Fourth Advanced Seminar on Foundations of Declarative Programming

Rule-Based Specifications and their Abstract Interpretation

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

Content

- Classical rule-based and fixpoint formal specifications methods;
- Generalization from set based to order-theoretic formal specification methods;
- Preservation of these various specification styles by abstract interpretation;
- Examples of formal/abstract semantic specifications.

Classical Set-based Inductive Formal Specification Methods [1]

Reference

[1] P. Aczel. An introduction to inductive definitions. In J. Barwise, editor, *Handbook of Mathematical Logic*, volume 90 of *Studies in Logic and the Foundations of Mathematics*, pages 739–782. Elsevier Science Publishers B.V. (North-Holland), Amsterdam, 1977.

Formal Specification

- Objective: specify a subset S of a set U, called the *universe* (example: a programming language is a subset of the finite character strings);
- Methods:
  - Fixpoint specifications,
  - Inductive specifications by rule-based formal systems.
- The two methods (and many others) are equivalent.

Fixpoint Specification

The set S is specified as the smallest solution of an equation:

$$X = F(X)$$

where:

$$F \in \wp(U) \longmapsto \wp(U)$$

is upper-continuous on the complete lattice $(\wp(U), \subseteq, \emptyset, U, \cup, \cap)$, hence:

$$S = \mathrm{lfp}\, F$$

such that $S = F(S)$ and if $X = F(X)$ then $S \subseteq X$.

Example : Fixpoint Specification of the Even Natural Numbers

$\mathbb{N} \stackrel{\text{def}}{=} \{0, 1, 2, 3, 4, 5, \ldots\}$ Universe (natural numbers)

$$\begin{aligned}\mathbb{E} &\stackrel{\text{def}}{=} \{0, 2, 4, 6, \ldots\} \\ &= \operatorname{lfp} \lambda X \bullet \{0\} \cup \{n + 2 \mid n \in X\}\ .\end{aligned}$$

Even natural numbers

so that:

$$\begin{aligned}
X^0 &= \emptyset \\
X^1 &= \{0\} \\
X^2 &= \{0, 2\} \\
\ldots &= \ldots \\
X^n &= \{0, 2, 4, \ldots, 2n - 2\} \\
X^{n+1} &= \{0\} \cup \{k + 2 \mid k \in \{0, 2, 4, \ldots, 2n\}\} \\
&= \{0, 2, 4, \ldots, 2n - 2\} \\
\ldots &= \ldots \\
\operatorname{lfp} \lambda X \bullet \{0\} \cup \{n + 2 \mid n \in X\} &= \bigcup_{n \in \mathbb{N}} X^n \;=\; \{0, 2, 4, \ldots, 2n, \ldots\}
\end{aligned}$$

Rule-based Specification

S is the smallest subset of the universe U defined by:

- *axioms*[1]:

$$a, \qquad a \in U;$$

  the element of U defined by the axioms belong to S ;

- *inference rules* :

$$\frac{P}{c}, \qquad P \subseteq U \;\&\; c \in U \;;$$

  if all elements of the *premiss* P belong to S then the *conclusion* c belongs to E;

[1] The axioms a are particular cases of inference rules of the form $\frac{\emptyset}{a}$ where $\emptyset$ is the empty set.

Formal Proof

- S is the set of elements of U which are *provable* by a formal proof;
- A *formal proof* of $e \in U$ is a finite sequence:

$$e_1, \ldots, e_i, \ldots, e_n$$

such that [2], [3] :

$$\forall i \in [1, n], \exists \frac{P}{c} : P \subseteq \{e_1, \ldots, e_{i-1}\} \wedge e_i = c$$
$$e_n = e$$

---

2 The axioms a are assumed to be written as rules $\frac{\emptyset}{a}$.

3 For $i = 1$, $\{e_1, \ldots, e_{i-1}\} = \emptyset$ hence e_1 must be an axiom.

Example : Rule-based Specification of the Even Natural Numbers

$$0 \in \mathbb{E}, \qquad \frac{n \in \mathbb{E}}{n+2 \in \mathbb{E}}$$

with is an abridged notation for the formal system:

$$\frac{\emptyset}{0}\,(a) \quad \frac{\{0\}}{2}\,(b) \quad \frac{\{1\}}{3}\,(c) \quad \frac{\{2\}}{4}\,(d) \quad \frac{\{3\}}{5}\,(e) \quad \frac{\{4\}}{6}\,(f) \quad \ldots$$

The proof that 6 is an even natural number is

(1)	0	by (a)
(2)	2	by (1) and (b)
(3)	4	by (2) and (d)
(4)	6	by (3) and (f)

Generalization from set-theoretic to order-theoretic formal inductive specification methods [2], [3]

References

[2] P. Cousot and R. Cousot. Inductive definitions, semantics and abstract interpretation. In *Conf. Rec. 19th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 83–94, Albuquerque, New Mexico, 1992. ACM Press.

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

Formal Specification

- We consider equivalent formal specifications of $S \in \mathcal{D}$ where $\langle \mathcal{D}, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$ is a complete lattice;

- This is a generalization of the set-based formal specicifications where $\langle \mathcal{D}, \sqsubseteq \rangle = \langle \wp(U), \subseteq \rangle$ and U is the universe.

Fixpoint Specification

Given the monotonic operator:

$$F \in \mathcal{D} \xrightarrow{\mathrm{m}} \mathcal{D}$$

S is defined as the least fixpoint [4]:

$$S \stackrel{\mathrm{def}}{=} \mathrm{lfp}^{\sqsubseteq} F$$

[4] By Tarski's fixpoint theorem $\mathrm{lfp}^{\sqsubseteq} F$ exists since $\langle \mathcal{D}, \sqsubseteq \rangle$ is a complete lattice and F is monotonic.

Equational Specification

Given the monotonic operator:

$$F \in \mathcal{D} \overset{\mathrm{m}}{\longmapsto} \mathcal{D}$$

S is defined as the $\sqsubseteq$-least element of $\mathcal{D}$ which is a solution to the equation [5]:

$$X = F(X)$$

[5] By Tarski's fixpoint theorem this $\sqsubseteq$-least solution exists and is precisely $\mathrm{lfp}^{\sqsubseteq} F = \sqcap\{X \mid X = F(X)\}$.

CONSTRAINT-BASED SPECIFICATION

Given the monotonic operator:

$$F \in \mathcal{D} \xrightarrow{\text{m}} \mathcal{D}$$

S is defined as the $\sqsubseteq$-least element of $\mathcal{D}$ satisfying the constraint [6]:

$$F(X) \sqsubseteq X$$

[6] By Tarski's fixpoint theorem this $\sqsubseteq$-least solution exists and is precisely $\mathrm{lfp}^{\sqsubseteq} F = \sqcap\{X \mid F(X) \sqsubseteq X\}$.

Closure-condition Specification

- Given a complete lattice $(\mathcal{D}, \sqsubseteq)$, a *closure-condition* is:

$$C \in \wp(\mathcal{D} \times \mathcal{D})$$

  which is monotonic in its second component, that is, $\forall x, X, Y \in L$:

$$C(x, X) \wedge X \sqsubseteq Y \Rightarrow C(x, Y)$$

  where $C(x, X)$ is true if and only if $\langle x,\ X\rangle \in C$;
- A *closure-specification* has the form:

  S is the $\sqsubseteq$-least element X of $\mathcal{D}$ satisfying:

$$\forall x \in L : C(x, X) \Longrightarrow x \sqsubseteq X$$

Example: Informal Closure-Condition Specification of the Syntax of Regular Expressions

1. ϵ is a regular expression; *empty*
2. If $a \in A$ then a is a regular expression; *letter*
3. If ρ_1 and ρ_2 are regular expressions then:

   3.1 $\rho_1 | \rho_2$ *alternative*

   3.2 $\rho_1 \rho_2$ *concatenation*

   are regular expressions;
4. If ρ is a regular expression then:

   4.1 $\rho^\star$ *repetition, 0 or more times*

   4.2 (ρ) *parenthesized expression*

   are regular expressions.

