URL: http://www.elsevier.nl/locate/entcs/volume6.html 24 pages

# Constructive Design of a Hierarchy of Semantics of a Transition System by Abstract Interpretation (Extended Abstract) ⋆

Patrick Cousot

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

**Abstract**

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

## 1 Introduction

The main idea of abstract interpretation is that program static analyzers effectively compute an approximation of the program semantics so that the specification of program analyzers should be formally derivable from the specification of the semantics [8]. The approximation process which is involved in this derivation has been formalized using Galois connections and/or widening narrowing operators [9]. The question of choosing which semantics one should start from in this calculation based development of the analyzer is not obvious: originally developed for small-step operational and predicate transformer semantics [10], the Galois connection based abstract interpretation theory was later extended to cope in the same way with denotational semantics [13]. In

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

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

## 2 Abstraction of Fixpoint Semantics

### 2.1 Fixpoint Semantics

A *fixpoint semantic specification* is a pair $\langle D, F\rangle$ where the *semantic domain* $\langle D, \sqsubseteq, \bot, \sqcup\rangle$ is a poset with partial order $\sqsubseteq$, infimum $\bot$ and partially defined least upper bound (lub) $\sqcup$ and the *semantic transformer* $F \in D \xmapsto{\mathrm{m}} D$ is a total monotone map from $D$ to $D$ assumed to be such that the transfinite *iterates of* $F$ *from* $\bot$, that is $F^0 = \bot$, $F^{\delta+1} = F(F^\delta)$ for successor ordinals $\delta+1$ and $F^\lambda = \bigsqcup_{\delta<\lambda} F^\delta$ for limit ordinals $\lambda$ are well-defined (e.g. when $\langle D, \sqsubseteq, \bot, \sqcup\rangle$ is a directed-complete partial order or DCPO [1]). By monotony, these iterates form an increasing chain, hence reach a fixpoint so that the *iteration order* can be defined as the least ordinal $\epsilon$ such that $F(F^\epsilon) = F^\epsilon$. This specifies the *fixpoint semantics* $S$ as the $\sqsubseteq$-least fixpoint $S = \mathrm{lfp}^{\sqsubseteq} F = F^\epsilon$ of $F$.

### 2.2 Fixpoint Semantics Transfer

In abstract interpretation, the *concrete semantics* $S^\natural$ is approximated by a (usually computable) *abstract semantics* $S^\sharp$ via an abstraction function $\alpha \in D^\natural \longmapsto D^\sharp$ such that $\alpha(S^\natural) \sqsubseteq^\sharp S^\sharp$ [1]. The abstraction is *exact* if $\alpha(S^\natural) = S^\sharp$ and *approximate* if $\alpha(S^\natural) \sqsubset^\sharp S^\sharp$. When the abstraction must be exact we can use the following fixpoint transfer theorem, which provide guidelines for designing $S^\sharp$ from $S^\natural$ (or dually) in fixpoint form [10, theorem 7.1.0.4(3)], [14, lemma 4.3], [2, fact 2.3] (as usual, we call a function $f$ *Scott-continuous*, written $f : D \xmapsto{\mathrm{c}} E$, if it is monotone and preserves the lub of any directed subset $A$ of $D$ [1], it is $\bot$-*strict* if $f(\bot) = \bot$):

**Theorem 2.1 (S. Kleene fixpoint transfer)** *Let* $\langle D^\natural, F^\natural\rangle$ *and* $\langle D^\sharp, F^\sharp\rangle$ *be concrete and abstract fixpoint semantic specifications. If the* $\bot$*-strict Scott-continuous abstraction function* $\alpha \in D^\natural \xmapsto{\bot,\mathrm{c}} D^\sharp$ *satisfies the* commutation condition $F^\sharp \circ \alpha = \alpha \circ F^\natural$ *then* $\alpha(\mathrm{lfp}^{\sqsubseteq^\natural} F^\natural) = \mathrm{lfp}^{\sqsubseteq^\sharp} F^\sharp$*. Moreover the respective iterates* $F^{\natural\delta}$ *and* $F^{\sharp\delta}$*,* $\delta \in \mathbb{O}$ *of* $F^\natural$ *and* $F^\sharp$ *from* $\bot^\natural$ *and* $\bot^\sharp$ *satisfy* $\forall \delta \in \mathbb{O}$*:* $\alpha(F^{\natural\delta}) = F^{\sharp\delta}$ *and the iteration order of* $F^\sharp$ *is less than or equal to that of* $F^\natural$*.*

Observe that in theorem 2.1, Scott-continuity of the abstraction function $\alpha$ is a too strong hypothesis since we only use the fact that $\alpha$ preserves the

[1] More generally, we look for an abstract semantics $S^\sharp$ such that $\alpha(S^\natural) \preceq^\sharp S^\sharp$ for the *approximation partial ordering* $\preceq^\sharp$ corresponding to logical implication which may differ from the *computational partial orderings* $\sqsubseteq$ used to define least fixpoints [13].

lub of the iterates of $F^\natural$ starting from $\bot^\natural$. When this is not the case, but $\alpha$ preserves glbs, we can use:

**Theorem 2.2 (A. Tarski fixpoint transfer)** *Let $\langle D^\natural,\ F^\natural\rangle$ and $\langle D^\sharp,\ F^\sharp\rangle$ be concrete and abstract fixpoint semantic specifications such that $\langle D^\natural,\ \sqsubseteq^\natural,\ \bot^\natural,\ \top^\natural,\ \sqcup^\natural,\ \sqcap^\natural\rangle$ and $\langle D^\sharp,\ \sqsubseteq^\sharp,\ \bot^\sharp,\ \top^\sharp,\ \sqcup^\sharp,\ \sqcap^\sharp\rangle$ are complete lattices. If the abstraction function $\alpha \in D^\natural \overset{\sqcap}{\longmapsto} D^\sharp$ is a complete $\sqcap$-morphism satisfying the* commutation inequality $F^\sharp \circ \alpha \sqsubseteq^\sharp \alpha \circ F^\natural$ *and the* post-fixpoint correspondence $\forall y \in D^\sharp : F^\sharp(y) \sqsubseteq^\sharp y \Longrightarrow \exists x \in D^\natural : \alpha(x) = y \wedge F^\natural(x) \sqsubseteq^\natural x$ *then* $\alpha(\mathrm{lfp}^{\sqsubseteq^\natural} F^\natural) = \mathrm{lfp}^{\sqsubseteq^\sharp} F^\sharp$.

## *2.3 Semantics Abstraction*

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

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

which means that $\langle D^\natural,\ \sqsubseteq^\natural\rangle$ and $\langle D^\sharp,\ \sqsubseteq^\sharp\rangle$ are posets, $\alpha \in D^\natural \longmapsto D^\sharp$, $\gamma \in D^\sharp \longmapsto D^\natural$, and $\forall x \in D^\natural : \forall y \in D^\sharp : \alpha(x) \sqsubseteq^\sharp y \iff x \sqsubseteq^\natural \gamma(y)$. If $\alpha$ is surjective (resp. injective, bijective) then we have a *Galois insertion* written $\underset{\alpha}{\overset{\gamma}{\substack{\longleftarrow \\ \twoheadrightarrow}}}$ (resp. *embedding*[2] written $\underset{\alpha}{\overset{\gamma}{\substack{\twoheadleftarrow \\ \longrightarrow}}}$, *bijection* written $\underset{\alpha}{\overset{\gamma}{\substack{\twoheadleftarrow \\ \twoheadrightarrow}}}$). The use of Galois connections in abstract interpretation was motivated by the fact that $\alpha(x)$ is the best possible approximation of $x \in D^\natural$ within $D^\sharp$ [9,10]. We often use the fact that Galois connections compose[3]. If $\langle D^\flat,\ \sqsubseteq^\flat\rangle \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \langle D^\natural,\ \sqsubseteq^\natural\rangle$ and $\langle D^\natural,\ \sqsubseteq^\natural\rangle \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \langle D^\sharp,\ \sqsubseteq^\sharp\rangle$ then $\langle D^\flat,\ \sqsubseteq^\flat\rangle \underset{\alpha_2\circ\alpha_1}{\overset{\gamma_1\circ\gamma_2}{\leftrightarrows}} \langle D^\sharp,\ \sqsubseteq^\sharp\rangle$. Finally, to reason by duality, observe that the dual of $\langle D^\natural,\ \sqsubseteq^\natural\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle D^\sharp,\ \sqsubseteq^\sharp\rangle$ is $\langle D^\sharp,\ \sqsupseteq^\sharp\rangle \underset{\gamma}{\overset{\alpha}{\leftrightarrows}} \langle D^\natural,\ \sqsupseteq^\natural\rangle$.

## *2.4 Fixpoint Semantics Fusion*

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

**Theorem 2.3 (Fixpoint fusion)** *Let $D^+$, $D^\omega$ be a partition of $D^\infty$ and $\langle\wp(D^+),\ F^+\rangle$ and $\langle\wp(D^\omega),\ F^\omega\rangle$ be fixpoint semantic specifications. Partially*

---

[2] If $\alpha$ and $\gamma$ are Scott-continuous then this is an embedding-projection pair.

