URL: http://www.elsevier.nl/locate/entcs/volume6.html 46 pages

Constructive Design of a Hierarchy of Semantics of a Transition System by Abstract Interpretation ⋆

Patrick Cousot

LIENS, DMI, École Normale Supérieure, 45 rue d'Ulm, 75230 Paris cedex 05, France, cousot@dmi.ens.fr, http://www.dmi.ens.fr/~cousot

Abstract

We construct a hierarchy of semantics by successive abstract interpretations. Starting from a maximal trace semantics of a transition system, we derive a big-step semantics, termination and nontermination semantics, natural, demoniac and angelic relational semantics and equivalent nondeterministic denotational semantics, D. Scott's deterministic denotational semantics, generalized/conservative/liberal predicate transformer semantics, generalized/total/partial correctness axiomatic semantics and corresponding proof methods. All semantics are presented in uniform fixpoint form and the correspondence between these semantics are established through composable Galois connection.

1 Introduction

The main idea of abstract interpretation is that program static analyzers effectively compute an approximation of the program semantics so that the specification of program analyzers should be formally derivable from the specification of the semantics [8]. The approximation process which is involved in this derivation has been formalized using Galois connections and/or widening narrowing operators [9]. The question of choosing which semantics one should start from in this calculation based development of the analyzer is not obvious: originally developed for small-step operational and predicate transformer semantics [11], the Galois connection based abstract interpretation theory was later extended to cope in the same way with denotational semantics [14]. In order to make the theory of abstract interpretation independent of the initial choice of the semantics we show in this paper that the specifications of these

⋆ Expanded version of an invited address presented at the Thirteenth Annual Conference on Mathematical Foundations of Programming Semantics (MFPS XIII, CMU, Pittsburgh, PA, USA, 24 March 1997) dedicated to Professor Dana S. Scott on the occasion of his 65th birthday year. This work was supported in part by ESPRIT ATLANTIQUE, HCM network ABILE and LTR project 8130 "LOMAPS".

semantics can themselves be developed by the same Galois connection based calculation process. It follows that the initial choice is no longer a burden, since the initial semantics can later be refined or abstracted exactly without calling into question the soundness (and may be the completeness) of the previous semantic abstractions.

2 Abstraction of Fixpoint Semantics

2.1 Fixpoint Semantics

A *fixpoint semantic specification* is a pair $\langle D, F\rangle$ where the *semantic domain* $\langle D, \sqsubseteq, \bot, \sqcup\rangle$ is a poset with partial order $\sqsubseteq$, infimum $\bot$ and partially defined least upper bound (lub) $\sqcup$ and the *semantic transformer* $F \in D \xmapsto{\mathrm{m}} D$ is a total monotone map from D to D assumed to be such that the transfinite *iterates of* F *from* $\bot$, that is $F^0 \triangleq \bot$, $F^{\delta+1} \triangleq F(F^\delta)$ for successor ordinals $\delta+1$ and $F^\lambda \triangleq \bigsqcup_{\delta<\lambda} F^\delta$ for limit ordinals λ are well-defined (e.g. when $\langle D, \sqsubseteq, \bot, \sqcup\rangle$ is a directed-complete partial order or DCPO [1]). By monotony, these iterates form an increasing chain, hence reach a fixpoint so that the *iteration order* can be defined as the least ordinal ϵ such that $F(F^\epsilon) = F^\epsilon$. This specifies the *fixpoint semantics* S as the $\sqsubseteq$-least fixpoint $S \triangleq \mathrm{lfp}^{\sqsubseteq} F = F^\epsilon$ of F. We prefer semantic specifications in fixpoint form which directly leads to proof methods using D. Park [32] or D. Scott [17] induction and to iterative program analysis algorithms by fixpoint approximation [9]. Other presentations, in particular in rule-based form, are equivalent [15].

2.2 Fixpoint Semantics Approximation

In abstract interpretation, the *concrete semantics* $S^\natural$ is approximated by a (usually computable) *abstract semantics* $S^\sharp$ via an abstraction function $\alpha \in D^\natural \longmapsto D^\sharp$ such that $\alpha(S^\natural) \sqsubseteq^\sharp S^\sharp$ [1]. The abstraction is *exact* if $\alpha(S^\natural) = S^\sharp$ and *approximate* if $\alpha(S^\natural) \sqsubset^\sharp S^\sharp$. To derive $S^\sharp$ from $S^\natural$ by abstraction or $S^\natural$ from $S^\sharp$ by refinement, we can use the following fixpoint approximation theorems (as usual, we call a function f *Scott-continuous*, written $f : D \xmapsto{\mathrm{c}} E$, if it is monotone and preserves the lub of any directed subset A of D [1]):

Theorem 2.1 (S. Kleene fixpoint approximation) *Let* $\langle\langle D^\natural, \sqsubseteq^\natural, \bot^\natural, \sqcup^\natural\rangle, F^\natural\rangle$ *and* $\langle\langle D^\sharp, \sqsubseteq^\sharp, \bot^\sharp, \sqcup^\sharp\rangle, F^\sharp\rangle$ *be concrete and abstract fixpoint semantic specifications. If the $\bot$-strict Scott-continuous abstraction function* $\alpha \in D^\natural \xmapsto{\bot, c} D^\sharp$ *is such that for all* $x \in D^\natural$ *such that* $x \sqsubseteq^\natural F^\natural(x)$ *there exists* $y \sqsubseteq^\natural x$ *such that* $\alpha(F^\natural(x)) \sqsubseteq^\sharp F^\sharp(\alpha(y))$ *then* $\alpha(\mathrm{lfp}^{\sqsubseteq^\natural} F^\natural) \sqsubseteq^\sharp \mathrm{lfp}^{\sqsubseteq^\sharp} F^\sharp$.

Proof. Let $F^{\natural\delta}$ and $F^{\sharp\delta}$, $\delta \in \mathbb{O}$ be the respective ordinal-termed $\sqsubseteq$-increasing ultimately stationary chains of transfinite iterates of $F^\natural$ and $F^\sharp$ [10]. We have $\alpha(F^{\natural 0}) = \alpha(\bot^\natural) = \bot^\sharp = F^{\sharp 0}$ by strictness of α and definition of the

[1] More generally, we look for an abstract semantics $S^\sharp$ such that $\alpha(S^\natural) \preceq^\sharp S^\sharp$ for the *approximation partial ordering* $\preceq^\sharp$ corresponding to logical implication which may differ from the *computational partial orderings* $\sqsubseteq$ used to define least fixpoints [14].

iterates. Assume $\alpha(F^{\natural\delta}) \sqsubseteq^\sharp F^{\sharp\delta}$ by induction hypothesis. We have $F^{\natural\delta} \sqsubseteq^\natural F^\natural(F^{\natural\delta}) = F^{\natural\delta+1}$ so that, by hypothesis, $\exists y \sqsubseteq^\natural F^{\natural\delta}$ such that $\alpha(F^{\natural\delta+1}) \sqsubseteq^\sharp F^\sharp(\alpha(y))$. By monotony of $F^\sharp$ and α, $F^\sharp(\alpha(y)) \sqsubseteq^\natural F^\sharp(\alpha(F^{\natural\delta}))$ whence by transitivity, induction hypothesis, monotony of $F^\sharp$ and definition of the iterates, $\alpha(F^{\natural\delta+1}) \sqsubseteq^\sharp F^\sharp(\alpha(F^{\natural\delta})) \sqsubseteq^\sharp F^\sharp(F^{\sharp\delta}) = F^{\sharp\delta+1}$. Given a limit ordinal λ, assume $\alpha(F^{\natural\delta}) \sqsubseteq^\sharp F^{\sharp\delta}$ for all $\delta < \lambda$. Then by definition of the iterates, continuity of α, induction hypothesis and definition of lubs, $\alpha(F^{\natural\lambda}) = \alpha(\bigsqcup^\natural_{\delta<\lambda} F^{\natural\delta}) = \bigsqcup^\sharp_{\delta<\lambda} \alpha(F^{\natural\delta}) \sqsubseteq^\sharp \bigsqcup^\sharp_{\delta<\lambda} F^{\sharp\delta} = F^{\sharp\lambda}$. By transfinite induction, we conclude $\forall\delta \in \mathbb{O} : \alpha(F^{\natural\delta}) \sqsubseteq^\sharp F^{\sharp\delta}$. Let ϵ and ϵ' be the iteration orders such that $F^{\natural\epsilon} = \mathrm{lfp}^{\sqsubseteq^\natural} F^\natural$ and $F^{\sharp\epsilon'} = \mathrm{lfp}^{\sqsubseteq^\sharp} F^\sharp$.

In particular $\alpha(\mathrm{lfp}^{\sqsubseteq^\natural} F^\natural) = \alpha(F^{\natural\epsilon}) = \alpha(F^{\natural\max\{\epsilon,\epsilon'\}}) \sqsubseteq^\sharp F^{\sharp\max\{\epsilon,\epsilon'\}} = F^{\sharp\epsilon'} = \mathrm{lfp}^{\sqsubseteq^\sharp} F^\sharp$. □

Theorem 2.2 (A. Tarski fixpoint approximation) *Let $\langle D^\natural, F^\natural\rangle$ and $\langle D^\sharp, F^\sharp\rangle$ be concrete and abstract fixpoint semantic specifications such that $\langle D^\natural, \sqsubseteq^\natural, \perp^\natural, \top^\natural, \sqcup^\natural, \sqcap^\natural\rangle$ and $\langle D^\sharp, \sqsubseteq^\sharp, \perp^\sharp, \top^\sharp, \sqcup^\sharp, \sqcap^\sharp\rangle$ are complete lattices. If the monotone abstraction function $\alpha \in D^\natural \stackrel{m}{\longmapsto} D^\sharp$ is such that for all $y \in D^\sharp$ such that $F^\sharp(y) \sqsubseteq^\sharp y$ there exists $x \in D^\natural$ such that $\alpha(x) \sqsubseteq^\sharp y$ and $F^\natural(x) \sqsubseteq^\natural x$ then $\alpha(\mathrm{lfp}^{\sqsubseteq^\natural} F^\natural) \sqsubseteq^\sharp \mathrm{lfp}^{\sqsubseteq^\sharp} F^\sharp$.*

Proof. By A. Tarski's fixpoint theorem [39], monotony of α, hypothesis and definition of greatest lower bounds (glb), we have $\alpha(\mathrm{lfp}^{\sqsubseteq^\natural} F^\natural) = \alpha(\sqcap^\natural\{x \mid F^\natural(x) \sqsubseteq^\natural x\}) \sqsubseteq^\sharp \sqcap^\sharp\{\alpha(x) \mid F^\natural(x) \sqsubseteq^\natural x\} \sqsubseteq^\sharp \sqcap^\sharp\{y \mid F^\sharp(y) \sqsubseteq^\sharp y\} = \mathrm{lfp}^{\sqsubseteq^\sharp} F^\sharp$. □

2.3 Fixpoint Semantics Transfer

When the abstraction must be exact, that is $\alpha(S^\natural) = S^\sharp$, we can use the following fixpoint transfer theorem, which provide guidelines for designing $S^\sharp$ from $S^\natural$ (or dually) in fixpoint form [11, theorem 7.1.0.4(3)], [16, lemma 4.3], [2, fact 2.3]:

Theorem 2.3 (S. Kleene fixpoint transfer) *Let $\langle D^\natural, F^\natural\rangle$ and $\langle D^\sharp, F^\sharp\rangle$ be concrete and abstract fixpoint semantic specifications. If the $\perp$-strict Scott-continuous abstraction function $\alpha \in D^\natural \stackrel{\perp,c}{\longmapsto} D^\sharp$ satisfies the* commutation condition *$F^\sharp \circ \alpha = \alpha \circ F^\natural$ then $\alpha(\mathrm{lfp}^{\sqsubseteq^\natural} F^\natural) = \mathrm{lfp}^{\sqsubseteq^\sharp} F^\sharp$. Moreover the respective iterates $F^{\natural\delta}$ and $F^{\sharp\delta}$, $\delta \in \mathbb{O}$ of $F^\natural$ and $F^\sharp$ from $\perp^\natural$ and $\perp^\sharp$ satisfy $\forall\delta \in \mathbb{O}$: $\alpha(F^{\natural\delta}) = F^{\sharp\delta}$ and the iteration order of $F^\sharp$ is less than or equal to that of $F^\natural$.*

Proof. Let $F^{\natural\delta}$ and $F^{\sharp\delta}$, $\delta \in \mathbb{O}$ be the respective ordinal-termed $\sqsubseteq$-increasing ultimately stationary chains of transfinite iterates of $F^\natural$ and $F^\sharp$. We have $\alpha(F^{\natural 0}) = \alpha(\perp^\natural) = \perp^\sharp = F^{\sharp 0}$ by strictness of α and definition of the iterates. Assume $\alpha(F^{\natural\delta}) = F^{\sharp\delta}$ by induction hypothesis. By definition of the iterates, commutation condition and induction hypothesis, we have $\alpha(F^{\natural\delta+1}) = \alpha(F^\natural(F^{\natural\delta})) = F^\sharp(\alpha(F^{\natural\delta})) = F^\sharp(F^{\sharp\delta}) = F^{\sharp\delta+1}$. Given a limit ordinal λ, assume $\alpha(F^{\natural\delta}) = F^{\sharp\delta}$ for all $\delta < \lambda$. Then by definition of the iterates, continuity of α and induction hypothesis, $\alpha(F^{\natural\lambda}) = \alpha(\bigsqcup^\natural_{\delta<\lambda} F^{\natural\delta}) = \bigsqcup^\sharp_{\delta<\lambda} \alpha(F^{\natural\delta}) = \bigsqcup^\sharp_{\delta<\lambda} F^{\sharp\delta} = F^{\sharp\lambda}$.

By transfinite induction, we conclude $\forall \delta \in \mathbb{O} : \alpha(F^{\natural\delta}) = F^{\sharp\delta}$. In particular $\alpha(\mathrm{lfp}^{\sqsubseteq^\natural} F^\natural) = \alpha(F^{\natural\epsilon}) = \alpha(F^{\natural\max\{\epsilon,\epsilon'\}}) = F^{\sharp\max\{\epsilon,\epsilon'\}} = F^{\sharp\epsilon'} = \mathrm{lfp}^{\sqsubseteq^\sharp} F^\sharp$ where ϵ and ϵ' are the respective iteration orders. $F^{\natural\epsilon}$ is a fixpoint of $F^\natural$ so that by the correspondence between iterates and the commutation condition, we have $F^\sharp(F^{\sharp\epsilon}) = F^\sharp(\alpha(F^{\natural\epsilon})) = \alpha(F^\natural(F^{\natural\epsilon})) = \alpha(F^{\natural\epsilon}) = F^{\sharp\epsilon}$ proving that $\epsilon' \leq \epsilon$. □

Observe that in theorem 2.3 (as well as in theorem 2.1), Scott-continuity of the abstraction function α is a too strong hypothesis since we only use the fact that α preserves the lub of the iterates of $F^\natural$ starting from $\bot^\natural$. When this is not the case, but α preserves glbs, we can use:

Theorem 2.4 (A. Tarski fixpoint transfer) *Let* $\langle D^\natural, F^\natural\rangle$ *and* $\langle D^\sharp, F^\sharp\rangle$ *be concrete and abstract fixpoint semantic specifications such that* $\langle D^\natural, \sqsubseteq^\natural, \bot^\natural, \top^\natural, \sqcup^\natural, \sqcap^\natural\rangle$ *and* $\langle D^\sharp, \sqsubseteq^\sharp, \bot^\sharp, \top^\sharp, \sqcup^\sharp, \sqcap^\sharp\rangle$ *are complete lattices. If the abstraction function* $\alpha \in D^\natural \overset{\sqcap}{\longmapsto} D^\sharp$ *is a complete* $\sqcap$*-morphism satisfying the* commutation inequality $F^\sharp \circ \alpha \sqsubseteq^\sharp \alpha \circ F^\natural$ *and the* post-fixpoint correspondence $\forall y \in D^\sharp : F^\sharp(y) \sqsubseteq^\sharp y \Longrightarrow \exists x \in D^\natural : \alpha(x) = y \wedge F^\natural(x) \sqsubseteq^\natural x$ *then* $\alpha(\mathrm{lfp}^{\sqsubseteq^\natural} F^\natural) = \mathrm{lfp}^{\sqsubseteq^\sharp} F^\sharp$.

Proof. If $F^\sharp(x) \sqsubseteq^\natural x$ then $\alpha \circ F^\sharp(x) \sqsubseteq^\natural \alpha(x)$ since α is monotone whence $F^\sharp \circ \alpha(x) \sqsubseteq^\natural \alpha(x)$ by the commutation inequality. Together with the post-fixpoint correspondence, this implies $\{\alpha(x) \mid F^\natural(x) \sqsubseteq^\natural x\} = \{y \mid F^\sharp(y) \sqsubseteq^\sharp y\}$. By A. Tarski's fixpoint theorem [39] and meet preservation, it follows that $\alpha(\mathrm{lfp}^{\sqsubseteq^\natural} F^\natural) = \alpha(\sqcap^\natural\{x \mid F^\natural(x) \sqsubseteq^\natural x\}) = \sqcap^\sharp\{\alpha(x) \mid F^\natural(x) \sqsubseteq^\natural x\} = \sqcap^\sharp\{y \mid F^\sharp(y) \sqsubseteq^\sharp y\} = \mathrm{lfp}^{\sqsubseteq^\sharp} F^\sharp$. □

2.4 Semantics Abstraction

An important particular case of abstraction function $\alpha \in D^\natural \longmapsto D^\sharp$ is when α preserves existing lubs $\alpha(\underset{i\in\Delta}{\sqcup^\natural} x_i) = \underset{i\in\Delta}{\sqcup^\sharp} \alpha(x_i)$. In this case there exists a unique map $\gamma \in D^\sharp \longmapsto D^\natural$ (so-called the *concretization function* [9]) such that the pair $\langle\alpha, \gamma\rangle$ is a *Galois connection*, written:

$$\langle D^\natural, \sqsubseteq^\natural\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle D^\sharp, \sqsubseteq^\sharp\rangle ,$$

which means that $\langle D^\natural, \sqsubseteq^\natural\rangle$ and $\langle D^\sharp, \sqsubseteq^\sharp\rangle$ are posets, $\alpha \in D^\natural \longmapsto D^\sharp$, $\gamma \in D^\sharp \longmapsto D^\natural$, and $\forall x \in D^\natural : \forall y \in D^\sharp : \alpha(x) \sqsubseteq^\sharp y \Longleftrightarrow x \sqsubseteq^\natural \gamma(y)$. If α is surjective (resp. injective, bijective) then we have a *Galois insertion* written $\underset{\alpha}{\overset{\gamma}{\substack{\longleftarrow \\ \twoheadrightarrow}}}$ (resp. *embedding* [2] written $\underset{\alpha}{\overset{\gamma}{\substack{\twoheadleftarrow \\ \longrightarrow}}}$, *bijection* written $\underset{\alpha}{\overset{\gamma}{\substack{\twoheadleftarrow \\ \twoheadrightarrow}}}$). The use of Galois connections in abstract interpretation was motivated by the fact that $\alpha(x)$ is the best possible approximation of $x \in D^\natural$ within $D^\sharp$ [9,11].

Example 2.5 (Subset abstraction) If $D^\natural$ is a set and $D^\sharp \subseteq D^\natural$ then $\langle\wp(D^\natural), \subseteq\rangle \underset{\alpha}{\overset{\gamma}{\substack{\longleftarrow \\ \twoheadrightarrow}}} \langle\wp(D^\sharp), \subseteq\rangle$ where $\alpha(X) \triangleq X \cap D^\sharp$ and $\gamma(Y) \triangleq X \cup \neg D^\sharp$ (where the *complement* of $\mathcal{E} \subseteq \mathcal{D}$ is $\neg\mathcal{E} \triangleq \{x \in \mathcal{D} \mid x \notin \mathcal{E}\}$). □

[2] If α and γ are Scott-continuous then this is an embedding-projection pair.

Example 2.6 (Elementwise set abstraction) If $\texttt{@} \in D^\natural \longmapsto D^\sharp$, the abstraction function $\alpha \in \wp(D^\natural) \longmapsto \wp(D^\sharp)$ is defined by $\alpha(X) \triangleq \{\texttt{@}(x) \mid x \in X\}$ and the concretization function $\gamma \in \wp(D^\sharp) \longmapsto \wp(D^\natural)$ is defined by $\gamma(Y) \triangleq \{x \mid \texttt{@}(x) \in Y\}$ then $\langle \wp(D^\natural),\ \subseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \wp(D^\natural),\ \subseteq\rangle$. Moreover, if $\texttt{@}$ is surjective then so is α. □

We often use the fact that Galois connections compose[3]. If $\langle D^\flat,\ \sqsubseteq^\flat\rangle \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \langle D^\natural,\ \sqsubseteq^\natural\rangle$ and $\langle D^\natural,\ \sqsubseteq^\natural\rangle \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \langle D^\sharp,\ \sqsubseteq^\sharp\rangle$ then $\langle D^\flat,\ \sqsubseteq^\flat\rangle \underset{\alpha_2 \circ \alpha_1}{\overset{\gamma_1 \circ \gamma_2}{\leftrightarrows}} \langle D^\sharp,\ \sqsubseteq^\sharp\rangle$.

Example 2.7 (Elementwise subset abstraction) If $\mathcal{S} \subseteq D^\natural$ and $\texttt{@} \in \mathcal{S} \longmapsto D^\sharp$ then by composition of examples 2.5 and 2.6, we get $\langle \wp(D^\natural),\ \subseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \wp(D^\natural),\ \subseteq\rangle$ where $\alpha(X) \triangleq \{\texttt{@}(x) \mid x \in X \cap \mathcal{S}\}$ and $\gamma \triangleq \{x \mid \texttt{@}(x) \in Y\} \cup \neg\mathcal{S}$. □

Finally, to reason by duality, observe that the dual of $\langle D^\natural,\ \sqsubseteq^\natural\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle D^\sharp,\ \sqsubseteq^\sharp\rangle$ is $\langle D^\sharp,\ \sqsupseteq^\sharp\rangle \underset{\gamma}{\overset{\alpha}{\leftrightarrows}} \langle D^\natural,\ \sqsupseteq^\natural\rangle$.

2.5 Fixpoint Semantics Fusion

The joint of two disjoint powerset fixpoint semantics can be expressed in fixpoint form, trivially as follows:

Theorem 2.8 (Fixpoint fusion) *Let D^+, D^ω be a partition of D^∞ and $\langle \wp(D^+),\ F^+\rangle$ and $\langle \wp(D^{\omega)},\ F^\omega\rangle$ be fixpoint semantic specifications. Partially define:*

$$\begin{array}{rlrl}
X^+ & \triangleq X \cap D^+, & \bot^\infty & \triangleq \bot^+ \cup \bot^\omega, \\
X^\omega & \triangleq X \cap D^\omega, & \top^\infty & \triangleq \top^+ \cup \top^\omega, \\
F^\infty(X) & \triangleq F^+(X^+) \cup F^\omega(X^\omega), & \displaystyle\bigsqcup_{i\in\Delta}^\infty X_i & \triangleq \displaystyle\bigsqcup_{i\in\Delta}^+ X^+ \cup \bigsqcup_{i\in\Delta}^\omega X_i{}^\omega, \\
X \sqsubseteq^\infty Y & \triangleq X^+ \sqsubseteq^+ Y^+ \wedge X^\omega \sqsubseteq^\omega Y^\omega, & \displaystyle\bigsqcap_{i\in\Delta}^\infty X_i & \triangleq \displaystyle\bigsqcap_{i\in\Delta}^+ X^+ \cup \bigsqcap_{i\in\Delta}^\omega X_i{}^\omega \ .
\end{array}$$

If $\langle \wp(D^+),\ \sqsubseteq^+\rangle$ and $\langle \wp(D^\omega),\ \sqsubseteq^\omega\rangle$ are posets (respectively DCPOs, complete lattices) then so is $\langle \wp(D^\infty),\ \sqsubseteq^\infty\rangle$. If F^+ and F^ω are monotone (resp. Scott-continuous, a complete $\sqcup$-morphism) then so is F^∞. In all cases, $\mathrm{lfp}^{\sqsubseteq^\infty} F^\infty = \mathrm{lfp}^{\sqsubseteq^+} F^+ \cup \mathrm{lfp}^{\sqsubseteq^\omega} F^\omega$.

2.6 Fixpoint Iterates Reordering

For some fixpoint semantic specifications $\langle D,\ F\rangle$ the fixpoint semantics $S \triangleq \mathrm{lfp}^{\sqsubseteq} F = \mathrm{lfp}^{\preceq} F$ can be characterized using several different orderings $\sqsubseteq$, $\preceq$, etc. on the semantic domain D, in which case the iterates are the same but just ordered differently:

[3] contrary to Galois's original definition corresponding to the semi-dual $\langle D^\natural, \sqsubseteq^\natural\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle D^\sharp, \sqsupseteq^\sharp\rangle$.

Theorem 2.9 (Fixpoint iterates reordering) *Let $\langle\langle D, \sqsubseteq, \perp, \sqcup\rangle, F\rangle$ be a fixpoint semantic specification (the iterates of F, i.e. $F^0 \triangleq \perp$, $F^{\delta+1} \triangleq F(F^\delta)$ for successor ordinals $\delta+1$ and $F^\lambda \triangleq \bigsqcup\limits_{\delta<\lambda} F^\delta$ for limit ordinals λ, being well-defined). Let E be a set and $\preceq$ be a binary relation on E, such that:*

(i) *$\preceq$ is a pre-order on E;*
(ii) *all iterates F^δ, $\delta \in \mathbb{O}$ of F belong to E;*
(iii) *$\perp$ is the $\preceq$-infimum of E;*
(iv) *the restriction $F|_E$ of F to E is $\preceq$-monotone;*
(v) *for all $x \in E$, if λ is a limit ordinal and $\forall \delta < \lambda : F^\delta \preceq x$ then $\bigsqcup\limits_{\delta<\lambda} F^\delta \preceq x$.*

Then $\mathrm{lfp}_\perp^{\sqsubseteq} F = \mathrm{lfp}_\perp^{\preceq} F|_E \in E$.

Proof. Let ϵ be the order of the iterates of F. By (ii), $F^\epsilon \in E$ whence $F|_E(F^\epsilon) = F(F^\epsilon) = F^\epsilon$ is a fixpoint of $F|_E$.

Let $x \in E$ be another fixpoint of $F|_E$. By (ii) and (iii), $F^0 = \perp \preceq x$. If $F^\delta \preceq x$ by induction hypothesis then by (ii) and (iv), $F^{\delta+1} = F(F^\delta) = F|_E(F^\delta) \preceq F|_E(x) = x$. By induction hypothesis and (v), $F^\lambda \preceq x$ for limit ordinals λ. By transfinite induction, $\forall \delta \in \mathbb{O} : F^\delta \preceq x$ so $\mathrm{lfp}_\perp^{\sqsubseteq} F = F^\epsilon \preceq x$. □

3 Transition/Small-Step Operational Semantics

The transition/small-step operational semantics of a programming language associates a *discrete transition system* to each program of the language that is a pair $\langle\Sigma, \tau\rangle$ where Σ is a (non-empty) set of states [4], $\tau \subseteq \Sigma \times \Sigma$ is the binary transition relation between a state and its possible successors. We write $s \; \tau \; s'$ or $\tau(s, s')$ for $\langle s, s'\rangle \in \tau$ using the isomorphism $\wp(\Sigma \times \Sigma) \simeq (\Sigma \times \Sigma) \longmapsto \mathbb{B}$ where $\mathbb{B} \triangleq \{\mathrm{tt}, \mathrm{ff}\}$ is the set of booleans. $\check{\tau} \triangleq \{s \in \Sigma \mid \forall s' \in \Sigma : \neg(s \; \tau \; s')\}$ is the set of *final/blocking states.*

4 Finite and Infinite Sequences

Computations are modeled using traces that is maximal finite and infinite sequences of states such that two consecutive states in a sequence are in the transition relation.

4.1 Sequences

Let A be a non-empty alphabet. $A^{\vec{0}} \triangleq \{\vec{\epsilon}\}$ where $\vec{\epsilon}$ is the empty sequence. When $n > 0$, $A^{\vec{n}} \triangleq [0, n-1] \longmapsto A$ is the set of finite sequences $\sigma = \sigma_0 \ldots \sigma_{n-1}$ of length $|\sigma| \triangleq n \in \mathbb{N}$ over alphabet A. $A^{\vec{+}} \triangleq \bigcup\limits_{n>0} A^{\vec{n}}$ is the set of non-empty finite sequences over A. The finite sequences are $A^{\vec{*}} \triangleq A^{\vec{+}} \cup A^{\vec{0}}$ while the infinite ones $\sigma = \sigma_0 \ldots \sigma_n \ldots$ are $A^{\vec{\omega}} \triangleq \mathbb{N} \longmapsto A$. The length of an

[4] We could also consider actions as in process algebra [28].

infinite sequence $\sigma \in A^{\vec{\omega}}$ is $|\sigma| \triangleq \omega$. The sequences are $A^{\vec{\propto}} \triangleq A^{\vec{*}} \cup A^{\vec{\omega}}$ while the non-empty ones are $A^{\vec{\infty}} \triangleq A^{\vec{+}} \cup A^{\vec{\omega}}$.

4.2 Concatenation of Sequences

The *concatenation* $\sigma = \eta \cdot \xi$ of sequences $\eta, \xi \in A^{\vec{\propto}}$ has length $|\sigma| = |\eta| \oplus |\xi|$ (where $\ell_1 \oplus \ell_2 = \ell_1 + \ell_2$ when $\ell_1, \ell_2 \in \mathbb{N}$, $\omega \oplus \ell = \ell \oplus \omega = \omega$ when $\ell \in \mathbb{N} \cup \{\omega\}$) and is such that $\sigma_\ell = \eta_\ell$ when $\ell < |\eta|$ while $\sigma_\ell = \xi_{\ell - |\eta|}$ if $|\eta| \leq \ell < |\sigma|$. Thus if $\eta, \xi \in A^{\vec{*}}$, $\eta \cdot \xi$ is the ordinary concatenation. For all $\eta \in A^{\vec{\omega}}$, $\xi \in A^{\vec{\propto}}$, one has $\eta \cdot \xi = \eta$. For all $\eta \in A^{\vec{\propto}}$, $\vec{\epsilon} \cdot \eta = \eta \cdot \vec{\epsilon} = \eta$. The concatenation extends to sets of sequences A and $B \in \wp(A^{\vec{\propto}})$ by $A \cdot B \triangleq \{\eta \cdot \xi \mid \eta \in A \wedge \xi \in B\}$.

4.3 Junction of Sequences

Non-empty finite sequences $\eta \in A^{\vec{\ell}}$ and $\xi \in A^{\vec{m}}$ are *joinable*, written $\eta \mathrel{\bar{?}} \xi$, iff $\eta_{\ell-1} = \xi_0$. Their *join* is then $\sigma = \eta \frown \xi \in A^{\overrightarrow{\ell+m-1}}$ such that $\sigma_n = \eta_n$ when $0 \leq n < \ell$ and $\sigma_{\ell-1+n} = \xi_n$ when $0 \leq n \leq m - 1$.

Non-empty infinitary sequences $\eta \in A^{\vec{\infty}}$ of length $|\eta| = \ell$ and $\xi \in A^{\vec{\infty}}$ of length $|\xi| = m$ ($\ell, m \in \mathbb{N} \cup \{\omega\}$) are *joinable*, written $\eta \mathrel{\bar{?}} \xi$, iff $\ell = \omega$ or $\ell \in \mathbb{N}$, in which case $\eta_{\ell-1} = \xi_0$. The length of their join $\sigma = \eta \frown \xi \in A^{\vec{\infty}}$ is then $|\sigma| = \ell \oplus m \ominus 1$ (where $\ell_1 \ominus \ell_2 = \ell_1 - \ell_2$ when $\ell_1, \ell_2 \in \mathbb{N}$ and $\omega - 1 = \omega$). Their join $\sigma = \eta \frown \xi$ satisfies $\sigma_n = \eta_n$ when $0 \leq n < \ell$ while $\sigma_{\ell-1+n} = \xi_n$ when $\ell < \omega \wedge 0 \leq n < m \ominus 1$. In particular, $\eta \frown \xi = \eta$ when $\eta \in A^{\vec{\omega}}$ is infinite.

The junction of sets A and $B \in \wp(A^{\vec{\infty}})$ of non-empty sequences is $A \frown B \triangleq \{\eta \frown \xi \mid \eta \in A \wedge \xi \in B \wedge \eta \mathrel{\bar{?}} \xi\}$. Observe that $A \frown (\bigcup_{i \in \Delta} B_i) = \bigcup_{i \in \Delta} (A \frown B_i)$ and $(\bigcup_{i \in \Delta} A_i) \frown B = \bigcup_{i \in \Delta} (A_i \frown B)$ but set of sequences junction is not Scott-co-continuous on $\wp(A^{\vec{\infty}})$. A counter example on the alphabet $A = \{a\}$ uses $X = \{a^\omega\}$ and the $\subseteq$-decreasing chain $Y_n = \{a^\ell \mid \ell \in \mathbb{N} \wedge \ell > n\}$, $n \in \mathbb{N}$ such that $X \frown (\bigcap_{n \in \mathbb{N}} Y_n) = \emptyset$ and $(\bigcap_{n \in \mathbb{N}} X \frown Y_n) = \{a^\omega\}$.

5 Maximal Trace Semantics

The *maximal trace semantics* $\tau^{\vec{\infty}}$ of the transition system $\langle \Sigma,\, \tau \rangle$ is the join $\tau^{\vec{\infty}} \triangleq \tau^{\vec{+}} \cup \tau^{\vec{\omega}}$ of the *infinite traces* $\tau^{\vec{\omega}} \triangleq \{\sigma \in \Sigma^{\vec{\omega}} \mid \forall i \in \mathbb{N} : \sigma_i \; \tau \; \sigma_{i+1}\}$ and the *maximal finite traces* $\tau^{\vec{+}} \triangleq \bigcup_{n > 0} \tau^{\vec{n}}$ including all sets $\tau^{\vec{n}} \triangleq \{\sigma \in \tau^{\dot{\vec{n}}} \mid \sigma_{n-1} \in \check{\tau}\}$ of traces of length n terminating with a final/blocking state in $\check{\tau} \triangleq \{s \in \Sigma \mid \forall s' \in \Sigma : \neg(s \; \tau \; s')\}$ where $\tau^{\dot{\vec{n}}} \triangleq \{\sigma \in \Sigma^{\vec{n}} \mid \forall i < n - 1 : \sigma_i \; \tau \; \sigma_{i+1}\}$ is the set of *partial execution traces* of length n.

5.1 Fixpoint Finite Trace Semantics

The *finite trace semantics* $\tau^{\vec{+}}$ can be presented in unique fixpoint form as follows [13, example 17] ($\mathrm{lfp}_a^{\sqsubseteq}$ is the $\sqsubseteq$-least fixpoint of F greater than or equal to a, if it exists and dually, $\mathrm{gfp}_a^{\sqsubseteq} \triangleq \mathrm{lfp}_a^{\sqsupseteq}$ is the $\sqsubseteq$-greatest fixpoint of F less than or equal to a, if it exists):

Theorem 5.1 (Fixpoint finite trace semantics) $\tau^{\vec{+}} = \operatorname{lfp}^{\subseteq}_{\emptyset} F^{\vec{+}} = \operatorname{gfp}^{\subseteq}_{\Sigma^{\vec{+}}} F^{\vec{+}}$ *where* $F^{\vec{+}} \in \wp(\Sigma^{\vec{+}}) \xmapsto{\cup} \wp(\Sigma^{\vec{+}})$ *defined as* $F^{\vec{+}}(X) \triangleq \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X$ *is a complete* $\cup$- *and* $\cap$-*morphism on the complete lattice* $\langle \wp(\Sigma^{\vec{+}}),\ \subseteq,\ \emptyset,\ \Sigma^{\vec{+}},\ \cup,\ \cap \rangle$.

Proof. The first iterates of $F^{\vec{+}}$ for $\operatorname{lfp}^{\subseteq}_{\emptyset} F^{\vec{+}}$ are $X^0 = \emptyset$, $X^1 = F^{\vec{+}}(X^0) = \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown \emptyset = \tau^{\vec{1}} \cup \emptyset = \tau^{\vec{1}}$, $X^2 = F^{\vec{+}}(X^1) = \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown \tau^{\vec{1}} = \tau^{\vec{1}} \cup \tau^{\vec{2}}$, etc. By recurrence, the n-th iterate is $X^n = \bigcup_{i=1}^{n} \tau^{\vec{i}}$ since $X^{n+1} = F^{\vec{+}}(X^n) = \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown (\bigcup_{i=1}^{n} \tau^{\vec{i}}) = \tau^{\vec{1}} \cup \bigcup_{i=1}^{n} (\tau^{\dot{\vec{2}}} \frown \tau^{\vec{i}}) = \tau^{\vec{1}} \cup \bigcup_{i=1}^{n} \tau^{\overrightarrow{i+1}} = \tau^{\vec{1}} \cup \bigcup_{j=2}^{n+1} \tau^{\vec{j}} = \bigcup_{i=1}^{n+1} \tau^{\vec{i}}$. $F^{\vec{+}}$ is a complete $\cup$-morphism so that by S. Kleene's fixpoint theorem, $\operatorname{lfp}^{\subseteq}_{\emptyset} F^{\vec{+}} = \bigcup_{n \in \mathbb{N}} X^n = \bigcup_{n \in \mathbb{N}} \bigcup_{i=1}^{n} \tau^{\vec{i}} = \bigcup_{i>0} \tau^{\vec{i}} = \tau^{\vec{+}}$.

