleq \alpha^{\sqsubseteq}(P) \subseteq \alpha^{\sqsubseteq}(Q)$ and $P \curlyvee^{\overline{F}} Q \triangleq \alpha^{\overline{F}}(\alpha^{\sqsubseteq}(P) \cup \alpha^{\sqsubseteq}(Q))$. □

Define the principal ideal ${\downarrow}^{\sqsubseteq}(P) \triangleq \{P' \in \mathbb{L} \mid P' \sqsubseteq P\}$. The following lemma 18.8 is a characterization of $\alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L}))$ that corrects and generalizes [66, Proposition 1].

Lemma 18.8. *If* $\mathcal{P} \in \alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L}))$ *then* $\mathcal{P} = \bigcup\limits_{P \in \alpha^{\overline{F}}(\mathcal{P})} {\downarrow}^{\sqsubseteq}(P)$.

Proof of lemma 18.8.

$$
\begin{array}{ll}
\quad\mathcal{P} & \\
= \alpha^{\sqsubseteq\overline{F}}(\mathcal{P}) & \lbag \mathcal{P} \in \alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L})) \text{ and lemma 18.7} \rbag \\
= \alpha^{\sqsubseteq}(\alpha^{\underline{F}}(\mathcal{P})) & \lbag \text{dual def. (93) of } \alpha^{\sqsubseteq\underline{F}} \text{ and composition } \circ \rbag \\
= \{P' \in \mathbb{L} \mid \exists P \in \alpha^{\underline{F}}(\mathcal{P}) \mathrel{.} P' \sqsubseteq P\} & \lbag \text{def. (91) of } \alpha^{\sqsubseteq} \rbag \\
= \displaystyle\bigcup_{P \in \alpha^{\underline{F}}(\mathcal{P})} \{P' \in \mathbb{L} \mid P' \sqsubseteq P\} & \lbag \text{def. } \cup \rbag \\
= \displaystyle\bigcup_{P \in \alpha^{\underline{F}}(\mathcal{P})} {\downarrow}^{\sqsubseteq}(P) & \lbag \text{def. } {\downarrow}^{\sqsubseteq}(P) \triangleq \{P' \in \mathbb{L} \mid P' \sqsubseteq P\} \rbag \qquad \square
\end{array}
$$

19 Chain Limit Abstraction

19.1 Chain Limit Abstraction Definition and Properties

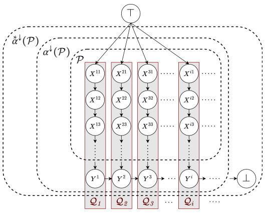
Another possible representation of order ideal abstractions would be by limits of chains. Define

$$\alpha^{\downarrow}(\mathcal{P}) \quad \triangleq \quad \{\bigsqcap_{i\in\mathbb{N}} P_i \mid \langle P_i,\ i \in \mathbb{N}\rangle \in \mathcal{P} \text{ is a decreasing chain with existing glb}\} \tag{95}$$

$\alpha^{\downarrow}$ is $\subseteq$ increasing and extensive but not necessarily idempotent as shown by counter example 19.1 below. The iteration of $\alpha^{\downarrow}$ (possibly transfinitely)

$$\overset{*}{\alpha}{}^{\downarrow}(\mathcal{P}) \quad \triangleq \quad \mathsf{lfp}^{\subseteq}\, \boldsymbol{\lambda} X \mathbin{\bullet} \mathcal{P} \cup \alpha^{\downarrow}(X) \tag{96}$$

yields an upper closure operator [20, lemma 29.1].



Counter example 19.1. Consider the complete lattice $\mathbb{L}$ on the right. Let $\mathcal{P} = \{X^{ij} \mid i, j > 0\}$. We have $\alpha^{\downarrow}(\mathcal{P}) = \{X^{ij} \mid i, j > 0\} \cup \{Y^i \mid i > 0\}$. We have $\bigsqcap\{Y^i \mid i > 0\} = \bot$ so $\alpha^{\downarrow}(\alpha^{\downarrow}(\mathcal{P})) = \{X^{ij} \mid i, j > 0\} \cup \{Y^i \mid i > 0\} \cup \{\bot\} \neq \alpha^{\downarrow}(\mathcal{P})$.
Moreover $\overset{*}{\alpha}{}^{\downarrow}(\mathcal{Q}_i) \in \overset{*}{\alpha}{}^{\downarrow}(\wp(\mathbb{L}))$, $i > 0$ but $\bigcup_{i>0} \overset{*}{\alpha}{}^{\downarrow}(\mathcal{Q}_i) \notin \overset{*}{\alpha}{}^{\downarrow}(\wp(\mathbb{L}))$. ■

Lemma 19.2. $\langle \wp(\mathbb{L}),\ \subseteq\rangle \xrightleftharpoons[\overset{*}{\alpha}{}^{\downarrow}]{\mathbb{1}} \langle \overset{*}{\alpha}{}^{\downarrow}(\wp(\mathbb{L})),\ \subseteq\rangle$ *and* $\langle \overset{*}{\alpha}{}^{\downarrow}(\wp(\mathbb{L})),\ \subseteq,\ \emptyset,\ \mathbb{L},\ \boldsymbol{\lambda} X \mathbin{\bullet} \overset{*}{\alpha}{}^{\downarrow}(\bigcup X),\ \bigcap\rangle$ *is a complete lattice.*

Proof of lemma 19.2. By [20, lemma 29.1], $\overset{*}{\alpha}{}^{\downarrow}$ is the smallest upper closure operator pointwise greater than or equal to $\alpha^{\downarrow}$. By Morgan Ward's [83, theorem 4.1], $\langle \overset{*}{\alpha}{}^{\downarrow}(\wp(\mathbb{L})),\ \subseteq\rangle$ is a complete lattice with infimum $\overset{*}{\alpha}{}^{\downarrow}(\{\bot\}) = \{\bot\}$ and join $\boldsymbol{\lambda} X \mathbin{\bullet} \overset{*}{\alpha}{}^{\downarrow}(\bigcup X)$. □

Lemma 19.3. *$\forall \mathcal{P} \in \wp(\mathbb{L}) \mathrel{.} \alpha^{\downarrow}(\overset{*}{\alpha}{}^{\downarrow}(\mathcal{P})) = \overset{*}{\alpha}{}^{\downarrow}(\mathcal{P})$.*

Proof of lemma 19.3. By the fixpoint definition (96) of $\overset{*}{\alpha}{}^{\downarrow}$, we have $\overset{*}{\alpha}{}^{\downarrow}(\mathcal{P}) = \mathsf{lfp}^{\subseteq}\, \boldsymbol{\lambda} X \mathbin{\bullet} \mathcal{P} \cup \alpha^{\downarrow}(X)$ so $\overset{*}{\alpha}{}^{\downarrow}(\mathcal{P}) = \mathcal{P} \cup \alpha^{\downarrow}(\overset{*}{\alpha}{}^{\downarrow}(\mathcal{P}))$. Since $\alpha^{\downarrow}$ and $\overset{*}{\alpha}{}^{\downarrow}$ are extensive, we have $\mathcal{P} \subseteq \overset{*}{\alpha}{}^{\downarrow}(\mathcal{P}) \subseteq \alpha^{\downarrow}(\overset{*}{\alpha}{}^{\downarrow}(\mathcal{P}))$ so $\mathcal{P} \cup \alpha^{\downarrow}(\overset{*}{\alpha}{}^{\downarrow}(\mathcal{P})) = \alpha^{\downarrow}(\overset{*}{\alpha}{}^{\downarrow}(\mathcal{P}))$ proving $\overset{*}{\alpha}{}^{\downarrow}(\mathcal{P}) = \alpha^{\downarrow}(\overset{*}{\alpha}{}^{\downarrow}(\mathcal{P}))$ by transitivity. □

Lemma 19.4. *For all $\mathcal{P} \in \wp(\mathbb{L})$, $\alpha^{\downarrow}(\mathcal{P}) = \mathcal{P}$ implies $\overset{*}{\alpha}{}^{\downarrow}(\mathcal{P}) = \mathcal{P}$.*

Proof of lemma 19.4. Consider the iterates of $\mathsf{lfp}^{\subseteq}\, \boldsymbol{\lambda} X \mathbin{\bullet} \mathcal{P} \cup \alpha^{\downarrow}(X)$ from $X^0 = \emptyset$. $X^1 = \mathcal{P} \cup \alpha^{\downarrow}(X^0) = \mathcal{P} \cup \alpha^{\downarrow}(\emptyset) = \mathcal{P}$ since $\alpha^{\downarrow}(\emptyset) = \emptyset$ by definition (95). We have $X^2 = \mathcal{P} \cup \alpha^{\downarrow}(X^1) = \mathcal{P} \cup \alpha^{\downarrow}(\mathcal{P}) = \mathcal{P} \cup \mathcal{P} = \mathcal{P} = X^1$ by hypothesis $\alpha^{\downarrow}(\mathcal{P}) = \mathcal{P}$. By (96), we conclude that $\overset{*}{\alpha}{}^{\downarrow}(\mathcal{P}) = \mathsf{lfp}^{\subseteq}\, \boldsymbol{\lambda} X \mathbin{\bullet} \mathcal{P} \cup \alpha^{\downarrow}(X) = \mathcal{P}$. □

$\alpha^{\uparrow}$ is defined $\sqsubseteq$ dually, and $\overset{*}{\alpha}{}^{\uparrow}(\mathcal{P}) \triangleq \mathsf{lfp}^{\subseteq}\, \boldsymbol{\lambda} X \mathbin{\bullet} \mathcal{P} \cup \alpha^{\uparrow}(X)$ is an upper closure operator.

19.2 Forall Exists Hyperproperties

Assuming that $\langle \mathbb{L},\ \sqsubseteq\rangle = \langle \wp(\Pi),\ \subseteq\rangle$ (where e.g. $\Pi = \Sigma^{+\infty}$ is a set of traces) $\forall\exists$ hyperproperties have the form

$$\mathcal{AEH} \quad \triangleq \quad \{\{P \in \wp(\Pi) \mid \forall \pi_1 \in P\ .\ \exists \pi_2 \in P\ .\ \langle \pi_1,\ \pi_2\rangle \in A\} \mid A \in \wp(\Pi \times \Pi)\} \tag{97}$$

(this easily generalizes to $\forall \pi_1, \ldots, \pi_n \in P\ .\ \exists \pi_1', \ldots, \pi_m' \in P\ .\ \langle \pi_1,\ \ldots,\ \pi_n,\ \pi_1',\ \ldots,\ \pi_m'\rangle \in A$ [40]).

Example 19.5 (Generalized non-interference). A typical forall exists hyperproperty is generalized non interference [35, 69, 70] for the trace semantics of appendix 4. Let $\mathtt{L} \in \mathbb{X}$ be a low variable and $\mathtt{H} \in \mathbb{X}$ be a high variable, we have

$$\begin{aligned} GNI \quad \triangleq \quad \{P \in \wp(\Sigma^+) \mid \forall \sigma_1\pi_1\sigma_1', \sigma_2\pi_2\sigma_2' \in P\ .\ \exists \sigma_3\pi_3\sigma_3' \in P\ .\ (\sigma_1(\mathtt{L}) = \sigma_2(\mathtt{L})) \Rightarrow \\ (\sigma_3(\mathtt{L}) = \sigma_1(\mathtt{L}) \wedge \sigma_3(\mathtt{H}) = \sigma_2(\mathtt{H}) \wedge \sigma_3'(\mathtt{L}) = \sigma_1'(\mathtt{L}))\} \end{aligned} \tag{98}$$

■

Assuming chain-complete lattices in 3.2.A and 3.2.C, chain limit closed semantic properties in $\overset{*}{\alpha}{}^{\uparrow}(\wp(\wp(\Pi)))$ subsume $\forall\exists$ hyperproperties in $\mathcal{AEH}$ in that

$$\mathcal{AEH} \quad \subseteq \quad \overset{*}{\alpha}{}^{\uparrow}(\wp(\wp(\Pi))) \tag{99}$$

Proof of (99). We must prove that $\forall \mathcal{P} \in \mathcal{AEH}\ .\ \overset{*}{\alpha}{}^{\uparrow}(\mathcal{P}) \in \mathcal{AEH}$. By the dual of lemma 19.4, it is sufficient to assume that $\mathcal{P} \in \mathcal{AEH}$ and prove that $\alpha^{\uparrow}(\mathcal{P}) \in \mathcal{AEH}$.

$\alpha^{\uparrow}(\mathcal{P})$

$= \{\bigcup_{i\in\mathbb{N}} P_i \mid \langle P_i,\ i \in \mathbb{N}\rangle \in \mathcal{P}$ is an increasing chain with existing lub$\}$ $\quad \lbag$dual def. (95) of $\alpha^{\uparrow}\rbag$

$= \{\bigcup_{i\in\mathbb{N}} P_i \mid \langle P_i,\ i \in \mathbb{N}\rangle \in \mathcal{P}$ is an increasing chain$\}$ $\quad \lbag$chain completeness hypothesis$\rbag$

$= \{\bigcup_{i\in\mathbb{N}} P_i \mid \langle P_i,\ i \in \mathbb{N}\rangle \in \mathcal{P}$ is an increasing chain $\wedge\ \forall i \in \mathbb{N}\ .\ \forall \pi_1 \in P_i\ .\ \exists \pi_2 \in P_i\ .\ \langle \pi_1,\ \pi_2\rangle \in A\}$

$\lbag\mathcal{P} \in \mathcal{AEH}$ and def. $\mathcal{AEH}\rbag$

$= \{P \in \mathcal{P} \mid \forall \pi_1 \in P\ .\ \exists \pi_2 \in P\ .\ \langle \pi_1,\ \pi_2\rangle \in A\}$

$\lbag(\subseteq)$ if $\pi_1 \in \bigcup_{i\in\mathbb{N}} P_i$ then there exists $i \in \mathbb{N}$ such that $\pi_1 \in P_i$ so that, by hypothesis, $\exists \pi_2 \in P_i\ .\ \langle \pi_1,\ \pi_2\rangle \in A$, proving $\exists \pi_2 \in \bigcup_{i\in\mathbb{N}} P_i\ .\ \langle \pi_1,\ \pi_2\rangle \in A$;
$(\supseteq)$ conversely, consider the chain $\langle P,\ i \in \mathbb{N}\rangle$ so that $\bigcup_{i\in\mathbb{N}} P = P$.$\rbag$

$= \mathcal{P}$ $\quad \lbag$since $\mathcal{P} \in \mathcal{AEH}$ so that by (97) the condition holds for all elements of $\mathcal{P}\rbag$ □

20 Chain Limit Order Ideal Abstraction

20.1 Chain Limit Order Ideal Abstraction Definition and Properties

Define

$$\alpha^{\sqsubseteq\uparrow} \quad \triangleq \quad \alpha^{\sqsubseteq} \circ \alpha^{\uparrow} \qquad\qquad \text{and} \qquad\qquad \overset{*}{\alpha}{}^{\sqsubseteq\uparrow}(\mathcal{P}) \quad \triangleq \quad \mathsf{lfp}^{\subseteq}\, \boldsymbol{\lambda} X \bullet \mathcal{P} \cup \alpha^{\sqsubseteq\uparrow}(X) \tag{100}$$

to get an upper closure operator (since $\alpha^{\sqsubseteq\uparrow}$ is increasing and expansive although not idempotent).

Counter example 20.1. Define $\langle \mathbb{L},\ \sqsubseteq\rangle = \langle \wp(\mathbb{N}),\ \subseteq\rangle$ and $\mathcal{N} \triangleq \{\mathbb{N} \setminus \{n\} \mid n \in \mathbb{N}\} \in \wp(\mathbb{N})$ to be the set of all sets $\mathbb{N}$ with one missing element. Since any two different elements of $\mathcal{N}$ are $\subseteq$- incomparable, $\mathcal{N}$ is both a lower and upper frontier so chains are reduced to one element. Therefore $\overset{*}{\alpha}{}^{\downarrow}(\mathcal{N}) = \overset{*}{\alpha}{}^{\uparrow}(\mathcal{N}) = \mathcal{N}$. By (100), it follows that $\alpha^{\sqsubseteq\uparrow}(\mathcal{N}) = \alpha^{\sqsubseteq}(\mathcal{N}) = \wp(\mathbb{N}) \setminus \{\mathbb{N}\}$. Consider the increasing chain $\mathcal{C} = \langle \{i \mid i < j\},\ j \in \mathbb{N}\rangle$ of elements of $\overset{*}{\alpha}{}^{\uparrow}(\mathcal{N})$. Its limit is $\bigcup_{j\in\mathbb{N}} \{i \mid i < j\} = \mathbb{N} \notin \alpha^{\sqsubseteq\uparrow}(\mathcal{N}) = \wp(\mathbb{N}) \setminus \{\mathbb{N}\}$ proving that $\alpha^{\sqsubseteq\uparrow}$ is not idempotent. ■

Lemma 20.2. $\langle \wp(\mathbb{L}),\ \subseteq\rangle \xrightleftharpoons[\overset{*}{\alpha}{}^{\sqsubseteq\uparrow}]{\mathbb{1}} \langle \overset{*}{\alpha}{}^{\sqsubseteq\uparrow}(\wp(\mathbb{L})),\ \subseteq\rangle$ *and* $\langle \overset{*}{\alpha}{}^{\sqsubseteq\uparrow}(\wp(\mathbb{L})),\ \subseteq,\ \varnothing,\ \mathbb{L},\ \boldsymbol{\lambda} X \bullet \overset{*}{\alpha}{}^{\sqsubseteq\uparrow}(\bigcup X),\ \bigcap\rangle$ *is a complete lattice.*

Proof of lemma 20.2. By [20, lemma 29.1], $\overset{*}{\alpha}{}^{\sqsubseteq\uparrow}$ is the smallest upper closure operator pointwise greater than or equal to $\alpha^{\sqsubseteq\uparrow}$. By Morgan Ward's [83, theorem 4.1], $\langle \overset{*}{\alpha}{}^{\sqsubseteq\uparrow}(\wp(\mathbb{L})),\ \subseteq\rangle$ is a complete lattice with infimum $\overset{*}{\alpha}{}^{\uparrow}(\{\bot\}) = \{\bot\}$ and join $\boldsymbol{\lambda} X \bullet \overset{*}{\alpha}{}^{\sqsubseteq\uparrow}(\bigcup X)$. □

20.2 Forall Hyperproperties

$\forall$ hyperproperties are usually defined in the context of trace semantics of section 4, for which, in absence of $\mathtt{break}$s, $\langle \mathbb{L}, \sqsubseteq \rangle = \langle \wp(\Sigma^{+\infty}), \subseteq \rangle)$ as in section 4.3. In this case, by definition of $\subseteq$, we get

$$\mathcal{AAH} \quad \triangleq \quad \{\{P \in \wp(\Sigma^{+\infty}) \mid \forall \pi_1, \pi_2 \in P \,.\, \langle \pi_1,\ \pi_2 \rangle \in A\} \mid A \in \wp(\Sigma^{+\infty} \times \Sigma^{+\infty})\} \tag{101}$$

Example 20.3 (Non-interference). A typical forall hyperproperty is non interference $\mathit{NI} \in \mathcal{AAH}$ for the trace semantics of section 4 [16, 47, 48]. Let $\mathtt{L} \in \mathbb{X}$ be a low variable, we have

$$\mathit{NI} \quad \triangleq \quad \{P \in \wp(\Sigma^{+}) \mid \forall \sigma_1\pi_1\sigma_1', \sigma_2\pi_2\sigma_2' \in P \,.\, (\sigma_1(\mathtt{L}) = \sigma_2(\mathtt{L})) \Rightarrow (\sigma_1'(\mathtt{L}) = \sigma_2'(\mathtt{L}))\} \tag{102}$$

We have $\mathit{NI} \in \mathcal{AAH}$ by defining $A \triangleq \{\langle \sigma_1\pi_1\sigma_1',\ \sigma_2\pi_2\sigma_2' \rangle \mid (\sigma_1(\mathtt{L}) = \sigma_2(\mathtt{L})) \Rightarrow (\sigma_1'(\mathtt{L}) = \sigma_2'(\mathtt{L}))\}$. ■

21 Logic Rule for Chain Limit Order Ideal Abstract Semantic Properties

[30, sect. 5.3] have introduced a sound but incomplete logic for proving $\forall^*\exists^*$ hyperproperties. We generalize the rule in our algebraic lattice-theoretic framework for the chain limit abstract semantic properties in $\mathring{\alpha}^{\uparrow}(\wp(\mathbb{L}))$.

