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

Patrick Cousot[a]

[a]Département d'Informatique, École Normale Supérieure, 45 rue d'Ulm, 75230 Paris cedex 05, France, `Patrick.Cousot@ens.fr`, `http://www.di.ens.fr/~cousot`

We construct a hierarchy of semantics by successive abstract interpretations. Starting from the maximal trace semantics of a transition system, we derive the big-step semantics, termination and nontermination semantics, Plotkin's natural, Smyth's demoniac and Hoare's angelic relational semantics and equivalent nondeterministic denotational semantics (with alternative powerdomains to the Egli-Milner and Smyth constructions), D. Scott's deterministic denotational semantics, the generalized and Dijkstra's conservative/liberal predicate transformer semantics, the generalized/total and Hoare's partial correctness axiomatic semantics and the corresponding proof methods. All the semantics are presented in a uniform fixpoint form and the correspondences between these semantics are established through composable Galois connections, each semantics being formally calculated by abstract interpretation of a more concrete one using Kleene and/or Tarski fixpoint approximation transfer theorems.

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 [9,12]. The approximation process which is involved in this derivation has been formalized using, among equivalent formalizations, by Galois connections for static approximation and by widening narrowing operators for dynamic approximation [13].

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 [15], the Galois connection based abstract interpretation theory was later extended to cope in exactly the same way with denotational semantics [18].

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 semantics can themselves be derived from each other by the same Galois connection based calculation process. It follows, by composition, 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.

The correspondance which is established between the considered semantics provides a unifying point of view which is also a contribution to the long-dating study of relationships between semantic descriptions of programming languages (e.g. [3,34,44]).

2. Abstraction of Fixpoint Semantics

2.1. Fixpoint Semantics

A *fixpoint semantics specification* is a pair $\langle D,\ F\rangle$ where

– the *semantic domain* $\langle D,\ \sqsubseteq,\ \bot,\ \sqcup\rangle$ is a poset that is a set D equipped with

  - a partial order $\sqsubseteq\ \subseteq D \times D$ (which is reflexive ($\forall x \in D : x \sqsubseteq x$), antisymmetric ($\forall x, y \in D : (x \sqsubseteq y \wedge y \sqsubseteq x) \Longrightarrow (x = y)$) and transitive ($\forall x, y, z \in D : (x \sqsubseteq y \wedge y \sqsubseteq z) \Longrightarrow (x \sqsubseteq z)$)),
  - an infimum $\bot$ (such that $\forall x \in D : \bot \sqsubseteq x$),
  - a partially defined least upper bound $\sqcup$ (lub), which is an upper bound ($\forall S \subseteq D : \forall s \in S : s \sqsubseteq \sqcup S$) and the least one ($\forall S \subseteq D : \forall m \in D : (\forall s \in S : s \sqsubseteq m) \Longrightarrow (\sqcup S \sqsubseteq m)$);

– the *semantic transformer* F is a total map from D to D (denoted $F \in D \longmapsto D$) assumed to be

  - monotone (denoted $F \in D \overset{\mathrm{m}}{\longmapsto} D \triangleq$ [1] $\{\varphi \in D \longmapsto D \mid \forall x, y \in D : (x \sqsubseteq y) \Longrightarrow (\varphi(x) \sqsubseteq \varphi(y))\}$)
  - iteratable (that is the transfinite *iterates of* F *from* $\bot$ (defined as $F^0 \triangleq \bot$, $F^{\delta+1} \triangleq F(F^\delta)$ for successor ordinals $\delta + 1$ and $F^\lambda \triangleq \bigsqcup\limits_{\delta<\lambda} F^\delta$ for limit ordinals λ) are well-defined).

For example if $\langle D,\ \sqsubseteq,\ \bot,\ \sqcup\rangle$ is a directed-complete partial order or DCPO then monotony implies iteratability [1].

The Kleenian fixpoint theorem (see a.o. [14] for a proof) states that by monotony, these transfinite 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 fixpoint is the $\sqsubseteq$-least one $F^\epsilon = \mathrm{lfp}^{\sqsubseteq}\ F$.

So the *fixpoint semantics* S can be specified as the $\sqsubseteq$-least fixpoint $S \triangleq \mathrm{lfp}^{\sqsubseteq}\ F = F^\epsilon$ of F.

We prefer semantics specifications in fixpoint form which directly leads to proof methods using D. Park [45] or D. Scott [22] induction and to iterative program analysis algorithms by fixpoint approximation [13]. Other presentations, in particular in rule-based form, are equivalent after a suitable generalization as proposed in [19].

For example, by partially defining the meaning of rules

$$\left\{\frac{P_i}{C_i}\ \middle|\ i \in \Delta\right\}$$

[1] $\triangleq$ stands for "is defined as".

on the semantic domain $\langle D,\ \sqsubseteq,\ \bot,\ \sqcup\rangle$ as:

$$\operatorname{lfp}^{\sqsubseteq} \lambda X \bullet \bigsqcup\{C_i \mid i \in \Delta \wedge P_i \sqsubseteq X\}\ ,$$

if it exists, then an equivalent rule-based presentation of the fixpoint semantics is:

$$\left\{\frac{X}{F(X)}\ \middle|\ X \in D\right\}\ ,$$

with meaning $\operatorname{lfp}^{\sqsubseteq} F$ since $\lambda X \bullet \sqcup\{C_i \mid i \in \Delta \wedge P_i \sqsubseteq X\} = F$ [2].

2.2. Fixpoint Semantics Approximation

In abstract interpretation, the *concrete semantics* $S^{\vee}$ is approximated by a *abstract semantics* $S^{\wedge}$ via an abstraction function $\alpha \in D^{\vee} \longmapsto D^{\wedge}$ such that $\alpha(S^{\vee}) \sqsubseteq^{\wedge} S^{\wedge}$ [3,4]. The abstraction is *exact* [5] if $\alpha(S^{\vee}) = S^{\wedge}$ and *approximate* if $\alpha(S^{\vee}) \sqsubset^{\wedge} S^{\wedge}$. To derive $S^{\wedge}$ from $S^{\vee}$ by abstraction or $S^{\vee}$ from $S^{\wedge}$ by refinement, we can use the following fixpoint approximation theorems (as usual, we say that a function f is *Scott-continuous*, written $f : D \overset{\mathrm{c}}{\longmapsto} E$, if and only if it is monotone and preserves the lub of any directed subset A of D [1] and $\bot$-*strict*, written $f : D \overset{\bot}{\longmapsto} E$, if and only if $f(\bot) = \bot$):

Theorem 1. (Kleenian fixpoint approximation). Let $\langle\langle D^{\vee},\ \sqsubseteq^{\vee},\ \bot^{\vee},\ \sqcup^{\vee}\rangle,\ F^{\vee}\rangle$ and $\langle\langle D^{\wedge},\ \sqsubseteq^{\wedge},\ \bot^{\wedge},\ \sqcup^{\wedge}\rangle,\ F^{\wedge}\rangle$ be concrete and abstract fixpoint semantics specifications.

Assume that the $\bot$-strict Scott-continuous abstraction function $\alpha \in D^{\vee} \overset{\bot,\mathrm{c}}{\longmapsto} D^{\wedge}$ is such that for all $x \in D^{\vee}$ such that $x \sqsubseteq^{\vee} F^{\vee}(x)$ there exists $y \sqsubseteq^{\vee} x$ such that $\alpha(F^{\vee}(x)) \sqsubseteq^{\wedge} F^{\wedge}(\alpha(y))$.

Then $\alpha(\operatorname{lfp}^{\sqsubseteq^{\vee}} F^{\vee}) \sqsubseteq^{\wedge} \operatorname{lfp}^{\sqsubseteq^{\wedge}} F^{\wedge}$.

Proof. Let $F^{\vee\delta}$ and $F^{\wedge\delta}$, $\delta \in \mathbb{O}$ be the respective ordinal-termed $\sqsubseteq$-increasing ultimately stationary chains of transfinite iterates of $F^{\vee}$ and $F^{\wedge}$ [14]. We have $\alpha(F^{\vee 0}) = \alpha(\bot^{\vee}) = \bot^{\wedge} = F^{\wedge 0}$ by strictness of α and definition of the iterates. Assume $\alpha(F^{\vee\delta}) \sqsubseteq^{\wedge} F^{\wedge\delta}$ by induction hypothesis. We have $F^{\vee\delta} \sqsubseteq^{\vee} F^{\vee}(F^{\vee\delta}) = F^{\vee\delta+1}$ so that, by hypothesis, $\exists y \sqsubseteq^{\vee} F^{\vee\delta}$ such that $\alpha(F^{\vee\delta+1}) \sqsubseteq^{\wedge} F^{\wedge}(\alpha(y))$. By monotony of $F^{\wedge}$ and α, $F^{\wedge}(\alpha(y)) \sqsubseteq^{\vee} F^{\wedge}(\alpha(F^{\vee\delta}))$ whence by transitivity, induction hypothesis, monotony of $F^{\wedge}$ and definition of the iterates, $\alpha(F^{\vee\delta+1}) \sqsubseteq^{\wedge} F^{\wedge}(\alpha(F^{\vee\delta})) \sqsubseteq^{\wedge} F^{\wedge}(F^{\wedge\delta}) = F^{\wedge\delta+1}$. Given a limit ordinal λ, assume $\alpha(F^{\vee\delta}) \sqsubseteq^{\wedge} F^{\wedge\delta}$ for all $\delta < \lambda$. Then by definition of the iterates, continuity of α, induction hypothesis and definition of lubs, $\alpha(F^{\vee\lambda}) = \alpha(\bigsqcup^{\vee}_{\delta<\lambda} F^{\vee\delta}) = \bigsqcup^{\wedge}_{\delta<\lambda} \alpha(F^{\vee\delta}) \sqsubseteq^{\wedge} \bigsqcup^{\wedge}_{\delta<\lambda} F^{\wedge\delta} = F^{\wedge\lambda}$. By transfinite

[2] Observe that in both the fixpoint and the rule-based presentations of the semantics we make abstraction of the metalanguage which has to be used for formally defining the semantics of the programming language. So our approach is model-oriented or "relative" (in the sense for example of relative completeness) since we reason on the mathematical objects which should be defined by the metasemantics of this metalanguage, not on the way they are or can be formally specified by this metalanguage.

[3] More generally, we look for an abstract semantics $S^{\wedge}$ such that $\alpha(S^{\vee}) \preceq^{\wedge} S^{\wedge}$ for the *approximation partial ordering* $\preceq^{\wedge}$ corresponding to logical implication which may differ from the *computational partial orderings* $\sqsubseteq$ used to define least fixpoints [18].

[4] For program static analysis, the abstract semantics $S^{\wedge}$ is computable or can be dynamically approximated by widening/narrowing [9,13].

[5] We use the term *exactness* in preference to *completeness* as used in [15,29] in order to avoid a possible confusion with (relative) completeness in Hoare logic [11].

induction, we conclude $\forall\delta \in \mathbb{O} : \alpha(\check{F}^{\delta}) \mathrel{\hat{\sqsubseteq}} \hat{F}^{\delta}$. Let ϵ and ϵ' be the respective iteration orders such that $\check{F}^{\epsilon} = \mathrm{lfp}^{\check{\sqsubseteq}}\, \check{F}$ and $\hat{F}^{\epsilon'} = \mathrm{lfp}^{\hat{\sqsubseteq}}\, \hat{F}$. In particular $\alpha(\mathrm{lfp}^{\check{\sqsubseteq}}\, \check{F}) = \alpha(\check{F}^{\epsilon}) = \alpha(\check{F}^{\max\{\epsilon,\epsilon'\}}) \mathrel{\hat{\sqsubseteq}} \hat{F}^{\max\{\epsilon,\epsilon'\}} = \hat{F}^{\epsilon'} = \mathrm{lfp}^{\hat{\sqsubseteq}}\, \hat{F}$. $\square$

A. Tarski's fixpoint theorem [52] provides the basis for another fixpoint approximation theorem whenever any abstract post-fixpoint is an upper-approximation of the abstraction of a concrete post-fixpoint:

Theorem 2. (Tarskian fixpoint approximation). Let $\langle \check{D},\, \check{F}\rangle$ and $\langle \hat{D},\, \hat{F}\rangle$ be concrete and abstract fixpoint semantics specifications such that $\langle \check{D},\, \check{\sqsubseteq}, \check{\bot}, \check{\top}, \check{\sqcup}, \check{\sqcap}\rangle$ and $\langle \hat{D},\, \hat{\sqsubseteq}, \hat{\bot}, \hat{\top}, \hat{\sqcup}, \hat{\sqcap}\rangle$ are complete lattices.

Assume that the monotone abstraction function $\alpha \in \check{D} \xmapsto{\mathrm{m}} \hat{D}$ is such that for all $y \in \hat{D}$ such that $\hat{F}(y) \mathrel{\hat{\sqsubseteq}} y$ there exists $x \in \check{D}$ such that $\alpha(x) \mathrel{\hat{\sqsubseteq}} y$ and $\check{F}(x) \mathrel{\check{\sqsubseteq}} x$.

Then $\alpha(\mathrm{lfp}^{\check{\sqsubseteq}}\, \check{F}) \mathrel{\hat{\sqsubseteq}} \mathrm{lfp}^{\hat{\sqsubseteq}}\, \hat{F}$.

Proof. By the A. Tarski's fixpoint theorem [52], monotony of α, hypothesis and definition of greatest lower bounds (glb), we have $\alpha(\mathrm{lfp}^{\check{\sqsubseteq}}\, \check{F}) = \alpha(\check{\sqcap}\{x \mid \check{F}(x) \mathrel{\check{\sqsubseteq}} x\}) \mathrel{\hat{\sqsubseteq}} \hat{\sqcap}\{\alpha(x) \mid \check{F}(x) \mathrel{\check{\sqsubseteq}} x\} \mathrel{\hat{\sqsubseteq}} \hat{\sqcap}\{y \mid \hat{F}(y) \mathrel{\hat{\sqsubseteq}} y\} = \mathrm{lfp}^{\hat{\sqsubseteq}}\, \hat{F}$. $\square$

2.3. Fixpoint Semantics Transfer

When the abstraction must be exact, that is $\alpha(\check{S}) = \hat{S}$, we can use the following fixpoint transfer theorem, which provides guidelines for designing $\hat{S}$ from $\check{S}$ (or dually) in fixpoint form [15, theorem 7.1.0.4(3)], [21, lemma 4.3], [3, fact 2.3] [6]:

Theorem 3. (Kleenian fixpoint transfer). Let $\langle \check{D},\, \check{F}\rangle$ and $\langle \hat{D},\, \hat{F}\rangle$ be concrete and abstract fixpoint semantics specifications.

Assume that the $\bot$-strict Scott-continuous abstraction function $\alpha \in \check{D} \xmapsto{\bot,\mathrm{c}} \hat{D}$ satisfies the *commutation condition* $\hat{F} \circ \alpha = \alpha \circ \check{F}$.

Then

- the respective iterates $\check{F}^{\delta}$ and $\hat{F}^{\delta}$, $\delta \in \mathbb{O}$ of $\check{F}$ and $\hat{F}$ from $\check{\bot}$ and $\hat{\bot}$ satisfy $\forall\delta \in \mathbb{O}$: $\alpha(\check{F}^{\delta}) = \hat{F}^{\delta}$;
- $\alpha(\mathrm{lfp}^{\check{\sqsubseteq}}\, \check{F}) = \mathrm{lfp}^{\hat{\sqsubseteq}}\, \hat{F}$;
- the iteration order of $\hat{F}$ is less than or equal to that of $\check{F}$.

Proof. Let $\check{F}^{\delta}$ and $\hat{F}^{\delta}$, $\delta \in \mathbb{O}$ be the respective ordinal-termed $\sqsubseteq$-increasing ultimately stationary chains of transfinite iterates of $\check{F}$ and $\hat{F}$.

We have $\alpha(\check{F}^{0}) = \alpha(\check{\bot}) = \hat{\bot} = \hat{F}^{0}$ by strictness of α and definition of the iterates. Assume $\alpha(\check{F}^{\delta}) = \hat{F}^{\delta}$ by induction hypothesis. By definition of the iterates, commutation condition and induction hypothesis, we have $\alpha(\check{F}^{\delta+1}) = \alpha(\check{F}(\check{F}^{\delta})) = \hat{F}(\alpha(\check{F}^{\delta})) =$

[6] The composition of relations r_1 and r_2 is $r_1 \circ r_2 \triangleq \{\langle x,\, z\rangle \mid \exists y : \langle x,\, y\rangle \in r_1 \wedge \langle y,\, z\rangle \in r_2\}$ whence the composition of functions is $f \circ g(x) \triangleq f(g(x))$.

$F^{\hat{}}(F^{\hat{}\delta}) = F^{\hat{}\delta+1}$. Given a limit ordinal λ, assume $\alpha(F^{\check{}\delta}) = F^{\hat{}\delta}$ for all $\delta < \lambda$. Then by definition of the iterates, continuity of α and induction hypothesis, $\alpha(F^{\check{}\lambda}) = \alpha(\bigsqcup^{\check{}}_{\delta<\lambda} F^{\check{}\delta})$ $= \bigsqcup^{\hat{}}_{\delta<\lambda} \alpha(F^{\check{}\delta}) = \bigsqcup^{\hat{}}_{\delta<\lambda} F^{\hat{}\delta} = F^{\hat{}\lambda}$. By transfinite induction, we conclude $\forall \delta \in \mathbb{O} : \alpha(F^{\check{}\delta})$ $= F^{\hat{}\delta}$. In particular $\alpha(\mathrm{lfp}^{\sqsubseteq^{\check{}}} F^{\check{}}) = \alpha(F^{\check{}\epsilon}) = \alpha(F^{\check{}\max\{\epsilon,\epsilon'\}}) = F^{\hat{}\max\{\epsilon,\epsilon'\}} = F^{\hat{}\epsilon'} = \mathrm{lfp}^{\sqsubseteq^{\hat{}}} F^{\hat{}}$ where ϵ and ϵ' are the respective iteration orders.

$F^{\check{}\epsilon}$ is a fixpoint of $F^{\check{}}$ so that by the correspondence between iterates and the commutation condition, we have $F^{\hat{}}(F^{\hat{}\epsilon}) = F^{\hat{}}(\alpha(F^{\check{}\epsilon})) = \alpha(F^{\check{}}(F^{\check{}\epsilon})) = \alpha(F^{\check{}\epsilon}) = F^{\hat{}\epsilon}$ proving that $\epsilon' \leq \epsilon$. $\square$

Observe that in theorem 3 (as well as in theorem 1), Scott-continuity of the abstraction function α is a too strong hypothesis since in the proof we only use the fact that α preserves the lub of the iterates of $F^{\check{}}$ starting from $\bot^{\check{}}$.

When this is not the case, but α preserves glbs, we can rely on A. Tarski's fixpoint theorem [52], the commutation inequality ($F^{\hat{}} \circ \alpha \sqsubseteq^{\hat{}} \alpha \circ F^{\check{}}$) and the post-fixpoint correspondence (each abstract post-fixpoint of $F^{\hat{}}$ is the abstraction by α of some concrete post-fixpoint of $F^{\check{}}$):

Theorem 4. (Tarskian fixpoint transfer). Let $\langle D^{\check{}},\ F^{\check{}}\rangle$ and $\langle D^{\hat{}},\ F^{\hat{}}\rangle$ be concrete and abstract fixpoint semantics specifications such that $\langle D^{\check{}},\ \sqsubseteq^{\check{}}, \bot^{\check{}}, \top^{\check{}}, \sqcup^{\check{}},\ \sqcap^{\check{}}\rangle$ and $\langle D^{\hat{}},\ \sqsubseteq^{\hat{}}, \bot^{\hat{}}, \top^{\hat{}}, \sqcup^{\hat{}},\ \sqcap^{\hat{}}\rangle$ are complete lattices.

Assume that the abstraction function $\alpha \in D^{\check{}} \stackrel{\sqcap}{\longmapsto} D^{\hat{}}$ is a complete $\sqcap$-morphism satisfying the *commutation inequality* $F^{\hat{}} \circ \alpha \sqsubseteq^{\hat{}} \alpha \circ F^{\check{}}$ and the *post-fixpoint correspondence* $\forall y \in D^{\hat{}} : F^{\hat{}}(y) \sqsubseteq^{\hat{}} y \Longrightarrow \exists x \in D^{\check{}} : \alpha(x) = y \wedge F^{\check{}}(x) \sqsubseteq^{\check{}} x$.

Then $\alpha(\mathrm{lfp}^{\sqsubseteq^{\check{}}} F^{\check{}}) = \mathrm{lfp}^{\sqsubseteq^{\hat{}}} F^{\hat{}}$.

Proof. If $F^{\check{}}(x) \sqsubseteq^{\check{}} x$ then $\alpha \circ F^{\check{}}(x) \sqsubseteq^{\hat{}} \alpha(x)$ since α is monotone whence $F^{\hat{}} \circ \alpha(x) \sqsubseteq^{\hat{}} \alpha(x)$ by the commutation inequality. Together with the post-fixpoint correspondence, this implies $\{\alpha(x) \mid F^{\check{}}(x) \sqsubseteq^{\check{}} x\} = \{y \mid F^{\hat{}}(y) \sqsubseteq^{\hat{}} y\}$. By the A. Tarski's fixpoint theorem [52] and meet preservation, it follows that $\alpha(\mathrm{lfp}^{\sqsubseteq^{\check{}}} F^{\check{}}) = \alpha(\sqcap^{\check{}}\{x \mid F^{\check{}}(x) \sqsubseteq^{\check{}} x\}) = \sqcap^{\hat{}}\{\alpha(x) \mid F^{\check{}}(x) \sqsubseteq^{\check{}} x\} = \sqcap^{\hat{}}\{y \mid F^{\hat{}}(y) \sqsubseteq^{\hat{}} y\} = \mathrm{lfp}^{\sqsubseteq^{\hat{}}} F^{\hat{}}$. $\square$

2.4. Semantics Abstraction

An important particular case of abstraction function $\alpha \in D^{\check{}} \longmapsto D^{\hat{}}$ is when α preserves existing lubs $\alpha(\bigsqcup^{\check{}}_{i\in\Delta} x_i) = \bigsqcup^{\hat{}}_{i\in\Delta} \alpha(x_i)$. In this case there exists a unique map $\gamma \in D^{\hat{}} \longmapsto D^{\check{}}$ (so-called the *concretization function* [13]) such that the pair $\langle\alpha,\ \gamma\rangle$ is a *Galois connection*, written:

$$\langle D^{\check{}},\ \sqsubseteq^{\check{}}\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle D^{\hat{}},\ \sqsubseteq^{\hat{}}\rangle\ ,$$

which means that

- $\langle D^{\check{}},\ \sqsubseteq^{\check{}}\rangle$ and $\langle D^{\hat{}},\ \sqsubseteq^{\hat{}}\rangle$ are posets;
- $\alpha \in D^{\check{}} \longmapsto D^{\hat{}}$;

– $\gamma \in D^{\text{ˆ}} \longmapsto D^{\text{ˇ}}$;

– $\forall x \in D^{\text{ˇ}} : \forall y \in D^{\text{ˆ}} : \alpha(x) \sqsubseteq^{\text{ˆ}} y \Longleftrightarrow x \sqsubseteq^{\text{ˇ}} \gamma(y)$.

If α is surjective (resp. injective, bijective) then we have a *Galois insertion* written $\underset{\alpha}{\overset{\gamma}{\leftarrow\!\!\twoheadrightarrow}}$ (resp. *embedding*[7] written $\underset{\alpha}{\overset{\gamma}{\twoheadleftarrow\!\!\rightarrow}}$, *isomorphism* written $\underset{\alpha}{\overset{\gamma}{\twoheadleftarrow\!\!\twoheadrightarrow}}$). The use of Galois connections in abstract interpretation was motivated by the fact that $\alpha(x)$ is the best possible approximation of $x \in D^{\text{ˇ}}$ within $D^{\text{ˆ}}$ [13,15].

Example 5. (Subset abstraction). If $D^{\text{ˇ}}$ is a set and $D^{\text{ˆ}} \subseteq D^{\text{ˇ}}$ then $\langle \wp(D^{\text{ˇ}}), \subseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftarrow\!\!\twoheadrightarrow}} \langle \wp(D^{\text{ˆ}}), \subseteq \rangle$ where $\alpha(X) \triangleq X \cap D^{\text{ˆ}}$ and $\gamma(Y) \triangleq Y \cup \neg D^{\text{ˆ}}$ (where the *complement* of $\mathcal{E} \subseteq \mathcal{D}$ is $\neg\mathcal{E} \triangleq \{x \in \mathcal{D} \mid x \notin \mathcal{E}\}$). $\square$

Example 6. (Elementwise set abstraction). If $\mathtt{@} \in D^{\text{ˇ}} \longmapsto D^{\text{ˆ}}$, the abstraction function $\alpha \in \wp(D^{\text{ˇ}}) \longmapsto \wp(D^{\text{ˆ}})$ is defined by $\alpha(X) \triangleq \{\mathtt{@}(x) \mid x \in X\}$ and the concretization function $\gamma \in \wp(D^{\text{ˆ}}) \longmapsto \wp(D^{\text{ˇ}})$ is defined by $\gamma(Y) \triangleq \{x \mid \mathtt{@}(x) \in Y\}$ then $\langle \wp(D^{\text{ˇ}}), \subseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \wp(D^{\text{ˆ}}), \subseteq \rangle$. Moreover, if $\mathtt{@}$ is surjective then so is α. Classical examples are the rule of signs [15] (where $\forall z < 0 : \mathtt{@}(z) = -1$, $\mathtt{@}(0) = 0$ and $\forall z > 0 : \mathtt{@}(z) = +1$) and abstract model checking [20, Section 14]. $\square$

Example 7. (Supremus abstraction). If $\langle D^{\text{ˆ}}, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$ is a complete lattice and $\mathtt{@} \in D^{\text{ˇ}} \longmapsto D^{\text{ˆ}}$ then $\langle \wp(D^{\text{ˇ}}), \subseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle D^{\text{ˆ}}, \sqsubseteq \rangle$ with $\alpha(X) \triangleq \sqcup\{\mathtt{@}(x) \mid x \in X\}$ and $\gamma(Y) \triangleq \{x \mid \mathtt{@}(x) \sqsubseteq Y\}$. $\square$

We often use the fact that Galois connections compose[8]. If $\langle D^{\text{ˇ}}, \sqsubseteq^{\text{ˇ}} \rangle \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \langle D^{\text{ˇ}}, \sqsubseteq^{\text{ˇ}} \rangle$ and $\langle D^{\text{ˇ}}, \sqsubseteq^{\text{ˇ}} \rangle \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \langle D^{\text{ˆ}}, \sqsubseteq^{\text{ˆ}} \rangle$ then $\langle D^{\text{ˇ}}, \sqsubseteq^{\text{ˇ}} \rangle \underset{\alpha_2 \circ \alpha_1}{\overset{\gamma_1 \circ \gamma_2}{\leftrightarrows}} \langle D^{\text{ˆ}}, \sqsubseteq^{\text{ˆ}} \rangle$.