The first iterates of $F^{\vec{+}}$ for $\operatorname{gfp}^{\subseteq}_{\Sigma^{\vec{+}}} F^{\vec{+}}$ are $Y^0 = \Sigma^{\vec{+}}$, $Y^1 = F^{\vec{+}}(Y^0) = \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown \Sigma^{\vec{+}}$, etc. By recurrence, the n-th iterate is $Y^n = \bigcup_{i=1}^{n} \tau^{\vec{i}} \cup \tau^{\dot{\overrightarrow{n+1}}} \frown \Sigma^{\vec{+}}$ since $Y^{n+1} = F^{\vec{+}}(Y^n) = \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown (\bigcup_{i=1}^{n} \tau^{\vec{i}} \cup \tau^{\dot{\overrightarrow{n+1}}} \frown \Sigma^{\vec{+}}) = \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown (\bigcup_{i=1}^{n} \tau^{\vec{i}}) \cup \tau^{\dot{\vec{2}}} \frown \tau^{\dot{\overrightarrow{n+1}}} \frown \Sigma^{\vec{+}} = \bigcup_{i=1}^{n+1} \tau^{\vec{i}} \cup \tau^{\dot{\overrightarrow{n+2}}} \frown \Sigma^{\vec{+}}$. $F^{\vec{+}}$ is a complete $\cap$-morphism so that by S. Kleene's dual fixpoint theorem, $\operatorname{gfp}^{\subseteq}_{\Sigma^{\vec{+}}} F^{\vec{+}} = \bigcap_{n \in \mathbb{N}} Y^n = \bigcap_{n \in \mathbb{N}} (\bigcup_{i=1}^{n} \tau^{\vec{i}} \cup \tau^{\dot{\overrightarrow{n+1}}} \frown \Sigma^{\vec{+}}) = \bigcup_{i>0} \tau^{\vec{i}} = \tau^{\vec{+}}$ because $\forall i, n \in \mathbb{N} : \tau^{\vec{i}} \subseteq Y^n$ and for all successive states $\langle \sigma_i,\ \sigma_{i+1} \rangle$ of a finite trace σ in $\bigcap_{n \in \mathbb{N}} Y^n$, we have $\sigma_i\ \tau\ \sigma_{i+1}$ since otherwise $\sigma \notin Y^{i+2}$.

□

5.2 Fixpoint Infinite Trace Semantics

The *infinite trace semantics* $\tau^{\vec{\omega}}$ can be presented in $\subseteq$-greatest fixpoint form as follows [13, example 20]:

Theorem 5.2 (Fixpoint infinite trace semantics) $\tau^{\vec{\omega}} = \operatorname{gfp}^{\subseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}}$ *where* $F^{\vec{\omega}} \in \wp(\Sigma^{\vec{\omega}}) \xmapsto{\cap} \wp(\Sigma^{\vec{\omega}})$ *defined as* $F^{\vec{\omega}}(X) \triangleq \tau^{\dot{\vec{2}}} \frown X$ *is a complete* $\cap$-*morphism on the complete lattice* $\langle \wp(\Sigma^{\vec{\omega}}),\ \supseteq,\ \Sigma^{\vec{\omega}},\ \emptyset,\ \cap,\ \cup \rangle$. $\operatorname{lfp}^{\subseteq}_{\emptyset} F^{\vec{\omega}} = \emptyset$.

Proof. The first iterates of $F^{\vec{\omega}}$ for $\operatorname{gfp}^{\subseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}}$ are $X^0 = \Sigma^{\vec{\omega}} = \tau^{\dot{\vec{1}}} \frown \Sigma^{\vec{\omega}}$, $X^1 = F^{\vec{\omega}}(X^0) = \tau^{\dot{\vec{2}}} \frown \tau^{\dot{\vec{1}}} \frown \Sigma^{\vec{\omega}} = \tau^{\dot{\vec{2}}} \frown \Sigma^{\vec{\omega}}$, etc. By recurrence $\forall n \in \mathbb{N} : X^n = \tau^{\dot{\overrightarrow{n+1}}} \frown \Sigma^{\vec{\omega}}$ since $X^{n+1} = F^{\vec{\omega}}(X^n) = \tau^{\dot{\vec{2}}} \frown X^n = \tau^{\dot{\vec{2}}} \frown \tau^{\dot{\overrightarrow{n+1}}} \frown \Sigma^{\vec{\omega}} = \tau^{\dot{\overrightarrow{n+2}}} \frown \Sigma^{\vec{\omega}}$. $F^{\vec{\omega}} = \lambda X \bullet \tau^{\dot{\vec{2}}} \frown X$ is a complete $\cap$-morphism on $\wp(\Sigma^{\vec{\omega}})$ so by S. Kleene dual fixpoint theorem, $\operatorname{gfp}^{\subseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}} = \bigcap_{n \in \mathbb{N}} X^n = \bigcap_{n \in \mathbb{N}} \tau^{\dot{\overrightarrow{n+1}}} \frown \Sigma^{\vec{\omega}} = \bigcap_{n>0} \tau^{\dot{\vec{n}}} \frown \Sigma^{\vec{\omega}} = \tau^{\vec{\omega}}$ because $\forall n \in \mathbb{N} : \tau^{\vec{\omega}} \subseteq X^n$ and for all successive states $\langle \sigma_i,\ \sigma_{i+1} \rangle$ of an infinite trace σ in $\bigcap_{n \in \mathbb{N}} X^n$, we have $\sigma_i\ \tau\ \sigma_{i+1}$ since otherwise $\sigma \notin X^i$. □

5.3 Fixpoint Maximal Trace Semantics

By the fixpoint fusion theorem 2.8 and fixpoint theorems 5.1 and 5.2, the *maximal trace semantics* $\tau^{\vec{\infty}}$ can now be presented in two different fixpoint forms, as follows [13, examples 21 & 28]:

Theorem 5.3 (Fixpoint maximal trace semantics) $\tau^{\vec{\infty}} = \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\infty}}} F^{\vec{\infty}} = \mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\perp^{\vec{\infty}}} F^{\vec{\infty}}$ *where* $F^{\vec{\infty}} \in \wp(\Sigma^{\vec{\infty}}) \xrightarrow{\sqcup^{\vec{\infty}}} \wp(\Sigma^{\vec{\infty}})$ *defined as* $F^{\vec{\infty}}(X) \triangleq \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X$ *is a complete* $\sqcup^{\vec{\infty}}$*-morphism on the complete lattice* $\langle \wp(\Sigma^{\vec{\infty}}), \sqsubseteq^{\vec{\infty}}, \perp^{\vec{\infty}}, \top^{\vec{\infty}}, \sqcup^{\vec{\infty}}, \sqcap^{\vec{\infty}} \rangle$ *with* $X \sqsubseteq^{\vec{\infty}} Y \triangleq X^{\vec{+}} \subseteq Y^{\vec{+}} \wedge X^{\vec{\omega}} \supseteq Y^{\vec{\omega}}$, $X^{\vec{+}} \triangleq X \cap \top^{\vec{\infty}}$, $\top^{\vec{\infty}} = \Sigma^{\vec{+}}$, $X^{\vec{\omega}} \triangleq X \cap \perp^{\vec{\infty}}$ *and* $\perp^{\vec{\infty}} = \Sigma^{\vec{\omega}}$.

Proof. We have $\tau^{\vec{\infty}} \triangleq \tau^{\vec{+}} \cup \tau^{\vec{\omega}} = \mathrm{lfp}^{\subseteq}_{\emptyset} F^{\vec{+}} \cup \mathrm{lfp}^{\supseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}} = \mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\Sigma^{\vec{\omega}}} F^{\vec{\infty}}$ by theorems 5.1, 5.2 and 2.8, where $F^{\vec{\infty}}(X) \triangleq F^{\vec{+}}(X^{\vec{+}}) \cup F^{\vec{\omega}}(X^{\vec{\omega}}) = \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X^{\vec{+}} \cup \tau^{\dot{\vec{2}}} \frown X^{\vec{\omega}} = \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown (X^{\vec{+}} \cup X^{\vec{\omega}}) = \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X$. Moreover, $\bigsqcup\limits_i^{\vec{\infty}} F^{\vec{\infty}}(X_i) = \bigsqcup\limits_i^{\vec{\infty}} \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X_i = \bigcup\limits_i (\tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X_i^{\vec{+}}) \cup \bigcap\limits_i (\tau^{\dot{\vec{2}}} \frown X_i^{\vec{\omega}}) = \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown (\bigcup\limits_i X_i^{\vec{+}} \cup \bigcap\limits_i X_i^{\vec{\omega}}) = F^{\vec{\infty}}(\bigsqcup\limits_i^{\vec{\infty}} X_i)$.

By theorems 5.1, 5.2 and the dual of theorem 2.8, we also have: $\tau^{\vec{\infty}} \triangleq \tau^{\vec{+}} \cup \tau^{\vec{\omega}} = \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{+}}} F^{\vec{+}} \cup \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}} = \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\infty}}} F^{\vec{\infty}}$. □

The non-determinism of the transition system $\langle \Sigma, \tau \rangle$ may be unbounded. Observe that this does not imply absence of Scott-continuity of the transformer $F^{\vec{\infty}}$ of the fixpoint semantics $\tau^{\vec{\infty}} = \mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\perp^{\vec{\infty}}} F^{\vec{\infty}}$, as already observed by [4] using program execution trees. This is not in contradiction with [2, theorem 3.4] proving that there is no fully abstract continuous compositional least fixpoint semantics that has a continuous full abstraction function. However this is for a specific operational semantic domain only and does not apply to all semantic domains. For example, unbounded nondeterminism is equivalent to weak fairness and the description of fair executions can be refined into maximal execution traces for a transition relation including an explicit universal scheduler.

Corollary 5.4 (Arrangement of the iterates of $F^{\vec{\infty}}$) *Let* $F^{\vec{\infty}\delta}$, $\delta \in \mathbb{O}$ *be the iterates of* $F^{\vec{\infty}}$ *from* $\perp^{\vec{\infty}}$*. Their order is* ω *and* $\tau^{\vec{\infty}} = F^{\vec{\infty}\omega} = \bigsqcup\limits_{n<\omega}^{\vec{\infty}} F^{\vec{\infty}n}$*. We have* $\forall n < \omega : F^{\vec{\infty}n} = \bigcup\limits_{i=1}^{n} \tau^{\vec{i}} \cup \tau^{\dot{\overrightarrow{n+1}}} \frown \Sigma^{\vec{\omega}}$*.*

Proof. Let $F^{\vec{+}\delta}$ (resp. $F^{\vec{\omega}\delta}$), $\delta \in \mathbb{O}$ be the iterates of $F^{\vec{+}}$ (resp. $F^{\vec{\omega}}$) from $\perp^{\vec{+}}$ (resp. $\perp^{\vec{\omega}}$). Both have order ω. By transfinite induction, $\forall \delta \in \mathbb{O} : F^{\vec{\infty}\delta} = F^{\vec{+}\delta} \cup F^{\vec{\omega}\delta}$ where for all $n < \omega$, $F^{\vec{+}n} = \bigcup\limits_{i=1}^{n} \tau^{\vec{i}}$ and $F^{\vec{\omega}n} = \tau^{\dot{\overrightarrow{n+1}}} \frown \Sigma^{\vec{\omega}}$ as shown by the respective proofs of theorems 5.1 and 5.2. □

One may wonder why, following [13], we have characterized the trace semantics as $\tau^{\vec{\infty}} = \mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\perp^{\vec{\infty}}} F^{\vec{\infty}}$ while $\tau^{\vec{\infty}} = \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\infty}}} F^{\vec{\infty}}$ is both more frequently used in the literature (e.g. [3]) and apparently simpler. This is because $\tau^{\vec{\infty}} = \mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\perp^{\vec{\infty}}} F^{\vec{\infty}}$ may lift to further abstractions while $\tau^{\vec{\infty}} = \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\infty}}} F^{\vec{\infty}}$ does not. For an example, let us consider potential termination.

5.4 Potential Termination Semantics

The *potential termination semantics* $\tau^{\trianglelefteq}$ of a transition system $\langle \Sigma,\, \tau \rangle$ provides the set of states starting an execution which *may* terminate, that is $\tau^{\trianglelefteq} \triangleq \alpha^{\trianglelefteq}(\tau^{\vec{\infty}})$ where the Galois insertion $\langle \wp(\Sigma^{\vec{\infty}}),\, \sqsubseteq^{\vec{\infty}} \rangle \underset{\alpha^{\trianglelefteq}}{\overset{\gamma^{\trianglelefteq}}{\leftrightarrows}} \langle \wp(\Sigma),\, \subseteq \rangle$ is defined by $\alpha^{\trianglelefteq}(X) \triangleq \{\sigma_0 \mid \sigma \in X \cap \Sigma^{\vec{+}}\}$ and $\gamma^{\trianglelefteq}(Y) \triangleq \{\sigma \in \Sigma^{\vec{+}} \mid \sigma_0 \in Y\} \cup \Sigma^{\vec{\omega}}$. In fixpoint form, we have (the *left image* of $s \in \Sigma$ by a transition relation $\tau \subseteq \Sigma \times \Sigma$ is $\tau^{\blacktriangleleft\bullet}(s) \triangleq \{s' \mid s' \;\tau\; s\}$ while for $S \subseteq \Sigma$, it is $\tau^{\blacktriangleleft}(S) \triangleq \bigcup_{s \in S} \tau^{\blacktriangleleft\bullet}(s) = \{s' \mid \exists s \in S : s' \;\tau\; s\}$):

Theorem 5.5 (Fixpoint potential termination semantics) $\tau^{\trianglelefteq} = \mathrm{lfp}_{\emptyset}^{\subseteq} F^{\trianglelefteq}$ *where* $F^{\trianglelefteq} \in \wp(\Sigma) \overset{\cup}{\longmapsto} \wp(\Sigma)$ *defined as* $F^{\trianglelefteq}(X) \triangleq \check{\tau} \cup \tau^{\blacktriangleleft}(X)$ *is a complete* $\cup$*-morphism on the complete lattice* $\langle \wp(\Sigma),\, \subseteq,\, \emptyset,\, \Sigma,\, \cup,\, \cap \rangle$.

Proof. We have $\alpha^{\trianglelefteq}(X) \subseteq Y \iff \forall \sigma \in X^{\vec{+}} : \sigma_0 \in Y \iff X^{\vec{+}} \subseteq (\{\sigma \in \Sigma^{\vec{+}} \mid \sigma_0 \in Y\} \cup \Sigma^{\vec{\omega}}) \cap \Sigma^{\vec{+}} \iff X^{\vec{+}} \subseteq (\gamma^{\trianglelefteq}(Y))^{\vec{+}} \wedge X^{\vec{\omega}} \supseteq \emptyset \iff X^{\vec{+}} \subseteq (\gamma^{\trianglelefteq}(Y))^{\vec{+}} \wedge X^{\vec{\omega}} \supseteq (\gamma^{\trianglelefteq}(Y))^{\vec{\omega}} \iff X \sqsubseteq^{\vec{\infty}} \gamma^{\trianglelefteq}(Y)$ so that $\langle \wp(\Sigma^{\vec{\infty}}),\, \sqsubseteq^{\vec{\infty}} \rangle \underset{\alpha^{\trianglelefteq}}{\overset{\gamma^{\trianglelefteq}}{\leftrightarrows}} \langle \wp(\Sigma),\, \subseteq \rangle$. Moreover $\alpha^{\trianglelefteq}(\perp^{\vec{\infty}}) = \alpha^{\trianglelefteq}(\Sigma^{\vec{\omega}}) = \emptyset$ so that by S. Kleene's fixpoint transfer theorem 2.3 and 5.3, we have $\tau^{\trianglelefteq} = \alpha^{\trianglelefteq}(\tau^{\vec{\infty}}) = \alpha^{\trianglelefteq}(\mathrm{lfp}_{\perp^{\vec{\infty}}}^{\sqsubseteq^{\vec{\infty}}} F^{\vec{\infty}}) = \mathrm{lfp}_{\emptyset}^{\subseteq} F^{\trianglelefteq}$ where the commutation condition leads to the design of the transformer $F^{\trianglelefteq}$ as follows: $\alpha^{\trianglelefteq} \circ F^{\vec{\infty}}(X) = \alpha^{\trianglelefteq}(\tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X) = \alpha^{\trianglelefteq}(\tau^{\vec{1}}) \cup \alpha^{\trianglelefteq}(\tau^{\dot{\vec{2}}} \frown X) = \{\sigma_0 \mid \sigma \in \tau^{\vec{1}}\} \cup \{\sigma_0 \mid \sigma \in (\tau^{\dot{\vec{2}}} \frown X) \cap \Sigma^{\vec{+}}\} = \check{\tau} \cup \{s \mid \exists s' \in \alpha^{\trianglelefteq}(X) : s \;\tau\; s'\} = F^{\trianglelefteq}(X)$ by defining $F^{\trianglelefteq}(X) \triangleq \check{\tau} \cup \tau^{\blacktriangleleft}(X)$.□

In general $\tau^{\trianglelefteq} \neq \mathrm{gfp}_{\Sigma}^{\subseteq} F^{\trianglelefteq}$ (so that $\alpha^{\trianglelefteq}$ is not co-continuous). A counter-example is given by $\Sigma \triangleq \{a\}$, $\tau \triangleq \{\langle a,\, a \rangle\}$ so that $\check{\tau} = \emptyset$ and $\tau^{\trianglelefteq} = \emptyset$ while $\mathrm{gfp}_{\Sigma}^{\subseteq} F^{\trianglelefteq} = \{a\}$. Hence $\alpha^{\trianglelefteq}$ transfers $\mathrm{lfp}_{\perp^{\vec{\infty}}}^{\sqsubseteq^{\vec{\infty}}} F^{\vec{\infty}}$ but not $\mathrm{gfp}_{\Sigma^{\vec{\infty}}}^{\subseteq} F^{\vec{\infty}}$.

6 The Maximal Trace Semantics as a Refinement of the Transition Semantics

The trace semantics is a refinement of the transition/small-step operational semantics by the Galois insertion $\langle \wp(\Sigma^{\vec{\infty}}),\, \subseteq \rangle \underset{\alpha^{\tau}}{\overset{\gamma^{\tau}}{\leftrightarrows}} \langle \wp(\Sigma \times \Sigma),\, \subseteq \rangle$ where the abstraction collects possible transitions $\alpha^{\tau}(T) \triangleq \{\langle s,\, s' \rangle \mid \exists \sigma \in \Sigma^{\vec{*}} : \exists \sigma' \in \Sigma^{\vec{\infty}} : \sigma \cdot ss' \cdot \sigma' \in T\}$ while the concretization builds maximal execution traces $\gamma^{\tau}(t) \triangleq t^{\vec{\infty}}$. In general $T \subsetneq \gamma^{\tau}(\alpha^{\tau}(T))$ as shown by the set of fair traces $T = \{a^n b \mid n \in \mathbb{N}\}$ for which $\alpha^{\tau}(T) = \{\langle a,\, a \rangle, \langle a,\, b \rangle\}$ and $\gamma^{\tau}(\alpha^{\tau}(T)) = \{a^n b \mid n \in \mathbb{N}\} \cup \{a^{\omega}\}$ is unfair for b.

7 Relational Semantics

The relational semantics associates an input-output relation to a program [29], possibly using D. Scott's bottom $\bot \notin \Sigma$ to denote non-termination [26]. It is an abstraction of the maximal trace semantics where intermediate computation states are ignored.

7.1 Finite/Angelic Relational Semantics

The *finite/angelic relational semantics* (also called big-step operational semantics by G. Plotkin [35], natural semantics by G. Kahn [25], relational semantics by R. Milner & M. Tofte [29] and evaluation semantics by A. Pitts [34]) is $\tau^+ \triangleq \alpha^+(\tau^{\vec{+}})$ where the Galois insertion $\langle \wp(\Sigma^{\vec{+}}),\, \subseteq\rangle \underset{\alpha^+}{\overset{\gamma^+}{\leftrightarrows}} \langle \wp(\Sigma \times \Sigma),\, \subseteq\rangle$ is defined by $\alpha^+(X) \triangleq \{@^+(\sigma) \mid \sigma \in X\}$ and $\gamma^+(Y) \triangleq \{\sigma \mid @^+(\sigma) \in Y\}$ where $@^+ \in \Sigma^{\vec{+}} \longmapsto (\Sigma \times \Sigma)$ is $@^+(\sigma) \triangleq \langle \sigma_0,\, \sigma_{n-1}\rangle$, for all $\sigma \in \Sigma^{\vec{n}}$, $n \in \mathbb{N}$. Using S. Kleene fixpoint transfer 2.3 and theorem 5.1, we can express τ^+ in fixpoint form ($\bar{\tau} \triangleq \{\langle s,\, s\rangle \mid s \in \check{\tau}\}$ is the set of final/blocking state pairs):

Theorem 7.1 (Fixpoint finite/angelic relational semantics) $\tau^+ = \mathrm{lfp}_{\emptyset}^{\subseteq} F^+$ *where* $F^+ \in \wp(\Sigma \times \Sigma) \overset{\cup}{\longmapsto} \wp(\Sigma \times \Sigma)$ *defined as* $F^+(X) \triangleq \bar{\tau} \cup \tau \circ X$ *is a complete* $\cup$*-morphism on the complete lattice* $\langle \wp(\Sigma \times \Sigma),\, \subseteq,\, \emptyset,\, \Sigma \times \Sigma,\, \cup,\, \cap\rangle$.

Proof. By S. Kleene fixpoint transfer theorem 2.3, using the Galois insertion of example 2.6 and $\alpha^+ \circ F^{\vec{+}}(X) = \{@^+(x) \mid x \in \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X\} = \{\langle s,\, s\rangle \mid \forall s' \in \Sigma : \neg(s\ \tau\ s')\} \cup \{\langle s,\, \sigma_{n-1}\rangle \mid n > 0 \wedge \sigma \in \Sigma^{\vec{n}} \wedge s\ \tau\ \sigma_0 \wedge \sigma \in X\} = \bar{\tau} \cup \tau \circ \alpha^+(X)$ $= F^+ \circ \alpha^+(X)$ by defining $F^+(X) \triangleq \bar{\tau} \cup \tau \circ X$ where $\bar{\tau} \triangleq \{\langle s,\, s\rangle \mid s \in \check{\tau}\}$. □

Observe that A. Tarski fixpoint transfer theorem 2.4 is not applicable since α^+ is a $\cap$-morphism but not co-continuous hence not a complete $\cap$-morphism. A counter example is given by the $\subseteq$-decreasing chain $X^k \triangleq \{a^n b \mid n \geq k\}, k > 0$ such that $\bigcap_{k>0} \alpha^+(X^k) = \bigcap_{k>0} \{\langle a,\, b\rangle\} = \{\langle a,\, b\rangle\}$ while $\bigcap_{k>0} X^k = \emptyset$ since $a^n b \in \bigcap_{k>0} X^k$ for $n > 0$ is in contradiction with $a^n b \notin X^{n+1}$ so that $\alpha^+(\bigcap_{k>0} X^k) = \alpha^+(\emptyset) = \emptyset$.

7.2 Infinite Relational Semantics

The *infinite relational semantics* is $\tau^\omega \triangleq \alpha^\omega(\tau^{\vec{\omega}})$ where the Galois insertion $\langle \wp(\Sigma^{\vec{\omega}}),\, \subseteq\rangle \underset{\alpha^\omega}{\overset{\gamma^\omega}{\leftrightarrows}} \langle \wp(\Sigma \times \{\bot\}),\, \subseteq\rangle$ is defined by $\alpha^\omega(X) \triangleq \{@^\omega(\sigma) \mid \sigma \in X\}$ and $\gamma^\omega(Y) \triangleq \{\sigma \mid @^\omega(\sigma) \in Y\}$ where $@^\omega \in \Sigma^{\vec{\omega}} \longmapsto (\Sigma \times \{\bot\})$ is $@^\omega(\sigma) \triangleq \langle \sigma_0,\, \bot\rangle$.

By the Galois connection, α^ω is a complete $\cup$-morphism. It is a $\cap$-morphism but not co-continuous. A counter-example is given by the $\subseteq$-decreasing chain $X^k \triangleq \{a^n b^\omega \mid n \geq k\}$, $k > 0$ such that $\bigcap_{k>0} \alpha^\omega(X^k) = \bigcap_{k>0} \{\langle a,\, \bot\rangle\} = \{\langle a,\, \bot\rangle\}$ while $\bigcap_{k>0} X^k = \emptyset$ since $a^n b^\omega \in \bigcap_{k>0} X^k$ for $n > 0$ is in contradiction with

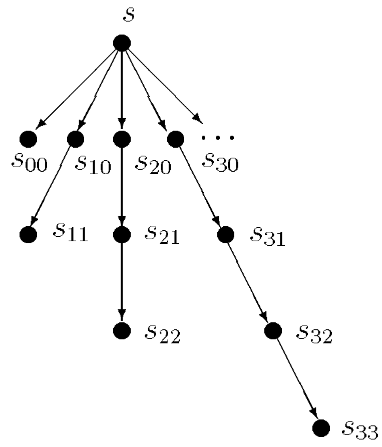


Fig. 1. Transition system with unbounded nondeterminism

$a^n b^\omega \notin X^{n+1}$ whence $\alpha^\omega(\bigcap\limits_{k>0} X^k) = \alpha^\omega(\emptyset) = \emptyset$. Using A. Tarski fixpoint transfer theorem 2.4 and theorem 5.2, we get:

Theorem 7.2 (Fixpoint infinite relational semantics) $\tau^\omega = \mathrm{gfp}^{\subseteq}_{\Sigma\times\{\bot\}} F^\omega$ *where* $F^\omega \in \wp(\Sigma \times \{\bot\}) \xmapsto{m} \wp(\Sigma \times \{\bot\})$ *defined as* $F^\omega(X) \triangleq \tau \circ X$ *is a* $\subseteq$*-monotone map on the complete lattice* $\langle \wp(\Sigma \times \{\bot\}),\, \subseteq,\, \emptyset,\, \Sigma \times \{\bot\},\, \cup,\, \cap\rangle$.

Proof. By the Galois connection, α^ω is a complete $\cup$-morphism. To design F^ω, we have $\alpha^\omega \circ F^{\vec{\omega}}(X) = \alpha^\omega(\tau^{\vec{\dot{2}}} \frown X) = \{\text{@}^\omega(\eta \frown \xi) \mid \eta \in \tau^{\vec{\dot{2}}} \wedge \xi \in X \wedge \eta \mathrel{?} \xi\}$ $= \{\langle \eta_0,\, \bot\rangle \mid \eta_0 \;\tau\; \xi_0 \wedge \xi \in X\} = \{\langle s,\, \bot\rangle \mid \exists s' : s \;\tau\; s' \wedge \langle s',\, \bot\rangle \in \alpha^\omega(X)\} =$ $\tau \circ \alpha^\omega(X) = F^\omega \circ \alpha^\omega(X)$ by defining $F^\omega(X) \triangleq \tau \circ X$.

We have to prove that $\forall Y \in \wp(\Sigma \times \{\bot\}) : F^\omega(Y) \supseteq Y \Longrightarrow \exists X \in \Sigma^{\vec{\omega}} :$ $\alpha^\omega(X) = Y \wedge F^{\vec{\omega}}(X) \supseteq X$. We let $X \triangleq \{\sigma \in \tau^\omega \mid \forall i \in \mathbb{N} : \langle \sigma_i,\, \bot\rangle \in Y\}$.

To prove that $Y \subseteq \alpha^\omega(X)$, observe (a) that $Y \subseteq F^\omega(Y) = \tau \circ Y = \{\langle s,$ $\bot\rangle \mid \exists s' : s \;\tau\; s' \wedge \langle s',\, \bot\rangle \in Y\}$. Hence if $\sigma_0 \dots \sigma_n$ is such that $\sigma_i \;\tau\; \sigma_{i+1}$, $i < n$ and $\langle \sigma_i,\, \bot\rangle \in Y$, $i \leq n$ then $\langle \sigma_n,\, \bot\rangle \in Y$ and (a) imply $\exists \sigma_{n+1}$: $\sigma_n \;\tau\; \sigma_{n+1}$ $\wedge$ $\langle \sigma_{n+1},\, \bot\rangle \in Y$. So, by induction, we can built $\sigma \in \tau^\omega$ such that $\forall i \in \mathbb{N}$: $\langle \sigma_i,\, \bot\rangle \in Y$. We have $\sigma \in X$ and $\langle \sigma_0,\, \bot\rangle \in \alpha^\omega(X)$ proving that $Y \subseteq \alpha^\omega(X)$. Moreover $\alpha^\omega(X) \subseteq Y$ is obvious since $\sigma \in X$ implies $\langle \sigma_0,\, \bot\rangle \in Y$ proving that $\alpha^\omega(X) = Y$ by antisymmetry.

To prove that $F^\omega(X) \supseteq X$ observe that $F^\omega(X) \supseteq X \Longleftrightarrow X \subseteq \tau^{\vec{\dot{2}}} \frown X$ $\Longleftrightarrow \forall \sigma \in X : \sigma_0 \;\tau\; \sigma_1 \wedge \sigma^{\geq 1} \in X$ where the suffix $\sigma^{\geq 1}$ is η such that $\forall i \in \mathbb{N} : \eta_i = \sigma_{i+1}$. $\sigma_0 \;\tau\; \sigma_1$ holds since $X \subseteq \tau^\omega$. $\eta \in \tau^\omega$ and $\forall i \in \mathbb{N} : \langle \eta_i,$ $\bot\rangle = \langle \sigma_i,\, \bot\rangle \in Y$ proving that $\eta = \sigma^{\geq 1} \in X$.

We conclude by the dual of A. Tarski's fixpoint transfer theorem 2.4. □

In general F^ω is not co-continuous, as shown by the following example where the iterates for $\mathrm{gfp}^{\subseteq}_{\Sigma\times\{\bot\}} F^\omega$ do not stabilize at ω.

Example 7.3 (Unbounded nondeterminism) Let us consider the transition system $\langle \Sigma,\, \tau\rangle$ of figure 1 such that $\Sigma = \{s\} \cup \{s_{ij} \mid i, j \in \mathbb{N} \wedge 0 \leq j \leq i\}$ (where $s \neq s_{ij} \neq s_{k\ell}$ whenever $i \neq k$ or $j \neq \ell$) and $\tau = \{\langle s, s_{i0}\rangle \mid i \in \mathbb{N}\} \cup \{\langle s_{ij},$ $s_{i(j+1)}\rangle \mid 0 \leq j < i\}$ [40].

The iterates of $F^{\omega}(X) = \tau \circ X$ are $X^0 = \{\langle s,\, \bot\rangle\} \cup \{\langle s_{ij},\, \bot\rangle \mid 0 \leq j \leq i\}$, $X^1 = F^{\omega}(X^0) = \{\langle s,\, \bot\rangle\} \cup \{\langle s_{ij},\, \bot\rangle \mid 1 \leq j \leq i\}$ so that by recurrence $X^n = \{\langle s,\, \bot\rangle\} \cup \{\langle s_{ij},\, \bot\rangle \mid n \leq j \leq i\}$ whence $X^{\omega} = \bigcap_{n \in \mathbb{N}} X^n = \{\langle s,\, \bot\rangle\}$. Now $X^{\omega+1} = F^{\omega}(X^{\omega}) = \emptyset = \mathrm{gfp}^{\subseteq}_{\Sigma \times \{\bot\}}\, F^{\omega} = \tau^{\omega}$. □

It follows that S. Kleene fixpoint transfer theorem 2.3 is not applicable to prove theorem 7.2 since otherwise the convergence of the iterates of F^{ω} would be as fast as those of $F^{\vec{\omega}}$, hence would be stable at ω.

7.3 Inevitable Termination Semantics

The possibly nonterminating executions could alternatively have been characterized using the isomorphic *inevitable termination semantics* providing the set of states starting an execution which *must* terminate, that is $\tau^{\lhd} \triangleq \alpha^{\lhd}(\tau^{\omega})$ where the Galois bijection $\langle \wp(\Sigma \times \{\bot\}),\, \subseteq\rangle \underset{\alpha^{\lhd}}{\overset{\gamma^{\lhd}}{\rightleftarrows}} \langle \wp(\Sigma),\, \supseteq\rangle$ is defined by $\alpha^{\lhd}(X) \triangleq \{s \mid \langle s,\, \bot\rangle \notin X\}$ and $\gamma^{\lhd}(Y) \triangleq \{\langle s,\, \bot\rangle \mid s \notin Y\}$.

The *right image* of $s \in \Sigma$ by a relation $\tau \subseteq \Sigma \times \Sigma'$ is $\tau^{\bullet\!\!\rightarrow}(s) \triangleq \{s' \mid s\ \tau\ s'\}$ (in particular if $f \in \Sigma \longmapsto \Sigma'$ then $f^{\bullet\!\!\rightarrow}(s) = \{f(s)\}$) while for $P \subseteq \Sigma$, $\tau^{\blacktriangleright}(P) = \{s' \mid \exists s \in P : s\ \tau\ s'\}$ (in particular, $f^{\blacktriangleright}(P) = \{f(s) \mid s \in P\}$). The *inverse* of τ is $\tau^{-1} \triangleq \{\langle s',\, s\rangle \mid s\ \tau\ s'\}$ so that $\tau^{\leftarrow\!\!\bullet} \triangleq (\tau^{-1})^{\bullet\!\!\rightarrow}$ and $\tau^{\blacktriangleleft} \triangleq (\tau^{-1})^{\blacktriangleright}$. The dual of a map $F \in \wp(\Sigma) \longmapsto \wp(\Sigma')$ is $\widetilde{F} \triangleq \lambda P \bullet \neg F(\neg P)$. Finally, $\widetilde{\tau^{-1\blacktriangleright}}(P) = \{s' \mid \forall s : s'\ \tau\ s \Longrightarrow s \in P\}$. Applying the semi-dual of S. Kleene fixpoint transfer theorem 2.3 to the fixpoint characterization 7.2 of the infinite relational semantics τ^{ω}, we get the

Theorem 7.4 (Fixpoint inevitable termination semantics) $\tau^{\lhd} = \mathrm{lfp}^{\subseteq}_{\emptyset}\, F^{\lhd}$ *where* $F^{\lhd} \in \wp(\Sigma) \xmapsto{\cup} \wp(\Sigma)$ *defined as* $F^{\lhd}(X) \triangleq \widetilde{\tau^{-1\blacktriangleright}}(X) = \check{\tau} \cup \widetilde{\tau^{-1\blacktriangleright}}(X)$ *is a complete* $\cup$*-morphism on the complete lattice* $\langle \wp(\Sigma),\, \subseteq,\, \emptyset,\, \Sigma,\, \cup,\, \cap\rangle$.

Proof. $\alpha^{\lhd}$ is bottom strict since $\alpha^{\lhd}(\langle \Sigma,\, \{\bot\}\rangle) = \emptyset$. $\alpha^{\lhd}$ is continuous by $\langle \wp(\Sigma \times \{\bot\}),\, \subseteq\rangle \underset{\alpha^{\lhd}}{\overset{\gamma^{\lhd}}{\rightleftarrows}} \langle \wp(\Sigma),\, \supseteq\rangle$. Finally, we have $\alpha^{\lhd} \circ F^{\omega}(X) = \{s \mid \langle s,\, \bot\rangle \notin \tau \circ X\} = \{s \mid \langle s,\, \bot\rangle \notin \{\langle s,\, s''\rangle \mid \exists s' : \langle s,\, s'\rangle \in \tau \wedge \langle s',\, s''\rangle \in X\}\} = \{s \mid \forall s' : s\ \tau\ s' \Longrightarrow \neg\langle s',\, \bot\rangle \in X\} = \{s \mid \forall s' : s\ \tau\ s' \Longrightarrow s' \in \alpha^{\lhd}(X)\} = F^{\lhd} \circ \alpha^{\lhd}(X)$ by defining $F^{\lhd}(X) \triangleq \widetilde{\tau^{-1\blacktriangleright}}(X) = \check{\tau} \cup \widetilde{\tau^{-1\blacktriangleright}}(X)$. □

7.4 Natural Relational Semantics

We now mix together the descriptions of the finite and infinite executions of a transition system $\langle \Sigma,\, \tau\rangle$. The *natural relational semantics* $\tau^{\infty} \triangleq \tau^{+} \cup \tau^{\omega}$ is the fusion of the finite relational semantics τ^{+} and the infinite relational semantics τ^{ω}. It is more traditional [5,33] to consider the product of the finite relational semantics τ^{+} and the inevitable termination semantics $\tau^{\lhd}$. The reason for preferring the infinite relational semantics to the inevitable termination semantics 7.4 is that the fixpoint characterizations 7.1 of τ^{+} and 7.2 of τ^{ω} fuse naturally by the fixpoint fusion theorem 2.8. This leads to a simple fixpoint characterization of the natural relational semantics using the *mixed ordering* $\sqsubseteq^\infty$ first introduced in [13, proposition 25]:

Theorem 7.5 (Fixpoint natural relational semantics) $\tau^\infty = \mathrm{lfp}_{\perp^\infty}^{\sqsubseteq^\infty} F^\infty$ *where* $F^\infty \in \wp(\Sigma \times \Sigma_\perp) \xmapsto{m} \wp(\Sigma \times \Sigma_\perp)$ *defined as* $F^\infty(X) \triangleq \bar{\tau} \cup \tau \circ X$ *is a* $\sqsubseteq^\infty$*-monotone map on the complete lattice* $\langle \wp(\Sigma \times \Sigma_\perp), \sqsubseteq^\infty, \perp^\infty, \top^\infty, \sqcup^\infty, \sqcap^\infty \rangle$ *with* $\Sigma_\perp \triangleq \Sigma \cup \{\perp\}$*,* $X \sqsubseteq^\infty Y \triangleq X^+ \subseteq Y^+ \wedge X^\omega \supseteq Y^\omega$*,* $X^+ \triangleq X \cap \top^\infty$*,* $\top^\infty = \Sigma \times \Sigma$*.* $X^\omega \triangleq X \cap \perp^\infty$ *and* $\perp^\infty = \Sigma \times \{\perp\}$*.*

Proof. $\tau^\infty = \tau^+ \cup \tau^\omega = \mathrm{lfp}_\emptyset^{\subseteq} F^+ \cup \mathrm{lfp}_{\Sigma \times \{\perp\}}^{\supseteq} F^\omega = \mathrm{lfp}_{\perp^\infty}^{\sqsubseteq^\infty} F^\infty$. □

By defining $\alpha^\infty(X) \triangleq \alpha^+(X^+) \cup \alpha^\omega(X^\omega)$, we have $\tau^\infty = \alpha^\infty(\tau^{\vec{\infty}})$. Neither S. Kleene fixpoint transfer theorem 2.3 nor A. Tarski fixpoint transfer theorem 2.4 is directly applicable to derive that $\tau^\infty = \alpha^\infty(\mathrm{lfp}_{\perp^{\vec{\infty}}}^{\sqsubseteq^{\vec{\infty}}} F^{\vec{\infty}}) = \mathrm{lfp}_{\perp^\infty}^{\sqsubseteq^\infty} F^\infty$. Observe however that we proceeded by fusion of independent parts, using α^+ to transfer the finitary part $\tau^{\vec{+}}$ by S. Kleene fixpoint transfer theorem 2.3 (but A. Tarski's one was not applicable) and the infinitary part $\tau^{\vec{\omega}}$ by A. Tarski fixpoint transfer theorem 2.4 (but S. Kleene's one was not applicable).