Corresponding Formal Definition

The closure-condition is $C \in \wp(\vec{A^*}) \times \wp(\vec{A^*}) \longmapsto \{\mathrm{tt}, \mathrm{ff}\}$

$$
\begin{aligned}
C(x, X) = \; & (x = \{\epsilon\}) \vee \\
& (x = \{a\} \wedge a \in A) \vee \\
& (x = \{\rho_1|\rho_2\} \wedge \rho_1 \in X \wedge \rho_2 \in X) \vee \\
& (x = \{\rho_1\rho_2\} \wedge \rho_1 \in X \wedge \rho_2 \in X) \vee \\
& (x = \{\rho^\star\} \wedge \rho \in X) \vee \\
& (x = \{(\rho)\} \wedge \rho \in X)
\end{aligned}
$$

Presentation of a Closure-condition in Fixpoint Form

The $\sqsubseteq$-least element X of $\mathcal{D}$ satisfying:

$$\forall x \in \mathcal{D} : C(x, X) \Rightarrow x \sqsubseteq X$$

is:

$$\mathrm{lfp}^{\sqsubseteq} F$$

where:

$$F \stackrel{\mathrm{def}}{=} \lambda X \bullet \bigsqcup \{x \in \mathcal{D} \mid C(x, X)\}$$

Presentation of a Fixpoint Specification as a Closure-Specification

If

- $\langle \mathcal{D}, \sqsubseteq, \perp, \bigsqcup \rangle$ is a complete lattice, and
- $F \in \mathcal{D} \stackrel{\mathrm{m}}{\longmapsto} \mathcal{D}$

then the closure-specification with condition

$$C(x, X) = x \sqsubseteq F(X)$$

defines

$$\operatorname{lfp}^{\sqsubseteq} F \ .$$

Principle of the Generalization of Rule-Based Specifications

Inference rules:

$$\frac{P}{c}, \qquad P \subseteq U \;\&\; c \in U \;;$$

can also be written:

$$\frac{P}{\{c\}}, \qquad P \subseteq U \;\&\; \{c\} \subseteq U \;.$$

Rule-Based Specification

- An element S of the complete lattice $\langle \mathcal{D}, \sqsubseteq \rangle$ can be defined by the rule instances:

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

such that for all $i \in \Delta$: $P_i \in \mathcal{D}$ and $C_i \in \mathcal{D}$;

- By definition, this denotes:

$$\mathrm{lfp}^{\sqsubseteq}\, \Phi_R$$

where the *R-operator* Φ_R is [7]:

$$\Phi_R \stackrel{\text{def}}{=} \lambda X \bullet \bigsqcup \{ C_i \mid \exists i \in \Delta : P_i \sqsubseteq X \}$$

[7] Φ_R is monotonic hence the rule-based specification is well-defined.

Rule-Based Presentation of a Fixpoint Specification

- Let $F \in L \stackrel{\mathrm{m}}{\longmapsto} L$ be a monotonic map on the complete lattice $\langle L, \sqsubseteq, \perp, \sqcup \rangle$;
- $\mathrm{lfp}^{\sqsubseteq}$ is defined by the rule instances:

$$R = \left\{ \frac{P}{C} \;\middle|\; C, P \in L \wedge C \sqsubseteq F(P) \right\} \tag{1}$$

Derivation [8]

- Let $R = \left\{ \dfrac{P_i}{C_i} \;\middle|\; i \in \Delta \right\}$

  and $\Phi_R \stackrel{\text{def}}{=} \lambda X \bullet \bigsqcup \{C_i \mid \exists i \in \Delta : P_i \sqsubseteq X\}$;
- A *derivation* of an element x of the complete lattice $\langle \mathcal{D}, \sqsubseteq \rangle$ is a transfinite sequence x_κ, $\kappa \leq \lambda$, $\lambda \in \mathbb{O}$ such that:
  - $x_0 = \bot$,
  - $x_\kappa \sqsubseteq \Phi_R(\bigsqcup_{\beta < \kappa} x_\beta)$ for all $0 < \kappa \leq \lambda$,
  - $x_\lambda = x$;

[8] This generalizes the notion of proof in formal systems.

Derivable Elements

- An element x of the complete lattice $\langle \mathcal{D}, \sqsubseteq \rangle$ is said to be *derivable* whenever it has a derivation;
- An element $x \in \mathcal{D}$ is *derivable* if and only if $x \sqsubseteq \operatorname{lfp}^{\sqsubseteq} \Phi_R$;
- It follows that:

$$\operatorname{lfp}^{\sqsubseteq} \Phi_R = \bigsqcup \{x \in \mathcal{D} \mid x \text{ is derivable}\}$$

Game-Theoretic Specification

- Given a complete lattice $\langle L, \sqsubseteq \rangle$, a game is defined by rules $R \subseteq L \times L$. The corresponding *R-operator* Φ is:

$$\Phi \stackrel{\text{def}}{=} \lambda X \cdot \bigsqcup \{C \mid \exists \langle C, P \rangle \in R : P \sqsubseteq X\}$$

- The game $\mathcal{G}(R, a)$ with rules R starting from initial position $a \in L$ is played by two players I and II.
- Player I must start by choosing $x_0 = a$.
- If player I chooses x_n in the n-th move, then player II must respond by $X_n \in \wp(L)$ such that $x_n \sqsubseteq \Phi(\bigsqcup X_n)$.
- For the next move, player I must choose some $x_{n+1} \in X_n$.
- A player who is blocked has lost.
- If the game goes on forever then player II has lost.

Initial Winning Positions

- We define $\mathcal{W}(R)$ as the set of initial winning positions for player II:

$$\mathcal{W}(R) \stackrel{\text{def}}{=} \{a \in L \mid \text{player II has a winning strategy} \\ \text{in game } \mathcal{G}(R, a)\}$$

- $\operatorname{lfp} \Phi = \bigsqcup \mathcal{W}(R)$.

Fixpoint Specification in Equivalent Game-Theoretic Form

- Let $\langle L, \sqsubseteq\rangle$ be a cpo and $F \in L \stackrel{\text{m}}{\longmapsto} L$ be monotonic;
- $\quad \operatorname{lfp} F = \bigsqcup \mathcal{W}(R)$

  for the game with rules:

  $\quad R = \{\langle C, P\rangle \mid P \in L \wedge C \sqsubseteq F(P)\}$.

EXAMPLE: TRACE SEMANTIC SPECIFICATION

Maximal execution trace semantics

- $\langle \Sigma, \; \tau \rangle$ — transition system
- $\tau^{\dot{\vec{n}}}$ — partial traces of length $n > 0$
- $\tau^{\check{\vec{n}}}$ — maximal traces of length $n > 0$
- $\tau^{\check{\vec{+}}} = \bigcup_{n>0} \tau^{\check{\vec{n}}}$ — maximal non-empty finitary trace semantics
- $\tau^{\vec{\omega}}$ — infinitary trace semantics
- $\tau^{\vec{\infty}} = \tau^{\check{\vec{+}}} \cup \tau^{\vec{\omega}}$ — maximal bifinitary trace semantics

Example (Prolog): Σ: set of subgoals with substitutions, τ: replacement of a subgoal in the set by a resolvent for a clause selected in the program.

Junction of State Sequences

- Joinable nonempty finite state sequences:

$$\alpha_0 \ldots \alpha_{\ell-1} \overset{?}{\frown} \beta_0 \ldots \beta_{m-1} \text{ iff } \alpha_{\ell-1} = \beta_0$$

- Their join is:

$$\frac{\begin{array}{cccccc} \alpha_0 & \ldots & \alpha_{\ell-1} & & & \\ & & = & & & \\ & & \beta_0 & \beta_1 & \ldots & \beta_{m-1} \end{array}}{\alpha_0 \ldots \alpha_{\ell-1} \frown \beta_0 \ldots \beta_{m-1} \stackrel{\text{def}}{=} \alpha_0 \ \ldots \ \alpha_{\ell-1} \ \beta_1 \ \ldots \ \beta_{m-1}}$$

- Joinable infinite state sequences:

$$\begin{array}{rcll}
\alpha_0 \ldots \alpha_\ell \ldots & \stackrel{?}{\frown} & \beta_0 \ldots \beta_{m-1} & \text{is true} \\
\alpha_0 \ldots \alpha_\ell \ldots & \stackrel{?}{\frown} & \beta_0 \ldots \beta_m \ldots & \text{is true} \\
\alpha_0 \ldots \alpha_{\ell-1} & \stackrel{?}{\frown} & \beta_0 \ldots \beta_m \ldots & \text{iff } \alpha_{\ell-1} = \beta_0
\end{array}$$

- Their join is:

$$\begin{array}{rcl}
\alpha_0 \ldots \alpha_\ell \ldots \frown \beta_0 \ldots \beta_{m-1} & \stackrel{\text{def}}{=} & \alpha_0 \; \ldots \; \alpha_\ell \; \ldots \\
\alpha_0 \ldots \alpha_\ell \ldots \frown \beta_0 \ldots \beta_m \ldots & \stackrel{\text{def}}{=} & \alpha_0 \; \ldots \; \alpha_\ell \; \ldots \\
& & \alpha_0 \; \ldots \; \alpha_{\ell-1} \\
& & \qquad\quad = \\
& & \qquad\quad \beta_0 \; \beta_1 \; \ldots \; \beta_m \ldots \\
\hline
\alpha_0 \ldots \alpha_{\ell-1} \frown \beta_0 \ldots \beta_m \ldots & \stackrel{\text{def}}{=} & \alpha_0 \; \ldots \; \alpha_{\ell-1} \; \beta_1 \; \ldots \; \beta_m \ldots
\end{array}$$

