Design of Semantics by Abstract Interpretation

Patrick COUSOT

École Normale Supérieure

DMI, 45, rue d'Ulm

75230 Paris cedex 05

France

cousot@dmi.ens.fr

http://www.dmi.ens.fr/~cousot

MPI-Kolloquium, Max-Planck-Institut für Informatik, Saarbrücken, am Montag, dem 2. Juni 1997 um 14.15 Uhr [1]

[1] Extended version of the invited address at MFPS XIII, CMU, Pittsburgh, March 24, 1997

Content

Application of abstract interpretation ideas to the design of formal semantics:

- Examples of abstract interpretations;
- Abstraction of fixpoint semantics;
  - Maximal **trace semantics** of nondeterministic transition systems;
  - Abstraction of the trace into a natural/demoniac/angelic **relational semantics**;

.../...

.../...
- Abstraction of the relational into a **nondeterministic** Plotkin/-Smyth/Hoare **denotational/functional semantics**;
- Abstraction of the natural/demoniac relational into a **deterministic denotational/functional semantics**; Scott's semantics;
- Abstraction of nondeterministic denotational semantics to weakest precondition/strongest postcondition **predicate transformer semantics**;
- Abstraction of predicate transformer semantics to à la Hoare **axiomatic semantics**; Program proof methods;
- Extension to the λ-calculus.

EXAMPLES OF ABSTRACT INTERPRETATIONS

Applications of Abstract Interpretation

- Mainly used for specifying *program analyzers* constructively derived from a formal semantics;
- Such analyzers can be used to statically and fully automatically determine *run-time properties of programs*;
- Such run-time information can be used in complement to classical program provers, model-checkers, ... for program *verification* (abstract debugging, ...) and *transformation* (compiler optimization, partial evaluation, parallelization, ...);
- We will show that abstract interpretation can be used to relate and *design program semantics* (and program proof methods).

Program Analysis by Abstract Interpretation

- (Bit-vector) data flow analysis;
- Strictness analysis and comportment analysis (generalizing strictness, termination, projection and PER analysis);
- Binding time analysis;
- Pointer analysis;
- Set/grammar-based analysis;
- Data dependence analysis (e.g. for vectorization/parallelization);
- Descriptive/soft and prescriptive (polymorphic) typing and type inference;
- Effect systems;
- ...

Approximation

- The central idea of abstract interpretation [2, 3] is that of *approximation*;
- A *program analyzer* computes a finite approximation of the infinite set of possible run-time behaviors of the program for all possible execution environments (inputs, interrupts, ...);
- A *program semantics* specifies an approximation of the run-time program behaviors in all possible execution environments abstracting away from implementation details.

---

[2] P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Conference Record of the Fourth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 238–252, Los Angeles, California, 1977. ACM Press, New York, New York, USA.

[3] P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Conference Record of the Sixth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 269–282, San Antonio, Texas, 1979. ACM Press, New York, USA.

Program Debugging by Abstract Interpretation

- SYNTOX [4, 5] by François Bourdoncle: interval analysis for PASCAL programs;
- For *abstract debugging*, the user can provide:
  - Invariant assertions: `{% ... %}`,
  - Intermittent assertions: `{% ... ? %}` (termination is required by `{% true ? %}` before final `end.`),
- At each program point the analysis provides for each numerical variable `v` a corresponding invariant interval assertion (`v [l..h]`). A star (`*`) on one of the bounds (first: `First Condition`, next: `»`, previous: `«`) indicates a *necessary* condition in the form of a run-time check to be inserted in the program for the user assertions to be satisfied. A sharp `#` indicates a possible overflow.

[4] F. Bourdoncle, *Abstract Debugging of Higher-Order Imperative Languages*, Proc. PLDI'93, ACM Press, 1993, pp. 46–55.

[5] http://www.ensmp.fr/ bourdonc/syntox.tar.Z

- Arithmetic
  congruences [8]:
  $$x = 1 \bmod 2$$
  $$\wedge\ y = 0 \bmod 2$$

- Interval
  congruences [9]:
  $$x \in [0,\,2] \bmod 4$$
  $$\wedge\ y = [0,\,1] \bmod 3$$

[8] P. Granger. Static analysis of arithmetical congruences. *Int. J. of Comp. Math.*, 30:165–190, 1989.

[9] F. Masdupuy. Semantic analysis of interval congruences. In D. Bjørner, M. Broy, and I.V. Pottosin, editors, *Proc. FMPA*, Academgorodok, Novosibirsk, Russia, LNCS 735, pages 142–155. Springer-Verlag, June 28–July 2, 1993.

Examples of independent numerical abstractions

- Signs [6]:
  $$x > 0$$
  $$\wedge\ y > 0$$

- Intervals [7]:
  $$1 \le x \le 5$$
  $$\wedge\ 1 \le y \le 4$$

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

[7] P. Cousot and R. Cousot. Static determination of dynamic properties of programs. In *Proc. 2nd International Symposium on Programming*, pages 106–130. Dunod, 1976.

Examples of relational numerical abstractions

- Linear equalities [10]:
  $$-3x + 4y = 1$$
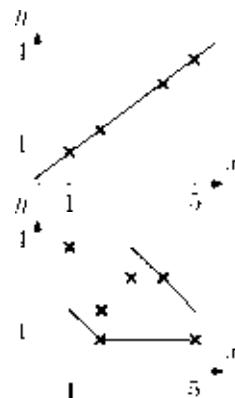
- Simple sections [11]:
  $$1 \le x \le 5$$
  $$\wedge\ 1 \le y \le 4$$
  $$\wedge\ 3 \le x + y \le 7$$
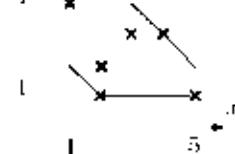
[10] M. Karr. Affine relationships among variables of a program. *Acta Inf.*, 6:133–151, 1976.

[11] V. Balasundaram and K. Kennedy. A technique for summarizing data access and its use in parallelism enhancing transformations. In *SIGPLAN'89 PLDI*, pages 41–53, Portland, Ore., June 21–23, 1989.

- Linear inequalities [12]:
$$3x + y \geq 7$$
$$\wedge \; 2x + y \leq 11$$
$$\wedge \;\;\;\;\;\;\; y \geq 1$$
$$\wedge \; x + 3y \leq 13$$

- Linear congruences [13]:
$$2x + y = 1 \bmod 2$$
$$\wedge \;\;\;\;\; y = 0 \bmod 2$$

---

[12] P. Cousot and N. Halbwachs. Automatic discovery of linear restraints among variables of a program. In 5th POPL, pages 84–97, Tucson, Arizona, 1978. ACM Press.

[13] P. Granger. Static analysis of linear congruence equalities among variables of a program. In S. Abramsky and T.S.E. Maibaum, editors, TAPSOFT'91, Proc. Int. Joint Conf. on Theory and Practice of Software Development, Brighton, U.K., Volume 1 (CAAP'91), LNCS 493, pages 169–192. Springer-Verlag, 1991.

- Trapezoidal congruences [14, 15]:

---
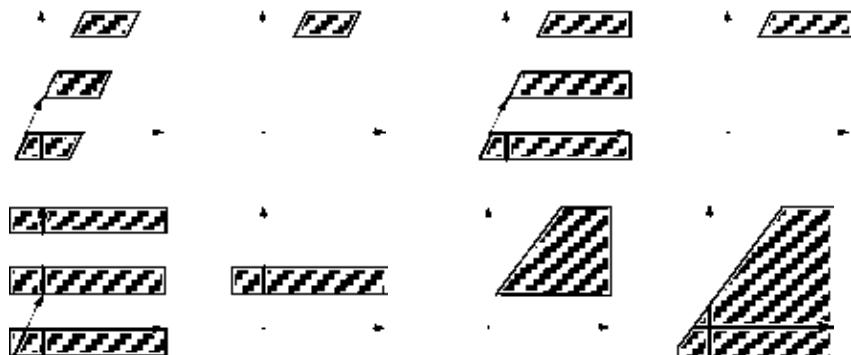
[14] F. Masdupuy. Using abstract interpretation to detect array data dependencies. In Proc. International Symposium on Supercomputing, pages 19–27, Fukuoka, Japan, Nov. 1991. Kyushu U. Press.

[15] F. Masdupuy. Array operations abstraction using semantic analysis of trapezoid congruences. In Proc. ACM International Conference on Supercomputing, ICS'92, pages 226–235, Washington D.C., July 1992.

$$\boxed{\text{ABSTRACTION OF FIXPOINT SEMANTICS}}$$

Fixpoint Semantics Specification $\langle D, F \rangle$

- $\langle D, \sqsubseteq, \bot, \sqcup \rangle$ Semantic domain
  - $\langle D, \sqsubseteq \rangle$ poset
  - $\bot$ infimum
  - $\sqcup$ (partially defined) least upper bound
- $F \in D \overset{\mathrm{m}}{\longmapsto} D$ Total monotone semantic transformer
- The *iterates of F from* $\bot$ are assumed to be well-defined: $F^0 \overset{\Delta}{=} \bot$, $F^{\delta+1} = F(F^\delta)$ and $F^\lambda \overset{\Delta}{=} \underset{\delta < \lambda}{\sqcup} F^\delta$, λ limit ordinal;

- The semantics is $S \overset{\Delta}{=} \mathrm{lfp}_{\bot}^{\sqsubseteq} F = F^\epsilon$ where ϵ is the *order of the iterates* (i.e. the least ordinal such that $F(F^\epsilon) = F^\epsilon$).

Benefits of a Fixpoint Presentation of the Semantics

- Many other equivalent possible presentations [16]:
  - equational,
  - constraint,
  - closure condition,
  - rule-based,
  - game-theoretic;

[16] 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, ed., *Proc. 7th Int. Conf. on Computer Aided Verification, CAV '95*, LNCS 939, pp 293–308. Springer-Verlag, 3–5 July 1995.

- Fixpoints directly lead to proof methods, e.g.:
  - Scott induction:

    $$P(\bot) \,\wedge\, \forall X : P(X) \Rightarrow P(F(X)) \,\wedge\, P \text{ admissible}$$
    $$\Rightarrow P(\mathrm{lfp}_{\bot}^{\sqsubseteq} F)$$

    (with the hypotheses of Kleene's fixpoint theorem);
  - Park induction:

    $$\mathrm{lfp}_{\bot}^{\sqsubseteq} F \sqsubseteq P$$
    $$\Longleftrightarrow \exists I : F(I) \sqsubseteq I \,\wedge\, I \sqsubseteq P$$

    (with the hypotheses of Tarski's fixpoint theorem).

- By approximation, fixpoints directly lead to iterative program analysis algorithms [17, 18];
- Fixpoint presentation of the semantics is not always possible (without further refinement of the semantic domain).

[17] P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Conference Record of the Fourth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 238–252, Los Angeles, California, 1977. ACM Press, New York, New York, USA.
[18] P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Conference Record of the Sixth Annual ACM SIG-PLAN-SIGACT Symposium on Principles of Programming Languages*, pages 269–282, San Antonio, Texas, 1979. ACM Press, New York, New York, USA.