To prove that the iterates of F^∞ are ordered according to Egli-Milner ordering, we will use the following:

Lemma 7.6 (Arrangement of the iterates of F^∞) *Let* $F^{\infty\delta}$*,* $\delta \in \mathbb{O}$ *be the iterates of* $F^\infty = \lambda X \cdot \bar{\tau} \cup \tau \circ X$ *from* $\perp^\infty$*. For all* $\eta < \xi \in \mathbb{O}$*,* $s, s' \in \Sigma$*, if* $\langle s,\ s' \rangle \in F^{\infty\xi}$ *and* $\langle s,\ s' \rangle \notin F^{\infty\eta}$ *then* $\langle s,\ \perp \rangle \in F^{\infty\eta}$*.*

Proof. By transfinite induction on $\xi > 0$.

The lemma is true for $\xi = 1$ since for $\eta = 0$ we have $F^{\infty 0} = \perp^\infty = \Sigma \times \{\perp\}$.

We have $F^{\infty 1} = \bar{\tau} \cup \tau \circ F^{\infty 0}$, $F^{\infty\delta}$, $\delta \in \mathbb{O}$ is a $\sqsubseteq^\infty$-increasing chain so that $(F^{\infty\delta})^+$, $\delta \in \mathbb{O}$ is a $\subseteq$-increasing chain and $\forall \delta \in \mathbb{O}$: $(F^{\infty\delta})^+ \subseteq F^{\infty\delta}$ proving that $\forall \delta \in \mathbb{O} : \bar{\tau} \subseteq F^{\infty\delta}$.

Assume that the lemma holds for all $\xi' < \xi$ and ξ is a limit ordinal. Assume $\eta < \xi$, $\langle s,\ s' \rangle \in F^{\infty\xi}$ and $\langle s,\ s' \rangle \notin F^{\infty\eta}$. We have $F^{\infty\xi} = \bigsqcup^\infty_{\xi' < \xi} F^{\infty\xi'}$ hence $(F^{\infty\xi})^+ = \bigcup_{\xi' < \xi} (F^{\infty\xi'})^+$ so that $\langle s,\ s' \rangle \in F^{\infty\xi}$ implies the existence of $\xi' < \xi$ such that $\langle s,\ s' \rangle \in (F^{\infty\xi'})^+ \subseteq F^{\infty\xi'}$. But $(F^{\infty\delta})^+$, $\delta \in \mathbb{O}$ is a $\subseteq$-increasing chain, so that $\langle s,\ s' \rangle \notin F^{\infty\eta}$ implies $\eta < \xi'$. It follows by induction hypothesis that $\langle s,\ \perp \rangle \in F^{\infty\eta}$.

Assume now that $\xi = \xi' + 1$ is a successor ordinal, $\eta \leq \xi'$, $\langle s,\ s' \rangle \in F^{\infty\xi}$ and $\langle s,\ s' \rangle \notin F^{\infty\eta}$.

I. If $\langle s,\ \perp \rangle \in F^{\infty\xi'}$ then $(F^{\infty\delta})^\omega$, $\delta \in \mathbb{O}$ is a $\subseteq$-decreasing chain so that $\eta \leq \xi'$ implies $\langle s,\ \perp \rangle \in F^{\infty\eta}$.

II. If $\langle s,\ \perp \rangle \notin F^{\infty\xi'}$ then $F^{\infty\xi} = F^{\infty\xi'+1} = F^\infty(F^{\infty\xi'}) = \bar{\tau} \cup \tau \circ F^{\infty\xi'}$ so that $\langle s,\ s' \rangle \in \tau \circ F^{\infty\xi'}$ since $\bar{\tau} \subseteq F^{\infty\eta}$ which implies the existence of $s'' \in \Sigma$ such that $s \ \tau \ s''$ and $\langle s'',\ s' \rangle \in F^{\infty\xi'}$.

II.1. If $\langle s'',\ s' \rangle \notin F^{\infty\eta}$ then by induction hypothesis $\langle s'',\ \perp \rangle \in F^{\infty\eta}$ so that $\langle s,\ \perp \rangle \in F^{\infty\eta+1}$ proving $\langle s,\ \perp \rangle \in F^{\infty\eta}$ since $F^{\infty\delta}$, $\delta \in \mathbb{O}$ is $\sqsubseteq^\infty$-increasing whence $(F^{\infty\delta})^\omega$, $\delta \in \mathbb{O}$ is $\subseteq$-decreasing.

II.2. If $\langle s'',\ s'\rangle \in F^{\infty\eta}$ then $\langle s,\ s'\rangle \in F^{\infty\eta+1}$.

II.2.A. If $\eta < \xi'$, $\eta+1 < \xi$ so that, by induction hypothesis, $\langle s,\ s'\rangle \in F^{\infty\eta+1}$ and $\langle s,\ s'\rangle \notin F^{\infty\eta}$ imply $\langle s,\ \bot\rangle \in F^{\infty\eta}$.

II.2.B. Otherwise $\eta = \xi'$.

II.2.B.a. If $\eta = \xi'$ is a successor ordinal with predecessor $\xi' - 1$ then we have $\langle s'',\ s'\rangle \notin F^{\infty\xi'-1}$ since otherwise $s\ \tau\ s''$ and $\langle s'',\ s'\rangle \in F^{\infty\xi'-1}$ would imply $\langle s,\ s'\rangle \in F^{\infty\xi'}$, in contradiction with $\langle s,\ s'\rangle \notin F^{\infty\eta}$ and $\eta = \xi'$. But $\langle s'',\ s'\rangle \in F^{\infty\eta} = F^{\infty\xi'}$ so $\langle s'',\ s'\rangle \notin F^{\infty\xi'-1}$ and $\xi' < \xi$ imply, by induction hypothesis, that $\langle s'',\ \bot\rangle \in F^{\infty\xi'}$ hence $\langle s'',\ \bot\rangle \in F^{\infty\xi'-1}$. Then $s\ \tau\ s''$ implies $\langle s,\ \bot\rangle \in F^{\infty\xi'} = F^{\infty\eta}$.

II.2.B.b. If $\eta = \xi'$ is a limit ordinal then we have $\langle s'',\ s'\rangle \notin F^{\infty\zeta}$ for all $\zeta < \eta = \xi'$ since otherwise $s\ \tau\ s''$ and $\langle s'',\ s'\rangle \in F^{\infty\zeta}$ would imply $\langle s,\ s'\rangle \in F^{\infty\zeta+1}$ so $\langle s,\ s'\rangle \in F^{\infty\xi'}$, in contradiction with $\langle s,\ s'\rangle \notin F^{\infty\eta}$ and $\eta = \xi'$. But $\langle s'',\ s'\rangle \in F^{\infty\eta} = F^{\infty\xi'}$, $\langle s'',\ s'\rangle \notin F^{\infty\zeta}$ and $\zeta < \xi' < \xi$ imply, by induction hypothesis that $\langle s'',\ \bot\rangle \in F^{\infty\zeta}$ so $\langle s,\ \bot\rangle \in F^{\infty\zeta+1}$ hence $\langle s,\ \bot\rangle \in F^{\infty\zeta}$ and therefore $\langle s,\ \bot\rangle \in F^{\infty\xi'} = F^{\infty\eta}$ since $F^{\infty\xi'} = \bigsqcup^{\infty}_{\zeta<\xi'} F^{\infty\zeta}$. □

Lemma 7.7 (Totality of the iterates of F^{∞}) *Let $F^{\infty\delta}$, $\delta \in \mathbb{O}$ be the iterates of $F^{\infty} = \lambda X \bullet \bar{\tau} \cup \tau \circ X$ from $\bot^{\infty}$. $\forall \delta \in \mathbb{O} : \forall s \in \Sigma : \exists s' \in \Sigma_{\bot} : \langle s,\ s'\rangle \in F^{\infty\delta}$.*

Proof. By transfinite induction on $\delta \in \mathbb{O}$.

For $\delta = 0$, $\forall s \in \Sigma : \langle s,\ \bot\rangle \in F^{\infty 0} = \bot^{\infty} = \Sigma \times \Sigma_{\bot}$.

Assume that the lemma is true for $\delta \in \mathbb{O}$. $F^{\infty\delta+1} = \bar{\tau} \cup \tau \circ F^{\infty\delta}$. If $s \in \bar{\tau}$ then $\langle s,\ s\rangle \in F^{\infty\delta+1}$ or $\exists s' \in \Sigma : s\ \tau\ s'$ so that, by induction hypothesis, $\exists s'' \in \Sigma_{\bot} : \langle s',\ s''\rangle \in F^{\infty\delta}$ proving that $\langle s,\ s''\rangle \in \tau \circ (F^{\infty\delta})^{+} \subseteq (F^{\infty\delta+1})^{+} \subseteq F^{\infty\delta+1}$.

If λ is a limit ordinal and the lemma is true for all $\delta < \lambda$ then either $\forall \delta < \lambda : \langle s,\ \bot\rangle \in F^{\infty\delta}$ in which case $\langle s,\ \bot\rangle \in F^{\infty\lambda}$ since $(F^{\infty\lambda})^{\omega} = \bigcap_{\delta<\lambda} (F^{\infty\delta})^{\omega}$. Otherwise, $\exists \delta < \lambda : \langle s,\ \bot\rangle \notin F^{\infty\delta}$, in which case, by induction hypothesis, $\exists s' \in \Sigma : \langle s,\ s'\rangle \in F^{\infty\delta}$ so that $\langle s,\ s'\rangle \in F^{\infty\lambda}$ since $(F^{\infty\delta})^{+} \subseteq (F^{\infty\lambda})^{+}$. □

Lemma 7.8 (Final states of the iterates of F^{∞}) *Let $F^{\infty\delta}$, $\delta \in \mathbb{O}$ be the iterates of $F^{\infty} = \lambda X \bullet \bar{\tau} \cup \tau \circ X$ from $\bot^{\infty}$. $\forall \delta \in \mathbb{O} : \forall s, s' \in \Sigma : \langle s,\ s'\rangle \in F^{\infty\delta} \Longrightarrow (s' \in \check{\tau}) \wedge (\forall s'' \in \Sigma_{\bot} : \langle s',\ s''\rangle \in F^{\infty\delta} \Longrightarrow s'' = s')$.*

Proof. By transfinite induction on $\delta \in \mathbb{O}$.

The lemma vacuously holds for $\delta = 0$ since $\forall s, s' \in \Sigma : \langle s,\ s'\rangle \notin F^{\infty 0} = \Sigma \times \{\bot\}$.

Assume that the lemma holds for $\delta \in \mathbb{O}$ and $\langle s,\ s'\rangle \in F^{\infty\delta+1} = \bar{\tau} \cup \tau \circ F^{\infty\delta}$. If $\langle s, s'\rangle \in \bar{\tau}$ then $s' = s \in \check{\tau}$ hence $\forall s'' \in \Sigma_{\bot} : \langle s', s''\rangle \in F^{\infty\delta+1} \Longrightarrow (s = s' \wedge \langle s,\ s''\rangle \in \bar{\tau}) \Longrightarrow (s = s' = s'')$. Otherwise, $\exists s'' \in \Sigma : s\ \tau\ s''$ and $\langle s'',\ s'\rangle \in F^{\infty\delta}$ in which case, by induction hypothesis, $s' \in \check{\tau}$. Moreover $\forall s'' \in \Sigma_{\bot} : \langle s',\ s''\rangle \in F^{\infty\delta+1} \Longrightarrow \langle s',\ s''\rangle \in \bar{\tau} \cup \tau \circ F^{\infty\delta}$. But $s' \in \check{\tau}$ so $\langle s',\ s''\rangle \in \bar{\tau}$ which implies $s'' = s'$.

Let λ be a limit ordinal such that the lemma holds for all $\delta < \lambda$. If $\langle s,\ s'\rangle \in F^{\infty\lambda}$ then $(F^{\infty\lambda})^{+} = \bigcup_{\delta<\lambda} (F^{\infty\delta})^{+}$ implies $\exists \delta < \lambda : \langle s,\ s'\rangle \in F^{\infty\delta}$ whence

$s' \in \check{\tau}$ by induction hypothesis. Moreover, $\forall s'' \in \Sigma_\bot : \langle s',\ s''\rangle \in F^{\infty^\delta} \Longrightarrow \exists \eta < \lambda : \langle s',\ s''\rangle \in F^{\infty^\eta}$. Let $\xi = \max(\delta, \eta) < \lambda$. We have $\langle s,\ s'\rangle \in F^{\infty^\xi}$ and $\langle s',\ s''\rangle \in F^{\infty^\xi}$ since F^{∞^δ}, $\delta \in \mathbb{O}$ is $\sqsubseteq^\infty$-increasing whence $\left(F^{\infty^\delta}\right)^+$, $\delta \in \mathbb{O}$ is $\subseteq$-increasing. By induction hypothesis, $s'' = s'$ □

7.5 Demoniac Relational Semantics

The *demoniac relational semantics* is derived from the natural relational semantics by approximating nontermination by chaos: $\tau^\partial \triangleq \alpha^\partial(\tau^\infty)$ where $\alpha^\partial(X) \triangleq X \cup \{\langle s,\ s'\rangle \mid \langle s,\ \bot\rangle \in X \wedge s' \in \Sigma\}$ and $\gamma^\partial(Y) \triangleq Y$ so that $\langle \wp(\Sigma \times \Sigma_\bot),\ \subseteq\rangle \underset{\alpha^\partial}{\overset{\gamma^\partial}{\leftrightarrows}} \langle D^\partial,\ \subseteq\rangle$ where $D^\partial \triangleq \{Y \in \wp(\Sigma \times \Sigma_\bot) \mid \forall s \in \Sigma : \langle s,\ \bot\rangle \in Y \Longrightarrow (\forall s \in \Sigma : \langle s,\ s'\rangle \in Y)\}$. By definition of τ^∂, fixpoint characterization of the natural relational semantics 7.5 and S. Kleene fixpoint transfer theorem 2.3, we derive:

Theorem 7.9 (Fixpoint demoniac relational semantics) $\tau^\partial = \mathrm{lfp}^{\sqsubseteq^\partial}_{\bot^\partial}\ F^\partial$ *where* $F^\partial \in D^\partial \xmapsto{m} D^\partial$ *defined as* $F^\partial(X) \triangleq \bar{\tau} \cup \tau \circ X$ *is a* $\sqsubseteq^\partial$*-monotone map on the complete lattice* $\langle D^\partial, \sqsubseteq^\partial, \bot^\partial, \top^\partial, \sqcup^\partial, \sqcap^\partial\rangle$ *with* $X \sqsubseteq^\partial Y = \forall s \in \Sigma : \langle s,\ \bot\rangle \in X \vee (\langle s,\ \bot\rangle \notin Y \wedge X \cap (\{s\} \times \Sigma) \subseteq Y \cap (\{s\} \times \Sigma))$, $\bot^\partial \triangleq \Sigma \times \Sigma_\bot$, $\top^\partial \triangleq \Sigma \times \Sigma$, $\bigsqcup^\partial_{i \in \Delta} X_i \triangleq \{\langle s,\ s'\rangle \mid (\forall i \in \Delta : \langle s,\ \bot\rangle \in X_i \wedge s' \in \Sigma_\bot) \vee (\exists i \in \Delta : \langle s,\ \bot\rangle \notin X_i \wedge \langle s,\ s'\rangle \in X_i)\}$ *and* $\bigsqcap^\partial_{i \in \Delta} X_i \triangleq \{\langle s,\ s'\rangle \mid (\exists i \in \Delta : \langle s,\ \bot\rangle \in X_i \wedge s' \in \Sigma_\bot) \vee (\forall i \in \Delta : \langle s,\ \bot\rangle \notin X_i \wedge \langle s,\ s'\rangle \in X_i)\}$.

Moreover $X \sqsubseteq^\partial Y \triangleq \gamma^{\bar\partial}(X) \sqsubseteq^\infty \gamma^{\bar\partial}(Y)$ *where* $\gamma^{\bar\partial}(X) \triangleq \{\langle s,\ \bot\rangle \mid \langle s,\ \bot\rangle \in X\} \cup \{\langle s,\ s'\rangle \mid \langle s,\ \bot\rangle \notin X \wedge \langle s,\ s'\rangle \in X\}$ *so that* $\langle \wp(\Sigma \times \Sigma_\bot), \sqsupseteq^\infty\rangle \underset{\alpha^\partial}{\overset{\gamma^{\bar\partial}}{\leftrightarrows}} \langle D^\partial, \sqsupseteq^\partial\rangle$.

Proof. For the Galois insertion $\langle \wp(\Sigma \times \Sigma_\bot),\ \subseteq\rangle \underset{\alpha^\partial}{\overset{\gamma^\partial}{\leftrightarrows}} \langle D^\partial,\ \subseteq\rangle$ observe that $\alpha^\partial(X) \subseteq Y$ implies $X \cup \{\langle s,\ s'\rangle \mid \langle s,\ \bot\rangle \in X \wedge s' \in \Sigma\} \subseteq Y$ hence $X \subseteq \gamma^\partial(Y)$ and, reciprocally, $X \subseteq \gamma^\partial(Y)$ implies $X \cup \{\langle s,\ s'\rangle \mid \langle s,\ \bot\rangle \in X \wedge s' \in \Sigma\} \subseteq Y \cup \{\langle s,\ s'\rangle \mid \langle s,\ \bot\rangle \in X \wedge s' \in \Sigma\} = Y$ by definition of D^∂ hence $\alpha^\partial(X) \subseteq Y$. This implies that α^∂ is $\cup$-preserving. Moreover $D^\partial \subseteq \wp(\Sigma \times \Sigma_\bot)$ and $\forall X \in D^\partial : \alpha^\partial(X) = X$ proving that α^∂ is surjective.

Assume that $\gamma^{\bar\partial}(X) = \gamma^{\bar\partial}(Y)$. For all $s \in \Sigma$, we have $\langle s,\ \bot\rangle \in X$ iff $\langle s,\ \bot\rangle \in \gamma^{\bar\partial}(X)$ iff $\langle s,\ \bot\rangle \in \gamma^{\bar\partial}(Y)$ iff $\langle s,\ \bot\rangle \in Y$. So if $\langle s,\ \bot\rangle \in X$ then $\langle s,\ \bot\rangle \in Y$ whence by definition of D^∂, $\langle s,\ s'\rangle \in X$ and $\langle s,\ s'\rangle \in Y$ for all $s' \in \Sigma_\bot$. Moreover if $\langle s,\ \bot\rangle \notin X$ then $\langle s,\ \bot\rangle \notin Y$ so that $\gamma^{\bar\partial}(X) = \gamma^{\bar\partial}(Y)$ implies $\{\langle s,\ s'\rangle \mid \langle s,\ s'\rangle \in X\} = \{\langle s,\ s'\rangle \mid \langle s,\ s'\rangle \in Y\}$. It follows that $X = Y$ proving that $\gamma^{\bar\partial}$ is injective.

It follows that the relation defined by $X \sqsubseteq^\partial Y \triangleq \gamma^{\bar\partial}(X) \sqsubseteq^\infty \gamma^{\bar\partial}(Y)$ on D^∂ is a partial order. We have $\gamma^{\bar\partial}(X) \sqsubseteq^\infty \gamma^{\bar\partial}(Y) = (\gamma^{\bar\partial}(X) \cap (\Sigma \times \Sigma) \subseteq \gamma^{\bar\partial}(Y) \cap (\Sigma \times \Sigma)) \wedge (\gamma^{\bar\partial}(X) \cap (\Sigma \times \{\bot\}) \supseteq \gamma^{\bar\partial}(Y) \cap (\Sigma \times \{\bot\})) = (\{\langle s,\ s'\rangle \mid \langle s,\ \bot\rangle \notin X \wedge \langle s,\ s'\rangle \in X\} \subseteq \{\langle s,\ s'\rangle \mid \langle s,\ \bot\rangle \notin Y \wedge \langle s,\ s'\rangle \in Y\}) \wedge (\{\langle s,\ \bot\rangle \mid \langle s,\ \bot\rangle \in X\} \supseteq \{\langle s,\ \bot\rangle \mid \langle s,\ \bot\rangle \in Y\}) = \forall s \in \Sigma : \langle s,\ \bot\rangle \in X \vee (\langle s,$

$\bot\rangle \notin Y \wedge X \cap (\{s\} \times \Sigma) \subseteq Y \cap (\{s\} \times \Sigma))$.

By definition, $\gamma^{\overline{\partial}}$ is monotone.

We have $\gamma^{\overline{\partial}} \circ \alpha^{\partial}(X) = \gamma^{\overline{\partial}}(X \cup \{\langle s, s'\rangle \mid \langle s, \bot\rangle \in X \wedge s' \in \Sigma\}) = \{\langle s, \bot\rangle \mid \langle s, \bot\rangle \in X \cup \{\langle s, s'\rangle \mid \langle s, \bot\rangle \in X \wedge s' \in \Sigma\}\} \cup \{\langle s, s'\rangle \mid \langle s, \bot\rangle \notin X \cup \{\langle s, s'\rangle \mid \langle s, \bot\rangle \in X \wedge s' \in \Sigma\} \wedge \langle s, s'\rangle \in X \cup \{\langle s, s'\rangle \mid \langle s, \bot\rangle \in X \wedge s' \in \Sigma\}\} = \{\langle s, \bot\rangle \mid \langle s, \bot\rangle \in X\} \cup \{\langle s, s'\rangle \mid \langle s, \bot\rangle \notin X \wedge \langle s, s'\rangle \in X\}$.

If follows that $X \cap (\Sigma \times \Sigma) \supseteq \gamma^{\overline{\partial}} \circ \alpha^{\partial}(X) \cap (\Sigma \times \Sigma)$ and $X \cap (\Sigma \times \{\bot\}) = \gamma^{\overline{\partial}} \circ \alpha^{\partial}(X) \cap (\Sigma \times \{\bot\})$ proving that $\gamma^{\overline{\partial}} \circ \alpha^{\partial}(X) \sqsubseteq^{\infty} X$.

If $X \sqsubseteq^{\infty} Y$ then $X \cap (\Sigma \times \Sigma) \subseteq Y \cap (\Sigma \times \Sigma)$ and $X \cap (\Sigma \times \{\bot\}) \supseteq Y \cap (\Sigma \times \{\bot\})$ so that for all $s \in \Sigma$, we have $\{\langle s, \bot\rangle \mid \langle s, \bot\rangle \in X\} \supseteq \{\langle s, \bot\rangle \mid \langle s, \bot\rangle \in Y\}$. Moreover $\langle s, \bot\rangle \notin X \Longrightarrow \langle s, \bot\rangle \notin Y$ whence $\{\langle s, s'\rangle \mid \langle s, \bot\rangle \notin X \wedge \langle s, s'\rangle \in X\} \subseteq \{\langle s, s'\rangle \mid \langle s, \bot\rangle \notin Y \wedge \langle s, s'\rangle \in Y\}$ proving that $\gamma^{\overline{\partial}} \circ \alpha^{\partial}(X) \sqsubseteq^{\infty} \gamma^{\overline{\partial}} \circ \alpha^{\partial}(Y)$ whence $\alpha^{\partial}(X) \sqsubseteq^{\partial} \alpha^{\partial}(Y)$. This shows that α^{∂} is monotone.

$\alpha^{\partial} \circ \gamma^{\overline{\partial}}(X) = \alpha^{\partial}(\{\langle s, \bot\rangle \mid \langle s, \bot\rangle \in X\} \cup \{\langle s, s'\rangle \mid \langle s, \bot\rangle \notin X \wedge \langle s, s'\rangle \in X\}) = \alpha^{\partial}(\{\langle s, \bot\rangle \mid \langle s, \bot\rangle \in X\}) \cup \alpha^{\partial}(\{\langle s, s'\rangle \mid \langle s, \bot\rangle \notin X \wedge \langle s, s'\rangle \in X\})$ since α^{∂} is $\cup$-preserving. This is equal to $\{\langle s, s'\rangle \mid \langle s, \bot\rangle \in X \wedge s' \in \Sigma_{\bot}\} \cup \{\langle s, s'\rangle \mid \langle s, s'\rangle \in X\} = X$ by definition of D^{∂}.

We have $\langle \wp(\Sigma \times \Sigma_{\bot}), \sqsupseteq^{\infty}\rangle \underset{\alpha^{\partial}}{\overset{\gamma^{\overline{\partial}}}{\leftrightarrows}} \langle D^{\partial}, \sqsupseteq^{\partial}\rangle$ since α^{∂} and $\gamma^{\overline{\partial}}$ are monotone, $\alpha^{\partial} \circ \gamma^{\overline{\partial}}$ is the identity on D^{∂} and $\gamma^{\overline{\partial}} \circ \alpha^{\partial}$ is $\sqsupseteq^{\partial}$-extensive, a characteristic property of Galois insertions. Since $\langle \wp(\Sigma \times \Sigma_{\bot}), \sqsubseteq^{\infty}, \bot^{\infty}, \top^{\infty}, \sqcup^{\infty}, \sqcap^{\infty}\rangle$ is a complete lattice, it follows that $\langle D^{\partial}, \sqsubseteq^{\partial}, \bot^{\partial}, \top^{\partial}, \sqcup^{\partial}, \sqcap^{\partial}\rangle$ is also a complete lattice.

The infimum is $\alpha^{\partial}(\bot^{\infty}) = \alpha^{\partial}(\Sigma \times \{\bot\}) = \Sigma \times \Sigma_{\bot}$.

The supremum is $\alpha^{\partial}(\top^{\infty}) = \alpha^{\partial}(\Sigma \times \Sigma) = \Sigma \times \Sigma$.

The join is $\bigsqcup^{\partial}_{i \in \Delta} X_i = \alpha^{\partial}(\bigsqcup^{\infty}_{i \in \Delta} \gamma^{\overline{\partial}}(X_i)) = \alpha^{\partial}((\bigcup_{i \in \Delta} \gamma^{\overline{\partial}}(X_i) \cap \top^{\infty}) \cup (\bigcap_{i \in \Delta} \gamma^{\overline{\partial}}(X_i) \cap \bot^{\infty})) = (\bigcup_{i \in \Delta} \alpha^{\partial}(\gamma^{\overline{\partial}}(X_i) \cap (\Sigma \times \Sigma))) \cup (\alpha^{\partial}(\bigcap_{i \in \Delta} \gamma^{\overline{\partial}}(X_i) \cap (\Sigma \times \{\bot\})))$ by definition of $\sqcup^{\infty}$ and since α^{∂} is $\cup$-preserving. This is equal to $\bigcup_{i \in \Delta}(\alpha^{\partial}(\{\langle s, s'\rangle \mid \langle s, \bot\rangle \notin X_i \wedge \langle s, s'\rangle \in X_i\})) \cup (\alpha^{\partial}(\bigcap_{i \in \Delta}\{\langle s, \bot\rangle \mid \langle s, \bot\rangle \in X_i\})) = \bigcup_{i \in \Delta}\{\langle s, s'\rangle \mid \langle s, \bot\rangle \notin X_i \wedge \langle s, s'\rangle \in X_i\} \cup \{\langle s, s'\rangle \mid \forall i \in \Delta : \langle s, \bot\rangle \in X_i \wedge s' \in \Sigma_{\bot}\}$ by definition of α^{∂}.

The same way, the meet is $\bigsqcap^{\partial}_{i \in \Delta} X_i = \alpha^{\partial}(\bigsqcap^{\infty}_{i \in \Delta} \gamma^{\overline{\partial}}(X_i)) = \{\langle s, s'\rangle \mid (\forall i \in \Delta : \langle s, \bot\rangle \notin X_i \wedge \langle s, s'\rangle \in X_i) \vee (\exists i \in \Delta : \langle s, \bot\rangle \in X_i \wedge s' \in \Sigma_{\bot})\}$.

α^{∂} is not $\sqcup^{\infty}$-preserving. A counter example for $\Sigma = \{a, b\}$ is $\alpha^{\partial}(\{\langle a, a\rangle\} \sqcup^{\infty} \{\langle a, b\rangle, \langle a, \bot\rangle\}) = \alpha^{\partial}(\{\langle a, a\rangle, \langle a, b\rangle\}) = \{\langle a, a\rangle, \langle a, b\rangle\}$ whereas $\alpha^{\partial}(\{\langle a, a\rangle\}) \sqcup^{\partial} \alpha^{\partial}(\{\langle a, b\rangle, \langle a, \bot\rangle\}) = \{\langle a, a\rangle\} \sqcup^{\partial} \{\langle a, a\rangle, \langle a, b\rangle, \langle a, \bot\rangle\} = \{\langle a, a\rangle\}$. However α^{∂} is Scott-continuous. To prove this, let X_i, $i < \delta$ be a $\sqsubseteq^{\infty}$-increasing chain. By definition of $\sqcup^{\infty}$, α^{∂} is $\cup$-preserving and definition of α^{∂}, we have $\alpha^{\partial}(\bigsqcup^{\infty}_{i<\delta} X_i) = \alpha^{\partial}(\bigcup_{i<\delta} X_i \cap (\Sigma \times \Sigma) \cup \bigcap_{i<\delta} X_i \cap (\Sigma \times \{\bot\})) = \bigcup_{i<\delta} \alpha^{\partial}(X_i \cap (\Sigma \times \Sigma)) \cup \alpha^{\partial}(\bigcap_{i<\delta} X_i \cap (\Sigma \times \{\bot\}) = A \cup B$ where $A = \{\langle s, s'\rangle \mid \exists i < \delta : \langle s, s'\rangle \in X_i \cap (\Sigma \times \Sigma)\}$ and $B = \{\langle s, s'\rangle \mid \forall i < \delta : \langle s, \bot\rangle \in X_i \wedge s' \in \Sigma_{\bot}\}$. Let $A' = \{\langle s, s'\rangle \mid \exists i < \delta : \langle s, \bot\rangle \notin X_i \wedge \langle s, s'\rangle \in X_i\}$

so that $A' \subseteq A$ whence $A' \cup B \subseteq A \cup B$. Reciprocally, if $\langle s,\, s'\rangle \in A$ then there exists $i < \delta$ such that $\langle s,\, s'\rangle \in X_i \cap (\Sigma \times \Sigma)$. Either $\forall j < \delta : \langle s,\, \bot\rangle \in X_j$ in which case $\langle s,\, s'\rangle \in B$ or $\exists j < \delta : \langle s,\, \bot\rangle \notin X_j$. X_k, $k < \delta$ is a $\sqsubseteq^\infty$-increasing chain so that if $i \leq j$ then $\langle s,\, s'\rangle \in X_j$ since $X_k \cap (\Sigma \times \Sigma)$, $k < \delta$ is $\subseteq$-increasing so that $\langle s,\, s'\rangle \in A'$. Otherwise $j < i$, in which case $X_k \cap (\Sigma \times \{\bot\})$, $k < \delta$ is $\subseteq$-decreasing so that $\langle s,\, \bot\rangle \notin X_i$ which again implies $\langle s,\, s'\rangle \in A'$. By antisymmetry, we have $A \cup B = A' \cup B = \{\langle s,\, s'\rangle \mid \exists i < \delta : \langle s,\, \bot\rangle \notin \alpha^\partial(X_i) \wedge \langle s,\, s'\rangle \in \alpha^\partial(X_i)\} \cup \{\langle s,\, s'\rangle \mid \forall i < \delta : \langle s,\, \bot\rangle \notin \alpha^\partial(X_i) \wedge s' \in \Sigma_\bot\}$ since $\langle s,\, \bot\rangle \in X_i \Longleftrightarrow \langle s,\, \bot\rangle \in \alpha^\partial(X_i)$ and $\langle s,\, s'\rangle \in X_i \Longleftrightarrow \langle s,\, s'\rangle \in \alpha^\partial(X_i)$ whenever $\langle s,\, \bot\rangle \notin X_i$. This is equal to $\bigsqcup^\partial_{i<\delta} \alpha^\partial(X_i)$ proving Scott-continuity.

By definition of F^∞, α^∂, $\bar{\tau}$ and $\circ$, we have $\alpha^\partial \circ F^\infty(X) = \alpha^\partial(\bar{\tau} \cup \tau \circ X) = \bar{\tau} \cup \tau \circ X \cup \{\langle s,\, s'\rangle \mid \langle s,\, \bot\rangle \in \bar{\tau} \cup \tau \circ X \wedge s' \in \Sigma\} = \bar{\tau} \cup \tau \circ X \cup \{\langle s,\, s'\rangle \mid \langle s,\, \bot\rangle \in \tau \circ X \wedge s' \in \Sigma\} = \bar{\tau} \cup \tau \circ X \cup \tau \circ \{\langle s'',\, s'\rangle \mid \langle s'',\, \bot\rangle \in X \wedge s' \in \Sigma\} = \bar{\tau} \cup \tau \circ (X \cup \{\langle s'',\, s'\rangle \mid \langle s'',\, \bot\rangle \in X \wedge s' \in \Sigma\}) = \bar{\tau} \cup \tau \circ \alpha^\partial(X) = F^\partial \circ \alpha^\partial(X)$ by defining $F^\partial(X) \triangleq \bar{\tau} \cup \tau \circ X$.

If $X \sqsubseteq^\partial Y$ then $\forall s \in \Sigma : \langle s,\, \bot\rangle \in X \vee (\langle s,\, \bot\rangle \notin Y \wedge X \cap (\{s\} \times \Sigma) \subseteq Y \cap (\{s\} \times \Sigma))$ which implies $\forall s' \in \Sigma : \langle s',\, \bot\rangle \in \bar{\tau} \cup \tau \circ X \vee (\langle s',\, \bot\rangle \notin \bar{\tau} \cup \tau \circ Y \wedge (\bar{\tau} \cup \tau \circ X) \cap (\{s'\} \times \Sigma) \subseteq (\bar{\tau} \cup \tau \circ Y) \cap (\{s'\} \times \Sigma))$ that is $F^\partial(X) \sqsubseteq^\partial F^\partial(Y)$ so that F^∂ is monotone.

By definition of τ^∂, fixpoint characterization of the natural relational semantics 7.5 and S. Kleene fixpoint transfer theorem 2.3, we conclude that $\tau^\partial \triangleq \alpha^\partial(\tau^\infty) = \alpha^\partial(\mathrm{lfp}^{\sqsubseteq^\infty}_{\bot^\infty} F^\infty) = \mathrm{lfp}^{\sqsubseteq^\partial}_{\bot^\partial} F^\partial$. □

Lemma 7.10 (Arrangement of the iterates of F^∂) *Let F^{∂^β}, $\beta \in \mathbb{O}$ be the iterates of F^∂ from $\bot^\partial$. For all $\eta < \xi$, $s, s' \in \Sigma$, if $\langle s,\, s'\rangle \in F^{\partial^\xi}$ and $\langle s,\, s'\rangle \notin F^{\partial^\eta}$ then $\forall s' \in \Sigma_\bot : \langle s,\, s'\rangle \in F^{\partial^\eta}$.*

Proof. Follows from lemma 7.6 and the proof of theorem 7.9, showing by S. Kleene fixpoint theorem 2.3 that $\forall \beta \in \mathbb{O} : F^{\partial^\beta} = \alpha^\partial(F^{\infty^\beta})$. □

Lemma 7.11 (Totality of the iterates of F^∂) *Let F^{∂^β}, $\beta \in \mathbb{O}$ be the iterates of F^∂ from $\bot^\partial$. $\forall \beta \in \mathbb{O} : \forall s \in \Sigma : \exists s' \in \Sigma_\bot : \langle s,\, s'\rangle \in F^{\partial^\delta}$.*

Proof. Follows from lemma 7.7 and the proof of theorem 7.9, showing by S. Kleene fixpoint theorem 2.3 that $\forall \beta \in \mathbb{O} : F^{\partial^\beta} = \alpha^\partial(F^{\infty^\beta})$. □

Lemma 7.12 (Final states of the iterates of F^∂) *Let F^{∂^β}, $\beta \in \mathbb{O}$ be the iterates of F^∂ from $\bot^\partial$. $\forall \beta \in \mathbb{O} : \forall s, s' \in \Sigma : (\langle s,\, s'\rangle \in F^{\partial^\beta} \wedge \langle s,\, \bot\rangle \notin F^{\partial^\beta}) \Longrightarrow (s' \in \check{\tau}) \wedge (\forall s'' \in \Sigma_\bot : \langle s',\, s''\rangle \in F^{\partial^\delta} \Longrightarrow s'' = s')$.*

Proof. The proof of theorem 7.9 shows, by S. Kleene fixpoint theorem 2.3, that $\forall \beta \in \mathbb{O} : F^{\partial^\beta} = \alpha^\partial(F^{\infty^\beta})$. So if $\langle s,\, \bot\rangle \notin F^{\partial^\beta}$ then $\langle s,\, s'\rangle \in F^{\partial^\beta}$ implies $\langle s,\, s'\rangle \in F^{\infty^\beta}$ by definition of α^∂ whence $s' \in \check{\tau}$ by lemma 7.8. We have $\langle s',\, \bot\rangle \notin F^{\partial^\beta}$ since otherwise $\langle s',\, \bot\rangle \in F^{\infty^\beta}$ which is impossible by lemma 7.8 since $s' \neq \bot$. So if $s'' \in \Sigma_\bot$ then $\langle s',\, s''\rangle \in F^{\partial^\beta}$ implies $\langle s',\, s''\rangle \in F^{\infty^\beta}$ since $\langle s',\, \bot\rangle \notin F^{\infty^\beta}$ so that $s'' = s'$ by lemma 7.8. □

In order to place the demoniac relational semantics τ^∂ in the hierarchy of semantics, we will use the following:

Theorem 7.13 $\tau^{\omega} = \alpha^{\partial\,\omega}(\tau^{\partial})$ *where* $\alpha^{\partial\,\omega}(X) \triangleq X \cap (\Sigma \times \{\bot\})$.