Example 8. (Elementwise subset abstraction). If $\mathcal{S} \subseteq D^{\text{ˇ}}$ and $\mathtt{@} \in \mathcal{S} \longmapsto D^{\text{ˆ}}$ then by composition of examples 5 and 6, we get $\langle \wp(D^{\text{ˇ}}), \subseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \wp(D^{\text{ˇ}}), \subseteq \rangle$ where $\alpha(X) \triangleq \{\mathtt{@}(x) \mid x \in X \cap \mathcal{S}\}$ and $\gamma \triangleq \{x \mid \mathtt{@}(x) \in Y\} \cup \neg\mathcal{S}$. $\square$

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

2.5. Fixpoint Semantics Fusion

Fixpoint semantics can often be defined by parts (e.g. corresponding respectively to finite behaviors and infinite behaviors) which can be then fused into a single fixpoint semantics (e.g. corresponding to all possible finite or infinite behaviors). The fusion of two disjoint powerset fixpoint semantics can be expressed in fixpoint form, trivially as follows:

---

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

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

Theorem 9. (Fixpoint fusion). Let $\{D^+, D^\omega\}$ be a partition of D^∞ and $\langle\langle\wp(D^+), \sqsubseteq^+\rangle, F^+\rangle$ and $\langle\langle\wp(D^\omega), \sqsubseteq^\omega\rangle, F^\omega\rangle$ be fixpoint semantics specifications. Partially define:

$$\begin{array}{rcl@{\qquad}rcl}
X^+ & \triangleq & X \cap D^+, & \bot^\infty & \triangleq & \bot^+ \cup \bot^\omega, \\
X^\omega & \triangleq & X \cap D^\omega, & \top^\infty & \triangleq & \top^+ \cup \top^\omega, \\
F^\infty(X) & \triangleq & F^+(X^+) \cup F^\omega(X^\omega), & \bigsqcup^\infty_{i\in\Delta} X_i & \triangleq & \bigsqcup^+_{i\in\Delta} X^+ \cup \bigsqcup^\omega_{i\in\Delta} X_i^\omega, \\
X \sqsubseteq^\infty Y & \triangleq & X^+ \sqsubseteq^+ Y^+ \wedge X^\omega \sqsubseteq^\omega Y^\omega, & \bigsqcap^\infty_{i\in\Delta} X_i & \triangleq & \bigsqcap^+_{i\in\Delta} X^+ \cup \bigsqcap^\omega_{i\in\Delta} X_i^\omega \ .
\end{array}$$

Then

- 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, complete $\sqcup$-morphisms) then so is F^∞;
- in all cases, $\mathrm{lfp}^{\sqsubseteq^\infty} F^\infty = \mathrm{lfp}^{\sqsubseteq^+} F^+ \cup \mathrm{lfp}^{\sqsubseteq^\omega} F^\omega$ whenever these fixpoints are well-defined.

Proof. These results are known for the cartesian product $\wp(D^+) \times \wp(D^\omega)$ with componentwise ordering $\sqsubseteq^+ \times \sqsubseteq^\omega$ whence follow by the correspondance $\langle\wp(D^+) \times \wp(D^\omega), \sqsubseteq^+ \times \sqsubseteq^\omega\rangle \xleftarrow[\alpha]{\gamma}\!\!\twoheadrightarrow \langle\wp(D^\infty), \sqsubseteq^\infty\rangle$ where $\alpha(\langle X, Y\rangle) = X \cup Y$ and $\gamma(X) = \langle X^+, X^\omega\rangle$ which is a Galois isomorphism since $\{D^+, D^\omega\}$ is assumed to be a partition of D^∞. $\square$

2.6. Fixpoint Iterates Reordering

For some fixpoint semantics 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 equally ordered by different orderings:

Theorem 10. (Fixpoint iterates reordering). Let $\langle\langle D, \sqsubseteq, \bot, \sqcup\rangle, F\rangle$ be a fixpoint semantics specification (the iterates of F, i.e. $F^0 \triangleq \bot$, $F^{\delta+1} \triangleq F(F^\delta)$ for successor ordinals $\delta + 1$ and $F^\lambda \triangleq \bigsqcup_{\delta<\lambda} F^\delta$ for limit ordinals λ, being well-defined). Let E be a set and $\preceq$ be a binary relation on E, such that:

1. $\preceq$ is a pre-order on E;
2. all iterates F^δ, $\delta \in \mathbb{O}$ of F belong to E;
3. $\bot$ is the $\preceq$-infimum of E;
4. the restriction $F|_E$ of F to E is $\preceq$-monotone;
5. for all $x \in E$, if λ is a limit ordinal and $\forall\delta < \lambda : F^\delta \preceq x$ then $\bigsqcup_{\delta<\lambda} F^\delta \preceq x$.

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

Proof. Let ϵ be the order of the iterates of F. By (2), $F^\epsilon \in E$ 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 (2) and (3), $F^0 = \bot \preceq x$. If $F^\delta \preceq x$ by induction hypothesis then by (2) and (4), $F^{\delta+1} = F(F^\delta) = F|_E(F^\delta) \preceq F|_E(x) = x$. By induction hypothesis and (5), $F^\lambda \preceq x$ for limit ordinals λ. By transfinite induction, $\forall \delta \in \mathbb{O} : F^\delta \preceq x$ so $\mathrm{lfp}^{\sqsubseteq}_{\bot} F = F^\epsilon \preceq x$. $\square$

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 (nonempty) set of states[9];
- $\tau \subseteq \Sigma \times \Sigma$ 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 and

$$\check{\tau} \quad \triangleq \quad \{s \in \Sigma \mid \forall s' \in \Sigma : \neg(s \ \tau \ s')\}$$

is the set of *final/blocking states*.

4. Finite and Infinite Sequences

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

4.1. Sequences

Let A be a nonempty 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 the alphabet A.
- $A^{\vec{+}} \triangleq \bigcup\limits_{n>0} A^{\vec{n}}$ is the set of nonempty finite sequences over A.
- The finite sequences are $A^{\vec{*}} \triangleq A^{\vec{+}} \cup A^{\vec{0}}$.
- The infinite sequences $\sigma = \sigma_0 \ldots \sigma_n \ldots$ are $A^{\vec{\omega}} \triangleq \mathbb{N} \longmapsto A$.
- The length of an infinite sequence $\sigma \in A^{\vec{\omega}}$ is $|\sigma| \triangleq \omega$.
- The sequences are $A^{\vec{\propto}} \triangleq A^{\vec{*}} \cup A^{\vec{\omega}}$.
- The nonempty sequences are $A^{\vec{\infty}} \triangleq A^{\vec{+}} \cup A^{\vec{\omega}}$.

[9] We could also consider actions as in [33] or in process algebra [40].

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

Nonempty finite sequences $\eta \in A^{\vec{\ell}}$ and $\xi \in A^{\vec{m}}$ are *joinable*, written $\eta \mathrel{\overset{\frown}{?}} \xi$, 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 $0 \leq n \leq m-1$.

Nonempty 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 $\eta \mathrel{\overset{\frown}{?}} \xi$, 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 nonempty sequences is $A \frown B \triangleq \{\eta \frown \xi \mid \eta \in A \wedge \xi \in B \wedge \eta \mathrel{\overset{\frown}{?}} \xi\}$.

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

Trace (or path) semantics model program computations by a set of finite or infinite sequences of states (which can also be understood as representing a tree which nodes are states). They have been used to specify the semantics both of programming languages [33] and of modal logics [37].

Given a transition system $\langle \Sigma, \tau \rangle$, $\Sigma^{\vec{n}}$ is the set of finite sequences of length n over the alphabet Σ and $\Sigma^{\vec{\omega}}$ is set of infinite sequences over Σ, as defined in Section 4.1. The maximal trace semantics $\tau^{\vec{\infty}}$ of this transition system $\langle \Sigma, \tau \rangle$ is defined as follows:

- $\tau^{\dot{\vec{n}}} \triangleq \{\sigma \in \Sigma^{\vec{n}} \mid \forall i < n-1 : \sigma_i \; \tau \; \sigma_{i+1}\}$ is the set of *partial execution traces* of length $n > 0$;

- $\tau^{\vec{n}} \triangleq \{\sigma \in \tau^{\dot{\vec{n}}} \mid \sigma_{n-1} \in \check{\tau}\}$ is the set of *maximal/complete execution traces* of length $n > 0$ terminating with a final/blocking state;

- $\tau^{\vec{+}} \triangleq \bigcup_{n>0} \tau^{\vec{n}}$ is the *maximal finite trace semantics*;

- $\tau^{\vec{\omega}} \triangleq \{\sigma \in \Sigma^{\vec{\omega}} \mid \forall i \in \mathbb{N} : \sigma_i \; \tau \; \sigma_{i+1}\}$ is the *infinite trace semantics*;

– Their join $\tau^{\vec{\infty}} \triangleq \tau^{\vec{+}} \cup \tau^{\vec{\omega}}$ is the *maximal trace semantics*.

5.1. Fixpoint Finite Trace Semantics

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

Theorem 11. (Fixpoint finite trace semantics). $\tau^{\vec{+}} = \mathrm{lfp}_{\emptyset}^{\subseteq} F^{\vec{+}} = \mathrm{gfp}_{\Sigma^{\vec{+}}}^{\subseteq} F^{\vec{+}}$ 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 $\mathrm{lfp}_{\emptyset}^{\subseteq} F^{\vec{+}}$ are $X^0 = \emptyset$, $X^1 = F^{\vec{+}}(X^0) = \tau^{\vec{1}} \cup (\tau^{\dot{\vec{2}}} \frown \emptyset) = \tau^{\vec{1}}$, $X^2 = F^{\vec{+}}(X^1) = \tau^{\vec{1}} \cup (\tau^{\dot{\vec{2}}} \frown \tau^{\vec{1}}) = \tau^{\vec{1}} \cup \tau^{\vec{2}}$, etc. By recurrence, the n-th iterate of $F^{\vec{+}}$ 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 the Kleenian fixpoint theorem, $\mathrm{lfp}_{\emptyset}^{\subseteq} F^{\vec{+}} = \bigcup_{n\in\mathbb{N}} X^n = \bigcup_{n\in\mathbb{N}} \bigcup_{i=1}^{n} \tau^{\vec{i}} = \bigcup_{i>0} \tau^{\vec{i}} = \tau^{\vec{+}}$.

The first iterates of $F^{\vec{+}}$ for $\mathrm{gfp}_{\Sigma^{\vec{+}}}^{\subseteq} F^{\vec{+}}$ 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 of $F^{\vec{+}}$ 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 the Kleenian dual fixpoint theorem, $\mathrm{gfp}_{\Sigma^{\vec{+}}}^{\subseteq} F^{\vec{+}} = \bigcap_{n\in\mathbb{N}} Y^n = \bigcap_{n\in\mathbb{N}} ((\bigcup_{i=1}^{n} \tau^{\vec{i}}) \cup (\tau^{\dot{\overrightarrow{n+1}}} \frown \Sigma^{\vec{+}})) = \bigcup_{i>0} \tau^{\vec{i}} = \tau^{\vec{+}}$ 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 $\sigma \notin Y^{i+2}$. $\square$

5.2. Fixpoint Infinite Trace Semantics

The *infinite trace semantics* $\tau^{\vec{\omega}}$ can be presented in $\subseteq$-greatest fixpoint form as follows [17, example 20]:

Theorem 12. (Fixpoint infinite trace semantics). $\tau^{\vec{\omega}} = \mathrm{gfp}_{\Sigma^{\vec{\omega}}}^{\subseteq} F^{\vec{\omega}}$ 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 $\langle \wp(\Sigma^{\vec{\omega}}),\ \supseteq, \Sigma^{\vec{\omega}}, \emptyset, \cap, \cup\rangle$. $\mathrm{lfp}_{\emptyset}^{\subseteq} F^{\vec{\omega}} = \emptyset$.

Proof. The first iterates of $F^{\vec{\omega}}$ for $\mathrm{gfp}_{\Sigma^{\vec{\omega}}}^{\subseteq} F^{\vec{\omega}}$ 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 the dual Kleenian fixpoint theorem, $\mathrm{gfp}_{\Sigma^{\vec{\omega}}}^{\subseteq} F^{\vec{\omega}} = \bigcap_{n\in\mathbb{N}} X^n = \bigcap_{n\in\mathbb{N}} \tau^{\dot{\overrightarrow{n+1}}} \frown \Sigma^{\vec{\omega}}$

$= \bigcap\limits_{n>0} \tau^{\vec{n}} \frown \Sigma^{\vec{\omega}} = \tau^{\vec{\omega}}$ 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 $\bigcap\limits_{n\in\mathbb{N}} X^n$, we have $\sigma_i\ \tau\ \sigma_{i+1}$ since otherwise $\sigma \notin X^i$. $\square$

5.3. Fixpoint Maximal Trace Semantics

By the fixpoint fusion theorem 9 and fixpoint theorems 11 and 12, the *maximal trace semantics* $\tau^{\vec{\infty}}$ can now be presented in two different fixpoint forms, as follows [17, examples 21 & 28]:

Theorem 13. (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 11, 12 and 9, 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 11, 12 and the dual of theorem 9, we also have: $\tau^{\vec{\infty}} \triangleq \tau^{\vec{+}} \cup \tau^{\vec{\omega}} = \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{+}}} F^{\vec{+}}$ $\cup\ \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}} = \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\infty}}} F^{\vec{\infty}}$. $\square$

The nondeterminism 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 [5] using program execution trees. This is not in contradiction with [3, theorem 3.4] proving that there is no fully abstract continuous compositional least fixpoint semantics that has a continuous full abstraction function. This result is proved for a specific operational semantic domain only and does not apply to all semantic domains. For example, unbounded nondeterminism is equivalent[10] 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.

We characterize the iterates of the various semantics that we consider in order to be able to reorder them as described in section 2.6. This will show that besides the classical partial

[10]informally, in the sense that unbounded nondeterminism can be used to simulate weak fairness and reciprocally.

orderings which are traditionally considered in fixpoint semantics, there exist alternative orderings which coincide on the iterates but may differ elsewhere hence may be more simple and/or expressive.

Corollary 14. (Arrangement of the iterates of $\vec{F^{\infty}}$). Let $\vec{F^{\infty}}^{\delta}$, $\delta \in \mathbb{O}$ be the iterates of $\vec{F^{\infty}}$ from $\perp^{\vec{\infty}}$. Their order is ω and $\tau^{\vec{\infty}} = \vec{F^{\infty}}^{\omega} = \bigsqcup^{\vec{\infty}}_{n<\omega} \vec{F^{\infty}}^{n}$. We have $\forall n < \omega :$ $\vec{F^{\infty}}^{n} = (\bigcup_{i=1}^{n} \tau^{\vec{i}}) \cup (\tau^{\overrightarrow{n+1}} \frown \Sigma^{\vec{\omega}})$.

Proof. Let $\vec{F^{+}}^{\delta}$ (resp. $\vec{F^{\omega}}^{\delta}$), $\delta \in \mathbb{O}$ be the iterates of $\vec{F^{+}}$ (resp. $\vec{F^{\omega}}$) from $\perp^{\vec{+}}$ (resp. $\perp^{\vec{\omega}}$). Both have order ω. By transfinite induction, $\forall \delta \in \mathbb{O} : \vec{F^{\infty}}^{\delta} = \vec{F^{+}}^{\delta} \cup \vec{F^{\omega}}^{\delta}$ where for all $n < \omega$, $\vec{F^{+}}^{n} = \bigcup_{i=1}^{n} \tau^{\vec{i}}$ and $\vec{F^{\omega}}^{n} = \tau^{\overrightarrow{n+1}} \frown \Sigma^{\vec{\omega}}$ as shown by the respective proofs of theorems 11 and 12. $\square$

One may wonder why, following [17], we have characterized the trace semantics as $\tau^{\vec{\infty}} = \mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\perp^{\vec{\infty}}} \vec{F^{\infty}}$ while $\tau^{\vec{\infty}} = \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\infty}}} \vec{F^{\infty}}$ is both more frequently used in the literature (e.g. [4]) and apparently simpler. This is because $\tau^{\vec{\infty}} = \mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\perp^{\vec{\infty}}} \vec{F^{\infty}}$ may lift to further abstractions while $\tau^{\vec{\infty}} = \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\infty}}} \vec{F^{\infty}}$ does not. For an example, let us consider potential termination. This also illustrates the fundamental idea in abstract interpretation that the abstraction specifies the observable properties on program behavior which can be specified in fixpoint form by Kleenian or Tarskian fixpoint transfer (and fixpoint fusion).

5.4. Potential Termination Semantics

The *potential termination abstraction* $\alpha^{\dashv?}$ is the elementwise finite trace subset abstraction (example 8, that is the composition of examples 5 and 6) where an element, that is a trace, is abstracted by its first state:

$$\begin{aligned}
\alpha^{\vec{+}}(X) &\triangleq X \cap \Sigma^{\vec{+}} ,\\
\alpha^{\downarrow 0}(X) &\triangleq \{@^{\downarrow 0}(x) \mid x \in X\} \qquad \text{where} \qquad @^{\downarrow 0}(\sigma) \triangleq \sigma_0 ,\\
\alpha^{\dashv?}(X) &\triangleq \alpha^{\downarrow 0} \circ \alpha^{\vec{+}} = \{\sigma_0 \mid \sigma \in X \cap \Sigma^{\vec{+}}\} .
\end{aligned}$$

By defining the concretization

$$\gamma^{\dashv?}(Y) \triangleq \gamma^{\vec{+}} \circ \gamma^{\downarrow 0}(Y) = \{\sigma \in \Sigma^{\vec{+}} \mid \sigma_0 \in Y\} \cup \Sigma^{\vec{\omega}} ,$$

this is a Galois insertion:

Lemma 15. $\langle \wp(\Sigma^{\vec{\infty}}), \sqsubseteq^{\vec{\infty}} \rangle \underset{\alpha^{\dashv?}}{\overset{\gamma^{\dashv?}}{\leftrightarrows}} \langle \wp(\Sigma), \subseteq \rangle$.

Proof. We have $\alpha^{\dashv?}(X) \subseteq Y \iff \forall \sigma \in X^{\vec{+}} : \sigma_0 \in Y \iff X^{\vec{+}} \subseteq (\{\sigma \in \Sigma^{\vec{+}} \mid \sigma_0 \in Y\} \cup \Sigma^{\vec{\omega}}) \cap \Sigma^{\vec{+}} \iff X^{\vec{+}} \subseteq (\gamma^{\dashv?}(Y))^{\vec{+}} \wedge X^{\vec{\omega}} \supseteq \emptyset \iff X^{\vec{+}} \subseteq (\gamma^{\dashv?}(Y))^{\vec{+}} \wedge X^{\vec{\omega}} \supseteq (\gamma^{\dashv?}(Y))^{\vec{\omega}}$ $\iff X \sqsubseteq^{\vec{\infty}} \gamma^{\dashv?}(Y)$ so that $\langle \wp(\Sigma^{\vec{\infty}}), \sqsubseteq^{\vec{\infty}} \rangle \underset{\alpha^{\dashv?}}{\overset{\gamma^{\dashv?}}{\leftrightarrows}} \langle \wp(\Sigma), \subseteq \rangle$. $\square$

The *potential termination semantics* $\tau^{\dashv ?}$ of a transition system $\langle\Sigma,\ \tau\rangle$ provides the set of states starting an execution which *may* terminate, that is

$$\tau^{\dashv ?} \ \triangleq\ \alpha^{\dashv ?}(\tau^{\vec{\infty}}) \ .$$

We define the *left image* of a state $s \in \Sigma$ by a transition relation $\tau \subseteq \Sigma \times \Sigma$ as

$$\tau^{\blacktriangleleft}(s) \ \triangleq\ \{s' \mid s' \ \tau \ s\} \ ,$$

while for a set $S \subseteq \Sigma$ of states, it is

$$\tau^{\blacktriangleleft}(S) \ \triangleq\ \bigcup_{s\in S} \tau^{\blacktriangleleft}(s) \ =\ \{s' \mid \exists s \in S : s' \ \tau \ s\} \ .$$

The fixpoint form of $\tau^{\dashv ?} = \alpha^{\dashv ?}(\tau^{\vec{\infty}}) = \mathrm{lfp}^{\subseteq}_{\emptyset} F^{\dashv ?}$ is derived from that of $\tau^{\vec{\infty}} = \mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\bot^{\vec{\infty}}} F^{\vec{\infty}}$ (theorem 13) by Kleenian fixpoint transfer. In the proof, the commutation condition $\alpha^{\dashv ?} \circ F^{\vec{\infty}} = F^{\dashv ?} \circ \alpha^{\dashv ?}$ leads to the calculational design of $F^{\dashv ?}$ starting from the definition $F^{\dashv ?}$.

Theorem 16. (Fixpoint potential termination semantics). $\tau^{\dashv ?} = \mathrm{lfp}^{\subseteq}_{\emptyset} F^{\dashv ?}$ where $F^{\dashv ?} \in \wp(\Sigma) \xrightarrow{\ \cup\ } \wp(\Sigma)$ defined as $F^{\dashv ?}(X) \triangleq \check{\tau} \cup \tau^{\blacktriangleleft}(X)$ is a complete $\cup$-morphism on the complete lattice $\langle\wp(\Sigma),\ \subseteq, \emptyset, \Sigma, \cup, \cap\rangle$.

Proof. We have $\alpha^{\dashv ?}(\bot^{\vec{\infty}}) = \alpha^{\dashv ?}(\Sigma^{\vec{\omega}}) = \emptyset$ so that by lemma 15 and the Kleenian fixpoint transfer theorem 3 and 13, we have $\tau^{\dashv ?} = \alpha^{\dashv ?}(\tau^{\vec{\infty}}) = \alpha^{\dashv ?}(\mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\bot^{\vec{\infty}}} F^{\vec{\infty}}) = \mathrm{lfp}^{\subseteq}_{\emptyset} F^{\dashv ?}$ where the commutation condition leads to the design of the transformer $F^{\dashv ?}$ as follows: $\alpha^{\dashv ?} \circ F^{\vec{\infty}}(X)$ $= \alpha^{\dashv ?}(\tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X) = \alpha^{\dashv ?}(\tau^{\vec{1}}) \cup \alpha^{\dashv ?}(\tau^{\dot{\vec{2}}} \frown X) = \{\sigma_0 \mid \sigma \in \tau^{\vec{1}}\} \cup \{\sigma_0 \mid \sigma \in (\tau^{\dot{\vec{2}}} \frown X) \cap \Sigma^{\vec{+}}\} =$ $\check{\tau} \cup \{s \mid \exists s' \in \alpha^{\dashv ?}(X) : s \ \tau \ s'\} = F^{\dashv ?}(\alpha^{\dashv ?}(X))$ by defining $F^{\dashv ?}(X) \triangleq \check{\tau} \cup \tau^{\blacktriangleleft}(X)$. $\square$

For example if $\Sigma \triangleq \{a, b\}$ and $\tau \triangleq \{\langle a,\ a\rangle, \langle a,\ b\rangle\}$ then $\tau^{\dashv ?} = \{a, b\}$ since any execution starting in state b immediately terminates while any execution starting in state a may always potentially terminate by choosing the $\langle a,\ b\rangle$ transition (although it is possible to never terminate by always choosing the $\langle a,\ a\rangle$ transition).

In general $\tau^{\dashv ?} \neq \mathrm{gfp}^{\subseteq}_{\Sigma} F^{\dashv ?}$ (so that $\alpha^{\dashv ?}$ 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 $\tau^{\dashv ?} = \emptyset$ while $\mathrm{gfp}^{\subseteq}_{\Sigma} F^{\dashv ?} = \{a\}$. Hence $\alpha^{\dashv ?}$ transfers $\mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\bot^{\vec{\infty}}} F^{\vec{\infty}}$ but not $\mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\infty}}} F^{\vec{\infty}}$.

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 [41], possibly using D. Scott's bottom $\bot \notin \Sigma$ to denote nontermination [38]. 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* (first named *big-step operational semantics* by G. Plotkin [48] and later *natural semantics* by G. Kahn [36], *relational semantics* by R. Milner & M. Tofte [41] and *evaluation semantics* by A. Pitts [47]) is

$$\tau^{+} \quad \stackrel{\Delta}{=} \quad \alpha^{+}(\tau^{\vec{+}})$$

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:

$$\alpha^{+}(X) \quad \stackrel{\Delta}{=} \quad \{\texttt{@}^{+}(\sigma) \mid \sigma \in X\} \quad \text{and}$$
$$\gamma^{+}(Y) \quad \stackrel{\Delta}{=} \quad \{\sigma \mid \texttt{@}^{+}(\sigma) \in Y\}$$

where:

$$\texttt{@}^{+} \quad \in \quad \Sigma^{\vec{+}} \longmapsto (\Sigma \times \Sigma)\ ,$$
$$\texttt{@}^{+}(\sigma) \quad \stackrel{\Delta}{=} \quad \langle \sigma_0,\ \sigma_{n-1}\rangle\ ,$$

for all $\sigma \in \Sigma^{\vec{n}}$ and $n \in \mathbb{N}$.

Defining the set

$$\bar{\tau} \quad \stackrel{\Delta}{=} \quad \{\langle s,\ s\rangle \mid s \in \check{\tau}\}$$

of *final/blocking state pairs* and using the Kleenian fixpoint transfer 3 and the theorem 11, we can express τ^{+} in fixpoint form:

Theorem 17. (Fixpoint finite/angelic relational semantics). $\tau^{+} = \mathrm{lfp}_{\emptyset}^{\subseteq} F^{+}$ where $F^{+} \in \wp(\Sigma \times \Sigma) \xrightarrow{\ \cup\ } \wp(\Sigma \times \Sigma)$ defined as $F^{+}(X) \stackrel{\Delta}{=} \bar{\tau} \cup (\tau \circ X)$ is a complete $\cup$-morphism on the complete lattice $\langle \wp(\Sigma \times \Sigma),\ \subseteq, \emptyset, \Sigma \times \Sigma, \cup, \cap\rangle$.