Abstraction of Fixpoint Semantics

- Concrete semantics fixpoint semantics:
  - $\langle D, \sqsubseteq \rangle$ concrete semantic domain
  - $S[\![\tau]\!] \in D$ concrete semantics of τ
    $$\triangleq \mathrm{lfp}_{\bot}^{\sqsubseteq} F \text{ where } F \in D \xmapsto{\;\mathrm{m}\;} D \text{ is } \sqsubseteq\text{-monotonic}$$
- Abstraction function: $\alpha \in D \longmapsto D^{\sharp}$
- Abstract semantics fixpoint semantics:
  - $D^{\sharp}$ abstract semantic domain
  - $S^{\sharp}[\![\tau]\!] \triangleq \alpha(S[\![\tau]\!]) \in D^{\sharp}$ abstract semantics of τ
- Fixpoint characterization problem:
  - Find $\sqsubseteq^{\sharp}$ and $F^{\sharp} \in D^{\sharp} \xmapsto{\;\mathrm{m}\;} D^{\sharp}$, $\sqsubseteq^{\sharp}$-monotonic such that:

    $$\alpha(\mathrm{lfp}_{\bot}^{\sqsubseteq} F) \,=\, \mathrm{lfp}_{\bot^{\sharp}}^{\sqsubseteq^{\sharp}} F^{\sharp}$$

Kleene Fixpoint Transfer Theorem

If $\langle \mathcal{D}^\natural,\, F^\natural \rangle$ and $\langle \mathcal{D}^\sharp,\, F^\sharp \rangle$ are semantic specifications and

$$\alpha(\bot^\natural) \;=\; \bot^\sharp$$

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

$$\forall \sqsubseteq^\natural\text{-increasing chains } X^\natural_\kappa, \kappa \in \Delta : \alpha\Big(\bigsqcup_{\kappa\in\Delta}^\natural X^\natural_\kappa\Big) \;=\; \bigsqcup_{\kappa\in\Delta}^\sharp \alpha(X^\natural_\kappa)$$

then

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

Note: The condition $F^\sharp \circ \alpha = \alpha \circ F^\natural$ provides guidelines for designing $F^\sharp$ when knowing $F^\natural$ and α.

Convergence

The convergence of the abstract iterates for $F^\sharp$ (at ϵ') is at least as fast as the convergence of the concrete iterates for F (at ϵ, i.e. $\epsilon' \le \epsilon$).

Proof

$$
\begin{aligned}
& & F(X^{\natural\epsilon}) \;=\; X^{\natural\epsilon} && \text{hypothesis} \\
\Rightarrow\;\; & & \alpha(F(X^{\natural\epsilon})) \;=\; \alpha(X^{\natural\epsilon}) && \\
\Rightarrow\;\; & & F^\sharp(\alpha(X^{\natural\epsilon})) \;=\; \alpha(X^{\natural\epsilon}) && \text{since } F^\sharp \circ \alpha = \alpha \circ F^\natural \\
\Rightarrow\;\; & & F^\sharp(X^{\sharp\epsilon}) \;=\; X^{\sharp\epsilon} && \text{since } X^{\sharp\epsilon} = \alpha(X^{\natural\epsilon}) \\
\Rightarrow\;\; & & \epsilon' \le \epsilon &&
\end{aligned}
$$

□

Sketch of Proof of Kleene Fixpoint Transfer Theorem
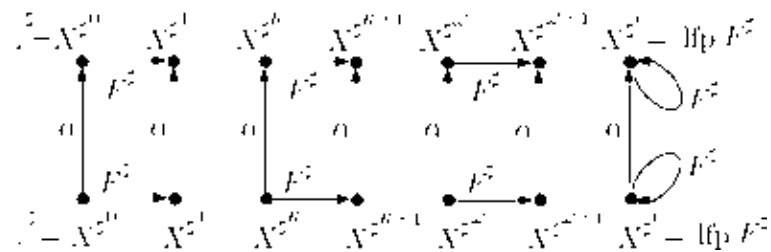
Abstraction function

- An important particular case of abstraction function:

$$\alpha \in \langle \mathcal{D}^\natural,\, \sqsubseteq^\natural \rangle \longmapsto \langle \mathcal{D}^\sharp,\, \sqsubseteq^\sharp \rangle$$

  is when α preserves existing lubs:

$$\alpha\Big(\bigsqcup_{i\in\Delta}^\natural x_i\Big) \;=\; \bigsqcup_{i\in\Delta}^\sharp \alpha(x_i)$$

- In this case there exists a unique $\gamma \in \langle \mathcal{D}^\sharp,\, \sqsubseteq^\sharp \rangle \longmapsto \langle \mathcal{D}^\natural,\, \sqsubseteq^\natural \rangle$ such that the pair $\langle \alpha,\, \gamma \rangle$ is a Galois connection.

Galois Connection

Given posets $\langle \mathcal{D}^\natural, \sqsubseteq^\natural \rangle$ and $\langle \mathcal{D}^\sharp, \sqsubseteq^\sharp \rangle$, a *Galois connection* is a pair of maps such that:

$$\alpha \in \mathcal{D}^\natural \longmapsto \mathcal{D}^\sharp$$

$$\gamma \in \mathcal{D}^\sharp \longmapsto \mathcal{D}^\natural$$

$$\forall x \in \mathcal{D}^\natural : \forall y \in \mathcal{D}^\sharp : \alpha(x) \sqsubseteq^\sharp y \Leftrightarrow x \sqsubseteq^\natural \gamma(y)$$

in which case we write:

$$\langle \mathcal{D}^\natural, \sqsubseteq^\natural \rangle \xleftarrow[\alpha]{\gamma} \langle \mathcal{D}^\sharp, \sqsubseteq^\sharp \rangle$$

If α is surjective then we have a *Galois insertion* and write:

$$\langle \mathcal{D}^\natural, \sqsubseteq^\natural \rangle \xleftarrow[\alpha]{\gamma}\!\!\!\rightarrow \langle \mathcal{D}^\sharp, \sqsubseteq^\sharp \rangle$$

Example of Galois Connection: Elementwise Abstraction

• If

  – $@ \in \mathcal{D}^\natural \longmapsto \mathcal{D}^\sharp$

  – $\alpha \in \wp(\mathcal{D}^\natural) \longmapsto \wp(\mathcal{D}^\sharp)$

    $\alpha(X) \triangleq \{@(x) \mid x \in X\}$

  – $\gamma \in \wp(\mathcal{D}^\sharp) \longmapsto \wp(\mathcal{D}^\natural)$

    $\gamma(Y) \triangleq \{x \mid @(x) \in Y\}$

  then

$$\langle \wp(\mathcal{D}^\natural), \subseteq \rangle \xleftarrow[\alpha]{\gamma} \langle \wp(\mathcal{D}^\sharp), \subseteq \rangle$$

If $@$ is surjective then so is α.

Proof $\alpha(X) \subseteq Y \Leftrightarrow \{@(x) \mid x \in X\} \subseteq Y \Leftrightarrow \forall x \in X : @(x) \in Y$
$\Leftrightarrow X \subseteq \{x \mid @(x) \in Y\} \Leftrightarrow X \subseteq \gamma(Y)$. $\square$

Tarski Fixpoint Transfer Theorem

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, $F^\natural \in \mathcal{D}^\natural \xmapsto{\text{m}} \mathcal{D}^\natural$, $F^\sharp \in \mathcal{D}^\sharp \xmapsto{\text{m}} \mathcal{D}^\sharp$ are monotonic and

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

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

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

then

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

Proof

(d) $F^\natural(x) \sqsubseteq^\natural x$

    $\Rightarrow \alpha \circ F^\natural(x) \sqsubseteq^\sharp \alpha(x)$ since α is monotonic by (a)

    $\Rightarrow F^\sharp \circ \alpha(x) \sqsubseteq^\sharp \alpha(x)$ by (b)

(e) $\{\alpha(x) \mid F^\natural(x) \sqsubseteq^\natural x\} = \{y \mid F^\sharp(y) \sqsubseteq^\sharp y\}$ by (c) and (d)

(f) $\sqcap^\sharp \{\alpha(x) \mid F^\natural(x) \sqsubseteq^\natural x\} = \sqcap^\sharp \{y \mid F^\sharp(y) \sqsubseteq^\sharp y\}$ by (e)

    $\Rightarrow \alpha(\sqcap^\natural \{x \mid F^\natural(x) \sqsubseteq^\natural x\}) = \sqcap^\sharp \{y \mid F^\sharp(y) \sqsubseteq^\sharp y\}$ by (a)

    $\Rightarrow$ $\alpha(\mathrm{lfp}^{\sqsubseteq^\natural} F^\natural) = \mathrm{lfp}^{\sqsubseteq^\sharp} F^\sharp$ by Tarski's fixpt th.

$\square$

Slide 33

$$\boxed{\text{TRACE SEMANTICS}}$$

Slide 35

Sequences

Finite Sequences

- $\mathcal{A}$ non-empty alphabet
- $\mathcal{A}^{\vec{0}} \triangleq \{\vec{\varepsilon}\}$ empty sequence
- $\mathcal{A}^{\vec{n}} \triangleq [0,\, n-1] \longmapsto \mathcal{A}$ when $n > 0$ finite sequences of length n

- $\mathbb{N}_+ \triangleq \{n \in \mathbb{N} \mid n > 0\}$ positive naturals
- $\mathcal{A}^{\vec{+}} \triangleq \bigcup\limits_{n \in \mathbb{N}_+} \mathcal{A}^{\vec{n}}$ non-empty finite sequences
- $\mathcal{A}^{\vec{\star}} \triangleq \mathcal{A}^{\vec{+}} \cup \{\vec{\varepsilon}\}$ finite sequences
- The length of a finite sequence $\sigma \in \mathcal{A}^{\vec{n}}$ is $|\sigma| \triangleq n$;

Slide 34

Transition System

- A transition system is a pair $\langle \Sigma,\, \tau \rangle$ where:
  - Σ is a (non-empty) set of states,
  - We could also consider actions as in process algebra,
  - $\tau \subseteq \Sigma \times \Sigma$ is the binary transition relation between a state and its possible successors;
- We write $s\ \tau\ s'$ or $\tau(s, s')$ for $\langle s,\, s' \rangle \in \tau$ using the isomorphism $\wp(\Sigma \times \Sigma) \simeq (\Sigma \times \Sigma) \longmapsto \mathbb{B}$;
- $\mathbb{B} \triangleq \{\text{tt}, \text{ff}\}$ is the set of boolean values;
- $\check{\tau} \triangleq \{s \in \Sigma \mid \forall s' \in \Sigma : \neg(s\ \tau\ s')\}$ is the set of final/blocking states.

Slide 36

Infinite Sequences

- $\mathcal{A}^{\vec{\omega}} \triangleq \mathbb{N} \longmapsto \mathcal{A}$ infinite sequences
- $\mathcal{A}^{\vec{\infty}} \triangleq \mathcal{A}^{\vec{\star}} \cup \mathcal{A}^{\vec{\omega}}$ sequences
- $\mathcal{A}^{\vec{\propto}} \triangleq \mathcal{A}^{\vec{+}} \cup \mathcal{A}^{\vec{\omega}}$ non-empty sequences
- The length of an infinite sequence $\sigma \in \mathcal{A}^{\vec{\omega}}$ is $|\sigma| \triangleq \omega$

Junction of Finite Sequences

- Joinable non-empty finite sequences:

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

- Their join is:

$$
\begin{array}{c}
\alpha_0 \;\ldots\; \alpha_{\ell-1} \\
= \\
\beta_0 \quad \beta_1 \;\ldots\; \beta_{m-1} \\
\hline
\alpha_0 \ldots \alpha_{\ell-1} \frown \beta_0 \ldots \beta_{m-1} \overset{\Delta}{=} \alpha_0 \;\ldots\; \alpha_{\ell-1} \; \beta_1 \;\ldots\; \beta_{m-1}
\end{array}
$$

$$\alpha_0 \ldots \alpha_\ell \ldots \; \mathbin{\overset{?}{\frown}} \; \beta_0 \ldots \beta_{m-1} \text{ is true}$$
$$\alpha_0 \ldots \alpha_\ell \ldots \; \mathbin{\overset{?}{\frown}} \; \beta_0 \ldots \beta_m \ldots \text{ is true}$$
$$\alpha_0 \ldots \alpha_{\ell-1} \; \mathbin{\overset{?}{\frown}} \; \beta_0 \ldots \beta_m \ldots \text{ iff } \alpha_{\ell-1} = \beta_0$$