Proof. By definition of $\alpha^{\partial\,\omega}$, τ^{∂}, τ^{∞}, α^{∂}, $\tau^{+} \subseteq \Sigma \times \Sigma$, $\bot \not\in \Sigma$ and $\tau^{\omega} \subseteq \Sigma \times \{\bot\}$, we have $\alpha^{\partial\,\omega}(\tau^{\partial}) = \tau^{\partial} \cap (\Sigma \times \{\bot\}) = \alpha^{\partial}(\tau^{\infty}) \cap (\Sigma \times \{\bot\}) = (\tau^{+} \cup \tau^{\omega} \cup \{\langle s, s'\rangle \mid \langle s,\ \bot\rangle \in \tau^{+} \cup \tau^{\omega} \wedge s' \in \Sigma\}) \cap (\Sigma \times \{\bot\}) = \tau^{\omega} \cup \{\langle s,\ \bot\rangle \mid \langle s,\ \bot\rangle \in \tau^{\omega}\} = \tau^{\omega}$. □

8 Denotational Semantics

In contrast to operational semantics, denotational semantics abstracts away from the history of computations by considering input-output functions [36]. For that purpose, given any partial order $\leqslant$ on $\wp(\mathcal{D} \times \mathcal{E})$, we use the right-image isomorphism: $\langle \wp(\mathcal{D} \times \mathcal{E}),\ \leqslant\rangle \underset{\alpha^{\blacktriangleright}}{\overset{\gamma^{\blacktriangleright}}{\leftrightarrows}} \langle \mathcal{D} \longmapsto \wp(\mathcal{E}),\ \dot{\leqslant}\rangle$ where $\alpha^{\blacktriangleright}(R) \triangleq R^{\blacktriangleright} = \lambda x \centerdot \{y \mid \langle x,\ y\rangle \in R\}$, $\gamma^{\blacktriangleright}(f) \triangleq \{\langle x,\ y\rangle \mid y \in f(x)\}$ and $f \mathrel{\dot{\leqslant}} g \triangleq \gamma^{\blacktriangleright}(f) \leqslant \gamma^{\blacktriangleright}(g)$.

8.1 Nondeterministic Denotational Semantics

Our initial goal was to derive the nondeterministic denotational semantics of [2] by abstract interpretation of the trace semantics (in a succinct form, using transition systems instead of imperative iterative programs). Surprisingly enough, we obtain *new* fixpoint characterizations using different partial orderings.

8.1.1 Natural Nondeterministic Denotational Semantics

The *natural nondeterministic denotational semantics* is defined as the right-image abstraction $\tau^{\natural} \triangleq \alpha^{\blacktriangleright}(\tau^{\infty})$ of the natural relational semantics τ^{∞}. By the fixpoint characterization 7.5 of τ^{∞} and S. Kleene fixpoint transfer theorem 2.3, we derive a fixpoint characterization of the fixpoint natural nondeterministic denotational semantics (where $\dot{\check{\tau}} \triangleq \lambda s \centerdot \{s \mid \forall s' \in \Sigma : \neg(s\ \tau\ s')\}$):

Theorem 8.1 (Fixpoint natural nondeterministic denotational semantics) $\tau^{\natural} = \mathrm{lfp}_{\dot{\bot}^{\natural}}^{\dot{\sqsubseteq}^{\natural}}\, F^{\natural}$ *where* $\dot{D}^{\natural} \triangleq \Sigma \longmapsto \wp(\Sigma_{\bot})$, $F^{\natural} \in \dot{D}^{\natural} \overset{m}{\longmapsto} \dot{D}^{\natural}$ *defined as* $F^{\natural}(f) \triangleq \dot{\check{\tau}}\ \dot{\cup}\ \bigcup f^{\blacktriangleright} \circ \tau^{\bullet\blacktriangleright}$ *is a* $\dot{\sqsubseteq}^{\natural}$*-monotone map on the complete lattice* $\langle \dot{D}^{\natural},\ \dot{\sqsubseteq}^{\natural},\ \dot{\bot}^{\natural},\ \dot{\top}^{\natural},\ \dot{\sqcup}^{\natural},\ \dot{\sqcap}^{\natural}\rangle$ *which is the pointwise extension of the complete lattice* $\langle D^{\natural},\ \sqsubseteq^{\natural},\ \bot^{\natural},\ \top^{\natural},\ \sqcup^{\natural},\ \sqcap^{\natural}\rangle$ *with* $D^{\natural} \triangleq \wp(\Sigma_{\bot})$, $X \sqsubseteq^{\natural} Y \triangleq X^{+} \subseteq Y^{+} \wedge X^{\omega} \supseteq Y^{\omega}$, $X^{+} \triangleq X \cap \top^{\natural}$, $\top^{\natural} \triangleq \Sigma$, $X^{\omega} \triangleq X \cap \bot^{\natural}$ *and* $\bot^{\natural} \triangleq \{\bot\}$.

Proof. The order structure of $\Sigma \longmapsto \wp(\Sigma_{\bot})$ is chosen to be $\langle \alpha^{\blacktriangleright},\ \gamma^{\blacktriangleright}\rangle$-isomorphic to the complete lattice $\langle \wp(\Sigma \times \Sigma_{\bot}),\ \sqsubseteq^{\infty},\ \bot^{\infty},\ \top^{\infty},\ \sqcup^{\infty},\ \sqcap^{\infty}\rangle$ of theorem 7.5. Therefore we have a complete lattice $\langle \Sigma \longmapsto \wp(\Sigma_{\bot}),\ \dot{\sqsubseteq}^{\natural},\ \dot{\bot}^{\natural},\ \dot{\top}^{\natural},\ \dot{\sqcup}^{\natural},\ \dot{\sqcap}^{\natural}\rangle$ such that the infimum is $\dot{\bot}^{\natural} \triangleq \alpha^{\blacktriangleright}(\bot^{\infty}) = \alpha^{\blacktriangleright}(\Sigma \times \{\bot\}) = \lambda s \centerdot \bot^{\natural}$ where $\bot^{\natural} \triangleq \{\bot\}$. The supremum is $\dot{\top}^{\natural} \triangleq \alpha^{\blacktriangleright}(\top^{\infty}) = \alpha^{\blacktriangleright}(\Sigma \times \Sigma) = \lambda s \centerdot \top^{\natural}$ where $\top^{\natural} \triangleq \Sigma$.

The partial order is $f \mathrel{\dot{\sqsubseteq}^{\natural}} g \triangleq \gamma^{\blacktriangleright}(f) \sqsubseteq^{\infty} \gamma^{\blacktriangleright}(g) = \{\langle s,\ s'\rangle \mid s' \in f(s) \cap \Sigma\} \subseteq \{\langle s, s'\rangle \mid s' \in g(s) \cap \Sigma\} \wedge \{\langle s, s'\rangle \mid s' \in f(s) \cap \{\bot\}\} \supseteq \{\langle s, s'\rangle \mid s' \in g(s) \cap \{\bot\}\} =$

$\forall s \in \Sigma : f(s) \cap \Sigma \subseteq g(s) \cap \Sigma \wedge f(s) \cap \{\bot\} \supseteq g(s) \cap \{\bot\} = \forall s \in \Sigma : f(s) \sqsubseteq^\natural g(s)$ by defining $X \sqsubseteq^\natural Y \triangleq X^+ \subseteq Y^+ \wedge X^\omega \supseteq Y^\omega$, $X^+ \triangleq X \cap \top^\natural$ and $X^\omega \triangleq X \cap \bot^\natural$.

For the lub, we have $\alpha^\blacktriangleright(\bigcup_i X_i) = \dot{\bigcup_i} \alpha^\blacktriangleright(X_i)$, $\alpha^\blacktriangleright(\bigcap_i X_i) = \dot{\bigcap_i} \alpha^\blacktriangleright(X_i)$, $\alpha^\blacktriangleright(X^+) = X \dot\cap \dot\top^\natural$ and $\alpha^\blacktriangleright(X^\omega) = X \dot\cap \dot\bot^\natural$ whence $\alpha^\blacktriangleright(\bigsqcup_i^\infty X_i) = \alpha^\blacktriangleright(\bigcup_i X_i{}^+ \cup \bigcap_i X_i{}^\omega) = \dot{\bigcup_i} (\alpha^\blacktriangleright(X_i))^+ \dot\cup \dot{\bigcap_i} (\alpha^\blacktriangleright(X_i))^\omega) = \dot{\bigsqcup_i}^\natural \alpha^\blacktriangleright(X_i)$ pointwise, by defining $\bigsqcup_i^\natural X_i \triangleq \bigcup_i X_i{}^+ \cup \bigcap_i X_i{}^\omega$.

We design the semantic transformer $F^\natural$, using the commutation requirement: $\alpha^\blacktriangleright \circ F^\infty(X) = \alpha^\blacktriangleright(\bar\tau \cup \tau \circ X) = \alpha^\blacktriangleright(\bar\tau) \dot\cup \alpha^\blacktriangleright(\tau \circ X) = \lambda s \bullet \{s' \mid \langle s, s'\rangle \in \bar\tau\} \dot\cup \lambda s \bullet \{s'' \mid \langle s, s''\rangle \in \tau \circ X\} = \lambda s \bullet \{s \mid \forall s' : \neg(s \;\tau\; s')\} \cup \{s'' \mid \exists s' \in \Sigma : s \;\tau\; s" \wedge \langle s', s''\rangle \in X\} = \lambda s \bullet \{s \mid \forall s' : \neg(s \;\tau\; s')\} \cup \{s'' \mid \exists s' \in \Sigma : s \;\tau\; s" \wedge s'' \in \alpha^\blacktriangleright(X)(s')\} = F^\natural \circ \alpha^\blacktriangleright(X)$ by defining $F^\natural(f) \triangleq \lambda s \bullet \{s \mid \forall s' \in \Sigma : \neg(s \;\tau\; s')\} \cup \{s'' \mid \exists s' \in \Sigma : s \;\tau\; s' \wedge s'' \in f(s')\} = \dot{\check\tau} \;\dot\cup\; \lambda s \bullet \bigcup\{f(s') \mid s \;\tau\; s'\} = \dot{\check\tau} \;\dot\cup\; \dot{\bigcup} \lambda s \bullet \{f(s') \mid s' \in \tau^{\bullet\!\blacktriangleright}(s)\} = \dot{\check\tau} \;\dot\cup\; \dot{\bigcup} f^\blacktriangleright \circ \tau^{\bullet\!\blacktriangleright}$.

If $f \;\dot\sqsubseteq^\natural\; g$ then $\forall s \in \Sigma : f(s) \sqsubseteq^\natural g(s)$ that is $\forall s \in \Sigma : f(s) \cap \Sigma \subseteq g(s) \cap \Sigma \wedge f(s) \cap \{\bot\} \supseteq g(s) \cap \{\bot\}$. By definition of $F^\natural$, we have $F^\natural(f)s \cap \Sigma = \{s \mid \forall s' \in \Sigma : \neg(s \;\tau\; s')\} \cup \{s'' \mid \exists s' \in \Sigma : s \;\tau\; s' \wedge s'' \in f(s') \cap \Sigma\} \subseteq \{s \mid \forall s' \in \Sigma : \neg(s \;\tau\; s')\} \cup \{s'' \mid \exists s' \in \Sigma : s \;\tau\; s' \wedge s'' \in g(s') \cap \Sigma\} = F^\natural(g)s \cap \Sigma$ and $F^\natural(f)s \cap \{\bot\} = \{\bot \mid \exists s' \in \Sigma : s \;\tau\; s' \wedge \bot \in f(s') \cap \{\bot\}\} \supseteq \{\bot \mid \exists s' \in \Sigma : s \;\tau\; s' \wedge \bot \in g(s') \cap \{\bot\}\} = F^\natural(g)s \cap \{\bot\}$ so that $\forall s \in \Sigma : F^\natural(f)s \sqsubseteq^\natural F^\natural(g)s$ proving $F^\natural(f) \;\dot\sqsubseteq^\natural\; F^\natural(g)$ hence that $F^\natural$ is monotone. □

Lemma 8.2 (Arrangement of the iterates of $F^\natural$) *Let $F^{\natural\delta}$, $\delta \in \mathbb{O}$ be the iterates of $F^\natural$ from $\bot^\natural$. For all $\eta < \xi$, $s, s' \in \Sigma$, if $s' \in F^{\natural\xi}(s)$ and $s' \notin F^{\natural\eta}(s)$ then $\bot \in F^{\natural\eta}(s)$.*

Proof. Follows from lemma 7.6 and the proof of theorem 8.1, showing by S. Kleene fixpoint theorem 2.3 that $\forall \delta \in \mathbb{O} : F^{\natural\delta} = \alpha^\blacktriangleright(F^{\infty\delta})$. □

Lemma 8.3 (Totality of the iterates of $F^\natural$) *Let $F^{\natural\delta}$, $\delta \in \mathbb{O}$ be the iterates of $F^\natural$ from $\bot^\natural$. $\forall \delta \in \mathbb{O} : \forall s \in \Sigma : F^{\natural\delta}(s) \neq \emptyset$.*

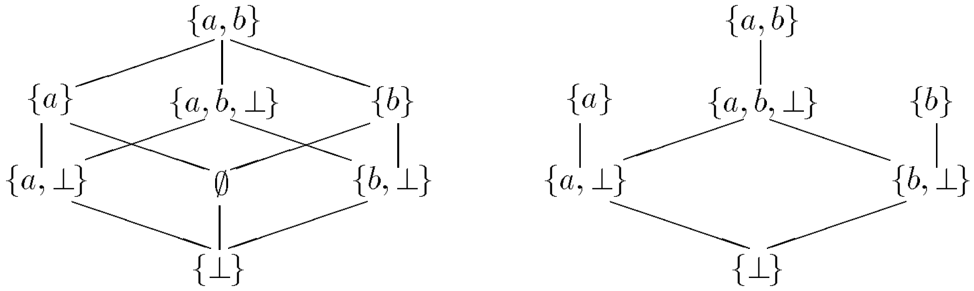
Proof. Follows from lemma 7.7 and the proof of theorem 8.1, showing by S. Kleene fixpoint theorem 2.3 that $\forall \delta \in \mathbb{O} : F^{\natural\delta} = \alpha^\blacktriangleright(F^{\infty\delta})$. □

Lemma 8.4 (Final states of the iterates of $F^\natural$) *Let $F^{\natural\delta}$, $\delta \in \mathbb{O}$ be the iterates of $F^\natural$ from $\bot^\natural$. $\forall \delta \in \mathbb{O} : \forall s, s' \in \Sigma : (s' \in F^{\natural\delta}(s) \wedge \bot \notin F^{\natural\delta}(s)) \Longrightarrow (s' \in \check\tau \wedge F^{\natural\delta}(s') = \{s'\})$.*

Proof. Follows from lemma 7.8 and the proof of theorem 8.1, showing by S. Kleene fixpoint theorem 2.3 that $\forall \delta \in \mathbb{O} : F^{\natural\delta} = \alpha^\blacktriangleright(F^{\infty\delta})$. □

8.1.2 Convex/Plotkin Nondeterministic Denotational Semantics

Unexpectedly, the natural semantic domain $D^\natural = \wp(\Sigma_\bot)$ with the mixed ordering $\sqsubseteq^\natural$ differs from the usual convex/Plotkin powerdomain with Egli-Milner ordering $\sqsubseteq^{\mathrm{EM}}$ [22] (see figure 2). Apart from the presence of $\emptyset$ (which can be easily eliminated), the difference is that $\sqsubseteq^{\mathrm{EM}} \subsetneq \sqsubseteq^\natural$ which can be useful, e.g.



Mixed ordering $\sqsubseteq^{\natural}$ Egli-Milner ordering $\sqsubseteq^{\mathrm{EM}}$

Fig. 2.

to define the semantics of the parallel **or** as $[\![f \textbf{ or } g]\!] \triangleq \lambda\rho\bullet [\![f]\!]\rho \sqcup^{\natural} [\![g]\!]\rho$ [5].

We let $(c_1 \; ? \; v_1 \; | \; c_2 \; ? \; v_2 \; | \; \ldots \; \text{¿} \; w)$ be v_1 if condition c_1 holds else v_2 if condition c_2 holds, etc. and w otherwise. Let us recall [2, fact 2.4] that G. Plotkin convex powerdomain $\langle D^{\mathrm{EM}}, \sqsubseteq^{\mathrm{EM}}, \bot^{\mathrm{EM}}, \sqcup^{\mathrm{EM}}\rangle$ is the DCPO $\{A \subseteq \Sigma_\bot \mid A \neq \emptyset\}$ with Egli-Milner ordering $A \sqsubseteq^{\mathrm{EM}} B \triangleq \forall a \in A : \exists b \in B : a \sqsubseteq^{\mathrm{D}} b \wedge \forall b \in B : \exists a \in A : a \sqsubseteq^{\mathrm{D}} b$ based upon D. Scott flat ordering $\forall x \in \Sigma_\bot : \bot \sqsubseteq^{\mathrm{D}} x \sqsubseteq^{\mathrm{D}} x$ such that $A \sqsubseteq^{\mathrm{EM}} B \Longleftrightarrow (\bot \in A \; ? \; A \setminus \{\bot\} \subseteq B \; \text{¿} \; A = B)$, with infimum $\bot^{\mathrm{EM}} \triangleq \{\bot\}$ and lub of increasing chains $\bigsqcup^{\mathrm{EM}}_{i\in\Delta} X_i \triangleq (\bigcup_{i\in\Delta} X_i \setminus \{\bot\}) \cup \{\bot \mid \forall i \in \Delta : \bot \in X_i\}$. Applying the fixpoint iterates reordering theorem 2.9 to theorem 8.1, we get [2]:

Corollary 8.5 (G. Plotkin fixpoint nondeterministic denotational semantics) $\tau^{\natural} = \mathrm{lfp}^{\dot{\sqsubseteq}^{\mathrm{EM}}}_{\dot{\bot}^{\mathrm{EM}}} F^{\natural}$ *where* $F^{\natural}$ *is a* $\dot{\sqsubseteq}^{\mathrm{EM}}$*-monotone map on the pointwise extension* $\langle \dot{D}^{\mathrm{EM}}, \dot{\sqsubseteq}^{\mathrm{EM}}, \dot{\bot}^{\mathrm{EM}}, \dot{\sqcup}^{\mathrm{EM}}\rangle$ *of G. Plotkin convex powerdomain* $\langle D^{\mathrm{EM}}, \sqsubseteq^{\mathrm{EM}}, \bot^{\mathrm{EM}}, \sqcup^{\mathrm{EM}}\rangle$*.*

Proof. We apply theorem 2.9 with $E = \dot{D}^{\mathrm{EM}} = \Sigma \longmapsto \wp(\Sigma_\bot) \setminus \{\lambda s\bullet \emptyset\}$.

$\dot{\sqsubseteq}^{\mathrm{EM}}$ is a preorder on $\dot{D}^{\mathrm{EM}}$.

By lemma 8.3, no iterate $F^{\natural^\delta}$, $\delta \in \mathbb{O}$ of $F^{\natural}$ from $\dot{\bot}^{\natural}$ is $\lambda s\bullet \emptyset$.

$\dot{\bot}^{\natural} = \lambda s\bullet\{\bot\}$ is the infimum of $\langle \dot{D}^{\mathrm{EM}}, \dot{\sqsubseteq}^{\mathrm{EM}}\rangle$.

If $f \; \dot{\sqsubseteq}^{\mathrm{EM}} \; g$ then $\forall s \in \Sigma : (\bot \in F(s) \; ? \; f(s) \setminus \{\bot\} \subseteq g(s) \; \text{¿} \; f(s) = g(s))$ so that we must show that $\forall s \in \Sigma : F^{\natural}(f)s \sqsubseteq^{\mathrm{EM}} F^{\natural}(g)s \Longleftrightarrow \forall s \in \Sigma : \dot{\check{\tau}}(s) \cup \bigcup f^{\blacktriangleright} \circ \tau^{\bullet\!\!\rightarrow}(s) \sqsubseteq^{\mathrm{EM}} \dot{\check{\tau}}(s) \cup \bigcup g^{\blacktriangleright} \circ \tau^{\bullet\!\!\rightarrow}(s) \Longleftrightarrow \forall s \in \Sigma : (\bot \in \bigcup\{f(s') \mid s \; \tau \; s'\} \; ? \; \bigcup\{f(s') \mid s \; \tau \; s'\} \setminus \{\bot\} \subseteq \bigcup\{g(s') \mid s \; \tau \; s'\} \; \text{¿} \; \bigcup\{f(s') \mid s \; \tau \; s'\} = \bigcup\{g(s') \mid s \; \tau \; s'\})$. Let us consider any $s' \in \Sigma$ such that $s \; \tau \; s'$. If $\bot \in f(s')$ then $f(s') \setminus \{\bot\} \subseteq g(s')$ else $f(s') = g(s')$ so that in both cases $f(s') \setminus \{\bot\} \subseteq g(s')$. It follows that $\bigcup\{f(s') \mid s \; \tau \; s'\} \setminus \{\bot\} \subseteq \bigcup\{g(s') \mid s \; \tau \; s'\}$ proving $F^{\natural}(f)s \sqsubseteq^{\mathrm{EM}} F^{\natural}(g)s$ in case $\bot \in \bigcup\{f(s') \mid s \; \tau \; s'\}$. Otherwise, $\forall s' \in \Sigma : s \; \tau \; s' \Longrightarrow \bot \notin f(s')$ hence $f(s') = g(s')$ so that $\bigcup\{f(s') \mid s \; \tau \; s'\} = \bigcup\{g(s') \mid s \; \tau \; s'\}$ and again $F^{\natural}(f)s \sqsubseteq^{\mathrm{EM}} F^{\natural}(g)s$. It follows that $F^{\natural}$ hence $F^{\natural}|_{\dot{D}^{\mathrm{EM}}}$ is $\dot{\sqsubseteq}^{\mathrm{EM}}$-monotonic.

In order to prove that for all $g \in \dot{D}^{\mathrm{EM}}$, if λ is a limit ordinal and $\forall \delta <$

[5] Observe that $\sqcup^{\natural}$ is monotonic for $\sqsubseteq^{\natural}$ which is not in contradiction with [6] since by lemma 8.3 failure is excluded i.e. would have to be explicitly denoted by $\Omega \notin \Sigma$.

$\lambda : F^{\natural\delta} \mathrel{\dot{\sqsubseteq}^{\mathrm{EM}}} g$ then $\dot{\bigsqcup\limits_{\delta<\lambda}}^{\natural} F^{\natural\delta} \mathrel{\dot{\sqsubseteq}^{\mathrm{EM}}} g$, let us assume that $\forall s \in \Sigma : \forall \delta < \lambda : F^{\natural\delta}(s) \sqsubseteq^{\mathrm{EM}} g(s)$ that is $(\bot \in F^{\natural\delta}(s)\ ?\ F^{\natural\delta}(s) \setminus \{\bot\} \subseteq g(s)$ ¿ $F^{\natural\delta}(s) = g(s))$. We have $\bigsqcup\limits_{\delta<\lambda}^{\natural} F^{\natural\delta}(s) = (\bigcup\limits_{\delta<\lambda} F^{\natural\delta}(s) \cap \Sigma) \cup (\bigcap\limits_{\delta<\lambda} F^{\natural\delta}(s) \cap \{\bot\})$

A. If $\bot \in \bigsqcup\limits_{\delta<\lambda}^{\natural} F^{\natural\delta}(s)$ then $\forall \delta < \lambda : \bot \in F^{\natural\delta}(s)$ which implies $\forall \delta < \lambda : F^{\natural\delta}(s) \setminus \{\bot\} \subseteq g(s)$ since $F^{\natural\delta}(s) \sqsubseteq^{\mathrm{EM}} g(s)$. Therefore $(\bigcup\limits_{\delta<\lambda} F^{\natural\delta}(s)) \setminus \{\bot\} \subseteq g(s)$ hence $(\bigsqcup\limits_{\delta<\lambda}^{\natural} F^{\natural\delta}(s)) \setminus \{\bot\} \subseteq g(s)$ proving $\bigsqcup\limits_{\delta<\lambda}^{\natural} F^{\natural\delta}(s) \sqsubseteq^{\natural} g(s)$.

B. If $\bot \notin \bigsqcup\limits_{\delta<\lambda}^{\natural} F^{\natural\delta}(s)$ then there exists $\eta' < \lambda : \bot \notin F^{\natural\eta'}(s)$. Moreover $F^{\natural\eta'}(s) = g(s)$ since $F^{\natural\eta'}(s) \sqsubseteq^{\natural} g(s)$. Let $\eta > 0$ be the least such η' ($\eta \neq 0$ since $F^{\natural 0}(s) = \{\bot\}$). For all $\delta \leq \eta$, we have $F^{\natural\delta} \cap \Sigma \subseteq F^{\natural\eta}(s) \cap \Sigma = g(s)$ so that $\bigcup\limits_{\delta\leq\eta} F^{\natural\delta}(s) \cap \Sigma = g(s)$. Now if $\eta \leq \delta < \lambda$ then $g(s) = F^{\natural\eta}(s) \cap \Sigma \subseteq F^{\natural\delta}(s) \cap \Sigma$ so that by reductio ad absurdum $F^{\natural\delta}(s) \cap \Sigma \neq g(s)$ would imply $\exists s' \in \Sigma : s' \in F^{\natural\delta}(s) \cap \Sigma \wedge s' \notin F^{\natural\eta}(s) \cap \Sigma$ so $\exists s' \in \Sigma : s' \in F^{\natural\delta}(s) \wedge s' \notin F^{\natural\eta}(s)$ and $\delta \neq \eta$, whence $\eta < \delta$ proving, by the lemma 7.6 that $\bot \in F^{\natural\eta}(s)$, a contradiction. For all δ such that $\eta \leq \delta < \lambda$, we have $F^{\natural\delta}(s) \cap \Sigma = g(s)$ so that $\bigcup\limits_{\delta<\lambda} F^{\natural\delta}(s) \cap \Sigma = g(s)$ whence $\bigsqcup\limits_{\delta<\lambda} F^{\natural\delta}(s) \sqsubseteq^{\mathrm{EM}} g(s)$.

By theorems 8.1 and 2.9, we conclude that $\tau^{\natural} = \mathrm{lfp}_{\dot{\bot}^{\natural}}^{\dot{\sqsubseteq}^{\natural}} F^{\natural} = \mathrm{lfp}_{\dot{\bot}^{\mathrm{EM}}}^{\dot{\sqsubseteq}^{\mathrm{EM}}} F^{\natural}$. □

8.1.3 Demoniac Nondeterministic Denotational Semantics

The *demoniac nondeterministic denotational semantics* is the right-image abstraction $\tau^{\sharp} \triangleq \alpha^{\blacktriangleright}(\tau^{\partial})$ of the demoniac relational semantics τ^{∂}.

In order to place the demoniac nondeterministic denotational semantics $\tau^{\sharp}$ in the hierarchy of semantics, we will use the following:

Theorem 8.6 (Denotational demoniac abstraction) $\tau^{\sharp} = \alpha^{\sharp}(\tau^{\natural})$ *where* $\alpha^{\sharp}(f) \triangleq \lambda s \boldsymbol{\cdot} f(s) \cup \{s' \in \Sigma \mid \bot \in f(s)\}$ *and* $\gamma^{\sharp}(g) \triangleq g$ *satisfies* $\langle \Sigma \longmapsto \wp(\Sigma_{\bot}), \dot{\subseteq}\rangle \underset{\alpha^{\sharp}}{\overset{\gamma^{\sharp}}{\leftrightarrows\!\!\!\!\twoheadrightarrow}} \langle \Sigma \longmapsto (\wp(\Sigma) \cup \{\Sigma_{\bot}\}), \dot{\subseteq}\rangle$.

Proof. $\alpha^{\sharp}(f) \mathrel{\dot{\subseteq}} g \iff \forall s \in \Sigma : f(s) \cup \{s' \in \Sigma \mid \bot \in f(s)\} \subseteq g(s) \Longrightarrow \forall s \in \Sigma : f(s) \subseteq g(s) \iff f \mathrel{\dot{\subseteq}} \gamma^{\sharp}(g)$. Reciprocally, if $\forall s \in \Sigma : f(s) \subseteq g(s)$ then either $\bot \in g(s)$ so $g(s) = \Sigma_{\bot}$ hence $\alpha^{\sharp}(f)s \mathrel{\dot{\subseteq}} g(s)$ or $\bot \notin g(s)$ hence $\bot \notin f(s)$ and again $\alpha^{\sharp}(f)s \mathrel{\dot{\subseteq}} g(s)$ proving $\alpha^{\sharp}(f) \mathrel{\dot{\subseteq}} g$. We conclude that $\langle \Sigma \longmapsto \wp(\Sigma_{\bot}), \dot{\subseteq}\rangle \underset{\alpha^{\sharp}}{\overset{\gamma^{\sharp}}{\leftrightarrows\!\!\!\!\twoheadrightarrow}} \langle \Sigma \longmapsto (\wp(\Sigma) \cup \{\Sigma_{\bot}\}), \dot{\subseteq}\rangle$.

We have $\alpha^{\blacktriangleright} \circ \alpha^{\partial} = \lambda X \boldsymbol{\cdot} \lambda s \boldsymbol{\cdot} \{s' \mid (\langle s,\ s'\rangle \in X) \vee (\langle s,\ \bot\rangle \in X \wedge s' \in \Sigma)\} = \lambda X \boldsymbol{\cdot} \lambda s \boldsymbol{\cdot} \{s' \mid (s' \in \alpha^{\blacktriangleright}(X)s) \vee (\bot \in \alpha^{\blacktriangleright}(X)s \wedge s' \in \Sigma)\} = \alpha^{\sharp} \circ \alpha^{\blacktriangleright}$. It follows that $\tau^{\sharp} \triangleq \alpha^{\blacktriangleright}(\tau^{\partial}) = \alpha^{\blacktriangleright} \circ \alpha^{\partial}(\tau^{\infty}) = \alpha^{\sharp} \circ \alpha^{\blacktriangleright}(\tau^{\infty}) = \alpha^{\sharp}(\tau^{\natural})$. □

Let us recall the properties of lifting:

Lemma 8.7 (Lifting) *Given a complete lattice* $\langle D,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$ *(respectively poset* $\langle D,\ \sqsubseteq,\ \sqcup\rangle$*, DCPO* $\langle D,\ \sqsubseteq,\ \bot,\ \sqcup\rangle$*), the* lift of D by $\underline{\bot} \notin D$ *is the complete lattice (resp. poset, DCPO)* $\langle D_{\underline{\bot}}, \preceq, \underline{\bot}, \top, \coprod, \prod\rangle$ *with* $D_{\underline{\bot}} \triangleq D \cup \{\underline{\bot}\}$,

$x \preceq y \triangleq (x = \bot) \vee (y \in D \wedge x \sqsubseteq y)$, infimum $\bot$, supremum $\top$, join $\coprod_{i\in\Delta} X_i \triangleq (\forall i \in \Delta : X_i = \bot \;?\; \bot \;¿\; \sqcup\{X_i \mid i \in \Delta \wedge X_i \neq \bot\})$ and the meet is $\prod_{i\in\Delta} X_i \triangleq (\exists i \in \Delta : X_i = \bot \;?\; \bot \;¿\; \sqcap\{X_i \mid i \in \Delta \wedge X_i \neq \bot\})$.

By the fixpoint characterization 7.9 of τ^{∂} and S. Kleene fixpoint transfer theorem 2.3, we get:

Theorem 8.8 (Fixpoint demoniac nondeterministic denotational semantics) *$\tau^{\sharp} = \mathrm{lfp}_{\dot{\bot}^{\sharp}}^{\dot{\sqsubseteq}^{\sharp}} F^{\sharp}$ where $F^{\sharp}(f) \triangleq \dot{\check{\tau}} \;\dot{\cup}\; \dot{\bigcup} f^{\blacktriangleright} \circ \tau^{\blacktriangleleft\!\blacktriangleright}$ is a $\dot{\sqsubseteq}^{\sharp}$-monotone map on the pointwise extension $\langle \dot{D}^{\sharp}, \dot{\sqsubseteq}^{\sharp}, \dot{\bot}^{\sharp}, \dot{\top}^{\sharp}, \dot{\sqcup}^{\sharp}, \dot{\sqcap}^{\sharp}\rangle$ of the lift $\langle D^{\sharp}, \sqsubseteq^{\sharp}, \bot^{\sharp}, \top^{\sharp}, \sqcup^{\sharp}, \sqcap^{\sharp}\rangle$ of the complete lattice $\langle \wp(\Sigma), \subseteq, \emptyset, \Sigma, \cup, \cap\rangle$ by the infimum $\Sigma_{\bot}$.*

Proof. The order structure of $\dot{D}^{\sharp}$ is chosen to be $\langle \alpha^{\blacktriangleright}, \gamma^{\blacktriangleright}\rangle$-isomorphic to the complete lattice $\langle D^{\partial}, \sqsubseteq^{\partial}, \bot^{\partial}, \top^{\partial}, \sqcup^{\partial}, \sqcap^{\partial}\rangle$ of theorem 7.9. Therefore we have a complete lattice $\langle \dot{D}^{\sharp}, \dot{\sqsubseteq}^{\sharp}, \dot{\bot}^{\sharp}, \dot{\top}^{\sharp}, \dot{\sqcup}^{\sharp}, \dot{\sqcap}^{\sharp}\rangle$ such that the partial order is $f \;\dot{\sqsubseteq}^{\sharp}\; g \triangleq \gamma^{\blacktriangleright}(f) \sqsubseteq^{\partial} \gamma^{\blacktriangleright}(g) = \forall s \in \Sigma : \langle s, \bot\rangle \in \gamma^{\blacktriangleright}(f) \vee (\langle s, \bot\rangle \notin \gamma^{\blacktriangleright}(g) \wedge \gamma^{\blacktriangleright}(f) \cap (\{s\} \times \Sigma) \subseteq \gamma^{\blacktriangleright}(g) \cap (\{s\} \times \Sigma)) = \forall s \in \Sigma : \bot \in f(s) \vee (\bot \notin g(s) \wedge f(s) \subseteq g(s)) = \forall s \in \Sigma : f(s) \sqsubseteq^{\sharp} g(s)$ by defining $X \sqsubseteq^{\sharp} Y \triangleq \bot \in X \vee (\bot \notin Y \wedge X \subseteq Y)$, pointwise. Consequently, by lemma 8.7, $\langle D^{\sharp}, \sqsubseteq^{\sharp}, \bot^{\sharp}, \top^{\sharp}, \sqcup^{\sharp}, \sqcap^{\sharp}\rangle$ is the lift of the complete lattice $\langle \wp(\Sigma), \subseteq, \emptyset, \Sigma, \cup, \cap\rangle$ by the infimum $\Sigma_{\bot}$. It follows that the infimum is $\dot{\bot}^{\sharp} \triangleq \lambda s \bullet \bot^{\sharp}$ where $\bot^{\sharp} \triangleq \Sigma_{\bot}$, the supremum is $\dot{\top}^{\sharp} \triangleq \lambda s \bullet \top^{\sharp}$ where $\top^{\sharp} \triangleq \Sigma$, the lub $\bigsqcup^{\sharp}_{i\in\Delta} X_i = (\forall i \in \Delta : X_i = \Sigma_{\bot} \;?\; \Sigma_{\bot} \;¿\; \cup\{X_i \mid i \in \Delta : \wedge X_i \neq \Sigma_{\bot}\})$ satisfies $\alpha^{\blacktriangleright}(\bigsqcup^{\partial}_{i\in\Delta} X_i) = \dot{\bigsqcup}^{\sharp}_{i\in\Delta} \alpha^{\blacktriangleright}(X_i)$. The same way , by lemma 8.7, the glb is $\bigsqcap^{\sharp}_{i\in\Delta} X_i \triangleq (\exists i \in \Delta : X_i = \Sigma_{\bot} \;?\; \Sigma_{\bot} \;¿\; \cap\{X_i \mid i \in \Delta : \wedge X_i \neq \Sigma_{\bot}\})$.

The design of the semantic transformer $F^{\sharp}$ is identical to that of $F^{\natural}$ in the proof of theorem 8.1.

Monotony directly follows from that of F^{∂} using the $\langle \alpha^{\blacktriangleright}, \gamma^{\blacktriangleright}\rangle$-isomorphism.□

Lemma 8.9 (Arrangement of the iterates of $F^{\sharp}$) *Let $F^{\sharp\delta}$, $\delta \in \mathbb{O}$ be the iterates of $F^{\sharp}$ from $\dot{\bot}^{\sharp}$. For all $\eta < \xi$, $s, s' \in \Sigma$, if $s' \in F^{\sharp\xi}(s)$ and $s' \notin F^{\sharp\eta}(s)$ then $F^{\natural\eta}(s) = \Sigma_{\bot}$.*

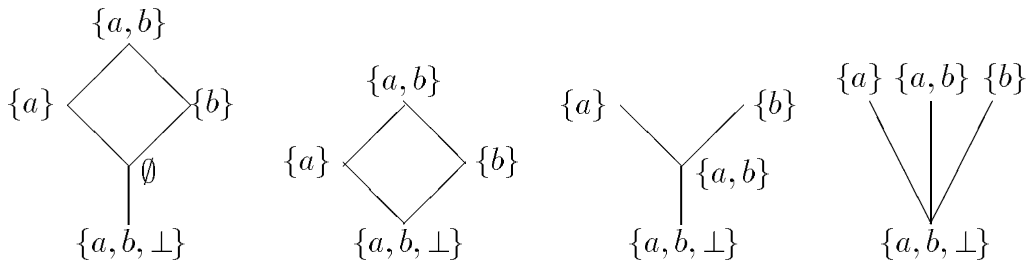
Proof. Follows from lemma 7.10 and the proof of theorem 8.8, showing by S. Kleene fixpoint theorem 2.3 that $\forall \beta \in \mathbb{O} : F^{\sharp\beta} = \alpha^{\blacktriangleright}(F^{\partial\beta})$. □

Lemma 8.10 (Totality of the iterates of $F^{\sharp}$) *Let $F^{\sharp\delta}$, $\delta \in \mathbb{O}$ be the iterates of $F^{\sharp}$ from $\dot{\bot}^{\sharp}$. $\forall \delta \in \mathbb{O} : \forall s \in \Sigma : F^{\sharp\delta}(s) \neq \emptyset$.*

Proof. Follows from lemma 7.11 and the proof of theorem 8.8, showing by S. Kleene fixpoint theorem 2.3 that $\forall \beta \in \mathbb{O} : F^{\sharp\beta} = \alpha^{\blacktriangleright}(F^{\partial\beta})$. □

Lemma 8.11 (Final states of the iterates of $F^{\sharp}$) *Let $F^{\sharp\delta}$, $\delta \in \mathbb{O}$ be the iterates of $F^{\sharp}$ from $\dot{\bot}^{\sharp}$. $\forall \delta \in \mathbb{O} : \forall s, s' \in \Sigma : (s' \in F^{\sharp\delta}(s) \wedge \bot \notin F^{\sharp\delta}(s)) \Longrightarrow (s' \in \check{\tau} \wedge F^{\sharp\delta}(s') = \{s'\})$.*

Proof. Follows from lemma 7.12 and the proof of theorem 8.8, showing by S. Kleene fixpoint theorem 2.3 that $\forall \beta \in \mathbb{O} : F^{\sharp\beta} = \alpha^{\blacktriangleright}(F^{\partial\beta})$. □



Demoniac ordering $\sqsubseteq^\sharp$ Demoniac ordering $\sqsubseteq^\diamond$ Smyth ordering $\sqsubseteq^{\mathrm{S}}$ Flat ordering $\sqsubseteq^=$

Fig. 3.