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

*define:*

$$X^+ = X \cap D^+, \qquad \bot^\infty = \bot^+ \cup \bot^\omega,$$

$$X^\omega = X \cap D^\omega, \qquad \top^\infty = \top^+ \cup \top^\omega,$$

$$F^\infty(X) = F^+(X^+) \cup F^\omega(X^\omega), \qquad \bigsqcup_{i\in}^{\infty} X_i = \bigsqcup_{i\in}^{+} X^+ \cup \bigsqcup_{i\in}^{\omega} X_i{}^\omega,$$

$$X \sqsubseteq^\infty Y = X^+ \sqsubseteq^+ Y^+ \wedge X^\omega \sqsubseteq^\omega Y^\omega, \qquad \bigsqcap_{i\in}^{\infty} X_i = \bigsqcap_{i\in}^{+} X^+ \cup \bigsqcap_{i\in}^{\omega} X_i{}^\omega \ .$$

*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 $F^\omega$ are monotone (resp. Scott-continuous, a complete $\sqcup$-morphism) then so is $F^\infty$. In all cases, $\mathrm{lfp}^{\sqsubseteq^\infty} F^\infty = \mathrm{lfp}^{\sqsubseteq^+} F^+ \cup \mathrm{lfp}^{\sqsubseteq^\omega} F^\omega$.*

### *2.5 Fixpoint Iterates Reordering*

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

**Theorem 2.4 (Fixpoint iterates reordering)** *Let $\langle\langle D,\ \sqsubseteq,\ \bot,\ \sqcup\rangle,\ F\rangle$ be a fixpoint semantic specification (the iterates of $F$, i.e. $F^0 = \bot$, $F^{\delta+1} = F(F^\delta)$ for successor ordinals $\delta+1$ and $F^\lambda = \bigsqcup_{\delta<\lambda} F^\delta$ for limit ordinals $\lambda$, being well-defined). Let $E$ be a set and $\preceq$ be a binary relation on $E$, such that:*

(i) *$\preceq$ is a pre-order on $E$;*

(ii) *all iterates $F^\delta$, $\delta \in \mathbb{O}$ of $F$ belong to $E$;*

(iii) *$\bot$ is the $\preceq$-infimum of $E$;*

(iv) *the restriction $F|_E$ of $F$ to $E$ is $\preceq$-monotone;*

(v) *for all $x \in E$, if $\lambda$ is a limit ordinal and $\forall \delta < \lambda : F^\delta \preceq x$ then $\bigsqcup_{\delta<\lambda} F^\delta \preceq x$.*

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

## 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 $\langle\ ,\ \tau\rangle$ where is a (non-empty) set of states[4], $\tau \subseteq\ \times\ $ 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 $\wp(\ \times\ ) \simeq (\ \times\ ) \longmapsto \mathbb{B}$ where $\mathbb{B} = \{\mathrm{tt}, \mathrm{ff}\}$ is the set of booleans. $\check{\tau} = \{s \in\ \mid \forall s' \in\ : \neg(s\ \tau\ s')\}$ is the set of *final/blocking states.*

[4] We could also consider actions as in process algebra [25].

# 4 Finite and Infinite Sequences

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

### 4.1 Sequences

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

### 4.2 Concatenation and Junction of Sequences

The *concatenation* of sequences $\eta, \xi \in A^{\vec{\propto}}$ is $\eta \cdot \xi = \eta$ when $|\eta| = \omega$ whereas it is $\eta \cdot \xi = \eta_0 \ldots \eta_{n-1}\xi_0\xi_1 \ldots$ when $|\eta| = n$. The empty sequence is neutral $\vec{\epsilon} \cdot \eta = \eta \cdot \vec{\epsilon} = \eta$. The concatenation extends to sets of sequences $A$ and $B \in \wp(A^{\vec{\propto}})$ by $A \cdot B = \{\eta \cdot \xi \mid \eta \in A \wedge \xi \in B\}$.

Non-empty sequences $\eta, \xi \in A^{\vec{\infty}}$ are *joinable*, written $\eta \mathrel{\overset{\frown}{?}} \xi$, if $|\eta| = \omega$ in which case the *join* $\eta \frown \xi$ is $\eta$ or $|\eta| = n$ and $\eta_{n-1} = \xi_0$ in which case the join $\eta \frown \xi$ is $\eta_0 \ldots \eta_{n-1}\xi_1\xi_2 \ldots$. The junction of sets $A$ and $B \in \wp(A^{\vec{\infty}})$ of non-empty sequences is $A \frown B = \{\eta \frown \xi \mid \eta \in A \wedge \xi \in B \wedge \eta \mathrel{\overset{\frown}{?}} \xi\}$.

# 5 Maximal Trace Semantics

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

### 5.1 Fixpoint Finite Trace Semantics

The *finite trace semantics* $\tau^{\vec{+}}$ can be presented in unique fixpoint form as follows [12, example 17] ($\mathrm{lfp}_a^{\sqsubseteq}$ is the $\sqsubseteq$-least fixpoint of $F$ greater than or equal to $a$, if it exists and dually, $\mathrm{gfp}_a^{\sqsubseteq} = \mathrm{lfp}_a^{\sqsupseteq}$ is the $\sqsubseteq$-greatest fixpoint of $F$ less than or equal to $a$, if it exists):

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

### 5.2 Fixpoint Infinite Trace Semantics

The *infinite trace semantics* $\tau^{\vec{\omega}}$ can be presented in $\subseteq$-greatest fixpoint form as follows [12, example 20]:

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

### 5.3 Fixpoint Maximal Trace Semantics

By the fixpoint fusion theorem 2.3 and fixpoint theorems 5.1 and 5.2, the *maximal trace semantics* $\tau^{\vec{\infty}}$ can now be presented in two different fixpoint forms, as follows [12, examples 21 & 28]:

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

The non-determinism of the transition system $\langle ,\ \tau \rangle$ may be unbounded. Observe that this does not imply absence of Scott-continuity of the transformer $F^{\vec{\infty}}$ of the fixpoint semantics $\tau^{\vec{\infty}} = \mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\perp^{\vec{\infty}}}\, F^{\vec{\infty}}$, as already observed by [4] using program execution trees.

One may wonder why, following [12], we have characterized the trace semantics as $\tau^{\vec{\infty}} = \mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\perp^{\vec{\infty}}}\, F^{\vec{\infty}}$ while $\tau^{\vec{\infty}} = \mathrm{gfp}^{\subseteq}_{\vec{\infty}}\, F^{\vec{\infty}}$ is both more frequently used in the literature (e.g. [3]) and apparently simpler. This is because $\tau^{\vec{\infty}} = \mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\perp^{\vec{\infty}}}\, F^{\vec{\infty}}$ may lift to further abstractions while $\tau^{\vec{\infty}} = \mathrm{gfp}^{\subseteq}_{\vec{\infty}}\, F^{\vec{\infty}}$ does not. For an example, let us consider potential termination.

### 5.4 Potential Termination Semantics

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

**Theorem 5.4 (Fixpoint potential termination semantics)** $\tau^{\trianglelefteq} = \mathrm{lfp}^{\subseteq}_{\emptyset}\, F^{\trianglelefteq}$ *where* $F^{\trianglelefteq} \in \wp() \overset{\cup}{\longmapsto} \wp()$ *defined as* $F^{\trianglelefteq}(X) = \check{\tau} \cup \tau^{\blacktriangleleft}(X)$ *is a complete* $\cup$*-morphism on the complete lattice* $\langle \wp(),\ \subseteq,\ \emptyset,\ ,\ \cup,\ \cap \rangle$.

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

# 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 $\langle \wp(^{\vec{\infty}}),\, \subseteq\rangle \underset{\alpha^{\tau}}{\overset{\gamma^{\tau}}{\leftrightarrows}} \langle \wp(\ \times\ ),\, \subseteq\rangle$ where the abstraction collects possible transitions $\alpha^{\tau}(T) = \{\langle s,\, s'\rangle \mid \exists \sigma \in {}^{\vec{\star}} : \exists \sigma' \in {}^{\vec{\infty}} : \sigma \cdot ss' \cdot \sigma' \in T\}$ while the concretization builds maximal execution traces $\gamma^{\tau}(t) = t^{\vec{\infty}}$. 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 [26], possibly using D. Scott's bottom $\perp \notin$ to denote non-termination [23]. It is an abstraction of the maximal trace semantics where intermediate computation states are ignored.

## *7.1 Finite/Angelic Relational Semantics*

The *finite/angelic relational semantics* (also called big-step operational semantics by G. Plotkin [32], natural semantics by G. Kahn [22], relational semantics by R. Milner & M. Tofte [26] and evaluation semantics by A. Pitts [31]) is $\tau^{+} = \alpha^{+}(\tau^{\vec{+}})$ where the Galois insertion $\langle \wp(^{\vec{+}}),\, \subseteq\rangle \underset{\alpha^{+}}{\overset{\gamma^{+}}{\leftrightarrows}} \langle \wp(\ \times\ ),\, \subseteq\rangle$ is defined by $\alpha^{+}(X) = \{@^{+}(\sigma) \mid \sigma \in X\}$ and $\gamma^{+}(Y) = \{\sigma \mid @^{+}(\sigma) \in Y\}$ where $@^{+} \in {}^{\vec{+}} \longmapsto (\ \times\ )$ is $@^{+}(\sigma) = \langle \sigma_0,\, \sigma_{n-1}\rangle$, for all $\sigma \in {}^{\vec{n}}$, $n \in \mathbb{N}$. Using S. Kleene fixpoint transfer 2.1 and theorem 5.1, we can express $\tau^{+}$ in fixpoint form ($\bar{\tau} = \{\langle s,\, s\rangle \mid s \in \check{\tau}\}$ is the set of final/blocking state pairs):

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

Observe that A. Tarski fixpoint transfer theorem 2.2 is not applicable since $\alpha^{+}$ 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 $X^k = \{a^n b \mid n \geq k\}, k > 0$ 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 $\alpha^{+}(\bigcap_{k>0} X^k) = \alpha^{+}(\emptyset) = \emptyset$.

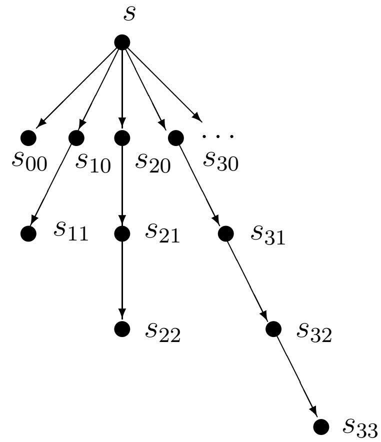



Fig. 1. Transition system with unbounded nondeterminism

### *7.2 Infinite Relational Semantics*

The *infinite relational semantics* is $\tau^\omega = \alpha^\omega(\tau^{\varpi})$ where the Galois insertion $\langle \wp(^{\varpi}),\ \subseteq\rangle \xrightarrow[\alpha^\omega]{\gamma^\omega} \langle \wp(\ \times \{\bot\}),\ \subseteq\rangle$ is defined by $\alpha^\omega(X) = \{@^\omega(\sigma) \mid \sigma \in X\}$ and $\gamma^\omega(Y) = \{\sigma \mid @^\omega(\sigma) \in Y\}$ where $@^\omega \in {}^{\varpi} \longmapsto (\ \times \{\bot\})$ is $@^\omega(\sigma) = \langle \sigma_0,\ \bot\rangle$.

