TOWARDS A FIXPOINT SEMANTICS MODELING FINITE FAILURE

- an example of derivation by abstract interpretation of a useful new semantics
- in order to get what you want you often need to start with something more concrete

Motivations

- A property χ, χ induces an *observational equivalence* $\approx_\chi$ on programs.
  $P_1 \approx_\chi P_2$ if P_1 and P_2 are indistinguishable according to the property χ.

- The semantics $\mathcal{S}$ is *correct* w.r.t. χ if
  $\mathcal{S}(P_1) = \mathcal{S}(P_2) \Rightarrow P_1 \approx_\chi P_2$.

- The semantics $\mathcal{S}$ is *fully abstract* if
  $P_1 \approx_\chi P_2 \Rightarrow \mathcal{S}(P_1) = \mathcal{S}(P_2)$.

- Moreover, the semantics $\mathcal{S}$ is *and-compositional* if
  $\mathcal{S}(G_1 \wedge G_2) = \mathcal{S}(G_1)\mathcal{S}(\wedge)\mathcal{S}(G_2)$.

We define the *observational equivalence* $\approx_{ff}$ on programs
$P_1 \approx_{ff} P_2$ if a goal G finitely fail in P_1 iff G finitely fail in P_2.

Which Semantics for Finite Failure?

- $\mathsf{FF_P} = \{\ A \mid\ A$ is ground and $\leftarrow A$ has a fair finitely failed SLD-tree in $\mathsf{P}\ \}$

  $\mathsf{FF_P}$ is not correct w.r.t. $\approx_{\mathsf{ff}}$.

  Example

  $\mathsf{P_1}$: `p(f(X)):-p(X)` $\mathsf{P_2}$: `p(f(X)):-p(X),p(a)`

  $$\mathsf{FF_{P_1}} = \mathsf{FF_{P_2}} = \{\ \mathsf{p(a), p(f(a)), p(f(f(a))),\ldots\ldots}\}$$

  $\leftarrow \mathsf{p(X)}$ *finitely fails in* $\mathsf{P_2}$ *but not in* $\mathsf{P_1}$.

- The Non-Ground Finite Failure set [Levi et al.90]

  $\mathsf{NGFF_P} = \{A \mid\ \leftarrow A$ has a fair finitely failed SLD-tree in $\mathsf{P}\}$

  $\mathsf{NGFF_P}$ is correct, fully abstract and AND-compositional [Gori et al.97].

But $\mathsf{NGFF_P}$ has no a direct fixpoint characterization.

$$\Downarrow$$

- $\mathsf{NGFF_P}$ can not be computed by an iterative fixpoint operator.
- all the semantics-based analysis and inductive verification methods can not be applied to finite failure.

The Idea: to use abstract interpretation

We extend the Abstract Interpretation Framework [Comini et al.99] to deal with

- fair selection rule
- infinite derivations

The steps:

1. To define a domain of collections, i.e. functions which associate to each goal G the set of (possibly infinite) derivations of G via a fair selection rule.

2. To define the semantics of a program P as the greatest fixpoint of a co-continuous operator on collections.

3. Using the theory of abstract interpretation, establish sufficient conditions so that the abstract fixpoint semantics is *precise* ($\alpha(\mathsf{gfp}(\mathsf{T})) = \mathsf{gfp}(\mathsf{T}^{a})$) with respect to the concrete one.

4. To apply the previous framework to derive a fixpoint semantics based on a co-continuous operator modeling finite failure.

- A collection D is a partial function,
  $$\mathsf{D}(\mathsf{G}) = \{\ \mathsf{d}|\ \ \mathsf{d} = \mathsf{G} \overset{\mathsf{G}}{\underset{c_1\ 1}{\longrightarrow}} \vartheta_1 \cdots \overset{\vartheta_n}{\underset{c_n}{\longrightarrow}} \quad \mathsf{G}_n \ldots$$
  d is an SLD derivation via a parallel rule $\}$
  $$\mathsf{G} = \mathsf{A}_1, \ldots,\ \underset{\uparrow_j}{\mathsf{A}_i},\ \underset{\uparrow_{j+1}}{\mathsf{A}_{i+1}}, \ldots, \mathsf{A}_n$$

- $\mathbb{C}$ is the domain of collections and $(\mathbb{C}\ \sqsubseteq)$ is the concrete domain, where $\mathsf{D}_1 \sqsubseteq \mathsf{D}_2$ if $\forall \mathsf{G},\ \mathsf{D}_1(\mathsf{G}) \subseteq \mathsf{D}_2(\mathsf{G})$.

Denotational semantics

The Denotational semantics is defined inductively on the syntax, using the semantic operators $+, \odot, \times, \triangleright$.