Junction of Sets of Bifinitary State Sequences

- For sets A and $B \in \wp(\mathcal{A}^{\vec{\propto}})$ of sequences, we have:

$$A \frown B \stackrel{\text{def}}{=} \{\alpha \frown \beta \mid \alpha \in A \wedge \beta \in B \wedge \alpha \stackrel{\frown}{?} \beta\}$$ set junction

Fixpoint Specification of the Maximal Finitary Trace Semantics of Transition Systems

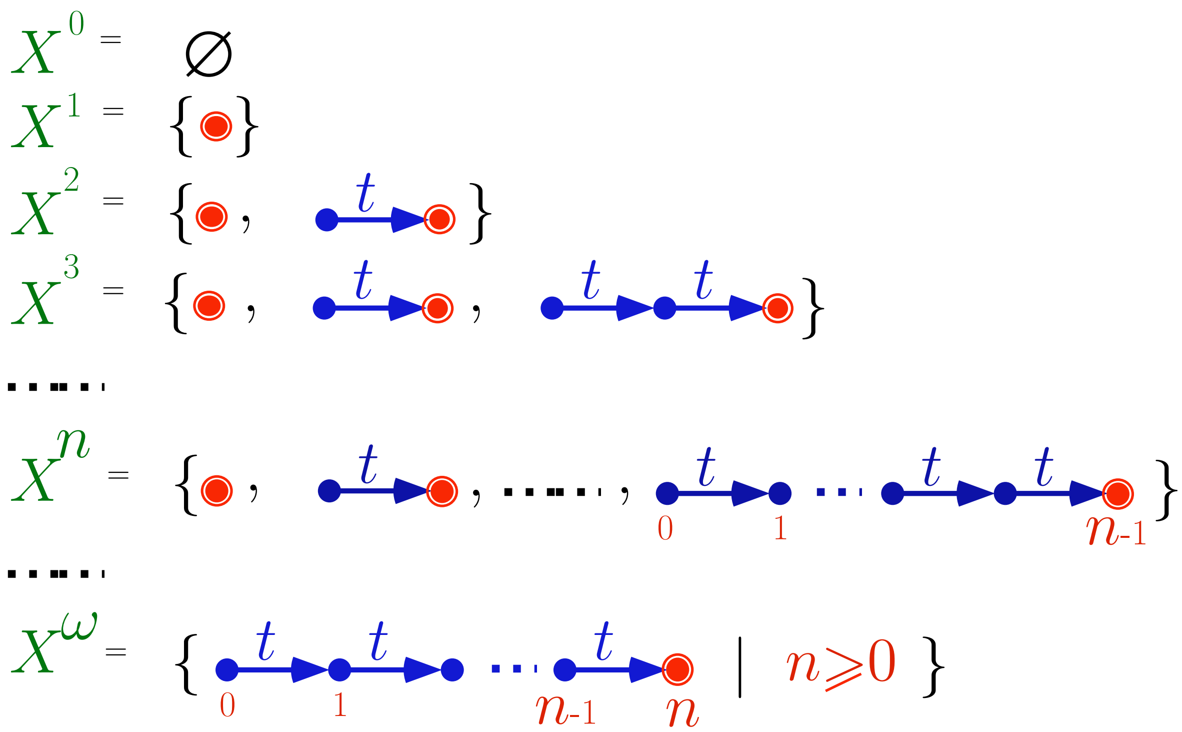
$$\tau^{\check{\vec{+}}} = \mathrm{lfp}_{\emptyset}^{\subseteq} F^{\check{\vec{+}}} = \mathrm{gfp}_{\Sigma^{\vec{+}}}^{\subseteq} F^{\check{\vec{+}}} \tag{2}$$

where the set of finite traces transformer $F^{\check{\vec{+}}}$ is:

$$F^{\check{\vec{+}}}(X) \stackrel{\text{def}}{=} \tau^{\check{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown X$$

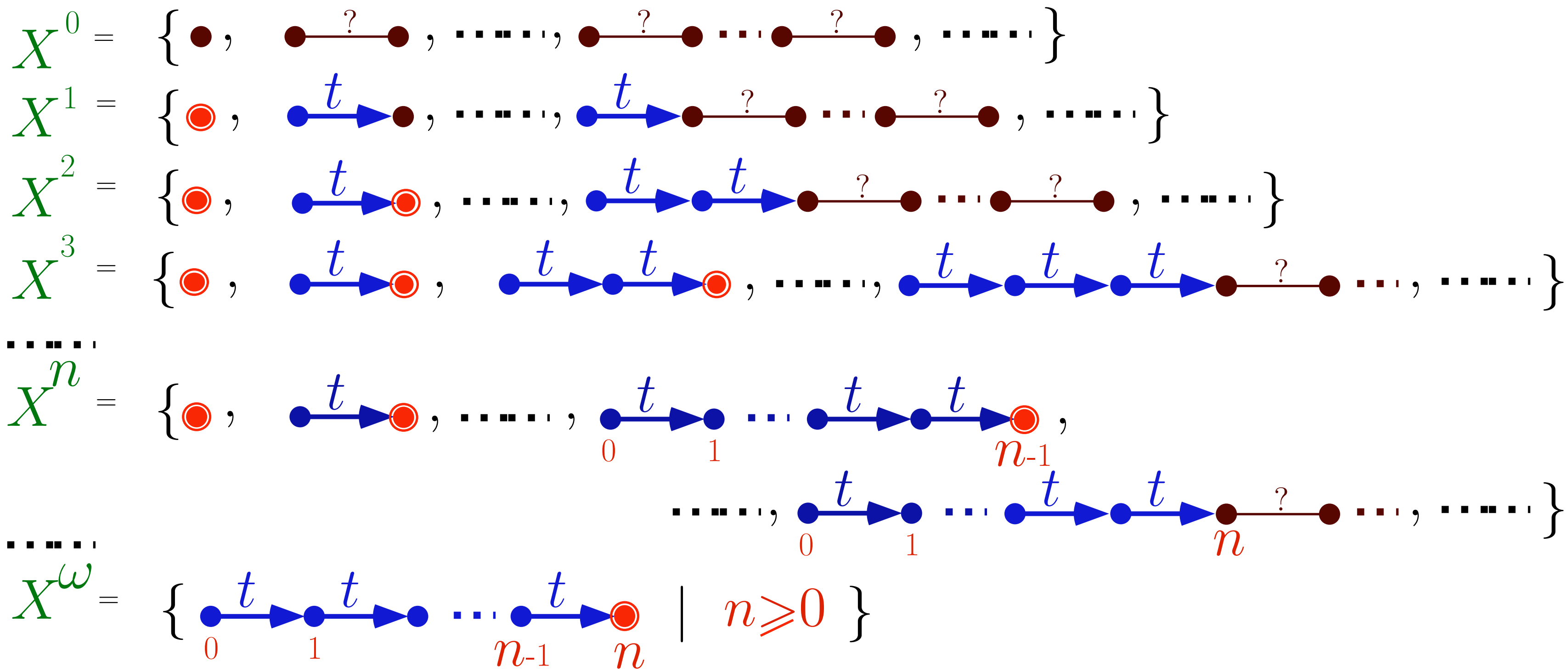
Sketch of Proof

$$\tau^{\vec{\check{+}}} = \bigcup_{i\in\mathbb{N}} \tau^{\vec{\check{i}}} = \mathrm{lfp}_{\emptyset}^{\subseteq} F^{\vec{\check{+}}} \qquad\qquad F^{\vec{\check{+}}}(X) \stackrel{\text{def}}{=} \tau^{\vec{\check{1}}} \cup \tau^{\vec{\dot{2}}} \frown X$$



$$\tau^{\check{\vec{+}}} = \bigcup_{i>0} \tau^{\check{\vec{i}}} = \bigcap_{n\in\mathbb{N}} \Big(\bigcup_{i=1}^{n} \tau^{\check{\vec{i}}} \cup \tau^{\dot{\vec{n+1}}} \frown \Sigma^{\vec{+}} \Big) = \operatorname{gfp}^{\subseteq}_{\Sigma^{\vec{+}}} F^{\check{\vec{+}}}$$

$$F^{\check{\vec{+}}}(X) \stackrel{\text{def}}{=} \tau^{\check{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown X$$



Fixpoint Specification of Maximal Infinitary Trace Semantics of Transition Systems