Proof. By the Kleenian fixpoint transfer theorem 3, using the Galois insertion of example 6 and $\alpha^{+} \circ F^{\vec{+}}(X) = \{\texttt{@}^{+}(x) \mid x \in \tau^{\vec{1}} \cup (\tau^{\dot{\vec{2}}} \frown X)\} = \{\langle s,\ s\rangle \mid \forall s' \in \Sigma : \neg(s\ \tau\ s')\} \cup \{\langle s,\ \sigma_{n-1}\rangle \mid n > 0 \wedge \sigma \in \Sigma^{\vec{n}} \wedge s\ \tau\ \sigma_0 \wedge \sigma \in X\} = \bar{\tau} \cup (\tau \circ \alpha^{+}(X)) = F^{+} \circ \alpha^{+}(X)$ by defining $F^{+}(X) \stackrel{\Delta}{=} \bar{\tau} \cup (\tau \circ X)$. $\square$

Observe that the Tarskian fixpoint transfer theorem 4 is not applicable since α^{+} is a $\cap$-morphism but <u>not</u> co-continuous hence <u>not</u> a complete $\cap$-morphism. A counter example is given by the $\subseteq$-decreasing chain $X^{k} \stackrel{\Delta}{=} \{a^{n}b \mid n \geq k\}, k > 0$ 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 $\alpha^{+}(\bigcap_{k>0} X^{k}) = \alpha^{+}(\emptyset) = \emptyset$.

In order to place the potential termination semantics $\tau^{\dashv ?}$ in the hierarchy of semantics, we will use the following:

Theorem 18. $\tau^{\dashv?} = \alpha^{\text{Dmn}}(\tau^{+})$ where the *domain abstraction*:

$$\langle \wp(\Sigma \times \Sigma),\ \subseteq\rangle \xleftarrow[\alpha^{\text{Dmn}}]{\gamma^{\text{Dmn}}} \langle \wp(\Sigma),\ \subseteq\rangle$$

is defined by:

$$\begin{aligned}\alpha^{\text{Dmn}}(R) &\triangleq \{s \mid \exists s' \in \Sigma : \langle s,\ s'\rangle \in R\} \quad \text{and}\\ \gamma^{\text{Dmn}}(D) &\triangleq \{\langle s,\ s'\rangle \mid s \in D \wedge s' \in \Sigma\}\ .\end{aligned}$$

Proof. By definition of τ^{+}, $\tau^{\vec{+}}$, $\tau^{\vec{\infty}}$, α^{Dmn}, α^{+}, $\alpha^{\dashv?}$ and $\tau^{\dashv?}$, we have:
$\alpha^{\text{Dmn}}(\tau^{+}) = \alpha^{\text{Dmn}}(\alpha^{+}(\tau^{\vec{+}})) = \alpha^{\text{Dmn}}(\alpha^{+}(\tau^{\vec{\infty}} \cap \Sigma^{\vec{+}})) = \{s \mid \exists s' \in \Sigma : \langle s,\ s'\rangle \in \alpha^{+}(\tau^{\vec{\infty}} \cap \Sigma^{\vec{+}})\}$
$= \{\sigma_0 \mid \sigma \in \tau^{\vec{\infty}} \cap \Sigma^{\vec{+}}\} = \alpha^{\dashv?}(\tau^{\vec{\infty}}) = \tau^{\dashv?}$. ☐

7.2. Infinite Relational Semantics

The *infinite relational semantics* is

$$\tau^{\omega} \triangleq \alpha^{\omega}(\tau^{\vec{\omega}})$$

where the Galois insertion:

$$\langle \wp(\Sigma^{\vec{\omega}}),\ \subseteq\rangle \xleftarrow[\alpha^{\omega}]{\gamma^{\omega}} \langle \wp(\Sigma \times \{\bot\}),\ \subseteq\rangle$$

is defined by

$$\begin{aligned}\alpha^{\omega}(X) &\triangleq \{@^{\omega}(\sigma) \mid \sigma \in X\} \quad \text{and}\\ \gamma^{\omega}(Y) &\triangleq \{\sigma \mid @^{\omega}(\sigma) \in Y\}\end{aligned}$$

where:

$$\begin{aligned}@^{\omega} &\in \Sigma^{\vec{\omega}} \longmapsto (\Sigma \times \{\bot\}) \quad \text{is}\\ @^{\omega}(\sigma) &\triangleq \langle \sigma_0,\ \bot\rangle\ .\end{aligned}$$

By the Galois connection, α^{ω} is a complete $\cup$-morphism. It is a $\cap$-morphism but <u>not</u> a complete $\cap$-morphism since indeed it is <u>not</u> 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 $a^n b^{\omega} \notin X^{n+1}$ whence $\alpha^{\omega}(\bigcap_{k>0} X^k) = \alpha^{\omega}(\emptyset) = \emptyset$.

Using the Tarskian fixpoint transfer theorem 4 and theorem 12, we get:

Theorem 19. (Fixpoint infinite relational semantics). $\tau^{\omega} = \text{gfp}^{\subseteq}_{\Sigma \times \{\bot\}} F^{\omega}$ where $F^{\omega} \in \wp(\Sigma \times \{\bot\}) \xrightarrow{\text{m}} \wp(\Sigma \times \{\bot\})$ 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 $\alpha^\omega \circ F^{\vec{\omega}}(X) = \alpha^\omega(\tau^{\dot{\vec{2}}} \frown X) = \{\mathtt{@}^\omega(\eta \frown \xi) \mid \eta \in \tau^{\dot{\vec{2}}} \wedge \xi \in X \wedge \eta \mathrel{?} \xi\} = \{\langle\eta_0, \perp\rangle \mid \eta_0 \ \tau \ \xi_0 \wedge \xi \in X\} = \{\langle s, \perp\rangle \mid \exists s' : s \ \tau \ s' \wedge \langle s', \perp\rangle \in \alpha^\omega(X)\} = \tau \circ \alpha^\omega(X) = F^\omega \circ \alpha^\omega(X)$ by defining $F^\omega(X) \triangleq \tau \circ X$.

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

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

To prove that $F^\omega(X) \supseteq X$ observe that $F^\omega(X) \supseteq X \Longleftrightarrow X \subseteq \tau^{\dot{\vec{2}}} \frown X \Longleftrightarrow \forall\sigma \in X : \sigma_0 \ \tau \ \sigma_1 \wedge \sigma^{\geq 1} \in X$ 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 $X \subseteq \tau^{\vec{\omega}}$. $\eta \in \tau^{\vec{\omega}}$ and $\forall i \in \mathbb{N} : \langle\eta_i, \perp\rangle = \langle\sigma_i, \perp\rangle \in Y$ proving that $\eta = \sigma^{\geq 1} \in X$.

We conclude by the dual of the Tarskian fixpoint transfer theorem 4. $\square$

We say that *the nondeterminism of* τ *is bounded by* $n \in \mathbb{N}$ if and only if $\forall s \in \Sigma : |\{s' \mid \tau(s, s')\}| < n$ where $|S|$ is the cardinal of class S.

Lemma 20. If $X_\delta, \delta < \eta$ is a $\subseteq$-decreasing chain of subsets of $\Sigma \times \Sigma$ and the nondeterminism of τ is bounded by n then for all $s, s' \in \Sigma$:

$$\begin{aligned} & \forall\delta < \eta : \exists s'' : \tau(s, s'') \wedge \langle s'', s'\rangle \in X_\delta \\ \Longleftrightarrow\ & \exists s'' : \tau(s, s'') \wedge \forall\delta < \eta : \langle s'', s'\rangle \in X_\delta \ . \end{aligned}$$

Proof. The proof of $\Longleftarrow$ is obvious. For $\Longrightarrow$, we reason by reductio ad absurdum, assuming that:

$$\begin{aligned} & \forall\delta < \eta : \exists s'' : \tau(s, s'') \wedge \langle s'', s'\rangle \in X_\delta && (1) \\ \wedge\ \ & \forall s'' : \tau(s, s'') \Longrightarrow \exists\delta < \eta : \langle s'', s'\rangle \notin X_\delta \ . && (2) \end{aligned}$$

If η is a successor ordinal, then (1) implies that there exists s'' such that $\tau(s, s'') \wedge \langle s'', s'\rangle \in X_{\eta-1}$ so by (2) there exists $\delta \leq \eta - 1$ such that $\langle s'', s'\rangle \notin X_\delta$, in contradiction with the decreasing chain hypothesis implying that $X_\delta \supseteq X_{\eta-1}$.

If η is a limit ordinal, let us show that we can construct infinite sequences s_0, s_1, s_2, ... and $\delta_0 \leq \delta_1 \leq \delta_2 \leq \ldots < \eta$ such that for all $k \in \mathbb{N}$:

$$\tau(s, s_k) \wedge \langle s_k, s'\rangle \in X_{\delta_k} \wedge \langle s_k, s'\rangle \notin X_{\delta_{k+1}} \ . \qquad (3)$$

We let $\delta_0 = 0$ so that by (1) there exists s_0 such that $\tau(s, s_0) \wedge \langle s_0, s'\rangle \in X_{\delta_0}$ hence by (2) there exists $\delta_0 = 0 \leq \delta_1 < \eta$ such that $\langle s_0, s'\rangle \notin X_{\delta_1}$. Assuming that we have constructed $s_0, \ldots, s_i$ and $\delta_0 \leq \ldots \leq \delta_i \leq \delta_{i+1} < \eta$ satisfying (3) for all $0 \leq k \leq i$. By (1) there exists s_{i+1} such that $\tau(s, s_{i+1}) \wedge \langle s_{i+1}, s'\rangle \in X_{\delta_{i+1}}$ hence by (2) there exists $\delta < \eta$ such that $\langle s_{i+1}, s'\rangle \notin X_\delta$. We define $\delta_{i+2} \triangleq \max(\delta, \delta_{i+1})$ so that $\delta \leq \delta_{i+2}$ whence, by the $\subseteq$-decreasing

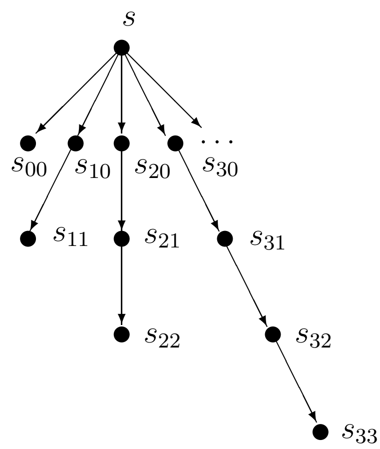


Figure 1. Transition system with unbounded nondeterminism

chain hypothesis, $X_\delta \supseteq X_{\delta_{i+2}}$ proving that $\langle s_{i+1},\ s'\rangle \notin X_{\delta_{i+2}}$. So we have constructed s_0, $\ldots$, s_{i+1} and $\delta_0 \leq \ldots \leq \delta_{i+1} \leq \delta_{i+2} < \eta$ satisfying (3) for all $0 \leq k \leq i+1$. The sequences can be extended to infinite ones by recurrence. Observe that in $s_0, \ldots, s_i, \ldots$ if $i < j$ then s_i must be distinct from s_j since otherwise $\langle s_i,\ s'\rangle \in X_{\delta_i}$ and $\langle s_i,\ s'\rangle \in X_{\delta_{i+1}} \supseteq X_{\delta_j}$ so $\langle s_i,\ s'\rangle \notin X_{\delta_i}$ in contradiction with $\langle s_j,\ s'\rangle \in X_{\delta_j}$ and $s_j = s_i$. So in the infinite sequence $s_0, \ldots, s_i, \ldots$ the states are distinct two by two proving that $|\{s_0, \ldots, s_k, \ldots\}| = \omega$. Moreover (3) implies that $\{s_0, \ldots, s_i, \ldots\} \subseteq \{s' \mid \tau(s, s')\}$ so $|\{s' \mid \tau(s, s')\}| \geq \omega$ in contradiction with the bounded nondeterminism hypothesis $|\{s' \mid \tau(s, s')\}| \leq n \in \mathbb{N}$. $\square$

Lemma 21. If the nondeterminism of τ is bounded then F^ω is co-continuous.

Proof. If $X_\delta, \delta < \eta$ is a $\subseteq$-decreasing chain of subsets of $\Sigma \times \Sigma$ then by definition of F^ω and lemma 20, we have $F^\omega(\bigcap_{\delta<\eta} X_\delta) = \tau \circ (\bigcap_{\delta<\eta} X_\delta) = \{\langle s,\ s'\rangle \mid \exists s'' : \tau(s, s'') \wedge \forall \delta < \eta : \langle s'',\ s'\rangle \in X_\delta\} = \{\langle s,\ s'\rangle \mid \forall \delta < \eta : \exists s'' : \tau(s, s'') \wedge \langle s'',\ s'\rangle \in X_\delta\} = \bigcap_{\delta<\eta}(\tau \circ X_\delta) = \bigcap_{\delta<\eta} F^\omega(X_\delta)$. $\square$

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

Example 22. (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 $\tau = \{\langle s,\ s_{i0}\rangle \mid i \in \mathbb{N}\} \cup \{\langle s_{ij},\ s_{i(j+1)}\rangle \mid 0 \leq j < i\}$ [53].

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

It follows that the Kleenian fixpoint transfer theorem 3 is not applicable to prove theorem 19 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

$$\tau^{\dashv !} \quad \triangleq \quad \alpha^{\dashv !}(\tau^{\omega})$$

where the Galois isomorphism:

$$\langle \wp(\Sigma \times \{\bot\}),\ \subseteq\rangle \underset{\alpha^{\dashv !}}{\overset{\gamma^{\dashv !}}{\leftrightarrows}} \langle \wp(\Sigma),\ \supseteq\rangle$$

is defined by

$$\begin{aligned} \alpha^{\dashv !}(X) \quad &\triangleq \quad \{s \mid \langle s,\ \bot\rangle \notin X\} \quad \text{and} \\ \gamma^{\dashv !}(Y) \quad &\triangleq \quad \{\langle s,\ \bot\rangle \mid s \notin Y\}\ . \end{aligned}$$

Given a relation $\tau \subseteq \Sigma \times \Sigma'$, a state $s \in \Sigma$ and a set of states $P \subseteq \Sigma$:

- The *right image of* s *by* τ is $\tau^{\bullet\!\blacktriangleright}(s) \triangleq \{s' \mid s\ \tau\ s'\}$ (in particular if $f \in \Sigma \longmapsto \Sigma'$ then $f^{\bullet\!\blacktriangleright}(s) = \{f(s)\}$).

- The *right image of* P *by* τ is $\tau^{\blacktriangleright}(P) = \{s' \mid \exists s \in P : s\ \tau\ s'\}$ (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 $\tau^{\blacktriangleleft\!\bullet} \triangleq (\tau^{-1})^{\bullet\!\blacktriangleright}$ 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 the Kleenian fixpoint transfer theorem 3 to the fixpoint characterization 19 of the infinite relational semantics τ^{ω}, we get the

Theorem 23. (Fixpoint inevitable termination semantics). $\tau^{\dashv !} = \mathrm{lfp}^{\subseteq}_{\emptyset}\ F^{\dashv !}$ where $F^{\dashv !} \in \wp(\Sigma) \overset{\cup}{\longmapsto} \wp(\Sigma)$ defined as $F^{\dashv !}(X) \triangleq \widetilde{\tau^{-1\blacktriangleright}}(X) = \check{\tau} \cup \widetilde{\tau^{-1\blacktriangleright}}(X)$ is a complete $\cup$-morphism on the complete lattice $\langle \wp(\Sigma),\ \subseteq, \emptyset, \Sigma, \cup, \cap\rangle$.

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

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*

$$\tau^{\infty} \quad \stackrel{\Delta}{=} \quad \tau^{+} \cup \tau^{\omega}$$

is the fusion of the finite relational semantics τ^{+} and the infinite relational semantics τ^{ω}.

It is more traditional [7,46] to consider the cartesian product of the finite relational semantics τ^{+} and the inevitable termination semantics $\tau^{\dashv\!!}$ (the interpretation being that any execution starting from a state $s \in \tau^{\dashv\!!}$ must terminate in a state s' such that $\langle s, s' \rangle \in \tau^{+}$). The reason for preferring the infinite relational semantics to the inevitable termination semantics 23 is that the fixpoint characterizations 17 of τ^{+} and 19 of τ^{ω} fuse naturally by the fixpoint fusion theorem 9. This leads to a simple fixpoint characterization of the natural relational semantics using the *mixed ordering* $\sqsubseteq^{\infty}$ first introduced in [17, proposition 25]:

Theorem 24. (Fixpoint natural relational semantics). $\tau^{\infty} = \mathrm{lfp}_{\perp^{\infty}}^{\sqsubseteq^{\infty}} F^{\infty}$ where $F^{\infty} \in \wp(\Sigma \times \Sigma_{\perp}) \stackrel{\mathrm{m}}{\longmapsto} \wp(\Sigma \times \Sigma_{\perp})$ defined as $F^{\infty}(X) \stackrel{\Delta}{=} \bar{\tau} \cup (\tau \circ X)$ 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

- $\Sigma_{\perp} \stackrel{\Delta}{=} \Sigma \cup \{\perp\}$,
- $X \sqsubseteq^{\infty} Y \stackrel{\Delta}{=} X^{+} \subseteq Y^{+} \wedge X^{\omega} \supseteq Y^{\omega}$,
- $X^{+} \stackrel{\Delta}{=} X \cap \top^{\infty}$,
- $\top^{\infty} = \Sigma \times \Sigma$,
- $X^{\omega} \stackrel{\Delta}{=} X \cap \perp^{\infty}$ 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 $\alpha^{\infty}(X) \stackrel{\Delta}{=} \alpha^{+}(X^{\vec{+}}) \cup \alpha^{\vec{\omega}}(X^{\omega})$, we have $\tau^{\infty} = \alpha^{\infty}(\tau^{\vec{\infty}})$. Neither the Kleenian fixpoint transfer theorem 3 nor the Tarskian fixpoint transfer theorem 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 the Kleenian fixpoint transfer theorem 3 (but the Tarskian's one was not applicable) and the infinitary part $\tau^{\vec{\omega}}$ by the Tarskian fixpoint transfer theorem 4 (but the Kleenian's one was not applicable).

To prove that the iterates of F^{∞} are ordered according to Egli-Milner ordering in corollary 37, we will use the following characterization of the iterates of F^{∞}. Intuitively if a new finite behavior does appear in the iterates, nontermination cannot yet be excluded.

Lemma 25. (Arrangement 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 $\perp^{\infty}$. 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 $F^{\infty 0} = \bot^{\infty} = \Sigma \times \{\bot\}$.

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 $\langle s,\ \bot\rangle \in F^{\infty\eta}$.

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

II. If $\langle s,\ \bot\rangle \notin F^{\infty\xi'}$ 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 $\langle s'',\ \bot\rangle \in F^{\infty\eta}$ so that $\langle s,\ \bot\rangle \in F^{\infty\eta+1}$ proving $\langle s,\ \bot\rangle \in F^{\infty\eta}$ 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 $F^{\infty\xi'} = \bigsqcup^{\infty}_{\zeta<\xi'} F^{\infty\zeta}$. □

The totality of the iterates expresses that an initial state must lead to at least one terminating or nonterminating behavior.

Lemma 26. (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 $(F^{\infty\delta})^{+} \subseteq (F^{\infty\lambda})^{+}$. $\square$

Finally all final states of the iterates cannot be simultaneously terminating and nonterminating states.

Lemma 27. (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 $F^{\infty\delta}$, $\delta \in \mathbb{O}$ is $\sqsubseteq^{\infty}$-increasing whence $(F^{\infty\delta})^{+}$, $\delta \in \mathbb{O}$ is $\subseteq$-increasing. By induction hypothesis, $s'' = s'$ $\square$

7.5. Demoniac Relational Semantics

The *demoniac*[11] *relational semantics* is derived from the natural relational semantics by approximating nontermination by chaos:

$$\tau^{\partial} \triangleq \alpha^{\partial}(\tau^{\infty})$$

where:

$$\begin{aligned} \alpha^{\partial}(X) &\triangleq X \cup \{\langle s, s'\rangle \mid \langle s, \bot\rangle \in X \wedge s' \in \Sigma\} \quad \text{and} \\ \gamma^{\partial}(Y) &\triangleq Y \end{aligned}$$

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 24 and the Kleenian fixpoint transfer theorem 3, we derive:

[11] alternatively *demoniacal* or *demonic*.

Theorem 28. (Fixpoint demoniac relational semantics). $\tau^\partial = \operatorname{lfp}^{\sqsubseteq^\partial}_{\bot^\partial} F^\partial$ where $F^\partial \in D^\partial \xrightarrow{\mathrm{m}} D^\partial$ 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

- $X \sqsubseteq^\partial Y = \forall s \in \Sigma : \langle s, \bot\rangle \in X \vee (\langle s, \bot\rangle \notin Y \wedge X \cap (\{s\} \times \Sigma) \subseteq Y \cap (\{s\} \times \Sigma))$,
- $\bot^\partial \triangleq \Sigma \times \Sigma_\bot$,
- $\top^\partial \triangleq \Sigma \times \Sigma$,
- $\bigsqcup\limits^\partial_{i\in\Delta} X_i \triangleq \{\langle s, s'\rangle \mid (\forall i \in \Delta : \langle s, \bot\rangle \in X_i \wedge s' \in \Sigma_\bot) \vee (\exists i \in \Delta : \langle s, \bot\rangle \notin X_i \wedge \langle s, s'\rangle \in X_i)\}$ and
- $\bigsqcap\limits^\partial_{i\in\Delta} X_i \triangleq \{\langle s, s'\rangle \mid (\exists i \in \Delta : \langle s, \bot\rangle \in X_i \wedge s' \in \Sigma_\bot) \vee (\forall i \in \Delta : \langle s, \bot\rangle \notin X_i \wedge \langle s, s'\rangle \in X_i)\}$.

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

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 $\gamma^{\eth}(X) = \gamma^{\eth}(Y)$. For all $s \in \Sigma$, we have $\langle s, \bot\rangle \in X$ iff $\langle s, \bot\rangle \in \gamma^{\eth}(X)$ iff $\langle s, \bot\rangle \in \gamma^{\eth}(Y)$ 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 $\gamma^{\eth}(X) = \gamma^{\eth}(Y)$ 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 $\gamma^{\eth}$ is injective.

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

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

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

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

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 $\gamma^{\eth} \circ \alpha^{\partial}(X) \sqsubseteq^{\infty} \gamma^{\eth} \circ \alpha^{\partial}(Y)$ whence $\alpha^{\partial}(X) \sqsubseteq^{\partial} \alpha^{\partial}(Y)$. This shows that α^{∂} is monotone.

$\alpha^{\partial} \circ \gamma^{\eth}(X) = \alpha^{\partial}(\{\langle s,\, \bot\rangle \mid \langle s,\, \bot\rangle \in X\} \cup \{\langle s,\, s'\rangle \mid \langle s,\, \bot\rangle \notin X \wedge \langle s,\, s'\rangle \in X\}) = \alpha^{\partial}(\{\langle s,\, \bot\rangle \mid \langle s,\, \bot\rangle \in X\}) \cup \alpha^{\partial}(\{\langle s,\, s'\rangle \mid \langle s,\, \bot\rangle \notin X \wedge \langle s,\, s'\rangle \in X\})$ 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 $\langle \wp(\Sigma \times \Sigma_{\bot}),\, \sqsupseteq^{\infty}\rangle \underset{\alpha^{\partial}}{\overset{\gamma^{\eth}}{\leftrightarrows}} \langle D^{\partial},\, \sqsupseteq^{\partial}\rangle$ since α^{∂} and $\gamma^{\eth}$ are monotone, $\alpha^{\partial} \circ \gamma^{\eth}$ is the identity on D^{∂} and $\gamma^{\eth} \circ \alpha^{\partial}$ 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 $\bigsqcup^{\partial}_{i\in\Delta} X_i = \alpha^{\partial}(\bigsqcup^{\infty}_{i\in\Delta} \gamma^{\eth}(X_i)) = \alpha^{\partial}((\bigcup_{i\in\Delta} \gamma^{\eth}(X_i) \cap \top^{\infty}) \cup (\bigcap_{i\in\Delta} \gamma^{\eth}(X_i) \cap \bot^{\infty})) = (\bigcup_{i\in\Delta} \alpha^{\partial}(\gamma^{\eth}(X_i) \cap (\Sigma \times \Sigma))) \cup (\alpha^{\partial}(\bigcap_{i\in\Delta} \gamma^{\eth}(X_i) \cap (\Sigma \times \{\bot\})))$ 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 $\bigsqcap^{\partial}_{i\in\Delta} X_i = \alpha^{\partial}(\bigsqcap^{\infty}_{i\in\Delta} \gamma^{\eth}(X_i)) = \{\langle s, s'\rangle \mid (\forall i \in \Delta : \langle s, \bot\rangle \notin X_i \wedge \langle s,\, s'\rangle \in X_i) \vee (\exists i \in \Delta : \langle s,\, \bot\rangle \in X_i \wedge s' \in \Sigma_{\bot})\}$.

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 $\langle s,\, \bot\rangle \in X_i \iff \langle s,\, \bot\rangle \in \alpha^{\partial}(X_i)$ and $\langle s,\, s'\rangle \in X_i \iff \langle s,\, s'\rangle \in \alpha^{\partial}(X_i)$ 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 24 and the Kleenian fixpoint transfer theorem 3, we conclude that $\tau^\partial \triangleq \alpha^\partial(\tau^\infty) = \alpha^\partial(\mathrm{lfp}^{\sqsubseteq^\infty}_{\perp^\infty} F^\infty)$ $= \mathrm{lfp}^{\sqsubseteq^\partial}_{\perp^\partial} F^\partial$. ☐

Lemma 29. (Arrangement of the iterates of F^∂). Let $F^{\partial\,\beta}$, $\beta \in \mathbb{O}$ be the iterates of F^∂ from $\perp^\partial$. 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 $\forall s' \in \Sigma_\perp : \langle s,\ s'\rangle \in F^{\partial\,\eta}$.

Proof. Follows from lemma 25 and the proof of theorem 28, showing by the Kleenian fixpoint transfer theorem 3 that $\forall \beta \in \mathbb{O} : F^{\partial\,\beta} = \alpha^\partial(F^{\infty\beta})$. ☐

Lemma 30. (Totality of the iterates of F^∂). Let $F^{\partial\,\beta}$, $\beta \in \mathbb{O}$ be the iterates of F^∂ from $\perp^\partial$. $\forall \beta \in \mathbb{O} : \forall s \in \Sigma : \exists s' \in \Sigma_\perp : \langle s,\ s'\rangle \in F^{\partial\,\delta}$.