21.1 A Sound and Incomplete Rule

[30] does not consider $\mathtt{break}$s and nontermination so that the fields $\bot$ and b of $\langle e : F,\ \bot : I,\ b : B \rangle$ in (12) can be ignored and the tuple reduces to the value F of the field e. In this section, 3.2.A is a lattice which is increasing chain complete, 3.2.C and 3.2.D.c are omitted, and limits of increasing chains are assumed to be preserved in 3.2.D.d. We also assume that $\llbracket \neg\mathtt{B} \rrbracket_e^\sharp \fatsemi^\sharp \llbracket \neg\mathtt{B} \rrbracket_e^\sharp = \llbracket \neg\mathtt{B} \rrbracket_e^\sharp$, $\llbracket \neg\mathtt{B} \rrbracket_e^\sharp \fatsemi^\sharp \llbracket \mathtt{B} \rrbracket_e^\sharp = \llbracket \mathtt{B} \rrbracket_e^\sharp \fatsemi^\sharp \llbracket \neg\mathtt{B} \rrbracket_e^\sharp = \bot_+^\sharp$, and $\llbracket \mathtt{skip} \rrbracket_e^\sharp \triangleq \mathsf{skip}^\sharp = \mathsf{init}^\sharp$ in (3), which does not hold for traces but holds e.g. for a relational semantics.

The rule of [30] generalizes to

$$\frac{\mathcal{P} \subseteq \mathcal{I}, \quad \overline{\{\!|}\,\mathcal{I}\,\overline{|\!\}}\,\mathtt{if\ (B)\ else\ skip}\,\overline{\{\!|}\,\mathcal{I}\,\overline{|\!\}}, \quad \overline{\{\!|}\,\mathcal{I}\,\overline{|\!\}}\,\neg\mathtt{B}\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}}{\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathtt{while\ (B)\ S}\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}}, \quad \mathcal{Q} \in \mathring{\alpha}^{\uparrow}(\wp(\mathbb{L}^\sharp)) \tag{103}$$

The key idea to prove that for any $P \in \mathcal{P} \in \wp(\mathbb{L}_+^\sharp)$, the exact postcondition $Q = \mathsf{post}^\sharp\llbracket \mathtt{while\ (B)\ S} \rrbracket_e^\sharp P$ will be in $\mathcal{Q}$ is to exhibit an increasing chain in $\mathcal{Q}$ with least upper bound Q, also in $\mathcal{Q}$ by the hypothesis that $\mathcal{Q}$ is a chain limit order ideal abstract semantic property.

21.2 A Soundness Proof of (103)

Let $P \in \wp(\mathbb{L}_+^\sharp)$. The iterates $\langle X^i,\ i \in \mathbb{N} \cup \{\omega\} \rangle$ of $\boldsymbol{\lambda} X \bullet P \sqcup_+^\sharp \mathsf{post}^\sharp\llbracket \mathtt{if(B)\ S\ else\ skip} \rrbracket_e^\sharp(X)$ from $\bot_+^\sharp$ are defined as

$$\begin{array}{rcl} X^0 & \triangleq & P \\ X^{n+1} & \triangleq & \mathsf{post}^\sharp\llbracket \mathtt{if\ (B)\ S\ else\ skip} \rrbracket_e^\sharp X^n \\ X^\omega & \triangleq & \displaystyle\bigsqcup_{n\in\mathbb{N}}{}_+^\sharp\, X^n \end{array} \tag{104}$$

Since the iterates are a function of P, we write $X^i(P)$, $i \in \mathbb{N} \cup \{\omega\}$ when this dependency must be made clear.

Lemma 21.1.

$$\begin{array}{rcl} \forall n \in \mathbb{N} \,.\, X^n & = & \Big(\displaystyle\bigsqcup_{i=0}^{n-1}{}_+^\sharp\, \mathsf{post}^\sharp\llbracket \neg\mathtt{B} \rrbracket_e^\sharp((\mathsf{post}^\sharp\llbracket \mathtt{B;S} \rrbracket_e^\sharp)^i P) \sqcup_+^\sharp \big((\mathsf{post}^\sharp\llbracket \mathtt{B;S} \rrbracket_e^\sharp)^n P\big) \\ X^\omega & = & \displaystyle\bigsqcup_{n\in\mathbb{N}}{}_+^\sharp\, \mathsf{post}^\sharp\llbracket \neg\mathtt{B} \rrbracket_e^\sharp((\mathsf{post}^\sharp\llbracket \mathtt{B;S} \rrbracket_e^\sharp)^n P) \sqcup_+^\sharp \bigsqcup_{n\in\mathbb{N}}{}_+^\sharp(\mathsf{post}^\sharp\llbracket \mathtt{B;S} \rrbracket_e^\sharp)^n P \end{array} \tag{105}$$

Proof of lemma 21.1. The proof is by recurrence on n.

— For the basis, this is $\bot^\sharp_+ \sqcup^\sharp_+ \big(P \fatsemi^\sharp \mathsf{skip}\big) = P \fatsemi^\sharp \mathsf{init} = P = X^0$ by hypothesis $\llbracket\texttt{skip}\rrbracket^\sharp_e = \mathsf{init}^\sharp$, 3.2.A, and 3.2.D.a.

— For the induction step, we observe that $\langle X^i,\ i \leqslant n\rangle$ is a $\sqsubseteq^\sharp_+$-increasing chain, by definition of the lub $\sqcup^\sharp_+$. Then

$$
\begin{aligned}
& X^{n+1} \\
={}& \mathsf{post}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e X^n && \wr\text{def. } X^{n+1}\int \\
={}& \mathsf{post}^\sharp\llbracket\texttt{B;S}\rrbracket^\sharp_e X^n \sqcup^\sharp_+ \mathsf{post}^\sharp\llbracket\neg\texttt{B;skip}\rrbracket^\sharp_e X^n && \wr(34)\int \\
={}& \Big(X^n \fatsemi^\sharp \llbracket\texttt{B;S}\rrbracket^\sharp_e\Big) \sqcup^\sharp_+ \Big(X^n \fatsemi^\sharp \llbracket\neg\texttt{B}\rrbracket^\sharp_e\Big) && \wr\text{by def. (25) of post, } \llbracket\texttt{skip}\rrbracket^\sharp_e = \mathsf{init}^\sharp\text{, and 3.2.D.a}\int \\
={}& \Big(\big(\bigsqcup^{\sharp}_{+\,i=0}^{n-1} P \fatsemi^\sharp (\llbracket\texttt{B;S}\rrbracket^\sharp_e)^i \fatsemi^\sharp \llbracket\neg\texttt{B}\rrbracket^\sharp_e\big) \sqcup^\sharp_+ \big(P \fatsemi^\sharp (\llbracket\texttt{B;S}\rrbracket^\sharp_e)^n\big) \fatsemi^\sharp \llbracket\texttt{B;S}\rrbracket^\sharp_e\Big) \sqcup^\sharp_+ \Big(\big(\bigsqcup^{\sharp}_{+\,i=0}^{n-1} P \fatsemi^\sharp (\llbracket\texttt{B;S}\rrbracket^\sharp_e)^i \fatsemi^\sharp \llbracket\neg\texttt{B}\rrbracket^\sharp_e\big) \sqcup^\sharp_+ \\
& \big(P \fatsemi^\sharp (\llbracket\texttt{B;S}\rrbracket^\sharp_e)^n\big) \fatsemi^\sharp \llbracket\neg\texttt{B}\rrbracket^\sharp_e\Big) && \wr\text{induction hypothesis}\int \\
={}& \Big(\big(\bigsqcup^{\sharp}_{+\,i=0}^{n-1} P \fatsemi^\sharp (\llbracket\texttt{B;S}\rrbracket^\sharp_e)^i \fatsemi^\sharp \llbracket\neg\texttt{B}\rrbracket^\sharp_e\big) \sqcup^\sharp_+ \big(P \fatsemi^\sharp (\llbracket\texttt{B;S}\rrbracket^\sharp_e)^{n+1}\big)\Big) \sqcup^\sharp_+ \big(\bigsqcup^{\sharp}_{+\,i=0}^{n} P \fatsemi^\sharp (\llbracket\texttt{B;S}\rrbracket^\sharp_e)^i \fatsemi^\sharp \llbracket\neg\texttt{B}\rrbracket^\sharp_e\big) \\
& \qquad \wr\text{integrating the term } P \fatsemi^\sharp (\llbracket\texttt{B;S}\rrbracket^\sharp_e)^n\big) \fatsemi^\sharp \llbracket\neg\texttt{B}\rrbracket^\sharp_e \text{ in the join and } \llbracket\texttt{B;S}\rrbracket^\sharp_e \text{ in } P \fatsemi^\sharp (\llbracket\texttt{B;S}\rrbracket^\sharp_e)^n\big)\int \\
={}& \big(\bigsqcup^{\sharp}_{+\,i=0}^{n} P \fatsemi^\sharp (\llbracket\texttt{B;S}\rrbracket^\sharp_e)^i \fatsemi^\sharp \llbracket\neg\texttt{B}\rrbracket^\sharp_e\big) \sqcup^\sharp_+ \big(P \fatsemi^\sharp (\llbracket\texttt{B;S}\rrbracket^\sharp_e)^{n+1}\big) && \wr\text{idempotence of } \sqcup^\sharp_+\int \\
={}& \big(\bigsqcup^{\sharp}_{+\,i=0}^{n} \mathsf{post}^\sharp\llbracket\neg\texttt{B}\rrbracket^\sharp_e(\mathsf{post}^\sharp\llbracket\texttt{B;S}\rrbracket^\sharp_e)^i P) \sqcup^\sharp_+ \big((\mathsf{post}^\sharp\llbracket\texttt{B;S}\rrbracket^\sharp_e)^{n+1} P\big) && \wr\text{def. (25) of post}\int
\end{aligned}
$$

— For the limit, we have

$$
\begin{aligned}
& X^\omega \\
={}& \bigsqcup^{\sharp}_{+\,n\in\mathbb{N}}\Big(\big(\bigsqcup^{\sharp}_{+\,i=0}^{n-1} \mathsf{post}^\sharp\llbracket\neg\texttt{B}\rrbracket^\sharp_e(\mathsf{post}^\sharp\llbracket\texttt{B;S}\rrbracket^\sharp_e)^i P\big) \sqcup^\sharp_+ \big((\mathsf{post}^\sharp\llbracket\texttt{B;S}\rrbracket^\sharp_e)^n P\big)\Big) && \wr(104)\text{ and }(105)\int \\
={}& \bigsqcup^{\sharp}_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp\llbracket\neg\texttt{B}\rrbracket^\sharp_e((\mathsf{post}^\sharp\llbracket\texttt{B;S}\rrbracket^\sharp_e)^n P) \sqcup^\sharp_+ \bigsqcup^{\sharp}_{+\,n\in\mathbb{N}} (\mathsf{post}^\sharp\llbracket\texttt{B;S}\rrbracket^\sharp_e)^n P && \wr\sqcup^\sharp_+\text{ associative}\int \qquad \square
\end{aligned}
$$

Lemma 21.2. *For all $P \in \wp(\mathbb{L}^\sharp_+)$,*

$$
\mathsf{lfp}^{\sqsubseteq}\, \boldsymbol{\lambda} X \bullet P \sqcup^\sharp_+ \mathsf{post}^\sharp\llbracket\texttt{if(B) S else skip}\rrbracket^\sharp_e(X) \quad = \quad X^\omega \tag{106}
$$

Proof of lemma 21.2. The iterates $\langle X^i,\ i \in \mathbb{N} \cup \{\omega\}\rangle$ are characterized in lemma 21.1. Let use prove that $X^\omega = P \sqcup^\sharp_+ \mathsf{post}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e X^\omega$ is a fixpoint.

$$
\begin{aligned}
& P \sqcup^\sharp_+ \mathsf{post}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e X^\omega \\
={}& P \sqcup^\sharp_+ \mathsf{post}^\sharp\llbracket\texttt{B;S}\rrbracket^\sharp_e X^\omega \sqcup^\sharp_+ \mathsf{post}^\sharp\llbracket\neg\texttt{B;skip}\rrbracket^\sharp_e X^\omega && \wr(34)\int \\
={}& P \sqcup^\sharp_+ \Big(X^\omega \fatsemi^\sharp \llbracket\texttt{B;S}\rrbracket^\sharp_e\Big) \sqcup^\sharp_+ \Big(X^\omega \fatsemi^\sharp \llbracket\neg\texttt{B}\rrbracket^\sharp_e\Big) && \wr\text{by def. (25) of post, } \llbracket\texttt{skip}\rrbracket^\sharp_e = \mathsf{init}^\sharp\text{, and 3.2.D.a}\int \\
={}& P \sqcup^\sharp_+ \Big(\Big(\bigsqcup^{\sharp}_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp\llbracket\neg\texttt{B}\rrbracket^\sharp_e((\mathsf{post}^\sharp\llbracket\texttt{B;S}\rrbracket^\sharp_e)^n P) \sqcup^\sharp_+ \bigsqcup^{\sharp}_{+\,n\in\mathbb{N}} (\mathsf{post}^\sharp\llbracket\texttt{B;S}\rrbracket^\sharp_e)^n P\Big) \fatsemi^\sharp \llbracket\texttt{B;S}\rrbracket^\sharp_e\Big) \\
& \sqcup^\sharp_+ \\
& \Big(\Big(\bigsqcup^{\sharp}_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp\llbracket\neg\texttt{B}\rrbracket^\sharp_e((\mathsf{post}^\sharp\llbracket\texttt{B;S}\rrbracket^\sharp_e)^n P) \sqcup^\sharp_+ \bigsqcup^{\sharp}_{+\,n\in\mathbb{N}} (\mathsf{post}^\sharp\llbracket\texttt{B;S}\rrbracket^\sharp_e)^n P\Big) \fatsemi^\sharp \llbracket\neg\texttt{B}\rrbracket^\sharp_e\Big) \\
& && \wr\text{characterization (105) of } X^\omega\int
\end{aligned}
$$

$$= P \sqcup^\sharp_+ \Big(\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e\Big(\bigsqcup^\sharp_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp\llbracket \neg\mathtt{B}\rrbracket^\sharp_e((\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^n P) \sqcup^\sharp_+ \bigsqcup^\sharp_{+\,n\in\mathbb{N}} (\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^n P\Big)\Big)$$

$$\sqcup^\sharp_+$$

$$\Big(\mathsf{post}^\sharp\llbracket \neg\mathtt{B}\rrbracket^\sharp_e\Big(\bigsqcup^\sharp_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp\llbracket \neg\mathtt{B}\rrbracket^\sharp_e((\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^n P) \sqcup^\sharp_+ \bigsqcup^\sharp_{+\,n\in\mathbb{N}} (\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^n P\Big)\Big) \qquad \wr\text{def. (25) of post}\int$$

$$= P \sqcup^\sharp_+ \Big(\bigsqcup^\sharp_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e(\mathsf{post}^\sharp\llbracket \neg\mathtt{B}\rrbracket^\sharp_e((\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^n P)) \sqcup^\sharp_+ \bigsqcup^\sharp_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e(\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^n)P\Big)$$

$$\sqcup^\sharp_+$$

$$\Big(= \bigsqcup^\sharp_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp\llbracket \neg\mathtt{B}\rrbracket^\sharp_e(\mathsf{post}^\sharp\llbracket \neg\mathtt{B}\rrbracket^\sharp_e((\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^n P)) \sqcup^\sharp_+ \bigsqcup^\sharp_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp\llbracket \neg\mathtt{B}\rrbracket^\sharp_e((\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^n P)\Big)$$

$$\wr\mathsf{post}^\sharp(S)\text{ preserve joins of increasing chains by (3.2.D.d)}\int$$

$$= \Big(P \sqcup^\sharp_+ \bigsqcup^\sharp_{+\,n\in\mathbb{N}} (\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^{n+1} P\Big) \sqcup^\sharp_+ \Big(\bigsqcup^\sharp_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp\llbracket \neg\mathtt{B}\rrbracket^\sharp_e((\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^n P)\Big)$$

$$\wr\text{def. (25) of post and hypotheses } \llbracket \neg\mathtt{B}\rrbracket^\sharp_e \fatsemi^\sharp \llbracket \neg\mathtt{B}\rrbracket^\sharp_e = \llbracket \neg\mathtt{B}\rrbracket^\sharp_e \text{ and } \llbracket \neg\mathtt{B}\rrbracket^\sharp_e \fatsemi^\sharp \llbracket \mathtt{B}\rrbracket^\sharp_e = \llbracket \mathtt{B}\rrbracket^\sharp_e \fatsemi^\sharp \llbracket \neg\mathtt{B}\rrbracket^\sharp_e\ \int$$

$$= X^\omega \qquad \wr\text{integrating } P \text{ in the join with } \mathsf{post}^\sharp(S)^0 = \mathbb{1} \text{ and commutativity}\int$$

It follows that the sequence $\langle X^i,\ i \in \mathbb{N} \cup \{\omega\}\rangle$ is increasing and stationary at ω which is therefore the least fixpoint (106). □

Lemma 21.3.

$$\mathsf{post}^\sharp\llbracket \mathtt{while\ (B)\ S}\rrbracket^\sharp_e P \quad = \quad \mathsf{post}^\sharp\llbracket \neg\mathtt{B}\rrbracket^\sharp_e X^\omega \quad = \quad \bigsqcup^\sharp_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp\llbracket \neg\mathtt{B}\rrbracket^\sharp_e((\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^n P) \qquad (107)$$

Proof of lemma 21.3.