- Their join is:

$$\alpha_0 \ldots \alpha_\ell \ldots \frown \beta_0 \ldots \beta_{m-1} \overset{\Delta}{=} \alpha_0 \;\ldots\; \alpha_\ell \quad \ldots$$
$$\alpha_0 \ldots \alpha_\ell \ldots \frown \beta_0 \ldots \beta_m \ldots \overset{\Delta}{=} \alpha_0 \;\ldots\; \alpha_\ell \quad \ldots$$

$$
\begin{array}{c}
\alpha_0 \;\ldots\; \alpha_{\ell-1} \\
= \\
\beta_0 \quad \beta_1 \;\ldots\; \beta_m \ldots \\
\hline
\alpha_0 \ldots \alpha_{\ell-1} \frown \beta_0 \ldots \beta_m \ldots \overset{\Delta}{=} \alpha_0 \;\ldots\; \alpha_{\ell-1} \; \beta_1 \;\ldots\; \beta_m \ldots
\end{array}
$$

Junction of Infinitary Sequences

- Joinable infinitary sequences:

Junction of Sets of Sequences

- For sets A and $B \in \wp(\mathcal{A}^{\vec{\infty}})$ of non-empty sequences, we have:
  - $A \frown B \overset{\Delta}{=} \{\alpha \frown \beta \mid \alpha \in A \wedge \beta \in B \wedge \alpha \mathbin{\overset{?}{\frown}} \beta\}$ junction
- $A \frown \left(\bigcup_{i \in \Delta} B_i \right) = \bigcup_{i \in \Delta} (A \frown B_i)$ and $\left(\bigcup_{i \in \Delta} A_i \right) \frown B = \bigcup_{i \in \Delta} (A_i \frown B)$
- Not co-continuous on $\wp(\mathcal{A}^{\vec{\infty}})$! Counter example $(\mathcal{A} = \{a\})$:
  - $A = \{a^\omega\}$,
  - $B_n = \{a^\ell \mid \ell \in \mathbb{N} \wedge \ell > n\}$, $n \in \mathbb{N}$ is a $\subseteq$-decreasing chain,
  - $A \frown \left(\bigcap_{n \in \mathbb{N}} B_n \right) = \emptyset$ and $\left(\bigcap_{n \in \mathbb{N}} A \frown B_n \right) = \{a^\omega\}$.

Trace Semantics

- $\langle \Sigma, \tau \rangle$ transition system
- $\tau^{\dot{\vec{n}}} \triangleq \{\sigma \in \Sigma^{\vec{n}} \mid \forall i < n-1 : \sigma_i \ \tau \ \sigma_{i+1}\}$

                                               partial traces of length n

- $\check{\tau} \triangleq \{s \in \Sigma \mid \forall s' \in \Sigma : \neg(s \ \tau \ s')\}$ final/blocking states
- $\tau^{\vec{n}} \triangleq \{\sigma \in \tau^{\dot{\vec{n}}} \mid \sigma_{n-1} \in \check{\tau}\}$ complete traces of length n
- $\tau^{\vec{+}} \triangleq \bigcup_{n \in \mathbb{N}_+} \tau^{\vec{n}}$ finite complete traces
- $\tau^{\vec{\omega}} \triangleq \{\sigma \in \Sigma^{\vec{\omega}} \mid \forall i \in \mathbb{N} : \sigma_i \ \tau \ \sigma_{i+1}\}$ infinite traces
- $\tau^{\vec{\infty}} \triangleq \tau^{\vec{+}} \cup \tau^{\vec{\omega}}$ complete traces

---

Sketch of Proof of $\mathrm{lfp}_{\emptyset}^{\subseteq} F^{\vec{+}} = \bigcup_{i \in \mathbb{N}_+} \tau^{\vec{i}} = \tau^{\vec{+}}$
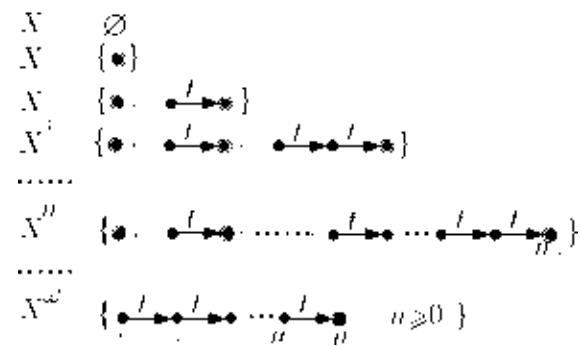
Fixpoint Characterization of $\tau^{\vec{+}}$
(finite complete execution traces)

$$\tau^{\vec{+}} = \mathrm{lfp}_{\emptyset}^{\subseteq} F^{\vec{+}}$$

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

$$F^{\vec{+}}(X) \triangleq \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X$$

Note: $F^{\vec{+}}$ is a complete $\cup$-morphism: $\bigcup_i F^{\vec{+}}(X_i) = F^{\vec{+}}(\bigcup_i X_i)$.

Fixpoint Characterization of $\tau^{\vec{\omega}}$
## (infinite execution traces)

$$\tau^{\vec{\omega}} = \mathrm{gfp}_{\Sigma^{\vec{\omega}}}^{\subseteq} F^{\vec{\omega}}$$

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

$$F^{\vec{\omega}}(X) \triangleq \tau^{\dot{\vec{2}}} \frown X$$

Note: $F^{\vec{\omega}}$ is a complete $\cap$-morphism: $\bigcap_i F^{\vec{\omega}}(X_i) = F^{\vec{\omega}}(\bigcap_i X_i)$.

Sketch of Proof of $\mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}} = \bigcap_{n \in \mathbb{N}} \tau^{\dot{\vec{n}}} \cap \Sigma^{\vec{\omega}} = \tau^{\vec{\omega}}$

---
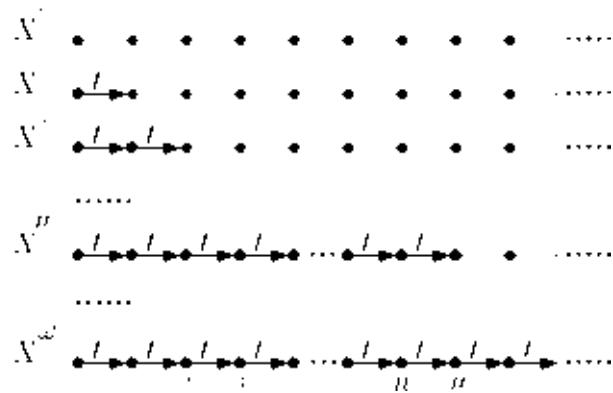
then:

- $\langle \wp(\Sigma^{\vec{\infty}}), \sqsubseteq^{\vec{\infty}}, \perp^{\vec{\infty}}, \sqcup^{\vec{\infty}} \rangle$ is a complete lattice (resp. cpo)

- $F^{\vec{\infty}}$ is monotonic (resp. continuous, a complete join morphism)

- $\mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\perp^{\vec{\infty}}} F^{\vec{\infty}} = \mathrm{lfp}^{\sqsubseteq^{\vec{+}}}_{\perp^{\vec{\infty}}} F^{\vec{+}} \cup \mathrm{lfp}^{\sqsubseteq^{\vec{\omega}}}_{\perp^{\vec{\infty}}} F^{\vec{\omega}}$

(Trivial) bi-fixpoint theorem

If
- $\Sigma^{\vec{+}}, \Sigma^{\vec{\omega}}$ is a partition of $\Sigma^{\vec{\infty}}$

- $\langle \wp(\Sigma^{\vec{+}}), \sqsubseteq^{\vec{+}}, \perp^{\vec{+}}, \sqcup^{\vec{+}} \rangle$ (resp. $\langle \wp(\Sigma^{\vec{\omega}}), \sqsubseteq^{\vec{\omega}}, \perp^{\vec{\omega}}, \sqcup^{\vec{\omega}} \rangle$) is a complete lattice (resp. cpo)

- $F^{\vec{+}} \in \wp(\Sigma^{\vec{+}}) \xmapsto{\mathrm{m}} \wp(\Sigma^{\vec{+}})$ (resp. $F^{\vec{\omega}} \in \wp(\Sigma^{\vec{\omega}}) \xmapsto{\mathrm{m}} \wp(\Sigma^{\vec{\omega}})$) is monotonic (resp. continuous, a complete join morphism)

- $X^{\vec{+}} \triangleq X \cap \Sigma^{\vec{+}}, X^{\vec{\omega}} \triangleq X \cap \Sigma^{\vec{\omega}}$

- $F^{\vec{\infty}}(X) \triangleq F^{\vec{+}}(X^{\vec{+}}) \cup F^{\vec{\omega}}(X^{\vec{\omega}})$

- $X \sqsubseteq^{\vec{\infty}} Y \triangleq X^{\vec{+}} \sqsubseteq^{\vec{+}} Y^{\vec{+}} \wedge X^{\vec{\omega}} \sqsubseteq^{\vec{\omega}} Y^{\vec{\omega}}$

- $\perp^{\vec{\infty}} \triangleq \perp^{\vec{+}} \cup \perp^{\vec{\omega}}$

- $\bigsqcup^{\vec{\infty}}_i X_i \triangleq \bigsqcup^{\vec{+}}_i X_i^{\vec{+}} \cup \bigsqcup^{\vec{\omega}}_i X_i^{\vec{\omega}}$

Approximation and Computational Orderings

- $\langle \wp(\Sigma^{\vec{\infty}}), \sqsubseteq^{\vec{\infty}}, \perp^{\vec{\infty}}, \sqcup^{\vec{\infty}} \rangle$ is a complete lattice (or cpo) for the *computational ordering* $\sqsubseteq^{\vec{\infty}}$;

- $\langle \wp(\Sigma^{\vec{\infty}}), \subseteq, \emptyset, \cup \rangle$ is a complete lattice for the *approximation ordering* $\subseteq$ (logical implication);

- Sometimes further abstractions identify $\sqsubseteq^{\vec{\infty}}$ and $\subseteq$ (e.g. strictness analysis).

Fixpoint Characterization of $\tau^{\vec{\infty}}$ (complete execution traces)

$$\tau^{\vec{\infty}} = \tau^{\vec{+}} \cup \tau^{\vec{\omega}} = \mathrm{lfp}^{\subseteq}_{\emptyset} F^{\vec{+}} \ \cup \ \mathrm{lfp}^{\supseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}} = \mathrm{lfp}^{\sqsubseteq^{\vec{\infty}}}_{\Sigma^{\vec{\infty}}} F^{\vec{\infty}}$$

by the bifixpoint theorem where the set of complete traces transformer $F^{\vec{\infty}}$ is:

$$F^{\vec{\infty}}(X) \triangleq \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X$$

Proof

$$
\begin{aligned}
F^{\vec{\infty}}(X) &\triangleq F^{\vec{+}}(X^{\vec{+}}) \cup F^{\vec{\omega}}(X^{\vec{\omega}}) \\
&= \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X^{\vec{+}} \cup \tau^{\dot{\vec{2}}} \frown X^{\vec{\omega}} \\
&= \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown (X^{\vec{+}} \cup X^{\vec{\omega}}) \\
&= \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X
\end{aligned}
$$

□

Continuity of the trace transformer $F^{\vec{\infty}}(X)$

Unbounded non-determinism does not imply absence of continuity of the transformer of the fixpoint semantics:

Proof

$$
\begin{aligned}
\bigsqcup_{i}^{\vec{\infty}} F^{\vec{\infty}}(X_i) &= \bigsqcup_{i}^{\vec{\infty}} \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X_i \\
&= \bigcup_{i}(\tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X_i^{\vec{+}}) \cup \bigcap_{i}(\tau^{\dot{\vec{2}}} \frown X_i^{\vec{\omega}}) \\
&= \tau^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown (\bigcup_{i} X_i^{\vec{+}} \cup \bigcap_{i} X_i^{\vec{\omega}}) \\
&= F^{\vec{\infty}}(\bigsqcup_{i}^{\vec{\infty}} X_i)
\end{aligned}
$$

□

Scott's thesis (slightly revisited)

The semantics of a program can be expressed as the least fixpoint of a <u>continuous</u> operator (even in presence of unbounded nondeterminism), *for a sufficiently refined semantic domain.*

TRANSITION VERSUS TRACE SEMANTICS

Maximal Trace Semantics/Transition Semantics

The transition/small-step operational semantics is an abstraction of the maximal trace semantics:

$$\tau = \alpha^\tau(\tau^{\vec{\infty}})$$

where

- the abstraction collects possible transitions $\alpha^\tau(T) \triangleq \{\langle s,\ s'\rangle \mid \exists \sigma \in \Sigma^{\vec{\star}} : \exists \sigma' \in \Sigma^{\vec{\infty}} : \sigma \cdot ss' \cdot \sigma' \in T\}$;

- the concretization builds maximal execution traces $\gamma^\tau(t) \triangleq t^{\vec{\infty}}$;

- $\langle \wp(\Sigma^{\vec{\infty}}),\ \subseteq\rangle \xleftarrow[\alpha^\tau]{\gamma^\tau} \langle \wp(\Sigma \times \Sigma),\ \subseteq\rangle$.