By the Galois connection, $\alpha^\omega$ is a complete $\cup$-morphism. It is a $\cap$-morphism but <u>not</u> co-continuous. A counter-example is given by the $\subseteq$-decreasing chain $X^k = \{a^n b^\omega \mid n \geq k\}$, $k > 0$ such that $\bigcap\limits_{k>0} \alpha^\omega(X^k) = \bigcap\limits_{k>0}\{\langle a,\ \bot\rangle\} = \{\langle a,\ \bot\rangle\}$ while $\bigcap\limits_{k>0} X^k = \emptyset$ since $a^n b^\omega \in \bigcap\limits_{k>0} X^k$ for $n > 0$ is in contradiction with $a^n b^\omega \notin X^{n+1}$ whence $\alpha^\omega(\bigcap\limits_{k>0} X^k) = \alpha^\omega(\emptyset) = \emptyset$. Using A. Tarski fixpoint transfer theorem 2.2 and theorem 5.2, we get:

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

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

**Example 7.3 (Unbounded nondeterminism)** Let us consider the transition system $\langle\ ,\ \tau\rangle$ of figure 1 such that $\ = \{s\} \cup \{s_{ij} \mid i, j \in \mathbb{N} \wedge 0 \leq j \leq i\}$ (where $s \neq s_{ij} \neq s_{k\ell}$ whenever $i \neq k$ or $j \neq \ell$) and $\tau = \{\langle s,\ s_{i0}\rangle \mid i \in \mathbb{N}\} \cup \{\langle s_{ij},\ s_{i(j+1)}\rangle \mid 0 \leq j < i\}$ [36].

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

It follows that S. Kleene fixpoint transfer theorem 2.1 is not applicable to prove theorem 7.2 since otherwise the convergence of the iterates of $F^\omega$ would be as fast as those of $F^{\varpi}$, hence would be stable at $\omega$.

### *7.3 Inevitable Termination Semantics*

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

The *right image* of $s \in$ by a relation $\tau \subseteq \times '$ is $\tau^{\bullet\blacktriangleright}(s) = \{s' \mid s\ \tau\ s'\}$ (in particular if $f \in \longmapsto '$ then $f^{\bullet\blacktriangleright}(s) = \{f(s)\}$) while for $P \subseteq$ , $\tau^{\blacktriangleright}(P) = \{s' \mid \exists s \in P : s\ \tau\ s'\}$ (in particular, $f^{\blacktriangleright}(P) = \{f(s) \mid s \in P\}$). The *inverse* of $\tau$ is $\tau^{-1} = \{\langle s',\, s\rangle \mid s\ \tau\ s'\}$ so that $\tau^{\blacktriangleleft\bullet} = (\tau^{-1})^{\bullet\blacktriangleright}$ and $\tau^{\blacktriangleleft} = (\tau^{-1})^{\blacktriangleright}$. The dual of a map $F \in \wp() \longmapsto \wp(')$ is $\widetilde{F} = \lambda P \bullet \neg F(\neg P)$. Finally, $\widetilde{\tau^{-1\blacktriangleright}}(P) = \{s' \mid \forall s : s'\ \tau\ s \Longrightarrow s \in P\}$. Applying the semi-dual of S. Kleene fixpoint transfer theorem 2.1 to the fixpoint characterization 7.2 of the infinite relational semantics $\tau^{\omega}$, we get the

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

### *7.4 Natural Relational Semantics*

We now mix together the descriptions of the finite and infinite executions of a transition system $\langle ,\, \tau\rangle$. The *natural relational semantics* $\tau^{\infty} = \tau^{+} \cup \tau^{\omega}$ is the fusion of the finite relational semantics $\tau^{+}$ and the infinite relational semantics $\tau^{\omega}$. It is more traditional [5,30] to consider the product of the finite relational semantics $\tau^{+}$ and the inevitable termination semantics $\tau^{\lhd}$. The reason for preferring the infinite relational semantics to the inevitable termination semantics 7.4 is that the fixpoint characterizations 7.1 of $\tau^{+}$ and 7.2 of $\tau^{\omega}$ fuse naturally by the fixpoint fusion theorem 2.3. This leads to a simple fixpoint characterization of the natural relational semantics using the *mixed ordering* $\sqsubseteq^{\infty}$ first introduced in [12, proposition 25]:

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

By defining $\alpha^{\infty}(X) = \alpha^{+}(X^{+}) \cup \alpha^{\omega}(X^{\omega})$, we have $\tau^{\infty} = \alpha^{\infty}(\tau^{\vec{\infty}})$. Neither S. Kleene fixpoint transfer theorem 2.1 nor A. Tarski fixpoint transfer theorem 2.2 is directly applicable to derive that $\tau^{\infty} = \alpha^{\infty}(\mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\bot^{\vec{\infty}}}\, F^{\vec{\infty}}) = \mathrm{lfp}^{\sqsubseteq^{\infty}}_{\bot^{\infty}}\, F^{\infty}$. Observe however that we proceeded by fusion of independent parts, using $\alpha^{+}$ to transfer the finitary part $\tau^{\vec{+}}$ by S. Kleene fixpoint transfer theorem 2.1 (but A. Tarski's one was not applicable) and the infinitary part $\tau^{\vec{\omega}}$ by A. Tarski fixpoint transfer theorem 2.2 (but S. Kleene's one was not applicable).

### *7.5 Demoniac Relational Semantics*

The *demoniac relational semantics* is derived from the natural relational semantics by approximating nontermination by chaos: $\tau^\partial = \alpha^\partial(\tau^\infty)$ where $\alpha^\partial(X) = X \cup \{\langle s,\ s'\rangle \mid \langle s,\ \perp\rangle \in X \wedge s' \in \ \}$ and $\gamma^\partial(Y) = Y$ so that $\langle\wp(\ \times\ _\perp),\ \subseteq\rangle \xleftarrow[\alpha^\partial]{\gamma^\partial} \langle D^\partial,\ \subseteq\rangle$ where $D^\partial = \{Y \in \wp(\ \times\ _\perp) \mid \forall s \in\ : \langle s,\ \perp\rangle \in Y \Longrightarrow (\forall s \in\ : \langle s,\ s'\rangle \in Y)\}$. By definition of $\tau^\partial$, fixpoint characterization of the natural relational semantics 7.5 and S. Kleene fixpoint transfer theorem 2.1, we derive:

**Theorem 7.6 (Fixpoint demoniac relational semantics)** $\tau^\partial = \mathrm{lfp}^{\sqsubseteq^\partial}_{\perp^\partial} F^\partial$ *where* $F^\partial \in D^\partial \stackrel{m}{\longmapsto} D^\partial$ *defined as* $F^\partial(X) = \bar{\tau} \cup \tau \circ X$ *is a* $\sqsubseteq^\partial$*-monotone map on the complete lattice* $\langle D^\partial,\ \sqsubseteq^\partial,\ \perp^\partial,\ \top^\partial,\ \sqcup^\partial,\ \sqcap^\partial\rangle$ *with* $X \sqsubseteq^\partial Y = \forall s \in\ : \langle s,\ \perp\rangle \in X \vee (\langle s,\ \perp\rangle \notin Y \wedge X \cap (\{s\} \times\ ) \subseteq Y \cap (\{s\} \times\ ))$, $\perp^\partial = \ \times\ _\perp$, $\top^\partial = \ \times\ $, $\bigsqcup^\partial_{i\in} X_i = \{\langle s,\ s'\rangle \mid (\forall i \in\ : \langle s,\ \perp\rangle \in X_i \wedge s' \in\ _\perp) \vee (\exists i \in\ : \langle s,\ \perp\rangle \notin X_i \wedge \langle s,\ s'\rangle \in X_i)\}$ *and* $\bigsqcap^\partial_{i\in} X_i = \{\langle s,\ s'\rangle \mid (\exists i \in\ : \langle s,\ \perp\rangle \in X_i \wedge s' \in\ _\perp) \vee (\forall i \in\ : \langle s,\ \perp\rangle \notin X_i \wedge \langle s,\ s'\rangle \in X_i)\}$.

*Moreover* $X \sqsubseteq^\partial Y = \gamma^{\eth}(X) \sqsubseteq^\infty \gamma^{\eth}(Y)$ *where* $\gamma^{\eth}(X) = \{\langle s,\ \perp\rangle \mid \langle s,\ \perp\rangle \in X\} \cup \{\langle s,\ s'\rangle \mid \langle s,\ \perp\rangle \notin X \wedge \langle s,\ s'\rangle \in X\}$ *so that* $\langle\wp(\ \times\ _\perp),\ \sqsupseteq^\infty\rangle \xleftarrow[\alpha^\partial]{\gamma^{\eth}} \langle D^\partial,\ \sqsupseteq^\partial\rangle$.

**Lemma 7.7 (Arrangement of the iterates of $F^\partial$)** *Let* $F^{\partial\,\beta}$, $\beta \in \mathbb{O}$ *be the iterates of* $F^\partial$ *from* $\perp^\partial$. *For all* $\eta < \xi$, $s, s' \in\ $, *if* $\langle s,\ s'\rangle \in F^{\partial\,\xi}$ *and* $\langle s,\ s'\rangle \notin F^{\partial\,\eta}$ *then* $\forall s' \in\ _\perp : \langle s,\ s'\rangle \in F^{\partial\,\eta}$.

**Lemma 7.8 (Final states of the iterates of $F^\partial$)** *Let* $F^{\partial\,\beta}$, $\beta \in \mathbb{O}$ *be the iterates of* $F^\partial$ *from* $\perp^\partial$. $\forall \beta \in \mathbb{O} : \forall s, s' \in\ : (\langle s,\ s'\rangle \in F^{\partial\,\beta} \wedge \langle s,\ \perp\rangle \notin F^{\partial\,\beta}) \Longrightarrow (s' \in \check{\tau}) \wedge (\forall s'' \in\ _\perp : \langle s',\ s''\rangle \in F^{\partial\,\delta} \Longrightarrow s'' = s')$.