$$\mathsf{post}^\sharp\llbracket \mathtt{while\ (B)\ S}\rrbracket^\sharp_e P$$

$$= \langle ok\ :\ \langle e\ :\ \mathsf{post}^\sharp(\llbracket \neg\mathtt{B}\rrbracket^\sharp_e \sqcup^\sharp_e \llbracket \mathtt{B;S}\rrbracket^\sharp_b)(\mathsf{lfp}^{\sqsubseteq^\sharp_+}(\vec{F}^\sharp_{pe}(P))), \bot\ :\ \mathsf{post}^\sharp(\llbracket \mathtt{B;S}\rrbracket^\sharp_\bot)(\mathsf{lfp}^{\sqsubseteq^\sharp_+}(\vec{F}^\sharp_{pe}(P))) \sqcup^\sharp_\infty$$

$$\mathsf{post}^\sharp(\mathsf{gfp}^{\sqsubseteq^\sharp_\infty} F^\sharp_{p\bot})P\rangle, br : P_{br}\rangle_e \qquad \wr\text{by (37)}\int$$

$$= \mathsf{post}^\sharp(\llbracket \neg\mathtt{B}\rrbracket^\sharp_e)(\mathsf{lfp}^{\sqsubseteq^\sharp_+}(\boldsymbol{\lambda} X \bullet \mathsf{post}^\sharp(\mathsf{init}^\sharp)P \sqcup^\sharp_+ \mathsf{post}^\sharp(\llbracket \mathtt{B;S}\rrbracket^\sharp_e)(X)))$$

$$\wr\text{in absence of } \mathtt{breaks} \text{ and ignoring non termination}\int$$

$$= \mathsf{post}^\sharp(\llbracket \neg\mathtt{B}\rrbracket^\sharp_e)(\mathsf{lfp}^{\sqsubseteq^\sharp_+}(\boldsymbol{\lambda} X \bullet \mathsf{post}^\sharp(\mathsf{init}^\sharp)P \sqcup^\sharp_+ \mathsf{post}^\sharp(\llbracket \mathtt{B;S}\rrbracket^\sharp_e)(X))) \qquad \wr\text{def. (35) of } \vec{F}^\sharp_{pe}\int$$

$$= \mathsf{post}^\sharp(\llbracket \neg\mathtt{B}\rrbracket^\sharp_e)(\mathsf{lfp}^{\sqsubseteq^\sharp_+}(\boldsymbol{\lambda} X \bullet P \sqcup^\sharp_+ \mathsf{post}^\sharp(\llbracket \mathtt{B;S}\rrbracket^\sharp_e)(X))) \qquad \wr\text{def. (25) of } \mathsf{post}^\sharp \text{ and 3.2.D.a}\int$$

$$= \mathsf{post}^\sharp(\llbracket \neg\mathtt{B}\rrbracket^\sharp_e)(X^\omega) \qquad \wr\text{lemma 21.2}\int$$

$$= \mathsf{post}^\sharp(\llbracket \neg\mathtt{B}\rrbracket^\sharp_e)(\bigsqcup^\sharp_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp\llbracket \neg\mathtt{B}\rrbracket^\sharp_e((\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^n P) \sqcup^\sharp_+ \bigsqcup^\sharp_{+\,n\in\mathbb{N}} (\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^n P) \qquad \wr\text{lemma 21.2}\int$$

$$= \bigsqcup^\sharp_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp\llbracket \neg\mathtt{B}\rrbracket^\sharp_e(\mathsf{post}^\sharp\llbracket \neg\mathtt{B}\rrbracket^\sharp_e((\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^n P)) \sqcup^\sharp_+ \bigsqcup^\sharp_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp\llbracket \neg\mathtt{B}\rrbracket^\sharp_e(\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^n P)$$

$$\wr\mathsf{post}^\sharp(S)\text{ preserves joins } \sqcup^\sharp_+ \text{ by def. (25) of post and 3.2.D.d}\int$$

$$= \bigsqcup^\sharp_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp\llbracket \neg\mathtt{B}\rrbracket^\sharp_e((\mathsf{post}^\sharp\llbracket \mathtt{B;S}\rrbracket^\sharp_e)^n P)$$

≀(33), def. (25) of $\mathsf{post}^\sharp$, hypotheses $\llbracket \mathtt{B}\rrbracket^\sharp_e \fatsemi^\sharp \llbracket \neg\mathtt{B}\rrbracket^\sharp_e = \bot^\sharp_+$ and $\llbracket \neg\mathtt{B}\rrbracket^\sharp_e \fatsemi^\sharp \llbracket \neg\mathtt{B}\rrbracket^\sharp_e = \llbracket \neg\mathtt{B}\rrbracket^\sharp_e$, def. function powers, and def. lub∫ □

Theorem 21.4. *Proof rule* (103) *is sound.*

Proof of theorem 21.4. Observe that if $P \in \mathcal{P}$ then $X^0 = P \in \mathcal{I}$ by $\mathcal{P} \subseteq \mathcal{I}$ by the premise of the rule (103). Assume $X^n \in \mathcal{I}$ then, by (62), $\overline{\{\!|}\,\mathcal{I}\,\overline{|\!\}}$ `if (B) else skip` $\overline{\{\!|}\,\mathcal{I}\,\overline{|\!\}}$ if and only if $\forall P \in \mathcal{I}$. $\mathsf{post}^\sharp\llbracket \mathtt{if\ (B)\ else\ skip}\rrbracket^\sharp P \in \mathcal{I}$ if and only if $\forall P \in \mathcal{I}$. $\mathsf{post}^\sharp\llbracket \mathtt{if\ (B)\ else\ skip}\rrbracket^\sharp_e P \in \mathcal{I}$ since nontermination and `breaks` are ignored. By (104), this implies that $X^{n+1} \in \mathcal{I}$. By recurrence $\forall n \in \mathbb{N}$. $X^n \in \mathcal{I}$.

By (25) and 3.2.D.d, $\mathsf{post}^\sharp[\![\neg\mathtt{B}]\!]^\sharp_e$ is increasing so that the sequence $\langle \mathsf{post}^\sharp[\![\neg\mathtt{B}]\!]^\sharp_e X^n,\ n \in \mathbb{N} \cup \{\omega\}\rangle$ is increasing.

By (62), $\overline{\{\!|}\,\mathcal{I}\,\overline{|\!\}}\ \neg\mathtt{B}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}} \Leftrightarrow \forall P \in \mathcal{I}\,.\ \mathsf{post}^\sharp[\![\neg\mathtt{B}]\!]^\sharp P \in \mathcal{Q} \Leftrightarrow \forall P \in \mathcal{I}\,.\ \mathsf{post}^\sharp[\![\neg\mathtt{B}]\!]^\sharp_e P \in \mathcal{Q}$ since nontermination and `break`s are ignored. Since $\forall n \in \mathbb{N}\ .\ X^n \in \mathcal{I}$, this implies that $\forall n \in \mathbb{N}\ .\ \mathsf{post}^\sharp[\![\neg\mathtt{B}]\!]^\sharp_e X^n \in \mathcal{Q}$. By hypothesis, $\mathcal{Q} \in \mathring{\alpha}^{\sqsubseteq\uparrow}(\wp(\mathbb{L}^\sharp_+))$ so that by the dual of (95), $\mathsf{post}^\sharp[\![\neg\mathtt{B}]\!]^\sharp_e X^\omega \in \mathcal{Q}$. It follows by (107) that $\mathsf{post}^\sharp[\![\mathtt{while\ \ (B)\ \ S}]\!]^\sharp_e P \in \mathcal{Q}$.

We conclude that $\forall P \in \mathcal{P}\ .\ \mathsf{post}^\sharp[\![\mathtt{while\ \ (B)\ \ S}]\!]^\sharp_e P = \mathsf{post}^\sharp[\![\neg\mathtt{B}]\!]^\sharp_e X^\omega \in \mathcal{Q}$ which, by (62), implies that $\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\ \mathtt{while\ \ (B)\ \ S}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}$, proving soundness of the rule (103). □

Lemma 21.5. *Proof rule* (103) *is incomplete.*

Proof of lemma (21.5). Consider $\overline{\{\!|}\,\{P\}\,\overline{|\!\}}\ \mathtt{while\ \ (B)\ \ S}\ \overline{\{\!|}\,\{\mathsf{post}^\sharp[\![\mathtt{while\ \ (B)\ \ S}]\!]^\sharp_e P\}\,\overline{|\!\}}$ which holds by (62). Since $\mathring{\alpha}^{\sqsubseteq\uparrow}(\{\mathsf{post}^\sharp[\![\mathtt{while\ \ (B)\ \ S}]\!]^\sharp_e P\}) = \{\mathsf{post}^\sharp[\![\mathtt{while\ \ (B)\ \ S}]\!]^\sharp_e P\}$, we can apply proof rule (103). By $\mathcal{P} \subseteq \mathcal{I}$, we should have $P \in \mathcal{I}$ so $X^0(P) \in \mathcal{I}$. The second condition $\overline{\{\!|}\,\mathcal{I}\,\overline{|\!\}}\ \mathtt{if\ \ (B)\ \ else\ \ skip}\ \overline{\{\!|}\,\mathcal{I}\,\overline{|\!\}}$ of the premise implies, by (62), that $\forall P \in \mathcal{I}\ .\ \mathsf{post}^\sharp[\![\mathtt{if\ \ (B)\ \ S\ \ else\ \ skip}]\!]^\sharp_e P$. Therefore by (104) and recurrence, $\forall n \in \mathbb{N}\ .\ X^n(P) \in \mathcal{I}$. Then the third condition of the premiss, requires that $\overline{\{\!|}\,\mathcal{I}\,\overline{|\!\}}\ \neg\mathtt{B}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}$, equivalently, by (62), $\forall P \in \mathcal{I}\,.\ \mathsf{post}^\sharp[\![\neg\mathtt{B}]\!]^\sharp P \in \{\mathsf{post}^\sharp[\![\mathtt{while\ \ (B)\ \ S}]\!]^\sharp_e P\}$ and therefore $\forall P \in \mathcal{I}\,.\ \mathsf{post}^\sharp[\![\neg\mathtt{B}]\!]^\sharp P = \mathsf{post}^\sharp[\![\mathtt{while\ \ (B)\ \ S}]\!]^\sharp_e P$. In particular, we must have $\forall n \in \mathbb{N}\ .\ \mathsf{post}^\sharp[\![\neg\mathtt{B}]\!]^\sharp X^n(P) = \mathsf{post}^\sharp[\![\mathtt{while\ \ (B)\ \ S}]\!]^\sharp_e P$. By the characterization (107) of $\mathsf{post}^\sharp[\![\mathtt{while\ \ (B)\ \ S}]\!]^\sharp_e P$, this means that $\forall n \in \mathbb{N}\ .\ \mathsf{post}^\sharp[\![\neg\mathtt{B}]\!]^\sharp X^n(P) = \bigsqcup^\sharp_{+\,n\in\mathbb{N}} \mathsf{post}^\sharp[\![\neg\mathtt{B}]\!]^\sharp_e((\mathsf{post}^\sharp[\![\mathtt{B;S}]\!]^\sharp_e)^n P)$. Otherwise stated the loop is never entered, which, apart from the cas where `B` is false, is not the case in general. □

21.3 Completeness Relative to an Abstract Hypercollecting Semantics

Lemma 21.5 shows that proof rule (103) is incomplete relative to the hypercollecting semantics (56) of section 7. We show that the rule is complete relative to the following abstraction of the hypercollecting semantics (56).

Definition 21.6 (Weak structural hypercollecting semantics for iteration).

$$\overline{\mathsf{Post}}^\sharp[\![\mathtt{while(B)\ \ S}]\!]^\sharp_e\mathcal{P} \triangleq \mathsf{Post}^\sharp[\![\neg B]\!]^\sharp_e(\mathsf{lfp}^{\subseteq}\,\boldsymbol{\lambda}\mathcal{X}\bullet\mathcal{P}\cup\overline{\mathsf{Post}}^\sharp[\![\mathtt{if(B)\ \ S\ \ else\ \ skip}]\!]^\sharp_e(\mathcal{X})) \tag{108}$$

$\overline{\mathsf{Post}}^\sharp[\![\mathtt{while(B)\ \ S}]\!]^\sharp_e$ is an algebraic form of the hypercollecting semantics postulated by [5, p. 877].

Theorem 21.7 (Characterization of the executions satisfying (108)).

$$\mathsf{lfp}^{\subseteq}\,\boldsymbol{\lambda}\mathcal{X}\bullet\mathcal{P}\cup\overline{\mathsf{Post}}^\sharp[\![\mathtt{if(B)\ \ S\ \ else\ \ skip}]\!]^\sharp_e(\mathcal{X}) \quad=\quad \{X^n(P)\mid P\in\mathcal{P}\wedge n\in\mathbb{N}\} \tag{109}$$

Proof of theorem 21.7. the iterates of $\boldsymbol{\lambda}\mathcal{X}\bullet\mathcal{P}\cup\overline{\mathsf{Post}}^\sharp[\![\mathtt{if(B)\ \ S\ \ else\ \ skip}]\!]^\sharp_e(\mathcal{X})$ are

$$\begin{aligned}
\mathcal{X}^0 &= \varnothing\\
\mathcal{X}^1 &= \mathcal{P}\\
\mathcal{X}^2 &= \mathcal{P}\cup\overline{\mathsf{Post}}^\sharp[\![\mathtt{if\ \ (B)\ \ S\ \ else\ \ skip}]\!]^\sharp_e(\mathcal{P})\\
&\ldots\\
\mathcal{X}^n &= \bigcup_{i=0}^{n}(\overline{\mathsf{Post}}^\sharp[\![\mathtt{if\ \ (B)\ \ S\ \ else\ \ skip}]\!]^\sharp_e)^i(\mathcal{P}) && \text{(induction hypothesis)}\\
\mathcal{X}^{n+1} &= \mathcal{P}\cup\overline{\mathsf{Post}}^\sharp[\![\mathtt{if(B)\ \ S\ \ else\ \ skip}]\!]^\sharp_e(\mathcal{X}^n)\\
&= \mathcal{P}\cup\overline{\mathsf{Post}}^\sharp[\![\mathtt{if(B)\ \ S\ \ else\ \ skip}]\!]^\sharp_e(\bigcup_{i=0}^{n}(\overline{\mathsf{Post}}^\sharp[\![\mathtt{if\ \ (B)\ \ S\ \ else\ \ skip}]\!]^\sharp_e)^i(\mathcal{P}))\\
&= \mathcal{P}\cup\bigcup_{i=1}^{n+1}(\overline{\mathsf{Post}}^\sharp[\![\mathtt{if\ \ (B)\ \ S\ \ else\ \ skip}]\!]^\sharp_e)^i(\mathcal{P})
\end{aligned}$$

$$= \bigcup_{i=0}^{n+1}(\overline{\mathsf{Post}}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e)^i(\mathcal{P})$$

A similar calculation shows that $\mathcal{X}^\omega = \bigcup\limits_{n\in\mathbb{N}}(\overline{\mathsf{Post}}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e)^n(\mathcal{P})$ is stable so is the least fixpoint $\mathsf{lfp}^{\subseteq}\boldsymbol{\lambda}\mathcal{X}\bullet\mathcal{P}\cup\overline{\mathsf{Post}}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e(\mathcal{X}) = \mathcal{X}^\omega$.

Observe that we have

— $(\overline{\mathsf{Post}}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e)^0(\mathcal{P})$

$$\begin{aligned}
&= \mathcal{P} && \wr\text{def. function powers}\int\\
&= \{X^0(P) \mid P\in\mathcal{P}\} && \wr\text{def. function powers}\int
\end{aligned}$$

— for induction

$$\begin{aligned}
&(\overline{\mathsf{Post}}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e)^{n+1}(\mathcal{P})\\
&= \overline{\mathsf{Post}}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e((\overline{\mathsf{Post}}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e)^n(\mathcal{P})) && \wr\text{def. powers}\int\\
&= \overline{\mathsf{Post}}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e(\{X^n(P) \mid P\in\mathcal{P}\}) && \wr\text{induction hypothesis}\int\\
&= \mathsf{Post}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e(\{X^n(P) \mid P\in\mathcal{P}\}) && \wr\text{def. }\overline{\mathsf{Post}}^\sharp\text{ for conditional}\int\\
&= \{\mathsf{post}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e X^n(P) \mid P\in\mathcal{P}\} && \wr\text{def. (40) of }\mathsf{Post}^\sharp\int\\
&= \{X^{n+1}(P) \mid P\in\mathcal{P}\} && \wr\text{def. (104) of the iterates}\int
\end{aligned}$$

We conclude, by recurrence, that $\forall n\in\mathbb{N}\mathrel{.}(\overline{\mathsf{Post}}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e)^n(\mathcal{P}) = \{X^n(P) \mid P\in\mathcal{P}\}$. It follows that

$$\begin{aligned}
&\mathsf{lfp}^{\subseteq}\boldsymbol{\lambda}\mathcal{X}\bullet\mathcal{P}\cup\overline{\mathsf{Post}}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e(\mathcal{X})\\
&= \mathcal{X}^\omega\\
&= \bigcup_{n\in\mathbb{N}}(\overline{\mathsf{Post}}^\sharp\llbracket\texttt{if (B) S else skip}\rrbracket^\sharp_e)^n(\mathcal{P})\\
&= \bigcup_{n\in\mathbb{N}}\{X^n(P) \mid P\in\mathcal{P}\}\\
&= \{X^n(P) \mid P\in\mathcal{P}\wedge n\in\mathbb{N}\} && \square
\end{aligned}$$

The following lemma 21.8 shows the correspondance between $\overline{\mathsf{Post}}^\sharp\llbracket\texttt{while(B) S}\rrbracket^\sharp_e$ and the hypercollecting semantics (56). It shows that $\overline{\mathsf{Post}}^\sharp\llbracket\texttt{while(B) S}\rrbracket^\sharp_e$ misses limits.

Lemma 21.8. $\forall\mathcal{P}\in\wp(\mathbb{L}^\sharp)\mathrel{.}\mathsf{Post}^\sharp\llbracket\texttt{while(B) S}\rrbracket^\sharp_e\mathcal{P}\subseteq\alpha^\uparrow(\overline{\mathsf{Post}}^\sharp\llbracket\texttt{while(B) S}\rrbracket^\sharp_e\mathcal{P})$.

Proof of lemma 21.8.

$$\begin{aligned}
&\mathsf{Post}^\sharp\llbracket\texttt{while(B) S}\rrbracket^\sharp_e\mathcal{P}\\
&= \{\mathsf{post}^\sharp\llbracket\texttt{while (B) S}\rrbracket^\sharp_e P \mid P\in\mathcal{P}\} && \wr(40)\int\\
&= \{\mathsf{post}^\sharp\llbracket\neg\texttt{B}\rrbracket^\sharp_e X^\omega(P) \mid P\in\mathcal{P}\} && \wr(107)\int\\
&= \{\mathsf{post}^\sharp\llbracket\neg\texttt{B}\rrbracket^\sharp_e(\bigsqcup^\sharp_{+\,n\in\mathbb{N}} X^n(P)) \mid P\in\mathcal{P}\} && \wr\text{def. (104) of }X^\omega\int\\
&= \{\bigsqcup^\sharp_{+\,n\in\mathbb{N}}\mathsf{post}^\sharp\llbracket\neg\texttt{B}\rrbracket^\sharp_e X^n(P) \mid P\in\mathcal{P}\} && \wr\text{join preservation 3.2.D.d}\int\\
&= \{\bigsqcup^\sharp_+\{\mathsf{post}^\sharp\llbracket\neg\texttt{B}\rrbracket^\sharp_e X^n(P) \mid n\in\mathbb{N}\} \mid P\in\mathcal{P}\} && \wr\text{def. of }\sqcup^\sharp_+\int\\
&\subseteq \alpha^\uparrow(\{\mathsf{post}^\sharp\llbracket\neg B\rrbracket^\sharp_e X^n(P) \mid P\in\mathcal{P}\wedge n\in\mathbb{N}\})
\end{aligned}$$

$$
\begin{aligned}
& \wr\text{Any } \textstyle\bigsqcup_{+}^{\sharp}\{\mathsf{post}^{\sharp}[\![\neg\mathtt{B}]\!]_{e}^{\sharp}X^{n}(P) \mid n\in\mathbb{N}\} \text{ is the least upper bound of the increasing chain}\\
& \quad \langle\mathsf{post}^{\sharp}[\![\neg\mathtt{B}]\!]_{e}^{\sharp}X^{n}(P),\ n\in\mathbb{N}\rangle \text{ of } \{\mathsf{post}^{\sharp}[\![\neg B]\!]_{e}^{\sharp}X^{n}(P) \mid P\in\mathcal{P}\wedge n\in\mathbb{N}\} \text{ which, by the dual}\\
& \quad \text{def. (95) of } \alpha^{\uparrow}\text{, belongs to } \alpha^{\uparrow}(\{\mathsf{post}^{\sharp}[\![\neg B]\!]_{e}^{\sharp}X^{n}(P) \mid P\in\mathcal{P}\wedge n\in\mathbb{N}\})\int\\
= {} & \alpha^{\uparrow}(\mathsf{Post}^{\sharp}[\![\neg B]\!]_{e}^{\sharp}(\{X^{n}(P) \mid P\in\mathcal{P}\wedge n\in\mathbb{N}\}) && \wr(40)\int\\
= {} & \alpha^{\uparrow}(\mathsf{Post}^{\sharp}[\![\neg B]\!]_{e}^{\sharp}(\mathsf{lfp}^{\subseteq}\boldsymbol{\lambda}\mathcal{X}\bullet\mathcal{P}\cup\overline{\mathsf{Post}}^{\sharp}[\![\mathtt{if(B)\ S\ else\ skip}]\!]_{e}^{\sharp}(\mathcal{X}))) && \wr(109\int\\
= {} & \alpha^{\uparrow}(\overline{\mathsf{Post}}^{\sharp}[\![\mathtt{while(B)\ S}]\!]_{e}^{\sharp}\mathcal{P}) && \wr(108\int \qquad \square
\end{aligned}
$$

Notice that $\overline{\mathsf{Post}}^{\sharp}[\![\mathtt{while(B)\ \ S}]\!]_{e}^{\sharp}\mathcal{P}$ may contain chains $\mathsf{post}^{\sharp}[\![\neg B]\!]_{e}^{\sharp}X^{n}(P_0) \sqsubseteq_{+}^{\sharp} \mathsf{post}^{\sharp}[\![\neg B]\!]_{e}^{\sharp}X^{n}(P_1) \sqsubseteq_{+}^{\sharp} \ldots \sqsubseteq_{+}^{\sharp} \mathsf{post}^{\sharp}[\![\neg B]\!]_{e}^{\sharp}X^{n}(P_k) \sqsubseteq_{+}^{\sharp} \ldots$ which limit will be in $\alpha^{\uparrow}(\overline{\mathsf{Post}}^{\sharp}[\![\mathtt{while(B)\ \ S}]\!]_{e}^{\sharp}\mathcal{P})$ but not necessarily in $\mathsf{Post}^{\sharp}[\![\mathtt{while(B)\ \ S}]\!]_{e}^{\sharp}\mathcal{P}$. It follows that $\overline{\mathsf{Post}}^{\sharp}[\![\mathtt{while(B)\ \ S}]\!]_{e}^{\sharp}$ may miss limits but also may introduce chains with irrelevant limits of infeasible executions (which invalidates [5, theorem 1] soundness claim).