The Transition Abstraction is Approximate

In general:
$$T \subsetneq \gamma^\tau(\alpha^\tau(T))$$

Counter-example:

- set of fair traces $T = \{a^n b \mid n \in \mathbb{N}\}$
- $\alpha^\tau(T) = \{\langle a,\ a\rangle, \langle a,\ b\rangle\}$
- $\gamma^\tau(\alpha^\tau(T)) = \{a^n b \mid n \in \mathbb{N}\} \cup \{a^\omega\}$ is unfair for b.

Relational Semantics

Finite Relational Abstraction

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

- $@^+ \in \Sigma^{\vec{+}} \longmapsto (\Sigma \times \Sigma)$

  $@^+(\sigma) \triangleq \langle \sigma_0,\ \sigma_{n-1}\rangle, \quad n \in \mathbb{N}_+,\ \sigma \in \Sigma^{\vec{n}}$

- $\alpha^+(X) \triangleq \{@^+(\sigma) \mid \sigma \in X\}$

  $\gamma^+(Y) \triangleq \{\sigma \mid @^+(\sigma) \in Y\}$

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

- Finitary relational / big-step operational / natural semantics:

$$\tau^+ \triangleq \alpha^+(\tau^{\vec{+}}) = \alpha^+(\mathrm{lfp}^{\subseteq}_{\emptyset} F^{\vec{+}})$$

- Fixpoint characterization:

$$\tau^+ = \mathrm{lfp}^{\subseteq}_{\emptyset} F^+$$
$$F^+(X) \triangleq \check{\tau} \cup \tau \circ X$$
$$\check{\tau} \triangleq \{\langle s, s \rangle \in \Sigma \mid \forall s' \in \Sigma : \neg(s \; \tau \; s')\}$$

Proof

- $\alpha^+(\emptyset) \triangleq \{ \mathbb{@}^+(\sigma) \mid \sigma \in \emptyset \} = \emptyset$
- $\alpha^+ \circ F^{\vec{+}} = \lambda X \cdot \alpha^+(\tau^{\vec{1}} \cup \tau^{\vec{2}} \frown X)$

$$= \lambda X \cdot \alpha^+(\tau^{\vec{1}}) \cup \alpha^+(\tau^{\vec{2}} \frown X)$$
$$= \lambda X \cdot \{ \langle s, s \rangle \in \Sigma \mid \forall s' \in \Sigma : \neg(s \; \tau \; s') \} \cup \alpha^+(\tau^{\vec{2}} \frown X)$$
$$= \lambda X \cdot \check{\tau} \cup \{ \mathbb{@}^+(\eta \frown \xi) \mid \eta \in \tau^{\vec{2}} \wedge \xi \in X \wedge \eta \; ? \; \xi \}$$
$$= \lambda X \cdot \check{\tau} \cup \{ \langle \eta_0, \xi_{n-1} \rangle \mid \eta_0 \; \tau \; \xi_0 \wedge n \in \mathbb{N}_+ \wedge \xi \in X \cap \Sigma^{\vec{n}} \}$$
$$= \lambda X \cdot \check{\tau} \cup \{ \langle s, s' \rangle \mid \exists s'' : s \; \tau \; s'' \wedge \langle s'', s' \rangle \in \alpha^+(X) \}$$
$$= \lambda X \cdot \check{\tau} \cup \tau \circ \alpha^+(X)$$
$$= F^+ \circ \alpha^+$$

- α^+ is continuous (Galois connection)
- $\tau^+ = \alpha^+(\mathrm{lfp}^{\subseteq}_{\emptyset} F^{\vec{+}}) = \mathrm{lfp}^{\subseteq}_{\emptyset} F^+$ by Kleene's fixpoint transfer th.

$\square$

- α^+ is a $\cap$-morphism but <u>not</u> co-continuous hence <u>not</u> a complete $\cap$-morphism.

Proof

- $X^k \triangleq \{ a^n b \mid n \geq k \}$
- $X^k, k \in \mathbb{N}_+$ is $\subseteq$-decreasing
- $\bigcap_{k \in \mathbb{N}_+} \alpha^+(X^k) = \bigcap_{k \in \mathbb{N}_+} \{ \langle a, b \rangle \} = \{ \langle a, b \rangle \}$
- $\bigcap_{k \in \mathbb{N}_+} X^k = \emptyset$ since $a^n b \in \bigcap_{k \in \mathbb{N}_+} X^k$ for $n \in \mathbb{N}_+$ is in contradiction with $a^n b \notin X^{n+1}$
- $\alpha^+(\bigcap_{k \in \mathbb{N}_+} X^k) = \alpha^+(\emptyset) = \emptyset$

$\square$

- It follows that Tarski fixpoint transfer would not have been applicable.

Infinitary Relational Abstraction

Replace infinite execution traces $\sigma_0 \sigma_1 \ldots \sigma_n \ldots$ by their initial state $\langle \sigma_0, \perp \rangle$, making non-termination by Scott's $\perp$:

- $\mathbb{@}^\omega \in \Sigma^{\vec{\omega}} \longmapsto \Sigma \times \{ \perp \}$ [19]

   $\perp \notin \Sigma$ non-termination notation

   $\mathbb{@}^\omega(\sigma) \triangleq \langle \sigma_0, \perp \rangle, \; \sigma \in \Sigma^{\vec{\omega}}$

- $\alpha^\omega(X) \triangleq \{ \mathbb{@}^\omega(\sigma) \mid \sigma \in X \}$

   $\gamma^\omega(Y) \triangleq \{ \sigma \mid \mathbb{@}^\omega(\sigma) \in Y \}$

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

---

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

- α^ω is a complete $\cup$-morphism (Galois connection, hence continuous) and a $\cap$-morphism but <u>not</u> co-continuous.

Proof

- $X^k \triangleq \{a^n b^\omega \mid n \geq k\}$
- $X^k, k \in \mathbb{N}_+$ is $\subseteq$-decreasing
- $\bigcap_{k \in \mathbb{N}_+} \alpha^\omega(X^k) = \bigcap_{k \in \mathbb{N}_+} \{\langle a, \perp \rangle\} = \{\langle a, \perp \rangle\}$
- $\bigcap_{k \in \mathbb{N}_+} X^k = \emptyset$ since $a^n b^\omega \in \bigcap_{k \in \mathbb{N}_+} X^k$ for $n \in \mathbb{N}_+$ is in contradiction with $a^n b^\omega \notin X^{n+1}$
- $\alpha^\omega(\bigcap_{k \in \mathbb{N}_+} X^k) = \alpha^\omega(\emptyset) = \emptyset$

$\square$

- It follows that Kleene dual fixpoint transfer does not apply.

Infinitary Relational Semantics
of a Transition System $\langle \Sigma, \tau \rangle$

- Infinitary relational semantics:

$$\tau^\omega \triangleq \alpha^\omega(\tau^{\vec{\omega}}) = \alpha^\omega(\mathrm{gfp}^{\subseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}}) = \alpha^\omega(\mathrm{lfp}^{\supseteq}_{\Sigma^{\vec{\omega}}} F^{\vec{\omega}})$$

- Fixpoint characterization:

$$\tau^\omega = \mathrm{lfp}^{\supseteq}_{\Sigma \times \{\perp\}} F^\omega = \mathrm{gfp}^{\subseteq}_{\Sigma \times \{\perp\}} F^\omega$$
$$F^\omega(X) = \tau \circ X$$

Proof

- α^ω is a complete $\cup$-morphism (G.c.) hence a complete meet morphism for $\supseteq$.
- $\alpha^\omega \circ F^{\vec{\omega}} = \lambda X \cdot \alpha^\omega(\tau^{\dot{\vec{2}}} \frown X)$
  $= \lambda X \cdot \{@^\omega(\eta \frown \xi) \mid \eta \in \tau^{\dot{\vec{2}}} \wedge \xi \in X \wedge \eta \, ? \, \xi\}$
  $= \lambda X \cdot \{\langle \eta_0, \perp \rangle \mid \eta_0 \, \tau \, \xi_0 \wedge \xi \in X\}$
  $= \lambda X \cdot \{\langle s, \perp \rangle \mid \exists s' : s \, \tau \, s' \wedge \langle s', \perp \rangle \in \alpha^\omega(X)\}$
  $= \lambda X \cdot \tau \circ \alpha^\omega(X)$
  $= F^\omega \circ \alpha^\omega$

- We prove that $\forall Y \in \wp(\Sigma \times \{\perp\}) : F^\omega(Y) \supseteq Y \Rightarrow \exists X \in \Sigma^{\vec{\omega}} : \alpha^\omega(X) = Y \wedge F^{\vec{\omega}}(X) \supseteq X$:
  - $X \triangleq \{\sigma \in \tau^{\vec{\omega}} \mid \forall i \in \mathbb{N} : \langle \sigma_i, \perp \rangle \in Y\}$
  - We first prove that $\alpha^\omega(X) = Y$:
    * $\alpha^\omega(X) \subseteq Y$ is obvious since $\sigma \in X$ implies $\langle \sigma_0, \perp \rangle \in Y$.

---

* $Y \subseteq \alpha^\omega(X)$
(a) $Y \subseteq F^\omega(Y) = \tau \circ Y = \{\langle s, \perp \rangle \mid \exists s' : s \, \tau \, s' \wedge \langle s', \perp \rangle \in Y\}$
(b) If $\sigma_0 \ldots \sigma_n$ is such that $\sigma_i \, \tau \, \sigma_{i+1}$, $i < n$ and $\langle \sigma_i, \perp \rangle \in Y$, $i \leq n$ then $\langle \sigma_n, \perp \rangle \in Y$ and (a) imply $\exists \sigma_{n+1} : \sigma_n \, \tau \, \sigma_{n+1} \wedge \langle \sigma_{n+1}, \perp \rangle \in Y$. So, by induction, we can built $\sigma \in \tau^{\vec{\omega}}$ such that $\forall i \in \mathbb{N} : \langle \sigma_i, \perp \rangle \in Y$. We have $\sigma \in X$ and $\langle \sigma_0, \perp \rangle \in \alpha^\omega(X)$ proving that $Y \subseteq \alpha^\omega(X)$;

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

- We conclude by Tarski's fixpoint transfer theorem.