From theorem 8.8, lemma 8.10 and the fixpoint iterates reordering theorem 2.9, we deduce another fixpoint characterization of $F^\sharp(f)$ with a different partial ordering:

Corollary 8.12 (Reordered fixpoint demoniac nondeterministic denotational semantics) $\tau^\sharp = \mathrm{lfp}^{\dot\sqsubseteq^\diamond}_{\dot\bot^\diamond} F^\sharp$ *where* $F^\sharp(f) \triangleq \dot{\tau} \mathbin{\dot\cup} \bigcup f^{\blacktriangleright} \circ \tau^{\blacktriangleright}$ *is a* $\dot\sqsubseteq^\diamond$*-monotone map on the pointwise extension* $\langle \dot D^\diamond, \dot\sqsubseteq^\diamond, \dot\bot^\diamond, \dot\top^\diamond, \dot\sqcup^\diamond, \dot\sqcap^\diamond\rangle$ *of the complete lattice* $\langle D^\diamond, \sqsubseteq^\diamond, \bot^\diamond, \top^\diamond, \sqcup^\diamond, \sqcap^\diamond\rangle$ *where* $D^\diamond \triangleq (\wp(\Sigma) \setminus \{\emptyset\}) \cup \{\bot^\diamond\}$, $\bot^\diamond \triangleq \Sigma_\bot$ *and* $X \sqsubseteq^\diamond Y \triangleq (X = \bot^\diamond) \vee (X \subseteq Y)$.

8.1.4 Upper/Smyth Nondeterministic Denotational Semantics

Unforeseenly, the demoniac semantic domain $D^\sharp$ with the demoniac ordering $\sqsubseteq^\sharp$ differs from the usual upper powerdomain with M. Smyth ordering [22] $\sqsubseteq^{\mathrm{S}}$ (see figure 3). Let us recall [2, fact 2.7] that M. Smyth upper powerdomain $\langle D^{\mathrm{S}}, \sqsubseteq^{\mathrm{S}}, \bot^{\mathrm{S}}, \sqcap^{\mathrm{S}}, \sqcup^{\mathrm{S}}\rangle$ is $D^{\mathrm{S}} \triangleq \{A \subseteq \Sigma \mid A \neq \emptyset\} \cup \{\Sigma_\bot\}$ ordered by the superset ordering $A \sqsubseteq^{\mathrm{S}} B \triangleq A \supseteq B$ which is a poset with infimum $\bot^{\mathrm{S}} \triangleq \Sigma_\bot$, the glb of nonempty families X_i, $i \in \Delta$ always exist being given by $\underset{i\in\Delta}{\sqcap^{\mathrm{S}}} X_i \triangleq \underset{i\in\Delta}{\cup} X_i$ and if X_i, $i \in \Delta$ has an upper bound, its lub exists and is $\underset{i\in\Delta}{\sqcup^{\mathrm{S}}} X_i \triangleq \underset{i\in\Delta}{\cap} X_i$. By applying the fixpoint iterates reordering theorem 2.9 to 8.8, we get [2]:

Corollary 8.13 (M. Smyth fixpoint nondeterministic denotational semantics) $\tau^\sharp = \mathrm{lfp}^{\dot\sqsubseteq^{\mathrm{S}}}_{\dot\bot^{\mathrm{S}}} F^\sharp$ *where* $F^\sharp$ *is a* $\dot\sqsubseteq^{\mathrm{S}}$*-monotone map on the pointwise extension* $\langle \dot D^{\mathrm{S}}, \dot\sqsubseteq^{\mathrm{S}}, \dot\bot^{\mathrm{S}}, \dot\sqcap^{\mathrm{S}}, \dot\sqcup^{\mathrm{S}}\rangle$ *of M. Smyth upper powerdomain* $\langle D^{\mathrm{S}}, \sqsubseteq^{\mathrm{S}}, \bot^{\mathrm{S}}, \sqcap^{\mathrm{S}}, \sqcup^{\mathrm{S}}\rangle$.

Proof. $\dot\sqsubseteq^{\mathrm{S}}$ is a partial order on $\dot D^{\mathrm{S}}$.

By lemma 8.10, all iterates $F^{\sharp^\delta}$, $\delta \in \mathbb{O}$ of $F^\sharp$ from $\dot\bot^\sharp$ belong to $D^{\mathrm{S}} = D^\sharp \setminus \{\lambda s \cdot \emptyset\}$.

If $f \mathrel{\dot\sqsubseteq^{\mathrm{S}}} g$ then $\forall s \in \Sigma : f(s) \sqsubseteq^{\mathrm{S}} g(s)$ so that $\forall s \in \Sigma : f(s) \supseteq g(s)$ which implies $\forall s \in \Sigma : \dot\tau(s) \;\cup\; \bigcup\{f(s') \mid s \;\tau\; s'\} \supseteq \dot\tau(s) \;\cup\; \bigcup\{g(s') \mid s \;\tau\; s'\}$ that is $\forall s \in \Sigma : F^\sharp(f)s \supseteq F^\sharp(g)s$ whence $F^\sharp(f) \mathrel{\dot\sqsubseteq^{\mathrm{S}}} F^\sharp(g)$ proving that $F^\sharp$ hence $F^\sharp|_{\dot D^{\mathrm{S}}}$ is $\dot\sqsubseteq^{\mathrm{S}}$-monotone.

Assume that $f \in \dot D^{\mathrm{S}}$, λ is a limit ordinal and $\forall \delta < \lambda : F^{\sharp^\delta} \mathrel{\dot\sqsubseteq^{\mathrm{S}}} f$, that is

$\forall \delta < \lambda : \forall s \in \Sigma : F^{\sharp^\delta}(s) \supseteq f(s)$. It follows that $\bigcap\limits_{\delta<\lambda} F^{\sharp^\delta}(s) \supseteq f(s)$ proving that $(\forall \delta < \lambda : F^{\sharp^\delta}(s) = \Sigma_\bot \mathrel{?} \Sigma_\bot ¿ \bigcap\limits_{\delta<\lambda} F^{\sharp^\delta}(s)) \supseteq f(s)$ that is $\dot{\bigsqcup\limits_{\delta<\lambda}}^{\sharp} F^{\sharp^\delta} \mathrel{\dot{\sqsubseteq}^{\mathrm{S}}} f$.

By theorems 8.8 and 2.9, we conclude that $\tau^\sharp = \mathrm{lfp}_{\dot\bot^\sharp}^{\dot\sqsubseteq^\sharp} F^\sharp = \mathrm{lfp}_{\dot\bot^{\mathrm{S}}}^{\dot\sqsubseteq^{\mathrm{S}}} F^\sharp$. □

8.1.5 Minimal Demoniac Nondeterministic Denotational Semantics

M. Smyth ordering $\dot\sqsubseteq^{\mathrm{S}}$ is not *minimal* since, for example on figure 3, $\{a\}$ and $\{a, b\}$ need not be comparable by lemma 7.10. This leads to:

Theorem 8.14 (Flat powerdomain fixpoint nondeterministic denotational semantics) $\tau^\sharp = \mathrm{lfp}_{\dot\bot^\natural}^{\dot\sqsubseteq^\natural} F^\sharp$ *where* $F^\sharp$ *is a* $\dot\sqsubseteq^\natural$*-monotone map on the DCPO* $\langle \dot{D}^\natural, \dot\sqsubseteq^\natural, \dot\bot^\natural, \dot\sqcup^\natural \rangle$ *which is the restriction of the pointwise extension of the flat DCPO* $\langle D^\natural, \sqsubseteq^\natural, \bot^\natural, \sqcup^\natural \rangle$. *with* $D^\natural \triangleq (\wp(\Sigma) \setminus \{\emptyset\}) \cup \{\bot^\natural\}$ *and infimum* $\bot^\natural \triangleq \Sigma_\bot$ *to* $\dot{D}^\natural \triangleq \{f \in \Sigma \longmapsto D^\natural \mid \forall s, s' \in \Sigma : (s' \in f(s) \wedge f(s) \neq \bot^\natural) \Longrightarrow (s' \in \check{\tau} \wedge f(s') = \{s'\})$.

Proof. $f \mathrel{\dot\sqsubseteq^\natural} g \Longleftrightarrow \forall s \in \Sigma : f(s) \sqsubseteq^\natural g(s)$ and $\sqsubseteq^\natural$ is the flat partial ordering with infimum $\bot^\natural$, so that $\dot\sqsubseteq^\natural$ is a partial order on $\dot{D}^\natural$.

To prove that $\langle \dot{D}^\natural, \dot\sqsubseteq^\natural \rangle$ is a DCPO, let λ be a limit ordinal, $f^\delta, \delta < \lambda$ be a $\dot\sqsubseteq^\natural$-increasing chain. Its lub in the pointwise extension of $\langle D^\natural, \sqsubseteq^\natural \rangle$ is $f^\lambda \triangleq \dot{\bigsqcup\limits_{\delta<\lambda}}^{\natural} f^\lambda$. Let us show that $f^\lambda \in \dot{D}^\natural$ which implies that f^λ is the lub in $\dot{D}^\natural$. To prove this, we have $\forall s \in \Sigma : f^\lambda(s) = \bigsqcup\limits_{\delta<\lambda}^{\natural} f^\delta(s)$ so that either $\forall \delta < \lambda : f^\delta(s) = \bot^\natural$ in which case $f^\lambda(s) = \bot^\natural$ or, by definition of the flat ordering, $\exists \eta < \lambda : f^\lambda(s) = \bigsqcup\limits_{\delta<\lambda}^{\natural} f^\delta(s) = f^\eta(s)$ so that $f^\eta \in \dot{D}^\natural$ implies $\forall s, s' \in \Sigma : (s' \in f^\lambda(s) \wedge f^\lambda(s) \neq \bot^\natural) \Longrightarrow s' \in (s' \in \check{\tau} \wedge f(s') = \{s'\})$ hence $f^\lambda \in \dot{D}^\natural$.

All iterates $F^{\sharp^\delta}$, $\delta \in \mathbb{O}$ of $F^\sharp(f) \triangleq \dot{\check{\tau}} \ \dot\cup \ \bigcup f^{\blacktriangleright} \circ \tau^{\bullet\!\blacktriangleright}$ from $\dot\bot^{\mathrm{S}} = \lambda s \bullet \Sigma_\bot = \dot\bot^\natural$ satisfy $F^{\sharp^\delta} \neq \lambda s \bullet \emptyset$ by lemma 8.10 and $\forall s, s' \in \Sigma : (s' \in F^{\sharp^\delta}(s) \wedge F^{\sharp^\delta}(s) \neq \bot^\natural) \Longrightarrow s' \in (s' \in \check{\tau} \wedge f(s') = \{s'\})$ by lemma 8.11, hence belong to $\dot{D}^\natural$.

$\dot\bot^\natural$ is the $\dot\sqsubseteq^\natural$-infimum of $\dot{D}^\natural$.

If $f \mathrel{\dot\sqsubseteq^\natural} g$ then $\forall s \in \Sigma : (f(s) = \Sigma_\bot) \vee (f(s) = g(s))$ so that $\forall s \in \Sigma : (\dot{\check{\tau}}(s) \cup \bigcup\{f(s') \mid s \mathrel{\tau} s'\} = \Sigma_\bot) \vee (\dot{\check{\tau}}(s) \cup \bigcup\{f(s') \mid s \mathrel{\tau} s'\} = \dot{\check{\tau}}(s) \cup \bigcup\{g(s') \mid s \mathrel{\tau} s'\})$ whence $F^\sharp(f) \mathrel{\dot\sqsubseteq^\natural} F^\sharp(g)$ proving that $F^\sharp$ hence $F^\sharp|_{\dot{D}^\natural}$ is $\dot\sqsubseteq^\natural$-monotone.

Assume that $f \in \dot{D}^\natural$, λ is a limit ordinal and $\forall \delta < \lambda : F^{\sharp^\delta} \mathrel{\dot\sqsubseteq^\natural} f$, that is $\forall \delta < \lambda : \forall s \in \Sigma : (F^{\sharp^\delta}(s) = \Sigma_\bot) \vee (F^{\sharp^\delta}(s) = f(s))$. It follows that either $\bigcap\limits_{\delta<\lambda} F^{\sharp^\delta}(s) = \Sigma_\bot$ or $\bigcap\limits_{\delta<\lambda} F^{\sharp^\delta}(s) = f(s)$ proving that $\dot{\bigsqcup\limits_{\delta<\lambda}}^{\mathrm{S}} F^{\sharp^\delta} \mathrel{\dot\sqsubseteq^\natural} f$.

By theorems 8.13 and 2.9, we conclude that $\tau^\sharp = \mathrm{lfp}_{\dot\bot^{\mathrm{S}}}^{\dot\sqsubseteq^{\mathrm{S}}} F^\sharp = \mathrm{lfp}_{\dot\bot^\natural}^{\dot\sqsubseteq^\natural} F^\sharp$. □

The poset $\langle \dot{D}^\natural, \dot\sqsubseteq^\natural \rangle$ is minimal for the fixpoint nondeterministic denotational semantics, in that:

Theorem 8.15 (Minimality of $\langle \dot{D}^\natural, \dot\sqsubseteq^\natural \rangle$) *Let* $\langle E, \preccurlyeq \rangle$ *be any poset such that* $\dot\bot^\natural$ *is the* $\preccurlyeq$*-infimum of* E, $F^\sharp[\![\tau]\!] \triangleq \lambda f \bullet \dot{\check{\tau}} \ \dot\cup \ \bigcup f^{\blacktriangleright} \circ \tau^{\bullet\!\blacktriangleright} \in E \xmapsto{m} E$ *is* $\preccurlyeq$*-monotone and* $\forall \tau : \tau^\sharp = \mathrm{lfp}_{\dot\bot^\natural}^{\preccurlyeq} F^\sharp[\![\tau]\!]$ *then* $\dot{D}^\natural \subseteq E$ *and* $\dot\sqsubseteq^\natural \subseteq \preccurlyeq$.

Proof. Assume, by reductio ad absurdum, that $\exists f \in \dot{D}^{=} : f \notin E$. We write $F^{\sharp}\llbracket\tau\rrbracket$ to explicitate which transition system $\langle\Sigma,\ \tau\rangle$ the transformer $F^{\sharp}$ depends upon. Let us define the particular transition relation $\tau \triangleq \{\langle s, s'\rangle \mid (s = s' \wedge \bot \in f(s)) \vee (s \neq s' \wedge \bot \notin f(s) \wedge s' \in f(s))\}$.

We have $\dot{\check{\tau}}(s) \triangleq \{s \mid \forall s' \in \Sigma : \neg(s\ \tau\ s')\} = \{s \mid \forall s' \in \Sigma : \neg(s = s' \wedge \bot \in f(s)) \wedge \neg(s \neq s' \wedge \bot \notin f(s) \wedge s' \in f(s))\} = \{s \mid (\forall s' \in \Sigma : s \neq s' \vee \bot \notin f(s)) \wedge (\forall s' \in \Sigma : s = s' \vee \bot \in f(s) \vee s' \notin f(s))\} = \{s \mid \bot \notin f(s) \wedge \forall s' \neq s : s' \notin f(s))\}$ $= \{s \mid f(s) = \{s\}\}$ since $f(s) \neq \emptyset$.

We have $\exists s' : s\ \tau\ s' = (\exists s' : s = s' \wedge \bot \in f(s)) \vee (\exists s' : s \neq s' \wedge \bot \notin f(s) \wedge s' \in f(s)) = (\bot \in f(s)) \vee (\exists s' \neq s : s' \in f(s)) = (\bot \in f(s)) \vee (f(s) \neq \{s\})$ since $f(s) \neq \emptyset$ so that $(\exists s' \neq s : s' \in f(s)) \Longleftrightarrow f(s) \neq \{s\}$.

The iterates ${F^{\sharp}}^{\delta}, \delta \in \mathbb{O}$ of $F^{\sharp}\llbracket\tau\rrbracket$ are as follows:

${F^{\sharp}}^{0} = \lambda s \mathbin{\bullet} \Sigma_{\bot}$.

${F^{\sharp}}^{1} = F^{\sharp}\llbracket\tau\rrbracket({F^{\sharp}}^{0}) = \lambda s \mathbin{\bullet} \dot{\check{\tau}}(s)\ \cup\ \bigcup\{{F^{\sharp}}^{0}(s') \mid s\ \tau\ s'\} = \lambda s \mathbin{\bullet} \{s \mid f(s) = \{s\}\}\ \cup\ \big(\bot \in f(s) \vee (f(s) \neq \{s\})\ ?\ \Sigma_{\bot}\ \text{¿}\ \emptyset\big) = \lambda s \mathbin{\bullet} \{s \mid f(s) = \{s\}\}\ \cup\ \big(\bot \in f(s)\ ?\ \Sigma_{\bot}\ \text{¿}\ \emptyset\big)\ \cup\ \big((f(s) \neq \{s\})\ ?\ \Sigma_{\bot}\ \text{¿}\ \emptyset\big)$.

${F^{\sharp}}^{2} = F^{\sharp}\llbracket\tau\rrbracket({F^{\sharp}}^{1}) = \lambda s \mathbin{\bullet} \{s \mid f(s) = \{s\}\} \cup A \cup B$ where:

$A = \bigcup\{\{s \mid f(s) = \{s\}\}\ \cup\ \big(\bot \in f(s)\ ?\ \Sigma_{\bot}\ \text{¿}\ \emptyset\big)\ \cup\ \big(f(s) \neq \{s\}\ ?\ \Sigma_{\bot}\ \text{¿}\ \emptyset\big) \mid \bot \in f(s)\} = \big(\bot \in f(s)\ ?\ \Sigma_{\bot}\ \text{¿}\ \emptyset\big) = \big(\bot \in f(s)\ ?\ f(s)\ \text{¿}\ \emptyset\big)$.

$B = \bigcup\{\{s' \mid f(s') = \{s'\}\}\ \cup\ \big(\bot \in f(s')\ ?\ \Sigma_{\bot}\ \text{¿}\ \emptyset\big)\ \cup\ \big((f(s') \neq \{s'\})\ ?\ \Sigma_{\bot}\ \text{¿}\ \emptyset\big) \mid s \neq s' \wedge \bot \notin f(s) \wedge s' \in f(s)\}$. Since $s' \in f(s)$ and $\bot \notin f(s)$ hence $f(s) \neq \Sigma_{\bot} = \bot^{=}$, we have $s' \in \check{\tau}$ hence $s' \in \dot{\check{\tau}}(s')$ so that, as shown above, $f(s') = \{s'\}$ and $\bot \notin f(s')$. Therefore $B = \bigcup\{\{s' \mid f(s') = \{s'\}\} \mid s \neq s' \wedge \bot \notin f(s) \wedge s' \in f(s)\} = \{s' \mid s \neq s' \wedge \bot \notin f(s) \wedge s' \in f(s)\}$.

It follows that ${F^{\sharp}}^{2} = \lambda s \mathbin{\bullet} \{s \mid f(s) = \{s\}\} \cup A \cup B = \lambda s \mathbin{\bullet} \{s \mid f(s) = \{s\}\} \cup \big(\bot \in f(s)\ ?\ f(s)\ \text{¿}\ \emptyset\big) \cup \{s' \mid s \neq s' \wedge \bot \notin f(s) \wedge s' \in f(s)\}$. If $\bot \in f(s)$ then ${F^{\sharp}}^{2}(s) = f(s)$. Otherwise $\bot \notin f(s)$ hence $f(s) \neq \bot^{=}$ in which case ${F^{\sharp}}^{2}(s) = \{s \mid f(s) = \{s\}\} \cup \{s' \mid s \neq s' \wedge s' \in f(s)\}$. But $s \in f(s) \wedge f(s) \neq \bot^{=} \wedge f \in \dot{D}^{=}$ implies $f(s) = \{s\}$ so ${F^{\sharp}}^{2}(s) = f(s)$.

We have shown that ${F^{\sharp}}^{2} = f$.

This is in contradiction with $f \notin E$ so that $\dot{D}^{=} \subseteq E$.

For all $f \in \dot{D}^{=}$, we have shown that there exists τ such that f is one of the iterates of $F^{\sharp}\llbracket\tau\rrbracket$ from $\dot{\bot}^{=}$. Since the iterates are $\preccurlyeq$-increasing, we must have $\dot{\bot}^{=} \preccurlyeq f$ proving that $\dot{\sqsubseteq}^{=} \subseteq \preccurlyeq$. □

Reciprocally, we have:

Theorem 8.16 (General fixpoint demoniac nondeterministic denotational semantics) *Let $\langle E,\ \preccurlyeq\rangle$ be a poset such that $\dot{D}^{=}\ \subseteq\ E$, $\dot{\sqsubseteq}^{=} \subseteq \preccurlyeq$, $\dot{\bot}^{=}$ is the $\preccurlyeq$-infimum of E, the $\preccurlyeq$-lub of $\dot{\sqsubseteq}^{=}$-increasing chains $f^{\delta}, \delta \in \lambda$ in $\dot{D}^{=}$ is $\dot{\bigsqcup}^{=}_{\delta<\lambda} f^{\delta}$ and $F^{\natural} \triangleq \lambda f \mathbin{\bullet} \dot{\check{\tau}}\ \dot{\cup}\ \dot{\bigcup} f^{\blacktriangleright} \circ \tau^{\bullet\!\blacktriangleright} \in E \stackrel{m}{\longmapsto} E$ is $\preccurlyeq$-monotonic. Then $\tau^{\sharp} = \operatorname{lfp}^{\preccurlyeq}_{\dot{\bot}^{=}} F^{\sharp}$.*

Proof. By the proof of theorem 8.14, we know that all iterates ${F^{\sharp}}^{\delta}$, $\delta \in \mathbb{O}$ of $F^{\sharp}$ are in $\dot{D}^{=}$. Let ϵ be the iteration order so that ${F^{\sharp}}^{\epsilon} = \operatorname{lfp}^{\dot{\sqsubseteq}^{=}}_{\dot{\bot}^{=}} F^{\sharp}$. Let $f \in E$

be any fixpoint of $F^\sharp$. We have $F^{\sharp 0} = \dot{\bot}^{=} \preccurlyeq f$ since $\dot{\bot}^{=}$ is the $\preccurlyeq$-infimum of E. If $F^{\sharp\delta} \preccurlyeq f$ then $F^{\sharp\delta+1} = F^\sharp(F^{\sharp\delta}) \preccurlyeq F^\sharp(f) = f$ since $F^\natural$ is $\preccurlyeq$-monotonic. If λ is a limit ordinal then $F^{\sharp\delta}$, $\delta < \lambda$ is a $\dot{\sqsubseteq}^{=}$-increasing chain so that its $\preccurlyeq$-lub is $\dot{\bigsqcup\limits_{\delta<\lambda}}^{=} F^{\sharp\delta} = F^{\sharp\lambda}$ whence $F^{\sharp\lambda} \preccurlyeq f$ since $\forall \delta < \lambda : F^{\sharp\delta} \preccurlyeq f$ by induction hypothesis. By transfinite induction, $\forall \delta \in \mathbb{O} : F^{\sharp\delta} \preccurlyeq f$ proving that $F^{\sharp\epsilon} = \mathrm{lfp}^{\preccurlyeq}_{\dot{\bot}^{=}} F^\sharp$. By theorem 8.14, $\tau^\sharp = \mathrm{lfp}^{\dot{\sqsubseteq}^{=}}_{\dot{\bot}^{=}} F^\sharp = \mathrm{lfp}^{\preccurlyeq}_{\dot{\bot}^{=}} F^\sharp$. □

8.1.6 Angelic/Lower/C.A.R. Hoare Nondeterministic Denotational Semantics

The *angelic nondeterministic denotational semantics* is the right-image abstraction $\tau^\flat \triangleq \alpha^{\blacktriangleright}(\tau^+)$ of the finite/angelic relational semantics τ^+. We also have $\tau^\flat = \alpha^\Sigma(\tau^\natural)$ where $\alpha^\Sigma(f) = \lambda s \bullet f(s) \cap \Sigma$. By theorem 7.1 and S. Kleene fixpoint transfer theorem 2.3, we get:

Corollary 8.17 (C.A.R. Hoare fixpoint nondeterministic denotational semantics) $\tau^\flat = \mathrm{lfp}^{\dot{\subseteq}}_{\dot{\emptyset}} F^\flat$ *where* $F^\flat = \lambda f \bullet \dot{\check{\tau}}\ \dot{\cup}\ \dot{\bigcup} f^{\blacktriangleright} \circ \tau^{\bullet\blacktriangleright}$ *is a complete* $\dot{\cup}$-*morphism on the complete lattice* $\langle \Sigma \longmapsto \wp(\Sigma),\ \dot{\subseteq},\ \dot{\emptyset},\ \lambda s \bullet \Sigma,\ \dot{\cup},\ \dot{\cap}\rangle$ *which is the pointwise extension of the powerset* $\langle \wp(\Sigma),\ \emptyset\rangle$.

Proof. The order structure of $\Sigma \longmapsto \wp(\Sigma)$ is chosen to be $\langle \alpha^{\blacktriangleright}, \gamma^{\blacktriangleright}\rangle$-isomorphic to the complete lattice $\langle \wp(\Sigma \times \Sigma),\ \sqsubseteq,\ \emptyset,\ \Sigma \times \Sigma,\ \cup,\ \cap\rangle$ of theorem 7.1 that is the pointwise extension of the powerset $\langle \wp(\Sigma),\ \subseteq\rangle$.

We have $\alpha^{\blacktriangleright}(\dot{\bigcup\limits_{i\in\Delta}} X_i) = \lambda s \bullet \{s' \mid \langle s,\ s'\rangle \in \bigcup\limits_{i\in\Delta} X_i)\} = \dot{\bigcup\limits_{i\in\Delta}} \lambda s \bullet \{s' \mid \langle s,\ s'\rangle \in X_i)\} = \dot{\bigcup\limits_{i\in\Delta}} \alpha^{\blacktriangleright}(X_i)$ so that $\alpha^{\blacktriangleright}$ is $\emptyset$-strict and Scott-continuous.

The commutation condition leads to the definition of $F^\flat$ as in the proof of theorem 8.1.

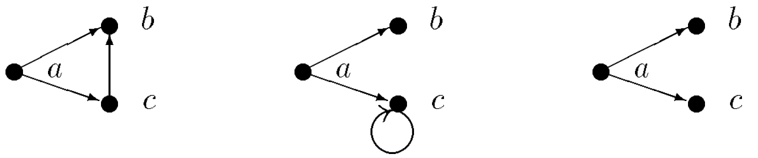
$F^\flat$ is a complete join-morphism since $(\dot{\cup}(\dot{\bigcup\limits_{i\in\Delta}} f_i)^{\blacktriangleright})(X) = \cup\{(\dot{\bigcup\limits_{i\in\Delta}} f_i)(s) \mid s \in X\} = \cup\{\bigcup\limits_{i\in\Delta} f_i(s) \mid s \in X\} = \bigcup\limits_{i\in\Delta}\{f_i(s) \mid s \in X\} = \bigcup\limits_{i\in\Delta} f_i{}^{\blacktriangleright}(X)$ so that $F^\flat(\dot{\bigcup\limits_{i\in\Delta}} f_i) = \dot{\check{\tau}}\ \dot{\cup}\ \dot{\bigcup}(\dot{\bigcup\limits_{i\in\Delta}} f_i)^{\blacktriangleright} \circ \tau^{\bullet\blacktriangleright} = \dot{\check{\tau}}\ \dot{\cup}\ \dot{\bigcup} \dot{\bigcup\limits_{i\in\Delta}} f_i{}^{\blacktriangleright} \circ \tau^{\bullet\blacktriangleright} = \dot{\bigcup\limits_{i\in\Delta}}(\dot{\check{\tau}}\ \dot{\cup}\ \dot{\bigcup} f_i{}^{\blacktriangleright} \circ \tau^{\bullet\blacktriangleright}) = \dot{\bigcup\limits_{i\in\Delta}} F^\flat(f_i)$.

Finally $\tau^\flat \triangleq \alpha^{\blacktriangleright}(\tau^+) = \alpha^{\blacktriangleright}(\mathrm{lfp}^{\subseteq}_{\emptyset} F^+) = \mathrm{lfp}^{\dot{\subseteq}}_{\dot{\emptyset}} F^\flat$. □

Observe that the angelic semantic domain $\langle \Sigma \longmapsto \wp(\Sigma),\ \dot{\subseteq}\rangle$ is exactly the pointwise extension of the usual lower/C.A.R. Hoare powerdomain [22].

8.2 Deterministic Denotational Semantics

In the *deterministic denotational semantics* the nondeterministic behaviors are ignored.



$\tau^\natural(a) \;=\{b\}$	$\tau^\natural(a) \;=\{b, \bot\}$	$\tau^\natural(a) \;=\{b, c\}$
$\tau^\top(a) = b$	$\tau^\top(a) = b$	$\tau^\top(a) = \top$
$\tau^\top(b) = b$	$\tau^\top(b) = b$	$\tau^\top(b) = b$
$\tau^\top(c) = b$	$\tau^\top(c) = \bot$	$\tau^\top(c) = c$

Fig. 4. Natural $\tau^\natural$ and deterministic $\tau^\top$ denotational semantics of nondeterministic transition systems τ

8.2.1 Deterministic Denotational Semantics of Nondeterministic Transition Systems

For nondeterministic transition systems, the nondeterministic behaviors are abstracted to *chaos* $\top$. We let $\alpha^\top(\emptyset) \triangleq \alpha^\top(\{\bot\}) \triangleq \bot$, $\forall s \in \Sigma : \alpha^\top(\{s\}) \triangleq \alpha^\top(\{s, \bot\}) \triangleq s$ and $\alpha^\top(X) \triangleq \top$ when $X \subseteq \Sigma_\bot$ has a cardinality such that $|X \setminus \{\bot\}| > 1$. Observe that $\alpha^\top$ ignores inevitable nontermination in the abstraction of nondeterminism (see figure 4). By letting $\forall \zeta \in \Sigma_\bot : \gamma^\top(\zeta) \triangleq \{\zeta, \bot\}$ and $\gamma^\top(\top) \triangleq \Sigma_\bot$, we get the Galois insertion $\langle \wp(\Sigma_\bot), \subseteq\rangle \underset{\alpha^\top}{\overset{\gamma^\top}{\leftrightarrows}} \langle \Sigma_\bot^\top, \sqsubseteq^\top\rangle$ where $\sqsubseteq^\top$ is given by $\bot \sqsubseteq^\top \zeta \sqsubseteq^\top \zeta \sqsubseteq^\top \top$ for $\zeta \in \Sigma_\bot^\top \triangleq \Sigma \cup \{\bot, \top\}$.

We define $\dot\alpha^\top \triangleq \lambda s\cdot \alpha^\top(f(s))$ pointwise so that $\tau^\top \triangleq \dot\alpha^\top(\tau^\natural)$. By theorem 8.1 and S. Kleene fixpoint transfer theorem 2.3, we get:

Theorem 8.18 (D. Scott fixpoint deterministic denotational semantics (complete lattices and continuous functions)) $\tau^\top = \mathrm{lfp}_{\bot}^{\dot\sqsubseteq^\top}\; F^\top$ *where* $F^\top \in (\Sigma \longmapsto \Sigma_\bot^\top) \longmapsto (\Sigma \longmapsto \Sigma_\bot^\top)$ *defined as* $F^\top(f) \triangleq \lambda s\cdot(\forall s' \in \Sigma : \neg(s\ \tau\ s')\ ?\ s\ ¿\ \sqcup^\top\{f(s') \mid s\ \tau\ s'\})$ *is a complete* $\dot\sqcup^\top$*-morphism on the complete lattice* $\langle \Sigma \longmapsto \Sigma_\bot^\top,\ \dot\sqsubseteq^\top,\ \dot\bot,\ \dot\top,\ \dot\sqcup^\top,\ \dot\sqcap^\top\rangle$ *which is the pointwise extension of the complete lattice* $\langle \Sigma_\bot^\top,\ \sqsubseteq^\top,\ \bot,\ \top,\ \sqcup^\top,\ \sqcap^\top\rangle$ *with* $\sqsubseteq^\top$ *such that* $\forall \zeta \in \Sigma_\bot^\top : \bot \sqsubseteq^\top \zeta \sqsubseteq^\top \zeta \sqsubseteq^\top \top$.

Proof. $\alpha^\top(X) \sqsubseteq^\top \zeta \Longleftrightarrow X \subseteq \gamma^\top(\zeta)$ is easily proved by case analysis. Either $\zeta = \bot$ and X can only be $\emptyset$ or $\{\bot\}$, or $\zeta = s$ and $X \subseteq \{s, \bot\}$, otherwise $\zeta = \top$ and this is obvious. We get $\langle \Sigma \longmapsto \wp(\Sigma_\bot),\ \dot\subseteq\rangle \underset{\dot\alpha^\top}{\overset{\dot\gamma^\top}{\leftrightarrows}} \langle \Sigma \longmapsto \Sigma_\bot^\top,\ \dot\sqsubseteq^\top\rangle$, pointwise.

The abstraction function $\dot\alpha^\top$ is strict since $\alpha^\top(\{\bot\}) = \bot$. If $\forall i \in \Delta : X_i \in \wp(\Sigma_\bot)$ then either $\forall i \in \Delta : X_i \subseteq \{\bot\}$ and then $\alpha^\top(\bigsqcup^\top_{i\in\Delta} X_i) = \bigsqcup^\top_{i\in\Delta} \alpha^\top(X_i) = \bot$ or $\exists s \in \Sigma : \forall i \in \Delta : X_i \subseteq \{s, \bot\} \wedge \exists k \in \Delta : s \in X_k$, in which case $\alpha^\top(\bigsqcup^\top_{i\in\Delta} X_i) = \bigsqcup^\top_{i\in\Delta} \alpha^\top(X_i) = s$, otherwise $\exists s, s' \in \Delta : s \neq s' \wedge \exists i \in \Delta : \{s, s'\} \subseteq X_i$, in which case $\alpha^\top(\bigsqcup^\top_{i\in\Delta} X_i) = \bigsqcup^\top_{i\in\Delta} \alpha^\top(X_i) = \top$ proving $\dot\alpha^\top(\dot\bigsqcup^\top_{i\in\Delta} f_i) = \dot\bigsqcup^\top_{i\in\Delta} \dot\alpha^\top(f_i)$, pointwise.

The commutation condition is used to design $F^{\top}$. $\dot{\alpha}^{\top} \circ F^{\natural}(f) = \dot{\alpha}^{\top}(\dot{\check{\tau}} \mathbin{\dot{\cup}} \dot{\bigcup} f^{\blacktriangleright} \circ \tau^{\boldsymbol{\rightarrow}}) = \lambda s \bullet \alpha^{\top}(\dot{\check{\tau}}(s) \cup \bigcup f^{\blacktriangleright} \circ \tau^{\boldsymbol{\rightarrow}}(s)) = \lambda s \bullet \alpha^{\top}(\{s \mid \forall s' \in \Sigma : \neg(s\ \tau\ s')\} \cup \bigcup\{f(s') \mid s\ \tau\ s'\}) = \lambda s \bullet (\forall s' \in \Sigma : \neg(s\ \tau\ s')\ ?\ \alpha^{\top}(\{s\})\ ¿\ \alpha^{\top}(\bigcup\{f(s') \mid s\ \tau\ s'\})) = \lambda s \bullet (\forall s' \in \Sigma : \neg(s\ \tau\ s')\ ?\ s\ ¿\ \sqcup^{\top}\{\alpha^{\top}(f(s')) \mid s\ \tau\ s'\}) = \lambda s \bullet (\forall s' \in \Sigma : \neg(s\ \tau\ s')\ ?\ s\ ¿\ \sqcup^{\top}\{\dot{\alpha}^{\top}(f)(s') \mid s\ \tau\ s'\}) = \lambda s \bullet F^{\top} \circ \dot{\alpha}^{\top}(f)$ by definition of $\dot{\alpha}^{\top}$ and $\alpha^{\top}$ which is a complete $\sqcup^{\top}$-complete morphism and by defining $F^{\top} \triangleq \lambda f \bullet \lambda s \bullet (\forall s' \in \Sigma : \neg(s\ \tau\ s')\ ?\ s\ ¿\ \sqcup^{\top}\{f(s') \mid s\ \tau\ s'\})$.

If $\forall i \in \Delta : f_i \in \Sigma \longmapsto \wp(\Sigma_{\perp})$ and $s \in \Sigma$ then $F^{\top}(\dot{\bigsqcup}^{\top}_{i\in\Delta} f_i)(s) = (\forall s' \in \Sigma : \neg(s\ \tau\ s')\ ?\ s\ ¿\ \sqcup^{\top}\{(\dot{\bigsqcup}^{\top}_{i\in\Delta} f_i)(s') \mid s\ \tau\ s'\}) = (\forall s' \in \Sigma : \neg(s\ \tau\ s')\ ?\ s\ ¿\ \sqcup^{\top}\{\bigsqcup^{\top}_{i\in\Delta} f_i(s') \mid s\ \tau\ s'\}) = (\forall s' \in \Sigma : \neg(s\ \tau\ s')\ ?\ s\ ¿\ \bigsqcup^{\top}_{i\in\Delta}\{f_i(s') \mid s\ \tau\ s'\}) = \bigsqcup^{\top}_{i\in\Delta}(\forall s' \in \Sigma : \neg(s\ \tau\ s')\ ?\ s\ ¿\ \{f_i(s') \mid s\ \tau\ s'\}) = \bigsqcup^{\top}_{i\in\Delta} F^{\top} f_i(s)$, proving $F^{\top}(\dot{\bigsqcup}^{\top}_{i\in\Delta} f_i) = \dot{\bigsqcup}^{\top}_{i\in\Delta} F^{\top}(f_i)$, pointwise.