In order to place the demoniac relational semantics $\tau^\partial$ in the hierarchy of semantics, we will use the following:

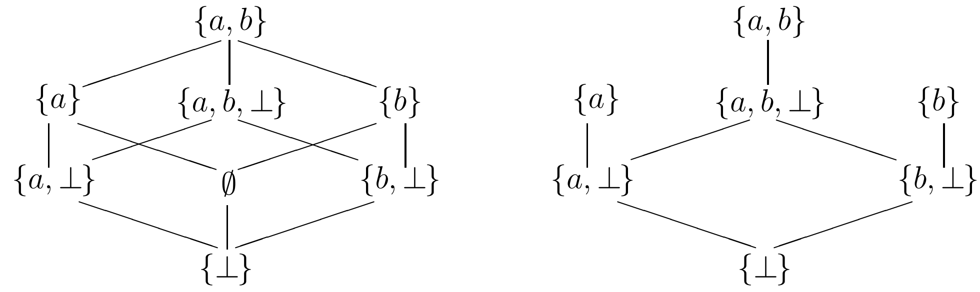
**Theorem 7.9** $\tau^\omega = \alpha^{\partial\,\omega}(\tau^\partial)$ *where* $\alpha^{\partial\,\omega}(X) = X \cap (\ \times \{\perp\})$.

## 8 Denotational Semantics

In contrast to operational semantics, denotational semantics abstracts away from the history of computations by considering input-output functions [33]. For that purpose, given any partial order $\leqslant$ on $\wp(\mathcal{D}\times\mathcal{E})$, we use the right-image isomorphism: $\langle\wp(\mathcal{D}\times\mathcal{E}),\ \leqslant\rangle \xleftarrow[\alpha^\blacktriangleright]{\gamma^\blacktriangleright} \langle\mathcal{D} \longmapsto \wp(\mathcal{E}),\ \dot{\leqslant}\rangle$ where $\alpha^\blacktriangleright(R) = R^\blacktriangleright = \lambda x \bullet \{y \mid \langle x,\ y\rangle \in R\}$, $\gamma^\blacktriangleright(f) = \{\langle x,\ y\rangle \mid y \in f(x)\}$ and $f \mathrel{\dot{\leqslant}} g = \gamma^\blacktriangleright(f) \leqslant \gamma^\blacktriangleright(g)$.

### *8.1 Nondeterministic Denotational Semantics*

Our initial goal was to derive the nondeterministic denotational semantics of [2] by abstract interpretation of the trace semantics (in a succinct form,




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

Fig. 2.

using transition systems instead of imperative iterative programs). Surprisingly enough, we obtain *new* fixpoint characterizations using different partial orderings.

### *8.1.1 Natural Nondeterministic Denotational Semantics*

The *natural nondeterministic denotational semantics* is defined as the right-image abstraction $\tau^\natural = \alpha^{\blacktriangleright}(\tau^\infty)$ of the natural relational semantics $\tau^\infty$. By the fixpoint characterization 7.5 of $\tau^\infty$ and S. Kleene fixpoint transfer theorem 2.1, we derive a fixpoint characterization of the fixpoint natural nondeterministic denotational semantics (where $\dot{\check{\tau}} = \lambda s \bullet \{s \mid \forall s' \in \ : \neg(s\ \tau\ s')\}$):

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

**Lemma 8.2 (Totality of the iterates of $F^\natural$)** *Let* ${F^\natural}^\delta$, $\delta \in \mathbb{O}$ *be the iterates of* $F^\natural$ *from* $\bot^\natural$. $\forall \delta \in \mathbb{O} : \forall s \in \ : {F^\natural}^\delta(s) \neq \emptyset$.

### *8.1.2 Convex/Plotkin Nondeterministic Denotational Semantics*

Unexpectedly, the natural semantic domain $D^\natural = \wp(_\bot)$ with the mixed ordering $\sqsubseteq^\natural$ differs from the usual convex/Plotkin powerdomain with Egli-Milner ordering $\sqsubseteq^{\mathrm{EM}}$ [19] (see figure 2). Apart from the presence of $\emptyset$ (which can be easily eliminated), the difference is that $\sqsubseteq^{\mathrm{EM}} \subsetneq \sqsubseteq^\natural$ which can be useful, e.g. to define the semantics of the parallel **or** as $[\![f \ \mathbf{or}\ g]\!] = \lambda\rho \bullet [\![f]\!]\,\rho \sqcup^\natural [\![g]\!]\,\rho$ [5].

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 [2, fact 2.4] that G. Plotkin convex powerdomain $\langle D^{\mathrm{EM}}, \sqsubseteq^{\mathrm{EM}}, \bot^{\mathrm{EM}}, \sqcup^{\mathrm{EM}} \rangle$ is the DCPO $\{A \subseteq \ _\bot \mid A \neq \emptyset\}$ with Egli-Milner ordering $A \sqsubseteq^{\mathrm{EM}} B = \forall a \in A : \exists b \in B : a \sqsubseteq^{\mathrm{D}} b \wedge \forall b \in B : \exists a \in A : a \sqsubseteq^{\mathrm{D}} b$ based upon D. Scott flat ordering

[5] Observe that $\sqcup^\natural$ is monotonic for $\sqsubseteq^\natural$ which is not in contradiction with [6] since by lemma 8.2 failure is excluded i.e. would have to be explicitly denoted by $\notin$ .

$\forall x \in {}_\perp : \perp \sqsubseteq^{\mathrm{D}} x \sqsubseteq^{\mathrm{D}} x$ such that $A \sqsubseteq^{\mathrm{EM}} B \iff (\perp \in A \;?\; A \setminus \{\perp\} \subseteq B \;¿\; A = B)$, with infimum $\perp^{\mathrm{EM}} = \{\perp\}$ and lub of increasing chains $\bigsqcup^{\mathrm{EM}}_{i\in} X_i = (\bigcup_{i\in} X_i \setminus \{\perp\}) \cup \{\perp \mid \forall i \in \; : \perp \in X_i\}$. Applying the fixpoint iterates reordering theorem 2.4 to theorem 8.1, we get [2]:

**Corollary 8.3 (G. Plotkin fixpoint nondeterministic denotational semantics)** $\tau^\natural = \mathrm{lfp}^{\dot\sqsubseteq^{\mathrm{EM}}}_{\dot\perp^{\mathrm{EM}}} F^\natural$ *where* $F^\natural$ *is a* $\dot\sqsubseteq^{\mathrm{EM}}$*-monotone map on the pointwise extension* $\langle \dot D^{\mathrm{EM}}, \dot\sqsubseteq^{\mathrm{EM}}, \dot\perp^{\mathrm{EM}}, \dot\sqcup^{\mathrm{EM}}\rangle$ *of G. Plotkin convex powerdomain* $\langle D^{\mathrm{EM}}, \sqsubseteq^{\mathrm{EM}}, \perp^{\mathrm{EM}}, \sqcup^{\mathrm{EM}}\rangle$.

*8.1.3 Demoniac Nondeterministic Denotational Semantics*

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

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

**Theorem 8.4 (Denotational demoniac abstraction)** $\tau^\sharp = \alpha^\sharp(\tau^\natural)$ *where* $\alpha^\sharp(f) = \lambda s \bullet f(s) \cup \{s' \in \; \mid \perp \in f(s)\}$ *and* $\gamma^\sharp(g) = g$ *satisfies* $\langle \; \longmapsto \wp({}_\perp), \dot\subseteq\rangle \xrightleftharpoons[\alpha^\sharp]{\gamma^\sharp} \langle \; \longmapsto (\wp() \cup \{{}_\perp\}), \dot\subseteq\rangle$.

Let us recall the properties of lifting:

**Lemma 8.5 (Lifting)** *Given a complete lattice* $\langle D, \sqsubseteq, \perp, \top, \sqcup, \sqcap\rangle$ *(respectively poset* $\langle D, \sqsubseteq, \sqcup\rangle$*, DCPO* $\langle D, \sqsubseteq, \perp, \sqcup\rangle$*), the* lift of $D$ by $\pm \not\in D$ *is the complete lattice (resp. poset, DCPO)* $\langle D_\pm, \preceq, \pm, \top, \coprod, \prod\rangle$ *with* $D_\pm = D \cup \{\pm\}$, $x \preceq y = (x = \pm) \vee (y \in D \wedge x \sqsubseteq y)$*, infimum* $\pm$*, supremum* $\top$*, join* $\coprod_{i\in} X_i = (\forall i \in \; : X_i = \pm \;?\; \pm \;¿\; \sqcup\{X_i \mid i \in \; \wedge X_i \neq \pm\})$ *and the meet is* $\prod_{i\in} X_i = (\exists i \in \; : X_i = \pm \;?\; \pm \;¿\; \sqcap\{X_i \mid i \in \; \wedge X_i \neq \pm\})$.

By the fixpoint characterization 7.6 of $\tau^\partial$ and S. Kleene fixpoint transfer theorem 2.1, we get:

**Theorem 8.6 (Fixpoint demoniac nondeterministic denotational semantics)** $\tau^\sharp = \mathrm{lfp}^{\dot\sqsubseteq^\sharp}_{\dot\perp^\sharp} F^\sharp$ *where* $F^\sharp(f) = \dot\tau \;\dot\cup\; \dot\bigcup f^\blacktriangleright \circ \tau^{\blacktriangleright}$ *is a* $\dot\sqsubseteq^\sharp$*-monotone map on the pointwise extension* $\langle \dot D^\sharp, \dot\sqsubseteq^\sharp, \dot\perp^\sharp, \dot\top^\sharp, \dot\sqcup^\sharp, \dot\sqcap^\sharp\rangle$ *of the lift* $\langle D^\sharp, \sqsubseteq^\sharp, \perp^\sharp, \top^\sharp, \sqcup^\sharp, \sqcap^\sharp\rangle$ *of the complete lattice* $\langle \wp(), \subseteq, \emptyset, \;, \cup, \cap\rangle$ *by the infimum* ${}_\perp$.

**Lemma 8.7 (Totality of the iterates of** $F^\sharp$**)** *Let* $F^{\sharp\delta}$, $\delta \in \mathbb{O}$ *be the iterates of* $F^\sharp$ *from* $\dot\perp^\sharp$. $\forall \delta \in \mathbb{O} : \forall s \in \; : F^{\sharp\delta}(s) \neq \emptyset$.