Proof. Follows from lemma 26 and the proof of theorem 28, showing by the Kleenian fixpoint transfer theorem 3 that $\forall \beta \in \mathbb{O} : F^{\partial\,\beta} = \alpha^\partial(F^{\infty\beta})$. ☐

Lemma 31. (Final states of the iterates of F^∂). Let $F^{\partial\,\beta}$, $\beta \in \mathbb{O}$ be the iterates of F^∂ from $\perp^\partial$. $\forall \beta \in \mathbb{O} : \forall s, s' \in \Sigma : (\langle s,\ s'\rangle \in F^{\partial\,\beta} \wedge \langle s,\ \perp\rangle \notin F^{\partial\,\beta}) \Longrightarrow (s' \in \check{\tau}) \wedge (\forall s'' \in \Sigma_\perp : \langle s',\ s''\rangle \in F^{\partial\,\delta} \Longrightarrow s'' = s')$.

Proof. The proof of theorem 28 shows, by the Kleenian fixpoint transfer theorem 3, that $\forall \beta \in \mathbb{O} : F^{\partial\,\beta} = \alpha^\partial(F^{\infty\beta})$. So if $\langle s,\ \perp\rangle \notin F^{\partial\,\beta}$ 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 27. We have $\langle s',\ \perp\rangle \notin F^{\partial\,\beta}$ since otherwise $\langle s',\ \perp\rangle \in F^{\infty\beta}$ which is impossible by lemma 27 since $s' \neq \perp$. So if $s'' \in \Sigma_\perp$ then $\langle s',\ s''\rangle \in F^{\partial\,\beta}$ implies $\langle s',\ s''\rangle \in F^{\infty\beta}$ since $\langle s',\ \perp\rangle \notin F^{\infty\beta}$ so that $s'' = s'$ by lemma 27. ☐

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

Theorem 32. $\tau^\omega = \alpha^{\partial\,\omega}(\tau^\partial)$ where $\alpha^{\partial\,\omega}(X) \triangleq X \cap (\Sigma \times \{\perp\})$.

Proof. By definition of $\alpha^{\partial\,\omega}$, τ^∂, τ^∞, α^∂, $\tau^+ \subseteq \Sigma \times \Sigma$, $\perp \notin \Sigma$ and $\tau^\omega \subseteq \Sigma \times \{\perp\}$, we have $\alpha^{\partial\,\omega}(\tau^\partial) = \tau^\partial \cap (\Sigma \times \{\perp\}) = \alpha^\partial(\tau^\infty) \cap (\Sigma \times \{\perp\}) = (\tau^+ \cup \tau^\omega \cup \{\langle s,\ s'\rangle \mid \langle s,\ \perp\rangle \in \tau^+ \cup \tau^\omega \wedge s' \in \Sigma\}) \cap (\Sigma \times \{\perp\}) = \tau^\omega \cup \{\langle s,\ \perp\rangle \mid \langle s,\ \perp\rangle \in \tau^\omega\} = \tau^\omega$. ☐

8. Denotational Semantics

In contrast to operational semantics, denotational semantics abstracts away from the history of computations by considering input-output functions [49]. For that purpose, given any partial order $\leqslant$ on $\wp(\mathcal{D} \times \mathcal{E})$, we use the right-image isomorphism:

$$\langle \wp(\mathcal{D} \times \mathcal{E}),\ \leqslant\rangle \underset{\alpha^{\blacktriangleright}}{\overset{\gamma^{\blacktriangleright}}{\twoheadleftarrow\!\!\twoheadrightarrow}} \langle \mathcal{D} \longmapsto \wp(\mathcal{E}),\ \dot{\leqslant}\rangle$$

where:

$$\begin{array}{rcl} \alpha^{\blacktriangleright}(R) & \triangleq & R^{\blacktriangleright} = \lambda x \centerdot \{y \mid \langle x,\, y\rangle \in R\}\ , \\ \gamma^{\blacktriangleright}(f) & \triangleq & \{\langle x,\, y\rangle \mid y \in f(x)\} \quad \text{and} \\ f \mathrel{\dot{\leqslant}} g & \triangleq & \gamma^{\blacktriangleright}(f) \leqslant \gamma^{\blacktriangleright}(g)\ . \end{array}$$

8.1. Nondeterministic Denotational Semantics

Our initial goal was to derive the nondeterministic denotational semantics of [3] 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. So there exist (infinitely many) alternative powersets to the Egli-Milner and Smyth constructions. The Egli-Milner ordering is minimal while Smyth ordering is not since intuitively it is possible to find a strict subordering for computing fixpoints without changing the semantics of any program.

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^{∞}. We let:

$$\dot{\tau} \ \triangleq\ \lambda s \centerdot \{s \mid \forall s' \in \Sigma : \neg(s\ \tau\ s')\}\ .$$

By the fixpoint characterization 24 of τ^{∞} and the Kleenian fixpoint transfer theorem 3, we derive a fixpoint characterization of the fixpoint natural nondeterministic denotational semantics. We write $\dot{\mathcal{O}}$ for the pointwise extension of operator $\mathcal{O}$. For example the pointwise extension of $\cup \in (\wp(\Sigma_{\perp}) \times \wp(\Sigma_{\perp})) \longmapsto \wp(\Sigma_{\perp})$ is $\dot{\cup} \in ((\Sigma \longmapsto \wp(\Sigma_{\perp})) \times (\Sigma \longmapsto \wp(\Sigma_{\perp}))) \longmapsto (\Sigma \longmapsto \wp(\Sigma_{\perp}))$ defined as $F \mathbin{\dot{\cup}} G \triangleq \lambda s \centerdot F(s) \cup G(s)$.

Theorem 33. (Fixpoint natural nondeterministic denotational semantics). $\tau^{\natural} = \mathrm{lfp}_{\dot{\perp}^{\natural}}^{\dot{\sqsubseteq}^{\natural}} F^{\natural}$ where $\dot{D}^{\natural} \triangleq \Sigma \longmapsto \wp(\Sigma_{\perp})$, $F^{\natural} \in \dot{D}^{\natural} \xrightarrow{\mathrm{m}} \dot{D}^{\natural}$ defined as:

$$\begin{array}{rcl} F^{\natural}(f) & \triangleq & \dot{\tau} \mathbin{\dot{\cup}} \dot{\bigcup} f^{\blacktriangleright} \circ \tau^{\blacktriangleright} \\ & = & \lambda f \centerdot \lambda s \centerdot \{s \mid \forall s' \in \Sigma : \neg(s\ \tau\ s')\} \cup \{s'' \mid \exists s' \in \Sigma : s\ \tau\ s' \wedge s'' \in f(s')\} \end{array}$$

is a $\dot{\sqsubseteq}^{\natural}$-monotone map on the complete lattice $\langle \dot{D}^{\natural},\, \dot{\sqsubseteq}^{\natural},\, \dot{\perp}^{\natural},\, \dot{\top}^{\natural},\, \dot{\sqcup}^{\natural},\, \dot{\sqcap}^{\natural}\rangle$ which is the pointwise extension of the complete lattice $\langle D^{\natural},\, \sqsubseteq^{\natural},\, \perp^{\natural},\, \top^{\natural},\, \sqcup^{\natural},\, \sqcap^{\natural}\rangle$ with:

- $D^{\natural} \triangleq \wp(\Sigma_{\perp})$, $X \sqsubseteq^{\natural} Y \triangleq X^{+} \subseteq Y^{+} \wedge X^{\omega} \supseteq Y^{\omega}$,
- $X^{+} \triangleq X \cap \top^{\natural}$,
- $\top^{\natural} \triangleq \Sigma$,
- $X^{\omega} \triangleq X \cap \perp^{\natural}$ 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 24. 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 $f\ \dot\sqsubseteq^\natural\ g \triangleq \gamma^\blacktriangleright(f) \sqsubseteq^\infty \gamma^\blacktriangleright(g) = \{\langle s,\ s'\rangle \mid s' \in f(s) \cap \Sigma\} \subseteq \{\langle s,\ s'\rangle \mid s' \in g(s) \cap \Sigma\} \wedge \{\langle s,\ s'\rangle \mid s' \in f(s) \cap \{\bot\}\} \supseteq \{\langle s,\ s'\rangle \mid s' \in g(s) \cap \{\bot\}\} = \forall s \in \Sigma : f(s) \cap \Sigma \subseteq g(s) \cap \Sigma \wedge f(s) \cap \{\bot\} \supseteq g(s) \cap \{\bot\} = \forall s \in \Sigma : f(s) \sqsubseteq^\natural g(s)$ 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 $\alpha^\blacktriangleright(\bigcup_i X_i) = \dot\bigcup_i \alpha^\blacktriangleright(X_i)$, $\alpha^\blacktriangleright(\bigcap_i X_i) = \dot\bigcap_i \alpha^\blacktriangleright(X_i)$, $\alpha^\blacktriangleright(X^+) = X \mathbin{\dot\cap} \dot\top^\natural$ and $\alpha^\blacktriangleright(X^\omega) = X \mathbin{\dot\cap} \dot\bot^\natural$ whence $\alpha^\blacktriangleright(\bigsqcup^\infty_i X_i) = \alpha^\blacktriangleright(\bigcup_i {X_i}^+ \cup \bigcap_i {X_i}^\omega) = \dot\bigcup_i (\alpha^\blacktriangleright(X_i))^+ \mathbin{\dot\cup} \dot\bigcap_i (\alpha^\blacktriangleright(X_i))^\omega)$ $= \dot\bigsqcup^\natural_i \alpha^\blacktriangleright(X_i)$ pointwise, by defining $\bigsqcup^\natural_i X_i \triangleq \bigcup_i {X_i}^+ \cup \bigcap_i {X_i}^\omega$.

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

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

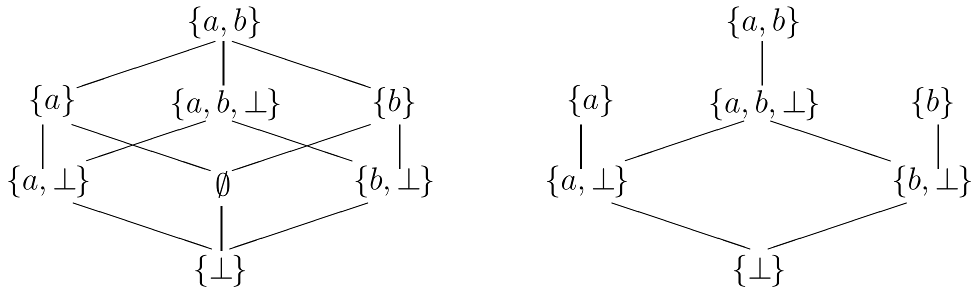
Proof. Follows from lemma 25 and the proof of theorem 33, showing by the Kleenian fixpoint transfer theorem 3 that $\forall \delta \in \mathbb{O} : {F^\natural}^\delta = \alpha^\blacktriangleright({F^\infty}^\delta)$. ☐

Lemma 35. (Totality of the iterates of $F^\natural$). Let ${F^\natural}^\delta$, $\delta \in \mathbb{O}$ be the iterates of $F^\natural$ from $\dot\bot^\natural$. $\forall \delta \in \mathbb{O} : \forall s \in \Sigma : {F^\natural}^\delta(s) \neq \emptyset$.

Proof. Follows from lemma 26 and the proof of theorem 33, showing the Kleenian fixpoint transfer theorem 3 that $\forall \delta \in \mathbb{O} : {F^\natural}^\delta = \alpha^\blacktriangleright({F^\infty}^\delta)$. ☐

Lemma 36. (Final states of the iterates of $F^\natural$). Let ${F^\natural}^\delta$, $\delta \in \mathbb{O}$ be the iterates of $F^\natural$ from $\dot\bot^\natural$. $\forall \delta \in \mathbb{O} : \forall s, s' \in \Sigma : (s' \in {F^\natural}^\delta(s) \wedge \bot \notin {F^\natural}^\delta(s)) \Longrightarrow (s' \in \check\tau \wedge {F^\natural}^\delta(s') = \{s'\})$.

Proof. Follows from lemma 27 and the proof of theorem 33, showing by the Kleenian fixpoint transfer theorem 3 that $\forall \delta \in \mathbb{O} : {F^\natural}^\delta = \alpha^\blacktriangleright({F^\infty}^\delta)$. ☐



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

Figure 2.

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 $\sqsubseteq^{\mathcal{EM}}$ [30] (see figure 2). Apart from the presence of $\emptyset$ (which can be easily eliminated), the difference is that $\sqsubseteq^{\mathcal{EM}} \subsetneq \sqsubseteq^{\natural}$ which can be useful, e.g. to define the semantics of the parallel **or** as $[\![f \textbf{ or } g]\!] \triangleq \lambda\rho\boldsymbol{\cdot}\, [\![f]\!]\,\rho \sqcup^{\natural} [\![g]\!]\,\rho$[12].

We let $(\, c_1 \;?\; v_1 \mid c_2 \;?\; v_2 \mid \ldots \;¿\; w\,)$ be v_1 if condition c_1 holds else v_2 if condition c_2 holds, etc. and w otherwise.

Let us recall [3, fact 2.4] that G. Plotkin convex powerdomain $\langle D^{\mathcal{EM}},\, \sqsubseteq^{\mathcal{EM}},\, \bot^{\mathcal{EM}},\, \sqcup^{\mathcal{EM}}\rangle$ is the DCPO $\{A \subseteq \Sigma_{\bot} \mid A \neq \emptyset\}$ with Egli-Milner ordering:

$$A \sqsubseteq^{\mathcal{EM}} B \;\;\triangleq\;\; \forall a \in A : \exists b \in B : a \sqsubseteq^{\mathcal{D}} b \wedge \forall b \in B : \exists a \in A : a \sqsubseteq^{\mathcal{D}} b$$

based upon D. Scott flat ordering $\forall x \in \Sigma_{\bot} : \bot \sqsubseteq^{\mathcal{D}} x \sqsubseteq^{\mathcal{D}} x$ such that

$$A \sqsubseteq^{\mathcal{EM}} B \iff (\, \bot \in A \;?\; A \setminus \{\bot\} \subseteq B \;¿\; A = B\,)\ ,$$

with infimum $\bot^{\mathcal{EM}} \triangleq \{\bot\}$ and lub of increasing chains $\bigsqcup^{\mathcal{EM}}_{i\in\Delta} X_i \triangleq (\bigcup_{i\in\Delta} X_i \setminus \{\bot\}) \cup \{\bot \mid \forall i \in \Delta : \bot \in X_i\}$.

Applying the fixpoint iterates reordering theorem 10 to theorem 33, we get [3]:

Corollary 37. (G. Plotkin fixpoint nondeterministic denotational semantics). $\tau^{\natural} = \operatorname{lfp}^{\dot{\sqsubseteq}^{\mathcal{EM}}}_{\dot{\bot}^{\mathcal{EM}}} F^{\natural}$ where $F^{\natural}$ (defined in theorem 33) is a $\dot{\sqsubseteq}^{\mathcal{EM}}$-monotone map on the pointwise extension $\langle \dot{D}^{\mathcal{EM}},\, \dot{\sqsubseteq}^{\mathcal{EM}},\, \dot{\bot}^{\mathcal{EM}},\, \dot{\sqcup}^{\mathcal{EM}}\rangle$ of G. Plotkin convex powerdomain $\langle D^{\mathcal{EM}},\, \sqsubseteq^{\mathcal{EM}},\, \bot^{\mathcal{EM}},\, \sqcup^{\mathcal{EM}}\rangle$.

Proof. We apply theorem 10 with $E = \dot{D}^{\mathcal{EM}} = \Sigma \longmapsto \wp(\Sigma_{\bot}) \setminus \{\lambda s\boldsymbol{\cdot}\, \emptyset\}$.

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

By lemma 35, no iterate $F^{\natural^{\delta}}$, $\delta \in \mathbb{O}$ of $F^{\natural}$ from $\dot{\bot}^{\natural}$ is $\lambda s\boldsymbol{\cdot}\, \emptyset$.

[12] Observe that $\sqcup^{\natural}$ is monotonic for $\sqsubseteq^{\natural}$ which is not in contradiction with [8] since by lemma 35 failure is excluded i.e. would have to be explicitly denoted by $\Omega \notin \Sigma$.

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

If $f \mathrel{\dot{\sqsubseteq}^{\mathcal{EM}}} g$ then $\forall s \in \Sigma : \big(\bot \in F(s)\ ?\ f(s) \setminus \{\bot\} \subseteq g(s)\ ¿\ f(s) = g(s)\big)$ so that we must show that $\forall s \in \Sigma : F^\natural(f)s \sqsubseteq^{\mathcal{EM}} F^\natural(g)s \iff \forall s \in \Sigma : \dot{\breve{\tau}}(s)\ \cup\ \bigcup f^\blacktriangleright \circ \tau^{\blacktriangleright}(s) \sqsubseteq^{\mathcal{EM}} \dot{\breve{\tau}}(s)\ \cup\ \bigcup g^\blacktriangleright \circ \tau^{\blacktriangleright}(s) \iff \forall s \in \Sigma : \big(\bot \in \bigcup\{f(s') \mid s\ \tau\ s'\}\ ?\ \bigcup\{f(s') \mid s\ \tau\ s'\} \setminus \{\bot\} \subseteq \bigcup\{g(s') \mid s\ \tau\ s'\}\ ¿\ \bigcup\{f(s') \mid s\ \tau\ s'\} = \bigcup\{g(s') \mid s\ \tau\ s'\}\big)$. 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 $F^\natural(f)s \sqsubseteq^{\mathcal{EM}} F^\natural(g)s$ 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 $F^\natural(f)s \sqsubseteq^{\mathcal{EM}} F^\natural(g)s$. It follows that $F^\natural$ hence $F^\natural|_{\dot{D}^{\mathcal{EM}}}$ is $\dot{\sqsubseteq}^{\mathcal{EM}}$-monotonic.

In order to prove that for all $g \in \dot{D}^{\mathcal{EM}}$, if λ is a limit ordinal and $\forall \delta < \lambda : F^{\natural^\delta} \mathrel{\dot{\sqsubseteq}^{\mathcal{EM}}} g$ then $\dot{\bigsqcup^\natural}_{\delta<\lambda} F^{\natural^\delta} \mathrel{\dot{\sqsubseteq}^{\mathcal{EM}}} g$, let us assume that $\forall s \in \Sigma : \forall \delta < \lambda : F^{\natural^\delta}(s) \sqsubseteq^{\mathcal{EM}} g(s)$ that is $\big(\bot \in F^{\natural^\delta}(s)\ ?\ F^{\natural^\delta}(s) \setminus \{\bot\} \subseteq g(s)\ ¿\ F^{\natural^\delta}(s) = g(s)\big)$. We have $\bigsqcup^\natural_{\delta<\lambda} F^{\natural^\delta}(s) = (\bigcup_{\delta<\lambda} F^{\natural^\delta}(s) \cap \Sigma) \cup (\bigcap_{\delta<\lambda} F^{\natural^\delta}(s) \cap \{\bot\})$

A. If $\bot \in \bigsqcup^\natural_{\delta<\lambda} F^{\natural^\delta}(s)$ 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 $F^{\natural^\delta}(s) \sqsubseteq^{\mathcal{EM}} g(s)$. Therefore $(\bigcup_{\delta<\lambda} F^{\natural^\delta}(s)) \setminus \{\bot\} \subseteq g(s)$ hence $(\bigsqcup^\natural_{\delta<\lambda} F^{\natural^\delta}(s)) \setminus \{\bot\} \subseteq g(s)$ proving $\bigsqcup^\natural_{\delta<\lambda} F^{\natural^\delta}(s) \sqsubseteq^\natural g(s)$.

B. If $\bot \notin \bigsqcup^\natural_{\delta<\lambda} F^{\natural^\delta}(s)$ 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 $\bigcup_{\delta \leq \eta} F^{\natural^\delta}(s) \cap \Sigma = g(s)$. 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 25 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 $\bigcup_{\delta<\lambda} F^{\natural^\delta}(s) \cap \Sigma = g(s)$ whence $\bigsqcup_{\delta<\lambda} F^{\natural^\delta}(s) \sqsubseteq^{\mathcal{EM}} g(s)$.

By theorems 33 and 10, we conclude that $\tau^\natural = \mathrm{lfp}^{\dot{\sqsubseteq}^\natural}_{\dot{\bot}^\natural} F^\natural = \mathrm{lfp}^{\dot{\sqsubseteq}^{\mathcal{EM}}}_{\dot{\bot}^{\mathcal{EM}}} F^\natural$. $\square$

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 abstraction

$$\alpha^\sharp(f) \ \triangleq\ \lambda s \cdot f(s) \cup \{s' \in \Sigma \mid \bot \in f(s)\}\ ,$$
$$\gamma^\sharp(g) \ \triangleq\ g$$

satisfying

$$\langle \Sigma \longmapsto \wp(\Sigma_\bot),\ \dot{\subseteq} \rangle \xleftarrow[\alpha^\sharp]{\gamma^\sharp} \langle \Sigma \longmapsto (\wp(\Sigma) \cup \{\Sigma_\bot\}),\ \dot{\subseteq} \rangle\ .$$

Proof. $\alpha^\sharp(f) \mathrel{\dot{\subseteq}} g \iff \forall s \in \Sigma : f(s) \cup \{s' \in \Sigma \mid \bot \in f(s)\} \subseteq g(s) \implies \forall s \in \Sigma : f(s) \subseteq g(s) \iff f \mathrel{\dot{\subseteq}} \gamma^\sharp(g)$. 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 $\langle \Sigma \longmapsto \wp(\Sigma_\bot), \dot{\subseteq}\rangle \xrightleftharpoons[\alpha^\sharp]{\gamma^\sharp} \langle \Sigma \longmapsto (\wp(\Sigma) \cup \{\Sigma_\bot\}), \dot{\subseteq}\rangle$. $\square$

The demoniac abstraction $\alpha^\sharp$ introduces any potential finite behavior for all initial states for which nontermination is possible (so that it it impossible to conclude anything on the finite behaviors when nontermination is possible).

Theorem 38. (Denotational demoniac abstraction). $\tau^\sharp = \alpha^\sharp(\tau^\natural)$.

Proof. 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 $\tau^\sharp \triangleq \alpha^\blacktriangleright(\tau^\partial) = \alpha^\blacktriangleright \circ \alpha^\partial(\tau^\infty) = \alpha^\sharp \circ \alpha^\blacktriangleright(\tau^\infty) = \alpha^\sharp(\tau^\natural)$. $\square$

Let us recall the properties of lifting:

Lemma 39. (Lifting). Given a complete lattice $\langle D,\, \sqsubseteq, \bot, \top, \sqcup,\, \sqcap\rangle$ (respectively a poset $\langle D,\, \sqsubseteq,\, \sqcup\rangle$, a DCPO $\langle D,\, \sqsubseteq, \bot,\, \sqcup\rangle$), the *lift of D by $\pm \notin D$* is the complete lattice (resp. poset, DCPO) $\langle D_\pm,\, \preceq, \pm, \top, \coprod,\, \prod\rangle$ with:

- $D_\pm \triangleq D \cup \{\pm\}$,
- partial order $x \preceq y \triangleq (x = \pm) \vee (y \in D \wedge x \sqsubseteq y)$,
- infimum $\pm$,
- supremum $\top$,
- join $\coprod\limits_{i \in \Delta} X_i \triangleq \big(\forall i \in \Delta : X_i = \pm \mathrel{?} \pm \mathrel{¿} \sqcup\{X_i \mid i \in \Delta \wedge X_i \neq \pm\}\big)$
- and meet $\prod\limits_{i \in \Delta} X_i \triangleq \big(\exists i \in \Delta : X_i = \pm \mathrel{?} \pm \mathrel{¿} \sqcap\{X_i \mid i \in \Delta \wedge X_i \neq \pm\}\big)$.

By the fixpoint characterization 28 of τ^∂ and the Kleenian fixpoint transfer theorem 3, we get:

Theorem 40. (Fixpoint demoniac nondeterministic denotational semantics). $\tau^\sharp = \operatorname{lfp}^{\dot{\sqsubseteq}^\sharp}_{\dot{\bot}^\sharp} F^\sharp$ where $F^\sharp(f) \triangleq \dot{\tau} \mathrel{\dot{\cup}} \dot{\bigcup} f^\blacktriangleright \circ \tau^{\blacktriangleright}$ 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 28. 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 $f \mathrel{\dot{\sqsubseteq}^\sharp} g \triangleq \gamma^\blacktriangleright(f) \sqsubseteq^\partial \gamma^\blacktriangleright(g) = \forall s \in \Sigma : \langle s,\, \bot\rangle \in \gamma^\blacktriangleright(f) \vee (\langle s,\, \bot\rangle \notin \gamma^\blacktriangleright(g) \wedge \gamma^\blacktriangleright(f) \cap (\{s\} \times \Sigma) \subseteq \gamma^\blacktriangleright(g) \cap (\{s\} \times \Sigma)) =$

$\forall s \in \Sigma : \bot \in f(s) \vee (\bot \notin g(s) \wedge f(s) \subseteq g(s)) = \forall s \in \Sigma : f(s) \sqsubseteq^\sharp g(s)$ by defining $X \sqsubseteq^\sharp Y \triangleq \bot \in X \vee (\bot \notin Y \wedge X \subseteq Y)$, pointwise.

Consequently, by lemma 39, $\langle D^\sharp, \sqsubseteq^\sharp, \bot^\sharp, \top^\sharp, \sqcup^\sharp, \sqcap^\sharp\rangle$ 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 $\bot^\sharp \triangleq \Sigma_\bot$ and the supremum is $\dot{\top}^\sharp \triangleq \lambda s \bullet \top^\sharp$ where $\top^\sharp \triangleq \Sigma$.

The lub $\bigsqcup^\sharp_{i\in\Delta} X_i = \big(\forall i \in \Delta : X_i = \Sigma_\bot \ ?\ \Sigma_\bot \ ¿\ \cup\{X_i \mid i \in \Delta : \wedge X_i \neq \Sigma_\bot\}\big)$ 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 39, the glb is $\bigsqcap^\sharp_{i\in\Delta} X_i \triangleq \big(\exists i \in \Delta : X_i = \Sigma_\bot \ ?\ \Sigma_\bot \ ¿\ \cap\{X_i \mid i \in \Delta : \wedge X_i \neq \Sigma_\bot\}\big)$.

The design of the semantic transformer $F^\sharp$ is identical to that of $F^\natural$ in the proof of theorem 33.