$\square$

Transfinite Iterations

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

$\Sigma \triangleq \{s\} \cup \{s_{ij} \mid 0 \leq j \leq i\}$
elements of Σ are distinct
two by two

$\tau \triangleq \{\langle s, s_{ii} \rangle \mid i \geq 0\} \cup$
$\{\langle s_{ij}, s_{ij-1} \rangle \mid 0 < j \leq i\}$

$\tau^{\vec{\omega}} = \emptyset$
$\tau^{\omega} = \emptyset$

Bifinite Relational Abstraction

- $\alpha^{\infty} \in \wp(\Sigma^{\vec{\infty}}) \longmapsto \wp(\Sigma \times \Sigma_{\perp}), \qquad \Sigma_{\perp} \triangleq \Sigma \cup \{\perp\}$

$\alpha^{\infty}(X) \triangleq \alpha^{+}(X^{\vec{+}}) \cup \alpha^{\omega}(X^{\vec{\omega}})$ where $X^{+} = X \cap (\Sigma \times \Sigma)$
and $\quad X^{\omega} = X \cap (\Sigma \times \{\perp\})$

- Bifinite relational semantics:

$\tau^{\infty} \triangleq \alpha^{\infty}(\tau^{\vec{\infty}})$
$= \alpha^{+}((\tau^{\vec{\infty}})^{\vec{+}}) \cup \alpha^{\omega}((\tau^{\vec{\infty}})^{\vec{\omega}})$
$= \alpha^{+}(\tau^{\vec{+}}) \cup \alpha^{\omega}(\tau^{\vec{\omega}})$
$= \tau^{+} \cup \tau^{\omega}$
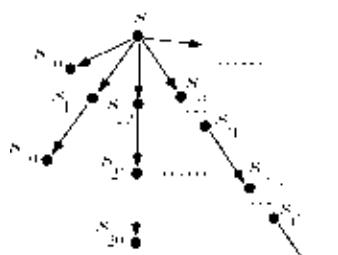
- Iterates: $\qquad\qquad\qquad F^{\omega}(X) = \tau \circ X$
  - $X^0 = \{\langle s, \perp \rangle\} \cup \{\langle s_{ij}, \perp \rangle \mid 0 \leq j \leq i\}$
  - $X^1 = F^{\omega}(X^0) = \{\langle s, \perp \rangle\} \cup \{\langle s_{ij}, \perp \rangle \mid 1 \leq j \leq i\}$

  ...
  - $X^n = \{\langle s, \perp \rangle\} \cup \{\langle s_{ij}, \perp \rangle \mid n \leq j \leq i\}$

  ...
  - $X^{\omega} = \bigcap_{n \in \mathbb{N}} X^n = \{\langle s, \perp \rangle\}$
  - $X^{\omega+1} = F^{\omega}(X^{\omega}) = \emptyset = \text{gfp}^{\subseteq}_{\Sigma \times \{\perp\}} F^{\omega} = \tau^{\omega}$

Fixpoint Bifinite Relational Semantics of a Transition System $\langle \Sigma, \tau \rangle$

- $\tau^{\infty} \triangleq \tau^{+} \cup \tau^{\omega}$
$= \text{lfp}^{\subseteq}_{\emptyset} \lambda X \cdot \check{\tau} \cup \tau \circ X \ \cup \ \text{lfp}^{\supseteq}_{\Sigma \times \{\perp\}} \lambda X \cdot \tau \circ X$
$= \text{lfp}^{\sqsubseteq^{\infty}}_{\perp^{\infty}} F^{\infty} \qquad\qquad$ by the bi-fixpoint theorem, where:

- $F^{\infty}(X) \triangleq \lambda X \cdot \check{\tau} \cup \tau \circ X^{+} \cup \tau \circ X^{\omega} = \lambda X \cdot \check{\tau} \cup \tau \circ (X^{+} \cup X^{\omega})$
$= \lambda X \cdot \check{\tau} \cup \tau \circ X$

- $X \sqsubseteq^{\infty} Y \triangleq X^{+} \subseteq Y^{+} \wedge X^{\omega} \supseteq Y^{\omega}$

- $\perp^{\infty} \triangleq \emptyset \cup (\Sigma \times \{\perp\}) = \Sigma \times \{\perp\}$

- $\bigsqcup^{\infty}_{i} X_i \triangleq \bigcup_{i} X_i^{+} \cup \bigcap_{i} X_i^{\omega}$

- $\langle \wp(\Sigma \times \Sigma_{\perp}), \sqsubseteq^{\infty}, \perp^{\infty}, \sqcup^{\infty} \rangle$ is a complete lattice.

Abstraction by Parts

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

- The finitary part transfers through α^+ by Kleene's fixpoint transfer theorem (but Tarski's one is not applicable);
- The infinitary part transfers through α^ω by Tarski's fixpoint transfer theorem (but Kleene's one is not applicable);
- The whole transfers through α^∞ by parts using the bifixpoint theorem (although Kleene's and Tarski's fixpoint transfer theorems are not applicable).

Natural Fixpoint Denotational/Functional Nondeterministic Semantics of a Transition System $\langle \Sigma, \tau \rangle$

- $\tau^\natural \triangleq \alpha^\natural(\tau^\infty)$
  $= \mathrm{lfp}^{\sqsubseteq^\natural}_{\perp^\natural} F^\natural$
- $F^\natural(f) \triangleq \lambda s \bullet (\forall s' \in \Sigma : \neg(s\ \tau\ s')\ ?\ \{s\}$
  $\qquad\qquad\qquad | \{s' \mid \exists s'' \in \Sigma : s\ \tau\ s'' \wedge s' \in f(s'')\})$

Proof

Trivial application of Kleene's fixpoint transfert theorem for the complete order-isomorphism $\alpha^\natural$.

$\square$

Denotational/Functional Nondeterministic Abstraction

We use the complete order isomorphism:

$$\langle \wp(\Sigma \times \Sigma_\perp), \sqsubseteq^\infty, \perp^\infty, \top^\infty, \sqcup^\infty, \sqcap^\infty \rangle$$
$$\xleftarrow[\;\;\;\alpha^\natural\;\;\;]{\;\;\;\gamma^\natural\;\;\;}$$
$$\langle \Sigma \longmapsto \wp(\Sigma_\perp), \dot\sqsubseteq^\natural, \dot\perp^\natural, \dot\top^\natural, \dot\sqcup^\natural, \dot\sqcap^\natural \rangle$$

defined by the right-image of a relation:

$$\alpha^\natural(r) = \lambda s \bullet \{s' \in \Sigma_\perp \mid r(s, s')\}$$
$$\gamma^\natural(f) = \{\langle s, s' \rangle \mid s' \in f(s)\}$$

Computational Ordering

$$f \dot\sqsubseteq^\natural g \;\triangleq\; \gamma^\natural(f) \sqsubseteq^\infty \gamma^\natural(g)$$
$$= \{\langle s, s' \rangle \mid s' \in f(s) \cap \Sigma\} \subseteq \{\langle s, s' \rangle \mid s' \in g(s) \cap \Sigma\}$$
$$\wedge \{\langle s, s' \rangle \mid f(s) = \perp\} \subseteq \{\langle s, s' \rangle \mid g(s) = \perp\}$$
$$= \forall s \in \Sigma : f(s)^+ \subseteq g(s)^+ \wedge f(s)^\omega \supseteq g(s)^\omega$$
$$\text{where } X^+ \triangleq X \cap \Sigma \text{ and } X^\omega \triangleq X \cap \{\perp\}$$
$$= \forall s \in \Sigma : f(s) \sqsubseteq^\natural g(s)$$
$$\text{where } X \sqsubseteq^\natural Y \triangleq X^+ \subseteq Y^+ \wedge X^\omega \supseteq Y^\omega$$

This is not the classical Egli-Milner ordering!

Orderings for the Nondeterministic Denotational Semantics, $\Sigma = \{a, b\}$
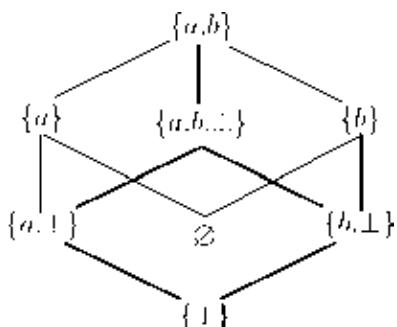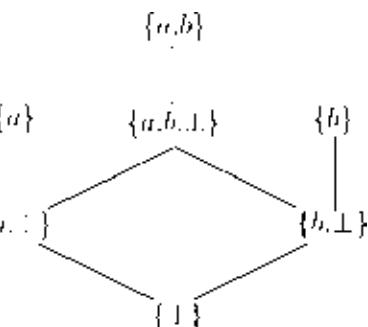
Computational ordering $\sqsubseteq^\natural$ Egli-Milner ordering $\sqsubseteq^{\mathrm{EM}}$

————— : possible iterates of $F^\natural$

Plotkin's Fixpoint
Denotational/Functional Nondeterministic Semantics of a Transition System $\langle \Sigma, \tau \rangle$

- $\tau^\natural \triangleq \alpha^\natural(\tau^\infty)$

$$= \mathrm{lfp}_{\lambda s \bullet \{\bot\}}^{\sqsubseteq^\natural} F^\natural = \mathrm{lfp}_{\lambda s \bullet \{\bot\}}^{\dot\sqsubseteq^{\mathrm{EM}}} F^\natural$$

Sketch of proof

- $\mathrm{lfp}_{\lambda s \bullet \{\bot\}}^{\dot\sqsubseteq^{\mathrm{EM}}} F^\natural$ exists since $F^\natural$ is Egli-Milner monotonic and $\langle \wp(\Sigma_\bot) - \{\emptyset\}, \dot\sqsubseteq^{\mathrm{EM}} \rangle$ is a cpo;
- $\mathrm{lfp}_{\lambda s \bullet \{\bot\}}^{\dot\sqsubseteq^{\mathrm{EM}}} F^\natural = \mathrm{lfp}_{\lambda s \bullet \{\bot\}}^{\dot\sqsubseteq^\natural} F^\natural$ since the iterates exactly coincide.
$\square$

Comparing the orderings $\sqsubseteq^\natural$ and $\dot\sqsubseteq^{\mathrm{EM}}$

- The lub $\sqcup^\natural$ provides a semantics to the parallel or:

$$[\![P \mid\mid Q]\!] = [\![P]\!] \sqcup^\natural [\![Q]\!]$$

(nontermination of $P \mid\mid Q$ only if both P and Q do not terminate);
- The lub $\sqcup^{\mathrm{EM}}$ may not be defined.

Fixpoint Iterates Reordering

- Let $\langle \langle D, \sqsubseteq, \bot, \sqcup \rangle, F \rangle$ be a fixpoint semantic specification;
- let E be a set and $\preceq$ be a binary relation on E, such that:
    1. $\preceq$ is a pre-order on E;
    2. all iterates F^δ, $\delta \in \mathbb{O}$ of F belong to E;
    3. $\bot$ is the $\preceq$-infimum of E;
    4. the restriction $F|_E$ of F to E is $\preceq$-monotone;
    5. for all $x \in E$, if λ is a limit ordinal and $\forall \delta < \lambda : F^\delta \preceq x$ then $\bigsqcup_{\delta < \lambda} F^\delta \preceq x$.
- Then $\mathrm{lfp}_\bot^\sqsubseteq F = \mathrm{lfp}_\bot^\preceq F|_E \in E$.