From theorem 8.6, lemma 8.7 and the fixpoint iterates reordering theorem 2.4, we deduce another fixpoint characterization of $F^\sharp(f)$ with a different partial ordering:

**Corollary 8.8 (Reordered fixpoint demoniac nondeterministic denotational semantics)** $\tau^\sharp = \mathrm{lfp}^{\dot\sqsubseteq^\Diamond}_{\dot\perp^\Diamond} F^\sharp$ *where* $F^\sharp(f) = \dot\tau \;\dot\cup\; \dot\bigcup f^\blacktriangleright \circ \tau^{\blacktriangleright}$ *is a*

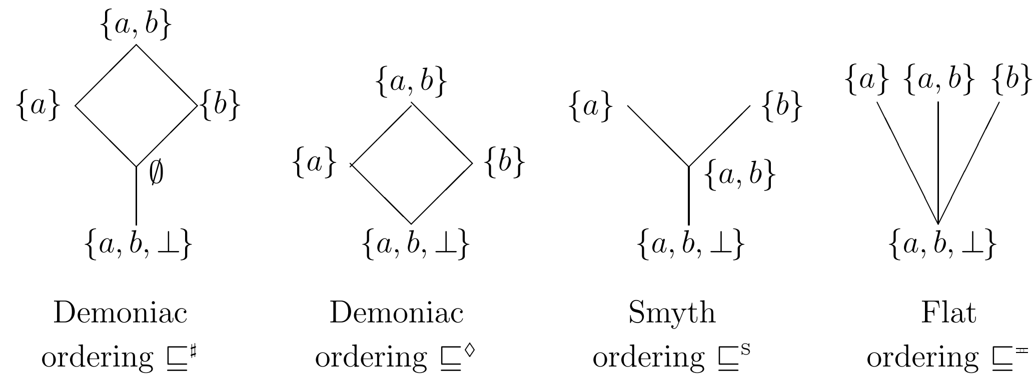



Fig. 3.

*$\dot{\sqsubseteq}^{\Diamond}$-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 $D^{\Diamond} = (\wp() \setminus \{\emptyset\}) \cup \{\bot^{\Diamond}\}$, $\bot^{\Diamond} = {}_{\bot}$ and $X \sqsubseteq^{\Diamond} Y = (X = \bot^{\Diamond}) \vee (X \subseteq Y)$.*

### *8.1.4 Upper/Smyth Nondeterministic Denotational Semantics*

Unforeseenly, the demoniac semantic domain $D^{\sharp}$ with the demoniac ordering $\sqsubseteq^{\sharp}$ differs from the usual upper powerdomain with M. Smyth ordering [19] $\sqsubseteq^{\mathrm{S}}$ (see figure 3). Let us recall [2, fact 2.7] that M. Smyth upper powerdomain $\langle D^{\mathrm{S}},\ \sqsubseteq^{\mathrm{S}},\ \bot^{\mathrm{S}},\ \sqcap^{\mathrm{S}},\ \sqcup^{\mathrm{S}}\rangle$ is $D^{\mathrm{S}} = \{A \subseteq \ \mid A \neq \emptyset\} \cup \{{}_{\bot}\}$ ordered by the superset ordering $A \sqsubseteq^{\mathrm{S}} B = A \supseteq B$ which is a poset with infimum $\bot^{\mathrm{S}} = {}_{\bot}$, the glb of nonempty families $X_i$, $i \in$ always exist being given by $\bigsqcap^{\mathrm{S}}_{i\in} X_i = \bigcup_{i\in} X_i$ and if $X_i$, $i \in$ has an upper bound, its lub exists and is $\bigsqcup^{\mathrm{S}}_{i\in} X_i = \bigcap_{i\in} X_i$. By applying the fixpoint iterates reordering theorem 2.4 to 8.6, we get [2]:

**Corollary 8.9 (M. Smyth fixpoint nondeterministic denotational semantics)** *$\tau^{\sharp} = \mathrm{lfp}^{\dot{\sqsubseteq}^{\mathrm{S}}}_{\dot{\bot}^{\mathrm{S}}} F^{\sharp}$ where $F^{\sharp}$ is a $\dot{\sqsubseteq}^{\mathrm{S}}$-monotone map on the pointwise extension $\langle \dot{D}^{\mathrm{S}},\ \dot{\sqsubseteq}^{\mathrm{S}},\ \dot{\bot}^{\mathrm{S}},\ \dot{\sqcap}^{\mathrm{S}},\ \dot{\sqcup}^{\mathrm{S}}\rangle$ of M. Smyth upper powerdomain $\langle D^{\mathrm{S}},\ \sqsubseteq^{\mathrm{S}},\ \bot^{\mathrm{S}},\ \sqcap^{\mathrm{S}},\ \sqcup^{\mathrm{S}}\rangle$.*

### *8.1.5 Minimal Demoniac Nondeterministic Denotational Semantics*

M. Smyth ordering $\dot{\sqsubseteq}^{\mathrm{S}}$ is not *minimal* since, for example on figure 3, $\{a\}$ and $\{a, b\}$ need not be comparable by lemma 7.7. This leads to:

**Theorem 8.10 (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 $D^{=} = (\wp() \setminus \{\emptyset\}) \cup \{\bot^{=}\}$ and infimum $\bot^{=} = {}_{\bot}$ to $\dot{D}^{=} = \{f \in \ \longmapsto D^{=} \mid \forall s, s' \in \ : (s' \in f(s) \wedge f(s) \neq \bot^{=}) \Longrightarrow (s' \in \check{\tau} \wedge f(s') = \{s'\})$.*

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

**Theorem 8.11 (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* $E$*,* $F^\sharp[\![\tau]\!] = \lambda f \bullet \dot{\check{\tau}} \; \dot{\cup} \; \bigcup f^{\blacktriangleright} \circ \tau^{\bullet\!\!\blacktriangleright} \in E \stackrel{m}{\longmapsto} E$ *is* $\preccurlyeq$*-monotone and* $\forall \tau : \tau^\sharp = \mathrm{lfp}^{\preccurlyeq}_{\dot{\bot}^{=}} F^\sharp[\![\tau]\!]$ *then* $\dot{D}^{=} \subseteq E$ *and* $\dot{\sqsubseteq}^{=} \subseteq \preccurlyeq$*.*

Reciprocally, we have:

**Theorem 8.12 (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* $F^\natural = \lambda f \bullet \dot{\check{\tau}} \; \dot{\cup} \; \bigcup f^{\blacktriangleright} \circ \tau^{\bullet\!\!\blacktriangleright} \in E \stackrel{m}{\longmapsto} E$ *is* $\preccurlyeq$*-monotonic. Then* $\tau^\sharp = \mathrm{lfp}^{\preccurlyeq}_{\dot{\bot}^{=}} F^\sharp$*.*

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

The *angelic nondeterministic denotational semantics* is the right-image abstraction $\tau^\flat = \alpha^{\blacktriangleright}(\tau^+)$ of the finite/angelic relational semantics $\tau^+$. We also have $\tau^\flat = \alpha(\tau^\natural)$ where $\alpha(f) = \lambda s \bullet f(s) \cap$ . By theorem 7.1 and S. Kleene fixpoint transfer theorem 2.1, we get:

**Corollary 8.13 (C.A.R. Hoare fixpoint nondeterministic denotational semantics)** $\tau^\flat = \mathrm{lfp}^{\dot{\subseteq}}_{\dot{\emptyset}} F^\flat$ *where* $F^\flat = \lambda f \bullet \dot{\check{\tau}} \; \dot{\cup} \; \bigcup f^{\blacktriangleright} \circ \tau^{\bullet\!\!\blacktriangleright}$ *is a complete* $\dot{\cup}$*-morphism on the complete lattice* $\langle \;\longmapsto \wp(), \dot{\subseteq}, \dot{\emptyset}, \lambda s \bullet \;, \dot{\cup}, \dot{\cap}\rangle$ *which is the pointwise extension of the powerset* $\langle\wp(), \emptyset\rangle$*.*

Observe that the angelic semantic domain $\langle \;\longmapsto \wp(), \dot{\subseteq}\rangle$ is exactly the pointwise extension of the usual lower/C.A.R. Hoare powerdomain [19].

## *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 $\alpha^\top(\emptyset) = \alpha^\top(\{\bot\}) = \bot$, $\forall s \in \; : \alpha^\top(\{s\}) = \alpha^\top(\{s, \bot\}) = s$ and $\alpha^\top(X) = \top$ when $X \subseteq {}_\bot$ has a cardinality such that $|X \setminus \{\bot\}| > 1$. Observe that $\alpha^\top$ ignores inevitable nontermination in the abstraction of nondeterminism. By letting $\forall \zeta \in {}_\bot : \gamma^\top(\zeta) = \{\zeta, \bot\}$ and $\gamma^\top(\top) = {}_\bot$, we get the Galois insertion $\langle\wp({}_\bot), \subseteq\rangle \underset{\alpha^\top}{\overset{\gamma^\top}{\leftrightarrows}} \langle{}^\top_\bot, \sqsubseteq^\top\rangle$ where $\sqsubseteq^\top$ is given by $\bot \sqsubseteq^\top \zeta \sqsubseteq^\top \zeta \sqsubseteq^\top \top$ for $\zeta \in {}^\top_\bot = \cup \{\bot, \top\}$.

We define $\dot{\alpha}^\top = \lambda s \bullet \alpha^\top(f(s))$ pointwise so that $\tau^\top = \dot{\alpha}^\top(\tau^\natural)$. By theorem 8.1 and S. Kleene fixpoint transfer theorem 2.1, we get:

**Theorem 8.14 (D. Scott fixpoint deterministic denotational semantics (complete lattices and continuous functions))** $\tau^\top = \mathrm{lfp}^{\dot{\sqsubseteq}^\top}_{\dot{\bot}} F^\top$ *where* $F^\top \in (\;\longmapsto {}^\top_\bot) \longmapsto (\;\longmapsto {}^\top_\bot)$ *defined as* $F^\top(f) = \lambda s \bullet \big(\forall s' \in \; : \neg(s \;\tau\; s')$ ?