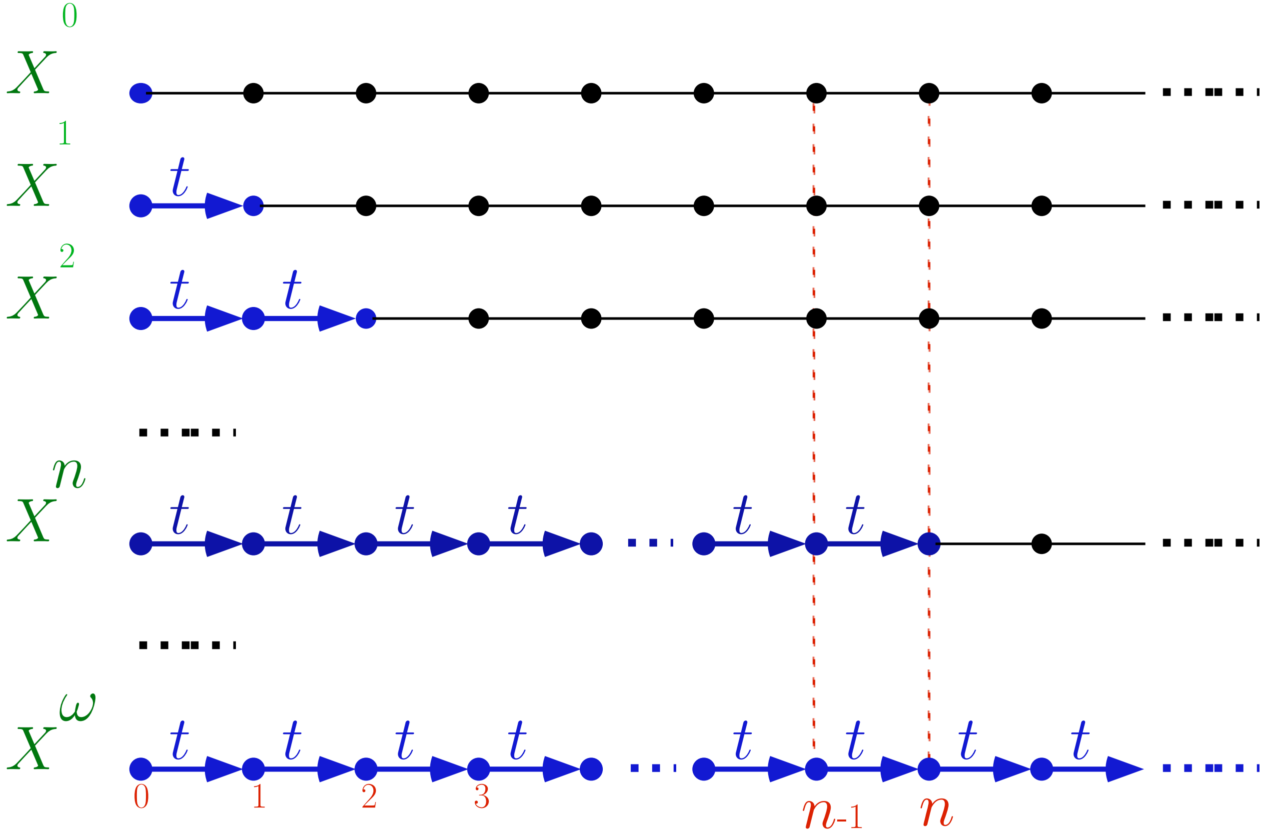
$$\tau^{\vec{\omega}} = \operatorname{gfp}_{\Sigma^{\vec{\omega}}}^{\subseteq} F^{\vec{\omega}} \tag{3}$$

where the set of infinite traces transformer $F^{\vec{\omega}}$ is:

$$F^{\vec{\omega}}(X) \stackrel{\text{def}}{=} \tau^{\dot{\vec{2}}} \frown X$$

Sketch of Proof

$$\tau^{\vec{\omega}} = \bigcap_{n \in \mathbb{N}} \tau^{\dot{\vec{n}}} \frown \Sigma^{\vec{\omega}} = \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}} \qquad F^{\vec{\omega}}(X) \stackrel{\mathrm{def}}{=} \tau^{\dot{\vec{2}}} \frown X$$



Coalesced Powerproduct

- If
  - $\{L^+, L^-\}$ is a *partition* of L (i.e. $L = L^+ \cup L^-$ and $L^+ \cap L^- = \emptyset$);
  - $\langle \wp(L^+), \sqsubseteq^+, \bot^+, \top^+, \sqcup^+, \sqcap^+ \rangle$ and $\langle \wp(L^-), \sqsubseteq^-, \bot^-, \top^-, \sqcup^-, \sqcap^- \rangle$ are posets (respectively cpos, complete lattices);

  then the *coalesced powerproduct* $\langle \wp(L), \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$ is a poset (respectively a cpo, a complete lattice), where:
  - $X^+ \stackrel{\text{def}}{=} X \cap L^+$ and $X^- \stackrel{\text{def}}{=} X \cap L^-$ projections
  - $X \sqsubseteq Y$ iff $X^+ \sqsubseteq^+ Y^+ \wedge X^- \sqsubseteq^- Y^-$ ordering
  - $\bot \stackrel{\text{def}}{=} \bot^+ \cup \bot^-$ infimum
  - $\top \stackrel{\text{def}}{=} \top^+ \cup \top^-$ supremum
  - $\bigsqcup_i X_i \stackrel{\text{def}}{=} \bigsqcup_i^+ (X_i)^+ \cup \bigsqcup_i^- (X_i)^-$ join
  - $\bigsqcap_i X_i \stackrel{\text{def}}{=} \bigsqcap_i^+ (X_i)^+ \cup \bigsqcap_i^- (X_i)^-$ meet

Coalesced Fixpoints Theorem

- If
  - $\langle \wp(L), \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$ is the coalesced powerproduct of $\langle \wp(L^+), \sqsubseteq^+, \bot^+, \top^+, \sqcup^+, \sqcap^+ \rangle$ and $\langle \wp(L^-), \sqsubseteq^-, \bot^-, \top^-, \sqcup^-, \sqcap^- \rangle$
  - $F^+ \in L^+ \longmapsto L^+$ and $F^- \in L^- \longmapsto L^-$ are monotonic (resp. upper-continuous, a complete join morphism)

  then the coalesced fixpoint is defined by:
  - $F \in L \longmapsto L$ where
    $$F(X) \stackrel{\text{def}}{=} F^+(X^+) \cup F^-(X^-)$$
    is monotonic (resp. upper-continuous, a complete join morphism);
  - $$\mathrm{lfp}^{\sqsubseteq} F = \mathrm{lfp}^{\sqsubseteq^+} F^+ \cup \mathrm{lfp}^{\sqsubseteq^-} F^-. \tag{4}$$

Fixpoint Specification of the Maximal Bifinitary Trace Semantics of Transition Systems

- The fixpoint characterization of the bifinitary maximal trace semantics of a transition system $\langle \Sigma, \tau \rangle$ is:

$$
\begin{aligned}
\tau^{\check{\vec{\infty}}} &= \mathrm{lfp}^{\sqsubseteq} F^{\check{\vec{\infty}}} = \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\infty}}} F^{\check{\vec{\infty}}} && (5)\\
F^{\check{\vec{\infty}}} &= \lambda X \bullet \tau^{\check{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown X
\end{aligned}
$$

$$
X \sqsubseteq Y \stackrel{\text{def}}{=} (X \cap \Sigma^{\vec{*}} \subseteq Y \cap \Sigma^{\vec{*}}) \wedge (X \cap \Sigma^{\vec{\omega}} \supseteq Y \cap \Sigma^{\vec{\omega}})
$$

Proof

- $\tau^{\check{\vec{\infty}}} \stackrel{\text{def}}{=} \tau^{\check{\vec{+}}} \cup \tau^{\vec{\omega}} = \mathrm{lfp}^{\subseteq}_{\emptyset} F^{\check{\vec{+}}} \cup \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}} = \mathrm{lfp}^{\subseteq}_{\emptyset} F^{\check{\vec{+}}} \cup \mathrm{lfp}^{\supseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}} = \mathrm{lfp}^{\sqsubseteq} F^{\check{\vec{\infty}}}$ by (2), (3), (4) and:

$$
\begin{aligned}
F^{\check{\vec{+}}}(X) &= F^{\check{\vec{+}}}(X \cap \Sigma^{\vec{*}}) \cup F^{\vec{\omega}}(X \cap \Sigma^{\vec{\omega}}) \\
&= (\tau^{\check{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown (X \cap \Sigma^{\vec{*}})) \cup (\tau^{\dot{\vec{2}}} \frown (X \cap \Sigma^{\vec{\omega}})) \\
&= \tau^{\check{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown ((X \cap \Sigma^{\vec{*}}) \cup (X \cap \Sigma^{\vec{\omega}})) \\
&= \tau^{\check{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown X
\end{aligned}
$$

- $\tau^{\check{\vec{\infty}}} \stackrel{\text{def}}{=} \tau^{\check{\vec{+}}} \cup \tau^{\vec{\omega}} = \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{+}}} F^{\check{\vec{+}}} \cup \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}} = \mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\infty}}} F^{\check{\vec{\infty}}}$ by (2), (3) and the dual of (4).