The following theorem shows the soundness and completeness of rule (103) for the abstract hypercollecting semantics $\overline{\mathsf{Post}}^{\sharp}[\![\mathtt{while(B)\ \ S}]\!]_{e}^{\sharp}$, which by (109), requires the consequent $\mathcal{Q}$ to contain the post condition of any number of iterations for any element P of the antecedent $\mathcal{P}$.

Theorem 21.9. *The proof rule* (103) *is sound and complete relative to* (108).

Proof of theorem 21.9. — The proof of soundness is similar to that of theorem 21.4.

— For completeness, let

$$\mathcal{I} \quad \triangleq \quad \{X^{n}(P) \mid P\in\mathcal{P}\wedge n\in\mathbb{N}\} \tag{110}$$

– The condition $\mathcal{P}\subseteq\mathcal{I}$ of the premise holds for $n = 0$;

– The second condition $\overline{\{\!|}\,\mathcal{I}\,\overline{|\!\}}\ \mathtt{if\ (B)\ else\ skip}\ \overline{\{\!|}\,\mathcal{I}\,\overline{|\!\}}$ of the premise is equivalent, by (62), to $\forall I\in\mathcal{I}\,.\,\mathsf{post}^{\sharp}[\![\mathtt{if\ (B)\ else\ skip}]\!]^{\sharp}I\in\mathcal{I}$, which holds by definition (104) of the iterates.

– The last condition $\overline{\{\!|}\,\mathcal{I}\,\overline{|\!\}}\ \neg\mathtt{B}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}$ of the premise follows from the hypothesis provided by the conclusion of the rule (103).

$$
\begin{aligned}
& \overline{\mathsf{Post}}^{\sharp}[\![\mathtt{while(B)\ \ S}]\!]_{e}^{\sharp}(\mathcal{P})\subseteq\mathcal{Q}\\
\Rightarrow {} & \mathsf{Post}^{\sharp}[\![\neg B]\!]_{e}^{\sharp}(\mathsf{lfp}^{\subseteq}\boldsymbol{\lambda}\mathcal{X}\bullet\mathcal{P}\cup\overline{\mathsf{Post}}^{\sharp}[\![\mathtt{if(B)\ S\ else\ skip}]\!]_{e}^{\sharp}(\mathcal{X}))\subseteq\mathcal{Q}\\
& && \wr\text{def. (108) of } \overline{\mathsf{Post}}^{\sharp}[\![\mathtt{while(B)\ \ S}]\!]_{e}^{\sharp}\mathcal{P}\int\\
\Rightarrow {} & \mathsf{Post}^{\sharp}[\![\neg B]\!]_{e}^{\sharp}(\{X^{n}(P) \mid P\in\mathcal{P}\wedge n\in\mathbb{N}\})\subseteq\mathcal{Q} && \wr\text{lemma 109}\int\\
\Rightarrow {} & \{\mathsf{post}^{\sharp}[\![\neg B]\!]_{e}^{\sharp}(X^{n}(P)) \mid P\in\mathcal{P}\wedge n\in\mathbb{N}\}\subseteq\mathcal{Q} && \wr(40)\int\\
\Rightarrow {} & \forall P\in\mathcal{P}, n\in\mathbb{N}\,.\,\mathsf{post}^{\sharp}[\![\neg B]\!]_{e}^{\sharp}(X^{n}(P))\in\mathcal{Q} && \wr\text{def. }\subseteq\int\\
\Rightarrow {} & \forall P\in\mathcal{I}.\ \mathsf{post}^{\sharp}[\![\neg\mathtt{B}]\!]^{\sharp}P\in\mathcal{Q} && \wr\text{def. (110) of }\mathcal{I}\int\\
\Rightarrow {} & \overline{\{\!|}\,\mathcal{I}\,\overline{|\!\}}\ \neg\mathtt{B}\ \overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}} && \wr(62)\int \qquad \square
\end{aligned}
$$

Theorem 21.9 illustrates the importance of the proper choice of the collecting semantics since proof rule (103) is unsound if $\mathcal{Q}\notin\mathring{\alpha}^{\uparrow}(\wp(\mathbb{L}^{\sharp}))$ and is complete for collecting semantics (108) but not with respect to collecting semantics (56) hence not for the algebraic semantics of section 3.

By deriving the collecting semantics post for execution properties and hypercollecting semantics Post for semantic properties by systematic abstraction of the algebraic semantics of section 3, we guarantee, by composition of successive abstractions satisfying definition 9.1, that the proof rules for these abstractions are sound with respect to any instance of the algebraic semantics satisfying definition 3.2. Moreover, the proof rules are guaranteed to be complete with respect to these abstract properties, by construction.

22 Sound and Complete Proof Rules for Generalized Exists Forall Hyperproperties

In section 22.1 of the appendix, we furthermore introduce conjunctive abstractions (i.e. conjunctions in logics or reduced products in static analysis).

22.1 Conjunctive Abstraction

In this part III, we have introduced abstractions and their compositions. We now consider their conjunctions by intersection. In static analysis with two different abstract domains this would correspond to a reduced product.

22.1.1 Conjunctive Abstractions of Dual Operators. We define the conjunction of abstractions introduced in previous sections of part III.

Definition 22.1 (Dual abstractions).

$$\mathbb{O}\mathbb{p}^{\sqsubseteq} \quad = \quad \{\alpha^{\sqsubseteq}, \alpha^{\sqsubseteq\overline{F}}, \overset{*}{\alpha}^{\sqsubseteq\uparrow}, \alpha^{\curlywedge}\} \tag{111}$$

$$\mathbb{O}\mathbb{p}^{\sqsupseteq} \quad = \quad \{\alpha^{\sqsupseteq}, \alpha^{\sqsupseteq\underline{F}}, \overset{*}{\alpha}^{\sqsupseteq\downarrow}, \alpha^{\curlyvee}\} \tag{112}$$

The conjunctive abstraction operator $\mathbf{R}$ takes two idempotent abstraction $\alpha_1 \in \mathbb{O}\mathbb{p}^{\sqsubseteq}$ and $\alpha_2 \in \mathbb{O}\mathbb{p}^{\sqsupseteq}$ and returns a new abstraction function that abstracts property $\mathcal{P}$ to the intersection of $\alpha_1(\mathcal{P})$ and $\alpha_2(\mathcal{P})$.

$$\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle} \triangleq \boldsymbol{\lambda}\mathcal{P} \bullet \alpha_1(\mathcal{P}) \cap \alpha_2(\mathcal{P}) \tag{113}$$

Lemma 22.2 (Properties of the well-defined conjunctive abstraction). *For any $\alpha_1 \in \mathbb{O}\mathbb{p}^{\sqsubseteq}$, $\alpha_2 \in \mathbb{O}\mathbb{p}^{\sqsupseteq}$, and $\mathcal{P} \in \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\wp(\mathbb{L}))$, we have* (1) *$\alpha_1(\wp(\mathbb{L})) \subseteq \alpha^{\sqsubseteq}(\wp(\mathbb{L}))$ and $\alpha_2(\wp(\mathbb{L})) \subseteq \alpha^{\sqsupseteq}(\wp(\mathbb{L}))$;* (2) *$\alpha^{\sqsubseteq}(\mathcal{P}) \cap \alpha^{\sqsupseteq}(\mathcal{P}) = \mathcal{P}$; and* (3) *if both α_1 and α_2 are upper-closures, then $\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}$ is also an upper-closure.*

Proof of lemma 22.2. (1) directly follows from the definitions. Let us then prove (2). For an arbitrary hyperproperty $\mathcal{Q} \in \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}$, we have $\mathcal{Q} = \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\mathcal{P})$ for some $\mathcal{P} \in \mathbb{L}$. It follows that

$$\begin{aligned}
& \alpha^{\sqsubseteq}(\mathcal{Q}) \cap \alpha^{\sqsupseteq}(\mathcal{Q}) \\
= {} & \alpha^{\sqsubseteq}(\alpha_1(\mathcal{P}) \cap \alpha_2(\mathcal{P})) \cap \alpha^{\sqsupseteq}(\alpha_1(\mathcal{P}) \cap \alpha_2(\mathcal{P})) && \text{(def. of } \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}\text{)} \\
\subseteq {} & \alpha^{\sqsubseteq} \circ \alpha_1(\mathcal{P}) \cap \alpha^{\sqsubseteq} \circ \alpha_2(\mathcal{P}) \cap \alpha^{\sqsupseteq} \circ \alpha_2(\mathcal{P}) \cap \alpha^{\sqsupseteq} \circ \alpha_1(\mathcal{P}) && \text{(def. of } \alpha^{\sqsubseteq} \text{ and } \alpha^{\sqsupseteq} \text{ that are increasing)} \\
= {} & \alpha^{\sqsubseteq} \circ \alpha_1(\mathcal{P}) \cap \alpha^{\sqsupseteq} \circ \alpha_2(\mathcal{P}) \\
& \text{(}\alpha^{\sqsupseteq} \circ \alpha_1(\mathcal{P}) = \mathbb{L} \text{ for non-empty } \alpha_1(\mathcal{P}) \text{ since } \{\bot\} \in \alpha_1(\mathcal{P})\text{. The equation trivially holds when } \alpha_1(\mathcal{P}) = \varnothing\text{)} \\
= {} & \alpha_1(\mathcal{P}) \cap \alpha_2(\mathcal{P}) && \text{(def. of } \alpha_1(\mathcal{P}) \in \alpha^{\sqsubseteq}(\wp(\mathbb{L})) \text{ and } \alpha_2(\mathcal{P}) \in \alpha^{\sqsupseteq}(\wp(\mathbb{L}))\text{)} \\
= {} & \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\mathcal{P}) = \mathcal{Q} && \text{(def. of } \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}\text{)}
\end{aligned}$$

The inverse holds because $\alpha^{\sqsubseteq} \cap \alpha^{\sqsupseteq}$ is extensive. Then we have $\alpha^{\sqsubseteq}(\mathcal{P}) \cap \alpha^{\sqsupseteq}(\mathcal{P}) = \mathcal{P}$.

Now let us now prove (3). $\mathrm{R}_{\langle\alpha_1,\,\alpha_2\rangle}$ is increasing and extensive by definition when α_1 and α_2 are increasing and extensive. We now prove that it is idempotent, which amounts to showing that $\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\mathcal{P}) \subseteq \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle} \circ \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\mathcal{P})$ for any $\mathcal{P} \in \wp(\mathbb{L})$.

$$\begin{aligned}
& \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle} \circ \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\mathcal{P}) \\
= {} & \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\alpha_1(\mathcal{P}) \cap \alpha_2(\mathcal{P})) && \text{(def. of } \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}\text{)} \\
= {} & \alpha_1(\alpha_1(\mathcal{P}) \cap \alpha_2(\mathcal{P})) \cap \alpha_2(\alpha_1(\mathcal{P}) \cap \alpha_2(\mathcal{P})) && \text{(def. of } \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}\text{)} \\
\subseteq {} & \alpha_1 \circ \alpha_1(\mathcal{P}) \cap \alpha_1 \circ \alpha_2(\mathcal{P}) \cap \alpha_2 \circ \alpha_2(\mathcal{P}) \cap \alpha_2 \circ \alpha_1(\mathcal{P}) && \text{(def. of } \alpha_1 \text{ and } \alpha_2 \text{ that are increasing)} \\
= {} & \alpha_1 \circ \alpha_1(\mathcal{P}) \cap \alpha_2 \circ \alpha_2(\mathcal{P})
\end{aligned}$$

⟅$\alpha_1 \circ \alpha_1(\varnothing) = \varnothing$. For non-empty $\mathcal{P}$, $\alpha_2 \circ \alpha_1(\mathcal{P}) = \mathbb{L}$, since $\bot \in \alpha_1(\mathcal{P})$. The equation trivially holds when $\alpha_1(\mathcal{P}) = \varnothing$⟆

$= \alpha_1(\mathcal{P}) \cap \alpha_2(\mathcal{P})$ ⟅def. of α_1 and α_2 that are idempotent⟆

$= \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\mathcal{P})$ ⟅def. of $\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}$⟆

As a result, $\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\mathcal{P})$ is idempotent since $\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\mathcal{P})$ is extensive that implies $\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\mathcal{P}) \supseteq \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle} \circ \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\mathcal{P})$. □

The domain conjunctive abstraction $\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}$ is more expressive than both both α_1 and α_2.

Lemma 22.3. *For a well-defined conjunctive abstraction $\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}$, we have the Galois retractions $\langle\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\wp(\mathbb{L})),\ \subseteq\rangle \underset{\alpha^{\sqsubseteq}}{\overset{\mathbb{1}}{\leftrightarrows}} \langle\alpha_1(\wp(\mathbb{L})),\ \subseteq\rangle$ and $\langle\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\wp(\mathbb{L})),\ \subseteq\rangle \underset{\alpha^{\sqsupseteq}}{\overset{\mathbb{1}}{\leftrightarrows}} \langle\alpha_2(\wp(\mathbb{L})),\ \subseteq\rangle$.*

Proof of lemma 22.3. Without any loss of generality, let us prove the first Galois connection.

We first show that for an arbitrary $\mathcal{P} \in \alpha_1(\wp(\mathbb{L}))$, $\mathbb{1}(\mathcal{P}) = \mathcal{P}$ is in $\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\wp(\mathbb{L}))$. $\mathcal{P}$ can be express by $\mathcal{P} = \alpha_1(\mathcal{Q})$ for some $\mathcal{Q} \in \mathbb{L}$. If $\mathcal{P} = \varnothing$, then it's trivially in $\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}$. If $\mathcal{P} \neq \varnothing$, then

$\mathcal{P} = \alpha_1(\mathcal{Q})$

$= \alpha_1 \circ \alpha_1(\mathcal{Q}) \cap \alpha_2 \circ \alpha_1(\mathcal{Q})$ ⟅α_1 is idempotent and $\alpha_2 \circ \alpha_1(\mathcal{Q}) = \mathbb{L}$ for non-empty $\alpha_1(\mathcal{Q})$⟆

$= \alpha_1(\mathcal{P}) \cap \alpha_2(\mathcal{P})$ ⟅replace $\alpha_1(\mathcal{Q})$ by $\mathcal{P}$⟆

Thus, $\mathcal{P}$ is in $\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\wp(\mathbb{L}))$. Since $\mathcal{P} \in \alpha^{\sqsubseteq}(\wp(\mathbb{L}))$ by (1) of lemma 22.2, we know that $\alpha^{\sqsubseteq} \circ \mathbb{1}(\mathcal{P}) = \mathcal{P}$, proving the Galois retraction. □

Lemma 22.4. *For a well-defined conjunctive abstraction operator $\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}$, if α_1 and α_2 are upper closure operators, so is $\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}$, and $\langle\wp(\mathbb{L}),\ \subseteq\rangle \underset{\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}}{\overset{\mathbb{1}}{\leftrightarrows}} \langle\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\wp(\mathbb{L})),\ \subseteq\rangle$.*

Proof. This follows from Lemma 22.2 implying that $\mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}$ is an upper closure operator. □

22.1.2 Proof Rule Simplification. Applying the consequence rule $\frac{\overline{\{\!\mid}\mathcal{P}\overline{\mid\!\}}\,\mathtt{S}\,\overline{\{\!\mid}\mathcal{Q}\overline{\mid\!\}}\quad \overline{\{\!\mid}\mathcal{P}\overline{\mid\!\}}\,\mathtt{S}\,\overline{\{\!\mid}\mathcal{R}\overline{\mid\!\}}}{\overline{\{\!\mid}\mathcal{P}\overline{\mid\!\}}\,\mathtt{S}\,\overline{\{\!\mid}\mathcal{Q}\cap\mathcal{R}\overline{\mid\!\}}}$, we get the following sound and complete rule for the conjunctive abstraction.

$$\frac{\overline{\{\!\mid}\mathcal{P}\overline{\mid\!\}}\,\mathtt{S}\,\overline{\{\!\mid}\alpha^{\sqsubseteq}(\mathcal{Q})\overline{\mid\!\}}\quad \overline{\{\!\mid}\mathcal{P}\overline{\mid\!\}}\,\mathtt{S}\,\overline{\{\!\mid}\alpha^{\sqsupseteq}(\mathcal{Q})\overline{\mid\!\}}}{\overline{\{\!\mid}\mathcal{P}\overline{\mid\!\}}\,\mathtt{S}\,\overline{\{\!\mid}\mathcal{Q}\overline{\mid\!\}}},\quad \mathcal{Q} \in \mathbf{R}_{\langle\alpha_1,\,\alpha_2\rangle}(\wp(\mathbb{L})) \tag{114}$$

Proof of (114).