*$s$ ¿ $\sqcup^{\top}\{f(s') \mid s\ \tau\ s'\}$) is a complete $\dot{\sqcup}^{\top}$-morphism on the complete lattice $\langle \longmapsto {}^{\top}_{\perp}, \dot{\sqsubseteq}^{\top}, \dot{\perp}, \dot{\top}, \dot{\sqcup}^{\top}, \dot{\sqcap}^{\top}\rangle$ which is the pointwise extension of the complete lattice $\langle {}^{\top}_{\perp}, \sqsubseteq^{\top}, \perp, \top, \sqcup^{\top}, \sqcap^{\top}\rangle$ with $\sqsubseteq^{\top}$ such that $\forall \zeta \in {}^{\top}_{\perp} : \perp \sqsubseteq^{\top} \zeta \sqsubseteq^{\top} \zeta \sqsubseteq^{\top} \top$.*

Observe that we have got a complete lattice as in the original work of D. Scott [34] 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* $\langle , \tau\rangle$ (i.e. $\forall s, s', s'' \in\ : s\ \tau\ s' \wedge s\ \tau\ s'' \Longrightarrow s' = s''$) the top element $\top$ can be withdrawn from the semantic domain:

**Lemma 8.15 (Iterates of $F^{\top}$ for deterministic transition systems)** *For locally deterministic transition systems $\langle , \tau\rangle$, $\forall s \in\ : \tau^{\top}(s) \neq \top$.*

It follows that we can define $\tau^{\mathrm{D}} = \tau^{\top} \cap ( \longmapsto {}_{\perp})$. By the fixpoint iterates reordering theorem 2.4 and theorem 8.14, we infer:

**Theorem 8.16 (D. Scott fixpoint deterministic denotational semantics (CPOs and continuous functions))** *$\tau^{\mathrm{D}} = \mathrm{lfp}^{\dot{\sqsubseteq}^{\mathrm{D}}}_{\dot{\perp}}\ F^{\mathrm{D}}$ where $F^{\mathrm{D}} \in ( \longmapsto {}_{\perp}) \longmapsto ( \longmapsto {}_{\perp})$ defined as $F^{\mathrm{D}}(f) = \lambda s \bullet (\, s\ \tau\ s'\ ?\ f(s')$ ¿ $s\,)$ is a Scott-continuous map on the DCPO $\langle \longmapsto {}_{\perp}, \dot{\sqsubseteq}^{\mathrm{D}}, \dot{\perp}, \dot{\sqcup}^{\mathrm{D}}\rangle$ which is the pointwise extension of DCPO $\langle {}_{\perp}, \sqsubseteq^{\mathrm{D}}, \perp, \sqcup^{\mathrm{D}}\rangle$ where the Scott-ordering $\sqsubseteq^{\mathrm{D}}$ is such that $\forall \zeta \in {}_{\perp} : \perp \sqsubseteq^{\mathrm{D}} \zeta \sqsubseteq^{\mathrm{D}} \zeta$.*

## 9 Predicate Transformer Semantics

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

### *9.1 Correspondences Between Denotational and Predicate Transformers Semantics*

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

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

$$
\begin{aligned}
\alpha^{\sim} &= \lambda \in \wp(D) \stackrel{\cup}{\longmapsto} \wp(E) \centerdot \lambda P \in \wp(D) \centerdot \neg(\lambda(\neg P))\\
\gamma^{\sim} &= \lambda \in \wp(E) \stackrel{\cap}{\longmapsto} \wp(D) \centerdot \lambda P \in \wp(D) \centerdot \neg(\lambda(\neg P))\\
\alpha^{\cap} &= \lambda \in \wp(D) \stackrel{\cap}{\longmapsto} \wp(E) \centerdot \lambda Q \in \wp(E) \centerdot \{s \mid \lambda(\neg\{s\}) \cup Q = E\}\\
\gamma^{\cap} &= \lambda \in \wp(E) \stackrel{\cap}{\longmapsto} \wp(D) \centerdot \lambda P \in \wp(D) \centerdot \{s' \mid \lambda(\neg\{s'\}) \cup P = D\}
\end{aligned}
$$

Following [11], the correspondences between denotational and predicate transformers semantics are given as follows:

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

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

After [21], we define ($f \in D \longmapsto \wp(E)$):

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

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 [15] weakest precondition [6] $\mathrm{wp}(\tau^{\infty}, Q) = \mathrm{gwp}[\![\tau^{\natural}]\!]\, Q$ and weakest liberal precondition $\mathrm{wlp}(\tau^{\infty}, Q) = \mathrm{gwp}[\![\tau^{\flat}]\!]\, Q$ of postcondition $Q \subseteq$ are well-known. E. Dijkstra postulated healthiness conditions of predicate transformers [15] indeed follow from $\mathrm{gwp}[\![\tau^{\natural}]\!] \in \wp() \stackrel{\cap}{\longmapsto} \wp()$ (Conjunctivitis) and $\mathrm{gwp}[\![\tau^{\natural}]\!]\, \emptyset = \emptyset$ since $\tau^{\natural}$ is total by theorem 8.1 and lemma 8.2 (Excluded Miracle).

In order to establish the equivalence of forward and backward predicate transformers and proof methods, we observe [7,16] 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:

---

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

**Lemma 9.2 (Correspondence between pre- and postcondition semantics)** *If* $f \in D \longmapsto \wp(E)$ *then* $\langle \wp(D),\, \subseteq\rangle \xleftrightarrow[\mathrm{gsp}[\![f]\!]]{\mathrm{gwp}[\![f]\!]} \langle \wp(E),\, \subseteq\rangle$.

### *9.2 Generalized Weakest Precondition Semantics*

The *generalized weakest precondition semantics* is $\tau^{\mathrm{gwp}} = \mathrm{gwp}[\![\tau^{\natural}]\!]$. It combines the expressive power of the conservative and liberal weakest preconditions since for $Q \subseteq$ , we have $\tau^{\mathrm{gwp}}[\![Q]\!] = \mathrm{wp}(\tau^{\check\infty}, Q)$ and $\tau^{\mathrm{gwp}}[\![Q \cup \{\perp\}]\!] = \mathrm{wlp}(\tau^{\check\infty}, Q)$. Applying S. Kleene transfer theorem 2.1 to the fixpoint natural nondeterministic denotational semantics 8.1 with the correspondence $\langle \alpha^{\mathrm{gwp}}, \gamma^{\mathrm{gwp}}\rangle$ where $\alpha^{\mathrm{gwp}} = \mathrm{gwp} = \alpha^{\sim} \circ \alpha^{\triangleright} \circ \alpha^{-1}$ and $\gamma^{\mathrm{gwp}} = \gamma^{-1} \circ \gamma^{\triangleright} \circ \gamma^{\sim}$ which, according to theorem 9.1, is a Galois bijection, we derive[7] :

**Theorem 9.3 (Fixpoint generalized weakest precondition semantics)** $\tau^{\mathrm{gwp}} = \mathrm{lfp}^{\sqsubseteq^{\mathrm{gwp}}}_{\perp^{\mathrm{gwp}}} F^{\mathrm{gwp}}$ *where* $F^{\mathrm{gwp}} \in D^{\mathrm{gwp}} \xmapsto{m} D^{\mathrm{gwp}}$ *defined as* $F^{\mathrm{gwp}}() = \lambda Q \bullet (\neg\check\tau \cup Q) \,\dot\cap\, \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!] \circ \; = \lambda Q \bullet (Q \cap \check\tau) \,\dot\cup\, \mathrm{wp}[\![\tau^{\blacktriangleright}]\!] \circ$ *where* $\mathrm{wp}[\![f]\!]\, Q = \{s \in \;\mid \exists s' \in \; : s' \in f(s) \wedge \forall s' \in f(s) : s' \in Q\}$ *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* $D^{\mathrm{gwp}} = \wp(_{\perp}) \xmapsto{\cap} \wp()$, $\sqsubseteq^{\mathrm{gwp}} = \forall Q \subseteq \; : (Q \cup \{\perp\}) \subseteq (Q \cup \{\perp\}) \wedge () \subseteq ()$, $\perp^{\mathrm{gwp}} = \lambda Q \bullet (\perp \in Q \;?\; ¿\, \emptyset)$ *and* $\bigsqcup^{\mathrm{gwp}}_{i \in} {}_i = \lambda Q \bullet \bigcap_{i \in} {}_i(Q \cup \{\perp\}) \cap (\perp \notin Q \;?\; \bigcup_{i \in} {}_i() \;¿\; )$.

**Lemma 9.4 (Final states of the iterates of $F^{\mathrm{gwp}}$)** *Let* $F^{\mathrm{gwp}^{\delta}}$, $\delta \in \mathbb{O}$ *be the iterates of* $F^{\mathrm{gwp}}$ *from* $\perp^{\mathrm{gwp}}$. $\forall \delta \in \mathbb{O} : \forall Q \subseteq {}_{\perp} : F^{\mathrm{gwp}^{\delta}}(Q \setminus \{\perp\}) \subseteq F^{\mathrm{gwp}^{\delta}}(\check\tau)$.

Total correctness is the conjunction of partial correctness and termination in that $\forall Q \subseteq \; : \tau^{\mathrm{gwp}}[\![Q]\!] = \tau^{\mathrm{gwp}}[\![Q \cup \{\perp\}]\!] \cap \tau^{\mathrm{gwp}}[\![]\!]$ since $\tau^{\mathrm{gwp}}$ is a complete $\cap$-morphism. We have $\check\tau \subseteq$ so $\tau^{\mathrm{gwp}}[\![\check\tau]\!] \subseteq \tau^{\mathrm{gwp}}[\![]\!]$ by monotony and $\tau^{\mathrm{gwp}}[\![]\!] \subseteq \tau^{\mathrm{gwp}}[\![\check\tau]\!]$ by lemma 9.4 and theorem 9.3 so that by antisymmetry: $\forall Q \subseteq \; : \tau^{\mathrm{gwp}}[\![Q]\!] = \tau^{\mathrm{gwp}}[\![Q \cup \{\perp\}]\!] \cap \tau^{\mathrm{gwp}}[\![\check\tau]\!]$.