$\square$

Rule-based Specification of the Maximal Bifinitary Trace Semantics of Transition Systems

- By the equivalence (1) of fixpoint and rule-based definitions, we can define an element S of:

$$\langle \wp(\Sigma^{\vec{\infty}}),\ \sqsubseteq,\ \Sigma^{\vec{\omega}},\ \Sigma^{\vec{+}},\ \sqcup,\ \sqcap \rangle$$

where $X \sqsubseteq Y \stackrel{\text{def}}{=} (X \cap \Sigma^{\vec{+}} \subseteq Y \cap \Sigma^{\vec{+}}) \wedge (X \cap \Sigma^{\vec{\omega}} \supseteq Y \cap \Sigma^{\vec{\omega}})$ by rule-instances:

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

where $P_i, C_i \subseteq \Sigma^{\vec{\infty}}$, such that:

$$S \stackrel{\text{def}}{=} \operatorname{lfp}^{\sqsubseteq} F \qquad \text{with} \qquad F \stackrel{\text{def}}{=} \lambda X \cdot \bigsqcup \{C_i | i \in \Delta \wedge P_i \sqsubseteq X\}$$

Set of Traces Rule-based Specification of the Maximal Bifinitary Trace Semantics of Transition Systems

$$\frac{\perp}{\perp \cup \check{\tau}} \sqsubseteq \qquad \text{where } \perp \stackrel{\text{def}}{=} \Sigma^{\vec{\omega}} \tag{6}$$

$$\frac{T}{\tau^{\dot{\vec{2}}} \frown T} \sqsubseteq \qquad \text{where } T \subseteq \Sigma^{\vec{\infty}} \tag{7}$$

Proof

$$
\begin{aligned}
\Phi &= \lambda X \cdot \bigsqcup \{C \mid \exists \frac{P}{C} : P \sqsubseteq X\} \\
&= \lambda X \cdot \bigsqcup \{\bot \cup \check{\tau} \mid \bot \sqsubseteq X\} \sqcup \bigsqcup \{\tau^{\dot{\vec{2}}} \frown T \mid T \sqsubseteq X\} \\
&= \lambda X \cdot (\bot \cup \check{\tau}) \sqcup \tau^{\dot{\vec{2}}} \frown X \\
&= \lambda X \cdot ((\bot \cup \check{\tau}) \cap \Sigma^{\vec{+}}) \cup (\tau^{\dot{\vec{2}}} \frown X \cap \Sigma^{\vec{+}}) \cup \\
&\qquad ((\bot \cup \check{\tau}) \cap \Sigma^{\vec{\omega}}) \cap (\tau^{\dot{\vec{2}}} \frown X \cap \Sigma^{\vec{\omega}}) \\
&= \lambda X \cdot \check{\tau} \cup (\tau^{\dot{\vec{2}}} \frown X \cap \Sigma^{\vec{+}}) \cup (\tau^{\dot{\vec{2}}} \frown X \cap \Sigma^{\vec{\omega}}) \\
&= \lambda X \cdot \check{\tau} \cup \tau^{\dot{\vec{2}}} \frown X
\end{aligned}
$$

□

Trace Rule-based Specification

- It is more intuitive to reason on a single trace;
- We can define an element S of:

$$\langle \wp(\Sigma^{\vec{\infty}}),\ \sqsubseteq,\ \Sigma^{\vec{\omega}},\ \Sigma^{\vec{+}},\ \sqcup,\ \sqcap \rangle$$

$$\text{where :} \qquad X \sqsubseteq Y \stackrel{\text{def}}{=} (X \cap \Sigma^{\vec{+}} \subseteq Y \cap \Sigma^{\vec{+}}) \wedge (X \cap \Sigma^{\vec{\omega}} \supseteq Y \cap \Sigma^{\vec{\omega}})$$

by rule-schemata:

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

where $P_i \subseteq \Sigma^{\vec{\infty}}$, $c_i \in \Sigma^{\vec{\infty}}$, with rule-instances:

$$\left\{ \frac{P}{\{c_i \mid i \in \Delta \wedge P_i \subseteq P\}}\sqsubseteq \;\middle|\; P \subseteq \Sigma^{\vec{\infty}} \right\}$$

Traces Rule-based Specification of the Maximal Bifinitary Trace Semantics of Transition Systems

- The rule schemata:

$$\frac{\emptyset}{\sigma^1}, \quad \sigma^1 \in \check{\tau} \qquad \frac{\{\sigma\}}{\sigma^2 \frown \sigma}, \quad \sigma^2 \in \tau^{\dot{\vec{2}}},\ \sigma \in \Sigma^{\vec{\infty}}$$

stand for the rule-instances:

$$\left\{ \frac{P}{\{\sigma^1 \mid \sigma^1 \in \check{\tau}\} \cup \{\sigma^2 \frown \sigma \mid \sigma^2 \in \tau^{\dot{\vec{2}}} \wedge \{\sigma\} \subseteq P\}} \;\middle|\; \begin{array}{l} \sigma^2 \in \tau^{\dot{\vec{2}}} \wedge \\ P \subseteq \Sigma^{\vec{\infty}} \end{array} \right\}$$

$$= \left\{ \frac{P}{\check{\tau} \cup \sigma^2 \frown P} \;\middle|\; \sigma^2 \in \tau^{\dot{\vec{2}}} \wedge P \subseteq \Sigma^{\vec{\infty}} \right\}$$

- The rule schemata specify:

$$\operatorname{lfp}^{\sqsubseteq} \Psi = \tau^{\check{\vec{\infty}}}$$

since:

$$\begin{aligned}\Psi &= \lambda X \bullet \bigsqcup \{\check{\tau} \cup \sigma^2 \frown P \mid \sigma^2 \in \tau^{\dot{\vec{2}}} \wedge P \sqsubseteq X\} \\ &= \lambda X \bullet \check{\tau} \cup \tau^{\dot{\vec{2}}} \frown X \qquad \text{by } \sqsubseteq\text{-monotonicity}\end{aligned}$$

Abstract interpretation of order-theoretic formal inductive specifications

Principle of Abstract Interpretation

- Establish a correspondance $\langle\alpha,\ \gamma\rangle$ between a concrete/exact/refined semantics and an abstract/approximate semantics:
  - Abstract semantics $= \alpha$(concrete semantics)   or
  - Concrete semantics $= \gamma$(abstract semantics)
- Derive a specification of the abstract semantics from the given specification of the concrete semantics (or inversely).

Kleenian Fixpoint Abstraction

If $\langle \mathcal{D}^\natural, \sqsubseteq^\natural, \bot^\natural, \sqcup^\natural \rangle$ is a cpo, $\langle \mathcal{D}^\sharp, \sqsubseteq^\sharp \rangle$ is a poset, $F^\natural \in \mathcal{D}^\natural \stackrel{\mathrm{m}}{\longmapsto} \mathcal{D}^\natural$, $F^\sharp \in \mathcal{D}^\sharp \stackrel{\mathrm{m}}{\longmapsto} \mathcal{D}^\sharp$, and

$$F^\sharp \circ \alpha \;=\; \alpha \circ F^\natural$$

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

then

$$\alpha(\mathrm{lfp}^{\sqsubseteq^\natural} F^\natural) \;=\; \mathrm{lfp}^{\sqsubseteq^\sharp} F^\sharp \tag{8}$$

TARSKIAN FIXPOINT ABSTRACTION

If $\langle \mathcal{D}^\natural, \sqsubseteq^\natural, \perp^\natural, \sqcup^\natural \rangle$ and $\langle \mathcal{D}^\sharp, \sqsubseteq^\sharp, \perp^\sharp, \sqcup^\sharp \rangle$ are complete lattices, $F^\natural \in \mathcal{D}^\natural \xrightarrow{\mathrm{m}} \mathcal{D}^\natural$, $F^\sharp \in \mathcal{D}^\sharp \xrightarrow{\mathrm{m}} \mathcal{D}^\sharp$ are monotonic and

– α is a complete $\sqcap$-morphism (a)

– $F^\sharp \circ \alpha \sqsubseteq^\sharp \alpha \circ F^\natural$ (b)

– $\forall y \in \mathcal{D}^\sharp : F^\sharp(y) \sqsubseteq^\sharp y \Longrightarrow \exists x \in \mathcal{D}^\natural : \alpha(x) = y \wedge F^\natural(x) \sqsubseteq^\natural x$ (c)

then

$$\alpha(\mathrm{lfp}^{\sqsubseteq^\natural} F^\natural) = \mathrm{lfp}^{\sqsubseteq^\sharp} F^\sharp \tag{9}$$