Nondeterministic Smyth/Demoniac Denotational Semantics

- $\tau^\sharp \triangleq \alpha^\sharp(\tau^\natural)$ where
  - $\alpha^\sharp(f) \triangleq \lambda s \cdot f(s) \cup \{s' \in \Sigma \mid \bot \in f(s)\}$;
  - $\gamma^\sharp(g) \triangleq g$.
- $\langle \Sigma \longmapsto \wp(\Sigma_\bot), \ \dot\subseteq \rangle \xleftrightarrow[\alpha^\sharp]{\gamma^\sharp} \langle \Sigma \longmapsto (\wp(\Sigma) \cup \{\Sigma_\bot\}), \ \dot\subseteq \rangle.$

P. Cousot

Examples of Other Possible Demoniac Iterate Orderings
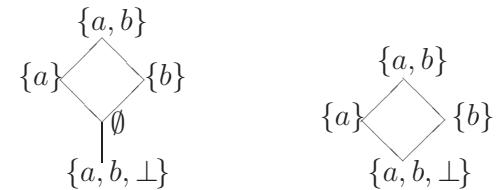
Demoniac ordering $\sqsubseteq^\sharp$ Demoniac ordering $\sqsubseteq^\diamond$
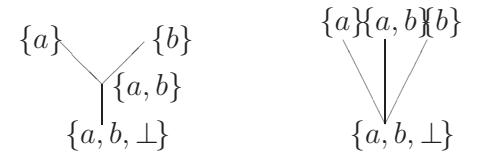
Smyth ordering $\sqsubseteq^s$ Flat ordering $\sqsubseteq^=$

Demoniac Denotational Semantics in Fixpoint Form

$$\tau^\sharp = \mathrm{lfp}_{\dot\bot^=}^{\dot\sqsubseteq^=} F^\natural$$

where:
- $F^\natural \triangleq \lambda s \cdot (\forall s' \in \Sigma : \neg(s \ \tau \ s') \ ? \ \{s\}$
  $\qquad\qquad\qquad \mid \{s' \mid \exists s'' \in \Sigma : s \ \tau \ s'' \wedge s' \in f(s'')\})$
- The DCPO [20] $\langle \dot D^=, \ \dot\sqsubseteq^=, \ \dot\bot^=, \ \dot\sqcup^= \rangle$ is the restriction of the pointwise extension of the flat DCPO $\langle D^=, \sqsubseteq^=, \bot^=, \sqcup^= \rangle$;
- $D^= \triangleq (\wp(\Sigma) \setminus \{\emptyset\}) \cup \{\bot^=\}$
- $\bot^= \triangleq \Sigma_\bot$
- $\dot D^= \triangleq \{f \in \Sigma \longmapsto D^= \mid \forall s, s' \in \Sigma : (s' \in f(s) \wedge f(s) \neq \bot^=) \ \Rightarrow$
  $\qquad\qquad\qquad\qquad\qquad (s' \in \check\tau \wedge f(s') = \{s'\})\}.$

This is not the classical Smyth ordering!

[20] Directed Complete POset.

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,
  - $F^\natural\llbracket \tau \rrbracket \triangleq \lambda s \cdot (\forall s' \in \Sigma : \neg(s \ \tau \ s') \ ? \ \{s\} \mid \{s' \mid \exists s'' \in \Sigma : s \ \tau \ s'' \wedge s' \in f(s'')\}) \in E \xmapsto{m} E$ is $\preccurlyeq$-monotone, and
  - $\forall \tau : \tau^\sharp = \mathrm{lfp}_{\dot\bot^=}^{\preccurlyeq} F^\natural\llbracket \tau \rrbracket$

  then:
  - $\dot D^= \subseteq E$, and
  - $\dot\sqsubseteq^= \subseteq \preccurlyeq.$

Hoare/Angelic Denotational Semantics

- $\tau^\flat \triangleq \dot\alpha^\flat(\tau^\natural)$

- $\dot\alpha^\flat(\varphi) \triangleq \lambda s \cdot \varphi(s) \cap \Sigma$

- $\dot\gamma^\flat(\phi) \triangleq \lambda s \cdot \phi(s) \cup \{\bot\}$

- $\langle \Sigma \longmapsto \wp(\Sigma_\bot),\ \dot\subseteq \rangle \xleftrightarrow[\dot\alpha^\flat]{\dot\gamma^\flat} \langle \Sigma \longmapsto \wp(\Sigma),\ \dot\subseteq \rangle$

- $\tau^\flat = \mathrm{lfp}^{\dot\subseteq}_{\dot\emptyset}\ F^\natural$ where $F^\natural = \lambda s \cdot (\forall s' \in \Sigma : \neg(s\ \tau\ s')\ ?\ \{s\}\ |\ \{s'\ |\ \exists s'' \in \Sigma : s\ \tau\ s'' \wedge s' \in f(s'')\})$ is a complete $\dot\cup$-morphism on the complete lattice $\langle \Sigma \longmapsto \wp(\Sigma),\ \dot\subseteq,\ \dot\emptyset,\ \lambda s \cdot \Sigma,\ \dot\cup,\ \dot\cap \rangle$ which is the pointwise extension of the powerset $\langle \wp(\Sigma),\ \emptyset \rangle$.

$$\boxed{\begin{array}{c} \textsc{Denotational/Functional} \\ \underline{\textsc{Deterministic}}\ \textsc{Semantics} \end{array}}$$

Denotational/Functional <u>Deterministic</u> Abstraction

- $\langle \wp(\Sigma_\bot),\ \subseteq \rangle \xleftrightarrow[\alpha^s]{\gamma^s} \langle \Sigma \cup \{\bot, \top\},\ \sqsubseteq^s \rangle$ where $\forall s \in \Sigma : \bot \sqsubseteq^s \bot \sqsubseteq^s s \sqsubseteq^s s \sqsubseteq^s \top \sqsubseteq^s \top$

- The abstraction α^s disregards nondeterminism:

$$\alpha^s(\emptyset) \triangleq \bot \qquad\qquad \gamma^s(\bot) \triangleq \{\bot\}$$
$$\alpha^s(\{\bot\}) \triangleq \bot$$
$$\alpha^s(\{s\}) = \alpha^s(\{s, \bot\}) \triangleq s,\ s \in \Sigma \qquad \gamma^s(s) \triangleq \{s, \bot\}$$
$$\alpha^s(X) \triangleq \top,\ \text{otherwise} \qquad \gamma^s(\top) \triangleq \Sigma_\bot$$

- $\langle \Sigma \longmapsto \wp(\Sigma_\bot),\ \subseteq \rangle \xleftrightarrow[\dot\alpha^s]{\dot\gamma^s} \langle \Sigma \longmapsto (\Sigma \cup \{\bot, \top\}),\ \dot\sqsubseteq^s \rangle$ where $\dot\alpha^s(f) \triangleq \lambda s \cdot \alpha^s(f(s))$ and $\dot\gamma^s(f) \triangleq \lambda s \cdot \gamma^s(f(s))$

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

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

Fixpoint Denotational/Functional Deterministic Semantics of a Transition System $\langle \Sigma, \tau \rangle$

- $\tau^s \triangleq \dot{\alpha}^s(\tau^\natural) = \dot{\alpha}^s(\mathrm{lfp}^{\sqsubseteq^\natural}_{\lambda s\bullet\{\bot\}} F^\natural) = \mathrm{lfp}^{\sqsubseteq^s}_{\lambda s\bullet\bot} F^s$

- $F^s \triangleq \lambda f\bullet\lambda s\bullet(\forall s' \in \Sigma : \neg(s\ \tau\ s')\ ?\ s\ |\ \sqcup^s\{f(s'') \mid s\ \tau\ s'\})$

Proof

  - $\dot{\alpha}^s(\lambda s\bullet\{\bot\}) = \lambda s\bullet\bot$;
  - $\dot{\alpha}^s \circ F^d = F^s \circ \dot{\alpha}^s$ leads to the definition of F^d;
  - $\dot{\alpha}^s(\dot{\bigsqcup}^\infty_i f_i) = \dot{\bigsqcup}^{ss}_i \dot{\alpha}^s(f_i)$ leads to the definition of the $\sqsubseteq^s$-lub $\dot{\bigsqcup}^s$;
  - F^s is monotonic for $\sqsubseteq^s$;
  - Kleene's fixpoint transfer theorem applies.

$\square$

The Rôle of $\top$

- The top element $\top$ is often eliminated from Scott's domains by lack of intuitive interpretation;
- We interpret $\top$ as an abstraction forgetting about nondeterminism.

Deterministic Transition System, Scott's Semantics

- If τ is deterministic, then $\tau \in \Sigma \nrightarrow \Sigma$ and

$$F^s = \lambda f\bullet\lambda s\bullet(s \notin \mathrm{dom}\,\tau\ ?\ s\ |\ \tau(s)) \qquad (1)$$

- $\top$ is unreachable and can be eliminated from the domain so that $\sqsubseteq^s$ is exactly Scott ordering.

PREDICATE TRANSFORMER SEMANTICS

Nondeterministic Denotational to Predicate Transformer Abstractions

$$\alpha^{-1} \triangleq \lambda f \in D \longmapsto \wp(E) \cdot \lambda s' \cdot \{s \mid s' \in f(s)\}$$

$$\gamma^{-1} \triangleq \lambda f \in E \longmapsto \wp(D) \cdot \lambda s \cdot \{s' \mid s \in f(s')\}$$

$$\alpha^{\triangleright} \triangleq \lambda f \in D \longmapsto \wp(E) \cdot \lambda P \in \wp(D) \cdot \{s' \mid \exists s \in P : s' \in f(s)\}$$

$$\gamma^{\triangleright} \triangleq \lambda \Psi \in \wp(D) \longmapsto \wp(E) \cdot \lambda s \cdot \Psi(\{s\})$$

$$\alpha^{\cup} \triangleq \lambda \Psi \in \wp(D) \longmapsto \wp(E) \cdot \lambda Q \in \wp(E) \cdot \{s \mid \Psi(\{s\}) \cap Q \neq \emptyset\}$$

$$\gamma^{\cup} \triangleq \lambda \Psi \in \wp(E) \longmapsto \wp(D) \cdot \lambda P \in \wp(D) \cdot \{s' \mid \Psi(\{s'\}) \cap P \neq \emptyset\}$$

$$\alpha^{\sim} \triangleq \lambda \Psi \in \wp(D) \longmapsto \wp(E) \cdot \lambda P \in \wp(D) \cdot \neg(\Psi(\neg P))$$

$$\gamma^{\sim} \triangleq \lambda \Psi \in \wp(E) \longmapsto \wp(D) \cdot \lambda P \in \wp(D) \cdot \neg(\Psi(\neg P))$$

$$\alpha^{\cap} \triangleq \lambda \Phi \in \wp(D) \longmapsto \wp(E) \cdot \lambda Q \in \wp(E) \cdot \{s \mid \Phi(\neg\{s\}) \cup Q = E\}$$

$$\gamma^{\cap} \triangleq \lambda \Phi \in \wp(E) \longmapsto \wp(D) \cdot \lambda P \in \wp(D) \cdot \{s' \mid \Phi(\neg\{s'\}) \cup P = D\}$$

Predicate Transformer Abstractions

If $f \in D \longmapsto \wp(E)$):

$$\text{gsp}[\![f]\!] \triangleq \alpha^{\triangleright}[f] \in \wp(D) \longmapsto \wp(E)$$
$$= \lambda P \in \wp(D) \cdot \{s' \in E \mid \exists s \in P : s' \in f(s)\}$$

$$\text{gspa}[\![f]\!] \triangleq \alpha^{\sim} \circ \alpha^{\triangleright}[f] \in \wp(D) \longmapsto \wp(E)$$
$$= \lambda P \in \wp(D) \cdot \{s' \in E \mid \forall s \in D : s' \in f(s) \Rightarrow s \in P\}$$

$$\text{gwp}[\![f]\!] \triangleq \alpha^{\sim} \circ \alpha^{\triangleright} \circ \alpha^{-1}[f] \in \wp(E) \longmapsto \wp(D)$$
$$= \lambda Q \in \wp(E) \cdot \{s \in D \mid \forall s' \in E : s' \in f(s) \Rightarrow s' \in Q\}$$

$$\text{gwpa}[\![f]\!] \triangleq \alpha^{\triangleright} \circ \alpha^{-1}[f] \in \wp(E) \longmapsto \wp(D)$$
$$= \lambda Q \in \wp(E) \cdot \{s \in D \mid \exists s' \in Q : s' \in f(s)\}$$