$\overline{\{\!\mid}\mathcal{P}\overline{\mid\!\}}\,\mathtt{S}\,\overline{\{\!\mid}\mathcal{Q}\overline{\mid\!\}}$

$\Leftrightarrow \mathsf{Post}[\![\mathtt{S}]\!]^\sharp(\mathcal{P}) \subseteq \mathcal{Q}$ ⟅def. of $\overline{\{\!\mid}\mathcal{P}\overline{\mid\!\}}\,\mathtt{S}\,\overline{\{\!\mid}\mathcal{Q}\overline{\mid\!\}}$⟆

$\Leftrightarrow \mathsf{Post}[\![\mathtt{S}]\!]^\sharp(\mathcal{P}) \subseteq \alpha^{\sqsubseteq}(\mathcal{Q}) \cap \alpha^{\sqsupseteq}(\mathcal{Q})$ ⟅By lemma 22.2⟆

$\Leftrightarrow \mathsf{Post}[\![\mathtt{S}]\!]^\sharp(\mathcal{P}) \subseteq \alpha^{\sqsubseteq}(\mathcal{Q}) \wedge \mathsf{Post}[\![\mathtt{S}]\!]^\sharp(\mathcal{P}) \subseteq \alpha^{\sqsupseteq}(\mathcal{Q})$ ⟅By consequence rule⟆

$\Leftrightarrow \overline{\{\!\mid}\mathcal{P}\overline{\mid\!\}}\,\mathtt{S}\,\overline{\{\!\mid}\alpha^{\sqsubseteq}(\mathcal{Q})\overline{\mid\!\}} \wedge \overline{\{\!\mid}\mathcal{P}\overline{\mid\!\}}\,\mathtt{S}\,\overline{\{\!\mid}\alpha^{\sqsupseteq}(\mathcal{Q})\overline{\mid\!\}}$ ⟅def. of $\overline{\{\!\mid}\mathcal{P}\overline{\mid\!\}}\,\mathtt{S}\,\overline{\{\!\mid}\mathcal{Q}\overline{\mid\!\}}$⟆ □

Lemma 22.3 shows that $\alpha^{\sqsubseteq}(\mathcal{Q}) \in \alpha_1(\wp(\mathbb{L}))$, and $\alpha^{\sqsupseteq}(\mathcal{Q}) \in \alpha_2(\wp(\mathbb{L}))$. Therefore we have similar rules for the case when the post-condition is in $\alpha_1(\wp(\mathbb{L}))$ and $\alpha_2(\wp(\mathbb{L}))$ respectively. An example is given in the next section.

22.2 Lower $\sqsubseteq$-closed and frontier elimination

Let us define the $\sqsubseteq$-closed lower closure operator $\varrho^{\sqsubseteq}$

$$\varrho^{\sqsubseteq} \quad \triangleq \quad \boldsymbol{\lambda}\mathcal{P}\bullet\{P\in\mathcal{P}\mid\forall P'\in\mathbb{L}\,.\,P'\sqsubseteq P\Rightarrow P'\in\mathcal{P}\} \tag{115}$$

Lemma 22.5. *$\varrho^{\sqsubseteq}$ is a lower-closure that is increasing, reductive and idempotent, and* $\langle\wp(\mathbb{L}),\supseteq\rangle \mathrel{\substack{\xleftarrow{\;\mathbb{1}\;}\\ \xrightarrow[\varrho^{\sqsubseteq}]{}}} \langle\alpha^{\sqsubseteq}(\wp(\mathbb{L})),\supseteq\rangle$

Proof of lemma 22.5. By definition of $\varrho^{\sqsubseteq}$, it is trivially increasing and reductive. Let us first prove that $\varrho^{\sqsubseteq}(\mathcal{P})\in\alpha^{\sqsubseteq}(\wp(\mathbb{L}))$ for arbitrary $\mathcal{P}\in\wp(\mathbb{P})$. We have

$\alpha^{\sqsubseteq}\circ\varrho^{\sqsubseteq}(\mathcal{P})$

$= \{P\in\mathbb{L}\mid\exists P'\in\varrho^{\sqsubseteq}(\mathcal{P})\,.\,P\sqsubseteq P'\}$ ≀def. of $\alpha^{\sqsubseteq}$ʃ

$= \{P\in\mathbb{L}\mid\exists P'\in\mathcal{P}\,.\,(\forall P''\in\mathbb{L}\,.\,P''\sqsubseteq P'\Rightarrow P''\in\mathcal{P})\wedge P\sqsubseteq P'\}$ ≀def. of $\varrho^{\sqsubseteq}$ʃ

$= \{P\in\mathbb{L}\mid P\in\mathcal{P}\wedge(\forall P''\in\mathbb{L}\,.\,P''\sqsubseteq P\Rightarrow P''\in\mathcal{P})\}$

≀($\subseteq$) holds as $\alpha^{\sqsubseteq}$ is extensive;
($\supseteq$) choose $P'=P$ʃ

$= \varrho^{\sqsubseteq}(\mathcal{P})$ ≀def. of $\varrho^{\sqsubseteq}$ʃ

We then prove that $\varrho^{\sqsubseteq}\circ\alpha^{\sqsubseteq}(\mathcal{P})=\alpha^{\sqsubseteq}(\mathcal{P})$

$\varrho^{\sqsubseteq}\circ\alpha^{\sqsubseteq}(\mathcal{P})$

$= \{P\in\alpha^{\sqsubseteq}(\mathcal{P})\mid\forall P'\in\mathbb{L}\,.\,P'\sqsubseteq P\Rightarrow P'\in\alpha^{\sqsubseteq}(\mathcal{P})\}$ ≀def. of $\varrho^{\sqsubseteq}$ʃ

$= \{P\in\mathbb{L}\mid(\exists Q\in\mathcal{P}\,.\,P\sqsubseteq Q)\wedge\forall P'\in\mathbb{L}\,.\,P'\sqsubseteq P\Rightarrow(\exists Q'\in\mathcal{Q}\,.\,P'\sqsubseteq Q')\}$ ≀def. of $\alpha^{\sqsubseteq}$ʃ

$= \{P\in\mathbb{L}\mid\exists Q\in\mathcal{P}\,.\,P\sqsubseteq Q\}$

≀($\supseteq$) as $\varrho^{\sqsubseteq}$ is reductive;
($\subseteq$) for all $P'\sqsubseteq P$, simply let $Q'=Q$, then $P'\sqsubseteq P\sqsubseteq Q=Q'$ holdsʃ

$= \alpha^{\sqsubseteq}(\mathcal{P})$ ≀def. of $\alpha^{\sqsubseteq}$ʃ

Thus, we have proved that $\varrho^{\sqsubseteq}(\wp(\mathbb{L}))=\alpha^{\sqsubseteq}(\wp(\mathbb{L}))$. For any $\mathcal{P}\in\mathbb{P}$, we have $\varrho^{\sqsubseteq}\circ\varrho^{\sqsubseteq}(\mathcal{P})=\varrho^{\sqsubseteq}(\mathcal{P})$, since $\varrho^{\sqsubseteq}(\mathcal{P})$ is included in $\alpha^{\sqsubseteq}(\wp(\mathbb{L}))$. □

22.3 Frontier ϱ-Elimination Abstraction

We define a new abstraction based on $\alpha^{\underline{F}}$ and $\varrho^{\sqsubseteq}$

$$\varrho^{\sqsubseteq\underline{F}} \quad \triangleq \quad \boldsymbol{\lambda}\mathcal{P}\bullet\bigcup_{F\in\alpha^{\underline{F}}(\mathcal{P})}\varphi^{\sqsubseteq}(F)\mathcal{P} \tag{116}$$

$$\text{where }\varphi^{\sqsubseteq} \quad \triangleq \quad \boldsymbol{\lambda}F\in\mathbb{L}\bullet\boldsymbol{\lambda}\mathcal{X}\in\wp(\mathbb{L})\bullet\{P\in\mathcal{X}\mid F\sqsubseteq P\wedge\forall P'\in\mathbb{L}\,.\,F\sqsubseteq P'\sqsubseteq P\Rightarrow P'\in\mathcal{X}\}$$

Lemma 22.6. *$\varrho^{\sqsubseteq\underline{F}}$ is reductive and idempotent*

Proof of lemma 22.6. For any $\mathcal{P}\in\wp(\mathbb{L})$ and $P\in\varrho^{\sqsubseteq\underline{F}}(\mathcal{P})$, we have $P\in\varphi^{\sqsubseteq}(F)\mathcal{P}$ for some $F\in\alpha^{\underline{F}}(\mathcal{P})$, meaning it is in $\mathcal{P}$. Thus $\varrho^{\sqsubseteq\underline{F}}$ is reductive. To prove idempotency, let us first prove that $\varrho^{\sqsubseteq\underline{F}}$ preserve lower-frontiers, that is $\alpha^{\underline{F}}(\mathcal{P})=\alpha^{\underline{F}}\circ\varrho^{\sqsubseteq\underline{F}}(\mathcal{P})$.

$\alpha^{\underline{F}}\circ\varrho^{\sqsubseteq\underline{F}}(\mathcal{P})$

$= \{P\in\varrho^{\sqsubseteq\underline{F}}(\mathcal{P})\mid\forall P'\in\varrho^{\sqsubseteq\underline{F}}(\mathcal{P})\,.\,P'\sqsubseteq P\Rightarrow P=P'\}$ ≀def. of $\alpha^{\underline{F}}$ʃ

$= \{P\in\mathcal{P}\mid(\exists F\in\alpha^{\underline{F}}(\mathcal{P})\,.\,F\sqsubseteq P\wedge\forall P'\in\mathbb{L}\,.\,F\sqsubseteq P'\sqsubseteq P\Rightarrow P'\in\mathcal{P})\wedge$
$\forall P_1\in\mathcal{P}\,.\,((\exists F_1\in\alpha^{\underline{F}}(\mathcal{P})\,.\,F_1\sqsubseteq P_1\wedge\forall P_1'\in\mathbb{L}\,.\,F_1\sqsubseteq P_1'\sqsubseteq P_1\Rightarrow P_1'\in\mathcal{P})\wedge P_1\sqsubseteq P)\Rightarrow P=P_1\}$
≀def. of $\varrho^{\sqsubseteq\underline{F}}$ʃ

$= \{P\in\mathbb{L}\mid\exists G\in\alpha^{\underline{F}}(P)\,.\,G=P\}=\alpha^{\underline{F}}(\mathcal{P})$

⟅$(\supseteq)$ When $G = P$, then for all P_1 such that $P_1 \sqsubseteq P$, $P_1 = P$ holds trivially;
$(\subseteq)$ Since $\exists F_1 \in \alpha^{\underline{F}}(\mathcal{P})\ .\ F_1 \sqsubseteq P_1 \wedge \forall P_1' \in \mathbb{L}\ .\ F_1 \sqsubseteq P_1' \sqsubseteq P_1 \Rightarrow P_1' \in \mathcal{P}$ holds if P_1 is instantiated to F, then the equality $P = F$ holds, where F is a lower-frontier. Thus we can simply let G to be F.⟆

We now prove idempotency. Since $\alpha^{\underline{F}}(\mathcal{P}) = \alpha^{\underline{F}} \circ \varrho^{\sqsubseteq\underline{F}}(\mathcal{P})$, it remains to prove that $\varphi^{\sqsubseteq}(F)\mathcal{P} = \varphi^{\sqsubseteq}(F)(\varrho^{\sqsubseteq\underline{F}}(\mathcal{P}))$ for any $F \in \alpha^{\underline{F}}(\mathcal{P})$.

$$\begin{aligned}
&\varphi^{\sqsubseteq}(F)(\varrho^{\sqsubseteq\underline{F}}(\mathcal{P}))\\
=\ &\{P \in \varrho^{\sqsubseteq\underline{F}}(\mathcal{P}) \mid F \sqsubseteq P \wedge \forall P' \in \mathbb{L}\ .\ F \sqsubseteq P' \sqsubseteq P \Rightarrow P' \in \varrho^{\sqsubseteq\underline{F}}(\mathcal{P})\} && \text{⟅def. of } \varphi^{\sqsubseteq}\text{⟆}\\
=\ &\{P \in \mathcal{P} \mid (\exists F_1 \in \alpha^{\underline{F}}(\mathcal{P})\ .\ F_1 \sqsubseteq P \wedge \forall P' \in \mathbb{L}\ .\ F_1 \sqsubseteq P' \sqsubseteq P \Rightarrow P' \in \mathcal{P}) \wedge F \sqsubseteq P \wedge\\
&\forall P_2 \in \mathbb{L}\ .\ F \sqsubseteq P_2 \sqsubseteq P \Rightarrow (\exists F_2 \in \alpha^{\underline{F}}(\mathcal{P})\ .\ F_2 \sqsubseteq P_2 \wedge (\forall P_2' \in \mathbb{L}\ .\ F_2 \sqsubseteq P_2' \sqsubseteq P_2 \Rightarrow P_2' \in \mathcal{P}))\}\\
& && \text{⟅def. of } \varrho^{\sqsubseteq\underline{F}}\text{, replace } P' \text{ with } P_2\text{⟆}\\
=\ &\{P \in \mathcal{P} \mid F \sqsubseteq P \wedge \forall P' \in \mathbb{L}\ .\ F \sqsubseteq P' \sqsubseteq P \Rightarrow P' \in \mathcal{P}\}
\end{aligned}$$

⟅$(\supseteq)$ since we have assumed that F is a lower frontier for $\mathcal{P}$, we can simply let $F_1 = F_2 = F$, and all the conditions do hold;
$(\subseteq)$ To prove $\forall P' \in \mathbb{L}\ .\ F \sqsubseteq P' \sqsubseteq P \Rightarrow P' \in \mathcal{P}$. We are allowed to instantiate $P_2 = P'$ in the premise $\forall P_2 \in \mathbb{L}\ .\ F \sqsubseteq P_2 \sqsubseteq P \Rightarrow \exists F_2 \in \alpha^{\underline{F}}(\mathcal{P})\ .\ F_2 \sqsubseteq P_2 \wedge (\forall P_2' \in \mathbb{L}\ .\ F_2 \sqsubseteq P_2' \sqsubseteq P_2 \Rightarrow P_2' \in \mathcal{P})$. Then we get $\forall P_2' \in \mathbb{L}\ .\ F_2 \sqsubseteq P_2' \sqsubseteq P' \Rightarrow P_2' \in \mathcal{P}$ for some frontier F_2 where $F_2 \sqsubseteq P'$. We are then allowed to instantiate P_2' to P', which implies that $P' \in \mathcal{P}$ holds.⟆

Therefore, we proved idempotency. □

22.4 Exist Forall Hyperproperties

Assuming that $\langle \mathbb{L}, \sqsubseteq\rangle \triangleq \langle \wp(\Pi), \subseteq\rangle$. $\exists\forall$ hyperproperties have the form

$$\mathcal{EAH} \quad\triangleq\quad \{\{P \in \wp(\Pi) \mid \exists \pi_1 \in P\ .\ \forall \pi_2 \in P\ ,\ \langle \pi_1,\ \pi_2\rangle \in A\} \mid A \in \wp(\Pi \times \Pi)\} \tag{117}$$

Example 22.7. The negation *GD* of the generalized non-interference properties *GNI* in (98) is a $\exists\forall$ hyperproperty expressing generalized dependency. A set of executions satisfies the generalized dependency when altering the initial values of high variables does change the set of possible final values of any low variable.

$$\begin{aligned}
GD \quad\triangleq\quad &\{P \in \mathbb{L} \mid \exists \sigma_1\pi_1\sigma_1', \sigma_2\pi\sigma_2' \in P\ .\ \forall \sigma_3\pi\sigma_3' \in P\ . &(118)\\
&\quad(\sigma_1(\mathtt{L}) = \sigma_2(\mathtt{L}) = \sigma_3(\mathtt{L})) \Rightarrow (\sigma_3(\mathtt{H}) = \sigma_2(\mathtt{H}) \Rightarrow \sigma_3'(\mathtt{L}) \neq \sigma_1'(\mathtt{L}))\} &\blacksquare
\end{aligned}$$

The hyperproperties with $\varrho^{\sqsubseteq\underline{F}}$ subsume $\exists\forall$ hyperproperties.

$$\mathcal{EAH} \quad\subseteq\quad \varrho^{\sqsubseteq\underline{F}}(\wp(\wp(\Pi))) \tag{119}$$

Proof of (119). We prove that $\forall \mathcal{P} \in \mathcal{EAH}\ .\ \mathcal{P} \in \varrho^{\sqsubseteq\underline{F}}(\wp(\wp(\Pi)))$. By Lemma 22.6, it is sufficient to prove that $\mathcal{P} \subseteq \varrho^{\sqsubseteq\underline{F}}(\mathcal{P})$ due to the fact that $\varrho^{\sqsubseteq\underline{F}}$ is reductive and idempotent. $\mathcal{P}$ is expressed as $\mathcal{P} \triangleq \{P \in \wp(\Pi) \mid \exists \pi_1 \in P\ .\ \forall \pi_2 \in P\ ,\ \langle \pi_1,\ \pi_2\rangle \in A\}$ for some A.

$$\begin{aligned}
&\varrho^{\sqsubseteq\underline{F}}(\mathcal{P})\\
=\ &\bigcup_{F \in \alpha^{\underline{F}}(\mathcal{P})} \varphi^{\sqsubseteq}(F)\mathcal{P} && \text{⟅def. of } \varrho^{\sqsubseteq\underline{F}}\text{⟆}\\
=\ &\bigcup_{F \in \alpha^{\underline{F}}(\mathcal{P})} \{P \in \mathcal{P} \mid F \subseteq P \wedge \forall P' \in \mathbb{L}\ .\ F \subseteq P' \subseteq P \Rightarrow P' \in \mathcal{P}\} && \text{⟅def. of } \varphi^{\sqsubseteq}\text{⟆}\\
=\ &\{P \in \mathcal{P} \mid \exists F \in \alpha^{\underline{F}}(\mathcal{P})\ .\ F \subseteq P \wedge \forall P' \in \mathbb{L}\ .\ F \subseteq P' \subseteq P \Rightarrow P' \in \mathcal{P}\} && \text{⟅def. of } \textstyle\bigcup\text{⟆}\\
\supseteq\ &\{P \in \wp(\Pi) \mid \exists \pi_1 \in P\ .\ \forall \pi_2 \in P\ .\ \langle \pi_1,\ \pi_2\rangle \in A\} = \mathcal{P}
\end{aligned}$$

⟅For arbitrary $P \in \mathcal{P}$, there exists $\pi \in P$ where for all $\langle \pi,\ \pi' \rangle \in A$ holds for all $\pi' \in P$. Let $F \triangleq \{\pi\}$, which would be in $\alpha^{\underline{F}}(\mathcal{P})$ as $\varnothing \notin \mathcal{P}$ by definition. Then $F \subseteq P$ holds trivially. For all P' such that $F = \{\pi\} \subseteq P' \subseteq P$. Let π be the existent π_1, then for all $\pi_2 \in P'$, it is also in P. Thus we have $\langle \pi,\ \pi_2 \rangle \in A$, meaning that $P' \in \mathcal{P}$ ⟆ □

22.5 Proof Rule Simplification

Using the consequence rule, we introduce a sound and complete proof rule that splits an abstract frontier-$\varrho^{\sqsubseteq}$ eliminated abstract hyperproperties into a conjunctive abstraction. This requires manual efforts that partition the precondition $\mathcal{P}$ into frontier-indexed preconditions $\mathcal{X}$ where $\mathcal{X}_F \in \wp(\mathbb{L})$ for $F \in \alpha^{\underline{F}}(\mathcal{Q})$. Then we can further use the consequence rule to prove the triple for the correspondent conjunctive abstraction.

$$\frac{\exists \mathcal{X} \in \alpha^{\underline{F}}(\mathcal{Q}) \to \wp(\mathbb{L}^{\sharp})\ .\ \forall F \in \alpha^{\underline{F}}(\mathcal{Q})\ .\ \overline{\{\!\!|}\,\mathcal{X}_F\,\overline{|\!\!\}}\ \mathsf{S}\ \overline{\{\!\!|}\,\varphi^{\sqsubseteq}(F)\mathcal{Q}\,\overline{|\!\!\}},\quad \mathcal{P} \subseteq \bigcup_{F \in \alpha^{\underline{F}}(\mathcal{Q})} \mathcal{X}_F}{\overline{\{\!\!|}\,\mathcal{P}\,\overline{|\!\!\}}\ \mathsf{S}\ \overline{\{\!\!|}\,\mathcal{Q}\,\overline{|\!\!\}}},\quad \mathcal{Q} \in \varrho^{\sqsubseteq\underline{F}}(\wp(\wp(\Pi))) \tag{120}$$

Proof of (120).