Example: Relational and Denotational Semantic Specifications

Finitary Relational Abstraction

Replace finite execution traces $\sigma_0\sigma_1 \ldots \sigma_{n-1}$ by their initial/final states $\langle\sigma_0,\ \sigma_{n-1}\rangle$:

- $\mathtt{@}^+ \in \Sigma^{\vec{+}} \longmapsto (\Sigma \times \Sigma)$
  $\mathtt{@}^+(\sigma) \stackrel{\text{def}}{=} \langle\sigma_0,\ \sigma_{n-1}\rangle,$
  $n \in \mathbb{N}_+,\ \sigma \in \Sigma^{\vec{n}}$
- $\alpha^+(X) \stackrel{\text{def}}{=} \{\mathtt{@}^+(\sigma) \mid \sigma \in X\}$
  $\gamma^+(Y) \stackrel{\text{def}}{=} \{\sigma \mid \mathtt{@}^+(\sigma) \in Y\}$
- $\langle\wp(\Sigma^{\vec{+}}),\ \subseteq\rangle \underset{\alpha^+}{\overset{\gamma^+}{\longleftarrow\!\!\!\longrightarrow\!\!\!\!\rightarrow}} \langle\wp(\Sigma \times \Sigma),\ \subseteq\rangle$ Galois connection

Maximal Finitary/Angelic Relational/Big-step Semantics of a Transition System

- Transition system $\langle \Sigma,\ \tau \rangle$
- Fixpoint specification:

$$\tau^{\check{+}} \stackrel{\text{def}}{=} \alpha^{+}(\tau^{\vec{\check{+}}}) = \alpha^{+}(\operatorname{lfp}_{\emptyset}^{\subseteq} F^{\vec{\check{+}}})$$

- By the Kleenian fixpoint abstraction th. (8) [9], we get the fixpoint specification:

$$\tau^{\check{+}} = \operatorname{lfp}_{\emptyset}^{\subseteq} F^{\check{+}} \qquad F^{\check{+}}(X) \stackrel{\text{def}}{=} \check{\bar{\tau}} \cup \tau \circ X \tag{10}$$

$$\check{\bar{\tau}} \stackrel{\text{def}}{=} \{\langle s,\ s \rangle \in \Sigma \mid \forall s' \in \Sigma : \neg(s\ \tau\ s')\}$$

[9] the Tarskian fixpoint abstraction does not apply since α^{+} is not co-continuous

Infinitary Relational Abstraction

Replace infinite execution traces $\sigma_0\sigma_1\ldots\sigma_n\ldots$ by their initial state $\langle\sigma_0,\ \bot\rangle$, marking nontermination by Scott's $\bot$:

- $@^\omega \in \Sigma^{\vec{\omega}} \longmapsto \Sigma \times \{\bot\}$ [10]

  $\bot \notin \Sigma$ — non-termination notation

  $@^\omega(\sigma) \stackrel{\text{def}}{=} \langle\sigma_0,\ \bot\rangle,\ \sigma \in \Sigma^{\vec{\omega}}$
- $\alpha^\omega(X) \stackrel{\text{def}}{=} \{@^\omega(\sigma) \mid \sigma \in X\}$

  $\gamma^\omega(Y) \stackrel{\text{def}}{=} \{\sigma \mid @^\omega(\sigma) \in Y\}$
- $\langle\wp(\Sigma^{\vec{\omega}}),\ \subseteq\rangle \underset{\alpha^\omega}{\overset{\gamma^\omega}{\leftrightarrows}} \langle\wp(\Sigma \times \{\bot\}),\ \subseteq\rangle$ — Galois connection

---

[10] or isomorphically $\alpha^\omega \in \wp(\Sigma^{\vec{\omega}}) \longmapsto \wp(\Sigma)$.

INFINITARY RELATIONAL SEMANTICS OF A TRANSITION SYSTEM

- Transition system $\langle \Sigma, \tau \rangle$
- Infinitary relational semantics:

$$\tau^\omega \stackrel{\text{def}}{=} \alpha^\omega(\tau^{\vec{\omega}}) = \alpha^\omega(\text{gfp}^{\subseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}}) = \alpha^\omega(\text{lfp}^{\supseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}})$$

- By the Tarskian fixpoint abstraction th. (9), we get the fixpoint specification [11]:

$$\begin{aligned} \tau^\omega &= \text{lfp}^{\supseteq}_{\Sigma\times\{\perp\}} F^\omega = \text{gfp}^{\subseteq}_{\Sigma\times\{\perp\}} F^\omega \\ F^\omega(X) &= \tau \circ X \end{aligned} \tag{11}$$

[11] The Kleene fixpoint abstraction th. (8) does not apply since α^ω is not co-continuous.

Bifinitary/Natural Relational Abstraction

- $\alpha^{\infty} \in \wp(\Sigma^{\vec{\infty}}) \longmapsto \wp(\Sigma \times \Sigma_{\perp})$, $\qquad \Sigma_{\perp} \stackrel{\text{def}}{=} \Sigma \cup \{\perp\}$
  $\alpha^{\infty}(X) \stackrel{\text{def}}{=} \alpha^{+}(X^{\vec{+}}) \cup \alpha^{\omega}(X^{\vec{\omega}})$

- $X^{+} = X \cap (\Sigma \times \Sigma)$ finitary projection
  $X^{\omega} = X \cap (\Sigma \times \{\perp\})$ infinitary projection

Maximal Bifinitary/Natural Relational Semantics

- $$\begin{aligned}
&\tau^{\check{\infty}} \\
\stackrel{\text{def}}{=}\ & \alpha^{\infty}(\tau^{\check{\vec{\infty}}}) \\
=\ & \alpha^{+}((\tau^{\check{\vec{\infty}}})^{\vec{+}}) \cup \alpha^{\omega}((\tau^{\check{\vec{\infty}}})^{\vec{\omega}}) \\
=\ & \alpha^{+}(\tau^{\check{\vec{+}}}) \cup \alpha^{\omega}(\tau^{\vec{\omega}}) \\
=\ & \tau^{\check{+}} \cup \tau^{\omega} \\
=\ & \{\langle s,\ s'\rangle \mid s \xrightarrow{\star} s' \wedge s' \not\longrightarrow\} \cup \{\langle s,\ \bot\rangle \mid s \xrightarrow{\omega}\}
\end{aligned}$$

where:

$$\begin{aligned}
s \xrightarrow{\star} s' &\stackrel{\text{def}}{=} \exists n \in \mathbb{N}_+ : \exists \sigma \in \Sigma^{\vec{n}} : s = \sigma_0 \wedge \forall i < n-1 : \sigma_i \ \tau \ \sigma_{i+1} \\
&\qquad\qquad \wedge s' = \sigma_{n-1} \\
s \not\longrightarrow &\stackrel{\text{def}}{=} \forall s' \in \Sigma : \neg(s \ \tau \ s') \\
s \xrightarrow{\omega} &\stackrel{\text{def}}{=} \exists \sigma \in \Sigma^{\vec{\omega}} : s = \sigma_0 \wedge \forall i \in \mathbb{N} : \sigma_i \ \tau \ \sigma_{i+1}
\end{aligned}$$

Fixpoint Maximal Bifinitary/Natural Relational Semantics of a Transition System

- Transition system $\langle \Sigma, \tau \rangle$
- $$\begin{aligned}\tau^{\check{\infty}} &\stackrel{\text{def}}{=} \tau^{\check{+}} \cup \tau^{\omega} \\ &= \operatorname{lfp}_{\emptyset}^{\subseteq} \lambda X \cdot \check{\check{\tau}} \cup \tau \circ X \;\cup\; \operatorname{lfp}_{\Sigma \times \{\bot\}}^{\supseteq} \lambda X \cdot \tau \circ X \\ &= \operatorname{lfp}_{\bot^{\check{\infty}}}^{\sqsubseteq^{\check{\infty}}} F^{\check{\infty}} \qquad (12)\end{aligned}$$

  fixpoint specification (by the coalesced fixpoints th. (4)):

  $$\begin{aligned}F^{\check{\infty}}(X) &\stackrel{\text{def}}{=} \lambda X \cdot \check{\check{\tau}} \cup \tau \circ X^{+} \cup \tau \circ X^{\omega} \\ &= \lambda X \cdot \check{\check{\tau}} \cup \tau \circ (X^{+} \cup X^{\omega}) \\ &= \lambda X \cdot \check{\check{\tau}} \cup \tau \circ X\end{aligned}$$