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

Lemma 41. (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 29 and the proof of theorem 40, showing by the Kleenian fixpoint transfer theorem 3 that $\forall \beta \in \mathbb{O} : F^{\sharp^\beta} = \alpha^\blacktriangleright(F^{\partial^\beta})$. $\square$

Lemma 42. (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 30 and the proof of theorem 40, showing by the Kleenian fixpoint transfer theorem 3 that $\forall \beta \in \mathbb{O} : F^{\sharp^\beta} = \alpha^\blacktriangleright(F^{\partial^\beta})$. $\square$

Lemma 43. (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 31 and the proof of theorem 40, showing by the Kleenian fixpoint transfer theorem 3 that $\forall \beta \in \mathbb{O} : F^{\sharp^\beta} = \alpha^\blacktriangleright(F^{\partial^\beta})$. $\square$

From theorem 40, lemma 42 and the fixpoint iterates reordering theorem 10, we deduce another fixpoint characterization of $F^\sharp(f)$ with a different partial ordering:

Corollary 44. (Reordered fixpoint demoniac nondeterministic denotational semantics). $\tau^\sharp = \operatorname{lfp}^{\dot{\sqsubseteq}^\diamond}_{\dot{\bot}^\diamond} F^\sharp$ where $F^\sharp(f) \triangleq \dot{\check{\tau}} \ \dot{\cup} \ \dot{\bigcup} f^\blacktriangleright \circ \tau^{\bullet\!\blacktriangleright}$ 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 $X \sqsubseteq^\diamond Y \triangleq (X = \bot^\diamond) \vee (X \subseteq Y)$.

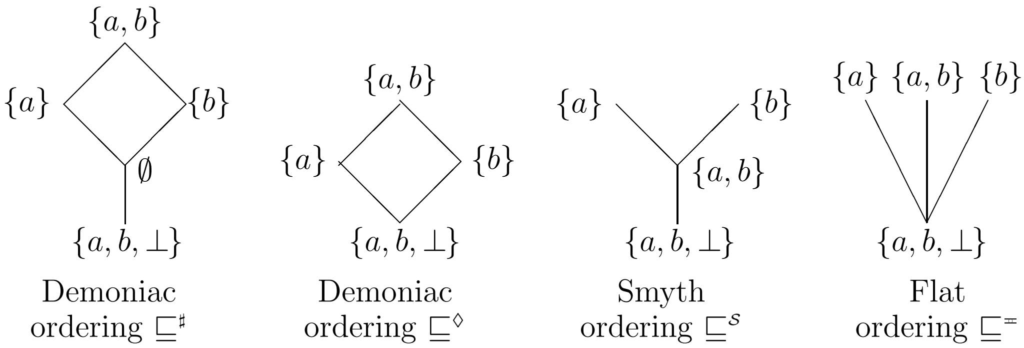


Figure 3.

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 [30] $\sqsubseteq^{\mathcal{S}}$ (see figure 3).

Let us recall [3, fact 2.7] that M. Smyth upper powerdomain $\langle D^{\mathcal{S}},\ \sqsubseteq^{\mathcal{S}}, \bot^{\mathcal{S}}, \sqcap^{\mathcal{S}},\ \sqcup^{\mathcal{S}}\rangle$ is $D^{\mathcal{S}} \triangleq \{A \subseteq \Sigma \mid A \neq \emptyset\} \cup \{\Sigma_\bot\}$ ordered by the superset ordering $A \sqsubseteq^{\mathcal{S}} B \triangleq A \supseteq B$ which is a poset with infimum $\bot^{\mathcal{S}} \triangleq \Sigma_\bot$, the glb of nonempty families X_i, $i \in \Delta$ always exist being given by $\underset{i\in\Delta}{\sqcap^{\mathcal{S}}} X_i \triangleq \bigcup_{i\in\Delta} X_i$ and if X_i, $i \in \Delta$ has an upper bound, its lub exists and is $\underset{i\in\Delta}{\sqcup^{\mathcal{S}}} X_i \triangleq \bigcap_{i\in\Delta} X_i$.

By applying the fixpoint iterates reordering theorem 10 to the fixpoint definition of $\tau^\sharp$ provided by theorem 40, we get [3]:

Corollary 45. (M. Smyth fixpoint nondeterministic denotational semantics). $\tau^\sharp = \mathrm{lfp}^{\dot{\sqsubseteq}^{\mathcal{S}}}_{\dot{\bot}^{\mathcal{S}}}\ F^\sharp$ where $F^\sharp$ is a $\dot{\sqsubseteq}^{\mathcal{S}}$-monotone map on the pointwise extension $\langle \dot{D}^{\mathcal{S}},\ \dot{\sqsubseteq}^{\mathcal{S}},\ \dot{\bot}^{\mathcal{S}},\ \dot{\sqcap}^{\mathcal{S}},\ \dot{\sqcup}^{\mathcal{S}}\rangle$ of M. Smyth upper powerdomain $\langle D^{\mathcal{S}},\ \sqsubseteq^{\mathcal{S}}, \bot^{\mathcal{S}}, \sqcap^{\mathcal{S}},\ \sqcup^{\mathcal{S}}\rangle$.

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

By lemma 42, all iterates $F^{\sharp^\delta}$, $\delta \in \mathbb{O}$ of $F^\sharp$ from $\dot{\bot}^\sharp$ belong to $D^{\mathcal{S}} = D^\sharp \setminus \{\lambda s \centerdot \emptyset\}$.

If $f \ \dot{\sqsubseteq}^{\mathcal{S}}\ g$ then $\forall s \in \Sigma : f(s) \sqsubseteq^{\mathcal{S}} g(s)$ 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 $F^\sharp(f)\ \dot{\sqsubseteq}^{\mathcal{S}}\ F^\sharp(g)$ proving that $F^\sharp$ hence $F^\sharp|_{\dot{D}^{\mathcal{S}}}$ is $\dot{\sqsubseteq}^{\mathcal{S}}$-monotone.

Assume that $f \in \dot{D}^{\mathcal{S}}$, λ is a limit ordinal and $\forall \delta < \lambda : F^{\sharp^\delta}\ \dot{\sqsubseteq}^{\mathcal{S}}\ f$, that is $\forall \delta < \lambda : \forall s \in \Sigma : F^{\sharp^\delta}(s) \supseteq f(s)$. It follows that $\bigcap_{\delta<\lambda} F^{\sharp^\delta}(s) \supseteq f(s)$ proving that $\big(\forall \delta < \lambda : F^{\sharp^\delta}(s) = \Sigma_\bot\ ?\ \Sigma_\bot$ ¿ $\bigcap_{\delta<\lambda} F^{\sharp^\delta}(s)\big) \supseteq f(s)$ that is $\underset{\delta<\lambda}{\dot{\sqcup}^\sharp} F^{\sharp^\delta}\ \dot{\sqsubseteq}^{\mathcal{S}}\ f$.

By theorems 40 and 10, we conclude that $\tau^\sharp = \mathrm{lfp}^{\dot{\sqsubseteq}^\sharp}_{\dot{\bot}^\sharp}\ F^\sharp = \mathrm{lfp}^{\dot{\sqsubseteq}^{\mathcal{S}}}_{\dot{\bot}^{\mathcal{S}}}\ F^\sharp$. $\square$

8.1.5. Minimal Demoniac Nondeterministic Denotational Semantics

M. Smyth ordering $\dot{\sqsubseteq}^{\mathcal{S}}$ is not *minimal* since, for example on figure 3, $\{a\}$ and $\{a, b\}$ need not be comparable by lemma 29. Intuitively the minimal ordering is designed to compare only elements of the powerdomain which can appear along the fixpoint iterates for some program as described by the arrangement of the iterates specified in lemma 29. This minimal ordering called the flat ordering leads to the same fixpoints as shown by the fixpoint iterates reordering considered in section 2.6.

Theorem 46. (Flat powerdomain fixpoint nondeterministic denotational semantics). $\tau^\sharp = \mathrm{lfp}^{\dot{\sqsubseteq}^=}_{\dot{\bot}^=} F^\sharp$ where $F^\sharp$ is a $\dot{\sqsubseteq}^=$-monotone map on the DCPO $\langle \dot{D}^=,\ \dot{\sqsubseteq}^=, \dot{\bot}^=, \dot{\sqcup}^= \rangle$ which is the restriction of the pointwise extension of the flat DCPO $\langle D^=,\ \sqsubseteq^=, \bot^=, \sqcup^= \rangle$. with $D^= \triangleq (\wp(\Sigma) \setminus \{\emptyset\}) \cup \{\bot^=\}$ and infimum $\bot^= \triangleq \Sigma_\bot$ to $\dot{D}^= \triangleq \{f \in \Sigma \longmapsto D^= \mid \forall s, s' \in \Sigma : (s' \in f(s) \wedge f(s) \neq \bot^=) \Longrightarrow (s' \in \check{\tau} \wedge f(s') = \{s'\})$.

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

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

All iterates $F^{\sharp^\delta}$, $\delta \in \mathbb{O}$ of $F^\sharp(f) \triangleq \dot{\check{\tau}} \mathbin{\dot{\cup}} \bigcup f^\blacktriangleright \circ \tau^{\blacktriangleright}$ from $\dot{\bot}^{\mathcal{S}} = \lambda s \bullet \Sigma_\bot = \dot{\bot}^=$ satisfy $F^{\sharp^\delta} \neq \lambda s \bullet \emptyset$ by lemma 42 and $\forall s, s' \in \Sigma : (s' \in F^{\sharp^\delta}(s) \wedge F^{\sharp^\delta}(s) \neq \bot^=) \Longrightarrow s' \in (s' \in \check{\tau} \wedge f(s') = \{s'\})$ by lemma 43, hence belong to $\dot{D}^=$.

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

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

Assume that $f \in \dot{D}^=$, λ is a limit ordinal and $\forall \delta < \lambda : F^{\sharp^\delta} \mathrel{\dot{\sqsubseteq}^=} f$, 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 $\bigcap_{\delta<\lambda} F^{\sharp^\delta}(s) = \Sigma_\bot$ or $\bigcap_{\delta<\lambda} F^{\sharp^\delta}(s) = f(s)$ proving that $\dot{\bigsqcup}^{\mathcal{S}}_{\delta<\lambda} F^{\sharp^\delta} \mathrel{\dot{\sqsubseteq}^=} f$.

By theorems 45 and 10, we conclude that $\tau^\sharp = \mathrm{lfp}^{\dot{\sqsubseteq}^{\mathcal{S}}}_{\dot{\bot}^{\mathcal{S}}} F^\sharp = \mathrm{lfp}^{\dot{\sqsubseteq}^=}_{\dot{\bot}^=} F^\sharp$. $\square$

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

Theorem 47. (Minimality of $\langle \dot{D}^=,\ \dot{\sqsubseteq}^= \rangle$). Let $\langle E,\ \preccurlyeq \rangle$ be any poset such that $\dot{\bot}^=$ is the $\preccurlyeq$-infimum of E, $F^\sharp[\![\tau]\!] \triangleq \lambda f \bullet \dot{\check{\tau}} \mathbin{\dot{\cup}} \bigcup f^\blacktriangleright \circ \tau^\blacktriangleright \in E \stackrel{\mathrm{m}}{\longmapsto} E$ is $\preccurlyeq$-monotone and $\forall \tau : \tau^\sharp = \mathrm{lfp}^{\preccurlyeq}_{\dot{\bot}^=} F^\sharp[\![\tau]\!]$ then $\dot{D}^= \subseteq E$ and $\dot{\sqsubseteq}^= \subseteq \preccurlyeq$.

Proof. Assume, by reductio ad absurdum, that $\exists f \in \dot{D}^= : f \notin E$. We write $F^\sharp[\![\tau]\!]$ 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 $F^{\natural^\delta}, \delta \in \mathbb{O}$ of $F^\natural[\![\tau]\!]$ are as follows:

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

$F^{\natural^1} = F^\natural[\![\tau]\!](F^{\natural^0}) = \lambda s \bullet \dot{\check{\tau}}(s) \ \cup\ \bigcup\{F^{\natural^0}(s') \mid s\ \tau\ s'\} = \lambda s \bullet \{s \mid f(s) = \{s\}\} \ \cup\ \big(\bot \in f(s) \vee (f(s) \neq \{s\})\ ?\ \Sigma_\bot\ ¿\ \emptyset\big) = \lambda s \bullet \{s \mid f(s) = \{s\}\} \ \cup\ \big(\bot \in f(s)\ ?\ \Sigma_\bot\ ¿\ \emptyset\big) \ \cup\ \big((f(s) \neq \{s\})\ ?\ \Sigma_\bot\ ¿\ \emptyset\big)$.

$F^{\natural^2} = F^\natural[\![\tau]\!](F^{\natural^1}) = \lambda s \bullet \{s \mid f(s) = \{s\}\} \cup A \cup B$ where:

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

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

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

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 $F^\natural[\![\tau]\!]$ from $\dot{\bot}^{=}$. Since the iterates are $\preccurlyeq$-increasing, we must have $\dot{\bot}^{=} \preccurlyeq f$ proving that $\dot{\sqsubseteq}^{=} \subseteq \preccurlyeq$. $\square$

Reciprocally, we have:

Theorem 48. (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 $F^\natural \triangleq \lambda f \bullet \dot{\check{\tau}} \ \dot{\cup}\ \dot{\bigcup} f^\blacktriangleright \circ \tau^\blacktriangleright \in E \overset{\text{m}}{\longmapsto} E$ is $\preccurlyeq$-monotonic. Then $\tau^\natural = \text{lfp}^{\preccurlyeq}_{\dot{\bot}^{=}} F^\natural$.

Proof. By the proof of theorem 46, we know that all iterates $F^{\natural^\delta}$, $\delta \in \mathbb{O}$ of $F^\natural$ are in $\dot{D}^{=}$. Let ϵ be the iteration order so that $F^{\natural^\epsilon} = \text{lfp}^{\dot{\sqsubseteq}^{=}}_{\dot{\bot}^{=}} F^\natural$. Let $f \in E$ be any fixpoint of $F^\natural$. We have $F^{\natural^0} = \dot{\bot}^{=} \preccurlyeq f$ since $\dot{\bot}^{=}$ is the $\preccurlyeq$-infimum of E. If $F^{\natural^\delta} \preccurlyeq f$ then $F^{\natural^{\delta+1}} = F^\natural(F^{\natural^\delta})$ $\preccurlyeq F^\natural(f) = f$ since $F^\natural$ is $\preccurlyeq$-monotonic. If λ is a limit ordinal then $F^{\natural^\delta}$, $\delta < \lambda$ is a $\dot{\sqsubseteq}^{=}$-increasing chain so that its $\preccurlyeq$-lub is $\dot{\bigsqcup}^{=}_{\delta<\lambda} F^{\natural^\delta} = F^{\natural^\lambda}$ whence $F^{\natural^\lambda} \preccurlyeq f$ since $\forall \delta < \lambda : F^{\natural^\delta} \preccurlyeq f$

by induction hypothesis. By transfinite induction, $\forall \delta \in \mathbb{O} : F^{\sharp^{\delta}} \preccurlyeq f$ proving that $F^{\sharp^{\epsilon}} = \mathrm{lfp}^{\preccurlyeq}_{\dot{\bot}^{\boxminus}} F^{\sharp}$. By theorem 46, $\tau^{\sharp} = \mathrm{lfp}^{\dot{\sqsubseteq}^{\boxminus}}_{\dot{\bot}^{\boxminus}} F^{\sharp} = \mathrm{lfp}^{\preccurlyeq}_{\dot{\bot}^{\boxminus}} F^{\sharp}$. $\square$

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

The *angelic nondeterministic denotational semantics* is the right-image abstraction

$$\tau^{\flat} \quad \triangleq \quad \alpha^{\blacktriangleright}(\tau^{+})$$

of the finite/angelic relational semantics τ^{+}. We also have $\tau^{\flat} = \alpha^{\Sigma}(\tau^{\natural})$ where $\alpha^{\Sigma}(f) = \lambda s \centerdot f(s) \cap \Sigma$.

By theorem 17 and the Kleenian fixpoint transfer theorem 3, we get:

Corollary 49. (C.A.R. Hoare fixpoint nondeterministic denotational semantics). $\tau^{\flat} = \mathrm{lfp}^{\dot{\subseteq}}_{\dot{\emptyset}} F^{\flat}$ where $F^{\flat} = \lambda f \centerdot \dot{\check{\tau}} \ \dot{\cup} \ \dot{\bigcup} f^{\blacktriangleright} \circ \tau^{\bullet\!\blacktriangleright}$ is a complete $\dot{\cup}$-morphism on the complete lattice $\langle \Sigma \longmapsto \wp(\Sigma),\ \dot{\subseteq}, \dot{\emptyset}, \lambda s \centerdot \Sigma, \dot{\cup}, \dot{\cap} \rangle$ which is the pointwise extension of the powerset $\langle \wp(\Sigma),\ \subseteq \rangle$.

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 17 that is the pointwise extension of the powerset $\langle \wp(\Sigma),\ \subseteq \rangle$.

We have $\alpha^{\blacktriangleright}(\dot{\bigcup}_{i \in \Delta} X_i) = \lambda s \centerdot \{s' \mid \langle s,\ s' \rangle \in \bigcup_{i \in \Delta} X_i)\} = \dot{\bigcup}_{i \in \Delta} \lambda s \centerdot \{s' \mid \langle s,\ s' \rangle \in X_i)\} = \dot{\bigcup}_{i \in \Delta} \alpha^{\blacktriangleright}(X_i)$ 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 33.

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

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

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 [30].

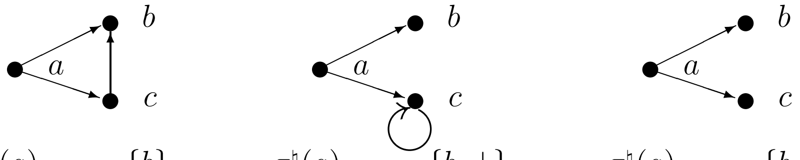
8.2. Deterministic Denotational Semantics

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

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 $|X \setminus \{\bot\}| > 1$.



$$\begin{array}{lcl} \tau^\natural(a) &=& \{b\} \\ \tau^\top(a) &=& b \\ \tau^\top(b) &=& b \\ \tau^\top(c) &=& b \end{array} \qquad \begin{array}{lcl} \tau^\natural(a) &=& \{b,\bot\} \\ \tau^\top(a) &=& b \\ \tau^\top(b) &=& b \\ \tau^\top(c) &=& \bot \end{array} \qquad \begin{array}{lcl} \tau^\natural(a) &=& \{b,c\} \\ \tau^\top(a) &=& \top \\ \tau^\top(b) &=& b \\ \tau^\top(c) &=& c \end{array}$$

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

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 $\dot{\alpha}^\top \triangleq \lambda s \bullet \alpha^\top(f(s))$ pointwise so that:

$$\tau^\top \quad \triangleq \quad \dot{\alpha}^\top(\tau^\natural)\ .$$

By theorem 33 and the Kleenian fixpoint transfer theorem 3, we get:

Theorem 50. (D. Scott fixpoint deterministic denotational semantics (complete lattices and continuous functions)). $\tau^\top = \mathrm{lfp}_{\dot{\bot}}^{\dot{\sqsubseteq}^\top} F^\top$ where $F^\top \in (\Sigma \longmapsto \Sigma_\bot^\top) \longmapsto (\Sigma \longmapsto \Sigma_\bot^\top)$ defined as $F^\top(f) \triangleq \lambda s \bullet \big(\forall s' \in \Sigma : \neg(s\ \tau\ s')\ ?\ s\ \text{¿}\ \sqcup^\top\{f(s') \mid s\ \tau\ s'\}\big)$ 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. $\alpha^\top(X) \sqsubseteq^\top \zeta \iff X \subseteq \gamma^\top(\zeta)$ 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 $F^\top$. $\dot{\alpha}^\top \circ F^\natural(f) = \dot{\alpha}^\top(\dot{\check{\tau}} \,\dot{\cup}\, \dot{\bigcup} f^\blacktriangleright \circ \tau^{\bullet\!\blacktriangleright}) = \lambda s \centerdot \alpha^\top(\dot{\check{\tau}}(s) \cup \bigcup f^\blacktriangleright \circ \tau^{\bullet\!\blacktriangleright}(s)) = \lambda s \centerdot \alpha^\top(\{s \mid \forall s' \in \Sigma : \neg(s\ \tau\ s')\} \cup \bigcup\{f(s') \mid s\ \tau\ s'\}) = \lambda s \centerdot \big(\forall s' \in \Sigma : \neg(s\ \tau\ s') \ ?\ \alpha^\top(\{s\}) \ ¿\ \alpha^\top(\bigcup\{f(s') \mid s\ \tau\ s'\})\big) = \lambda s \centerdot \big(\forall s' \in \Sigma : \neg(s\ \tau\ s') \ ?\ s \ ¿\ \sqcup^\top\{\alpha^\top(f(s')) \mid s\ \tau\ s'\}\big) = \lambda s \centerdot \big(\forall s' \in \Sigma : \neg(s\ \tau\ s') \ ?\ s \ ¿\ \sqcup^\top\{\dot{\alpha}^\top(f)(s') \mid s\ \tau\ s'\}\big) = \lambda s \centerdot F^\top \circ \dot{\alpha}^\top(f)$ by definition of $\dot{\alpha}^\top$ and $\alpha^\top$ which is a complete $\sqcup^\top$-complete morphism and by defining $F^\top \triangleq \lambda f \centerdot \lambda s \centerdot \big(\forall s' \in \Sigma : \neg(s\ \tau\ s') \ ?\ s \ ¿\ \sqcup^\top\{f(s') \mid s\ \tau\ s'\}\big)$.

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

Observe that we have got a complete lattice as in the original work of D. Scott [50] 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 51. (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 $s \in \Sigma$, $F^{\top\delta+1}(s) = F^\top(F^{\top\delta})(s) = \big(\forall s' \in \Sigma : \neg(s\ \tau\ s') \ ?\ s \ ¿\ \sqcup^\top\{F^{\top\delta}(s') \mid s\ \tau\ s'\}\big)$. 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 $\tau^{\mathcal{D}} = \tau^\top \cap (\Sigma \longmapsto \Sigma_\perp)$. By the fixpoint iterates reordering theorem 10 and theorem 50, we infer:

Theorem 52. (D. Scott fixpoint deterministic denotational semantics (CPOs and continuous functions)). $\tau^{\mathcal{D}} = \mathrm{lfp}_{\dot\perp}^{\dot\sqsubseteq^{\mathcal{D}}} F^{\mathcal{D}}$ where $F^{\mathcal{D}} \in (\Sigma \longmapsto \Sigma_\perp) \longmapsto (\Sigma \longmapsto \Sigma_\perp)$ defined as $F^{\mathcal{D}}(f) \triangleq \lambda s \bullet (\, s \;\tau\; s' \;?\; f(s') \;¿\; s\,)$ is a Scott-continuous map on the DCPO $\langle \Sigma \longmapsto \Sigma_\perp,\ \dot\sqsubseteq^{\mathcal{D}},\ \dot\perp,\ \dot\sqcup^{\mathcal{D}}\rangle$ which is the pointwise extension of DCPO $\langle \Sigma_\perp,\ \sqsubseteq^{\mathcal{D}},\ \perp,\ \sqcup^{\mathcal{D}}\rangle$ where the Scott-ordering $\sqsubseteq^{\mathcal{D}}$ is such that $\forall \zeta \in \Sigma_\perp : \perp \sqsubseteq^{\mathcal{D}} \zeta \sqsubseteq^{\mathcal{D}} \zeta$.

Proof. $\dot\sqsubseteq^{\mathcal{D}}$ is a partial order on $\Sigma \longmapsto \Sigma_\perp$ with infimum $\dot\perp^{\top} = \lambda s \bullet \perp$.

By lemma 51, all iterates of $F^{\top}$ belong to $\Sigma_\perp$.

We have $F^{\top}|_{\Sigma \longmapsto \Sigma_\perp} = \lambda f \in \Sigma \longmapsto \Sigma_\perp \bullet \lambda s \bullet F^{\top}(f)s = \lambda f \in \Sigma \longmapsto \Sigma_\perp \bullet \lambda s \bullet (\forall s' \in \Sigma : \neg(s \;\tau\; s') \;?\; s \;¿\; \sqcup^{\top}\{f(s') \mid s \;\tau\; s'\}\,) = \lambda f \in \Sigma \longmapsto \Sigma_\perp \bullet \lambda s \in \Sigma_\perp \bullet (\, s \;\tau\; s' \;?\; f(s') \;¿\; s\,) \triangleq F^{\mathcal{D}}$ since τ is locally deterministic so that s' is unique.

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

In conclusion $\tau^{\mathcal{D}} = \tau^{\top} \cap (\Sigma \longmapsto \Sigma_\perp) = \mathrm{lfp}_{\dot\perp}^{\dot\sqsubseteq^{\top}} F^{\top} = \mathrm{lfp}_{\dot\perp}^{\dot\sqsubseteq^{\top}} F^{\top}|_{\Sigma \longmapsto \Sigma_\perp} = \mathrm{lfp}_{\dot\perp}^{\dot\sqsubseteq^{\mathcal{D}}} F^{\mathcal{D}}$. □

9. Predicate Transformer Semantics

A *predicate* is a set of states that may be augmented by $\perp$ to denote nontermination. A *predicate transformer* maps predicates to predicates. So a predicate transformer is a mapping Φ of the form $\Phi \in \wp(D) \longmapsto \wp(E)$. Predicate transformer semantics [24–26,31] usually define the semantics of programs as a *backward predicate transformers* mapping a predicate called the *postcondition* to a predicate called the *precondition*. Symmetrically, this is formally equivalent to *forward predicate transformers* mapping a precondition to a postcondition. The fixpoint characterization of predicate transformer semantics is derived from that of the denotational semantics considered in section 8 by establishing Galois connection based correspondences between denotational and predicate transformers semantics. These Galois connection based correspondences imply the usual healthiness conditions postulated on predicate transformers [24–26,31] (that is *conjunctivitis* and *excluded miracle*).