We conclude $\tau^{\top} \triangleq \alpha^{\top}(\tau^{\natural}) = \alpha^{\top}(\mathrm{lfp}^{\dot{\sqsubseteq}^{\natural}}_{\dot{\perp}^{\natural}} F^{\natural}) = \mathrm{lfp}^{\dot{\sqsubseteq}^{\top}}_{\dot{\perp}^{\top}} F^{\top}$ where $\dot{\perp}^{\top} \triangleq \lambda s \bullet \perp$.□

Observe that we have got a complete lattice as in the original work of D. Scott [37] by giving the top element $\top$ the obvious meaning of abstraction of nondeterminism by chaos (so as to restrict to functions).

8.2.2 D. Scott Deterministic Denotational Semantics of Locally Deterministic Transition Systems

For *locally deterministic transition systems* $\langle\Sigma,\ \tau\rangle$ (i.e. $\forall s, s', s'' \in \Sigma : s\ \tau\ s' \wedge s\ \tau\ s'' \Longrightarrow s' = s''$) the top element $\top$ can be withdrawn from the semantic domain:

Lemma 8.19 (Iterates of $F^{\top}$ for deterministic transition systems) *For locally deterministic transition systems $\langle\Sigma,\ \tau\rangle$, $\forall s \in \Sigma : \tau^{\top}(s) \neq \top$.*

Proof. Let ϵ be the order of the $\dot{\sqsubseteq}^{\top}$-increasing chain of iterates $F^{\top\delta}$, $\delta \in \mathbb{O}$ of $F^{\top}$ from $\dot{\perp}^{\top}$. We show that $\forall s \in \Sigma : \forall \delta \in \mathbb{O} : F^{\top\delta}(s) \neq \top$.

We have $\forall s \in \Sigma : F^{\top 0}(s) = \perp \neq \top$.

If this is true for $\delta \in \mathbb{O}$ then for all $s \in \Sigma$, $F^{\top\delta+1}(s) = F^{\top}(F^{\top\delta})(s) = (\forall s' \in \Sigma : \neg(s\ \tau\ s')\ ?\ s\ ¿\ \sqcup^{\top}\{F^{\top\delta}(s') \mid s\ \tau\ s'\})$. If $\forall s' \in \Sigma : \neg(s\ \tau\ s')$ then $s \neq \top$. Otherwise their is a unique $s' \in \Sigma$ such that $s\ \tau\ s'$ and $F^{\top\delta}(s') \neq \top$ by induction hypothesis so $\sqcup^{\top}\{F^{\top\delta}(s') \mid s\ \tau\ s'\} \neq \top$.

Let λ be a limit ordinal such that $\forall \delta < \lambda : \forall s \in \Sigma : F^{\top\delta}(s) \neq \top$. Since the iterates form an increasing chain, we have either $\forall \delta < \lambda : F^{\top\delta}(s) = \perp$ in which case $\bigsqcup^{\top}_{\delta<\lambda} F^{\top\delta}(s) = \perp \neq \top$ or $\exists \zeta \in \Sigma : \forall \delta < \lambda : F^{\top\delta}(s) \sqsubseteq^{\top} \zeta$, in which case $\bigsqcup^{\top}_{\delta<\lambda} F^{\top\delta}(s) = \zeta \neq \top$.

By transfinite induction $\forall s \in \Sigma : \forall \delta \in \mathbb{O} : F^{\top\delta}(s) \neq \top$ thus proving that $\tau^{\top}(s) = (\mathrm{lfp}^{\dot{\sqsubseteq}^{\top}}_{\dot{\perp}^{\top}} F^{\top})(s) = F^{\top\epsilon}(s) \neq \top$. □

It follows that we can define $\tau^{\mathrm{D}} = \tau^{\top} \cap (\Sigma \longmapsto \Sigma_{\perp})$. By the fixpoint iterates reordering theorem 2.9 and theorem 8.18, we infer:

Theorem 8.20 (D. Scott fixpoint deterministic denotational semantics (CPOs and continuous functions)) $\tau^{\mathrm{D}} = \mathrm{lfp}_{\dot{\bot}}^{\dot{\sqsubseteq}^{\mathrm{D}}}\ F^{\mathrm{D}}$ *where* $F^{\mathrm{D}} \in (\Sigma \longmapsto \Sigma_{\bot}) \longmapsto (\Sigma \longmapsto \Sigma_{\bot})$ *defined as* $F^{\mathrm{D}}(f) \triangleq \lambda s \bullet (\, s\ \tau\ s'\ ?\ f(s')\ ¿\ s\,)$ *is a Scott-continuous map on the DCPO* $\langle \Sigma \longmapsto \Sigma_{\bot},\ \dot{\sqsubseteq}^{\mathrm{D}},\ \dot{\bot},\ \dot{\sqcup}^{\mathrm{D}} \rangle$ *which is the pointwise extension of DCPO* $\langle \Sigma_{\bot},\ \sqsubseteq^{\mathrm{D}},\ \bot,\ \sqcup^{\mathrm{D}} \rangle$ *where the Scott-ordering* $\sqsubseteq^{\mathrm{D}}$ *is such that* $\forall \zeta \in \Sigma_{\bot} : \bot \sqsubseteq^{\mathrm{D}} \zeta \sqsubseteq^{\mathrm{D}} \zeta$.

Proof. $\dot{\sqsubseteq}^{\mathrm{D}}$ is a partial order on $\Sigma \longmapsto \Sigma_{\bot}$ with infimum $\dot{\bot}^{\top} = \lambda s \bullet \bot$. By lemma 8.19, all iterates of $F^{\top}$ belong to $\Sigma_{\bot}$. We have $F^{\top}|_{\Sigma \longmapsto \Sigma_{\bot}} = \lambda f \in \Sigma \longmapsto \Sigma_{\bot} \bullet \lambda s \bullet F^{\top}(f)s = \lambda f \in \Sigma \longmapsto \Sigma_{\bot} \bullet \lambda s \bullet (\, \forall s' \in \Sigma : \neg(s\ \tau\ s')\ ?\ s\ ¿\ \sqcup^{\top}\{f(s') \mid s\ \tau\ s'\}\,) = \lambda f \in \Sigma \longmapsto \Sigma_{\bot} \bullet \lambda s \in \Sigma_{\bot} \bullet (\, s\ \tau\ s'\ ?\ f(s')\ ¿\ s\,) \triangleq F^{\mathrm{D}}$ since τ is locally deterministic so that s' is unique.

Moreover F^{D} is Scott-continuous since if f^{δ}, $\delta < \lambda$ is a $\dot{\sqsubseteq}^{\mathrm{D}}$ increasing chain and $s \in \Sigma$ then $F^{\mathrm{D}}(\bigsqcup_{\delta<\lambda} f^{\delta})(s) = (\, s\ \tau\ s'\ ?\ (\dot{\bigsqcup}_{\delta<\lambda} f^{\delta}))(s')\ ¿\ s\,) = (\, s\ \tau\ s'\ ?\ \bigsqcup_{\delta<\lambda} f^{\delta})(s')\ ¿\ s\,) = \bigsqcup_{\delta<\lambda}(\, s\ \tau\ s'\ ?\ f^{\delta}(s')\ ¿\ s\,) = \bigsqcup_{\delta<\lambda} F^{\mathrm{D}}(f^{\delta})(s) = (\dot{\bigsqcup}_{\delta<\lambda} F^{\mathrm{D}}(f^{\delta}))(s)$.

We conclude that $\tau^{\mathrm{D}} = \tau^{\top} \cap (\Sigma \longmapsto \Sigma_{\bot}) = \mathrm{lfp}_{\dot{\bot}}^{\dot{\sqsubseteq}^{\top}}\ F^{\top} = \mathrm{lfp}_{\dot{\bot}}^{\dot{\sqsubseteq}^{\top}}\ F^{\top}|_{\Sigma \longmapsto \Sigma_{\bot}} = \mathrm{lfp}_{\dot{\bot}}^{\dot{\sqsubseteq}^{\mathrm{D}}}\ F^{\mathrm{D}}$. □

9 Predicate Transformer Semantics

A *predicate* is a set of states may be augmented by $\bot$ to denote nontermination. A *predicate transformer* is a map of predicates to predicates. A *backward predicate transformer* maps a predicate called the *postcondition* to a predicate called the *precondition*. A *forward predicate transformer* maps a precondition to a postcondition.

9.1 Correspondences Between Denotational and Predicate Transformers Semantics

Various correspondences between denotational and predicate transformer semantics can be considered using the following maps (D, E are sets):

$$\begin{aligned}
\alpha^{-1} &\triangleq \lambda f \in D \longmapsto \wp(E) \bullet \lambda s' \bullet \{s \mid s' \in f(s)\}\\
\gamma^{-1} &\triangleq \lambda f \in E \longmapsto \wp(D) \bullet \lambda s \bullet \{s' \mid s \in f(s')\}\\
\alpha^{\triangleright} &\triangleq \lambda f \in D \longmapsto \wp(E) \bullet \lambda P \in \wp(D) \bullet \{s' \mid \exists s \in P : s' \in f(s)\}\\
\gamma^{\triangleright} &\triangleq \lambda \Psi \in \wp(D) \xrightarrow{\cup} \wp(E) \bullet \lambda s \bullet \Psi(\{s\})\\
\alpha^{\cup} &\triangleq \lambda \Psi \in \wp(D) \xrightarrow{\cup} \wp(E) \bullet \lambda Q \in \wp(E) \bullet \{s \mid \Psi(\{s\}) \cap Q \neq \emptyset\}\\
\gamma^{\cup} &\triangleq \lambda \Psi \in \wp(E) \xrightarrow{\cup} \wp(D) \bullet \lambda P \in \wp(D) \bullet \{s' \mid \Psi(\{s'\}) \cap P \neq \emptyset\}\\
\alpha^{\sim} &\triangleq \lambda \Psi \in \wp(D) \xrightarrow{\cup} \wp(E) \bullet \lambda P \in \wp(D) \bullet \neg(\Psi(\neg P))\\
\gamma^{\sim} &\triangleq \lambda \Psi \in \wp(E) \xrightarrow{\cap} \wp(D) \bullet \lambda P \in \wp(D) \bullet \neg(\Psi(\neg P))\\
\alpha^{\cap} &\triangleq \lambda \Phi \in \wp(D) \xrightarrow{\cap} \wp(E) \bullet \lambda Q \in \wp(E) \bullet \{s \mid \Phi(\neg\{s\}) \cup Q = E\}\\
\gamma^{\cap} &\triangleq \lambda \Phi \in \wp(E) \xrightarrow{\cap} \wp(D) \bullet \lambda P \in \wp(D) \bullet \{s' \mid \Phi(\neg\{s'\}) \cup P = D\}
\end{aligned}$$

Following [12], the correspondences between denotational and predicate transformers semantics are given as follows:

Theorem 9.1 (Denotational to predicate transformer Galois connection commutative diagram)

$$\begin{tikzcd}
\langle D \mapsto \wp(E),\ \dot{\subseteq}\rangle \arrow[r, shift left, leftarrow, two heads, "\gamma^{\triangleright}"] \arrow[r, shift right, two heads, "\alpha^{\triangleright}"'] \arrow[d, shift right, two heads, "\alpha^{-1}"'] \arrow[d, shift left, leftarrow, two heads, "\gamma^{-1}"] & \langle \wp(D) \overset{\cup}{\longmapsto} \wp(E),\ \dot{\subseteq}\rangle \arrow[r, shift left, leftarrow, two heads, "\gamma^{\sim}"] \arrow[r, shift right, two heads, "\alpha^{\sim}"'] \arrow[d, shift right, two heads, "\alpha^{\cup}"'] \arrow[d, shift left, leftarrow, two heads, "\gamma^{\cup}"] & \langle \wp(D) \overset{\cap}{\longmapsto} \wp(E),\ \dot{\supseteq}\rangle \arrow[d, shift right, two heads, "\alpha^{\cap}"'] \arrow[d, shift left, leftarrow, two heads, "\gamma^{\cap}"] \\
\langle E \mapsto \wp(D),\ \dot{\subseteq}\rangle \arrow[r, shift left, leftarrow, two heads, "\gamma^{\triangleright}"] \arrow[r, shift right, two heads, "\alpha^{\triangleright}"'] & \langle \wp(E) \overset{\cup}{\longmapsto} \wp(D),\ \dot{\subseteq}\rangle \arrow[r, shift left, leftarrow, two heads, "\gamma^{\sim}"] \arrow[r, shift right, two heads, "\alpha^{\sim}"'] & \langle \wp(E) \overset{\cap}{\longmapsto} \wp(D),\ \dot{\supseteq}\rangle
\end{tikzcd}$$

Proof. We have $\alpha^{-1} \circ \gamma^{-1}(\Phi) = \lambda s' \bullet \{s \mid s' \in \{s' \mid s \in \Phi(s')\}\} = \Phi$. The same way, $\gamma^{-1} \circ \alpha^{-1}(\Psi) = \lambda s \bullet \{s' \mid s \in \{s \mid s' \in \Psi(s)\}\} = \Psi$. We have $\alpha^{-1}(\Phi) \dot{\subseteq} \Psi$ if and only if $\forall s' : \alpha^{-1}(\Phi)(s') \subseteq \Psi(s')$ that is $\forall s' : \{s \mid s' \in \Phi(s)\} \subseteq \Psi(s')$ or equivalently $\forall s : \Phi(s) \subseteq \{s' \mid s \in \Psi(s')\}$ if and only if $\forall s : \Phi(s) \subseteq \gamma^{-1}(\Psi)(s)$ hence $\Phi \dot{\subseteq} \gamma^{-1}(\Psi)$. We conclude that $\langle D \longmapsto \wp(E),\ \dot{\subseteq}\rangle \underset{\alpha^{-1}}{\overset{\gamma^{-1}}{\leftrightarrows}} \langle E \longmapsto \wp(D),\ \dot{\subseteq}\rangle$.

If $f \in D \longmapsto \wp(E)$ then $\alpha^{\triangleright}[f](\bigcup_{i \in \Delta} P_i) = \{s' \mid \exists s \in \bigcup_{i \in \Delta} P_i : s' \in f(s)\} = \bigcup_{i \in \Delta} \{s' \mid \exists s \in P_i : s' \in f(s)\} = \bigcup_{i \in \Delta} \alpha^{\triangleright}[f](P_i)$ so that $\alpha^{\triangleright}[f] \in \wp(D) \overset{\cup}{\longmapsto} \wp(E)$.

$\alpha^{\triangleright}[f] \dot{\subseteq} \Psi$ if and only $\forall P \subseteq D : \forall s' \in E : \forall s \in P : s' \in f(s) \Longrightarrow s' \in \Psi(P)$ that is $\forall P \subseteq D : \forall s' \in E : \forall s \in D : s' \in f(s) \Longrightarrow (s \in P \Longrightarrow s' \in \Psi(P))$ whence $\forall P \subseteq D : f \dot{\subseteq} \lambda s \bullet \{s' \mid s \in P \Longrightarrow s' \in \Psi(P)\}$. It follows for $P = \{s\}$ that $f \dot{\subseteq} \lambda s \bullet \{s' \mid s' \in \Psi(\{s\})\}$ i.e. $f \dot{\subseteq} \gamma^{\triangleright}(\Psi)$. Reciprocally, $\forall s' \in f(s) : s' \in \Psi(\{s\})$ implies $\forall P \subseteq D : s' \in f(s) \Longrightarrow (s \in P \Longrightarrow s' \in \Psi(\{s\}))$ but $s \in P$ that is $\{s\} \subseteq P$ implies $\Psi(\{s\}) \subseteq \Psi(P)$ by monotony of $\Psi \in \wp(D) \overset{\cup}{\longmapsto} \wp(E)$, whence $\forall P \subseteq D : \forall s \in D : \forall s' \in E : s' \in f(s) \Longrightarrow (s \in P \Longrightarrow s' \in \Psi(P))$ thus proving $\alpha^{\triangleright}[f] \dot{\subseteq} \Psi$.

If $f \neq f'$ there exists $s' \in f(s)$ such that $s' \notin f'(s)$ or vice-versa. Therefore $\alpha^{\triangleright}[f](\{s\}) = \{s' \mid s' \in f(s)\} \neq \{s' \mid s' \in f'(s)\} = \alpha^{\triangleright}[f'](\{s\})$ so that $\alpha^{\triangleright}$ is injective.

If $\Psi \neq \Psi'$ then there is $P \subseteq D$ such that $\Psi(P) \neq \Psi'(P)$. This implies that there is a state $s \in P$ such that $\Psi(\{s\}) \neq \Psi'(\{s\})$ since otherwise $\Psi(P) = \Psi(\bigcup_{s \in P} \{s\}) = \bigcup_{s \in P} \Psi(\{s\}) = \bigcup_{s \in P} \Psi'(\{s\}) = \Psi'(P)$. It follows that $\exists s' \in \Psi(\{s\}) : s' \notin \Psi(\{s\})$ or vice-versa. Since $s' \in \gamma^{\triangleright}(\Psi)s$ but $s' \notin \gamma^{\triangleright}(\Psi')s$, we have $\gamma^{\triangleright}(\Psi) \neq \gamma^{\triangleright}(\Psi')$ proving that $\gamma^{\triangleright}$ is injective.

We conclude that $\langle D \longmapsto \wp(E),\ \dot{\subseteq}\rangle \underset{\alpha^{\triangleright}}{\overset{\gamma^{\triangleright}}{\leftrightarrows}} \langle \wp(D) \overset{\cup}{\longmapsto} \wp(E),\ \dot{\subseteq}\rangle$.

We have $\alpha^{\sim}[\Psi](\bigcap_{i \in \Delta} P_i) = \neg\Psi(\neg \bigcap_{i \in \Delta} P_i) = \neg\Psi(\bigcup_{i \in \Delta} \neg P_i) = \neg \bigcup_{i \in \Delta} \Psi(\neg P_i) = \bigcap_{i \in \Delta} \neg\Psi(\neg P_i) = \bigcap_{i \in \Delta} \alpha^{\sim}[\Psi](P_i)$. Dually, $\gamma^{\sim}[\Phi](\bigcup_{i \in \Delta} P_i) = \bigcap_{i \in \Delta} \gamma^{\sim}[\Psi](P_i)$.

We have $\alpha^{\sim}(\Psi) \dot{\subseteq} \Phi \Longleftrightarrow \forall P : \neg\Psi(\neg P) \subseteq \Phi(P) \Longleftrightarrow \forall P : \neg\Phi(P) \subseteq \Psi(\neg P) \Longleftrightarrow \forall Q : \neg\Phi(\neg Q) \subseteq \Psi(Q) \Longleftrightarrow \Psi \dot{\supseteq} \gamma^{\sim}(\Phi)$ where $Q = \neg P$.

Obviously $\alpha^{\sim}(\gamma^{\sim}(\Phi)) = \lambda P \bullet \neg\gamma^{\sim}(\Phi)(\neg P) = \lambda P \bullet \neg\neg\Phi(\neg\neg P) = \Phi$ and

$\gamma^{\sim}(\alpha^{\sim}(\Psi)) = \Psi$.

We conclude that $\langle \wp(D) \xmapsto{\cup} \wp(E),\ \dot{\subseteq}\rangle \mathrel{\underset{\alpha^{\sim}}{\overset{\gamma^{\sim}}{\leftrightarrows}}} \langle \wp(D) \xmapsto{\cap} \wp(E),\ \dot{\supseteq}\rangle$.

We have $\alpha^{\cup} \triangleq \alpha^{\triangleright} \circ \alpha^{-1} \circ \gamma^{\triangleright} = \lambda\Psi\boldsymbol{\cdot}\, \lambda Q\boldsymbol{\cdot}\{s \mid \exists s' \in Q : s \in \alpha^{-1} \circ \gamma^{\triangleright}(\Psi)s'\} = \lambda\Psi\boldsymbol{\cdot}\, \lambda Q\boldsymbol{\cdot}\{s \mid \exists s' \in Q : s' \in \gamma^{\triangleright}(\Psi)s\} = \lambda\Psi\boldsymbol{\cdot}\, \lambda Q\boldsymbol{\cdot}\{s \mid \exists s' \in Q : s' \in \Psi(\{s\})\} = \lambda\Psi\boldsymbol{\cdot}\, \lambda Q\boldsymbol{\cdot}\{s \mid \Psi(\{s\}) \cap Q \neq \emptyset\}$. Similarly $\gamma^{\cup} = \lambda\Psi\boldsymbol{\cdot}\, \lambda P\boldsymbol{\cdot}\{s' \mid \Psi(\{s'\}) \cap R \neq \emptyset\}$. By composition $\langle \wp(D) \xmapsto{\cup} \wp(E),\ \dot{\subseteq}\rangle \mathrel{\underset{\alpha^{\cup}}{\overset{\gamma^{\cup}}{\leftrightarrows}}} \langle \wp(E) \xmapsto{\cup} \wp(D),\ \dot{\subseteq}\rangle$.

Finally $\alpha^{\cap} = \alpha^{\sim} \circ \alpha^{\cup} \circ \gamma^{\sim} = \lambda\Phi\boldsymbol{\cdot}\, \alpha^{\sim}(\lambda Q\boldsymbol{\cdot}\, \alpha^{\cup}(\gamma^{\sim}(\Phi))(Q)) = \lambda\Phi\boldsymbol{\cdot}\, \lambda Q\boldsymbol{\cdot}\, \neg\alpha^{\cup}(\gamma^{\sim}(\Phi))(\neg Q) = \lambda\Phi\boldsymbol{\cdot}\, \lambda Q\boldsymbol{\cdot}\, \neg\{s \mid \gamma^{\triangleright}(\Phi)(\{s\}) \cap \neg Q \neq \emptyset\} = \lambda\Phi\boldsymbol{\cdot}\, \lambda Q\boldsymbol{\cdot}\{s \mid \neg\Phi(\neg\{s\}) \cap \neg Q = \emptyset\} = \lambda\Phi\boldsymbol{\cdot}\, \lambda Q\boldsymbol{\cdot}\{s \mid \neg(\neg\Phi(\neg\{s\}) \cap \neg)Q = \neg(\emptyset)\} = \lambda\Phi\boldsymbol{\cdot}\, \lambda Q\boldsymbol{\cdot}\{s \mid \Phi(\neg\{s\}) \cup Q = E\}$. The same way $\gamma^{\cap} = \lambda\Phi\boldsymbol{\cdot}\, \lambda P\boldsymbol{\cdot}\{s' \mid \Phi(\neg\{s'\}) \cup P = D\}$. By composition $\langle \wp(D) \xmapsto{\cap} \wp(E),\ \dot{\supseteq}\rangle \mathrel{\underset{\alpha^{\cap}}{\overset{\gamma^{\cap}}{\leftrightarrows}}} \langle \wp(E) \xmapsto{\cap} \wp(D),\ \dot{\supseteq}\rangle$. □

After [24], we define ($f \in D \longmapsto \wp(E)$):

$$\begin{aligned}
\mathrm{gsp}\llbracket f\rrbracket &\triangleq \alpha^{\triangleright}[f] \ \in\ \wp(D) \xmapsto{\cup} \wp(E)\\
&= \lambda P \in \wp(D)\boldsymbol{\cdot}\{s' \in E \mid \exists s \in P : s' \in f(s)\}\\
\mathrm{gspa}\llbracket f\rrbracket &\triangleq \alpha^{\sim} \circ \alpha^{\triangleright}[f] \ \in\ \wp(D) \xmapsto{\cap} \wp(E)\\
&= \lambda P \in \wp(D)\boldsymbol{\cdot}\{s' \in E \mid \forall s \in D : s' \in f(s) \Longrightarrow s \in P\}\\
\mathrm{gwp}\llbracket f\rrbracket &\triangleq \alpha^{\sim} \circ \alpha^{\triangleright} \circ \alpha^{-1}[f] \ \in\ \wp(E) \xmapsto{\cap} \wp(D)\\
&= \lambda Q \in \wp(E)\boldsymbol{\cdot}\{s \in D \mid \forall s' \in E : s' \in f(s) \Longrightarrow s' \in Q\}\\
\mathrm{gwpa}\llbracket f\rrbracket &\triangleq \alpha^{\triangleright} \circ \alpha^{-1}[f] \ \in\ \wp(E) \xmapsto{\cup} \wp(D)\\
&= \lambda Q \in \wp(E)\boldsymbol{\cdot}\{s \in D \mid \exists s' \in Q : s' \in f(s)\}
\end{aligned}$$

Combined with the natural $\tau^{\natural}$, angelic $\tau^{\flat}$ and demoniac $\tau^{\sharp}$ denotational semantics, we get twelve predicate transformer semantics, some of which such as E. Dijkstra [18] weakest precondition[6] $\mathrm{wp}(\tau^{\vec{\infty}}, Q) \triangleq \mathrm{gwp}\llbracket\tau^{\natural}\rrbracket\, Q$ and weakest liberal precondition $\mathrm{wlp}(\tau^{\vec{\infty}}, Q) \triangleq \mathrm{gwp}\llbracket\tau^{\flat}\rrbracket\, Q$ of postcondition $Q \subseteq \Sigma$ are well-known. E. Dijkstra postulated healthiness conditions of predicate transformers [18] indeed follow from $\mathrm{gwp}\llbracket\tau^{\natural}\rrbracket \in \wp(\Sigma) \xmapsto{\cap} \wp(\Sigma)$ (Conjunctivitis) and $\mathrm{gwp}\llbracket\tau^{\natural}\rrbracket\, \emptyset = \emptyset$ since $\tau^{\natural}$ is total by theorem 8.1 and lemma 8.3 (Excluded Miracle).

In order to establish the equivalence of forward and backward predicate transformers and proof methods, we observe [7,19] that $\mathrm{gsp}\llbracket f\rrbracket\, P \subseteq Q$ if and only if $\forall s' \in E : (\exists s \in P : s' \in f(s)) \Longrightarrow s' \in Q$ hence $\forall s \in P : (\forall s' \in E : s' \in f(s) \Longrightarrow s' \in Q)$ that is $P \subseteq \mathrm{gwp}\llbracket f\rrbracket\, Q$, and reciprocally, proving for all $f \in D \longmapsto \wp(E)$ that:

Lemma 9.2 (Correspondence between pre- and postcondition semantics) *If* $f \in D \longmapsto \wp(E)$ *then* $\langle \wp(D),\ \subseteq\rangle \mathrel{\underset{\mathrm{gsp}\llbracket f\rrbracket}{\overset{\mathrm{gwp}\llbracket f\rrbracket}{\leftrightarrows}}} \langle \wp(E),\ \subseteq\rangle$.

[6] E. Dijkstra's notation is $\mathrm{wp}(C, Q)$ where C is a command and Q is a postcondition so that we use $\tau^{\vec{\infty}}$ which should be understood as the maximal trace semantics of the command C.

9.2 Generalized Weakest Precondition Semantics

The *generalized weakest precondition semantics* is $\tau^{\mathrm{gwp}} \stackrel{\Delta}{=} \mathrm{gwp}[\![\tau^{\natural}]\!]$. It combines the expressive power of the conservative and liberal weakest preconditions since for $Q \subseteq \Sigma$, we have $\tau^{\mathrm{gwp}}[\![Q]\!] = \mathrm{wp}(\tau^{\vec{\infty}}, Q)$ and $\tau^{\mathrm{gwp}}[\![Q \cup \{\bot\}]\!] = \mathrm{wlp}(\tau^{\vec{\infty}}, Q)$. Applying S. Kleene transfer theorem 2.3 to the fixpoint natural nondeterministic denotational semantics 8.1 with the correspondence $\langle \alpha^{\mathrm{gwp}}, \gamma^{\mathrm{gwp}} \rangle$ where $\alpha^{\mathrm{gwp}} \stackrel{\Delta}{=} \mathrm{gwp} = \alpha^{\sim} \circ \alpha^{\triangleright} \circ \alpha^{-1}$ and $\gamma^{\mathrm{gwp}} \stackrel{\Delta}{=} \gamma^{-1} \circ \gamma^{\triangleright} \circ \gamma^{\sim}$ which, according to theorem 9.1, is a Galois bijection, we derive[7]:

Theorem 9.3 (Fixpoint generalized weakest precondition semantics) *$\tau^{\mathrm{gwp}} = \mathrm{lfp}_{\bot^{\mathrm{gwp}}}^{\sqsubseteq^{\mathrm{gwp}}} F^{\mathrm{gwp}}$ where $F^{\mathrm{gwp}} \in D^{\mathrm{gwp}} \xmapsto{m} D^{\mathrm{gwp}}$ defined as $F^{\mathrm{gwp}}(\Phi) \stackrel{\Delta}{=} \lambda Q \bullet (\neg\check{\tau} \cup Q) \,\dot{\cap}\, \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!] \circ \Phi = \lambda Q \bullet (Q \cap \check{\tau}) \,\dot{\cup}\, \mathrm{wp}[\![\tau^{\blacktriangleright}]\!] \circ \Phi$ where $\mathrm{wp}[\![f]\!]\, Q \stackrel{\Delta}{=} \{s \in \Sigma \mid \exists s' \in \Sigma : s' \in f(s) \wedge \forall s' \in f(s) : s' \in Q\}$ is a $\sqsubseteq^{\mathrm{gwp}}$-monotone map on the complete lattice $\langle D^{\mathrm{gwp}}, \sqsubseteq^{\mathrm{gwp}}, \bot^{\mathrm{gwp}}, \top^{\mathrm{gwp}}, \sqcup^{\mathrm{gwp}}, \sqcap^{\mathrm{gwp}} \rangle$ with $D^{\mathrm{gwp}} \stackrel{\Delta}{=} \wp(\Sigma_{\bot}) \xmapsto{\cap} \wp(\Sigma)$, $\Phi \sqsubseteq^{\mathrm{gwp}} \Psi \stackrel{\Delta}{=} \forall Q \subseteq \Sigma : \Psi(Q \cup \{\bot\}) \subseteq \Phi(Q \cup \{\bot\}) \wedge \Phi(\Sigma) \subseteq \Psi(\Sigma)$, $\bot^{\mathrm{gwp}} = \lambda Q \bullet (\bot \in Q \;?\; \Sigma \;¿\; \emptyset)$ and $\bigsqcup^{\mathrm{gwp}}_{i \in \Delta} \Psi_i \stackrel{\Delta}{=} \lambda Q \bullet \bigcap_{i \in \Delta} \Psi_i(Q \cup \{\bot\}) \cap (\bot \notin Q \;?\; \bigcup_{i \in \Delta} \Psi_i(\Sigma) \;¿\; \Sigma)$.*

Proof. By the Galois bijection $\langle \Sigma \longmapsto \wp(\Sigma_{\bot}), \dot{\subseteq} \rangle \underset{\alpha^{\mathrm{gwp}}}{\overset{\gamma^{\mathrm{gwp}}}{\leftrightarrows}} \langle \wp(\Sigma_{\bot} \xmapsto{\cup} \wp(\Sigma), \dot{\supseteq} \rangle$ $\langle D^{\mathrm{gwp}}, \sqsubseteq^{\mathrm{gwp}}, \bot^{\mathrm{gwp}}, \top^{\mathrm{gwp}}, \sqcup^{\mathrm{gwp}}, \sqcap^{\mathrm{gwp}} \rangle$ is a complete lattice where $\Phi \sqsubseteq^{\mathrm{gwp}} \Psi \stackrel{\Delta}{=} \gamma^{\mathrm{gwp}}(\Phi) \,\dot{\sqsubseteq}^{\natural}\, \gamma^{\mathrm{gwp}}(\Psi)$, $\bot^{\mathrm{gwp}} \stackrel{\Delta}{=} \alpha^{\mathrm{gwp}}(\bot^{\natural})$ (so that α^{gwp} is bottom-strict) and $\bigsqcup^{\mathrm{gwp}}_{i \in \Delta} \Phi_i \stackrel{\Delta}{=} \alpha^{\mathrm{gwp}}(\dot{\bigsqcup}^{\natural}_{i \in \Delta} \gamma^{\mathrm{gwp}}(\Phi_i))$ (so that α^{gwp} is Scott-continuous).

We get $\bot^{\mathrm{gwp}} \stackrel{\Delta}{=} \mathrm{gwp}(\bot^{\natural}) = \lambda Q \in \wp(\Sigma_{\bot}) \bullet \{s \in \Sigma \mid \forall s' \in \Sigma : s' \in \{\bot\} \Longrightarrow s' \in Q\} = \lambda Q \in \wp(\Sigma_{\bot}) \bullet \{s \in \Sigma \mid \bot \in Q\} = \lambda Q \in \wp(\Sigma_{\bot}) \bullet (\bot \in Q \;?\; \Sigma \;¿\; \emptyset)$. The same way, $\top^{\mathrm{gwp}} \stackrel{\Delta}{=} \mathrm{gwp}(\top^{\natural}) = \lambda Q \in \wp(\Sigma_{\bot}) \bullet \{s \in \Sigma \mid \forall s' \in \Sigma_{\bot} : s' \in \Sigma \Longrightarrow s' \in Q\} = \lambda Q \in \wp(\Sigma_{\bot}) \bullet \{s \in \Sigma \mid \forall s' \in \Sigma : s' \in Q\} = \lambda Q \in \wp(\Sigma_{\bot}) \bullet \{s \in \Sigma \mid \Sigma \subseteq Q\} = \lambda Q \in \wp(\Sigma_{\bot}) \bullet (\Sigma \subseteq Q \;?\; \Sigma \;¿\; \emptyset)$.

We have $\gamma^{\mathrm{gwp}}(\Phi) \stackrel{\Delta}{=} \gamma^{-1} \circ \gamma^{\triangleright} \circ \gamma^{\sim}(\Phi) = \lambda s \bullet \{s' \in \Sigma_{\bot} \mid s \in \gamma^{\triangleright} \circ \gamma^{\sim}(\Phi)(s')\} = \lambda s \bullet \{s' \in \Sigma_{\bot} \mid s \in \gamma^{\sim}(\Phi)(\{s'\})\} = \lambda s \bullet \{s' \in \Sigma_{\bot} \mid s \notin \Phi(\neg\{s'\})\}$.

It follows that $\Phi \sqsubseteq^{\mathrm{gwp}} \Psi \stackrel{\Delta}{=} \gamma^{\mathrm{gwp}}(\Phi) \,\dot{\sqsubseteq}^{\natural}\, \gamma^{\mathrm{gwp}}(\Psi) = \forall s \in \Sigma : \{s' \mid s \notin \Phi(\neg\{s'\})\} \cap \Sigma \subseteq \{s' \mid s \notin \Psi(\neg\{s'\})\} \cap \Sigma \wedge \{s' \mid s \notin \Phi(\neg\{s'\})\} \cap \{\bot\} \supseteq \{s' \mid s \notin \Psi(\neg\{s'\})\} \cap \{\bot\} = \forall s' \in \Sigma : \Psi(\neg\{s'\}) \subseteq \Phi(\neg\{s'\}) \wedge \Psi(\Sigma) \supseteq \Phi(\Sigma)$.

Assume that $\forall s' \in \Sigma : \Psi(\neg\{s'\}) \subseteq \Phi(\neg\{s'\})$ and $P \subseteq \Sigma$. Then $\Psi(\neg P) = \Psi(\bigcap_{s' \in P} \neg\{s'\}) = \bigcap_{s' \in P} \Psi(\neg\{s'\})$ and the same way for $\Phi \in D^{\mathrm{gwp}}$. So $\Psi(\neg P) \subseteq \Phi(\neg P)$ whence $\forall Q \subseteq \Sigma : \Psi(Q \cup \{\bot\}) \subseteq \Phi(Q \cup \{\bot\})$ where $Q \cup \{\bot\} = \neg P$ in $\Sigma_{\bot}$ whence $Q = \neg P$ in Σ. Reciprocally, if $\forall Q \subseteq \Sigma : \Psi(Q \cup \{\bot\}) \subseteq \Phi(Q \cup \{\bot\})$ then for all $s' \in \Sigma$ and $Q = \Sigma \setminus \{s'\}$ we have $Q \cup \{\bot\} = \Sigma_{\bot} \setminus \{s'\} = \neg\{s'\}$ whence $\Psi(\neg\{s'\}) \subseteq \Phi(\neg\{s'\})$.

[7] Observe that $\sqsubseteq^{\mathrm{gwp}}$ coincides with the partial ordering $\sqsubseteq$ of [31] except that the explicit use of $\bot$ to denote nontermination dispenses with the handling of two formulae to express τ^{gwp} in terms of τ^{wp} and τ^{wlp}.

We conclude that $\Phi \sqsubseteq^{\mathrm{gwp}} \Psi = \forall Q \subseteq \Sigma : \Psi(Q \cup \{\bot\}) \subseteq \Phi(Q \cup \{\bot\}) \wedge \Phi(\Sigma) \subseteq \Psi(\Sigma)$.

We have $\bigsqcup^{\natural}_{i\in\Delta} \gamma^{\mathrm{gwp}}(\Psi_i)(s) = \bigsqcup^{\natural}_{i\in\Delta} \{s' \in \Sigma_\bot \mid s \notin \Psi_i(\neg\{s'\})\} = \bigcup_{i\in\Delta} \{s' \in \Sigma \mid s \notin \Psi_i(\neg\{s'\})\} \cup \bigcap_{i\in\Delta} \{s' \in \{\bot\} \mid s \notin \Psi_i(\neg\{s'\})\} = \bigcup_{i\in\Delta} \{s' \in \Sigma \mid s \notin \Psi_i(\neg\{s'\})\} \cup \bigcap_{i\in\Delta} \{\bot \mid s \notin \Psi_i(\Sigma)\}$.