We have the bifinitary relational transformer:

$$F^{\check{\infty}} \in \wp(\Sigma \times \Sigma_\perp) \xrightarrow{\mathrm{m}} \wp(\Sigma \times \Sigma_\perp)$$

where the semantic domain:

$$\langle \wp(\Sigma \times \Sigma_\perp),\ \sqsubseteq^{\check{\infty}},\ \perp^{\check{\infty}},\ \sqcup^{\infty} \rangle$$

is a complete lattice, with

- $X \sqsubseteq^{\check{\infty}} Y \stackrel{\mathrm{def}}{=} X^+ \subseteq Y^+ \ \wedge\ X^\omega \supseteq Y^\omega$ ordering
- $\perp^{\check{\infty}} \ = \ \Sigma \times \{\perp\}$ infimum
- $\bigsqcup_i^{\infty} X_i \stackrel{\mathrm{def}}{=} \bigcup_i {X_i}^+ \ \cup\ \bigcap_i {X_i}^\omega$ join

Abstraction by Parts

$$\tau^{\check{\infty}} = \alpha^{\infty}(\mathrm{lfp}_{\perp^{\vec{\infty}}}^{\sqsubseteq^{\vec{\infty}}} F^{\vec{\check{\infty}}}) = \mathrm{lfp}_{\perp^{\check{\infty}}}^{\sqsubseteq^{\check{\infty}}} F^{\check{\infty}}$$

- The finitary part transfers through α^{+} by the Kleenian fixpoint abstraction theorem (8) (but the Tarskian one (9) is not applicable);
- The infinitary part transfers through α^{ω} by the Tarskian fixpoint abstraction theorem (9) (but the Kleenian one (8) is not applicable);
- The whole transfers through α^{∞} by parts using the coalesced fixpoints theorem (4) (although none of the Kleenian (8) and Tarskian (9) fixpoint abstraction theorems is applicable).

Relational to Denotational Semantics Abstraction

The maximal bifinitary/natural relational to denotational semantics abstraction is the right image isomorphism:

- $\langle \wp(\mathcal{D} \times \mathcal{E}),\ \leqslant\rangle$ semantic domain
- $\langle \wp(\mathcal{D} \times \mathcal{E}),\ \leqslant\rangle \xleftarrow[\alpha^{\blacktriangleright}]{\gamma^{\blacktriangleright}} \langle \mathcal{D} \longmapsto \wp(\mathcal{E}),\ \dot{\leqslant}\rangle$ right-image Galois isomorphism

where:

$$\alpha^{\blacktriangleright}(R) \stackrel{\text{def}}{=} R^{\blacktriangleright} = \lambda x \bullet \{y \mid \langle x,\ y\rangle \in R\}$$

$$\gamma^{\blacktriangleright}(f) \stackrel{\text{def}}{=} \{\langle x,\ y\rangle \mid y \in f(x)\}$$

$$f \mathrel{\dot{\leqslant}} g \stackrel{\text{def}}{=} \gamma^{\blacktriangleright}(f) \leqslant \gamma^{\blacktriangleright}(g)$$

Fixpoint Specification of the Natural Denotational Semantics

- $\tau^{\natural} \stackrel{\text{def}}{=} \alpha^{\blacktriangleright}(\tau^{\infty})$ right-image abstraction of the bifinitary relational semantics

$$= \operatorname{lfp}_{\dot{\bot}^{\natural}}^{\dot{\sqsubseteq}^{\natural}} F^{\natural} \tag{13}$$

where

- $\dot{\check{\tau}} \stackrel{\text{def}}{=} \lambda s \cdot \{s \mid \forall s' \in \Sigma : \neg(s \;\tau\; s')\}$
- $f^{\blacktriangleright} \stackrel{\text{def}}{=} \lambda P \cdot \{f(s) \mid s \in P\}$
- $\tau^{\bullet\!\blacktriangleright} \stackrel{\text{def}}{=} \lambda s \cdot \{s' \mid s \;\tau\; s'\}$
- $F^{\natural} \in \dot{D}^{\natural} \stackrel{\text{m}}{\longmapsto} \dot{D}^{\natural}, \qquad F^{\natural}(f) \stackrel{\text{def}}{=} \dot{\check{\tau}} \;\dot{\cup}\; \dot{\bigcup} f^{\blacktriangleright} \circ \tau^{\bullet\!\blacktriangleright}$

  is a $\dot{\sqsubseteq}^{\natural}$-monotone map on the complete lattice

$$\langle \dot{D}^{\natural}, \dot{\sqsubseteq}^{\natural}, \dot{\bot}^{\natural}, \dot{\top}^{\natural}, \dot{\sqcup}^{\natural}, \dot{\sqcap}^{\natural} \rangle \quad \text{where} \quad \dot{D}^{\natural} \stackrel{\text{def}}{=} \Sigma \longmapsto \wp(\Sigma_{\bot})$$

Rule-based Specification of the Natural Denotational Semantics

- The natural denotational semantics

$$\operatorname{lfp}^{\dot{\sqsubseteq}^\natural}_{\dot{\perp}^\natural} F^\natural$$

where

$$F^\natural(f) \stackrel{\text{def}}{=} \dot{\check{\tau}} \;\dot{\cup}\; \dot{\bigcup} f^\blacktriangleright \circ \tau^{\bullet\!\blacktriangleright}$$

is also defined by the following rules:

$$\frac{s' \in \dot{\check{\tau}}(s)}{s' \in f(s)} \qquad \frac{s\tau s', \quad s'' \in f(s')}{s'' \in f(s)} \qquad \frac{s\tau s', \quad \perp \in f(s')}{\perp \in f(s)}$$

<u>EXAMPLE</u>: RULE-BASED SPECFICATION OF A NONDETERMINISTIC DENOTATIONAL SEMANTICS

Syntax of a Nondeterministic Imperative Expression Language

- $\mathsf{p} \in \mathsf{P}$ programs

  $\mathsf{p} \rightarrow \mathsf{n} \mid \mathsf{v} \mid \mathsf{?} \mid \mathsf{p}_1 - \mathsf{p}_2 \mid \mathsf{v} := \mathsf{p} \mid \texttt{if } \mathsf{p}_1 \texttt{ then } \mathsf{p}_2 \texttt{ else } \mathsf{p}_3 \mid$
  $\quad \mathsf{p}_1 \; ; \; \mathsf{p}_2 \mid \texttt{repeat } \mathsf{p}_1 \texttt{ until } \mathsf{p}_2$

Semantic Domain

- $x \in \mathbb{Z}_\Omega$ values
- $\rho \in \mathcal{E} \stackrel{\text{def}}{=} \mathsf{V} \longmapsto \mathbb{Z}_\Omega$ environments
- $\langle x,\ \rho \rangle \in \Sigma \stackrel{\text{def}}{=} \mathbb{Z}_\Omega \times \mathcal{E}$ states
- $\bot \notin \Sigma$, $\Sigma_\bot \stackrel{\text{def}}{=} \Sigma \cup \{\bot\}$ non-termination
- $\dot{D}^\natural \stackrel{\text{def}}{=} \mathcal{E} \longmapsto \wp(\Sigma_\bot)$ semantic domain
- $\langle \dot{D}^\natural,\ \dot{\sqsubseteq}^\natural,\ \dot{\bot}^\natural,\ \dot{\top}^\natural,\ \dot{\sqcup}^\natural,\ \dot{\sqcap}^\natural \rangle$ complete lattice
- $\mathcal{S}^\natural[\![\mathsf{p}]\!] \in \mathcal{E} \longmapsto \wp(\Sigma_\bot)$ bifinitary nondeterministic denotational semantics

NUMBERS $\mathcal{S}^\natural[\![\mathsf{n}]\!]$

- $\mathcal{N}[\![\mathsf{0}]\!] \stackrel{\text{def}}{=} 0$
- $\ldots$
- $\mathcal{N}[\![\mathsf{9}]\!] \stackrel{\text{def}}{=} 9$
- $\mathcal{N}[\![\mathsf{nd}]\!] \stackrel{\text{def}}{=} (10 \times \mathcal{N}[\![\mathsf{n}]\!]) + \mathcal{N}[\![\mathsf{d}]\!]$
- $\dfrac{\mathtt{tt}}{\langle \mathcal{N}[\![\mathsf{n}]\!],\ \rho\rangle \ \in\ \mathcal{S}^\natural[\![\mathsf{n}]\!]\rho}$

VARIABLES $\mathcal{S}^\natural[\![\mathsf{v}]\!]$

- $$\frac{\mathrm{tt}}{\langle \rho(\mathsf{v}),\ \rho\rangle \in \mathcal{S}^\natural[\![\mathsf{v}]\!]\rho}$$

RANDOM $\mathcal{S}^\natural[\![?]\!]$

- $$\frac{i \ \in\ \mathbb{Z}}{\langle i,\ \rho\rangle \ \in\ \mathcal{S}^\natural[\![?]\!]\rho}$$