### *9.3 E. Dijkstra Weakest Conservative Precondition Semantics*

E. Dijkstra's *weakest conservative precondition semantics* [15] is $\tau^{\mathrm{wp}} = \alpha^{\mathrm{wp}}(\tau^{\mathrm{gwp}})$ (traditionally written $\lambda Q \in \wp() \bullet \mathrm{wp}(\tau^{\check\infty}, Q)$) where the abstraction $\alpha^{\mathrm{wp}} = \lambda \bullet |_{\wp()}$ satisfies:

**Lemma 9.5 (Weakest conservative precondition abstraction)** $\langle D^{\mathrm{gwp}}, \dot\supseteq\rangle \xleftrightarrow[\alpha^{\mathrm{wp}}]{\gamma^{\mathrm{wp}}} \langle D^{\mathrm{wp}}, \dot\supseteq\rangle$ *where* $D^{\mathrm{wp}} = \wp() \xmapsto{\cap} \wp()$ *and* $\gamma^{\mathrm{wp}}() = \lambda Q \bullet (\perp \notin Q \;?\; (Q) \;¿\; \emptyset)$.

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

**Lemma 9.6 (Abstraction of the demoniac nondeterministic denotational semantics)** $\tau^{\mathrm{wp}} = \alpha^{\mathrm{wp}}(\mathrm{gwp}[\![\tau^{\sharp}]\!])$.

---

[7] Observe that $\sqsubseteq^{\mathrm{gwp}}$ coincides with the partial ordering $\sqsubseteq$ of [28] except that the explicit use of $\perp$ to denote nontermination dispenses with the handling of two formulae to express $\tau^{\mathrm{gwp}}$ in terms of $\tau^{\mathrm{wp}}$ and $\tau^{\mathrm{wlp}}$.

E. Dijkstra's fixpoint characterization [15] of the conservative precondition semantics $\tau^{\mathrm{wp}}$ will be derived from theorem 8.10, by abstraction for a given post-condition $Q \subseteq$ :

**Lemma 9.7** *If* $Q \subseteq E$ *then* $\langle \wp(E) \stackrel{\cap}{\longmapsto} \wp(D),\ \dot{\supseteq}\rangle \xleftarrow[\alpha^{\mathrm{Q}}]{\gamma^{\mathrm{Q}}} \langle \wp(D),\ \supseteq\rangle$ *where* $\alpha^{\mathrm{Q}}() = (Q)$ *and* $\gamma^{\mathrm{Q}}(P) = \lambda R \boldsymbol{\cdot} (Q \subseteq R\ ?\ P\ ¿\ \emptyset)$.

By composition of lemmata 9.7, 9.6 and theorem 9.1, we get:

**Corollary 9.8 (Demoniac to weakest conservative precondition abstraction)** *For all* $Q \subseteq$ , $\langle \longmapsto \wp(_\perp),\ \dot{\subseteq}\rangle \xleftarrow[\gamma^{\mathrm{gwp}} \circ \gamma^{\mathrm{wp}} \circ \gamma^{\mathrm{Q}}]{\alpha^{\mathrm{Q}} \circ \alpha^{\mathrm{wp}} \circ \alpha^{\mathrm{gwp}}} \langle \wp(),\ \supseteq\rangle$ *where* $\alpha^{\mathrm{Q}} \circ \alpha^{\mathrm{wp}} \circ \alpha^{\mathrm{gwp}} = \lambda f \boldsymbol{\cdot} \mathrm{gwp}[\![f]\!]\, Q$.

By definition of $\tau^{\sharp}$ and S. Kleene fixpoint transfer theorem 2.1 applied to the fixpoint characterization of the nondeterministic demoniac semantics semantics 8.10 with the abstraction $\lambda f \boldsymbol{\cdot} \mathrm{gwp}[\![f]\!]\, Q$ for a given $Q \subseteq$ considered in corollary 9.8, we now obtain [16,17]:

**Theorem 9.9 (E. Dijkstra's fixpoint weakest conservative precondition semantics)** $\tau^{\mathrm{wp}} = \lambda Q \boldsymbol{\cdot} \mathrm{lfp}_{\emptyset}^{\subseteq}\ F^{\mathrm{wp}}[\![Q]\!]$ *where* $F^{\mathrm{wp}} \in \wp() \longmapsto \wp() \stackrel{m}{\longmapsto} \wp()$ *defined by* $F^{\mathrm{wp}}[\![Q]\!] = \lambda P \boldsymbol{\cdot} (Q \cap \check{\tau}) \cup \mathrm{wp}[\![\tau^{\bullet\!\!\rightarrow}]\!]\, P = \lambda P \boldsymbol{\cdot} (\neg\check{\tau} \cup Q) \cap \mathrm{gwp}[\![\tau^{\bullet\!\!\rightarrow}]\!]\, P$ *is a* $\subseteq$*-monotone map on the complete lattice* $\langle \wp(),\ \subseteq,\ \emptyset,\ ,\ \cup,\ \cap\rangle$.

### *9.4 E. Dijkstra Weakest Liberal Precondition Semantics*

E. Dijkstra's *weakest liberal precondition semantics* [15] $\lambda Q \in \wp() \boldsymbol{\cdot} \mathrm{wlp}(\tau^{\vec{\infty}}, Q)$ is $\tau^{\mathrm{wlp}} = \alpha^{\mathrm{wlp}}(\tau^{\mathrm{gwp}})$ where the abstraction $\alpha^{\mathrm{wlp}}$ satisfies:

**Lemma 9.10 (Weakest liberal precondition abstraction)** *If* $D^{\mathrm{wlp}} = \wp() \stackrel{\cap}{\longmapsto} \wp()$, $\alpha^{\mathrm{wlp}} = \lambda \boldsymbol{\cdot} \lambda Q \boldsymbol{\cdot} (Q \cup \{\perp\})$ *and* $\gamma^{\mathrm{wlp}}() = \lambda Q \boldsymbol{\cdot} (\perp \in Q\ ?\ (Q)\ ¿\ \emptyset)$ *then* $\langle D^{\mathrm{gwp}},\ \dot{\supseteq}\rangle \xleftarrow[\alpha^{\mathrm{wlp}}]{\gamma^{\mathrm{wlp}}} \langle D^{\mathrm{wlp}},\ \dot{\supseteq}\rangle$.

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

**Lemma 9.11 (Abstraction of the angelic nondeterministic denotational semantics)** $\tau^{\mathrm{wlp}} = \mathrm{gwp}[\![\tau^{\flat}]\!]$.

By lemma 9.11, theorem 8.13 and S. Kleene fixpoint transfer theorem 2.1, we deduce [16]:

**Theorem 9.12 (E. Dijkstra's fixpoint weakest liberal precondition semantics)** $\tau^{\mathrm{wlp}} = \lambda Q \boldsymbol{\cdot} \mathrm{gfp}^{\subseteq}\ F^{\mathrm{wp}}[\![Q]\!]$.

## 10 Galois Connections and Tensor Product

The set of Galois connections between posets (respectively DCPOs, complete lattices) $\langle D^{\natural}, \sqsubseteq^{\natural}\rangle$ and $\langle D^{\sharp}, \sqsubseteq^{\sharp}\rangle$ is denoted$\langle D^{\natural}, \sqsubseteq^{\natural}\rangle \leftrightarrows \langle D^{\sharp}, \sqsubseteq^{\sharp}\rangle = \{\langle \alpha, \gamma\rangle \mid \langle D^{\natural}, \sqsubseteq^{\natural}\rangle \xleftarrow[\alpha]{\gamma} \langle D^{\sharp},\ \sqsubseteq^{\sharp}\rangle\}$. It is a poset (resp. DCPOs, complete lattices) $\langle\langle D^{\natural},\ \sqsubseteq^{\natural}$

$\rangle \leftrightarrows \langle D^\sharp, \sqsubseteq^\sharp\rangle, \dot{\sqsubseteq}^\sharp \times \dot{\sqsubseteq}^\natural\rangle$ for the pairwise pointwise ordering $\langle \alpha, \gamma\rangle \ \dot{\sqsubseteq}^\sharp \times \dot{\sqsubseteq}^\natural \ \langle \alpha', \gamma'\rangle = (\alpha \ \dot{\sqsubseteq}^\sharp \ \alpha') \wedge (\gamma \ \dot{\sqsubseteq}^\natural \ \gamma')$ where $f \ \dot{\sqsubseteq} \ g = \forall x : f(x) \sqsubseteq g(x)$.

The set of *complete join morphisms* is$D^\natural \overset{\sqcup}{\longmapsto} D^\sharp = \{\alpha \in D^\natural \longmapsto D^\sharp \mid \forall X \subseteq D^\natural : \alpha(\sqcup^\natural X) = \sqcup^\sharp \alpha^\blacktriangleright(X)\}$. (also written $\langle D^\natural, \sqsubseteq^\natural\rangle \overset{\sqcup}{\longmapsto} \langle D^\sharp, \sqsubseteq^\sharp\rangle$ when the considered partial orderings are not understood). Dually, the set of *complete meet morphisms* is$D^\sharp \overset{\sqcap}{\longmapsto} D^\natural = \{\gamma \in D^\sharp \longmapsto D^\natural \mid \forall Y \subseteq D^\sharp : \gamma(\sqcap^\sharp Y) = \sqcap^\natural \gamma^\blacktriangleright(Y)\}$.

The *tensor product* $\otimes$ [35] [8] is:

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

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

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

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

Let us define the correspondences:

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

**Theorem 10.2 (Galois connections/tensor product commutative diagram)**

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

## 11 Axiomatic Semantics

Using theorems 9.2 and 10.2, we can define the generalized axiomatic semantics $\tau^{\mathrm{gH}}$ of a transition system $\langle, \tau\rangle$ as the element $\mathrm{HC}(\tau^{\mathrm{gwp}})$ of the tensor product $\wp() \otimes \wp(_\perp)$ corresponding to the weakest precondition semantics $\tau^{\mathrm{gwp}}$,

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

or equivalently as $\mathrm{HA}(\tau^{\mathrm{gsp}})$ corresponding to the strongest postcondition semantics $\tau^{\mathrm{gsp}}$. Writing $\langle P\rangle\tau\langle Q\rangle$ for $\langle P,\, Q\rangle \in \tau^{\mathrm{gH}}$, we have $\langle P\rangle\tau\langle Q\rangle$ if and only if $P \sqsubseteq^{\mathrm{gwp}} \tau^{\mathrm{gwp}}(Q)$ if and only if $\tau^{\mathrm{gsp}}(P) \sqsubseteq^{\mathrm{gwp}} Q$. Condition (i) of definition 10.1 is the consequence rule of C.A.R. Hoare logic [20]. Conditions (ii) and (iii) are also valid for the classical presentation of C.A.R. Hoare logic [20] 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 [18], C.A.R. Hoare [20] & P. Naur [27] *partial correctness semantics* is $\tau^{\mathrm{pH}} = \mathrm{HC}(\tau^{\mathrm{wlp}})$. We get R. Floyd & P. Naur's partial correctness verification conditions [18,27] using E. Dijkstra's fixpoint characterization 9.12 of the weakest liberal precondition semantics $\tau^{\mathrm{wlp}}$ and D. Park fixpoint induction [29]:

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

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

The condition $I \subseteq \mathrm{gwp}[\![\tau^{\bullet\!\to}]\!]\, I$ is given by C.A.R. Hoare [20] while R. Floyd & P. Naur partial correctness verification condition [18,27] corresponds more precisely to $\mathrm{gsp}[\![\tau^{\bullet\!\to}]\!]\, I \subseteq I$ which, by lemma 9.2, is equivalent.