Galois Connection Commutative Diagram

$$\langle D \longmapsto \wp(E), \dot\subseteq \rangle \xleftarrow[\alpha^{\triangleright}]{\gamma^{\triangleright}} \langle \wp(D) \longmapsto \wp(E), \dot\subseteq \rangle \xleftarrow[\alpha^{\sim}]{\gamma^{\sim}} \langle \wp(D) \longmapsto \wp(E), \dot\supseteq \rangle$$

$$\big\updownarrow \alpha^{-1} \ \gamma^{-1} \qquad \big\updownarrow \alpha^{\cup} \ \gamma^{\cup} \qquad \big\updownarrow \alpha^{\cap} \ \gamma^{\cap}$$

$$\langle E \longmapsto \wp(D), \dot\subseteq \rangle \xleftarrow[\alpha^{\triangleright}]{\gamma^{\triangleright}} \langle \wp(E) \longmapsto \wp(D), \dot\subseteq \rangle \xleftarrow[\alpha^{\sim}]{\gamma^{\sim}} \langle \wp(E) \longmapsto \wp(D), \dot\supseteq \rangle$$

Generalized Weakest Precondition Semantics

- $\tau^{\text{gwp}} \triangleq \text{gwp}[\![\tau^{\natural}]\!] = \text{lfp}_{\perp^{\text{gwp}}}^{\sqsubseteq^{\text{gwp}}} F^{\text{gwp}}$

- $F^{\text{gwp}} \in D^{\text{gwp}} \overset{\text{m}}{\longmapsto} D^{\text{gwp}} \triangleq \lambda \Phi \cdot \lambda Q \cdot (\neg\check\tau \cup Q) \dot\cap \text{gwp}[\![\tau^{\blacktriangleright}]\!] \circ \Phi$
$= \lambda \Phi \cdot \lambda Q \cdot (Q \cap \check\tau) \dot\cup \text{wp}[\![\tau^{\blacktriangleright}]\!] \circ \Phi$
  is a $\sqsubseteq^{\text{gwp}}$-monotone map on the complete lattice $\langle D^{\text{gwp}}, \sqsubseteq^{\text{gwp}}, \perp^{\text{gwp}}, \sqcup^{\text{gwp}} \rangle$

- $\text{wp}[\![f]\!]\, Q \triangleq \{s \in \Sigma \mid \exists s' \in \Sigma : s' \in f(s) \land \forall s' \in f(s) : s' \in Q\}$

- $D^{\text{gwp}} \triangleq \wp(\Sigma_\perp) \overset{\cap}{\longmapsto} \wp(\Sigma),$

- $\Phi \sqsubseteq^{\text{gwp}} \Psi \triangleq \forall Q \subseteq \Sigma : \Psi(Q \cup \{\perp\}) \subseteq \Phi(Q \cup \{\perp\}) \land \Phi(\Sigma) \subseteq \Psi(\Sigma),$

- $\perp^{\text{gwp}} = \lambda Q \cdot (\perp \in Q\ ?\ \Sigma \mid \emptyset)$

- $\underset{i \in \Delta}{\sqcup^{\text{gwp}}} \Psi_i \triangleq \lambda Q \cdot \underset{i \in \Delta}{\bigcap} \Psi_i(Q \cup \{\perp\}) \cap (\perp \notin Q\ ?\ \underset{i \in \Delta}{\bigcup} \Psi_i(\Sigma) \mid \Sigma).$

Dijkstra's Weakest Conservative Precondition Abstraction

- $\langle D^{\mathrm{gwp}}, \dot{\supseteq} \rangle \xleftarrow[\alpha^{\mathrm{wp}}]{\gamma^{\mathrm{wp}}} \langle D^{\mathrm{wp}}, \dot{\supseteq} \rangle$ where $D^{\mathrm{wp}} \triangleq \wp(\Sigma) \stackrel{\cap}{\longmapsto} \wp(\Sigma)$, $\alpha^{\mathrm{wp}} \triangleq$
  $\lambda \Phi \cdot \Phi|_{\wp(\Sigma)}$ and $\gamma^{\mathrm{wp}}(\Psi) \triangleq \lambda Q \cdot (\bot \notin Q ? \Psi(Q) \mid \emptyset)$;
- $\tau^{\mathrm{wp}} \triangleq \alpha^{\mathrm{wp}}(\tau^{\mathrm{gwp}}) = \alpha^{\mathrm{wp}}(\mathrm{gwp}[\![\tau^{\sharp}]\!])$;
- Dikstra's fixpoint characterization of τ^{wp} is for a given postcondition Q;
- 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
  $\alpha^{\mathrm{Q}}(\Phi) \triangleq \Phi(Q)$ and $\gamma^{\mathrm{Q}}(P) \triangleq \lambda R \cdot (Q \subseteq R ? P \mid \emptyset)$;

Dijkstra's Weakest Liberal Precondition Semantics

- $\langle D^{\mathrm{gwp}}, \dot{\supseteq} \rangle \xleftarrow[\alpha^{\mathrm{wlp}}]{\gamma^{\mathrm{wlp}}} \langle D^{\mathrm{wlp}}, \dot{\supseteq} \rangle$ where $D^{\mathrm{wlp}} \triangleq \wp(\Sigma) \stackrel{\cap}{\longmapsto} \wp(\Sigma)$, $\alpha^{\mathrm{wlp}} \triangleq$
  $\lambda \Phi \cdot \lambda Q \cdot \Phi(Q \cup \{\bot\})$ and $\gamma^{\mathrm{wlp}}(\Psi) \triangleq \lambda Q \cdot (\bot \in Q ? \Psi(Q) \mid \emptyset)$;
- $\tau^{\mathrm{wlp}} \triangleq \alpha^{\mathrm{wlp}}(\tau^{\mathrm{gwp}}) = \mathrm{gwp}[\![\tau^{\flat}]\!]$;
- By Kleene fixpoint transfer, $\tau^{\mathrm{wlp}} = \lambda Q \cdot \mathrm{gfp}_{\Sigma}^{\subseteq} F^{\mathrm{wp}}[\![Q]\!]$.

Dijkstra's Weakest Conservative Precondition Semantics

From $\tau^{\mathrm{wp}}(Q) = \alpha^{\mathrm{Q}}(\alpha^{\mathrm{wp}}(\tau^{\mathrm{gwp}}))$ and Kleene fixpoint transfer theorem, we derive:

- $\tau^{\mathrm{wp}}(Q) = \lambda Q \cdot \mathrm{lfp}_{\emptyset}^{\subseteq} F^{\mathrm{wp}}[\![Q]\!]$
- $F^{\mathrm{wp}} \in \wp(\Sigma) \longmapsto \wp(\Sigma) \stackrel{\mathrm{m}}{\longmapsto} \wp(\Sigma)$
- $\tau^{\blacktriangleright}(s) \triangleq \{s' \mid s \ \tau \ s'\}$;
- $F^{\mathrm{wp}}[\![Q]\!] \triangleq \lambda P \cdot (Q \cap \check{\tau}) \cup \mathrm{wp}[\![\tau^{\blacktriangleright}]\!] P$
  $\qquad = \lambda P \cdot (\neg \check{\tau} \cup Q) \cap \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!] P$
  is a $\subseteq$-monotone map on the complete lattice $\langle \wp(\Sigma), \subseteq, \emptyset, \Sigma, \cup, \cap \rangle$.

Correspondence Between Pre- and Postcondition Semantics

If $f \in D \longmapsto \wp(E)$ then $\langle \wp(D), \subseteq \rangle \xleftarrow[\mathrm{gsp}[\![f]\!]]{\mathrm{gwp}[\![f]\!]} \langle \wp(E), \subseteq \rangle$.

Panel 1 (top-left)

$$\boxed{\boxed{\text{Axiomatic Semantics}}}$$

Panel 2 (top-right)

Galois Connection Commutative Diagram

$$1(\langle \alpha,\ \gamma \rangle) \triangleq \alpha \qquad\qquad \mathrm{HA}(\alpha) \triangleq \{\langle x,\ y \rangle \in D^\natural \times D^\sharp \mid \alpha(x) \sqsubseteq^\sharp y\}$$

$$2(\langle \alpha,\ \gamma \rangle) \triangleq \gamma \qquad\qquad \mathrm{HC}(\gamma) \triangleq \{\langle x,\ y \rangle \in D^\natural \times D^\sharp \mid x \sqsubseteq^\natural \gamma(y)\}$$

$$\mathrm{AC}(\gamma) \triangleq \lambda x{\bullet} \sqcap^\sharp \{y \mid x \sqsubseteq^\natural \gamma(y)\} \quad \mathrm{AH}(H) \triangleq \lambda x{\bullet} \sqcap^\sharp \{y \mid \langle x,\ y \rangle \in H\}$$

$$\mathrm{CA}(\alpha) \triangleq \lambda y{\bullet} \sqcup^\natural \{x \mid \alpha(x) \sqsubseteq^\sharp y\} \quad \mathrm{CH}(H) \triangleq \lambda y{\bullet} \sqcup^\natural \{x \mid \langle x,\ y \rangle \in H\}$$

Panel 3 (bottom-left)

Galois Connections, Complete Join/Meet Morphisms and Tensor Product

- G. c.: $\langle D^\natural,\ \sqsubseteq^\natural \rangle \longleftrightarrow \langle D^\sharp,\ \sqsubseteq^\sharp \rangle \triangleq \{\langle \alpha,\ \gamma \rangle \mid \langle D^\natural,\ \sqsubseteq^\natural \rangle \xleftrightarrow[\alpha]{\gamma} \langle D^\sharp,\ \sqsubseteq^\sharp \rangle\}$;

- Complete join morphisms: $D^\natural \longmapsto D^\sharp \triangleq \{\alpha \in D^\natural \longmapsto D^\sharp \mid \forall X \subseteq D^\natural : \alpha(\sqcup^\natural X) = \sqcup^\sharp \alpha^{\blacktriangleright}(X)\}$;

- Complete meet morphisms: $D^\sharp \longmapsto D^\natural \triangleq \{\gamma \in D^\sharp \longmapsto D^\natural \mid \forall Y \subseteq D^\sharp : \gamma(\sqcap^\sharp Y) = \sqcap^\natural \gamma^{\blacktriangleright}(Y)\}$;

- Tensor products: $\langle D^\natural,\ \sqsubseteq^\natural \rangle \otimes \langle D^\sharp,\ \sqsubseteq^\sharp \rangle \triangleq \{H \in \wp(D^\natural \times D^\sharp) \mid (1) \land (2) \land (3)\}$ where the conditions are:

  1. $(X \sqsubseteq^\natural X' \land \langle X',\ Y' \rangle \in H \land Y' \sqsubseteq^\sharp Y) \Rightarrow (\langle X,\ Y \rangle \in H)$;

  2. $(\forall i \in \Delta : \langle X_i,\ Y \rangle \in H) \Rightarrow (\langle \underset{i \in \Delta}{\sqcup^\natural} X_i,\ Y \rangle \in H)$;

  3. $(\forall i \in \Delta : \langle X,\ Y_i \rangle \in H) \Rightarrow (\langle X,\ \underset{i \in \Delta}{\sqcap^\sharp} Y_i \rangle \in H)$.

Panel 4 (bottom-right)
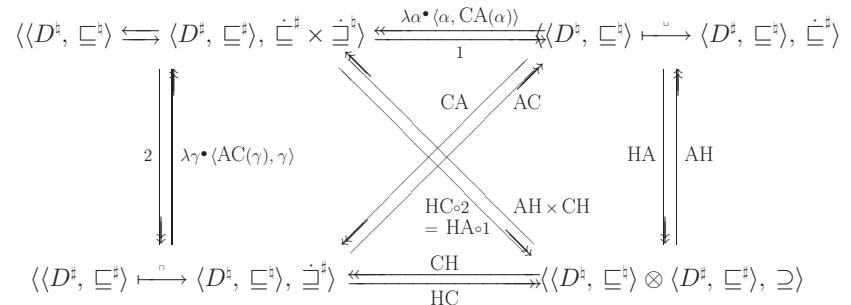
Floyd/Hoare/Naur Partial Correctness Semantics

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

- $\tau^{\mathrm{pH}} = \{\langle P,\ Q \rangle \in \wp(\Sigma) \otimes \wp(\Sigma) \mid \exists I \in \wp(\Sigma) : P \subseteq I \land I \subseteq \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!] I \land (I \cap \check{\tau}) \subseteq Q\}$.