Substraction $\mathcal{S}^\natural[\![\mathsf{e}_1 - \mathsf{e}_2]\!]$

- $$\frac{\langle\Omega,\ \rho'\rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho}{\langle\Omega,\ \rho'\rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1 - \mathsf{p}_2]\!]\rho}$$

- $$\frac{\langle i,\ \rho'\rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho, \quad \langle\Omega,\ \rho''\rangle \in \mathcal{S}^\natural[\![\mathsf{p}_2]\!]\rho, \quad i \in \mathbb{Z}}{\langle\Omega,\ \rho''\rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1 - \mathsf{p}_2]\!]\rho}$$

- $$\frac{\langle i,\ \rho'\rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho, \quad \langle j,\ \rho''\rangle \in \mathcal{S}^\natural[\![\mathsf{p}_2]\!]\rho', \quad i, j \in \mathbb{Z}}{\langle i - j,\ \rho''\rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1 - \mathsf{p}_2]\!]\rho}$$

- $$\frac{\bot \in \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho}{\bot \in \mathcal{S}^\natural[\![\mathsf{p}_1 - \mathsf{p}_2]\!]\rho}$$

- $$\frac{\langle i,\ \rho'\rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho, \quad \bot \in \mathcal{S}^\natural[\![\mathsf{p}_2]\!]\rho', \quad i \in \mathbb{Z}}{\bot \in \mathcal{S}^\natural[\![\mathsf{p}_1 - \mathsf{p}_2]\!]\rho}$$

Assignment $\mathcal{S}^\natural[\![\mathsf{v} := \mathsf{e}]\!]$

- $$\frac{\langle \Omega,\ \rho' \rangle \in \mathcal{S}^\natural[\![\mathsf{p}]\!]\rho}{\langle \Omega,\ \rho' \rangle \in \mathcal{S}^\natural[\![\mathsf{v} := \mathsf{p}]\!]\rho}$$
- $$\frac{\langle i,\ \rho' \rangle \in \mathcal{S}^\natural[\![\mathsf{p}]\!]\rho, \quad i \in \mathbb{Z}}{\langle i,\ \rho'[\mathsf{v} := i] \rangle \in \mathcal{S}^\natural[\![\mathsf{v} := \mathsf{p}]\!]\rho}$$
- $$\frac{\bot \in \mathcal{S}^\natural[\![\mathsf{p}]\!]\rho}{\bot \in \mathcal{S}^\natural[\![\mathsf{v} := \mathsf{p}]\!]\rho}$$

CONDITIONAL $\mathcal{S}^\natural[\![\texttt{if e}_1\ \texttt{then p}_2\ \texttt{else p}_3]\!]$

- $$\frac{\langle \Omega,\ \rho' \rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho}{\langle \Omega,\ \rho' \rangle\ \in\ \mathcal{S}^\natural[\![\texttt{if p}_1\ \texttt{then p}_2\ \texttt{else p}_3]\!]\rho}$$
- $$\frac{\langle 0,\ \rho' \rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho, \quad \sigma_2\ \in\ \mathcal{S}^\natural[\![\mathsf{p}_2]\!]\rho'}{\sigma_2\ \in\ \mathcal{S}^\natural[\![\texttt{if p}_1\ \texttt{then p}_2\ \texttt{else p}_3]\!]\rho}$$
- $$\frac{\langle i,\ \rho' \rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho, \quad \sigma_3\ \in\ \mathcal{S}^\natural[\![\mathsf{p}_3]\!]\rho', \quad i\ \in\ \mathbb{Z} - \{0\}}{\sigma_3\ \in\ \mathcal{S}^\natural[\![\texttt{if p}_1\ \texttt{then p}_2\ \texttt{else p}_3]\!]\rho}$$
- $$\frac{\bot\ \in\ \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho}{\bot\ \in\ \mathcal{S}^\natural[\![\texttt{if p}_1\ \texttt{then p}_2\ \texttt{else p}_3]\!]\rho}$$

Sequential Composition $\mathcal{S}^\natural[\![\mathsf{e}_1 \;;\; \mathsf{p}_2]\!]$

- $$\frac{\langle \Omega,\ \rho' \rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho}{\langle \Omega,\ \rho' \rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1 \;;\; \mathsf{p}_2]\!]\rho}$$
- $$\frac{\langle i,\ \rho' \rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho, \quad \sigma_2 \in \mathcal{S}^\natural[\![\mathsf{p}_2]\!]\rho', \quad i \in \mathbb{Z}}{\sigma_2 \in \mathcal{S}^\natural[\![\mathsf{p}_1 \;;\; \mathsf{p}_2]\!]\rho}$$
- $$\frac{\bot \in \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho}{\bot \in \mathcal{S}^\natural[\![\mathsf{p}_1 \;;\; \mathsf{p}_2]\!]\rho}$$

Repetition $\mathcal{S}^\natural[\![\texttt{repeat}\ \mathsf{p}_1\ \texttt{until}\ \mathsf{p}_2]\!]$

- [12] $$\frac{\bot \in \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho}{\bot \in \mathcal{S}^\natural[\![\texttt{repeat}\ \mathsf{p}_1\ \texttt{until}\ \mathsf{p}_2]\!]\rho}$$
- [13] $$\frac{\langle\Omega,\ \rho'\rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho}{\langle\Omega,\ \rho'\rangle \in \mathcal{S}^\natural[\![\texttt{repeat}\ \mathsf{p}_1\ \texttt{until}\ \mathsf{p}_2]\!]\rho}$$
- [14] $$\frac{\langle i,\ \rho'\rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho, \quad \bot \in \mathcal{S}^\natural[\![\mathsf{p}_2]\!]\rho'}{\bot \in \mathcal{S}^\natural[\![\texttt{repeat}\ \mathsf{p}_1\ \texttt{until}\ \mathsf{p}_2]\!]\rho}$$
- [15] $$\frac{\langle i,\ \rho'\rangle \in \mathcal{S}^\natural[\![\mathsf{p}_1]\!]\rho, \quad \langle\Omega,\ \rho''\rangle \in \mathcal{S}^\natural[\![\mathsf{p}_2]\!]\rho'}{\langle\Omega,\ \rho''\rangle \in \mathcal{S}^\natural[\![\texttt{repeat}\ \mathsf{p}_1\ \texttt{until}\ \mathsf{p}_2]\!]\rho}$$

---

12 Body does not terminate.
13 Body is erroneous, return error.
14 Body terminates but test does not.
15 Body terminates, test is erroneous, return error.

- [16] $$\frac{\langle i,\ \rho'\rangle \in \mathcal{S}^\natural[\![\mathtt{p}_1]\!]\rho, \quad \langle 0,\ \rho''\rangle \in \mathcal{S}^\natural[\![\mathtt{p}_2]\!]\rho'}{\langle i,\ \rho''\rangle\ \in\ \mathcal{S}^\natural[\![\mathtt{repeat}\ \mathtt{p}_1\ \mathtt{until}\ \mathtt{p}_2]\!]\rho}$$

- [17] $$\frac{\begin{array}{r}\langle i,\ \rho'\rangle\ \in\ \mathcal{S}^\natural[\![\mathtt{p}_1]\!]\rho, \\ \langle j,\ \rho''\rangle\ \in\ \mathcal{S}^\natural[\![\mathtt{p}_2]\!]\rho', \quad j\ \in\ \mathbb{Z}-\{0\}, \\ \sigma_3\ \in\ \mathcal{S}^\natural[\![\mathtt{repeat}\ \mathtt{p}_1\ \mathtt{until}\ \mathtt{p}_2]\!]\rho''\end{array}}{\sigma_3\ \in\ \mathcal{S}^\natural[\![\mathtt{repeat}\ \mathtt{p}_1\ \mathtt{until}\ \mathtt{p}_2]\!]\rho}$$

---

16 Body terminates, test is true, return value of the last iteration.

17 Body terminates, test is false, repeat.

Abstraction to: Natural/Big Step Structured Operational Semantics

- This abstraction, which forgets about nontermination, is:

$$\alpha \in (\mathcal{E} \longmapsto \wp(\Sigma_\perp)) \longmapsto (\mathcal{E} \longmapsto \wp(\Sigma))$$
$$\alpha(S)\rho \stackrel{\text{def}}{=} S(\rho) - \{\perp\}$$

- To get the rule-based specification:
  - Eliminate the infinitary rules (involving $\perp$);
  - Classical interpretation of the rules (for $\subseteq$).

Conclusion

- Declarative specification methods are fundamental in computer science;
- Set-theoretic rule-based specifications are commonly used (syntax, semantics, typing, program static analysis, etc.);
- Order-theoretic rule-based specifications are a useful generalization;

  $\Rightarrow$ e.g. denotational semantics in rule-based style!