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

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

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

*and the following inference rules:*

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

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

### *11.2 R. Floyd Total Correctness Semantics*

R. Floyd [18] *total correctness semantics* is $\tau^{\mathrm{tH}} = \mathrm{HC}(\tau^{\mathrm{wp}})$. We get R. Floyd's verification conditions using E. Dijkstra's fixpoint characterization 9.9 of $\tau^{\mathrm{wp}}$ and the following induction principle:

**Lemma 11.4 (Lower fixpoint induction)** *If* $\langle D,\, \sqsubseteq,\, \bot,\, \sqcup\rangle$ *is a DCPO,* $F \in D \xmapsto{m} D$ *is* $\sqsubseteq$*-monotone,* $\perp \in D$ *satisfies* $\perp \sqsubseteq F(\perp)$ *and* $P \in D$ *then*

$P \sqsubseteq \mathrm{lfp}^{\sqsubseteq}_{\pm} F \Longleftrightarrow (\exists \epsilon \in \mathbb{O} : \exists I \in (\epsilon + 1) \longmapsto D : I^0 \sqsubseteq \bot \wedge \forall \delta : 0 < \delta \leq \epsilon \Longrightarrow I^\delta \sqsubseteq F(\bigsqcup_{\zeta<\delta} I^\zeta) \wedge P \sqsubseteq I^\epsilon)$.

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

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

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

where the ordinal $\delta$ encodes the value of R. Floyd's *variant function* [17].

Writing *Z. Manna/A. Pnueli triples* $[P]\tau^{\vec\infty}[Q]$ for $\langle P, Q\rangle \in \tau^{\mathrm{tH}}$, $[P]\tau[Q]$ for $P \subseteq \mathrm{gwp}[\![\tau^{\bullet\!\rightarrow}]\!]\, Q$ and using a rule-based presentation of $\tau^{\mathrm{tH}}$, we get a set theoretic model of Z. Manna/A. Pnueli logic [24]:

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

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

## 12 Lattice of Semantics

A preorder can be defined on semantics $\tau^\natural \in D^\natural$ and $\tau^\sharp \in D^\sharp$ when $\tau^\sharp = \alpha^\sharp(\tau^\natural)$ and $\langle D^\natural, \leq\rangle \underset{\alpha^\sharp}{\overset{\gamma^\sharp}{\longleftrightarrow}} \langle D^\sharp, \leqq\rangle$. The quotient poset is isomorphic to M. Ward lattice [37] of upper closure operators $\gamma^\sharp \circ \alpha^\sharp$ on $\langle D^{\vec\infty}, \subseteq\rangle$, so that we get a lattice of semantics which is part of the lattice of abstract interpretations of [9, sec. 8], a sublattice of which is illustrated in figure 4.

## 13 Conclusion

We have shown that the classical semantics of programs, modeled as transition systems, can be derived from one another by Galois connection based abstract interpretations. All classical semantics of programming languages have been presented in a uniform framework which makes them easily comparable and better explains the striking similarities and correspondences between semantic models. Moreover the construction leads to new reorderings of the fixpoint semantics. Our presentation uses abstraction which proceeds by omitting some aspects of program execution but the inverse operation of semantic refinement (traditionally called concretization) is equally important [9] . This suggests con-

[9] 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 $\{s^\omega s' s'[X \leftarrow 1] \mid s, s' \in \}$ thus

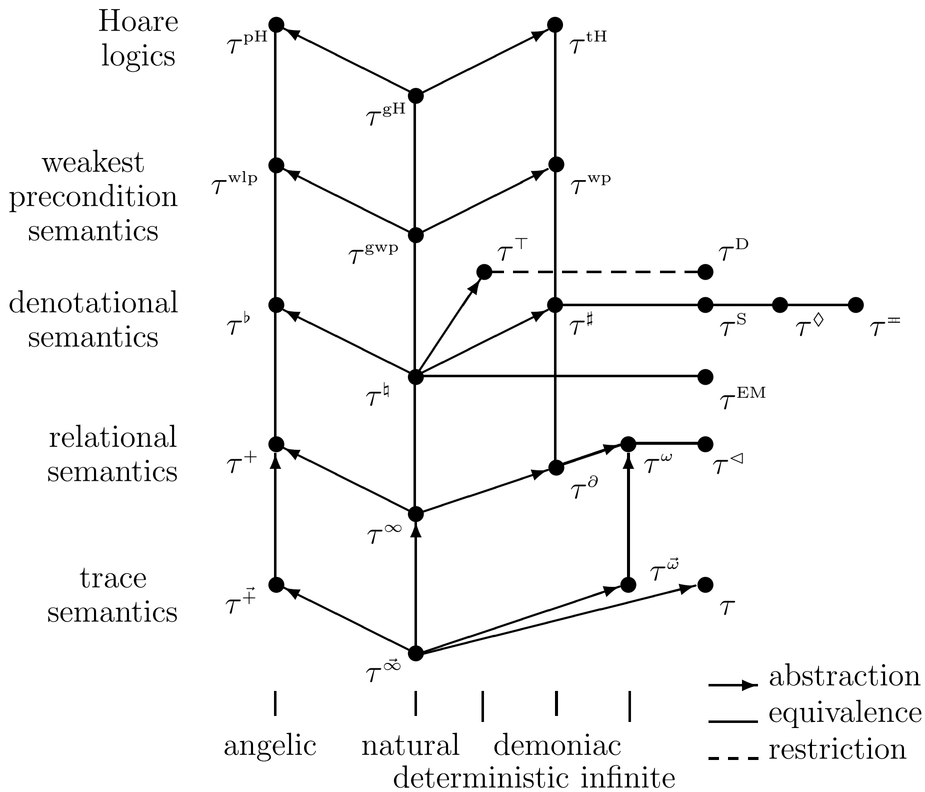



Fig. 4. The lattice of semantics

sidering hierarchies of semantics which can describe program properties, that is program executions, at various levels of abstraction or refinement in a uniform framework. Then for program analysis of a given class of properties there should be a natural choice of semantics in the hierarchy [8].

## References


[1] S. Abramsky & A. Jung. Domain theory. In S. Abramsky, Dov M. Gabbay, & T.S.E. Maibaum, eds., vol. 3 of *Handbook of Logic in Computer Science*, ch. 1, pp. 1–168. Clarendon Press, 1994.

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

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

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

[5] M. Broy, R. Gnatz & M. Wirsing. Semantics of nondeterministic and noncontinuous constructs. LNCS 69, pp. 553–592. Springer, 1979.


allowing the program slice with respect to variable `X` to be `X:=1` with semantics $\{s's'[X \leftarrow 1] \mid s' \in \}$. Slicing would not be consistent when considering the trace $\{s^{\omega} \mid s \in \}$ or denotational semantics $\lambda s \bullet \perp$ of the program.

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

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

[8] P. Cousot. Abstract interpretation. *ACM Comput. Surv.*, 28(2):324–328, 1996.

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

[10] P. Cousot & R. Cousot. Systematic design of program analysis frameworks. In *6^th POPL*, pp. 269–282. ACM Press, 1979.

[11] P. Cousot & R. Cousot. Induction principles for proving invariance properties of programs. In D. Néel, ed., *Tools & Notions for Program Construction*, pp. 43–119. Cambridge Univ. Press, 1982.

[12] P. Cousot & R. Cousot. Inductive definitions, semantics and abstract interpretation. In *19^th POPL*, pp. 83–94. ACM Press, 1992.

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

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

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

[16] E.W. Dijkstra & C.S. Scholten. *Predicate Calculus and Program Semantics.* Springer, 1990.

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

[18] R.W. Floyd. Assigning meaning to programs. In J.T. Schwartz, ed., *Proc. Symposium in Applied Mathematics*, vol. 19, pp. 19–32. AMS, 1967.

[19] C.A. Gunter & D.S. Scott. Semantic domains. In J. van Leeuwen, ed., vol. B of *Handbook of Theoretical Computer Science*, ch. 12, pp. 633–674. Elsevier, 1990.

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

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

[22] G. Kahn. Natural semantics. In K. Fuchi & M. Nivat, eds., *Programming of Future Generation Computers*, pp. 237–258. Elsevier, 1988.

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

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

[25] R. Milner. Operational and algebraic semantics of concurrent processes. In J. van Leeuwen, ed., volume B of *Handbook of Theoretical Computer Science*, ch. 19, pp. 1201–1242. Elsevier, 1990.

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

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

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

[29] D. Park. Fixpoint, induction and proofs of program properties. In B. Meltzer & D. Michie, eds., *Machine Intelligence*, volume 5, pp. 59–78. Edinburgh Univ. Press, 1969.

[30] D. Park. On the semantics of fair parallelism. LNCS 86, pp. 504–526. Springer, 1980.

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

[32] G.D. Plotkin. A structural approach to operational semantics. Tech. Report DAIMI FN-19, Aarhus Univ., 1981.

[33] D. Scott. Outline of a mathematical theory of computation. Tech. Monograph PRG-2, Oxford Univ. Computing Lab., Programming Research Group, Oxford, 1970.

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

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

[36] R.J. van Glabbeek. The linear time – branching time spectrum (extended abstract). LNCS 458, pp. 278–297. Springer, 1990.

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