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

Hoare Logic

- Hoare triples: $\{P\}\tau^{\vec{\infty}}\{Q\} \triangleq \langle P,\, Q \rangle \in \tau^{\mathrm{pH}}$, $\{P\}\tau\{Q\} \triangleq P \subseteq \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\,Q$;
- Hoare logic: $\{P\}\tau^{\vec{\infty}}\{Q\}$ if and only if it derives from the axiom:

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

and the following inference rules:

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

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

Manna/Pnueli Total Correctness Logic

- Manna/Pnueli triples: $[P]\tau^{\vec{\infty}}[Q] \triangleq \langle P,\, Q \rangle \in \tau^{\mathrm{tH}}$, $[P]\tau[Q] \triangleq P \subseteq \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\,Q$;
- Manna/Pnueli total correctness axiomatic semantics: $[P]\tau^{\vec{\infty}}[Q]$ if and only if it derives from the axiom (τ), the inference rules $(\Rightarrow)$, $(\wedge)$, $(\vee)$ and the following:

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

Floyd Total Correctness Semantics

- $\tau^{\mathrm{tH}} \triangleq \mathrm{HC}(\tau^{\mathrm{wp}})$;
- $\tau^{\mathrm{tH}} = \{\langle P,\, Q \rangle \in \wp(\Sigma) \otimes \wp(\Sigma) \mid \exists\epsilon \in \mathbb{O} : \exists I \in (\epsilon+1) \longmapsto \wp(\Sigma) :$
  $\forall\delta \leq \epsilon : I^\delta \subseteq (\neg\check{\tau} \cup Q) \cap \mathrm{gwp}[\![\tau^{\blacktriangleright}]\!]\big(\underset{\beta<\delta}{\cup}\,I^\beta\big) \wedge P \subseteq I^\epsilon\}.$

- Floyd (equivalent) verification conditions:

$$\forall s \in I^\delta : \underset{\vee}{}\ \forall s' : \neg(s\,\tau\,s') \wedge s \in Q$$
$$\exists s' : s\,\tau\,s' \wedge \forall s' : s\,\tau\,s' \Rightarrow (\exists\beta < \delta : s' \in I^\beta)$$

Proof By the lower fixpoint induction principle: if $\langle D,\, \sqsubseteq,\, \bot,\, \sqcup \rangle$ is a DCPO, $F \in D \overset{\mathrm{m}}{\longmapsto} D$ is $\sqsubseteq$-monotone, $\bot \in D$ satisfies $\bot \sqsubseteq F(\bot)$ and $P \in D$ then $P \sqsubseteq \mathrm{lfp}_\bot^\sqsubseteq F \iff (\exists\epsilon \in \mathbb{O} : \exists I \in (\epsilon+1) \longmapsto D : I^0 \sqsubseteq \bot \wedge \forall\delta : 0 < \delta \leq \epsilon \Rightarrow I^\delta \sqsubseteq F(\underset{\zeta<\delta}{\sqcup}\,I^\zeta) \wedge P \sqsubseteq I^\epsilon)$. $\square$


LATTICE OF SEMANTICS

Comparison of Semantics

- $\tau^\natural \in D^\natural \le \tau^\sharp \in D^\sharp$ iff $\tau^\sharp = \alpha^\sharp(\tau^\natural)$ and $\langle D^\natural,\, \le \rangle \xleftarrow[\alpha^\sharp]{\gamma^\sharp} \langle D^\sharp,\, \trianglelefteq \rangle$ is a preorder between semantics;

- The quotient poset is isomorphic to Ward lattice of upper closure operators $\gamma^\sharp \circ \alpha^\sharp$ on $\langle D^{\vec\infty},\, \subseteq \rangle$;

- We get a lattice of semantics which is part of the lattice of abstract interpretations.

Lattice of Semantics

$$\boxed{\text{APPLICATION TO THE (EAGER) LAMBDA-CALCULUS (PROSPECTIVE)}}$$
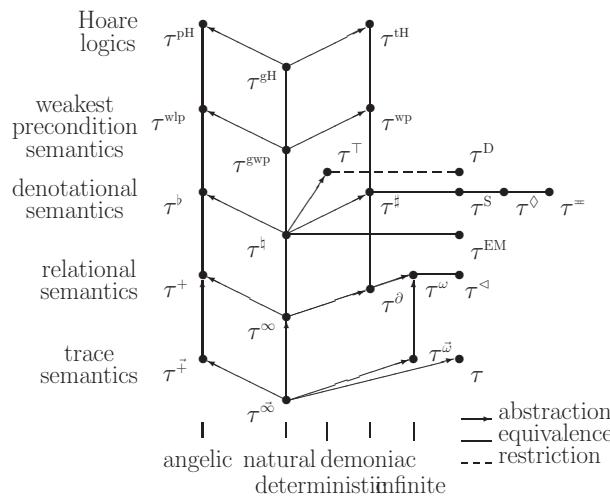
Relational Semantics with Closures

$$E \vdash\!\!\!- \lambda\mathbf{x} \cdot e \Rightarrow \langle \mathbf{x},\, e,\, E \rangle$$

$$\frac{E \vdash\!\!\!- e_1 \Rightarrow \bot}{E \vdash\!\!\!- e_1(e_2) \Rightarrow \bot}$$

$$\frac{c = \langle \mathbf{x},\, e,\, E[f \leftarrow c] \rangle}{E \vdash\!\!\!- \mu\mathbf{f} \cdot \lambda\mathbf{x} \cdot e \Rightarrow c}$$

$$\frac{\begin{array}{c} E \vdash\!\!\!- e_1 \Rightarrow \langle \mathbf{x}',\, e',\, E' \rangle \\ E \vdash\!\!\!- e_2 \Rightarrow \bot \end{array}}{E \vdash\!\!\!- e_1(e_2) \Rightarrow \bot}$$

$$\frac{\begin{array}{c} E \vdash\!\!\!- e_1 \Rightarrow \langle \mathbf{x}',\, e',\, E' \rangle \\ E \vdash\!\!\!- e_2 \Rightarrow v, v \ne \Omega \\ E'[\mathbf{x}' \leftarrow v] \vdash\!\!\!- e' \Rightarrow r \end{array}}{E \vdash\!\!\!- e_1(e_2) \Rightarrow r}$$

$$\frac{\begin{array}{c} E \vdash\!\!\!- e_1 \Rightarrow \langle \mathbf{x}',\, e',\, E' \rangle \\ E \vdash\!\!\!- e_2 \Rightarrow v, v \ne \Omega \\ E'[\mathbf{x}' \leftarrow v] \vdash\!\!\!- e' \Rightarrow \bot \end{array}}{E \vdash\!\!\!- e_1(e_2) \Rightarrow \bot}$$

Denotational Semantics

$$\mathsf{u}, \mathsf{f}, \varphi \in \mathbb{U} \cong \{\Omega\}_{\perp}^{\top} \oplus \mathbb{Z}_{\perp}^{\top} \oplus [\mathbb{U} \longmapsto \mathbb{U}]_{\perp}^{\top} \quad \text{values}$$

$$\mathsf{R} \in \mathbb{R} \triangleq \mathbb{X} \longmapsto \mathbb{U} \qquad \text{environments}$$

$$\phi \in \mathbb{S} \triangleq \mathbb{R} \longmapsto \mathbb{U} \qquad \text{semantic domain}$$

$$\mathbf{S}[\![\lambda\mathsf{x} \cdot e]\!]\mathsf{R} \triangleq \lambda\mathsf{u} \cdot (\mathsf{u} = \perp\ ?\ \perp$$
$$\qquad\qquad | \mathsf{u} = \Omega\ ?\ \Omega$$
$$\qquad\qquad | \mathbf{S}[\![e]\!]\mathsf{R}[\mathsf{x}{\leftarrow}\mathsf{u}])$$

$$\mathbf{S}[\![e_1(e_2)]\!]\mathsf{R} \triangleq (\mathbf{S}[\![e_1]\!]\mathsf{R} = \perp \vee \mathbf{S}[\![e_2]\!]\mathsf{R} = \perp\ ?\ \perp$$
$$\qquad\qquad | \mathbf{S}[\![e_1]\!]\mathsf{R} = \mathsf{f} \in [\mathbb{U} \longmapsto \mathbb{U}]\ ?\ \mathsf{f}\big(\mathbf{S}[\![e_2]\!]\mathsf{R}\big)$$
$$\qquad\qquad | \Omega)$$

$$\mathbf{S}[\![\mu\mathsf{f} \cdot \lambda\mathsf{x} \cdot e]\!]\mathsf{R} \triangleq \mathrm{lfp}^{\sqsubseteq}\ \lambda\varphi \cdot \mathbf{S}[\![\lambda\mathsf{x} \cdot e]\!]\mathsf{R}[\mathsf{f}{\leftarrow}\varphi]$$

Abstraction

- The rules of the relational semantics can be interpreted as least fix-points for the bifinite ordering;
- The abstraction function $\alpha \in \wp(\mathbb{V}) \longmapsto \mathbb{U}$ is as follows [21]:

$$\alpha(\emptyset) \triangleq \perp$$
$$\alpha(\{\perp\}) \triangleq \perp$$
$$\alpha(\{z\}) = \alpha(\{z, \perp\}) \triangleq z, \quad z \in \mathbb{Z}$$
$$\alpha(\{\Omega\}) \triangleq \Omega$$
$$\alpha(X) \triangleq \top, \quad \text{otherwise.}$$
$$\alpha(\langle\mathsf{x},\ e,\ E\rangle) \triangleq \lambda\mathsf{u} \in \mathbb{U} \cdot \alpha(\{r \mid \exists v \in \mathbb{V} : \alpha(\{v\}) = \mathsf{u}\ \wedge$$
$$E[\mathsf{x} \leftarrow v] \vdash e \Rightarrow r\})$$

---
[21] Liftinga and injections are omitted.

- $\alpha \in (\mathbb{X} \longmapsto \mathbb{V}) \longmapsto (\mathbb{X} \longmapsto \mathbb{U})$:

$$\alpha(E) \triangleq \lambda\mathsf{x} \cdot \alpha(E(\mathsf{x}))$$

- $\alpha \in \wp((\mathbb{X} \longmapsto \mathbb{V}) \times \mathbb{V}) \longmapsto ((\mathbb{X} \longmapsto \mathbb{U}) \longmapsto \mathbb{U})$:

$$\alpha(\Phi[\![e]\!]) \triangleq \lambda\mathsf{R} \cdot \alpha(\{r \mid \exists E : \alpha(E) = \mathsf{R} \wedge E \vdash e \Rightarrow r \in \Phi[\![e]\!]\})$$

Alternative Partitionning of Executions

- We have explored linear time (set of traces) semantics with partition between finite and infinite traces;
- A different partitionning for branching time (tree) semantics would be states with or without later possibility to branch toward a nonterminating execution.

Need for semantics at various levels of refinement

- Many semantics at different levels of abstraction are needed for program analysis;
- A unified framework for presenting all these semantics seems indispensable.

Further Work for Semanticians

- Consider realistic practical languages (C^{++}, Java, ML, etc);
- Consider computable approximations of semantic domains (to be used in program analysis);
- A need for mathematical foundations but also applications of programming semantics;
- A lot of work for future applied semanticians (like applied mathematicians).