It follows that $\bigsqcup^{\mathrm{gwp}}_{i\in\Delta} \Psi_i \stackrel{\Delta}{=} \mathrm{gwp}(\lambda s \bullet \bigsqcup^{\natural}_{i\in\Delta} \gamma^{\mathrm{gwp}}(\Psi_i)(s)) = \lambda Q \in \wp(\Sigma_\bot) \bullet \{s \in \Sigma \mid \forall s' \in \Sigma_\bot : s' \in (\bigcup_{i\in\Delta} \{s' \in \Sigma \mid s \in \neg\Psi_i(\neg\{s'\})\} \cup \bigcap_{i\in\Delta} \{\bot \mid s \in \neg\Psi_i(\Sigma)\}) \Longrightarrow s' \in Q\} = \lambda Q \in \wp(\Sigma_\bot) \bullet \{s \in \Sigma \mid \forall s' \in \Sigma : ((s \in \bigcup_{i\in\Delta} \neg\Psi_i(\neg\{s'\})) \Longrightarrow s' \in Q) \wedge ((s \in \bigcap_{i\in\Delta} \neg\Psi_i(\Sigma)) \Longrightarrow \bot \in Q)\} = \lambda Q \in \wp(\Sigma_\bot) \bullet \{s \in \Sigma \mid \forall s' \in \Sigma : ((s \notin \bigcap_{i\in\Delta} \Psi_i(\neg\{s'\})) \Longrightarrow s' \in Q) \wedge ((s \notin \bigcup_{i\in\Delta} \Psi_i(\Sigma)) \Longrightarrow \bot \in Q)\} = \lambda Q \in \wp(\Sigma_\bot) \bullet \{s \in \Sigma \mid \forall s' \in \Sigma : (s' \notin Q \Longrightarrow (s \in \bigcap_{i\in\Delta} \Psi_i(\neg\{s'\}))) \wedge (\bot \notin Q \Longrightarrow (s \in \bigcup_{i\in\Delta} \Psi_i(\Sigma)))\} = \lambda Q \in \wp(\Sigma_\bot) \bullet \{s \in \Sigma \mid \forall s' \in \Sigma \cap \neg Q : s \in \bigcap_{i\in\Delta} \Psi_i(\neg\{s'\})\} \cap (\, \bot \notin Q \;?\; \bigcup_{i\in\Delta} \Psi_i(\Sigma) \;\text{¿}\; \Sigma\,)$.

We have $\{s \in \Sigma \mid \forall s' \in \Sigma \cap \neg Q : s \in \bigcap_{i\in\Delta} \Psi_i(\neg\{s'\})\} = \bigcap_{s' \in \Sigma\cap\neg Q} \bigcap_{i\in\Delta} \Psi_i(\neg\{s'\}) = \bigcap_{i\in\Delta} \Psi_i(\bigcap_{s' \in \Sigma\cap\neg Q} \neg\{s'\}) = \bigcap_{i\in\Delta} \Psi_i(\neg \bigcup_{s' \in \Sigma\cap\neg Q} \{s'\}) = \bigcap_{i\in\Delta} \Psi_i(\neg(\Sigma \cap \neg Q)) = \bigcap_{i\in\Delta} \Psi_i(\{\bot\} \cup Q)$.

We conclude that $\bigsqcup^{\mathrm{gwp}}_{i\in\Delta} \Psi_i = \lambda Q \bullet \bigcap_{i\in\Delta} \Psi_i(\{\bot\} \cup Q) \cap (\, \bot \notin Q \;?\; \bigcup_{i\in\Delta} \Psi_i(\Sigma) \;\text{¿}\; \Sigma\,)$.

Finally we design F^{gwp} by the commutation condition. If $Q \in \wp(\Sigma_\bot)$ then $\alpha^{\mathrm{gwp}}(F^{\natural}(f))Q = \{s \in \Sigma \mid \forall s' : s' \in (\dot{\check{\tau}}(s) \cup \bigcup f^{\blacktriangleright} \circ \tau^{\blacktriangleright}(s)) \Longrightarrow s' \in Q\} = \{s \in \Sigma \mid (\forall s'' : \neg(s \;\tau\; s'')) \Longrightarrow s \in Q\} \cap \{s \in \Sigma \mid \forall s' : (\exists s'' : s \;\tau\; s'' \wedge s' \in f(s'')) \Longrightarrow s' \in Q\} = \{s \in \Sigma \mid \tau^{\blacktriangleright}(s) = \emptyset \vee s \in Q\} \cap \{s \in \Sigma \mid \forall s'' : s \;\tau\; s'' \Longrightarrow (\forall s' : s' \in f(s'') \Longrightarrow s' \in Q)\} = (\neg\check{\tau} \cup Q) \cap \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!] \circ \mathrm{gwp}[\![f]\!](Q) = F^{\mathrm{gwp}}(\alpha^{\mathrm{gwp}}(f))(Q)$, by defining $F^{\mathrm{gwp}} \stackrel{\Delta}{=} \lambda f \bullet \lambda Q \bullet (\neg\check{\tau} \cup Q) \mathbin{\dot{\cap}} \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!] \circ f$. But $\lambda Q \bullet (\neg\check{\tau} \cup Q) \cap \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!] \circ f(Q) = \lambda Q \bullet (\neg\check{\tau} \cup (\check{\tau} \cap Q)) \cap \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!] \circ f(Q) = \lambda Q \bullet (\neg\check{\tau} \cap \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!] \circ f(Q)) \cup (\check{\tau} \cap Q \cap \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!] \circ f(Q)) = \lambda Q \bullet \{s \mid \exists s' : s \;\tau\; s' \wedge \forall s' \in \tau^{\blacktriangleright}(s) : s' \in f(Q)\} \cup (Q \cap \{s \mid \forall s' : \neg(s \;\tau\; s') \wedge \forall s' \in \tau^{\blacktriangleright}(s) : s' \in f(Q)\}) = \lambda Q \bullet \mathrm{wp}[\![\tau^{\blacktriangleright}]\!] \circ f(Q) \cup (Q \cap \check{\tau})$.

By the commutation condition $\alpha^{\mathrm{gwp}} \circ F^{\natural} = F^{\mathrm{gwp}} \circ \alpha^{\mathrm{gwp}}$ so that $\alpha^{\mathrm{gwp}} \circ F^{\natural} \circ \gamma^{\mathrm{gwp}} = F^{\mathrm{gwp}} \circ \alpha^{\mathrm{gwp}} \circ \gamma^{\mathrm{gwp}} = F^{\mathrm{gwp}}$. It follows that $f \sqsubseteq^{\mathrm{gwp}} g$ implies $\gamma^{\mathrm{gwp}}(f) \sqsubseteq^{\natural} \gamma^{\mathrm{gwp}}(g)$ that is $F^{\natural}(\gamma^{\mathrm{gwp}}(f)) \sqsubseteq^{\natural} F^{\natural}(\gamma^{\mathrm{gwp}}(g))$ by theorem 7.5 whence $\gamma^{\mathrm{gwp}} \circ \alpha^{\mathrm{gwp}} \circ F^{\natural} \circ \gamma^{\mathrm{gwp}}(f) \sqsubseteq^{\natural} \gamma^{\mathrm{gwp}} \circ \alpha^{\mathrm{gwp}} \circ F^{\natural} \circ \gamma^{\mathrm{gwp}}(g)$. Therefore $\gamma^{\mathrm{gwp}}(F^{\mathrm{gwp}}(f)) \sqsubseteq^{\natural} \gamma^{\mathrm{gwp}}(F^{\mathrm{gwp}}(g))$ hence $F^{\mathrm{gwp}}(f) \sqsubseteq^{\mathrm{gwp}} F^{\mathrm{gwp}}(g)$ proving that F^{gwp} is $\sqsubseteq^{\mathrm{gwp}}$-monotone.□

Lemma 9.4 (Arrangement of the iterates of F^{gwp}) *Let $F^{\mathrm{gwp}^{\delta}}$, $\delta \in \mathbb{O}$ be the iterates of F^{gwp} from $\bot^{\mathrm{gwp}}$. For all $\eta < \xi$ and $Q \subseteq \Sigma_\bot$, we have $F^{\mathrm{gwp}^{\eta}}(Q \setminus \{\bot\}) \subseteq F^{\mathrm{gwp}^{\xi}}(Q \setminus \{\bot\})$.*

Proof. The proof of theorem 9.3 shows, by S. Kleene fixpoint theorem 2.3, that $\forall \delta \in \mathbb{O} : F^{\mathrm{gwp}^{\delta}} = \mathrm{gwp}[\![F^{\mathrm{gwp}^{\delta}}]\!]$. By reductio ad absurdum, if there exists $Q \subseteq \Sigma$ such that $F^{\mathrm{gwp}^{\eta}}(Q) \not\subseteq F^{\mathrm{gwp}^{\xi}}(Q)$ then $\exists s \in \mathrm{gwp}[\![F^{\natural^{\eta}}]\!]\,Q : s \notin \mathrm{gwp}[\![F^{\natural^{\xi}}]\!]\,Q$

which implies $\exists s : \forall s'' \in \Sigma_\bot : s'' \in F^{\natural^{\eta}}(s) \Longrightarrow s'' \in Q \wedge \exists s' \in \Sigma_\bot : s' \in F^{\natural^{\xi}}(s) \wedge s' \notin Q$ hence $\exists s, s' : \bot \notin F^{\natural^{\eta}}(s) \wedge s' \in F^{\natural^{\xi}}(s) \wedge s' \notin F^{\natural^{\eta}}(s)$ in contradiction with lemma 8.2. □

Lemma 9.5 (Strictness of the iterates of F^{gwp}) *Let $F^{\mathrm{gwp}^{\delta}}$, $\delta \in \mathbb{O}$ be the iterates of F^{gwp} from $\bot^{\mathrm{gwp}}$. $\forall \delta \in \mathbb{O} : F^{\mathrm{gwp}^{\delta}}(\emptyset) = \emptyset$.*

Proof. The proof of theorem 9.3 shows, by S. Kleene fixpoint theorem 2.3, that $\forall \delta \in \mathbb{O} : F^{\mathrm{gwp}^{\delta}} = \mathrm{gwp}\llbracket F^{\mathrm{gwp}^{\delta}} \rrbracket$. So $F^{\mathrm{gwp}^{\delta}}(\emptyset) = \{s \in \Sigma \mid \forall s' \in \Sigma_\bot : s' \in F^{\natural^{\delta}}(s) \Longrightarrow s' \in \emptyset\} = \{s \in \Sigma \mid \forall s' \in \Sigma_\bot : s' \notin F^{\natural^{\delta}}(s)\} = \{s \in \Sigma \mid F^{\natural^{\delta}}(s) = \emptyset\}$ $= \emptyset$ by lemma 8.3. □

Lemma 9.6 (Final states of the iterates of F^{gwp}) *Let $F^{\mathrm{gwp}^{\delta}}$, $\delta \in \mathbb{O}$ be the iterates of F^{gwp} from $\bot^{\mathrm{gwp}}$. $\forall \delta \in \mathbb{O} : \forall Q \subseteq \Sigma_\bot : F^{\mathrm{gwp}^{\delta}}(Q \setminus \{\bot\}) \subseteq F^{\mathrm{gwp}^{\delta}}(\check{\tau})$.*

Proof. The proof of theorem 9.3 shows, by S. Kleene fixpoint theorem 2.3, that $\forall \delta \in \mathbb{O} : F^{\mathrm{gwp}^{\delta}} = \mathrm{gwp}\llbracket F^{\natural^{\delta}} \rrbracket$. So if $s \in F^{\mathrm{gwp}^{\delta}}(Q \setminus \{\bot\})$ then $\forall s' \in \Sigma_\bot : s' \in F^{\natural^{\delta}}(s) \Longrightarrow s' \in Q \setminus \{\bot\}$ so $\bot \notin F^{\natural^{\delta}}(s)$ hence, by lemma 8.4, $\forall s' \in \Sigma_\bot : s' \in F^{\natural^{\delta}}(s) \Longrightarrow s' \in \check{\tau}$ proving that $s \in F^{\mathrm{gwp}^{\delta}}(\check{\tau})$. □

Total correctness is the conjunction of partial correctness and termination in that $\forall Q \subseteq \Sigma : \tau^{\mathrm{gwp}}\llbracket Q \rrbracket = \tau^{\mathrm{gwp}}\llbracket Q \cup \{\bot\} \rrbracket \cap \tau^{\mathrm{gwp}}\llbracket \Sigma \rrbracket$ since τ^{gwp} is a complete $\cap$-morphism. We have $\check{\tau} \subseteq \Sigma$ so $\tau^{\mathrm{gwp}}\llbracket \check{\tau} \rrbracket \subseteq \tau^{\mathrm{gwp}}\llbracket \Sigma \rrbracket$ by monotony and $\tau^{\mathrm{gwp}}\llbracket \Sigma \rrbracket \subseteq \tau^{\mathrm{gwp}}\llbracket \check{\tau} \rrbracket$ by lemma 9.6 and theorem 9.3 so that by antisymmetry: $\forall Q \subseteq \Sigma : \tau^{\mathrm{gwp}}\llbracket Q \rrbracket = \tau^{\mathrm{gwp}}\llbracket Q \cup \{\bot\} \rrbracket \cap \tau^{\mathrm{gwp}}\llbracket \check{\tau} \rrbracket$.

9.3 E. Dijkstra Weakest Conservative Precondition Semantics

E. Dijkstra's *weakest conservative precondition semantics* [18] is $\tau^{\mathrm{wp}} \triangleq \alpha^{\mathrm{wp}}(\tau^{\mathrm{gwp}})$ (traditionally written $\lambda Q \in \wp(\Sigma) \cdot \mathrm{wp}(\tau^{\vec{\infty}}, Q)$) where the abstraction $\alpha^{\mathrm{wp}} \triangleq \lambda \Phi \cdot \Phi|_{\wp(\Sigma)}$ satisfies:

Lemma 9.7 (Weakest conservative precondition abstraction) $\langle D^{\mathrm{gwp}}, \dot{\supseteq}\rangle \mathrel{\underset{\alpha^{\mathrm{wp}}}{\overset{\gamma^{\mathrm{wp}}}{\leftrightarrows}}} \langle D^{\mathrm{wp}}, \dot{\supseteq}\rangle$ *where* $D^{\mathrm{wp}} \triangleq \wp(\Sigma) \overset{\cap}{\longmapsto} \wp(\Sigma)$ *and* $\gamma^{\mathrm{wp}}(\Psi) \triangleq \lambda Q \cdot (\bot \notin Q \;?\; \Psi(Q) \;¿\; \emptyset)$.

Proof. $\alpha^{\mathrm{wp}}(\Phi) \mathrel{\dot{\supseteq}} \Psi \Longleftrightarrow \forall Q \subseteq \Sigma : \Phi|_{\wp(\Sigma)}(Q) \supseteq \Psi(Q) \Longleftrightarrow \forall Q \subseteq \Sigma_\bot : \Phi(Q) \supseteq (\bot \notin Q \;?\; \Psi(Q) \;¿\; \emptyset) \Longleftrightarrow \forall Q \subseteq \Sigma_\bot : \Phi(Q) \supseteq \gamma^{\mathrm{wp}}(\Psi)(Q) \Longleftrightarrow \Phi \mathrel{\dot{\supseteq}} \gamma^{\mathrm{wp}}(\Psi)$. □

Dijkstra's weakest conservative precondition semantics τ^{wp} is an abstraction of the demoniac denotational semantics [2]:

Lemma 9.8 (Abstraction of the demoniac nondeterministic denotational semantics) $\tau^{\mathrm{wp}} = \alpha^{\mathrm{wp}}(\mathrm{gwp}\llbracket \tau^{\sharp} \rrbracket)$.

Proof. We have $\tau^{\mathrm{wp}} \triangleq \alpha^{\mathrm{wp}}(\tau^{\mathrm{gwp}}) = \alpha^{\mathrm{wp}}(\mathrm{gwp}\llbracket \tau^{\natural} \rrbracket) = \lambda Q \in \wp(\Sigma) \cdot \{s \in \Sigma \mid \forall s' \in \Sigma_\bot : s' \in \tau^{\natural}(s) \Longrightarrow s' \in Q\} = \lambda Q \in \wp(\Sigma) \cdot \{s \in \Sigma \mid \bot \notin \tau^{\natural}(s) \wedge \forall s' \in \Sigma_\bot : s' \in \tau^{\natural}(s) \Longrightarrow s' \in Q\}$ since $\bot \notin Q$. This is $\lambda Q \in \wp(\Sigma) \cdot \{s \in \Sigma \mid \forall s' \in \Sigma_\bot : (\bot \in \tau^{\natural}(s) \Longrightarrow s' \in Q) \wedge (\bot \notin \tau^{\natural}(s) \wedge s' \in \tau^{\natural}(s) \Longrightarrow s' \in Q)\} =$

$\lambda Q \in \wp(\Sigma) \cdot \{s \in \Sigma \mid \forall s' \in \Sigma_\perp : (s' \in \tau^\natural(s) \cup \{s'' \in \Sigma \mid \perp \in \tau^\natural(s)\}) \Longrightarrow s' \in Q\} = \lambda Q \in \wp(\Sigma) \cdot \{s \in \Sigma \mid \forall s' \in \Sigma_\perp : s' \in \alpha^\sharp(\tau^\natural)(s) \Longrightarrow s' \in Q\} = \alpha^{\text{wp}}(\text{gwp}[\![\alpha^\sharp(\tau^\natural)]\!]) = \alpha^{\text{wp}}(\text{gwp}[\![\tau^\sharp]\!])$ by lemma 8.6. □

E. Dijkstra's fixpoint characterization [18] of the conservative precondition semantics τ^{wp} will be derived from theorem 8.14, by abstraction for a given post-condition $Q \subseteq \Sigma$:

Lemma 9.9 *If $Q \subseteq E$ then $\langle \wp(E) \overset{\cap}{\longmapsto} \wp(D),\ \dot{\supseteq} \rangle \underset{\alpha^Q}{\overset{\gamma^Q}{\leftrightarrows}} \langle \wp(D),\ \supseteq \rangle$ where $\alpha^Q(\Phi) \triangleq \Phi(Q)$ and $\gamma^Q(P) \triangleq \lambda R \cdot (Q \subseteq R\ ?\ P\ ¿\ \emptyset)$.*

Proof. If $Q \subseteq \bigcap_{i \in \Delta} P_i$ then $\forall i \in \Delta : Q \subseteq P_i$ whence $\gamma^Q(\bigcap_{i \in \Delta} P_i) = \bigcap_{i \in \Delta} \gamma^Q(P_i) = P$ else $Q \not\subseteq \bigcap_{i \in \Delta} P_i$ in which case $\exists j \in \Delta : Q \not\subseteq P_j$ whence $\gamma^Q(\bigcap_{i \in \Delta} P_i) = \gamma^Q(P_j) = \emptyset = \gamma^Q(\bigcap_{i \in \Delta} P_i)$ proving that $\gamma^Q \in \wp(D) \longmapsto (\wp(E) \overset{\cap}{\longmapsto} \wp(D))$.

Moreover $\alpha^Q(\Phi) \supseteq P \iff \Phi(Q) \supseteq P \iff \forall R : \Phi(R) \supseteq (Q = R\ ?\ P\ ¿\ \emptyset) \iff \Phi \mathrel{\dot{\supseteq}} \gamma^Q(P)$ since Φ is monotone. □

By composition of lemmata 9.9, 9.8 and theorem 9.1, we get:

Corollary 9.10 (Demoniac to weakest conservative precondition abstraction) *For all $Q \subseteq \Sigma$, $\langle \Sigma \longmapsto \wp(\Sigma_\perp),\ \dot{\subseteq} \rangle \underset{\gamma^{\text{gwp}} \circ \gamma^{\text{wp}} \circ \gamma^Q}{\overset{\alpha^Q \circ \alpha^{\text{wp}} \circ \alpha^{\text{gwp}}}{\leftrightarrows}} \langle \wp(\Sigma),\ \supseteq \rangle$ where $\alpha^Q \circ \alpha^{\text{wp}} \circ \alpha^{\text{gwp}} = \lambda f \cdot \text{gwp}[\![f]\!]\, Q$.*

By definition of $\tau^\sharp$ and S. Kleene fixpoint transfer theorem 2.3 applied to the fixpoint characterization of the nondeterministic demoniac semantics semantics 8.14 with the abstraction $\lambda f \cdot \text{gwp}[\![f]\!]\, Q$ for a given $Q \subseteq \Sigma$ considered in corollary 9.10, we now obtain [19,20]:

Theorem 9.11 (E. Dijkstra's fixpoint weakest conservative precondition semantics) $\tau^{\text{wp}} = \lambda Q \cdot \text{lfp}_{\emptyset}^{\subseteq} F^{\text{wp}}[\![Q]\!]$ *where $F^{\text{wp}} \in \wp(\Sigma) \longmapsto \wp(\Sigma) \overset{m}{\longmapsto} \wp(\Sigma)$ defined by $F^{\text{wp}}[\![Q]\!] \triangleq \lambda P \cdot (Q \cap \check{\tau}) \cup \text{wp}[\![\tau^{\rightarrow}]\!]\, P = \lambda P \cdot (\neg\check{\tau} \cup Q) \cap \text{gwp}[\![\tau^{\rightarrow}]\!]\, P$ is a $\subseteq$-monotone map on the complete lattice $\langle \wp(\Sigma),\ \subseteq,\ \emptyset,\ \Sigma,\ \cup,\ \cap \rangle$.*

Proof. The abstraction $\lambda f \cdot \text{gwp}[\![f]\!]\, Q$ for a given $Q \subseteq \Sigma$ is strict since $\text{gwp}[\![\dot{\perp}^{=}]\!]\, Q = \{s \mid \dot{\perp}^{=}(s) \subseteq Q\} = \{s \mid \Sigma_\perp \subseteq Q\} = \emptyset$.

Let $f^\delta, \delta \in \mathbb{O}$ be a $\dot{\sqsubseteq}^{=}$-increasing chain. We have $\text{gwp}[\![\dot{\bigsqcup}^{=}_{\delta \in \mathbb{O}} f^\delta]\!]\, Q = \{s \mid \bigsqcup^{=}_{\delta \in \mathbb{O}} f^\delta(s) \subseteq Q\}$. $f^\delta(s), \delta \in \mathbb{O}$ is a $\sqsubseteq^{=}$-increasing chain so that by definition of the flat DCPO $D^{=}$ we have either $\forall \delta \in \mathbb{O} : f^\delta(s) = \perp^{=} = \Sigma_\perp$ in which case $\{s \mid \bigsqcup^{=}_{\delta \in \mathbb{O}} f^\delta(s) \subseteq Q\}$ is $\{s \mid \Sigma_\perp \subseteq Q\} = \emptyset = \bigcup_{\delta \in \mathbb{O}} \text{gwp}[\![f^\delta]\!]\, Q$ or there exists $\beta \in \mathbb{O}$ and $P \in \wp(\Sigma) \setminus \{\emptyset\}$ such that $f^\delta(s) = \perp^{=}$ for all $\delta < \beta$ and $f^\delta(s) = P$ for all $\delta \geq \beta$. In this that case $\{s \mid \bigsqcup^{=}_{\delta \in \mathbb{O}} f^\delta(s) \subseteq Q\}$ is $\{s \mid P \subseteq Q\} = \bigcup_{\delta < \beta} \emptyset \cup \bigcup_{\delta \geq \beta} \{s \mid P \subseteq Q\} = \bigcup_{\delta < \beta} \{s \mid f^\delta(s) \subseteq Q\} \cup \bigcup_{\delta \geq \beta} \{s \mid f^\delta(s) \subseteq Q\} = \bigcup_{\delta \in \mathbb{O}} \text{gwp}[\![f^\delta]\!]\, Q$, proving Scott-continuity.

By theorems 8.8 and 8.1, we have $\alpha^{\mathrm{Q}} \circ \alpha^{\mathrm{wp}} \circ \alpha^{\mathrm{gwp}} \circ F^{\sharp}(f) = \alpha^{\mathrm{Q}} \circ \alpha^{\mathrm{wp}} \circ \alpha^{\mathrm{gwp}} \circ F^{\natural}(f) = \alpha^{\mathrm{Q}} \circ \alpha^{\mathrm{wp}} \circ F^{\mathrm{gwp}} \circ \alpha^{\mathrm{gwp}}(f)$ as shown in the proof of theorem 9.3. By definition of α^{Q} and α^{wp}, this is $F^{\mathrm{gwp}}(\alpha^{\mathrm{gwp}}(f))Q = (Q \cap \check{\tau}) \cup \mathrm{wp}[\![\tau^{\blacktriangleright}]\!](\alpha^{\mathrm{gwp}}(f)(Q))$ by theorem 9.3. Since $Q \subseteq \Sigma$, this is $(Q \cap \check{\tau}) \cup \mathrm{wp}[\![\tau^{\blacktriangleright}]\!](\alpha^{\mathrm{Q}} \circ \alpha^{\mathrm{wp}} \circ \alpha^{\mathrm{gwp}}(f)) = F^{\mathrm{wp}}[\![Q]\!] \circ \alpha^{\mathrm{Q}} \circ \alpha^{\mathrm{wp}} \circ \alpha^{\mathrm{gwp}}(f)$ by defining $F^{\mathrm{wp}}[\![Q]\!] \triangleq \lambda P \bullet (Q \cap \check{\tau}) \cup \mathrm{wp}[\![\tau^{\blacktriangleright}]\!]\, P$ thus proving the commutation property $\lambda f \bullet \mathrm{gwp}[\![f]\!]\, Q \circ F^{\sharp} = F^{\mathrm{wp}}[\![Q]\!] \circ \lambda f \bullet \mathrm{gwp}[\![f]\!]\, Q$. Moreover $F^{\mathrm{wp}}[\![Q]\!] = \lambda P \bullet (Q \cap \check{\tau}) \cup \mathrm{wp}[\![\tau^{\blacktriangleright}]\!]\, P = \lambda P \bullet (Q \cap \{s \mid \forall s' : \neg(s \;\tau\; s') \wedge \forall s' \in \tau^{\blacktriangleright} : s' \in P) \cup \{s \mid \exists s' : s \;\tau\; s' \wedge \forall s' \in \tau^{\blacktriangleright} : s' \in P\} = (Q \cap \check{\tau} \cap \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\, P) \cup (\neg\check{\tau} \cap \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\, P) = (\neg\check{\tau} \cup (Q \cap \check{\tau})) \cap \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\, P = (\neg\check{\tau} \cup Q) \cap \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\, P$.

We conclude that $\tau^{\mathrm{wp}} \triangleq \alpha^{\mathrm{wp}}(\mathrm{gwp}[\![\tau^{\infty}]\!]) = \lambda Q \in \wp(\Sigma) \bullet \mathrm{gwp}[\![\mathrm{lfp}^{\dot{\sqsubseteq}^{\natural}}_{\dot{\bot}^{\natural}}\, F^{\sharp}]\!]\, Q = \lambda Q \in \wp(\Sigma) \bullet \mathrm{lfp}^{\subseteq}_{\emptyset}\, F^{\mathrm{wp}}[\![Q]\!]$. □

9.4 E. Dijkstra Weakest Liberal Precondition Semantics

E. Dijkstra's *weakest liberal precondition semantics* [18] $\lambda Q \in \wp(\Sigma) \bullet \mathrm{wlp}(\tau^{\vec{\infty}}, Q)$ is $\tau^{\mathrm{wlp}} \triangleq \alpha^{\mathrm{wlp}}(\tau^{\mathrm{gwp}})$ where the abstraction α^{wlp} satisfies:

Lemma 9.12 (Weakest liberal precondition abstraction) *If* $D^{\mathrm{wlp}} \triangleq \wp(\Sigma) \overset{\cap}{\longmapsto} \wp(\Sigma)$, $\alpha^{\mathrm{wlp}} \triangleq \lambda \Phi \bullet \lambda Q \bullet \Phi(Q \cup \{\bot\})$ *and* $\gamma^{\mathrm{wlp}}(\Psi) \triangleq \lambda Q \bullet (\, \bot \in Q \;?\; \Psi(Q) \;\text{¿}\; \emptyset\,)$ *then* $\langle D^{\mathrm{gwp}},\, \dot{\supseteq} \rangle \underset{\alpha^{\mathrm{wlp}}}{\overset{\gamma^{\mathrm{wlp}}}{\leftrightarrows}} \langle D^{\mathrm{wlp}},\, \dot{\supseteq} \rangle$.

Proof. $\alpha^{\mathrm{wlp}}(\Phi) \mathrel{\dot{\supseteq}} \Psi \iff \forall Q \subseteq \Sigma : \Phi(Q \cup \{\bot\}) \supseteq \Psi(Q) \iff \forall Q \subseteq \Sigma_{\bot} : \Phi(Q) \supseteq (\, \bot \in Q \;?\; \Psi(Q) \;\text{¿}\; \emptyset\,) \iff \Phi \mathrel{\dot{\supseteq}} \gamma^{\mathrm{wlp}}(\Psi)$. □

Dijkstra's weakest liberal semantics τ^{wlp} is an abstraction of the angelic denotational semantics [2]:

Lemma 9.13 (Abstraction of the angelic nondeterministic denotational semantics) $\tau^{\mathrm{wlp}} = \mathrm{gwp}[\![\tau^{\flat}]\!]$.

Proof. We have $\tau^{\mathrm{wlp}} \triangleq \alpha^{\mathrm{wlp}}(\tau^{\mathrm{gwp}}) = \alpha^{\mathrm{wlp}}(\mathrm{gwp}[\![\tau^{\natural}]\!]) = \lambda Q \in \wp(\Sigma) \bullet \{s \in \Sigma \mid \forall s' \in \Sigma_{\bot} : s' \in \tau^{\natural}(s) \Longrightarrow s' \in Q \cup \{\bot\}\} = \lambda Q \in \wp(\Sigma) \bullet \{s \in \Sigma \mid \forall s' \in \Sigma : s' \in \tau^{\natural}(s) \cap \Sigma \Longrightarrow s' \in Q\} = \lambda Q \in \wp(\Sigma) \bullet \{s \in \Sigma \mid \forall s' \in \Sigma : s' \in \alpha^{\Sigma}(\tau^{\natural})(s) \Longrightarrow s' \in Q\} = \lambda Q \in \wp(\Sigma) \bullet \{s \in \Sigma \mid \tau^{\flat} \subseteq Q\} = \mathrm{gwp}[\![\tau^{\flat}]\!]$. □

By lemma 9.13, theorem 8.17 and S. Kleene fixpoint transfer theorem 2.3, we deduce [19]:

Theorem 9.14 (E. Dijkstra's fixpoint weakest liberal precondition semantics) $\tau^{\mathrm{wlp}} = \lambda Q \bullet \mathrm{gfp}^{\subseteq}_{\Sigma}\, F^{\mathrm{wp}}[\![Q]\!]$.

Proof. Given $Q \subseteq \Sigma$, we consider the abstraction $\lambda f \bullet \mathrm{gwp}[\![f]\!]\, Q$. We have $\mathrm{gwp}[\![\lambda s \bullet \emptyset]\!]\, Q = \{s \in \Sigma \mid \forall s' \in \Sigma : s' \in \emptyset \Longrightarrow s' \in Q\} = \Sigma$, proving strictness. $\mathrm{gwp}[\![\dot{\bigcup}_{i \in \Delta} f_i]\!]\, Q = \{s \in \Sigma \mid \forall s' \in \Sigma : s' \in \bigcup_{i \in \Delta} f_i(s) \Longrightarrow s' \in Q\} = \{s \in \Sigma \mid \forall i \in \Delta : \forall s' \in \Sigma : s' \in f_i(s) \Longrightarrow s' \in Q\} = \bigcap_{i \in \Delta} \mathrm{gwp}[\![f_i]\!]\, Q$, which implies Scott-continuity. The semantic transformer is designed using the commutation condition $F^\flat \circ \lambda f \cdot \mathrm{gwp}[\![f]\!]\,Q = \lambda f \cdot \mathrm{gwp}[\![f]\!]\,Q \circ F^{\mathrm{wp}}[\![Q]\!]$ as in the proof of theorem 9.11 since $F^\flat = F^\sharp$. $F^{\mathrm{wp}}[\![Q]\!]$ is $\subseteq$-monotone. We conclude that $\tau^{\mathrm{wlp}}(Q) = \mathrm{gwp}[\![\tau^\flat]\!]\,Q = \mathrm{gwp}[\![\mathrm{lfp}^{\dot\subseteq}_{\dot\emptyset}\, F^\flat]\!]\,Q = \mathrm{lfp}^{\supseteq}_{\Sigma}\, F^{\mathrm{wp}} = \mathrm{gfp}^{\subseteq}_{\Sigma}\, F^{\mathrm{wp}}$. □

10 Galois Connections and Tensor Product

The set of Galois connections between posets (respectively DCPOs, complete lattices) $\langle D^\natural,\, \sqsubseteq^\natural\rangle$ and $\langle D^\sharp,\, \sqsubseteq^\sharp\rangle$ is denoted:

$$\langle D^\natural,\, \sqsubseteq^\natural\rangle \leftrightarrows \langle D^\sharp,\, \sqsubseteq^\sharp\rangle \triangleq \{\langle \alpha,\, \gamma\rangle \mid \langle D^\natural,\, \sqsubseteq^\natural\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle D^\sharp,\, \sqsubseteq^\sharp\rangle\}\ .$$

It is a poset (resp. DCPOs, complete lattices) $\langle\langle D^\natural,\, \sqsubseteq^\natural\rangle \leftrightarrows \langle D^\sharp,\, \sqsubseteq^\sharp\rangle,\, \dot\sqsubseteq^\sharp \times \dot\sqsubseteq^\natural\rangle$ for the pairwise pointwise ordering $\langle \alpha,\, \gamma\rangle\ \dot\sqsubseteq^\sharp \times \dot\sqsubseteq^\natural\ \langle \alpha',\, \gamma'\rangle \triangleq (\alpha\ \dot\sqsubseteq^\sharp\ \alpha') \wedge (\gamma\ \dot\sqsubseteq^\natural\ \gamma')$ where $f\ \dot\sqsubseteq\ g \triangleq \forall x : f(x) \sqsubseteq g(x)$.

The set of *complete join morphisms* is:

$$D^\natural \overset{\sqcup}{\longmapsto} D^\sharp \triangleq \{\alpha \in D^\natural \longmapsto D^\sharp \mid \forall X \subseteq D^\natural : \alpha(\sqcup^\natural X) = \sqcup^\sharp \alpha^\blacktriangleright(X)\}\ .$$

(also written $\langle D^\natural,\, \sqsubseteq^\natural\rangle \overset{\sqcup}{\longmapsto} \langle D^\sharp,\, \sqsubseteq^\sharp\rangle$ when the considered partial orderings are not understood). Dually, the set of *complete meet morphisms* is:

$$D^\sharp \overset{\sqcap}{\longmapsto} D^\natural \triangleq \{\gamma \in D^\sharp \longmapsto D^\natural \mid \forall Y \subseteq D^\sharp : \gamma(\sqcap^\sharp Y) = \sqcap^\natural \gamma^\blacktriangleright(Y)\}\ .$$

The *tensor product* $\otimes$ [38] [8] is:

Definition 10.1 (Tensor product) $\langle D^\natural, \sqsubseteq^\natural\rangle \otimes \langle D^\sharp, \sqsubseteq^\sharp\rangle \triangleq \{H \in \wp(D^\natural \times D^\sharp) \mid$ (i) $\wedge$ (ii) $\wedge$ (iii)$\}$ where the conditions are:

(i) $(X \sqsubseteq^\natural X' \wedge \langle X',\, Y'\rangle \in H \wedge Y' \sqsubseteq^\sharp Y) \Longrightarrow (\langle X,\, Y\rangle \in H)$;

(ii) $(\forall i \in \Delta : \langle X_i,\, Y\rangle \in H) \Longrightarrow (\langle \bigsqcup^\natural_{i\in\Delta} X_i,\, Y\rangle \in H)$;

(iii) $(\forall i \in \Delta : \langle X,\, Y_i\rangle \in H) \Longrightarrow (\langle X,\, \bigsqcap^\natural_{i\in\Delta} Y_i\rangle \in H)$.

Let us define the correspondences:

$$\begin{array}{ll}
1(\langle \alpha,\, \gamma\rangle) \triangleq \alpha & \mathrm{HA}(\alpha) \triangleq \{\langle x,\, y\rangle \in D^\natural \times D^\sharp \mid \alpha(x) \sqsubseteq^\sharp y\} \\
2(\langle \alpha,\, \gamma\rangle) \triangleq \gamma & \mathrm{HC}(\gamma) \triangleq \{\langle x,\, y\rangle \in D^\natural \times D^\sharp \mid x \sqsubseteq^\natural \gamma(y)\} \\
\mathrm{AG}(\gamma) \triangleq \lambda x \cdot \sqcap^\sharp\{y \mid x \sqsubseteq^\natural \gamma(y)\} & \mathrm{AH}(H) \triangleq \lambda x \cdot \sqcap^\sharp\{y \mid \langle x,\, y\rangle \in H\} \\
\mathrm{CG}(\alpha) \triangleq \lambda y \cdot \sqcup^\natural\{x \mid \alpha(x) \sqsubseteq^\sharp y\} & \mathrm{CH}(H) \triangleq \lambda y \cdot \sqcup^\natural\{x \mid \langle x,\, y\rangle \in H\}
\end{array}$$

Theorem 10.2 (Galois connections/tensor product commutative diagram)

[8] This is the semi-dual version, so that Z. Shmuely original definition corresponds to $\langle D^\natural,\, \sqsubseteq^\natural\rangle \otimes \langle D^\sharp,\, \sqsupseteq^\sharp\rangle$.

$$\begin{tikzcd}
\langle\langle D^\natural, \sqsubseteq^\natural\rangle \leftrightarrows \langle D^\sharp, \sqsubseteq^\sharp\rangle, \dot{\sqsubseteq}^\sharp \times \dot{\sqsupseteq}^\natural\rangle \arrow[r, shift right, two heads, "1"'] \arrow[d, shift right, two heads, "2"'] \arrow[dr, shift right, two heads, "\begin{array}{c}\mathrm{HC}\circ 2\\ = \mathrm{HA}\circ 1\end{array}"'] & \langle\langle D^\natural, \sqsubseteq^\natural\rangle \xmapsto{\sqcup} \langle D^\sharp, \sqsubseteq^\natural\rangle, \dot{\sqsubseteq}^\sharp\rangle \arrow[l, shift right, two heads, "\lambda\alpha\bullet\langle\alpha, \mathrm{CG}(\alpha)\rangle"'] \arrow[d, shift right, two heads, "\mathrm{HA}"'] \arrow[dl, shift right, two heads, "\mathrm{CG}"'] \\
\langle\langle D^\sharp, \sqsubseteq^\sharp\rangle \xmapsto{\sqcap} \langle D^\natural, \sqsubseteq^\natural\rangle, \dot{\sqsupseteq}^\sharp\rangle \arrow[u, shift right, two heads, "\lambda\gamma\bullet\langle\mathrm{AG}(\gamma), \gamma\rangle"'] \arrow[ur, shift right, two heads, "\mathrm{AG}"'] \arrow[r, shift right, two heads, "\mathrm{HC}"'] & \langle\langle D^\natural, \sqsubseteq^\natural\rangle \otimes \langle D^\sharp, \sqsubseteq^\sharp\rangle, \supseteq\rangle \arrow[l, shift right, two heads, "\mathrm{CH}"'] \arrow[u, shift right, two heads, "\mathrm{AH}"'] \arrow[ul, shift right, two heads, "\mathrm{AH} \times \mathrm{CH}"']
\end{tikzcd}$$

Proof.