9.1. Correspondences Between Denotational and Predicate Transformers Semantics

Following [16], various correspondences between denotational and predicate transformer semantics can be established using the following maps which, being Galois isomorphisms, are intuitively understood thanks to their given functionality (D, E are sets):

– Inversion: $\langle D \longmapsto \wp(E),\ \dot\subseteq\rangle \underset{\alpha^{-1}}{\overset{\gamma^{-1}}{\leftrightarrows}} \langle E \longmapsto \wp(D),\ \dot\subseteq\rangle$ where

$$\alpha^{-1} \triangleq \lambda f \bullet \lambda s' \bullet \{s \mid s' \in f(s)\},$$
$$\gamma^{-1} \triangleq \lambda f \bullet \lambda s \bullet \{s' \mid s \in f(s')\}\ .$$

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 $\langle D \longmapsto \wp(E),\, \dot{\subseteq}\rangle \xrightleftharpoons[\alpha^{-1}]{\gamma^{-1}} \langle E \longmapsto \wp(D),\, \dot{\subseteq}\rangle$. $\square$

– Existential postimage: $\langle D \longmapsto \wp(E),\, \dot{\subseteq}\rangle \xrightleftharpoons[\alpha^{\triangleright}]{\gamma^{\triangleright}} \langle \wp(D) \overset{\cup}{\longmapsto} \wp(E),\, \dot{\subseteq}\rangle$ where

$$\begin{aligned}
\alpha^{\triangleright} &\triangleq \lambda f \centerdot \lambda P \centerdot \{s' \mid \exists s \in P : s' \in f(s)\},\\
\gamma^{\triangleright} &\triangleq \lambda \Psi \centerdot \lambda s \centerdot \Psi(\{s\}) \;.
\end{aligned}$$

Proof. 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 $\forall P \subseteq D : f \dot{\subseteq} \lambda s \centerdot \{s' \mid s \in P \Longrightarrow s' \in \Psi(P)\}$. It follows for $P = \{s\}$ that $f \dot{\subseteq} \lambda s \centerdot \{s' \mid s' \in \Psi(\{s\})\}$ 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 $\langle D \longmapsto \wp(E),\, \dot{\subseteq}\rangle \xrightleftharpoons[\alpha^{\triangleright}]{\gamma^{\triangleright}} \langle \wp(D) \overset{\cup}{\longmapsto} \wp(E),\, \dot{\subseteq}\rangle$. $\square$

– Join preserving map inversion: $\langle \wp(D) \overset{\cup}{\longmapsto} \wp(E),\, \dot{\subseteq}\rangle \xrightleftharpoons[\alpha^{\cup}]{\gamma^{\cup}} \langle \wp(E) \overset{\cup}{\longmapsto} \wp(D),\, \dot{\subseteq}\rangle$ where

$$\begin{aligned}
\alpha^{\cup} &\triangleq \lambda \Psi \centerdot \lambda Q \centerdot \{s \mid \Psi(\{s\}) \cap Q \neq \emptyset\},\\
\gamma^{\cup} &\triangleq \lambda \Psi \centerdot \lambda P \centerdot \{s' \mid \Psi(\{s'\}) \cap P \neq \emptyset\} \;.
\end{aligned}$$

Proof. We have $\alpha^{\cup} \triangleq \alpha^{\triangleright} \circ \alpha^{-1} \circ \gamma^{\triangleright} = \lambda \Psi \centerdot \lambda Q \centerdot \{s \mid \exists s' \in Q : s \in \alpha^{-1} \circ \gamma^{\triangleright}(\Psi)s'\} = \lambda \Psi \centerdot \lambda Q \centerdot \{s \mid \exists s' \in Q : s' \in \gamma^{\triangleright}(\Psi)s\} = \lambda \Psi \centerdot \lambda Q \centerdot \{s \mid \exists s' \in Q : s' \in \Psi(\{s\})\} = \lambda \Psi \centerdot \lambda Q \centerdot \{s \mid \Psi(\{s\}) \cap Q \neq \emptyset\}$. Similarly $\gamma^{\cup} = \lambda \Psi \centerdot \lambda P \centerdot \{s' \mid \Psi(\{s'\}) \cap R \neq \emptyset\}$. By composition $\langle \wp(D) \overset{\cup}{\longmapsto} \wp(E),\, \dot{\subseteq}\rangle \xrightleftharpoons[\alpha^{\cup}]{\gamma^{\cup}} \langle \wp(E) \overset{\cup}{\longmapsto} \wp(D),\, \dot{\subseteq}\rangle$. $\square$

– Dual: $\langle \wp(D) \overset{\cup}{\longmapsto} \wp(E),\, \dot{\subseteq}\rangle \xrightleftharpoons[\alpha^{\sim}]{\gamma^{\sim}} \langle \wp(D) \overset{\cap}{\longmapsto} \wp(E),\, \dot{\supseteq}\rangle$ where

$$\begin{aligned}
\alpha^{\sim} &\triangleq \lambda \Psi \centerdot \lambda P \centerdot \neg(\Psi(\neg P)),\\
\gamma^{\sim} &\triangleq \lambda \Psi \centerdot \lambda P \centerdot \neg(\Psi(\neg P)) \;.
\end{aligned}$$

Proof. By definition of $\alpha^{\sim}$ and $\neg$, 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 $\alpha^{\sim}(\Psi) \mathrel{\dot{\subseteq}} \Phi \iff \forall P : \neg\Psi(\neg P) \subseteq \Phi(P) \iff \forall P : \neg\Phi(P) \subseteq \Psi(\neg P) \iff$ $\forall Q : \neg\Phi(\neg Q) \subseteq \Psi(Q) \iff \Psi \mathrel{\dot{\supseteq}} \gamma^{\sim}(\Phi)$ 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 $\langle \wp(D) \overset{\cup}{\longmapsto} \wp(E),\ \dot{\subseteq}\rangle \underset{\alpha^{\sim}}{\overset{\gamma^{\sim}}{\leftrightarrows}} \langle \wp(D) \overset{\cap}{\longmapsto} \wp(E),\ \dot{\supseteq}\rangle$. $\square$

– Meet preserving map inversion:

$$\begin{array}{rcl}
\alpha^{\cap} & \in & (\wp(D) \overset{\cap}{\longmapsto} \wp(E)) \longmapsto (\wp(E) \overset{\cap}{\longmapsto} \wp(D)) \\
 & \triangleq & \lambda\Phi \bullet \lambda Q \bullet \{s \mid \Phi(\neg\{s\}) \cup Q = E\}, \\
\gamma^{\cap} & \in & (\wp(E) \overset{\cap}{\longmapsto} \wp(D)) \longmapsto (\wp(D) \overset{\cap}{\longmapsto} \wp(E)) \\
 & \triangleq & \lambda\Phi \bullet \lambda P \bullet \{s' \mid \Phi(\neg\{s'\}) \cup P = D\}\ .
\end{array}$$

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

These correspondences between denotational and predicate transformers semantics can be organized in a commutative diagram, as follows:

Theorem 53. (Denotational to predicate transformer Galois connection commutative diagram).

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

The various predicate transformers introduced in [35] can be derived from the denotational semantics, using the following isomorphic abstractions ($f \in D \longmapsto \wp(E)$):

– Existential postimage:

$$\begin{array}{rcl}
\mathrm{gsp}[\![f]\!] & \triangleq & \alpha^{\triangleright}[f]\ \in\ \wp(D) \overset{\cup}{\longmapsto} \wp(E) \\
 & = & \lambda P \in \wp(D) \bullet \{s' \in E \mid \exists s \in P : s' \in f(s)\}
\end{array}$$

– Universal postimage:

$$\begin{array}{rcl}
\mathrm{gspa}[\![f]\!] & \triangleq & \alpha^{\sim} \circ \alpha^{\triangleright}[f]\ \in\ \wp(D) \overset{\cap}{\longmapsto} \wp(E) \\
 & = & \lambda P \in \wp(D) \bullet \{s' \in E \mid \forall s \in D : s' \in f(s) \Longrightarrow s \in P\}
\end{array}$$

– Universal preimage:

$$\begin{aligned}\mathrm{gwp}[\![f]\!] &\triangleq \alpha^{\sim} \circ \alpha^{\triangleright} \circ \alpha^{-1}[f] \;\in\; \wp(E) \xmapsto{\;\cap\;} \wp(D)\\ &= \lambda Q \in \wp(E)\bullet\{s \in D \mid \forall s' \in E : s' \in f(s) \Longrightarrow s' \in Q\}\end{aligned}$$

– Existential preimage:

$$\begin{aligned}\mathrm{gwpa}[\![f]\!] &\triangleq \alpha^{\triangleright} \circ \alpha^{-1}[f] \;\in\; \wp(E) \xmapsto{\;\cup\;} \wp(D)\\ &= \lambda Q \in \wp(E)\bullet\{s \in D \mid \exists s' \in Q : s' \in f(s)\}\end{aligned}$$

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 [24–26,31] weakest precondition[13]:

$$\mathrm{wp}(\tau^{\vec{\infty}}, Q) \triangleq \mathrm{gwp}[\![\tau^{\natural}]\!]\, Q$$

and weakest liberal precondition:

$$\mathrm{wlp}(\tau^{\vec{\infty}}, Q) \triangleq \mathrm{gwp}[\![\tau^{\flat}]\!]\, Q$$

of postcondition $Q \subseteq \Sigma$ are well-known. E. Dijkstra postulated healthiness conditions of predicate transformers [24–26,31] indeed follow from $\mathrm{gwp}[\![\tau^{\natural}]\!] \in \wp(\Sigma) \xmapsto{\;\cap\;} \wp(\Sigma)$ (Conjunctivitis) and $\mathrm{gwp}[\![\tau^{\natural}]\!]\,\emptyset = \emptyset$ since $\tau^{\natural}$ is total by theorem 33 and lemma 35 (Excluded Miracle).

In order to establish the equivalence of forward and backward predicate transformers and proof methods, we observe [10,26] that $\mathrm{gsp}[\![f]\!]\, P \subseteq Q$ 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 $P \subseteq \mathrm{gwp}[\![f]\!]\, Q$, and reciprocally, proving for all $f \in D \longmapsto \wp(E)$ that:

Lemma 54. (Correspondence between pre- and postcondition semantics). If $f \in D \longmapsto \wp(E)$ then $\langle \wp(D),\, \subseteq\rangle \underset{\mathrm{gsp}[\![f]\!]}{\overset{\mathrm{gwp}[\![f]\!]}{\leftrightarrows}} \langle \wp(E),\, \subseteq\rangle$.

9.2. Generalized Weakest Precondition Semantics

The *generalized weakest precondition semantics* is:

$$\tau^{\mathrm{gwp}} \triangleq \mathrm{gwp}[\![\tau^{\natural}]\!] \;.$$

This definition is preferred to the classical alternative $\tau^{\mathrm{wp}} \triangleq \mathrm{gwp}[\![\tau^{\sharp}]\!]$ because the above generalized weakest precondition semantics τ^{gwp} combines the expressive power of both the conservative weakest precondition for total correctness and the liberal weakest precondition for partial correctness. Indeed given a predicate $Q \subseteq \Sigma$, we have $\tau^{\mathrm{gwp}}[\![Q]\!] = \mathrm{wp}(\tau^{\vec{\infty}}, Q)$ and $\tau^{\mathrm{gwp}}[\![Q \cup \{\bot\}]\!] = \mathrm{wlp}(\tau^{\vec{\infty}}, Q)$. It follows that a single weakest precondition semantics τ^{gwp} can handle both total correctness and partial correctness. Moreover the conservative weakest precondition semantics $\tau^{\mathrm{gwp}}[\![Q]\!] = \mathrm{wp}(\tau^{\vec{\infty}}, Q)$ and the liberal weakest precondition semantics $\tau^{\mathrm{gwp}}[\![Q \cup \{\bot\}]\!] = \mathrm{wlp}(\tau^{\vec{\infty}}, Q)$ are further abstractions of the generalized weakest precondition semantics τ^{gwp} (as respectively shown in sections 9.3 and 9.4).

[13]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.

Applying the Kleenian fixpoint transfer theorem 3 to the fixpoint natural nondeterministic denotational semantics 33 with the correspondence $\langle \alpha^{\mathrm{gwp}},\ \gamma^{\mathrm{gwp}} \rangle$ where:

$$\begin{array}{lcl} \alpha^{\mathrm{gwp}} & \triangleq & \mathrm{gwp} \quad = \quad \alpha^{\sim} \circ \alpha^{\triangleright} \circ \alpha^{-1} \quad \text{and} \\ \gamma^{\mathrm{gwp}} & \triangleq & \gamma^{-1} \circ \gamma^{\triangleright} \circ \gamma^{\sim} \end{array}$$

which, according to theorem 53, is a Galois isomorphism, we derive[14]:

Theorem 55. (Fixpoint generalized weakest precondition semantics). $\tau^{\mathrm{gwp}} = \mathrm{lfp}^{\sqsubseteq^{\mathrm{gwp}}}_{\perp^{\mathrm{gwp}}} F^{\mathrm{gwp}}$ where $F^{\mathrm{gwp}} \in D^{\mathrm{gwp}} \xmapsto{\mathrm{m}} D^{\mathrm{gwp}}$ defined as $F^{\mathrm{gwp}}(\Phi) \triangleq \lambda Q \bullet (\neg \check{\tau} \cup Q) \dot{\cap} \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!] \circ \Phi = \lambda Q \bullet (Q \cap \check{\tau}) \dot{\cup} \mathrm{wp}[\![\tau^{\blacktriangleright}]\!] \circ \Phi$ where $\mathrm{wp}[\![f]\!]\, Q \triangleq \{s \in \Sigma \mid \exists s' \in \Sigma : s' \in f(s) \wedge \forall s' \in f(s) : s' \in Q\}$ is a $\sqsubseteq^{\mathrm{gwp}}$-monotone map on the complete lattice $\langle D^{\mathrm{gwp}},\ \sqsubseteq^{\mathrm{gwp}},\ \perp^{\mathrm{gwp}},\ \top^{\mathrm{gwp}},\ \sqcup^{\mathrm{gwp}},\ \sqcap^{\mathrm{gwp}} \rangle$ with:

- $D^{\mathrm{gwp}} \triangleq \wp(\Sigma_\perp) \xmapsto{\cap} \wp(\Sigma)$,
- $\Phi \sqsubseteq^{\mathrm{gwp}} \Psi \triangleq \forall Q \subseteq \Sigma : \Psi(Q \cup \{\perp\}) \subseteq \Phi(Q \cup \{\perp\}) \wedge \Phi(\Sigma) \subseteq \Psi(\Sigma)$,
- $\perp^{\mathrm{gwp}} = \lambda Q \bullet \big(\, \perp \in Q \;?\; \Sigma \;¿\; \emptyset \,\big)$ and
- $\bigsqcup^{\mathrm{gwp}}_{i \in \Delta} \Psi_i \triangleq \lambda Q \bullet \bigcap_{i \in \Delta} \Psi_i(Q \cup \{\perp\}) \cap \big(\, \perp \notin Q \;?\; \bigcup_{i \in \Delta} \Psi_i(\Sigma) \;¿\; \Sigma \,\big)$.

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

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

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

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

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 $\forall Q \subseteq \Sigma : \Psi(Q \cup \{\perp\}) \subseteq \Phi(Q \cup \{\perp\})$ where $Q \cup \{\perp\} = \neg P$ in $\Sigma_\perp$ whence $Q = \neg P$ in Σ. Reciprocally, if $\forall Q \subseteq \Sigma : \Psi(Q \cup \{\perp\}) \subseteq \Phi(Q \cup \{\perp\})$ then for all $s' \in \Sigma$ and $Q = \Sigma \setminus \{s'\}$ we have $Q \cup \{\perp\} = \Sigma_\perp \setminus \{s'\} = \neg\{s'\}$ whence $\Psi(\neg\{s'\}) \subseteq \Phi(\neg\{s'\})$.

[14] Observe that $\sqsubseteq^{\mathrm{gwp}}$ coincides with the partial ordering $\sqsubseteq$ of [43] except that the explicit use of $\perp$ 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 $\Phi \sqsubseteq^{\text{gwp}} \Psi = \forall Q \subseteq \Sigma : \Psi(Q \cup \{\bot\}) \subseteq \Phi(Q \cup \{\bot\}) \wedge \Phi(\Sigma) \subseteq \Psi(\Sigma)$.

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

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

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

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

By the commutation condition $\alpha^{\text{gwp}} \circ F^\natural = F^{\text{gwp}} \circ \alpha^{\text{gwp}}$ so that $\alpha^{\text{gwp}} \circ F^\natural \circ \gamma^{\text{gwp}} = F^{\text{gwp}} \circ \alpha^{\text{gwp}} \circ \gamma^{\text{gwp}} = F^{\text{gwp}}$. It follows that $f \sqsubseteq^{\text{gwp}} g$ implies $\gamma^{\text{gwp}}(f) \sqsubseteq^\natural \gamma^{\text{gwp}}(g)$ that is $F^\natural(\gamma^{\text{gwp}}(f)) \sqsubseteq^\natural F^\natural(\gamma^{\text{gwp}}(g))$ by theorem 24 whence $\gamma^{\text{gwp}} \circ \alpha^{\text{gwp}} \circ F^\natural \circ \gamma^{\text{gwp}}(f) \sqsubseteq^\natural \gamma^{\text{gwp}} \circ \alpha^{\text{gwp}} \circ F^\natural \circ \gamma^{\text{gwp}}(g)$. Therefore $\gamma^{\text{gwp}}(F^{\text{gwp}}(f)) \sqsubseteq^\natural \gamma^{\text{gwp}}(F^{\text{gwp}}(g))$ hence $F^{\text{gwp}}(f) \sqsubseteq^{\text{gwp}} F^{\text{gwp}}(g)$ proving that F^{gwp} is $\sqsubseteq^{\text{gwp}}$-monotone. $\square$

Lemma 56. (Arrangement of the iterates of F^{gwp}). Let F^{gwp^δ}, $\delta \in \mathbb{O}$ be the iterates of F^{gwp} from $\bot^{\text{gwp}}$. For all $\eta < \xi$ and $Q \subseteq \Sigma_\bot$, we have $F^{\text{gwp}^\eta}(Q \setminus \{\bot\}) \subseteq F^{\text{gwp}^\xi}(Q \setminus \{\bot\})$.

Proof. The proof of theorem 55 shows, by the Kleenian fixpoint transfer theorem 3, that $\forall \delta \in \mathbb{O} : F^{\text{gwp}^\delta} = \text{gwp}[\![F^{\text{gwp}^\delta}]\!]$. By reductio ad absurdum, if there exists $Q \subseteq \Sigma$ such that $F^{\text{gwp}^\eta}(Q) \not\subseteq F^{\text{gwp}^\xi}(Q)$ then $\exists s \in \text{gwp}[\![F^{\natural^\eta}]\!]\, Q : s \notin \text{gwp}[\![F^{\natural^\xi}]\!]\, Q$ 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 34. $\square$

Lemma 57. (Strictness of the iterates of F^{gwp}). Let F^{gwp^δ}, $\delta \in \mathbb{O}$ be the iterates of F^{gwp} from $\bot^{\text{gwp}}$. $\forall \delta \in \mathbb{O} : F^{\text{gwp}^\delta}(\emptyset) = \emptyset$.

Proof. The proof of theorem 55 shows, by the Kleenian fixpoint transfer theorem 3, that $\forall \delta \in \mathbb{O} : F^{\mathrm{gwp}^\delta} = \mathrm{gwp}[\![F^{\mathrm{gwp}^\delta}]\!]$. So $F^{\mathrm{gwp}^\delta}(\emptyset) = \{s \in \Sigma \mid \forall s' \in \Sigma_\perp : s' \in F^{\natural^\delta}(s) \Longrightarrow s' \in \emptyset\}$ $= \{s \in \Sigma \mid \forall s' \in \Sigma_\perp : s' \notin F^{\natural^\delta}(s)\} = \{s \in \Sigma \mid F^{\natural^\delta}(s) = \emptyset\} = \emptyset$ by lemma 35. $\square$

Lemma 58. (Final states of the iterates of F^{gwp}). Let F^{gwp^δ}, $\delta \in \mathbb{O}$ be the iterates of F^{gwp} from $\perp^{\mathrm{gwp}}$. $\forall \delta \in \mathbb{O} : \forall Q \subseteq \Sigma_\perp : F^{\mathrm{gwp}^\delta}(Q \setminus \{\perp\}) \subseteq F^{\mathrm{gwp}^\delta}(\check{\tau})$.

Proof. The proof of theorem 55 shows, by the Kleenian fixpoint transfer theorem 3, that $\forall \delta \in \mathbb{O} : F^{\mathrm{gwp}^\delta} = \mathrm{gwp}[\![F^{\natural^\delta}]\!]$. So if $s \in F^{\mathrm{gwp}^\delta}(Q \setminus \{\perp\})$ then $\forall s' \in \Sigma_\perp : s' \in F^{\natural^\delta}(s) \Longrightarrow$ $s' \in Q \setminus \{\perp\}$ so $\perp \notin F^{\natural^\delta}(s)$ hence, by lemma 36, $\forall s' \in \Sigma_\perp : s' \in F^{\natural^\delta}(s) \Longrightarrow s' \in \check{\tau}$ proving that $s \in F^{\mathrm{gwp}^\delta}(\check{\tau})$. $\square$

Total correctness is the conjunction of partial correctness and termination in that $\forall Q \subseteq \Sigma : \tau^{\mathrm{gwp}}[\![Q]\!] = \tau^{\mathrm{gwp}}[\![Q \cup \{\perp\}]\!] \cap \tau^{\mathrm{gwp}}[\![\Sigma]\!]$ since τ^{gwp} is a complete $\cap$-morphism. We have $\check{\tau} \subseteq \Sigma$ so $\tau^{\mathrm{gwp}}[\![\check{\tau}]\!] \subseteq \tau^{\mathrm{gwp}}[\![\Sigma]\!]$ by monotony and $\tau^{\mathrm{gwp}}[\![\Sigma]\!] \subseteq \tau^{\mathrm{gwp}}[\![\check{\tau}]\!]$ by lemma 58 and theorem 55 so that by antisymmetry: $\forall Q \subseteq \Sigma : \tau^{\mathrm{gwp}}[\![Q]\!] = \tau^{\mathrm{gwp}}[\![Q \cup \{\perp\}]\!] \cap \tau^{\mathrm{gwp}}[\![\check{\tau}]\!]$.

9.3. E. Dijkstra Weakest Conservative Precondition Semantics

E. Dijkstra's *weakest conservative precondition semantics* [24–26,31] 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 [15]:

$$\alpha^{\mathrm{wp}} \ \triangleq\ \lambda \Phi \cdot \Phi|_{\wp(\Sigma)}$$

satisfies:

Lemma 59. (Weakest conservative precondition abstraction). $\langle D^{\mathrm{gwp}}, \dot{\supseteq}\rangle \underset{\alpha^{\mathrm{wp}}}{\overset{\gamma^{\mathrm{wp}}}{\longleftarrow\!\!\!\longrightarrow\!\!\!\!\rightarrow}}$ $\langle D^{\mathrm{wp}}, \dot{\supseteq}\rangle$ where $D^{\mathrm{wp}} \triangleq \wp(\Sigma) \overset{\cap}{\longmapsto} \wp(\Sigma)$ and $\gamma^{\mathrm{wp}}(\Psi) \triangleq \lambda Q \cdot (\perp \notin Q \mathrel{?} \Psi(Q) \mathrel{¿} \emptyset)$.

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

Dijkstra's weakest conservative precondition semantics τ^{wp} is an abstraction of the demoniac denotational semantics [3]:

Lemma 60. (Abstraction of the demoniac nondeterministic denotational semantics). $\tau^{\mathrm{wp}} = \alpha^{\mathrm{wp}}(\mathrm{gwp}[\![\tau^\sharp]\!])$.

Proof. We have $\tau^{\mathrm{wp}} \triangleq \alpha^{\mathrm{wp}}(\tau^{\mathrm{gwp}}) = \alpha^{\mathrm{wp}}(\mathrm{gwp}[\![\tau^\natural]\!]) = \lambda Q \in \wp(\Sigma) \cdot \{s \in \Sigma \mid \forall s' \in \Sigma_\perp : s' \in \tau^\natural(s) \Longrightarrow s' \in Q\} = \lambda Q \in \wp(\Sigma) \cdot \{s \in \Sigma \mid \perp \notin \tau^\natural(s) \wedge \forall s' \in \Sigma_\perp : s' \in \tau^\natural(s) \Longrightarrow s' \in Q\}$ since $\perp \notin Q$. This is $\lambda Q \in \wp(\Sigma) \cdot \{s \in \Sigma \mid \forall s' \in \Sigma_\perp : (\perp \in \tau^\natural(s) \Longrightarrow s' \in Q) \wedge (\perp \notin \tau^\natural(s) \wedge s' \in \tau^\natural(s) \Longrightarrow s' \in Q)\} = \lambda Q \in \wp(\Sigma) \cdot \{s \in \Sigma \mid \forall s' \in \Sigma_\perp : (s' \in \tau^\natural(s) \cup \{s'' \in \Sigma \mid \perp \in \tau^\natural(s)\}) \Longrightarrow s' \in Q\} = \lambda Q \in \wp(\Sigma) \cdot \{s \in \Sigma \mid \forall s' \in \Sigma_\perp : s' \in \alpha^\sharp(\tau^\natural)(s) \Longrightarrow s' \in Q\} = \alpha^{\mathrm{wp}}(\mathrm{gwp}[\![\alpha^\sharp(\tau^\natural)]\!]) = \alpha^{\mathrm{wp}}(\mathrm{gwp}[\![\tau^\sharp]\!])$ by lemma 38. $\square$

[15] Recall that $f|_X$ is the restriction of function f to the domain X.

Theorem 55 characterizes a predicate transformer τ^{gwp} as the least fixpoint $\operatorname{lfp}^{\sqsubseteq^{\text{gwp}}}_{\perp^{\text{gwp}}} F^{\text{gwp}}$ of a predicate transformer transformer F^{gwp} whereas [26,27] only use fixpoints of predicate transformers by reasoning on a given postcondition. Reasoning on a given postcondition $Q \subseteq \Sigma$ is indeed an abstraction $\alpha^{\text{Q}}(\Phi) \triangleq \Phi(Q)$ which can be used to derive E. Dijkstra's fixpoint characterization [24–26,31] of the conservative precondition semantics τ^{wp} from theorem 46:

Lemma 61. If $Q \subseteq E$ then $\langle \wp(E) \overset{\cap}{\longmapsto} \wp(D),\ \dot{\supseteq} \rangle \xleftrightarrows[\alpha^{\text{Q}}]{\gamma^{\text{Q}}} \langle \wp(D),\ \supseteq \rangle$ where $\alpha^{\text{Q}}(\Phi) \triangleq \Phi(Q)$ and $\gamma^{\text{Q}}(P) \triangleq \lambda R \centerdot (\, Q \subseteq R \;?\; P \;¿\; \emptyset\,)$.

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

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

By composition of lemmata 61, 60 and theorem 53, we get:

Corollary 62. (Demoniac to weakest conservative precondition abstraction). For all $Q \subseteq \Sigma$, $\langle \Sigma \longmapsto \wp(\Sigma_\perp),\ \dot{\subseteq} \rangle \xleftrightarrows[\gamma^{\text{gwp}} \circ \gamma^{\text{wp}} \circ \gamma^{\text{Q}}]{\alpha^{\text{Q}} \circ \alpha^{\text{wp}} \circ \alpha^{\text{gwp}}} \langle \wp(\Sigma),\ \supseteq \rangle$ where $\alpha^{\text{Q}} \circ \alpha^{\text{wp}} \circ \alpha^{\text{gwp}} = \lambda f \centerdot \operatorname{gwp}[\![f]\!]\, Q$.