$$\begin{array}{ll}
& \overline{\{\!\!|}\,\mathcal{P}\,\overline{|\!\!\}}\ \mathsf{S}\ \overline{\{\!\!|}\,\mathcal{Q}\,\overline{|\!\!\}} \\
\Leftrightarrow & \mathsf{Post}[\![\mathsf{S}]\!]^{\sharp}(\mathcal{P}) \subseteq \mathcal{Q} \hfill \wr\text{def. of } \overline{\{\!\!|}\,\mathcal{P}\,\overline{|\!\!\}}\ \mathsf{S}\ \overline{\{\!\!|}\,\mathcal{Q}\,\overline{|\!\!\}}\wr \\
\Leftrightarrow & \mathsf{Post}[\![\mathsf{S}]\!]^{\sharp}(\mathcal{P}) \subseteq \displaystyle\bigcup_{F \in \alpha^{\underline{F}}(\mathcal{Q})} \varphi^{\sqsubseteq}(F)\mathcal{Q} \hfill \wr\text{lemma 22.6}\wr \\
\Leftrightarrow & \exists \mathcal{X} \in \alpha^{\underline{F}}(\mathcal{Q}) \to \wp(\mathbb{L}^{\sharp})\ .\ \mathsf{Post}[\![\mathsf{S}]\!]^{\sharp}(\displaystyle\bigcup_{F \in \alpha^{\underline{F}}(\mathcal{Q})} \mathcal{X}_F) \subseteq \bigcup_{F \in \alpha^{\underline{F}}(\mathcal{Q})} \varphi^{\sqsubseteq}(F)\mathcal{Q} \quad\wedge\quad \mathcal{P} \subseteq \bigcup_{F \in \alpha^{\underline{F}}(\mathcal{Q})} \mathcal{X}_F \\
& \hfill \wr(\Rightarrow)\quad \text{let } \mathcal{X}_F = \mathcal{P} \text{ for all } F.\quad (\Leftarrow)\quad \mathsf{Post}[\![\mathsf{S}]\!]^{\sharp}(\mathcal{P}) \text{ is increasing.}\wr \\
\Leftrightarrow & \exists \mathcal{X} \in \alpha^{\underline{F}}(\mathcal{Q}) \to \wp(\mathbb{L}^{\sharp})\ .\ \displaystyle\bigcup_{F \in \alpha^{\underline{F}}(\mathcal{Q})} \mathsf{Post}[\![\mathsf{S}]\!]^{\sharp}(\mathcal{X}_F) \subseteq \bigcup_{F \in \alpha^{\underline{F}}(\mathcal{Q})} \varphi^{\sqsubseteq}(F)\mathcal{Q} \quad\wedge\quad \mathcal{P} \subseteq \bigcup_{F \in \alpha^{\underline{F}}(\mathcal{Q})} \mathcal{X}_F \\
& \hfill \wr\mathsf{Post}[\![\mathsf{S}]\!]^{\sharp} \text{ is join preserving}\wr \\
\Leftrightarrow & \exists \mathcal{X} \in \alpha^{\underline{F}}(\mathcal{Q}) \to \wp(\mathbb{L}^{\sharp})\ .\ \forall F \in \alpha^{\underline{F}}(\mathcal{Q})\ .\ \mathsf{Post}[\![\mathsf{S}]\!]^{\sharp}(\mathcal{X}_F) \subseteq^{\sqsubseteq} (F)\mathcal{Q} \quad\wedge\quad \mathcal{P} \subseteq \displaystyle\bigcup_{F \in \alpha^{\underline{F}}(\mathcal{Q})} \mathcal{X}_F \\
& \hfill \wr\text{consequence rule}\wr \\
\Leftrightarrow & \exists \mathcal{X} \in \alpha^{\underline{F}}(\mathcal{Q}) \to \wp(\mathbb{L}^{\sharp})\ .\ \forall F \in \alpha^{\underline{F}}(\mathcal{Q})\ .\ \overline{\{\!\!|}\,\mathcal{X}_F\,\overline{|\!\!\}}\ \mathsf{S}\ \overline{\{\!\!|}\,\varphi^{\sqsubseteq}(F)\mathcal{Q}\,\overline{|\!\!\}} \quad\wedge\quad \mathcal{P} \subseteq \displaystyle\bigcup_{F \in \alpha^{\underline{F}}(\mathcal{Q})} \mathcal{X}_F \\
& \hfill \wr\text{def. of } \overline{\{\!\!|}\,\mathcal{P}\,\overline{|\!\!\}}\ \mathsf{S}\ \overline{\{\!\!|}\,\mathcal{Q}\,\overline{|\!\!\}}\wr \quad \square
\end{array}$$

Now the problem is reduced to proving the premise $\overline{\{\!\!|}\,\mathcal{X}_F\,\overline{|\!\!\}}\ \mathsf{S}\ \overline{\{\!\!|}\,\varphi^{\sqsubseteq}(F)\mathcal{Q}\,\overline{|\!\!\}}$. Interestingly, we are able to apply the rule for conjunctive abstraction to $\varphi^{\sqsubseteq}(F)\mathcal{Q}$.

Lemma 22.8. *For arbitrary $\mathcal{P} \in \wp(\mathbb{L})$, and $F \in \alpha^{\underline{F}}(\mathcal{P})$, $\varphi^{\sqsubseteq}(F)\mathcal{P} \in \mathbf{R}_{\langle \alpha^{\sqsubseteq},\, \alpha^{\curlyvee} \rangle}(\wp(\mathbb{L}))$.*

Proof. By lemma 22.4, it's sufficient to prove that $\mathbf{R}_{\langle \alpha^{\sqsubseteq},\, \alpha^{\curlyvee} \rangle} \circ \varphi^{\sqsubseteq}(F)\mathcal{P} = \varphi^{\sqsubseteq}(F)\mathcal{P}$

$$\begin{array}{ll}
& \mathbf{R}_{\langle \alpha^{\sqsubseteq},\, \alpha^{\curlyvee} \rangle} \circ \varphi^{\sqsubseteq}(F)\mathcal{P} \\
= & \alpha^{\sqsubseteq} \circ \varphi^{\sqsubseteq}(F)\mathcal{P} \cap \alpha^{\curlyvee} \circ \varphi^{\sqsubseteq}(F)\mathcal{P} \hfill \wr\text{def. of } \mathbf{R}_{\langle \alpha^{\sqsubseteq},\, \alpha^{\curlyvee} \rangle}\wr \\
= & \{P \in \mathbb{L} \mid \exists P' \in \varphi^{\sqsubseteq}(F)\mathcal{P}\ .\ P \sqsubseteq P'\} \cap \{P \in \mathbb{L} \mid P \sqsupseteq \bigsqcap \varphi^{\sqsubseteq}(F)\mathcal{P}\} \hfill \wr\text{def. of } \alpha^{\sqsubseteq} \text{ and } \alpha^{\curlyvee}\wr \\
= & \{P \in \mathbb{L} \mid \exists P' \in \mathcal{P}\ .\ (F \sqsubseteq P' \wedge \forall P'' \in \mathbb{L}\ .\ F \sqsubseteq P'' \sqsubseteq P' \Rightarrow P'' \in \mathcal{P}) \wedge P \sqsubseteq P'\} \cap \{P \in \mathbb{L} \mid P \sqsupseteq \bigsqcap \varphi^{\sqsubseteq}(F)\mathcal{P}\} \\
& \hfill \wr\text{def. of } \varphi^{\sqsubseteq}\wr \\
= & \{P \in \mathbb{L} \mid \exists P' \in \mathcal{P}\ .\ (F \sqsubseteq P' \wedge \forall P'' \in \mathbb{L}\ .\ F \sqsubseteq P'' \sqsubseteq P' \Rightarrow P'' \in \mathcal{P}) \wedge P \sqsubseteq P' \wedge F \sqsubseteq P\} \wr\bigsqcap \varphi^{\sqsubseteq}(F)\mathcal{P} = F\wr
\end{array}$$

$= \{P \in \mathbb{L} \mid F \sqsubseteq P \wedge \forall P_1 \in \mathbb{L} \,.\, F \sqsubseteq P_1 \sqsubseteq P \Rightarrow P_1 \in \mathcal{P}\} = \varphi^{\sqsubseteq}(F)\mathcal{P}$

$\wr(\sqsupseteq)$ let $P' = P$, then $F \sqsubseteq P' \wedge \forall P'' \in \mathbb{L} \,.\, F \sqsubseteq P'' \sqsubseteq P' \Rightarrow P'' \in \mathcal{P}$ holds by replacing P'' with P_1;
$(\sqsubseteq)$ For any P_1 such that $F \sqsubseteq P_1 \sqsubseteq P$ holds, we have $F \sqsubseteq P \sqsubseteq P'$ for some P' so that $F \sqsubseteq P_1 \sqsubseteq P \sqsubseteq P'$ also holds, which implies that $P_1 \in \mathcal{P}$. By the premise, we have $\forall P'' \in \mathbb{L} \,.\, F \sqsubseteq P'' \sqsubseteq P' \Rightarrow P'' \in \mathcal{P}$, we are allowed to instantiate P'' to P_1 and have $P_1 \in \mathcal{P}\wr$ □

Lemma 22.9. *We can equivalently rewrite the rule in* (90) *and* (17) *by the following.*

$$\frac{\forall P \in \mathcal{P} \,.\, \underline{\{}P\underline{\}}\,\mathsf{S}\,\underline{\{}\sqcap \mathcal{Q}\underline{\}}}{\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\alpha^{\sqsupseteq}(\mathcal{Q})\,\overline{|\!\}}},\ \alpha^{\sqsubseteq}(\mathcal{Q}) \in \alpha^{\curlywedge}(\wp(\mathbb{L})) \qquad \frac{\forall P \in \mathcal{P} \,.\, \exists Q \in \mathcal{Q} \,.\, \overline{\{}P\overline{\}}\,\mathsf{S}\,\overline{\{}Q\overline{\}}}{\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\alpha^{\sqsubseteq}(\mathcal{Q})\,\overline{|\!\}}}$$

Proof of lemma 22.9. Let us prove the first one: by rule (90), it is sufficient to show that $\sqcap \mathcal{Q} = \sqcap \alpha^{\sqsupseteq}(\mathcal{Q})$. Since $\alpha^{\sqsupseteq}$ is extensive, then $\sqcap \mathcal{Q} \sqsupseteq \sqcap \alpha^{\sqsupseteq}(\mathcal{Q})$ holds trivially. For arbitrary P in $\alpha^{\sqsubseteq}(\mathcal{Q})$, there exists $Q \in \mathcal{Q}$ such that $Q \sqsubseteq P$ and then $\sqcap \mathcal{Q} \sqsubseteq P$. Thus $\sqcap \mathcal{Q}$ is a lower bound of $\alpha^{\sqsubseteq}(\mathcal{Q})$ and is smaller than the greatest lower bound of it. Now let us prove the second one:

$\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\alpha^{\sqsubseteq}(\mathcal{Q})\,\overline{|\!\}}$

$\Leftrightarrow$ $\mathsf{Post}[\![\mathsf{S}]\!]^{\sharp}(\mathcal{P}) \subseteq \alpha^{\sqsupseteq}(\mathcal{Q})$ $\wr$def. of $\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}\wr$

$\Leftrightarrow$ $\forall P \in \mathcal{P} \,.\, \mathsf{post}[\![\mathsf{S}]\!]^{\sharp}(P) \in \alpha^{\sqsupseteq}(\mathcal{Q})$ $\wr$def. of $\subseteq\wr$

$\Leftrightarrow$ $\forall P \in \mathcal{P} \,.\, \exists Q \in \mathcal{Q} \,.\, \mathsf{post}[\![\mathsf{S}]\!]^{\sharp}(P) \sqsubseteq Q$ $\wr$def. of $\alpha^{\sqsupseteq}\wr$

$\Leftrightarrow$ $\forall P \in \mathcal{P} \,.\, \exists Q \in \mathcal{Q} \,.\, \overline{\{}P\overline{\}}\,\mathsf{S}\,\overline{\{}Q\overline{\}}$ $\wr$def. of $\overline{\{}P\overline{\}}\,\mathsf{S}\,\overline{\{}Q\overline{\}}\wr$

□

Lemma 22.8 implies that we can simplify the proof rule (120) by further applying (114), and then Lemma 22.9, where its hypothesis is implied by 22.3. Since we have proved that all the intermediate rules are sound and complete, rule (??) is sound and complete for all postconditions $\mathcal{Q} \in \varrho^{\sqsubseteq\underline{F}}(\wp(\mathbb{L})$.

$$\frac{\exists \mathcal{X} \in \alpha^{\underline{F}}(\mathcal{Q}) \to \wp(\mathbb{L}^{\sharp}) \,.\, \mathcal{P} \subseteq \bigcup_{F \in \alpha^{\underline{F}}(\mathcal{Q})} \mathcal{X}_F \qquad \forall F \in \alpha^{\underline{F}}(\mathcal{Q}) \,.\, \dfrac{\dfrac{\forall P \in \mathcal{X}_F \,.\, \exists Q \in \varphi^{\sqsubseteq}(F)\mathcal{Q} \,.\, \overline{\{}P\overline{\}}\,\mathsf{S}\,\overline{\{}Q\overline{\}}}{\overline{\{\!|}\,\mathcal{X}_F\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\alpha^{\sqsubseteq} \circ \varphi^{\sqsubseteq}(F)\mathcal{Q}\,\overline{|\!\}}}(22.9) \quad \dfrac{\forall P \in \mathcal{X}_F \,.\, \underline{\{}P\underline{\}}\,\mathsf{S}\,\underline{\{}\sqcap \varphi^{\sqsubseteq}(F)\mathcal{Q}\underline{\}}}{\overline{\{\!|}\,\mathcal{X}_F\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\alpha^{\sqsupseteq} \circ \varphi^{\sqsubseteq}(F)\mathcal{Q}\,\overline{|\!\}}}(22.9)}{\overline{\{\!|}\,\mathcal{X}_F\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\varphi^{\sqsubseteq}(F)\mathcal{Q}\,\overline{|\!\}}}(114)}{\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{s}\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}}\ (120)$$

Removing the intermediate steps, the rule becomes

$$\frac{\exists \mathcal{X} \in \alpha^{\underline{F}}(\mathcal{Q}) \to \wp(\mathbb{L}^{\sharp}) \,.\, \mathcal{P} \subseteq \bigcup_{F \in \alpha^{\underline{F}}(\mathcal{Q})} \mathcal{X}_F \wedge (\forall F \in \alpha^{\underline{F}}(\mathcal{Q}) \,.\, \forall P \in \mathcal{X}_F \,.\, \exists Q \in \varphi^{\sqsubseteq}(F)\mathcal{Q} \,.\, \overline{\{}P\overline{\}}S\overline{\{}Q\overline{\}},\ \ \underline{\{}P\underline{\}}S\underline{\{}F\underline{\}})}{\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}}\ (??)$$

Example 22.10 (Proof reduction for frontier ϱ-elimination abstraction: bounded output). Consider the reachability without break and nontermination. Let the hyperproperties $\mathcal{P} \triangleq \{P \in \wp(\Sigma) \mid \exists \sigma_{max}, \sigma_{min} \in P \,.\, \forall \sigma \in P \,.\, \sigma_{min}(x) \le \sigma(x) \le \sigma_{max}(x)\}$, and $\mathcal{Q} \triangleq \{P \in \wp(\Sigma) \mid \exists \sigma_{max} \in P \,.\, \forall \sigma \in P \,.\, \sigma(x) \le \sigma_{max}(x)\}$, and we want to prove $\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}$ where $\mathsf{S} \triangleq$ `if(x>0) x=x else x=-x` using the rule (??). In this case $\alpha^{\underline{F}}(\mathcal{Q}) = \{\{\sigma\} \mid \sigma \in \Sigma\}$ is a set of singleton states. We let the partition variant $\mathcal{X}$ be

$$\begin{array}{rcl}
\mathcal{X} & \triangleq & \lambda\{\sigma\}\bullet\mathcal{X}_{\{\sigma\}}\cup\bar{\mathcal{X}}_{\{\sigma\}}\\
\text{where } \mathcal{X}_{\{\sigma\}} & \triangleq & \{P\in\wp(\Sigma)\mid \sigma\in P\wedge\forall\sigma'\in P\,.\,\sigma'(x)\leq\sigma(x)\wedge-\sigma'(x)\leq\sigma(x)\}\\
\text{and } \bar{\mathcal{X}}_{\{\sigma\}} & \triangleq & \{P\in\wp(\Sigma)\mid \bar{\sigma}\in P\wedge\forall\sigma'\in P\,.\,\sigma'(x)\leq\sigma(x)\wedge-\sigma'(x)\leq\sigma(x)\}
\end{array}$$

where $\bar{\sigma}$ is a shorthand for $\sigma[\mathtt{x}\leftarrow-\sigma(\mathtt{x})]$. Now let us prove the case of $\overline{\{\!|}\,\mathcal{X}_{\{\sigma\}}\,\overline{|\!\}}\ \mathtt{S}\ \overline{\{\!|}\,\varphi^{\sqsubseteq}(F)\mathcal{Q}\,\overline{|\!\}}$ for arbitrary σ, as the case for $\bar{\mathcal{X}}_{\{\sigma\}}$ is symmetrical and they can be combined by the consequence rules. Then the rule application proof steps are the following (for an arbitrary $P\in\mathcal{X}_{\{\sigma\}}$)

$$\cfrac{\text{let } Q=\{\sigma'\in\Sigma\mid\sigma'(x)\leq\sigma(x)\}\,.\ \cfrac{\cfrac{\text{by def of } Q}{\{\sigma\}\in Q}\quad\cfrac{\sigma''\in Q'\text{ implies }\sigma''\in Q}{\forall Q'\,.\,\{\sigma\}\subseteq Q'\subseteq Q\Rightarrow Q'\in\mathcal{X}_{\{\sigma\}}}}{Q\in\varphi^{\sqsubseteq}(F)\mathcal{Q}}\qquad\cfrac{\cfrac{\text{by def of } \mathcal{X}_{\sigma}\text{ and Q}}{\forall\sigma''\in P\,.\,\sigma''(x)\leq\sigma(\sigma)}}{\overline{\{}\,P\overline{\}}\ \mathtt{S}\ \overline{\{}Q\overline{\}}}}{\exists Q\in\varphi^{\sqsubseteq}(F)\mathcal{Q}\quad.\ \overline{\{}\,P\overline{\}}\ \mathtt{S}\ \overline{\{}Q\overline{\}}}$$

and

$$\cfrac{\cfrac{\text{by def of of } \mathcal{X}_{\sigma}\text{ where }\sigma'=\sigma}{\forall\sigma'\in F=\{\sigma\}\,.\,\sigma'\in\mathcal{X}_{\{\sigma\}}}}{\underline{\{}\,P\underline{\}}\ \mathtt{S}\ \underline{\{}F\underline{\}}}$$

Now it only remains to show that $\mathcal{P}\subseteq\bigcup\limits_{\sigma\in\Sigma}\mathcal{X}_{\{\sigma\}}\cup\bar{\mathcal{X}}_{\{\sigma\}}$. For arbitrary $P\in\mathcal{P}$, there exists σ_{min} and σ_{max} in P where $\sigma_{min}(x)\leq\sigma'(x)\sigma_{max}(x)$ for all σ' in P with two possible cases:

(1) $|\sigma_{min}(x)|\leq|\sigma_{max}(x)|$: then we know that P is in $\mathcal{X}_{\{\sigma_{max}\}}$ by definition.