In a Galois connection $\langle\alpha, \gamma\rangle$, α is a complete join morphism so that $1 \in (D^\natural \leftrightarrows D^\sharp) \longmapsto (D^\natural \xmapsto{\sqcup} D^\sharp)$ and γ is a complete meet morphism so that $2 \in (D^\natural \leftrightarrows D^\sharp) \longmapsto (D^\sharp \xmapsto{\sqcap} D^\natural)$.

To each $\alpha \in D^\natural \xmapsto{\sqcup} D^\sharp$, there corresponds a unique γ such that $D^\natural \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} D^\sharp$ given by $\gamma = \mathrm{CG}(\alpha) \triangleq \lambda y\bullet \sqcup^\natural\{x \mid \alpha(x) \sqsubseteq^\sharp y\}$. So $\lambda\alpha\bullet\langle\alpha, \mathrm{CG}(\alpha)\rangle \in (D^\natural \xmapsto{\sqcup} D^\sharp) \longmapsto (D^\natural \leftrightarrows D^\sharp)$. Dually, $\lambda\gamma\bullet\langle\mathrm{AG}(\gamma), \gamma\rangle \in (D^\sharp \xmapsto{\sqcap} D^\natural) \longmapsto (D^\natural \leftrightarrows D^\sharp)$. Moreover $\mathrm{CG} \in (D^\natural \xmapsto{\sqcup} D^\sharp) \longmapsto (D^\sharp \xmapsto{\sqcap} D^\natural)$ and dually $\mathrm{AG} \in (D^\sharp \xmapsto{\sqcap} D^\natural) \longmapsto (D^\natural \xmapsto{\sqcup} D^\sharp)$.

We have $\mathrm{HA} \in (D^\natural \xmapsto{\sqcup} D^\sharp) \longmapsto (D^\natural \otimes D^\sharp)$ since (i) if $x \sqsubseteq^\natural x' \wedge \alpha(x') \sqsubseteq^\sharp y' \wedge y' \sqsubseteq y$ then $\alpha(x) \sqsubseteq^\sharp \alpha(x')$ by monotony so that $\alpha(x) \sqsubseteq^\sharp y$ by transitivity; (ii) if $\forall i \in \Delta : \alpha(x_i) \sqsubseteq^\sharp y$ then $\bigsqcup^\sharp_{i\in\Delta} \alpha(x_i) \sqsubseteq^\sharp y$ by definition of lubs so that $\alpha(\bigsqcup^\natural_{i\in\Delta} x_i) \sqsubseteq^\sharp y$ since α is a complete join morphism and (iii) if $\forall i \in \Delta : \alpha(x) \sqsubseteq^\sharp y_i$ then $\alpha(x) \sqsubseteq^\sharp \bigsqcap^\sharp_{i\in\Delta} y_i$ by definition of glbs. Dually, we have $\mathrm{HC} \in (D^\sharp \xmapsto{\sqcap} D^\natural) \longmapsto (D^\natural \otimes D^\sharp)$.

We have $\langle x, y\rangle \in H$ implies $\sqcap^\sharp\{y' \mid \langle x, y'\rangle \in H\} \sqsubseteq^\sharp y$ by definition of glbs. Reciprocally $\langle x, \sqcap^\sharp\{y' \mid \langle x, y'\rangle \in H\}\rangle \in H$ by (iii) so that if $\sqcap^\sharp\{y' \mid \langle x, y'\rangle \in H\} \sqsubseteq^\sharp y$ then $\langle x, y\rangle \in H$ by (i). So $\langle x, y\rangle \in H$ if and only if $\sqcap^\sharp\{y' \mid \langle x, y'\rangle \in H\} \sqsubseteq^\sharp y$. Dually $\langle x, y\rangle \in H$ if and only if $x \sqsubseteq^\natural \sqcup^\natural\{x' \mid \langle x', y\rangle \in H\}$. It follows that for all $H \in D^\natural \otimes D^\sharp$, we have $\mathrm{AH}(H)x \sqsubseteq^\sharp y \iff \sqcap^\sharp\{y' \mid \langle x, y'\rangle \in H\} \sqsubseteq^\sharp y \iff \langle x, y\rangle \in H \iff x \sqsubseteq^\natural \sqcup^\natural\{x' \mid \langle x', y\rangle \in H\} \iff x \sqsubseteq^\natural \mathrm{CH}(H)y$ proving that $\langle D^\natural, \sqsubseteq^\natural\rangle \underset{\mathrm{AH}(H)}{\overset{\mathrm{CH}(H)}{\leftrightarrows}} \langle D^\sharp, \sqsubseteq^\sharp\rangle$ whence $\mathrm{AH} \times \mathrm{CH} \in (D^\natural \otimes D^\sharp) \longmapsto (D^\natural \leftrightarrows D^\sharp)$. It follows that $\mathrm{AH} = 1 \circ (\mathrm{AH} \times \mathrm{CH}) \in (D^\natural \otimes D^\sharp) \longmapsto (D^\natural \xmapsto{\sqcup} D^\sharp)$ and $\mathrm{CH} = 2 \circ (\mathrm{AH} \times \mathrm{CH}) \in (D^\natural \otimes D^\sharp) \longmapsto (D^\sharp \xmapsto{\sqcap} D^\natural)$.

To prove isomorphism, we assume $\langle\alpha, \gamma\rangle \in D^\natural \leftrightarrows D^\sharp$, $\alpha \in D^\natural \xmapsto{\sqcup} D^\sharp$ with pointwise ordering $\alpha \mathrel{\dot{\sqsubseteq}^\sharp} \alpha' \triangleq \forall x \in D^\natural : \alpha(x) \sqsubseteq^\sharp \alpha'(x)$, $\gamma \in D^\sharp \xmapsto{\sqcap} D^\natural$ with pointwise ordering $\gamma \mathrel{\dot{\sqsupseteq}^\natural} \gamma' \triangleq \forall y \in D^\sharp : \gamma(y) \sqsupseteq^\natural \gamma'(y)$ and $H \in D^\natural \otimes D^\sharp$ with superset ordering $\supseteq$.

We have $2 \circ \lambda\gamma\bullet\langle\mathrm{AG}(\gamma), \gamma\rangle(\gamma) = \gamma$ and $\lambda\gamma\bullet\langle\mathrm{AG}(\gamma), \gamma\rangle \circ 2(\langle\alpha, \gamma\rangle) = \langle\mathrm{AG}(\gamma), \gamma\rangle = \langle\alpha, \gamma\rangle$.

$1 \circ \lambda\alpha\bullet\langle\alpha, \mathrm{CG}(\alpha)\rangle(\alpha) = \alpha$, $\lambda\alpha\bullet\langle\alpha, \mathrm{CG}(\alpha)\rangle \circ 1(\langle\alpha, \gamma\rangle) = \langle\alpha, \mathrm{CG}(\alpha)\rangle = \gamma$.

$\mathrm{HC} \circ \mathrm{CH}(H) = \{\langle x,\, y\rangle \mid x \sqsubseteq^{\natural} \sqcup^{\natural}\{x' \mid \langle x',\, y\rangle \in H\}\} = \{\langle x,\, y\rangle \mid \langle x,\, y\rangle \in H\} = H$ since we have shown that $\langle x,\, y\rangle \in H$ if and only if $x \sqsubseteq^{\natural} \sqcup^{\natural}\{x' \mid \langle x',\, y\rangle \in H\}$. Dually, $\mathrm{HA} \circ \mathrm{AH}(H) = H$.

$\mathrm{CH} \circ \mathrm{HC}(\gamma) = \lambda y \centerdot \sqcup^{\natural}\{x \mid \langle x,\, y\rangle \in \mathrm{HC}(\gamma)\} = \lambda y \centerdot \sqcup^{\natural}\{x \mid x \sqsubseteq^{\natural} \gamma(y)\} = \gamma$. Dually, $\mathrm{AH} \circ \mathrm{HA}(\alpha) = \alpha$.

Since all maps in the diagram are monotone, it follows that we have Galois connections.

Let us now check the commutation property of the diagram.

We have shown that $\mathrm{AH} = \mathrm{AG} \circ \mathrm{CH}$ so $\mathrm{AH} \circ \mathrm{HC} = \mathrm{AG} \circ \mathrm{CH} \circ \mathrm{HC} = \mathrm{AG}$. Dually $\mathrm{CH} \circ \mathrm{HA} = \mathrm{CG}$.

$\lambda\gamma \centerdot \langle \mathrm{AG}(\gamma),\, \gamma\rangle \circ \mathrm{CH}(H) = \langle \mathrm{AG}(\mathrm{CH}(H)),\, \mathrm{CH}(H)\rangle = \langle \mathrm{AH}(H),\, \mathrm{CH}(H)\rangle \triangleq (\mathrm{AH} \times \mathrm{CH})(H)$. Similarly, $\lambda\alpha \centerdot \langle \alpha,\, \mathrm{CG}(\alpha)\rangle \circ \mathrm{AH} = \mathrm{AH} \times \mathrm{CH}$.

Finally, $1 \circ \lambda\gamma \centerdot \langle \mathrm{AG}(\gamma),\, \gamma\rangle = \mathrm{AG}$ and $2 \circ \lambda\alpha \centerdot \langle \alpha,\, \mathrm{CG}(\alpha)\rangle = \mathrm{CG}$. □

11 Axiomatic Semantics

Using theorems 9.2 and 10.2, we can define the generalized axiomatic semantics τ^{gH} of a transition system $\langle \Sigma,\, \tau\rangle$ as the element $\mathrm{HC}(\tau^{\mathrm{gwp}})$ of the tensor product $\wp(\Sigma) \otimes \wp(\Sigma_{\perp})$ corresponding to the weakest precondition semantics τ^{gwp}, or equivalently as $\mathrm{HA}(\tau^{\mathrm{gsp}})$ corresponding to the strongest postcondition semantics τ^{gsp}. Writing $\langle P\rangle\tau\langle Q\rangle$ for $\langle P,\, Q\rangle \in \tau^{\mathrm{gH}}$, we have $\langle P\rangle\tau\langle Q\rangle$ if and only if $P \sqsubseteq^{\mathrm{gwp}} \tau^{\mathrm{gwp}}(Q)$ if and only if $\tau^{\mathrm{gsp}}(P) \sqsubseteq^{\mathrm{gwp}} Q$. Condition (i) of definition 10.1 is the consequence rule of C.A.R. Hoare logic [23]. Conditions (ii) and (iii) are also valid for the classical presentation of C.A.R. Hoare logic [23] but have to be derived from the deduction rules by structural induction on the syntactic structure of programs.

11.1 R. Floyd/C.A.R. Hoare/P. Naur Partial Correctness Semantics

R. Floyd [21], C.A.R. Hoare [23] & P. Naur [30] *partial correctness semantics* is $\tau^{\mathrm{pH}} \triangleq \mathrm{HC}(\tau^{\mathrm{wlp}})$. We get R. Floyd & P. Naur's partial correctness verification conditions [21,30] using E. Dijkstra's fixpoint characterization 9.14 of the weakest liberal precondition semantics τ^{wlp} and D. Park fixpoint induction [32]:

Lemma 11.1 (D. Park fixpoint induction) *If $\langle D,\, \sqsubseteq,\, \perp,\, \top,\, \sqcup,\, \sqcap\rangle$ is a complete lattice, $F \in D \xmapsto{m} D$ is $\sqsubseteq$-monotone and $L \in D$ then $\mathrm{lfp}^{\sqsubseteq}_{\perp} F \sqsubseteq P \iff (\exists I : F(I) \sqsubseteq I \wedge I \sqsubseteq P)$.*

Proof. For soundness ($\Longleftarrow$), $\mathrm{lfp}^{\sqsubseteq}_{\pm} F \sqsubseteq P = \sqcap\{X \mid F(X) \sqsubseteq X\} \sqsubseteq I \sqsubseteq L$ by Tarski's fixpoint theorem [39] and definition of glbs.

For completeness ($\Longrightarrow$), $I = \mathrm{lfp}^{\sqsubseteq}_{\pm} F \sqsubseteq P$ satisfies $F(I) = I$ by definition.□

Theorem 11.2 (R. Floyd & P. Naur partial correctness semantics) $\tau^{\mathrm{pH}} = \{\langle P, Q\rangle \in \wp(\Sigma) \otimes \wp(\Sigma) \mid \exists I \in \wp(\Sigma) : P \subseteq I \wedge I \subseteq \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\, I \wedge (I \cap \check{\tau}) \subseteq Q\}$.

The condition $I \subseteq \mathrm{gwp}\llbracket\tau^{\blacktriangleright}\rrbracket\, I$ is given by C.A.R. Hoare [23] while R. Floyd & P. Naur partial correctness verification condition [21,30] corresponds more precisely to $\mathrm{gsp}\llbracket\tau^{\blacktriangleright}\rrbracket\, I \subseteq I$ which, by lemma 9.2, is equivalent.

Proof. $\tau^{\mathrm{pH}} \triangleq \mathrm{HC}(\tau^{\mathrm{wlp}}) = \mathrm{HC}(\lambda Q \cdot \mathrm{gfp}^{\subseteq}_{\Sigma}\, F^{\mathrm{wp}}\llbracket Q\rrbracket) = \{\langle P,\, Q\rangle \in \wp(\Sigma) \otimes \wp(\Sigma) \mid \mathrm{lfp}^{\supseteq}_{\Sigma}\, F^{\mathrm{wp}}\llbracket Q\rrbracket \supseteq P\}$ by theorem 9.14 and definition of HC. By D. Park induction 11.1, we derive $\{\langle P,\, Q\rangle \in \wp(\Sigma) \otimes \wp(\Sigma) \mid \exists I \in \wp(\Sigma) : F^{\mathrm{wp}}\llbracket Q\rrbracket(I) \supseteq I \wedge I \supseteq P\}$ which, by definition of F^{wp} in theorem 9.11, is $\{\langle P,\, Q\rangle \in \wp(\Sigma) \otimes \wp(\Sigma) \mid \exists I \in \wp(\Sigma) : I \subseteq (\neg\check{\tau} \cup Q) \cap \mathrm{gwp}\llbracket\tau^{\blacktriangleright}\rrbracket(I) \wedge P \subseteq I\} = \{\langle P,\, Q\rangle \in \wp(\Sigma) \otimes \wp(\Sigma) \mid \exists I \in \wp(\Sigma) : (I \cap \check{\tau}) \subseteq Q \wedge I \subseteq \mathrm{gwp}\llbracket\tau^{\blacktriangleright}\rrbracket(I) \wedge P \subseteq I\}$. □

Writing *C.A.R. Hoare triples* $\{P\}\tau^{\vec{\infty}}\{Q\}$ for $\langle P,\, Q\rangle \in \tau^{\mathrm{pH}}$, $\{P\}\tau\{Q\}$ for $P \subseteq \mathrm{gwp}\llbracket\tau^{\blacktriangleright}\rrbracket\, Q$ and using a rule-based presentation of τ^{pH}, we get a set theoretic model of C.A.R. Hoare logic:

Corollary 11.3 (C.A.R. Hoare partial correctness axiomatic semantics) $\{P\}\tau^{\vec{\infty}}\{Q\}$ *if and only if it derives from the axiom:*

$$\{\mathrm{gwp}\llbracket\tau^{\blacktriangleright}\rrbracket\, Q\}\tau\{Q\} \qquad (\tau)$$

and the following inference rules:

$$\frac{P \subseteq P',\ \{P'\}\tau^{\vec{\infty}}\{Q'\},\ Q' \subseteq Q}{\{P\}\tau^{\vec{\infty}}\{Q\}}\ (\Rightarrow) \qquad \frac{\{P_i\}\tau^{\vec{\infty}}\{Q\},\ i \in \Delta}{\{\bigcup_{i \in \Delta} P_i\}\tau^{\vec{\infty}}\{Q\}}\ (\vee)$$

$$\frac{\{P\}\tau^{\vec{\infty}}\{Q_i\},\ i \in \Delta}{\{P\}\tau^{\vec{\infty}}\{\bigcap_{i \in \Delta} Q_i\}}\ (\wedge) \qquad \frac{\{I\}\tau\{I\}}{\{I\}\tau^{\vec{\infty}}\{I \cap \check{\tau}\}}\ (\tau^{\vec{\infty}})$$

Proof. For soundness, rules $(\Rightarrow)$, $(\wedge)$ and $(\vee)$ follow from the definition of $\wp(\Sigma) \otimes \wp(\Sigma)$. The tautology $\mathrm{gwp}\llbracket\tau^{\blacktriangleright}\rrbracket\, Q \subseteq \mathrm{gwp}\llbracket\tau^{\blacktriangleright}\rrbracket\, Q$ implies the axiom (τ). Rule $(\tau^{\vec{\infty}})$ follows from theorem 11.2 where $P = I$ and $Q = (I \cap \check{\tau})$.

For relative completeness, if $\langle P,\, Q\rangle \in \tau^{\mathrm{pH}}$, then by theorem 11.2, there exists an invariant $I \in \wp(\Sigma)$ such that $P \subseteq I$, $I \subseteq \mathrm{gwp}\llbracket\tau^{\blacktriangleright}\rrbracket\, I$ and $(I \cap \check{\tau}) \subseteq Q$. By the axiom $\{\mathrm{gwp}\llbracket\tau^{\blacktriangleright}\rrbracket\, I\}\tau\{I\}$ and $I \subseteq I$ so that by the consequence rule $(\Rightarrow)$ $\{I\}\tau\{I\}$. Then by rule $(\tau^{\vec{\infty}})$ we derive $\{I\}\tau^{\vec{\infty}}\{I \cap \check{\tau}\}$ whence by the consequence rule $(\Rightarrow)$ we prove $\{P\}\tau^{\vec{\infty}}\{Q\}$, Q.E.D. □

11.2 R. Floyd Total Correctness Semantics

R. Floyd [21] *total correctness semantics* is $\tau^{\mathrm{tH}} \triangleq \mathrm{HC}(\tau^{\mathrm{wp}})$. We get R. Floyd's verification conditions using E. Dijkstra's fixpoint characterization 9.11 of τ^{wp} and the following induction principle:

Lemma 11.4 (Lower fixpoint induction) *If* $\langle D,\, \sqsubseteq,\, \bot,\, \sqcup\rangle$ *is a DCPO,* $F \in D \overset{m}{\longmapsto} D$ *is* $\sqsubseteq$*-monotone,* $\bot \in D$ *satisfies* $\bot \sqsubseteq F(\bot)$ *and* $P \in D$ *then* $P \sqsubseteq \mathrm{lfp}^{\sqsubseteq}_{\bot}\, F \iff (\exists \epsilon \in \mathbb{O} : \exists I \in (\epsilon + 1) \longmapsto D : I^0 \sqsubseteq \bot \wedge \forall \delta : 0 < \delta \leq \epsilon \Longrightarrow I^{\delta} \sqsubseteq F(\bigsqcup_{\zeta < \delta} I^{\zeta}) \wedge P \sqsubseteq I^{\epsilon})$.

Proof. For soundness $(\Longleftarrow)$, let $F^{\delta}, \delta \in \mathbb{O}$ be the increasing sequence of iterates of F from $\bot$, which can be defined as $F^0 = \bot$ and $F^{\delta} = F(\bigsqcup_{\zeta < \delta} F^{\zeta})$ for all $\delta > 0$ [10]. We have $I^0 \sqsubseteq \bot = F^0$. If, by induction hypothesis, $\forall \zeta < \delta$: $I^\zeta \sqsubseteq F^\zeta$ then $\bigsqcup_{\zeta<\delta} I^\zeta \sqsubseteq \bigsqcup_{\zeta<\delta} F^\zeta$ by definition of lubs so $F(\bigsqcup_{\zeta<\delta} I^\zeta) \sqsubseteq F(\bigsqcup_{\zeta<\delta} F^\zeta)$ by monotony proving $I^\delta \sqsubseteq F^\delta$ by hypothesis and definition of the iterates. By transfinite induction, $\forall \delta \leq \epsilon : I^\delta \sqsubseteq F^\delta$, so that in particular $P \sqsubseteq I^\epsilon \sqsubseteq F^\epsilon \sqsubseteq \mathrm{lfp}^{\sqsubseteq}_{\bot} F$.

For completeness ($\Longrightarrow$), we can always choose $I^\delta = F^\delta$ for all $\delta > 0$ so that $I^0 = \bot$ and $I^\delta = F(\bigsqcup_{\zeta<\delta} I^\zeta)$ for all $\delta \in \mathbb{O}$. We have $P \sqsubseteq \mathrm{lfp}^{\sqsubseteq}_{\bot} F = I^\epsilon$ where ϵ is the order of the iterates. □

Theorem 11.5 (R. Floyd total correctness semantics) $\tau^{\mathrm{tH}} = \{\langle P, Q\rangle \in \wp(\Sigma) \otimes \wp(\Sigma) \mid \exists \epsilon \in \mathbb{O} : \exists I \in (\epsilon + 1) \longmapsto \wp(\Sigma) : \forall \delta \leq \epsilon : I^\delta \subseteq (\neg\check{\tau} \cup Q) \cap \mathrm{gwp}[\![\tau^{\bullet\!\!\to}]\!](\bigcup_{\beta<\delta} I^\beta) \wedge P \subseteq I^\epsilon\}$.

The verification condition is better recognized as R. Floyd's verification condition in the equivalent form:

$$\forall s \in I^\delta : \begin{array}{l} \forall s' : \neg(s\ \tau\ s') \wedge s \in Q \\ \vee \\ \exists s' : s\ \tau\ s' \wedge \forall s' : s\ \tau\ s' \Longrightarrow (\exists \beta < \delta : s' \in I^\beta) \end{array}$$

where the ordinal δ encodes the value of R. Floyd's *variant function* [20].

Proof. Follows directly from lemma 11.4, theorem 9.11 and the definition $\tau^{\mathrm{tH}} = \mathrm{HC}(\tau^{\mathrm{wp}}) = \{\langle P, Q\rangle \in \wp(\Sigma) \otimes \wp(\Sigma) \mid P \subseteq \mathrm{lfp}^{\subseteq}_{\emptyset} F^{\mathrm{wp}}[\![Q]\!]\}$ where $I^0 \subseteq Q \cap \check{\tau} = F[\![\tau^{\bullet\!\!\to}]\!]\emptyset = \bot$. □

Writing *Z. Manna/A. Pnueli triples* $[P]\tau^{\vec{\infty}}[Q]$ for $\langle P, Q\rangle \in \tau^{\mathrm{tH}}$, $[P]\tau[Q]$ for $P \subseteq \mathrm{gwp}[\![\tau^{\bullet\!\!\to}]\!]Q$ and using a rule-based presentation of τ^{tH}, we get a set theoretic model of Z. Manna/A. Pnueli logic [27]:

Corollary 11.6 (Z. Manna/A. Pnueli total correctness axiomatic semantics) $[P]\tau^{\vec{\infty}}[Q]$ *if and only if it derives from the axiom* (τ)*, the inference rules* ($\Rightarrow$)*,* ($\wedge$)*,* ($\vee$) *and the following:*

$$\frac{I^0 \subseteq Q \cap \check{\tau}, \quad \bigwedge_{\delta=1}^{\epsilon} I^\delta \subseteq \neg\check{\tau} \cup Q, \quad \bigwedge_{\delta=1}^{\epsilon} [I^\delta]\tau[\bigcup_{\beta<\delta} I^\beta]}{[I^\epsilon]\tau^{\vec{\infty}}[Q]}\ (\tau^{\vec{\infty}})$$

Proof. For soundness, rules ($\Rightarrow$), ($\wedge$) and ($\vee$) follow from the definition of $\wp(\Sigma) \otimes \wp(\Sigma)$ while the axiom (τ) follows from the tautology $\mathrm{gwp}[\![\tau^{\bullet\!\!\to}]\!]Q \subseteq \mathrm{gwp}[\![\tau^{\bullet\!\!\to}]\!]Q$. Rule ($\tau^{\vec{\infty}}$) follows from theorem 11.5 where $P = I^\epsilon$, $I^0 \subseteq (\neg\check{\tau} \cup Q) \cap \mathrm{gwp}[\![\tau^{\bullet\!\!\to}]\!]\emptyset = \check{\tau} \cap Q$ and for $0 < \delta \leq \epsilon$, $I^\delta \subseteq (\neg\check{\tau} \cup Q)$ and $I^\delta \subseteq \mathrm{gwp}[\![\tau^{\bullet\!\!\to}]\!](\bigcup_{\beta<\delta} I^\beta)$ whence $[I^\delta]\tau[\bigcup_{\beta<\delta} I^\beta]$.

For relative completeness, if $\langle P, Q\rangle \in \tau^{\mathrm{tH}}$, then by theorem 11.5, there exists an ordinal ϵ and an invariant $I \in (\epsilon + 1) \longmapsto \wp(\Sigma)$ such that forall $\delta \in \mathbb{O}$ with $\delta \leq \epsilon$, we have $I^\delta \subseteq (\neg\check{\tau} \cup Q) \cup \mathrm{gwp}[\![\tau^{\bullet\!\!\to}]\!](\bigcup_{\beta<\delta} I^\beta)$ and $P \subseteq I^\epsilon$. For $\delta = 0$ this implies $I^0 \subseteq Q \cap \check{\tau}$. For $\delta > 1$, we have $I^\delta \subseteq (\neg\check{\tau} \cup Q)$. Moreover $I^\delta \subseteq \mathrm{gwp}[\![\tau^{\bullet\!\!\to}]\!](\bigcup_{\beta<\delta} I^\beta)$, the axiom $[\mathrm{gwp}[\![\tau^{\bullet\!\!\to}]\!](\bigcup_{\beta<\delta} I^\beta)]\tau[\bigcup_{\beta<\delta} I^\beta]$

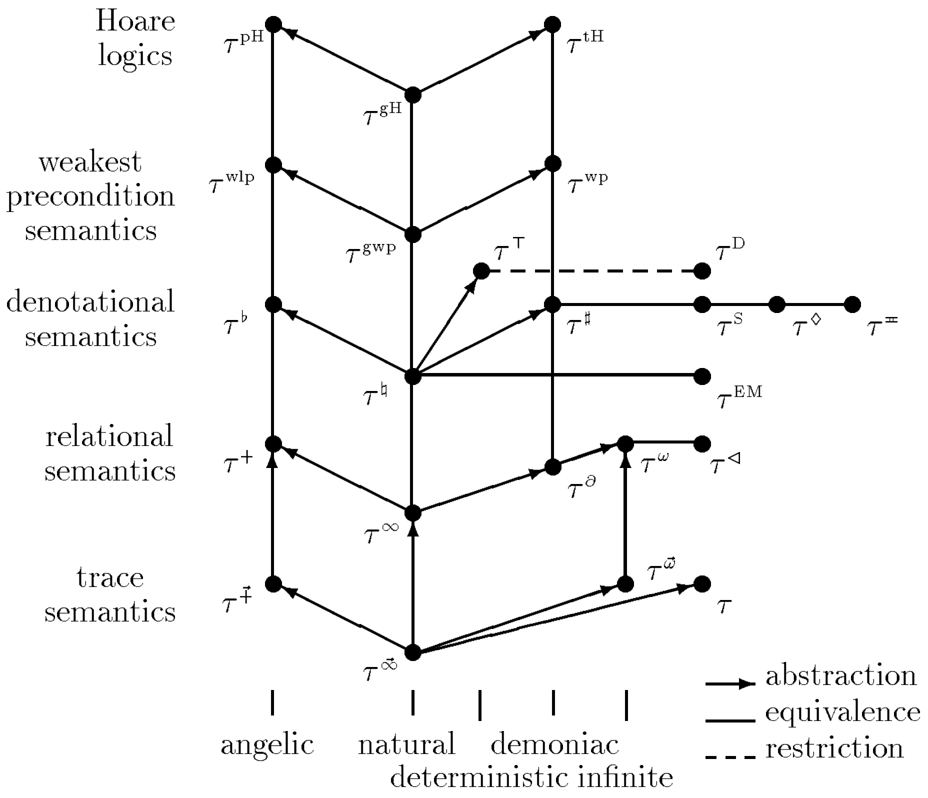


Fig. 5. The lattice of semantics

and $\bigcup\limits_{\beta<\delta} I^{\beta} \subseteq \bigcup\limits_{\beta<\delta} I^{\beta}$ together with the consequence rule ($\Rightarrow$) allows to derive $[I^{\delta}]\tau[\bigcup\limits_{\beta<\delta} I^{\beta}]$. Then by rule ($\tau^{\vec{\infty}}$) we derive $[I^{\epsilon}]\tau^{\vec{\infty}}[Q]$ whence $[P]\tau^{\vec{\infty}}[Q]$ by the consequence rule ($\Rightarrow$), Q.E.D. □

12 Lattice of Semantics

A preorder can be defined on semantics $\tau^{\natural} \in D^{\natural}$ and $\tau^{\sharp} \in D^{\sharp}$ when $\tau^{\sharp} = \alpha^{\sharp}(\tau^{\natural})$ and $\langle D^{\natural}, \leq\rangle \underset{\alpha^{\sharp}}{\overset{\gamma^{\sharp}}{\leftrightarrows}} \langle D^{\sharp}, \leqq\rangle$. The quotient poset is isomorphic to M. Ward lattice [41] of upper closure operators $\gamma^{\sharp} \circ \alpha^{\sharp}$ on $\langle D^{\vec{\infty}}, \subseteq\rangle$, so that we get a lattice of semantics which is part of the lattice of abstract interpretations of [9, sec. 8], a sublattice of which is illustrated in figure 5.

13 Conclusion

We have shown that the classical semantics of programs, modeled as transition systems, can be derived from one another by Galois connection based abstract interpretations. All classical semantics of programming languages have been presented in a uniform framework which makes them easily comparable and better explains the striking similarities and correspondences between semantic models. Moreover the construction leads to new reorderings of the fixpoint semantics. Our presentation uses abstraction which proceeds by omitting some aspects of program execution but the inverse operation of semantic refinement (traditionally called concretization) is equally important[9]. This suggests considering hierarchies of semantics which can describe program properties, that is program executions, at various levels of abstraction or refinement in a uniform framework. Then for program analysis of a given class of properties there should be a natural choice of semantics in the hierarchy [8].

References

[1] S. Abramsky and A. Jung. Domain theory. In S. Abramsky, Dov M. Gabbay, and T.S.E. Maibaum, editors, *Semantic Structures*, volume 3 of *Handbook of Logic in Computer Science*, chapter 1, pages 1–168. Clarendon Press, 1994.

[2] K.R. Apt and G.D. Plotkin. Countable nondeterminism and random assignment. *J. ACM*, 33(4):724–767, oct 1986.

[3] A. Arnold and M. Nivat. Formal computations of non deterministic recursive program schemes. *Math. System Theory*, 13:219–236, 1980.

[4] R.J.R. Back. A continuous semantics for unbounded nondeterminism. *TCS*, 23:187–210, 1983.

[5] M. Broy, R. Gnatz, and M. Wirsing. Semantics of nondeterministic and noncontinuous constructs. In F.L. Bauer and M. Broy, editors, *Program Construction. Lecture Notes of the International Summer School on Program Construction, Marktoberdorf 1978*, LNCS 69, pages 553–592. Springer-Verlag, 1979.

[6] M. Broy and G. Nelson. Can fair choice be added to Dijkstra's calculus. *TOPLAS*, 16(3):924–938, mar 1994.

[7] P. Cousot. Semantic foundations of program analysis. In S.S. Muchnick and N.D. Jones, editors, *Program Flow Analysis: Theory and Applications*, chapter 10, pages 303–342. Prentice-Hall, 1981.

[8] P. Cousot. Abstract interpretation. *Symposium on Models of Programming Languages and Computation, ACM Comput. Surv.*, 28(2):324–328, 1996.

[9] P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *4th POPL*, pages 238–252, Los Angeles, Calif., 1977. ACM Press.

[10] P. Cousot and R. Cousot. Constructive versions of Tarski's fixed point theorems. *Pacific J. Math.*, 82(1):43–57, 1979.

[11] P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *6th POPL*, pages 269–282, San Antonio, Texas, 1979. ACM Press.

[9] For example, the maximal trace semantics τ^∞ can be refined into transfinite traces so that e.g. `while true do skip; X:=1` would have semantics $\{s^\omega s' s'[X \leftarrow 1] \mid s, s' \in \Sigma\}$ thus allowing the program slice with respect to variable `X` to be `X:=1` with semantics $\{s' s'[X \leftarrow 1] \mid s' \in \Sigma\}$. Slicing would not be consistent when considering the trace $\{s^\omega \mid s \in \Sigma\}$ or denotational semantics $\lambda s \bullet \perp$ of the program.

[12] P. Cousot and R. Cousot. Induction principles for proving invariance properties of programs. In D. Néel, editor, *Tools & Notions for Program Construction*, pages 43–119. Cambridge U. Press, 1982.

[13] P. Cousot and R. Cousot. Inductive definitions, semantics and abstract interpretation. In *19th POPL*, pages 83–94, Albuquerque, N.M., 1992. ACM Press.

[14] P. Cousot and R. Cousot. Higher-order abstract interpretation (and application to comportment analysis generalizing strictness, termination, projection and PER analysis of functional languages), invited paper. In *Proc. 1994 ICCL*, Toulouse, FRA, pages 95–112. IEEE Comp. Soc. Press, 16–19 may 1994.

[15] P. Cousot and R. Cousot. Compositional and inductive semantic definitions in fixpoint, equational, constraint, closure-condition, rule-based and game-theoretic form, invited paper. In P. Wolper, editor, *Proc. 7th Int. Conf. CAV '95*, Liège, BEL, LNCS 939, pages 293–308. Springer-Verlag, 3–5 jul 1995.

[16] J.W. de Bakker, J.-J.Ch. Meyer, and J.I. Zucker. On infinite computations in denotational semantics. *TCS*, 26:53–82, 1983. (Corrigendum: TCS 29:229–230, 1984).

[17] J.W. de Bakker and D. Scott. A theory of programs. Unpublished notes, 1969.

[18] E.W. Dijkstra. Guarded commands, nondeterminacy and formal derivation of programs. *Comm. ACM*, 18(8):453–457, aug 1975.

[19] E.W. Dijkstra and C.S. Scholten. *Predicate Calculus and Program Semantics*. Springer-Verlag, 1990.

[20] E.W. Dijkstra and A.J.M. van Gasteren. A simple fixpoint argument without the restriction to continuity. *Acta Inf.*, 23:1–7, 1986.

[21] R.W. Floyd. Assigning meaning to programs. In J.T. Schwartz, editor, *Proc. Symposium in Applied Mathematics*, volume 19, pages 19–32. AMS, 1967.

[22] C.A. Gunter and D.S. Scott. Semantic domains. In J. van Leeuwen, editor, *Formal Models and Semantics*, volume B of *Handbook of Theoretical Computer Science*, chapter 12, pages 633–674. Elsevier, 1990.

[23] C.A.R. Hoare. An axiomatic basis for computer programming. *Comm. ACM*, 12(10):576–580, 583, oct 1969.

[24] D. Jacobs and D. Gries. General correctness: A unification of partial and total correctness. *Acta Inf.*, 22:67–83, 1985.

[25] G. Kahn. Natural semantics. In K. Fuchi and M. Nivat, editors, *Programming of Future Generation Computers*, pages 237–258. Elsevier, 1988.

[26] M.E. Majster-Cederbaum. A simple relation between relational and predicate transformer semantics for nondeterministic programs. *Inf. Process. Lett.*, 11(4, 5):190–192, 12 dec 1980.

[27] Z. Manna and A. Pnueli. Axiomatic approach to total correctness. *Acta Inf.*, 3:253–263, 1974.

[28] R. Milner. Operational and algebraic semantics of concurrent processes. In J. van Leeuwen, editor, *Formal Models and Semantics*, volume B of *Handbook of Theoretical Computer Science*, chapter 19, pages 1201–1242. Elsevier, 1990.

[29] R. Milner and M. Tofte. Co-induction in relational semantics. *TCS*, 87:209–220, 1991.

[30] P. Naur. Proofs of algorithms by general snapshots. *BIT*, 6:310–316, 1966.

[31] G. Nelson. A generalization of Dijkstra's calculus. *TOPLAS*, 11(4):517–561, apr 1989.

[32] D. Park. Fixpoint, induction and proofs of program properties. In B. Meltzer and D. Michie, editors, *Machine Intelligence*, volume 5, pages 59–78. Edinburgh University Press, Edinburgh, 1969.

[33] D. Park. On the semantics of fair parallelism. In D. Bjørner, editor, *Proc. of the Winter School on Abstract Software Specifications*, LNCS 86, pages 504–526. Springer-Verlag, 1980.

[34] A.M. Pitts. Operational semantics for program equivalence. Invited address, MFPS XIII, CMU, Pittsburgh, 23–26 mar 1997.
`http://www.cl.cam.ac.uk/users/ap/talks`.

[35] G.D. Plotkin. A structural approach to operational semantics. Technical Report DAIMI FN-19, Aarhus University, DEN, sep 1981.

[36] D. Scott. Outline of a mathematical theory of computation. Technical Monograph PRG-2, Oxford University Computing Laboratory, Programming Research Group, Oxford, GBR, nov 1970.

[37] D. Scott. The lattice of flow diagrams. In E. Engeler, editor, *Semantics of Algorithmic Languages*, LNM 188, pages 311–366. Springer-Verlag, 1971.

[38] Z. Shmuely. The structure of Galois connections. *Pacific J. Math.*, 54(2):209–225, 1974.

[39] A. Tarski. A lattice theoretical fixpoint theorem and its applications. *Pacific J. Math.*, 5:285–310, 1955.

[40] R.J. van Glabbeek. The linear time – branching time spectrum (extended abstract). In J.C.M. Baeten and J.W. Klop, editors, *Proc. CONCUR '90, Theories of Concurrency: Unification and Extension,* Amsterdam, August 1990, volume 458 of *LNCS*, pages 278–297. Springer-Verlag, 1990.

[41] M. Ward. The closure operators of a lattice. *Ann. Math.*, 43:191–196, 1942.