By definition of $\tau^\sharp$ and the Kleenian fixpoint transfer theorem 3 applied to the fixpoint characterization of the nondeterministic demoniac semantics semantics 46 with the abstraction $\lambda f \centerdot \operatorname{gwp}[\![f]\!]\, Q$ for a given $Q \subseteq \Sigma$ considered in corollary 62, we now obtain [26,27]:

Theorem 63. (E. Dijkstra's fixpoint weakest conservative precondition semantics). $\tau^{\text{wp}} = \lambda Q \centerdot \operatorname{lfp}^{\subseteq}_{\emptyset} F^{\text{wp}}[\![Q]\!]$ where $F^{\text{wp}} \in \wp(\Sigma) \longmapsto \wp(\Sigma) \overset{\text{m}}{\longmapsto} \wp(\Sigma)$ defined by $F^{\text{wp}}[\![Q]\!] \triangleq \lambda P \centerdot (Q \cap \check{\tau}) \cup \operatorname{wp}[\![\tau^{\blacktriangleright}]\!]\, P = \lambda P \centerdot (\neg\check{\tau} \cup Q) \cap \operatorname{gwp}[\![\tau^{\blacktriangleright}]\!]\, P$ is a $\subseteq$-monotone map on the complete lattice $\langle \wp(\Sigma),\ \subseteq, \emptyset, \Sigma, \cup, \cap \rangle$.

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

Let $f^\delta, \delta \in \mathbb{O}$ be a $\dot{\sqsubseteq}^{=}$-increasing chain. We have $\operatorname{gwp}[\![\dot{\bigsqcup}^{=}_{\delta\in\mathbb{O}} f^\delta]\!]\, Q = \{s \mid \bigsqcup^{=}_{\delta\in\mathbb{O}} f^\delta(s) \subseteq Q\}$. $f^\delta(s), \delta \in \mathbb{O}$ is a $\sqsubseteq^{=}$-increasing chain so that by definition of the flat DCPO $D^{\mp}$ 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 $\{s \mid \Sigma_\perp \subseteq Q\} = \emptyset = \bigcup_{\delta\in\mathbb{O}} \operatorname{gwp}[\![f^\delta]\!]\, Q$ 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 $\{s \mid P \subseteq Q\} = \bigcup_{\delta<\beta} \emptyset \cup \bigcup_{\delta\geq\beta} \{s \mid P \subseteq Q\} = \bigcup_{\delta<\beta} \{s \mid f^\delta(s) \subseteq Q\} \cup \bigcup_{\delta\geq\beta} \{s \mid f^\delta(s) \subseteq Q\} = \bigcup_{\delta\in\mathbb{O}} \operatorname{gwp}[\![f^\delta]\!]\, Q$, proving Scott-continuity.

By theorems 40 and 33, we have $\alpha^{\text{Q}} \circ \alpha^{\text{wp}} \circ \alpha^{\text{gwp}} \circ F^\sharp(f) = \alpha^{\text{Q}} \circ \alpha^{\text{wp}} \circ \alpha^{\text{gwp}} \circ F^\natural(f) = \alpha^{\text{Q}} \circ \alpha^{\text{wp}} \circ F^{\text{gwp}} \circ \alpha^{\text{gwp}}(f)$ as shown in the proof of theorem 55. By definition of α^{Q}

and α^{wp}, this is $F^{\text{gwp}}(\alpha^{\text{gwp}}(f))Q = (Q \cap \check{\tau}) \cup \text{wp}[\![\tau^{\bullet\!\!\to}]\!](\alpha^{\text{gwp}}(f)(Q))$ by theorem 55. Since $Q \subseteq \Sigma$, this is $(Q \cap \check{\tau}) \cup \text{wp}[\![\tau^{\bullet\!\!\to}]\!](\alpha^{\text{Q}} \circ \alpha^{\text{wp}} \circ \alpha^{\text{gwp}}(f)) = F^{\text{wp}}[\![Q]\!] \circ \alpha^{\text{Q}} \circ \alpha^{\text{wp}} \circ \alpha^{\text{gwp}}(f)$ by defining $F^{\text{wp}}[\![Q]\!] \triangleq \lambda P \bullet (Q \cap \check{\tau}) \cup \text{wp}[\![\tau^{\bullet\!\!\to}]\!]\, P$ thus proving the commutation property $\lambda f \bullet \text{gwp}[\![f]\!]\, Q \circ F^{\sharp} = F^{\text{wp}}[\![Q]\!] \circ \lambda f \bullet \text{gwp}[\![f]\!]\, Q$. Moreover $F^{\text{wp}}[\![Q]\!] = \lambda P \bullet (Q \cap \check{\tau}) \cup \text{wp}[\![\tau^{\bullet\!\!\to}]\!]\, P$ $= \lambda P \bullet (Q \cap \{s \mid \forall s' : \neg(s\ \tau\ s') \wedge \forall s' \in \tau^{\bullet\!\!\to} : s' \in P) \cup \{s \mid \exists s' : s\ \tau\ s' \wedge \forall s' \in \tau^{\bullet\!\!\to} : s' \in P\} =$ $(Q \cap \check{\tau} \cap \text{gwp}[\![\tau^{\bullet\!\!\to}]\!]\, P) \cup (\neg\check{\tau} \cap \text{gwp}[\![\tau^{\bullet\!\!\to}]\!]\, P) = (\neg\check{\tau} \cup (Q \cap \check{\tau})) \cap \text{gwp}[\![\tau^{\bullet\!\!\to}]\!]\, P = (\neg\check{\tau} \cup Q) \cap \text{gwp}[\![\tau^{\bullet\!\!\to}]\!]\, P$.

In conclusion, E. Dijkstra's fixpoint characterization of the weakest conservative precondition semantics is

$$\tau^{\text{wp}} \triangleq \alpha^{\text{wp}}(\text{gwp}[\![\tau^{\infty}]\!]) = \lambda Q \in \wp(\Sigma) \bullet \text{gwp}[\![\text{lfp}^{\dot{\sqsubseteq}^{=}}_{\dot{\bot}^{=}}\, F^{\sharp}]\!]\, Q = \lambda Q \in \wp(\Sigma) \bullet \text{lfp}^{\subseteq}_{\emptyset}\, F^{\text{wp}}[\![Q]\!]. \qquad \square$$

9.4. E. Dijkstra Weakest Liberal Precondition Semantics

E. Dijkstra's *weakest liberal precondition semantics* [24–26,31] $\lambda Q \in \wp(\Sigma) \bullet \text{wlp}(\tau^{\vec{\infty}}, Q)$ is

$$\tau^{\text{wlp}} \;\triangleq\; \alpha^{\text{wlp}}(\tau^{\text{gwp}})$$

where the abstraction α^{wlp} satisfies:

Lemma 64. (Weakest liberal precondition abstraction). If $D^{\text{wlp}} \triangleq \wp(\Sigma) \xmapsto{\cap} \wp(\Sigma)$, $\alpha^{\text{wlp}} \triangleq \lambda \Phi \bullet \lambda Q \bullet \Phi(Q \cup \{\bot\})$ and $\gamma^{\text{wlp}}(\Psi) \triangleq \lambda Q \bullet (\,\bot \in Q\ ?\ \Psi(Q)\ ¿\ \emptyset\,)$ then $\langle D^{\text{gwp}}, \dot{\supseteq}\rangle \underset{\alpha^{\text{wlp}}}{\overset{\gamma^{\text{wlp}}}{\longleftrightarrow\!\!\!\!\rightarrow}} \langle D^{\text{wlp}}, \dot{\supseteq}\rangle$.

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

Dijkstra's weakest liberal semantics τ^{wlp} is an abstraction of the angelic denotational semantics [3]:

Lemma 65. (Abstraction of the angelic nondeterministic denotational semantics). $\tau^{\text{wlp}} = \text{gwp}[\![\tau^{\flat}]\!]$.

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

By lemma 65, theorem 49 and the Kleenian fixpoint transfer theorem, we deduce [26]:

Theorem 66. (E. Dijkstra's fixpoint weakest liberal precondition semantics). $\tau^{\text{wlp}} = \lambda Q \bullet \text{gfp}^{\subseteq}_{\Sigma}\, F^{\text{wp}}[\![Q]\!]$.

Proof. Given $Q \subseteq \Sigma$, we consider the abstraction $\lambda f \bullet \text{gwp}[\![f]\!]\, Q$. We have $\text{gwp}[\![\lambda s \bullet \emptyset]\!]\, Q$ $= \{s \in \Sigma \mid \forall s' \in \Sigma : s' \in \emptyset \Longrightarrow s' \in Q\} = \Sigma$, proving strictness. $\text{gwp}[\![\dot{\bigcup}_{i \in \Delta} f_i]\!]\, Q = \{s \in \Sigma \mid$ $\forall s' \in \Sigma : s' \in \bigcup_{i \in \Delta} f_i(s) \Longrightarrow s' \in Q\} = \{s \in \Sigma \mid \forall i \in \Delta : \forall s' \in \Sigma : s' \in f_i(s) \Longrightarrow s' \in Q\}$ $= \bigcap_{i \in \Delta} \text{gwp}[\![f_i]\!]\, Q$, which implies Scott-continuity. The semantic transformer is designed using the commutation condition $F^{\flat} \circ \lambda f \bullet \text{gwp}[\![f]\!]\, Q = \lambda f \bullet \text{gwp}[\![f]\!]\, Q \circ F^{\text{wp}}[\![Q]\!]$ as in the proof of theorem 63 since $F^{\flat} = F^{\sharp}$. $F^{\text{wp}}[\![Q]\!]$ is $\subseteq$-monotone. We conclude that $\tau^{\text{wlp}}(Q) =$ $\text{gwp}[\![\tau^{\flat}]\!]\, Q = \text{gwp}[\![\text{lfp}^{\dot{\subseteq}}_{\dot{\emptyset}}\, F^{\flat}]\!]\, Q = \text{lfp}^{\supseteq}_{\Sigma}\, F^{\text{wp}} = \text{gfp}^{\subseteq}_{\Sigma}\, F^{\text{wp}}$. $\square$

10. Galois Connections and Tensor Product

The set of Galois connections between posets (respectively DCPOs, complete lattices) $\langle D^{\check{}}, \sqsubseteq^{\check{}}\rangle$ and $\langle D^{\hat{}}, \sqsubseteq^{\hat{}}\rangle$ is denoted

$$\langle D^{\check{}}, \sqsubseteq^{\check{}}\rangle \leftrightarrows \langle D^{\hat{}}, \sqsubseteq^{\hat{}}\rangle \quad \triangleq \quad \{\langle \alpha, \gamma\rangle \mid \langle D^{\check{}}, \sqsubseteq^{\check{}}\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle D^{\hat{}}, \sqsubseteq^{\hat{}}\rangle\} \ .$$

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

The set of *complete join morphisms* is:

$$D^{\check{}} \overset{\sqcup}{\longmapsto} D^{\hat{}} \quad \triangleq \quad \{\alpha \in D^{\check{}} \longmapsto D^{\hat{}} \mid \forall X \subseteq D^{\check{}} : \alpha(\sqcup^{\check{}} X) = \sqcup^{\hat{}} \alpha(X)\} \ .$$

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

$$D^{\hat{}} \overset{\sqcap}{\longmapsto} D^{\check{}} \quad \triangleq \quad \{\gamma \in D^{\hat{}} \longmapsto D^{\check{}} \mid \forall Y \subseteq D^{\hat{}} : \gamma(\sqcap^{\hat{}} Y) = \sqcap^{\check{}} \gamma(Y)\} \ .$$

The *tensor product* $\otimes$ [51] [16] is:

Definition 67. (Tensor product). $\langle D^{\check{}}, \sqsubseteq^{\check{}}\rangle \otimes \langle D^{\hat{}}, \sqsubseteq^{\hat{}}\rangle \triangleq \{H \in \wp(D^{\check{}} \times D^{\hat{}}) \mid (1) \wedge (2) \wedge (3)\}$ where the conditions are:

1. $(X \sqsubseteq^{\check{}} X' \wedge \langle X', Y'\rangle \in H \wedge Y' \sqsubseteq^{\hat{}} Y) \Longrightarrow (\langle X, Y\rangle \in H)$;
2. $(\forall i \in \Delta : \langle X_i, Y\rangle \in H) \Longrightarrow (\langle \underset{i\in\Delta}{\sqcup^{\check{}}} X_i, Y\rangle \in H)$;
3. $(\forall i \in \Delta : \langle X, Y_i\rangle \in H) \Longrightarrow (\langle X, \underset{i\in\Delta}{\sqcap^{\check{}}} Y_i\rangle \in H)$.

We now define correspondences between Galois connections, complete join/meet morphisms and tensor products. The projection for pairs:

$$\begin{aligned} 1(\langle \alpha, \gamma\rangle) &\triangleq \alpha, \\ 2(\langle \alpha, \gamma\rangle) &\triangleq \gamma \ . \end{aligned}$$

provides the correspondance between Galois connections and complete join morphisms (abstractions) as well as complete join/meet morphisms (concretization). In a Galois connection, the adjunct of a map is unique and provided by:

$$\begin{aligned} \mathrm{AC}(\gamma) &\triangleq \lambda x \bullet \sqcap^{\hat{}}\{y \mid x \sqsubseteq^{\check{}} \gamma(y)\}, \\ \mathrm{CA}(\alpha) &\triangleq \lambda y \bullet \sqcup^{\check{}}\{x \mid \alpha(x) \sqsubseteq^{\hat{}} y\} \ . \end{aligned}$$

We have the following Galois isomorphisms:

[16] This is the semi-dual version, so that Z. Shmuely original definition corresponds to $\langle D^{\check{}}, \sqsubseteq^{\check{}}\rangle \otimes \langle D^{\hat{}}, \sqsupseteq^{\hat{}}\rangle$.

Lemma 68. (Galois isomorphism between Galois connections and complete join/meet morphisms).

$$\langle\langle D^{\hat{}},\ \sqsubseteq^{\hat{}}\rangle \overset{\sqcap}{\longmapsto} \langle D^{\check{}},\ \sqsubseteq^{\check{}}\rangle,\ \dot{\sqsupseteq}^{\hat{}}\rangle \underset{2}{\overset{\lambda\gamma\bullet\langle \mathrm{AC}(\gamma),\gamma\rangle}{\twoheadleftarrow\!\!\twoheadrightarrow}} \langle\langle D^{\check{}},\ \sqsubseteq^{\check{}}\rangle \leftrightarrows \langle D^{\hat{}},\ \sqsubseteq^{\hat{}}\rangle,\ \dot{\sqsubseteq}^{\hat{}} \times \dot{\sqsupseteq}^{\check{}}\rangle$$
$$\underset{1}{\overset{\lambda\alpha\bullet\langle \alpha,\,\mathrm{CA}(\alpha)\rangle}{\twoheadleftarrow\!\!\twoheadrightarrow}} \langle\langle D^{\check{}},\ \sqsubseteq^{\check{}}\rangle \overset{\sqcup}{\longmapsto} \langle D^{\hat{}},\ \sqsubseteq^{\check{}}\rangle,\ \dot{\sqsubseteq}^{\hat{}}\rangle\ .$$

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

To each $\alpha \in D^{\check{}} \overset{\sqcup}{\longmapsto} D^{\hat{}}$, there corresponds a unique γ such that $D^{\check{}} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} D^{\hat{}}$ given by $\gamma = \mathrm{CA}(\alpha) \triangleq \lambda y\bullet \sqcup^{\check{}}\{x \mid \alpha(x) \sqsubseteq^{\hat{}} y\}$. So $\lambda\alpha\bullet\langle\alpha,\ \mathrm{CA}(\alpha)\rangle \in (D^{\check{}} \overset{\sqcup}{\longmapsto} D^{\hat{}}) \longmapsto (D^{\check{}} \leftrightarrows D^{\hat{}})$. Dually, $\lambda\gamma\bullet\langle\mathrm{AC}(\gamma),\ \gamma\rangle \in (D^{\hat{}} \overset{\sqcap}{\longmapsto} D^{\check{}}) \longmapsto (D^{\check{}} \leftrightarrows D^{\hat{}})$.

To prove isomorphism, we assume $\langle\alpha,\ \gamma\rangle \in D^{\check{}} \leftrightarrows D^{\hat{}}$, $\alpha \in D^{\check{}} \overset{\sqcup}{\longmapsto} D^{\hat{}}$ with pointwise ordering $\alpha \mathrel{\dot{\sqsubseteq}^{\hat{}}} \alpha' \triangleq \forall x \in D^{\check{}} : \alpha(x) \sqsubseteq^{\hat{}} \alpha'(x)$ and $\gamma \in D^{\hat{}} \overset{\sqcap}{\longmapsto} D^{\check{}}$ with pointwise ordering $\gamma \mathrel{\dot{\sqsupseteq}^{\check{}}} \gamma' \triangleq \forall y \in D^{\hat{}} : \gamma(y) \sqsupseteq^{\check{}} \gamma'(y)$.

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

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

Since all maps are monotone, it follows that we have Galois connections. $\square$

By composition of Galois isomorphisms, we get $\langle\langle D^{\hat{}}, \sqsubseteq^{\hat{}}\rangle \overset{\sqcap}{\longmapsto} \langle D^{\check{}}, \sqsubseteq^{\check{}}\rangle, \dot{\sqsupseteq}^{\hat{}}\rangle \underset{\mathrm{AC}}{\overset{\mathrm{CA}}{\twoheadleftarrow\!\!\twoheadrightarrow}} \langle\langle D^{\check{}}, \sqsubseteq^{\check{}}\rangle \overset{\sqcup}{\longmapsto} \langle D^{\hat{}},\ \sqsubseteq^{\check{}}\rangle,\ \dot{\sqsubseteq}^{\hat{}}\rangle$.

The correspondance between join/meet morphisms and tensor products is provided by:

$$\begin{aligned}
\mathrm{HA}(\alpha) &\triangleq \{\langle x,\ y\rangle \in D^{\check{}} \times D^{\hat{}} \mid \alpha(x) \sqsubseteq^{\hat{}} y\},\\
\mathrm{HC}(\gamma) &\triangleq \{\langle x,\ y\rangle \in D^{\check{}} \times D^{\hat{}} \mid x \sqsubseteq^{\check{}} \gamma(y)\}\ ;
\end{aligned}$$

The correspondance between tensor products and the adjuncts of Galois connections is:

$$\begin{aligned}
\mathrm{AH}(H) &\triangleq \lambda x\bullet \sqcap^{\hat{}}\{y \mid \langle x,\ y\rangle \in H\},\\
\mathrm{CH}(H) &\triangleq \lambda y\bullet \sqcup^{\check{}}\{x \mid \langle x,\ y\rangle \in H\}\ .
\end{aligned}$$

These correspondances are Galois isomorphisms:

Lemma 69. (Galois isomorphism between tensor products and complete join/meet morphisms).

$$\langle\langle D^{\hat{}},\ \sqsubseteq^{\hat{}}\rangle \overset{\sqcap}{\longmapsto} \langle D^{\check{}},\ \sqsubseteq^{\check{}}\rangle,\ \dot{\sqsupseteq}^{\hat{}}\rangle \underset{\mathrm{HC}}{\overset{\mathrm{CH}}{\twoheadleftarrow\!\!\twoheadrightarrow}} \langle\langle D^{\check{}},\ \sqsubseteq^{\check{}}\rangle \otimes \langle D^{\hat{}},\ \sqsubseteq^{\hat{}}\rangle,\ \supseteq\rangle \underset{\mathrm{AH}}{\overset{\mathrm{HA}}{\twoheadleftarrow\!\!\twoheadrightarrow}}$$
$$\langle\langle D^{\check{}},\ \sqsubseteq^{\check{}}\rangle \overset{\sqcup}{\longmapsto} \langle D^{\hat{}},\ \sqsubseteq^{\check{}}\rangle,\ \dot{\sqsubseteq}^{\hat{}}\rangle$$

Proof. We have $\mathrm{HA} \in (D^{\check{}} \overset{\sqcup}{\longmapsto} D^{\hat{}}) \longmapsto (D^{\check{}} \otimes D^{\hat{}})$ since (1) if $x \sqsubseteq^{\check{}} x' \wedge \alpha(x') \sqsubseteq^{\hat{}} y' \wedge y' \sqsubseteq y$ then $\alpha(x) \sqsubseteq^{\hat{}} \alpha(x')$ by monotony so that $\alpha(x) \sqsubseteq^{\hat{}} y$ by transitivity; (2) if $\forall i \in \Delta : \alpha(x_i) \sqsubseteq^{\hat{}} y$ then $\underset{i\in\Delta}{\sqcup^{\hat{}}} \alpha(x_i) \sqsubseteq^{\hat{}} y$ by definition of lubs so that $\alpha(\underset{i\in\Delta}{\sqcup^{\check{}}} x_i) \sqsubseteq^{\hat{}} y$ since

α is a complete join morphism and (3) if $\forall i \in \Delta : \alpha(x) \mathrel{\hat{\sqsubseteq}} y_i$ then $\alpha(x) \mathrel{\hat{\sqsubseteq}} \hat{\bigsqcap}_{i\in\Delta} y_i$ by definition of glbs. Dually, we have $\mathrm{HC} \in (\hat{D} \overset{\sqcap}{\longmapsto} \check{D}) \longmapsto (\check{D} \otimes \hat{D})$.

If $H \in \langle \check{D},\, \check{\sqsubseteq}\rangle \otimes \langle \hat{D},\, \hat{\sqsubseteq}\rangle$ then $\langle x,\, y\rangle \in H$ implies $\hat{\sqcap}\{y' \mid \langle x,\, y'\rangle \in H\} \mathrel{\hat{\sqsubseteq}} y$ by definition of glbs. Reciprocally $\langle x,\, \hat{\sqcap}\{y' \mid \langle x,\, y'\rangle \in H\}\rangle \in H$ by (3) so that if $\hat{\sqcap}\{y' \mid \langle x,\, y'\rangle \in H\} \mathrel{\hat{\sqsubseteq}} y$ then $\langle x,\, y\rangle \in H$ by (1). So $\langle x,\, y\rangle \in H$ if and only if $\hat{\sqcap}\{y' \mid \langle x,\, y'\rangle \in H\} \mathrel{\hat{\sqsubseteq}} y$. Dually $\langle x,\, y\rangle \in H$ if and only if $x \mathrel{\check{\sqsubseteq}} \check{\sqcup}\{x' \mid \langle x',\, y\rangle \in H\}$. It follows that for all $H \in \check{D} \otimes \hat{D}$, we have $\mathrm{AH}(H)x \mathrel{\hat{\sqsubseteq}} y \iff \hat{\sqcap}\{y' \mid \langle x,\, y'\rangle \in H\} \mathrel{\hat{\sqsubseteq}} y \iff \langle x,\, y\rangle \in H \iff x \mathrel{\check{\sqsubseteq}} \check{\sqcup}\{x' \mid \langle x', y\rangle \in H\} \iff x \mathrel{\check{\sqsubseteq}} \mathrm{CH}(H)y$ proving that $\langle \check{D}, \check{\sqsubseteq}\rangle \underset{\mathrm{AH}(H)}{\overset{\mathrm{CH}(H)}{\leftrightarrows}} \langle \hat{D}, \hat{\sqsubseteq}\rangle$ whence $\mathrm{AH} \times \mathrm{CH} \in (\check{D} \otimes \hat{D}) \longmapsto (\check{D} \leftrightarrows \hat{D})$. It follows that $\mathrm{AH} = 1 \circ (\mathrm{AH} \times \mathrm{CH}) \in (\check{D} \otimes \hat{D}) \longmapsto (\check{D} \overset{\sqcup}{\longmapsto} \hat{D})$ and $\mathrm{CH} = 2 \circ (\mathrm{AH} \times \mathrm{CH}) \in (\check{D} \otimes \hat{D}) \longmapsto (\hat{D} \overset{\sqcap}{\longmapsto} \check{D})$.

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

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

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

Since all maps are monotone, we have Galois connections. $\square$

By composition of Galois isomorphisms, we get $\langle \langle \hat{D}, \hat{\sqsubseteq}\rangle \overset{\sqcap}{\longmapsto} \langle \check{D}, \check{\sqsubseteq}\rangle, \dot{\check{\sqsupseteq}}\rangle \underset{\mathrm{HC}\circ 2 = \mathrm{HA}\circ 1}{\overset{\mathrm{AH}\times\mathrm{CH}}{\leftrightarrows}} \langle \langle \check{D},\, \check{\sqsubseteq}\rangle \otimes \langle \hat{D},\, \hat{\sqsubseteq}\rangle,\, \supseteq\rangle$.

The above Galois isomorphisms can be organized into the following commutative diagram:

Theorem 70. (Galois connections/tensor product commutative diagram).

$$\begin{tikzcd}[column sep=huge, row sep=huge]
\langle\langle \check{D},\, \check{\sqsubseteq}\rangle \leftrightarrows \langle \hat{D},\, \hat{\sqsubseteq}\rangle,\, \dot{\hat{\sqsubseteq}} \times \dot{\check{\sqsupseteq}}\rangle \arrow[r, shift right, two heads, "1"'] \arrow[d, shift right, two heads, "2"'] \arrow[dr, shift left, two heads, "\mathrm{HC}\circ 2 = \mathrm{HA}\circ 1" near end] & \langle\langle \check{D},\, \check{\sqsubseteq}\rangle \overset{\sqcup}{\longmapsto} \langle \hat{D},\, \hat{\sqsubseteq}\rangle,\, \dot{\hat{\sqsubseteq}}\rangle \arrow[l, shift right, two heads, "\lambda\alpha\bullet\langle\alpha,\, \mathrm{CA}(\alpha)\rangle"'] \arrow[d, shift right, two heads, "\mathrm{HA}"'] \arrow[dl, shift right, two heads, "\mathrm{CA}"' near start] \\
\langle\langle \hat{D},\, \hat{\sqsubseteq}\rangle \overset{\sqcap}{\longmapsto} \langle \check{D},\, \check{\sqsubseteq}\rangle,\, \dot{\check{\sqsupseteq}}\rangle \arrow[r, shift right, two heads, "\mathrm{HC}"'] \arrow[u, shift right, two heads, "\lambda\gamma\bullet\langle\mathrm{AC}(\gamma),\, \gamma\rangle"'] \arrow[ur, shift right, two heads, "\mathrm{AC}"' near end] & \langle\langle \check{D},\, \check{\sqsubseteq}\rangle \otimes \langle \hat{D},\, \hat{\sqsubseteq}\rangle,\, \supseteq\rangle \arrow[l, shift right, two heads, "\mathrm{CH}"'] \arrow[u, shift right, two heads, "\mathrm{AH}"'] \arrow[ul, shift left, two heads, "\mathrm{AH}\times\mathrm{CH}" near start]
\end{tikzcd}$$

Proof. We check the commutation property of the diagram. We have shown that $\mathrm{AH} = \mathrm{AC} \circ \mathrm{CH}$ so $\mathrm{AH} \circ \mathrm{HC} = \mathrm{AC} \circ \mathrm{CH} \circ \mathrm{HC} = \mathrm{AC}$. Dually $\mathrm{CH} \circ \mathrm{HA} = \mathrm{CA}$.