(2) $|\sigma_{min}(x)|>|\sigma_{max}(x)|$: then $\sigma_{min}(x)$ must be negative and $\sigma_{max}(x)<-\sigma_{min}(x)$. In this case, P would be in $\bar{\mathcal{X}}_{\bar{\sigma}_{min}}$ because of the following: $\bar{\bar{\sigma}}=\sigma$ has implied that $\bar{\bar{\sigma}}\in P$. Moreover, for arbitrary σ' in P, $\sigma'(x)\leq\sigma_{max}(x)<-\sigma_{min}(x)=\bar{\sigma}_{min}(x)$, so as $-\sigma'(x)\leq\sigma_{min}(x)$ holds as $\sigma_{min}(x)$ is the lower bound. ■

23 Hierarchy of hyperproperties abstractions

To compare these abstractions, we first show that chain limit order ideal abstract properties have an equivalent frontier order ideal representation.

$$\langle\alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L})),\,\subseteq\rangle\ \underset{\overset{*}{\alpha}^{\sqsubseteq\uparrow}}{\overset{\mathbb{1}}{\leftrightarrows}}\ \langle\overset{*}{\alpha}^{\sqsubseteq\uparrow}(\wp(\mathbb{L})),\,\subseteq\rangle \tag{121}$$

Proof of (121). Let $\mathcal{P}\in\alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L}))$ so that there exists $\mathcal{P}'$ such that $\mathcal{P}=\alpha^{\sqsubseteq\overline{F}}(\mathcal{P}')$. Let us consider

$$\begin{array}{ll}
\multicolumn{2}{l}{\quad\alpha^{\sqsubseteq\uparrow}(\mathcal{P})}\\
= \alpha^{\sqsubseteq\uparrow}(\alpha^{\sqsubseteq\overline{F}}(\mathcal{P}')) & \wr\text{def. }\mathcal{P}=\alpha^{\sqsubseteq\overline{F}}(\mathcal{P}')\int\\
= \alpha^{\sqsubseteq}(\alpha^{\uparrow}(\alpha^{\sqsubseteq}(\alpha^{\overline{F}}(\mathcal{P}')))) & \wr\text{def. (100) of }\alpha^{\sqsubseteq\uparrow}\text{ and dual def. (93) of }\alpha^{\sqsubseteq\overline{F}}\text{ and composition }\circ\int\\
= \{P'\in\mathbb{L}\mid\exists P\in\alpha^{\uparrow}(\alpha^{\sqsubseteq}(\alpha^{\overline{F}}(\mathcal{P}')))\,.\,P'\sqsubseteq P\} & \wr\text{def. (91) of }\alpha^{\sqsubseteq}\int\\
= \{P'\in\mathbb{L}\mid\exists P\in\{\bigsqcup\limits_{i\in\mathbb{N}}P_i\mid\langle P_i,\,i\in\mathbb{N}\rangle\in\alpha^{\sqsubseteq}(\alpha^{\overline{F}}(\mathcal{P}'))\text{ is an increasing chain with existing lub}\}\,.\,P'\sqsubseteq P\} & \wr\text{dual def. (95) of }\alpha^{\uparrow}\int\\
= \{P'\in\mathbb{L}\mid\exists\text{ an increasing chain }\langle P_i,\,i\in\mathbb{N}\rangle\text{ with existing lub }.\ \forall i\in\mathbb{N}\,.\,P_i\in\alpha^{\sqsubseteq}(\alpha^{\overline{F}}(\mathcal{P}'))\wedge P'\sqsubseteq\bigsqcup\limits_{i\in\mathbb{N}}P_i\} & \wr\text{def. }\in\int\\
= \{P'\in\mathbb{L}\mid\exists\text{ an increasing chain }\langle P_i,\,i\in\mathbb{N}\rangle\text{ with existing lub }.\ \forall i\in\mathbb{N}\,.\,P_i\in\{P'\in\mathbb{L}\mid\exists P''\in\alpha^{\overline{F}}(\mathcal{P}')\,.\,P'\sqsubseteq P''\}\wedge P'\sqsubseteq\bigsqcup\limits_{i\in\mathbb{N}}P_i\} & \wr\text{def. (91) of }\alpha^{\sqsubseteq}\int
\end{array}$$

$= \{P' \in \mathbb{L} \mid \exists$ an increasing chain $\langle P_i,\ i \in \mathbb{N}\rangle$ with existing lub $.\ \forall i \in \mathbb{N}\ .\ \exists P'' \in \alpha^{\overline{F}}(\mathcal{P}')\ .\ P_i \sqsubseteq P'' \wedge P' \sqsubseteq \bigsqcup_{i\in\mathbb{N}} P_i\}$ ⟅def. ∈⟆

$= \{P' \in \mathbb{L} \mid \exists P'' \in \alpha^{\overline{F}}(\mathcal{P}')\ .\ P' \sqsubseteq P''\}$

⟅(⇒) $\forall i \in \mathbb{N}\ .\ P_i \sqsubseteq P''$ implies $\bigsqcup_{i\in\mathbb{N}} P_i \sqsubseteq P''$ by def. existing lub, so that $P' \sqsubseteq P''$ by transitivity;
(⇐) Conversely choose the constant hence increasing chain $\langle P',\ i \in \mathbb{N}\rangle$ with existing lub P' so that $\forall i \in \mathbb{N}\ .\ P_i = P \sqsubseteq P'' \wedge P' \sqsubseteq \bigsqcup_{i\in\mathbb{N}} P_i = P$⟆

$= \alpha^{\sqsubseteq}(\alpha^{\overline{F}}(\mathcal{P}'))$ ⟅def. (91) of $\alpha^{\sqsubseteq}$⟆

$= \mathcal{P}$ ⟅def. $\mathcal{P}$⟆

It follows by the fixpoint definition (100) of $\mathring{\alpha}^{*\sqsubseteq\uparrow}(\mathcal{P}) \triangleq \mathsf{lfp}^{\subseteq}\, \boldsymbol{\lambda} X \bullet \mathcal{P} \cup \alpha^{\sqsubseteq\uparrow}(X)$ that $\mathring{\alpha}^{*\sqsubseteq\uparrow}(\mathcal{P}) = \mathcal{P}$ so that the Galois retraction (121) follows immediately. □

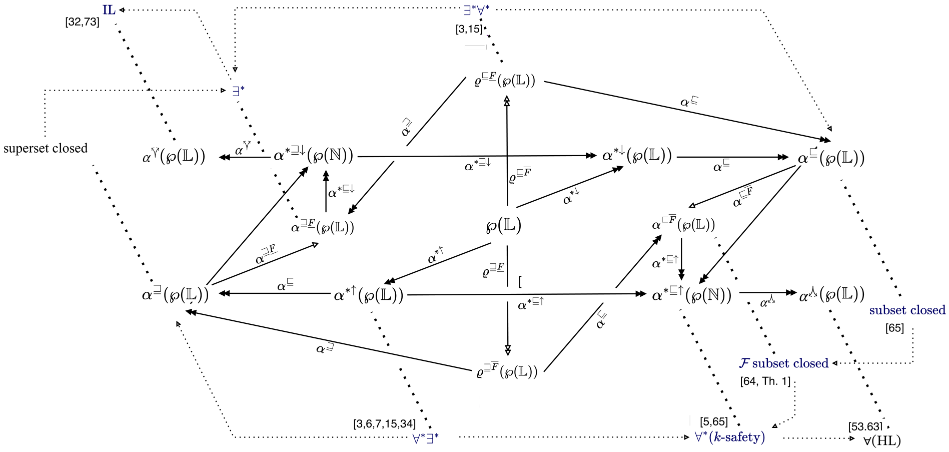

IL
[32,73]
∃*∀*
[3,15]
∃*
superset closed
$\varrho^{\sqsubseteq\underline{F}}(\wp(\mathbb{L}))$
$\alpha^{\sqsupseteq}$
$\alpha^{\sqsubseteq}$
$\alpha^{\curlyvee}(\wp(\mathbb{L}))$
$\alpha^{\curlyvee}$
$\alpha^{*\sqsupseteq\downarrow}(\wp(\mathbb{N}))$
$\alpha^{*\sqsupseteq\downarrow}$
$\alpha^{*\downarrow}(\wp(\mathbb{L}))$
$\alpha^{\sqsubseteq}$
$\alpha^{\sqsubseteq}(\wp(\mathbb{L}))$
$\varrho^{\sqsubseteq\overline{F}}$
$\alpha^{*\sqsubseteq\downarrow}$
$\alpha^{*\downarrow}$
$\alpha^{\sqsubseteq\overline{F}}$
$\alpha^{\sqsupseteq\underline{F}}(\wp(\mathbb{L}))$
$\wp(\mathbb{L})$
$\alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L}))$
$\alpha^{\sqsupseteq\underline{F}}$
$\alpha^{*\uparrow}$
$\alpha^{*\sqsubseteq\uparrow}$
$\varrho^{\sqsupseteq\underline{F}}$
[
$\alpha^{\sqsupseteq}(\wp(\mathbb{L}))$
$\alpha^{\sqsubseteq}$
$\alpha^{*\uparrow}(\wp(\mathbb{L}))$
$\alpha^{*\sqsubseteq\uparrow}(\wp(\mathbb{N}))$
$\alpha^{\curlywedge}$
$\alpha^{\curlywedge}(\wp(\mathbb{L}))$
subset closed
$\alpha^{*\sqsubseteq\uparrow}$
$\alpha^{\sqsubseteq}$
[65]
$\alpha^{\sqsupseteq}$
$\varrho^{\sqsupseteq\overline{F}}(\wp(\mathbb{L}))$
$\mathcal{F}$ subset closed
[64, Th. 1]
[3,6,7,15,34]
[5,65]
[53.63]
∀*∃*
∀*(k-safety)
∀(HL)

Fig. 1. The hierarchy of hyperproperties by abstraction. The arrow is interpreted as "more general than" where the double arrow represents Galois surjection. Dotted line indicated the hyperproperties subsumed by our abstract in the related works.

Figure 1 shows a lattice of hyperproperties derived by our abstractions as well as the related hyperproperties that they subsume.

Proof of figure.1. By (121), if $\mathcal{P} \in \mathring{\alpha}^{*\sqsubseteq\uparrow}(\wp(\mathbb{L}))$ then $\mathbb{1}(\mathcal{P}) = \mathcal{P} \in \alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L}))$ proving $\mathring{\alpha}^{*\sqsubseteq\uparrow}(\wp(\mathbb{L})) \subseteq \alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L}))$.

If $\mathcal{P} \in \alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L}))$ then $\exists \mathcal{Q} \in \wp(\mathbb{L})\ .\ \mathcal{P} = \alpha^{\sqsubseteq\overline{F}}(\mathcal{Q})$ so that, by idempotency in (91), $\alpha^{\sqsubseteq}(\alpha^{\sqsubseteq\overline{F}}(\mathcal{Q})) = \alpha^{\sqsubseteq\overline{F}}(\mathcal{Q}) = \mathcal{P}$, proving $\alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L})) \subseteq \alpha^{\sqsubseteq}(\wp(\mathbb{L}))$.

For arbitrary non-empty $\mathcal{P}$ in $\alpha^{\curlywedge}(\wp(\mathbb{L}))$ and consider then $\langle \alpha^{\curlywedge}(\wp(\mathbb{L})), \sqsubseteq\rangle$ is a sublattice which is complete, meaning that it is chain-closed. Thus, $\alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L}))(\mathcal{P}) = \mathcal{P}$, and so $\alpha^{\sqsubseteq\overline{F}}(\wp(\mathbb{L})) \subseteq \alpha^{\curlywedge}(\wp(\mathbb{L}))$

For arbitrary non-empty $\mathcal{P}$ in $\alpha^{\sqsupseteq\underline{F}}$, $\mathcal{P} = \bigcup_{F\in\alpha^{\underline{F}}(\mathcal{P})}\{P \in \mathbb{L}\ .\ F \sqsubseteq P\}$ by lemma 18.8, then for arbitrary P in $\mathcal{P}$, $F \sqsubseteq P$ for some F in $\alpha^{\underline{F}}(\mathcal{P})$. P would be in $\varphi^{\sqsubseteq}(F)\mathcal{P}$ as for all P' such that $F \sqsubseteq P' \sqsubseteq P$, $P' \in \{P' \in \mathbb{L} \mid F \sqsubseteq P'\}$ trivially. This implies that $\mathcal{P} \sqsubseteq \varrho^{\sqsubseteq\underline{F}}(\mathcal{P})$, meaning that $\mathcal{P} = \varrho^{\sqsubseteq\underline{F}}(\mathcal{P})$ as the inverse holds by the fact that $\varrho^{\sqsubseteq\underline{F}}$ is reducive. This proves that $\alpha^{\sqsupseteq\underline{F}}(\wp(\mathbb{L})) \subseteq \varrho^{\sqsubseteq\underline{F}}(\wp(\mathbb{L}))$.

For arbitrary non-empty $\mathcal{P}$ in $\alpha^{\sqsubseteq}(\wp(\mathbb{L}))$, $\alpha^{\underline{F}} = \{\bot\}$. Then $\varrho^{\sqsupseteq\underline{F}}(\mathcal{P}) = \varrho^{\sqsupseteq}(\mathcal{P}) = \mathcal{P}$. The last equation holds because $\varrho^{\sqsupseteq}$ is closure operator on $\alpha^{\sqsubseteq}(\wp(\mathbb{L}))$. This proves that $\alpha^{\subseteq}(\wp(\mathbb{L})) \sqsubseteq \varrho^{\sqsubseteq\underline{F}}(\wp(\mathbb{L}))$. □

24 Related Work

Algebraic semantics [45, 49, 58, 71] is rooted in the previous concept of program schemes [12, 37, 44, 46, 74]. The idea of handling logics algebraically using an abstract domain goes back to [28, section 5]. It requires a distinction between computational and logical orderings which first appeared in strictness analysis (using Scott partial order for computational ordering and inclusion for logical ordering [73]). It is not uncommon in abstract interpretation since then. The calculational methodology that we have used is based on [21]. Following the introduction of trace hyperproperties [14], most semantics [5, 66] and verification methods for semantic (hyper) properties have been on subclasses of hyperproperties [6–10, 13, 15, 29, 30, 67], further reviewed in extreme great detail in [30, section 6].

25 Conclusion and Future Work

Transformational (hyper) logics have traditionally been based on transformers themselves equivalent to an operational semantics. When considering nontermination, other semantics like denotational semantics are relevant, but the corresponding logics are in a separate world [1, 51].

In an attempt to design (hyper) logics valid for various (abstract) semantics, we have defined an algebraic semantics (which can be instantiated to operational, denotational, or relational semantics, and is also useful for deductive methods and static analysis).

We have designed, by calculus, a structural fixpoint collecting semantics post for execution properties (e.g. sets of execution traces), its hypercollecting semantics Post for semantic properties (e.g sets of sets of traces), and the various over or under approximation logics corresponding to these transformers for correctness and incorrectness (part III is for over approximation only, but the main reason to use the under approximation logic is to disprove over approximations which is expressible as $\neg\,\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}} \Leftrightarrow \exists\varnothing \subsetneq \mathcal{P}' \subseteq \mathcal{P}\,.\,\overline{\{\!|}\,\mathcal{P}'\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\neg\mathcal{Q}\,\overline{|\!\}}$).

Proof of $\neg\,\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}} \Leftrightarrow \exists\varnothing \subsetneq \mathcal{P}' \subseteq \mathcal{P}\,.\,\overline{\{\!|}\,\mathcal{P}'\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\neg\mathcal{Q}\,\overline{|\!\}}$.

$\neg\,\overline{\{\!|}\,\mathcal{P}\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\mathcal{Q}\,\overline{|\!\}}$

$\Leftrightarrow\ \neg(\mathsf{Post}^\sharp[\![\mathsf{S}]\!]^\sharp\mathcal{P} \subseteq \mathcal{Q})$ ⟅(62)⟆

$\Leftrightarrow\ \neg(\{\mathsf{post}^\sharp(S)P \mid P \in \mathcal{P}\} \subseteq \mathcal{Q})$ ⟅(40)⟆

$\Leftrightarrow\ \neg(\forall P \in \mathcal{P}\,.\,\mathsf{post}^\sharp(S)P \in \mathcal{Q})$ ⟅def. $\subseteq$⟆

$\Leftrightarrow\ \exists P \in \mathcal{P}\,.\,\mathsf{post}^\sharp(S)P \in \neg\mathcal{Q}$ ⟅def. negation⟆

$\Leftrightarrow\ \exists\varnothing \subsetneq \mathcal{P}' \subseteq \mathcal{P}\,.\,\{\mathsf{post}^\sharp(S)P' \mid P' \in \mathcal{P}'\} \subseteq \neg\mathcal{Q}$

⟅($\Rightarrow$) choose $\mathcal{P}' = \{P\}$ and def. $\subseteq$;
($\Leftarrow$) since $\varnothing \subsetneq \mathcal{P}' \subseteq \mathcal{P}$ there exists a $P \in \mathcal{P}'$ such that $P \in \mathcal{P}$ and $\{\mathsf{post}^\sharp(S)P' \mid P' \in \{P\}\} \subseteq \{\mathsf{post}^\sharp(S)P' \mid P' \in \mathcal{P}'\} \subseteq \neg\mathcal{Q}$ proving $\mathsf{post}^\sharp(S)P \in \neg\mathcal{Q}$. ⟆

$\Leftrightarrow\ \exists\varnothing \subsetneq \mathcal{P}' \subseteq \mathcal{P}\,.\,\mathsf{Post}^\sharp[\![\mathsf{S}]\!]^\sharp\mathcal{P}' \subseteq \mathcal{Q}$ ⟅(40)⟆

$\Leftrightarrow\ \exists\varnothing \subsetneq \mathcal{P}' \subseteq \mathcal{P}\,.\,\overline{\{\!|}\,\mathcal{P}'\,\overline{|\!\}}\,\mathsf{S}\,\overline{\{\!|}\,\neg\mathcal{Q}\,\overline{|\!\}}$ ⟅(62)⟆ □

Since, and contrary to classic logics, proofs of general semantic (hyper) properties relative to a program semantics requires the exact characterization of this semantics in the proof, an extreme complication, we have considered abstractions of the semantic properties for which this constraint can be relaxed. This has yielded to new sound and complete simplified proof rules, including for algebraic generalizations of forall-forall, forall-exists, and exists-forall semantic (hyper) properties.

The verification of semantic (hyper) properties is still in its infancy and far from reaching the simplicity observed in the verification of execution properties. Several compromises will be needed maybe by relaxing implication (e.g. using Egli-Milner order instead of inclusion), considering abstract properties (for classes of properties of practical interest), and possibly by preserving soundness but renouncing to completeness. However, in full generality, the sound and complete proof methods introduced in this paper, will ultimately be, up to equivalence, the only one applicable.

References

[1] Samson Abramsky. 1991. Domain Theory in Logical Form. *Ann. Pure Appl. Log.* 51, 1-2 (1991), 1–77. https://doi.org/10.1016/0168-0072(91)90065-T

[2] Peter Aczel. 1977. An Introduction to Inductive Definitions. In *Handbook of Mathematical Logic*, John Barwise (Ed.). North–Holland, Amsterdam, Chapter 7, 739–782.

[3] Timos Antonopoulos, Eric Koskinen, Ton Chanh Le, Ramana Nagasamudram, David A. Naumann, and Minh Ngo. 2023. An Algebra of Alignment for Relational Verification. *Proc. ACM Program. Lang.* 7, POPL (2023), 573–603. https://doi.org/10.1145/3571213

[4] Krzysztof R. Apt and Gordon D. Plotkin. 1986. Countable Nondeterminism and Random Assignment. *J. ACM* 33, 4 (1986), 724–767. https://doi.org/10.1145/6490.6494

[5] Mounir Assaf, David A. Naumann, Julien Signoles, Eric Totel, and Frédéric Tronel. 2017. Hypercollecting semantics and its application to static analysis of information flow. In *POPL*. ACM, 874–887. https://doi.org/10.1145/3009837.3009889

[6] Raven Beutner. 2024. Automated Software Verification of Hyperliveness. In *TACAS (2) (Lecture Notes in Computer Science, Vol. 14571)*. Springer, 196–216. https://doi.org/10.1007/978-3-031-57249-4_10

[7] Raven Beutner and Bernd Finkbeiner. 2022. Software Verification of Hyperproperties Beyond k-Safety. In *CAV (1) (Lecture Notes in Computer Science, Vol. 13371)*. Springer, 341–362. https://doi.org/10.1007/978-3-031-13185-1_17

[8] Raven Beutner and Bernd Finkbeiner. 2023. HyperATL*: A Logic for Hyperproperties in Multi-Agent Systems. *Log. Methods Comput. Sci.* 19, 2 (2023), 13:1–13:44. https://doi.org/10.46298/LMCS-19(2:13)2023

[9] Raven Beutner, Bernd Finkbeiner, Hadar Frenkel, and Niklas Metzger. 2023. Second-Order Hyperproperties. In *CAV (2) (Lecture Notes in Computer Science, Vol. 13965)*. Springer, 309–332. https://doi.org/10.1007/978-3-031-37703-7_15

[10] Raven Beutner, Bernd Finkbeiner, Hadar Frenkel, and Niklas Metzger. 2024. Monitoring Second-Order Hyperproperties. In *AAMAS*. International Foundation for Autonomous Agents and Multiagent Systems / ACM, 180–188. https://doi.org/10.5555/3635637.3662865

[11] Thomas S. Blyth. 2005. *Lattices and Ordered Algebraic Structures*. Springer. https://doi.org/10.1007/b139095

[12] Manfred Broy, Martin Wirsing, and Peter Pepper. 1987. On the Algebraic Definition of Programming Languages. *ACM Trans. Program. Lang. Syst.* 9, 1 (1987), 54–99. https://doi.org/10.1145/9758.10501

[13] Michael R. Clarkson, Bernd Finkbeiner, Masoud Koleini, Kristopher K. Micinski, Markus N. Rabe, and César Sánchez. 2014. Temporal Logics for Hyperproperties. In *POST (Lecture Notes in Computer Science, Vol. 8414)*. Springer, 265–284. https://doi.org/10.1007/978-3-642-54792-8_15

[14] Michael R. Clarkson and Fred B. Schneider. 2010. Hyperproperties. *J. Comput. Secur.* 18, 6 (2010), 1157–1210. https://doi.org/10.3233/JCS-2009-0393

[15] Norine Coenen, Bernd Finkbeiner, César Sánchez, and Leander Tentrup. 2019. Verifying Hyperliveness. In *CAV (1) (Lecture Notes in Computer Science, Vol. 11561)*. Springer, 121–139. https://doi.org/10.1007/978-3-030-25540-4_7

[16] Ellis S. Cohen. 1977. Information Transmission in Computational Systems. In *SOSP*. ACM, 133–139. https://doi.org/10.1145/800214.806556

[17] Bruno Courcelle and Maurice Nivat. 1978. The Algebraic Semantics of Recursive Program Schemes. In *Mathematical Foundations of Computer Science 1978, Proceedings, 7th Symposium, Zakopane, Poland, September 4-8, 1978 (Lecture Notes in Computer Science, Vol. 64)*, Józef Winkowski (Ed.). Springer, 16–30. https://doi.org/10.1007/3-540-08921-7_53

[18] Patrick Cousot. 2002. Constructive Design of a Hierarchy of Semantics of a Transition System by Abstract Interpretation. *Theor. Comput. Sci.* 277, 1–2 (2002), 47–103. https://doi.org/10.1016/S0304-3975(00)00313-3

[19] Patrick Cousot. 2019. On Fixpoint/Iteration/Variant Induction Principles for Proving Total Correctness of Programs with Denotational Semantics. In *LOPSTR (Lecture Notes in Computer Science, Vol. 12042)*. Springer, 3–18. https://doi.org/10.1007/978-3-030-45260-5_1

[20] Patrick Cousot. 2021. *Principles of Abstract Interpretation* (1 ed.). MIT Press.

[21] Patrick Cousot. 2024. Calculational Design of [In]Correctness Transformational Program Logics by Abstract Interpretation. *Proc. ACM Program. Lang.* 8, POPL (2024), 175–208. https://doi.org/10.1145/3632849

[22] Patrick Cousot. 2024. Full version of "Calculational Design of [In]Correctness Transformational Program Logics by Abstract Interpretation", Proc. ACM Program. Lang. 8, POPL (2024), 7:1–10:33, https://doi.org/10.1145/3632849. *Zenodo* (Dec. 2024), 66 pages. https://doi.org/10.5281/zenodo.10439108

[23] Patrick Cousot and Radhia Cousot. 1979. Constructive Versions of Tarski's Fixed Point Theorems. *Pacific J. of Math.* 82, 1 (1979), 43–57. https://doi.org/10.2140/pjm.1979.82.43

[24] Patrick Cousot and Radhia Cousot. 1992. Inductive Definitions, Semantics and Abstract Interpretation. In *POPL*. ACM Press, 83–94. https://doi.org/10.1145/143165.143184

[25] Patrick Cousot and Radhia Cousot. 1995. Compositional and Inductive Semantic Definitions in Fixpoint, Equational, Constraint, Closure-condition, Rule-based and Game-Theoretic Form. In *CAV (Lecture Notes in Computer Science, Vol. 939)*. Springer, 293–308. https://doi.org/10.1007/3-540-60045-0_58

[26] Patrick Cousot and Radhia Cousot. 2009. Bi-inductive structural semantics. *Inf. Comput.* 207, 2 (2009), 258–283. https://doi.org/10.1016/J.IC.2008.03.025

[27] Patrick Cousot and Radhia Cousot. 2012. An abstract interpretation framework for termination. In *POPL*. ACM, 245–258. https://doi.org/10.1145/2103656.2103687

[28] Patrick Cousot, Radhia Cousot, Francesco Logozzo, and Michael Barnett. 2012. An abstract interpretation framework for refactoring with application to extract methods with contracts. In *OOPSLA*. ACM, 213–232. https://doi.org/10.1145/2384616.2384633

[29] Thibault Dardinier. 2024. Formalization of Hyper Hoare Logic: A Logic to (Dis-)Prove Program Hyperproperties. Arch. Formal Proofs, 2023. https://www.isa-afp.org/entries/HyperHoareLogic.html

[30] Thibault Dardinier and Peter Müller. 2024. Hyper Hoare Logic: (Dis-)Proving Program Hyperproperties. *Proceedings of the ACM on Programming Languages (PACMPL)* 8, Issue PLDI, Article No.: 207 (June 2024), 1485–1509. https://doi.org/10.1145/3656437

[31] Brian A. Davey and Hilary A. Priestley. 2002. *Introduction to Lattices and Order, Second Edition.* Cambridge University Press. https://doi.org/10.1017/CBO9780511809088

[32] Edsko de Vries and Vasileios Koutavas. 2011. Reverse Hoare Logic. In *SEFM (Lecture Notes in Computer Science, Vol. 7041)*. Springer, 155–171. https://doi.org/10.1007/978-3-642-24690-6_12

[33] Jerry den Hartog and Erik P. de Vink. 2002. Verifying Probabilistic Programs Using a Hoare Like Logic. *Int. J. Found. Comput. Sci.* 13, 3 (2002), 315–340. https://doi.org/10.1142/S012905410200114X

[34] Klaus Denecke, Marcel Erné, and Shelly L. Wismath. 2003. *Galois Connections and Applications.* Kluwer Academic Publishers. https://doi.org/10.1007/978-1-4020-1898-5

[35] Robert Dickerson, Qianchuan Ye, Michael K. Zhang, and Benjamin Delaware. 2022. RHLE: Modular Deductive Verification of Relational ∀ ∃ Properties. In *APLAS (Lecture Notes in Computer Science, Vol. 13658)*. Springer, 67–87. https://doi.org/10.1007/978-3-031-21037-2_4

[36] Edsger W. Dijkstra. 1978. Program Inversion. In *Program Construction, International Summer School, July 26 - August 6, 1978, Marktoberdorf, Germany (Lecture Notes in Computer Science, Vol. 69)*, Friedrich L. Bauer and Manfred Broy (Eds.). Springer, 54–57. https://doi.org/10.1007/BFB0014657

[37] Andrei P. Ershov. 1979. Abstract computability on algebraic structures. In *Algorithms in Modern Mathematics and Computer Science (Lecture Notes in Computer Science, Vol. 122)*. Springer, 397–420. https://doi.org/10.1007/3-540-11157-3_38

[38] M. Escardó. 2003. Joins in the frame of nuclei. *Applied Categorical Structures* 11, 2 (April 2003), 117–124.

[39] Yuan Feng and Sanjiang Li. 2023. Abstract interpretation, Hoare logic, and incorrectness logic for quantum programs. *Inf. Comput.* 294 (2023), 105077. https://doi.org/10.1016/J.IC.2023.105077

[40] Bernd Finkbeiner and Christopher Hahn. 2016. Deciding Hyperproperties. In *CONCUR (LIPIcs, Vol. 59)*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 13:1–13:14. https://doi.org/10.4230/LIPICS.CONCUR.2016.13

[41] Roberto Giacobazzi and Isabella Mastroeni. 2005. Transforming semantics by abstract interpretation. *Theor. Comput. Sci.* 337, 1-3 (2005), 1–50. https://doi.org/10.1016/J.TCS.2004.12.021

[42] Roberto Giacobazzi and Isabella Mastroeni. 2018. Abstract Non-Interference: A Unifying Framework for Weakening Information-flow. *ACM Trans. Priv. Secur.* 21, 2 (2018), 9:1–9:31. https://doi.org/10.1145/3175660

[43] Roberto Giacobazzi, Isabella Mastroeni, and Elia Perantoni. 2024. Adversities in Abstract Interpretation - Accommodating Robustness by Abstract Interpretation. *ACM Trans. Program. Lang. Syst.* 46, 2 (2024), 5. https://doi.org/10.1145/3649309

[44] Joseph A. Goguen. 1974. On Homomorphisms, Correctness, Termination, Unfoldments, and Equivalence of Flow Diagram Programs. *J. Comput. Syst. Sci.* 8, 3 (1974), 333–365. https://doi.org/10.1016/S0022-0000(74)80028-0

[45] Joseph A. Goguen and Grant Malcolm. 1996. *Algebraic semantics of imperative programs.* MIT Press.

[46] Joseph A. Goguen and José Meseguer. 1977. Correctness of Recursive Flow Diagram Programs. In *MFCS (Lecture Notes in Computer Science, Vol. 53)*. Springer, 580–595. https://doi.org/10.1007/3-540-08353-7_183

[47] Joseph A. Goguen and José Meseguer. 1982. Security Policies and Security Models. In *S&P*. IEEE Computer Society, 11–20. https://doi.org/10.1109/SP.1982.10014

[48] Joseph A. Goguen and José Meseguer. 1984. Unwinding and Inference Control. In *S&P*. IEEE Computer Society, 75–87. https://doi.org/10.1109/SP.1984.10019

[49] Joseph A. Goguen, James W. Thatcher, Eric G. Wagner, and Jesse B. Wright. 1977. Initial Algebra Semantics and Continuous Algebras. *J. ACM* 24, 1 (1977), 68–95. https://doi.org/10.1145/321992.321997

[50] Irène Guessarian. 1978. Some Applications of Algebraic Semantics. In *Mathematical Foundations of Computer Science 1978, Proceedings, 7th Symposium, Zakopane, Poland, September 4-8, 1978 (Lecture Notes in Computer Science, Vol. 64)*, Józef Winkowski (Ed.). Springer, 257–266. https://doi.org/10.1007/3-540-08921-7_73

[51] Reinhold Heckmann. 1993. Power Domains and Second-Order Predicates. *Theor. Comput. Sci.* 111, 1&2 (1993), 59–88. https://doi.org/10.1016/0304-3975(93)90182-S

[52] Eric C. R. Hehner. 1990. A Practical Theory of Programming. *Sci. Comput. Program.* 14, 2-3 (1990), 133–158. https://doi.org/10.1016/0167-6423(90)90018-9

[53] Eric C. R. Hehner. 1993. *A Practical Theory of Programming.* Springer. https://doi.org/10.1007/978-1-4419-8596-5

[54] Eric C. R. Hehner. 1999. Specifications, Programs, and Total Correctness. *Sci. Comput. Program.* 34, 3 (1999), 191–205. https://doi.org/10.1016/S0167-6423(98)00027-6

[55] Charles Antony Richard Hoare. 1969. An Axiomatic Basis for Computer Programming. *Commun. ACM* 12, 10 (1969), 576–580. https://doi.org/10.1145/363235.363259

[56] C. A. R. Hoare, Ian J. Hayes, Jifeng He, Carroll Morgan, A. W. Roscoe, Jeff W. Sanders, Ib Holm Sørensen, J. Michael Spivey, and Bernard Sufrin. 1987. Laws of Programming. *Commun. ACM* 30, 8 (1987), 672–686. https://doi.org/10.1145/27651.27653

[57] Tony Hoare. 2013. Generic Models of the Laws of Programming. In *Theories of Programming and Formal Methods (Lecture Notes in Computer Science, Vol. 8051).* Springer, 213–226. https://doi.org/10.1007/978-3-642-39698-4_13

[58] Tony Hoare. 2014. Laws of Programming: The Algebraic Unification of Theories of Concurrency. In *CONCUR (Lecture Notes in Computer Science, Vol. 8704).* Springer, 1–6. https://doi.org/10.1007/978-3-662-44584-6_1

[59] Tony Hoare and Stephan van Staden. 2014. The laws of programming unify process calculi. *Sci. Comput. Program.* 85 (2014), 102–114. https://doi.org/10.1016/J.SCICO.2013.08.012

[60] Iu. I. Ianov and M. D. Friedman. 1958. On The Equivalence and Transformation of Program Schemes. *Commun. ACM* 1, 10 (1958), 8–12. https://doi.org/10.1145/368924.368930

[61] James C. King. 1976. Symbolic Execution and Program Testing. *Commun. ACM* 19, 7 (1976), 385–394. https://doi.org/10.1145/360248.360252

[62] Dexter Kozen. 1997. Kleene Algebra with Tests. *ACM Trans. Program. Lang. Syst.* 19, 3 (1997), 427–443. https://doi.org/10.1145/256167.256195

[63] Dexter Kozen. 2000. On Hoare logic and Kleene algebra with tests. *ACM Trans. Comput. Log.* 1, 1 (2000), 60–76. https://doi.org/10.1145/343369.343378

[64] Xavier Leroy and Hervé Grall. 2009. Coinductive big-step operational semantics. *Inf. Comput.* 207, 2 (2009), 284–304. https://doi.org/10.1016/J.IC.2007.12.004

[65] Zohar Manna and Amir Pnueli. 1974. Axiomatic Approach to Total Correctness of Programs. *Acta Inf.* 3 (1974), 243–263. https://doi.org/10.1007/BF00288637

[66] Isabella Mastroeni and Michele Pasqua. 2017. Hyperhierarchy of Semantics - A Formal Framework for Hyperproperties Verification. In *SAS (Lecture Notes in Computer Science, Vol. 10422).* Springer, 232–252. https://doi.org/10.1007/978-3-319-66706-5_12

[67] Isabella Mastroeni and Michele Pasqua. 2018. Verifying Bounded Subset-Closed Hyperproperties. In *SAS (Lecture Notes in Computer Science, Vol. 11002).* Springer, 263–283. https://doi.org/10.1007/978-3-319-99725-4_17

[68] Isabella Mastroeni and Michele Pasqua. 2023. Domain Precision in Galois Connection-Less Abstract Interpretation. In *Static Analysis - 30th International Symposium, SAS 2023, Cascais, Portugal, October 22-24, 2023, Proceedings (Lecture Notes in Computer Science, Vol. 14284)*, Manuel V. Hermenegildo and José F. Morales (Eds.). Springer, 434–459. https://doi.org/10.1007/978-3-031-44245-2_19

[69] Daryl McCullough. 1987. Specifications for Multi-Level Security and a Hook-Up Property. In *S&P.* IEEE Computer Society, 161–166. https://doi.org/10.1109/SP.1987.10009

[70] John McLean. 1996. A General Theory of Composition for a Class of ”Possibilistic” Properties. *IEEE Trans. Software Eng.* 22, 1 (1996), 53–67. https://doi.org/10.1109/32.481534

[71] Bernhard Möller, Peter W. O’Hearn, and Tony Hoare. 2021. On Algebra of Program Correctness and Incorrectness. In *RAMiCS (Lecture Notes in Computer Science, Vol. 13027).* Springer, 325–343. https://doi.org/10.1007/978-3-030-88701-8_20

[72] James Donald Monk. 1969. *Introduction to Set Theory.* McGraw–Hill. http://euclid.colorado.edu/~monkd/monk11.pdf

[73] Alan Mycroft. 1982. *Abstract interpretation and optimising transformations for applicative programs.* Ph. D. Dissertation. University of Edinburgh, UK. https://hdl.handle.net/1842/6602

[74] Maurice Nivat. 1980. Non Deterministic Programs: An Algebraic Overview. In *IFIP Congress.* North-Holland/IFIP, 17–28.

[75] Peter W. O'Hearn. 2020. Incorrectness logic. *Proc. ACM Program. Lang.* 4, POPL (2020), 10:1–10:32. https://doi.org/10.1145/3371078

[76] Oystein Ore. 1943. Combinations of Closure Relations. *Annals of Mathematics* 44, 3 (July 1943), 514–533. https://doi.org/10.2307/1968978

[77] David Michael Ritchie Park. 1969. Fixpoint Induction and Proofs of Program Properties. In *Machine Intelligence Volume 5*, Donald Mitchie and Bernard Meltzer (Eds.). Edinburgh Univ. Press, Chapter 3, 59–78.

[78] Gordon D. Plotkin. 1976. A Powerdomain Construction. *SIAM J. Comput.* 5, 3 (1976), 452–487. https://doi.org/10.1137/0205035

[79] Robert Rand and Steve Zdancewic. 2015. VPHL: A Verified Partial-Correctness Logic for Probabilistic Programs. In *The 31st Conference on the Mathematical Foundations of Programming Semantics, MFPS 2015, Nijmegen, The Netherlands, June 22-25, 2015 (Electronic Notes in Theoretical Computer Science, Vol. 319)*, Dan R. Ghica (Ed.). Elsevier, 351–367. https://doi.org/10.1016/J.ENTCS.2015.12.021

[80] Dana S. Scott and Christopher Strachey. 1971. *Towards a Mathematical Semantics for Computer Languages.* Technical Report PRG-6. Oxford University Computer Laboratory. 49 pages. https://www.cs.ox.ac.uk/files/3228/PRG06.pdf

[81] Alfred Tarski. 1955. A Lattice Theoretical Fixpoint Theorem and Its Applications. *Pacific J. of Math.* 5 (1955), 285–310. https://doi.org/10.2140/pjm.1955.5.285

[82] Lena Verscht and Benjamin Lucien Kaminski. 2023. Hoare-Like Triples and Kleene Algebras with Top and Tests: Towards a Holistic Perspective on Hoare Logic, Incorrectness Logic, and Beyond. *CoRR* abs/2312.09662 (2023), 4 pages. https://doi.org/10.48550/ARXIV.2312.09662

[83] Morgan Ward. 1942. The Closure Operators of a Lattice. *Annals of Mathematics* 43, 2 (April 1942), 191–196. https://doi.org/10.2307/1968865

[84] Peng Yan, Hanru Jiang, and Nengkun Yu. 2022. On incorrectness logic for Quantum programs. *Proc. ACM Program. Lang.* 6, OOPSLA1 (2022), 1–28. https://doi.org/10.1145/3527316

[85] Mingsheng Ying. 2011. Floyd-Hoare logic for quantum programs. *ACM Trans. Program. Lang. Syst.* 33, 6 (2011), 19:1–19:49. https://doi.org/10.1145/2049706.2049708

[86] Steve Zdancewic and Andrew C. Myers. 2003. Observational Determinism for Concurrent Program Security. In *CSFW*. IEEE Computer Society, 29. https://doi.org/10.1109/CSFW.2003.1212703