$\lambda\gamma\bullet\langle \mathrm{AC}(\gamma), \gamma\rangle \circ \mathrm{CH}(H) = \langle \mathrm{AC}(\mathrm{CH}(H)), \mathrm{CH}(H)\rangle = \langle \mathrm{AH}(H), \mathrm{CH}(H)\rangle \triangleq (\mathrm{AH} \times \mathrm{CH})(H)$. Similarly, $\lambda\alpha\bullet\langle \alpha,\, \mathrm{CA}(\alpha)\rangle \circ \mathrm{AH} = \mathrm{AH} \times \mathrm{CH}$.

Finally, $1 \circ \lambda\gamma\bullet\langle \mathrm{AC}(\gamma),\, \gamma\rangle = \mathrm{AC}$ and $2 \circ \lambda\alpha\bullet\langle \alpha,\, \mathrm{CA}(\alpha)\rangle = \mathrm{CA}$. $\square$

11. Axiomatic Semantics

Using theorems 54 and 70, 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 (1) of definition 67 is the consequence rule of C.A.R. Hoare logic [32]. Conditions (2) and (3) are also valid for the classical presentation of C.A.R. Hoare logic [32] 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 [28], C.A.R. Hoare [32] & P. Naur [42] *partial correctness semantics* is

$$\tau^{\mathrm{pH}} \;\triangleq\; \mathrm{HC}(\tau^{\mathrm{wlp}}) \;.$$

We get R. Floyd & P. Naur's partial correctness verification conditions [28,42] using E. Dijkstra's fixpoint characterization 66 of the weakest liberal precondition semantics τ^{wlp} and D. Park fixpoint induction [45]:

Lemma 71. (D. Park fixpoint induction). If $\langle D,\, \sqsubseteq,\, \perp, \top, \sqcup,\, \sqcap \rangle$ is a complete lattice, $F \in D \overset{\mathrm{m}}{\longmapsto} D$ is $\sqsubseteq$-monotone and $P \in D$ then $\mathrm{lfp}_\perp^{\sqsubseteq} F \sqsubseteq P \iff (\exists I : F(I) \sqsubseteq I \wedge I \sqsubseteq P)$.

Proof. For soundness ($\Longleftarrow$), $\mathrm{lfp}_\perp^{\sqsubseteq} F = \sqcap\{X \mid F(X) \sqsubseteq X\} \sqsubseteq I \sqsubseteq P$ by Tarski's fixpoint theorem [52] and definition of glbs.

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

Theorem 72. (R. Floyd & P. Naur partial correctness semantics). $\tau^{\mathrm{pH}} = \{\langle P,\, Q \rangle \in \wp(\Sigma) \otimes \wp(\Sigma) \mid \exists I \in \wp(\Sigma) : P \subseteq I \;\wedge\; I \subseteq \mathrm{gwp}[\![\tau^{\bullet\!\!\to}]\!]\, I \;\wedge\; (I \cap \check{\tau}) \subseteq Q\}$.

The condition $I \subseteq \mathrm{gwp}[\![\tau^{\bullet\!\!\to}]\!]\, I$ is given by C.A.R. Hoare [32] while R. Floyd & P. Naur partial correctness verification condition [28,42] corresponds more precisely to $\mathrm{gsp}[\![\tau^{\bullet\!\!\to}]\!]\, I \subseteq I$ which, by lemma 54, is equivalent.

Proof. $\tau^{\mathrm{pH}} \triangleq \mathrm{HC}(\tau^{\mathrm{wlp}}) = \mathrm{HC}(\lambda Q \bullet \mathrm{gfp}_\Sigma^{\subseteq} F^{\mathrm{wp}}[\![Q]\!]) = \{\langle P, Q \rangle \in \wp(\Sigma) \otimes \wp(\Sigma) \mid \mathrm{lfp}_\Sigma^{\supseteq} F^{\mathrm{wp}}[\![Q]\!] \supseteq P\}$ by theorem 66 and definition of HC. By D. Park induction 71, we derive $\{\langle P,\, Q \rangle \in \wp(\Sigma) \otimes \wp(\Sigma) \mid \exists I \in \wp(\Sigma) : F^{\mathrm{wp}}[\![Q]\!](I) \supseteq I \wedge I \supseteq P\}$ which, by definition of F^{wp} in theorem 63, is $\{\langle P,\, Q \rangle \in \wp(\Sigma) \otimes \wp(\Sigma) \mid \exists I \in \wp(\Sigma) : I \subseteq (\neg\check{\tau} \cup Q) \cap \mathrm{gwp}[\![\tau^{\bullet\!\!\to}]\!](I) \wedge P \subseteq I\}$ $= \{\langle P,\, Q \rangle \in \wp(\Sigma) \otimes \wp(\Sigma) \mid \exists I \in \wp(\Sigma) : (I \cap \check{\tau}) \subseteq Q \wedge I \subseteq \mathrm{gwp}[\![\tau^{\bullet\!\!\to}]\!](I) \wedge P \subseteq I\}$. □

Using *C.A.R. Hoare triples*:

$$\{P\}\tau^{\vec{\infty}}\{Q\} \;\triangleq\; \langle P,\, Q \rangle \in \tau^{\mathrm{pH}},$$
$$\{P\}\tau\{Q\} \;\triangleq\; P \subseteq \mathrm{gwp}[\![\tau^{\bullet\!\!\to}]\!]\, Q$$

and a rule-based presentation of τ^{pH}, we get a set theoretic model of C.A.R. Hoare logic:

Corollary 73. (C.A.R. Hoare partial correctness axiomatic semantics). $\{P\}\tau^{\vec{\infty}}\{Q\}$ if and only if it derives from the axiom:

$$\{\mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\,Q\}\tau\{Q\} \qquad (\tau)$$

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 $\mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\,Q \subseteq \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\,Q$ implies the axiom (τ). Rule $(\tau^{\vec{\infty}})$ follows from theorem 72 where $P = I$ and $Q = (I \cap \check{\tau})$.

For relative completeness, if $\langle P, Q\rangle \in \tau^{\mathrm{pH}}$, then by theorem 72, there exists an invariant $I \in \wp(\Sigma)$ such that $P \subseteq I$, $I \subseteq \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\,I$ and $(I \cap \check{\tau}) \subseteq Q$. The formal proof of $\{P\}\tau^{\vec{\infty}}\{Q\}$ is therefore as follows: "$I \subseteq \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\,I$, $\{\mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\,I\}\tau\{I\}$ by the axiom (τ) and $I \subseteq I$ imply $\{I\}\tau\{I\}$ by the consequence rule $(\Rightarrow)$. Then we derive $\{I\}\tau^{\vec{\infty}}\{I \cap \check{\tau}\}$ by rule $(\tau^{\vec{\infty}})$. So from $P \subseteq I$, $\{I\}\tau^{\vec{\infty}}\{I \cap \check{\tau}\}$ and $(I \cap \check{\tau}) \subseteq Q$, we infer $\{P\}\tau^{\vec{\infty}}\{Q\}$ by the consequence rule $(\Rightarrow)$, Q.E.D.". ☐

11.2. R. Floyd Total Correctness Semantics

R. Floyd [28] *total correctness semantics* is

$$\tau^{\mathrm{tH}} \ \stackrel{\Delta}{=}\ \mathrm{HC}(\tau^{\mathrm{wp}}) \ .$$

We get R. Floyd's verification conditions using E. Dijkstra's fixpoint characterization 63 of τ^{wp} and the following induction principle:

Lemma 74. (Lower fixpoint induction). If $\langle D, \sqsubseteq, \bot, \sqcup\rangle$ is a DCPO, $F \in D \xrightarrow{\mathrm{m}} D$ is $\sqsubseteq$-monotone, $\pm \in D$ satisfies $\pm \sqsubseteq F(\pm)$ and $P \in D$ then $P \sqsubseteq \mathrm{lfp}^{\sqsubseteq}_{\pm}\, F \iff (\exists \epsilon \in \mathbb{O} : \exists I \in (\epsilon + 1) \longmapsto D : I^0 \sqsubseteq \pm \wedge \forall \delta : 0 < \delta \leq \epsilon \Longrightarrow I^\delta \sqsubseteq F(\bigsqcup_{\zeta<\delta} I^\zeta) \wedge P \sqsubseteq I^\epsilon)$.

Proof. For soundness $(\Longleftarrow)$, let $F^\delta, \delta \in \mathbb{O}$ be the increasing sequence of iterates of F from $\pm$, which can be defined as $F^0 = \pm$ and $F^\delta = F(\bigsqcup_{\zeta<\delta} F^\zeta)$ for all $\delta > 0$ [14]. We have $I^0 \sqsubseteq \pm = F^0$. 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 $P \sqsubseteq I^\epsilon \sqsubseteq F^\epsilon \sqsubseteq \mathrm{lfp}^{\sqsubseteq}_{\pm}\, F$.

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

Theorem 75. (R. Floyd total correctness semantics). $\tau^{\mathrm{tH}} = \{\langle P, Q\rangle \in \wp(\Sigma) \otimes \wp(\Sigma) \mid \exists \epsilon \in \mathbb{O} : \exists I \in (\epsilon + 1) \longmapsto \wp(\Sigma) : \forall \delta \leq \epsilon : I^\delta \subseteq (\neg\check{\tau} \cup Q) \cap \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!](\bigcup_{\beta<\delta} I^\beta) \wedge P \subseteq I^\epsilon\}$.

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

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

where the ordinal δ encodes the value of R. Floyd's *variant function* [27].

Proof. Follows directly from lemma 74, theorem 63 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 $I^0 \subseteq Q \cap \check{\tau} = F[\![\tau^{\blacktriangleright}]\!]\,\emptyset = \pm$. $\square$

Using *Z. Manna/A. Pnueli triples*:

$$\begin{array}{rcl} [P]\tau^{\tilde\infty}[Q] & \triangleq & \langle P, Q\rangle \in \tau^{\mathrm{tH}}, \\ [P]\tau[Q] & \triangleq & P \subseteq \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\,Q \end{array}$$

and a rule-based presentation of τ^{tH}, we get a set theoretic model of Z. Manna/A. Pnueli logic [39]:

Corollary 76. (Z. Manna/A. Pnueli total correctness axiomatic semantics). $[P]\tau^{\tilde\infty}[Q]$ if and only if it derives from the axiom (τ), the inference rules $(\Rightarrow)$, $(\wedge)$, $(\vee)$ and the following:

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

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 $\mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\,Q \subseteq \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\,Q$. Rule $(\tau^{\tilde\infty})$ follows from theorem 75 where $P = I^\epsilon$, $I^0 \subseteq (\neg\check{\tau} \cup Q) \cap \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\,\emptyset = \check{\tau} \cap Q$ and for $0 < \delta \leq \epsilon$, $I^\delta \subseteq (\neg\check{\tau} \cup Q)$ and $I^\delta \subseteq \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!](\bigcup_{\beta<\delta} I^\beta)$ whence $[I^\delta]\tau[\bigcup_{\beta<\delta} I^\beta]$.

For relative completeness, if $\langle P, Q\rangle \in \tau^{\mathrm{tH}}$, then there exists an ordinal ϵ and an invariant $I \in (\epsilon + 1) \longmapsto \wp(\Sigma)$ satisfying the conditions of theorem 75. So the formal proof is as follows: "For all $\delta \in \mathbb{O}$ with $\delta \leq \epsilon$, we have $I^\delta \subseteq (\neg\check{\tau} \cup Q) \cap \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!](\bigcup_{\beta<\delta} I^\beta)$ 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 $I^\delta \subseteq \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!](\bigcup_{\beta<\delta} I^\beta)$, the axiom $[\mathrm{gwp}[\![\tau^{\blacktriangleright}]\!](\bigcup_{\beta<\delta} I^\beta)]\tau[\bigcup_{\beta<\delta} I^\beta]$ and $\bigcup_{\beta<\delta} I^\beta \subseteq \bigcup_{\beta<\delta} I^\beta$ together with the consequence rule $(\Rightarrow)$ allows to derive $[I^\delta]\tau[\bigcup_{\beta<\delta} I^\beta]$. Then by rule $(\tau^{\tilde\infty})$ we derive $[I^\epsilon]\tau^{\tilde\infty}[Q]$ whence $[P]\tau^{\tilde\infty}[Q]$ by the consequence rule $(\Rightarrow)$, Q.E.D.". $\square$

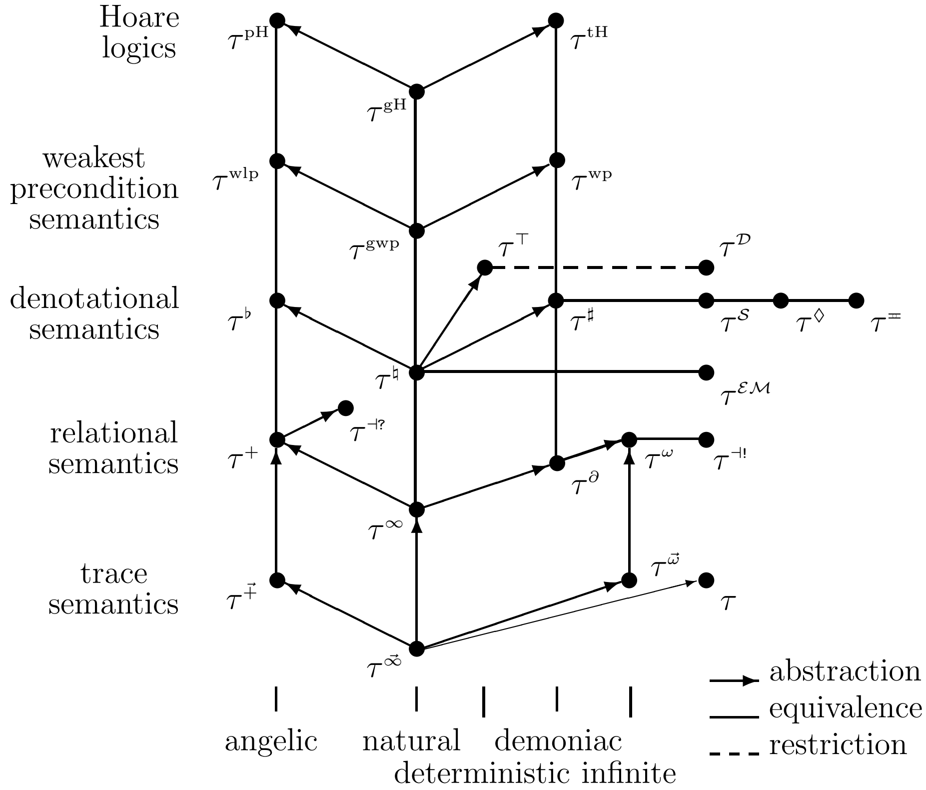


Figure 5. The hierarchy of semantics

12. Lattice of Semantics

A preorder can be defined on semantics $\tau^{\check{}} \in D^{\check{}}$ and $\tau^{\hat{}} \in D^{\hat{}}$ when $\tau^{\hat{}} = \alpha^{\hat{}}(\tau^{\check{}})$ and $\langle D^{\check{}}, \leq\rangle \underset{\alpha^{\hat{}}}{\overset{\gamma^{\hat{}}}{\leftrightarrows}} \langle D^{\hat{}}, \leqq\rangle$. The quotient poset is isomorphic to M. Ward lattice [54] of upper closure operators $\gamma^{\hat{}} \circ \alpha^{\hat{}}$ 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 [13, sec. 8], a subset 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[17]. 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 [18] . Then for program analysis of a given class of properties there should be a natural choice of semantics in the hierarchy [12].

Obviously, extension of this point of view for higher-order functional languages and to realistic programming languages is more difficult. The task would also be more difficult when considering other program properties involving interleaved combinations of fixpoints.

Acknowledgement

We thank the anonymous referees for the proposed clarifications.

REFERENCES

1. S. Abramsky and A. Jung. Domain theory. In S. Abramsky, Dov M. Gabbay, and T.S.E. Maibaum, editors, *Semantic Structures*, vol. 3 of *Handbook of Logic in Computer Science*, chapter 1, pages 1–168. Clarendon Press, Oxford, UK, 1994.
2. S. Abramsky and G. McCusker. Game semantics. In H. Schwichtenberg and U. Berger, editors, *Computational Logic*, vol. 165, pages 1–55. NATO Science Series, Series F: Computer and Systems Sciences. Springer-Verlag, Berlin, Germany, 1999.
3. K.R. Apt and G.D. Plotkin. Countable nondeterminism and random assignment. *Journal of the Association for Computing Machinary*, 33(4):724–767, October 1986.
4. A. Arnold and M. Nivat. Formal computations of non deterministic recursive program schemes. *Math. Systems Theory*, 13:219–236, 1980.
5. R.J.R. Back. A continuous semantics for unbounded nondeterminism. *Theoretical Computer Science*, 23:187–210, 1983.
6. C. Baier and M.E. Majster-Cederbaum. Metric semantics from partial order semantics. *Acta Informatica*, 34(9):701–735, 1997.
7. 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*, vol. 69 of *Lecture Notes in Computer Science*, pages 553–592. Springer-Verlag, Berlin, Germany, 1979.
8. M. Broy and G. Nelson. Can fair choice be added to Dijkstra's calculus. *ACM Transactions on Programming Languages and Systems*, 16(3):924–938, March 1994.
9. P. Cousot. *Méthodes itératives de construction et d'approximation de points fixes d'opérateurs monotones sur un treillis, analyse sémantique de programmes.* Thèse

[17]For example, the maximal trace semantics $\tau^{\vec{\infty}}$ 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.

[18]The correspondance between metric semantics [23] and domain theoretic denotational semantics in this hierarchy has been established by [6]. The correspondance with game semantics [2] is not immediate because of our language-independent presentation without any hypothesis on states and transitions whereas game semantics requires at least to make a distinction between transitions performed by the player and those performed by the opponent.

d'État ès sciences mathématiques, Université scientifique et médicale de Grenoble, Grenoble, France, 21 March 1978.
10. 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, Inc., Englewood Cliffs, New Jersey, 1981.
11. P. Cousot. Methods and logics for proving programs. In J. van Leeuwen, editor, *Formal Models and Semantics*, vol. B of *Handbook of Theoretical Computer Science*, chapter 15, pages 843–993. Elsevier Science Publishers B.V., Amsterdam, The Netherlands, 1990.
12. P. Cousot. Abstract interpretation. *Symposium on Models of Programming Languages and Computation, ACM Computing Surveys*, 28(2):324–328, 1996.
13. P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Conference Record of the Fourth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 238–252, Los Angeles, California, 1977. ACM Press, New York.
14. P. Cousot and R. Cousot. Constructive versions of Tarski's fixed point theorems. *Pacific Journal of Mathematics*, 82(1):43–57, 1979.
15. P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Conference Record of the Sixth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 269–282, San Antonio, Texas, 1979. ACM Press, New York.
16. 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 University Press, Cambridge, United Kindom, 1982.
17. P. Cousot and R. Cousot. Inductive definitions, semantics and abstract interpretation. In *Conference Record of the Ninthteenth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 83–94, Albuquerque, New Mexico, 1992. ACM Press, New York, New York, United States.
18. 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 *Proceedings of the 1994 International Conference on Computer Languages*, pages 95–112, Toulouse, France, 16–19 May 1994. IEEE Computer Society Press, Los Alamitos, California.
19. 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, *Proceedings of the SeventhInternational Conference on Computer Aided Verification, CAV '95*, Liège, Belgium, vol. 939 of *Lecture Notes in Computer Science*, pages 293–308. Springer-Verlag, Berlin, Germany, 3–5 July 1995.
20. P. Cousot and R. Cousot. Temporal abstract interpretation. In *Conference Record of the Twentyseventh Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, Boston, Massachusetts, January 2000. ACM Press, New York.
21. J.W. de Bakker, J.-J.Ch. Meyer, and J.I. Zucker. On infinite computations in de-

notational semantics. *Theoretical Computer Science*, 26:53–82, 1983. (Corrigendum: Theoretical Computer Science 29:229–230, 1984).

22. J.W. de Bakker and D. Scott. A theory of programs. Unpublished notes, 1969.
23. J.W. de Bakker and E. de Vink. *Control Flow Semantics.* Foundations of Computing Series. MIT Press, Cambridge, Mass., 1996.
24. E.W. Dijkstra. Guarded commands, nondeterminacy and formal derivation of programs. *Communications of the Association for Computing Machinary*, 18(8):453–457, August 1975.
25. E.W. Dijkstra. *A Discipline of Programming.* Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1976.
26. E.W. Dijkstra and C.S. Scholten. *Predicate Calculus and Program Semantics.* Springer-Verlag, Berlin, Germany, 1990.
27. E.W. Dijkstra and A.J.M. van Gasteren. A simple fixpoint argument without the restriction to continuity. *Acta Informatica*, 23:1–7, 1986.
28. R.W. Floyd. Assigning meaning to programs. In J.T. Schwartz, editor, *Proceedings of the Symposium in Applied Mathematics*, vol. 19, pages 19–32. American Mathematical Society, Providence, Rhode Island, 1967.
29. R. Giacobazzi and F. Ranzato. Completeness in abstract interpretation: A domain perspective. In M. Johnson, editor, *Proceedings of the SixthInternational Conference on Algebraic Methodology and Software Technology, AMAST '97, Sydney, Australia*, vol. 1349 of *Lecture Notes in Computer Science*, pages 231–245. Springer-Verlag, Berlin, Germany, 13–18 December 1997.
30. C.A. Gunter and D.S. Scott. Semantic domains. In J. van Leeuwen, editor, *Formal Models and Semantics*, vol. B of *Handbook of Theoretical Computer Science*, chapter 12, pages 633–674. Elsevier Science Publishers B.V., Amsterdam, The Netherlands, 1990.
31. W.H. Hesselink. *Programs, Recursion and Unbound Choice, predicate transformation semantics and transformation rules.* Oxford University Press, Oxford, UK, 1992.
32. C.A.R. Hoare. An axiomatic basis for computer programming. *Communications of the Association for Computing Machinary*, 12(10):576–580, October 1969.
33. C.A.R. Hoare. Some properties of predicate transformers. *Journal of the Association for Computing Machinary*, 25(3):461–480, July 1978.
34. C.A.R. Hoare and P.E. Lauer. Consistent and complementary formal theories of the semantics of programming languages. *Acta Informatica*, 3(2):135–153, 1974.
35. D. Jacobs and D. Gries. General correctness: A unification of partial and total correctness. *Acta Informatica*, 22:67–83, 1985.
36. G. Kahn. Natural semantics. In K. Fuchi and M. Nivat, editors, *Programming of Future Generation Computers*, pages 237–258. Elsevier Science Publishers B.V., Amsterdam, The Netherlands, 1988.
37. S. Kripke. A semantical analysis of modal logic I: normal modal propositional calculi. *Z. Math. Logik Grundlagen Math.*, 9:67–96, 1963.
38. M.E. Majster-Cederbaum. A simple relation between relational and predicate transformer semantics for nondeterministic programs. *Information Processing Letters*, 11(4, 5):190–192, 12 December 1980.
39. Z. Manna and A. Pnueli. Axiomatic approach to total correctness. *Acta Informatica*,

3:253–263, 1974.
40. R. Milner. Operational and algebraic semantics of concurrent processes. In J. van Leeuwen, editor, *Formal Models and Semantics*, vol. B of *Handbook of Theoretical Computer Science*, chapter 19, pages 1201–1242. Elsevier Science Publishers B.V., Amsterdam, The Netherlands, 1990.
41. R. Milner and M. Tofte. Co-induction in relational semantics. *Theoretical Computer Science*, 87:209–220, 1991.
42. P. Naur. Proofs of algorithms by general snapshots. *BIT*, 6:310–316, 1966.
43. G. Nelson. A generalization of Dijkstra's calculus. *ACM Transactions on Programming Languages and Systems*, 11(4):517–561, April 1989.
44. C.-H. L. Ong. Correspondence between operational and denotational semantics: the full abstraction problem for pcf. In S. Abramsky, D.M. Gabbay, and T.S.E. Maibaum, editors, *Semantic Modelling*, vol. 4 of *Handbook of Logic in Computer Science*, chapter 3, pages 269–356. Clarendon Press, Oxford, UK, 1995.
45. D. Park. Fixpoint, induction and proofs of program properties. In B. Meltzer and D. Michie, editors, *Machine Intelligence*, vol. 5, pages 59–78. Edinburgh University Press, Edinburg, Scotland, 1969.
46. D. Park. On the semantics of fair parallelism. In D. Bjørner, editor, *Proceedings of the of the Winter School on Abstract Software Specifications*, vol. 86 of *Lecture Notes in Computer Science*, pages 504–526. Springer-Verlag, Berlin, Germany, 1980.
47. A.M. Pitts. Operational semantics for program equivalence. Invited address, MFPS XIII, CMU, Pittsburgh, 23–26 March 1997. `http://www.cl.cam.ac.uk/users/ap/talks`.
48. G.D. Plotkin. A structural approach to operational semantics. Technical Report DAIMI FN-19, Aarhus University, Denmark, september 1981.
49. D. Scott. Outline of a mathematical theory of computation. Technical Monograph PRG-2, Oxford University Computing Laboratory, Programming Research Group, Oxford, UK, November 1970.
50. D. Scott. The lattice of flow diagrams. In E. Engeler, editor, *Semantics of Algorithmic Languages*, vol. 188 of *Lecture Notes in Mathematics*, pages 311–366. Springer-Verlag, Berlin, Germany, 1971.
51. Z. Shmuely. The structure of Galois connections. *Pacific Journal of Mathematics*, 54(2):209–225, 1974.
52. A. Tarski. A lattice theoretical fixpoint theorem and its applications. *Pacific Journal of Mathematics*, 5:285–310, 1955.
53. R.J. van Glabbeek. The linear time – branching time spectrum (extended abstract). In J.C.M. Baeten and J.W. Klop, editors, *Proceedings of CONCUR'90, Theories of Concurrency: Unification and Extension*, Amsterdam, August 1990, vol. 458 of *Lecture Notes in Computer Science*, pages 278–297. Springer-Verlag, Berlin, Germany, 1990.
54. M. Ward. The closure operators of a lattice. *Annals of Mathematics*, 43:191–196, 1942.