$$\mathcal{Q}[\![\mathsf{G}\ \mathit{in}\ \mathsf{P}]\!] := \mathcal{G}[\![\mathsf{G}]\!]_{gfp\, \mathcal{P}[\![\mathsf{P}]\!]}$$
$$\mathcal{G}[\![\mathsf{A}, \mathsf{G}]\!]_I := \mathcal{A}[\![\mathsf{A}]\!]_I \times \mathcal{G}[\![\mathsf{G}]\!]_I \qquad \mathcal{G}[\![\emptyset]\!]_I := \phi_{\emptyset}$$
$$\mathcal{A}[\![\mathsf{A}]\!]_I := \mathsf{A} \odot I$$
$$\mathcal{P}[\![\{c\} \cup \mathsf{P}]\!]_I := \mathcal{C}[\![c]\!]_I + \mathcal{P}[\![\mathsf{P}]\!]_I \qquad \mathcal{P}[\![\emptyset]\!]_I := \mathit{Id}_{\mathbb{I}}$$
$$\mathcal{C}[\![\mathsf{H} : -\, \mathsf{B}]\!]_I := \mathsf{tree}(\mathsf{H} : -\, \mathsf{B}) \triangleright \mathcal{G}[\![\mathsf{B}]\!]_I.$$

where

$$\mathsf{tree}(p(t) : -\mathsf{B}) := \phi \left[\{p(x), p(x) \overset{\{x/t\}}{\underset{p(t):-B}{\longrightarrow}} B\} \Big/ p(x) \right].$$

Program Denotation

The *fixpoint denotation* of the program P is $\mathcal{F}[\![\mathsf{P}]\!] := \mathsf{gfp}\,\mathcal{P}[\![\mathsf{P}]\!]$.

$\mathcal{F}[\![\mathsf{P}]\!]$ has the following properties:

- $\mathcal{P}[\![\mathsf{P}]\!]$ is co-continuous on $(\mathbb{C}, \sqsubseteq)$.
- $\mathsf{P}_1 \approx_{\mathsf{der}} \mathsf{P}_2$ if for every goal G, G has the same SLD-derivations (via the parallel rule) in P_1 and in P_2.
  $\mathcal{F}[\![\mathsf{P}]\!]$ is correct and fully abstract w.r.t. $\approx_{\mathsf{der}}$.

Example

$$\begin{array}{l} \mathsf{P} \\ \mathsf{q(a) :- p(X)} \\ \mathsf{p(f(X)) :- p(X)} \end{array}$$

$\mathsf{gfp}(\mathcal{P}[\![\mathsf{P}]\!])(\mathsf{q(X)}) =$

$$(\mathsf{d} := \mathsf{q(X)} \xrightarrow[\mathsf{q(a):-p(X_1)}]{\{\mathsf{X/a}\}} \mathsf{p(X_1)} \xrightarrow[\mathsf{p(f(X_2)):-p(X_2)}]{\{\mathsf{X_1/f(X_2)}\}} \mathsf{p(X_2)} \xrightarrow[\mathsf{p(f(X_3)):-p(X_3)}]{\{\mathsf{X_2/f(X_3)}\}} \mathsf{p(X_3)} \ldots; \bigcup \mathsf{prefixes(d)})$$

$\mathsf{gfp}(\mathcal{P}[\![\mathsf{P}]\!])(\mathsf{p(X)}) =$

$$(\mathsf{d'} := \mathsf{p(X)} \xrightarrow[\mathsf{p(f(X_1)):-p(X_1)}]{\{\mathsf{X/f(X_1)}\}} \mathsf{p(X_1)} \xrightarrow[\mathsf{p(f(X_2)):-p(X_2)}]{\{\mathsf{X_1/f(X_2)}\}} \mathsf{p(X_2)} \xrightarrow[\mathsf{p(f(X_3)):-p(X_3)}]{\{\mathsf{X_2/f(X_3)}\}} \mathsf{p(X_3)} \ldots; \bigcup \mathsf{prefixes(d')})$$

- An *observable* is any property which can be "observed" on the concrete semantics and can be formalized as a Galois insertion.

  Example *Consider the* computed answers *for the goal* $\mathsf{p}(\mathsf{X})$.
  We can observe $\vartheta := \vartheta_1 \cdot \ldots \vartheta_n$, *where*
  $\mathsf{p}(\mathsf{X}) \xrightarrow[c_1]{\vartheta_1} \mathsf{G}_1 \cdots \xrightarrow[c_n]{\vartheta_n} \mathsf{G}_n \rightarrow \Box \in \mathcal{F}[\![\mathsf{P}]\!](\mathsf{p}(\mathsf{X}))$.
  α_{ca} *is a Galois insertion.*

- With the observable α, we can systematically define the *optimal* abstract semantics operators $\widetilde{\odot}, \widetilde{\times}, \widetilde{\triangleright}, \widetilde{\sum}, \widetilde{\prod}$, simply as $\mathsf{A} \mathbin{\widetilde{\odot}} \mathsf{X} := \alpha(\mathsf{A} \odot \gamma(\mathsf{X}))$, *etc.*..

- Moreover if α, γ and the concrete operators satisfy also the following conditions

  1. $\alpha(\mathsf{A} \odot \mathsf{D}) = \alpha(\mathsf{A} \odot (\gamma \circ \alpha)\mathsf{D})$,
  2. $\alpha(\mathsf{D} \times \mathsf{D}') = \alpha((\gamma \circ \alpha)\mathsf{D} \times (\gamma \circ \alpha)\mathsf{D}')$,
  3. $\alpha(\mathsf{D} \triangleright \mathsf{D}') = \alpha(\mathsf{D} \triangleright (\gamma \circ \alpha)\mathsf{D}')$.
  4. $\alpha(\prod\{\mathcal{P}[\![\mathsf{P}]\!] \downarrow i\}_{i \in I}) = \alpha(\prod(\gamma \circ \alpha)\{\mathcal{P}[\![\mathsf{P}]\!] \downarrow i\}_{i \in I})$,
  5. $\alpha(\prod \gamma(\{\mathsf{X}_i\}_{i \in I})) = \mathsf{glb}\{\mathsf{X}_i\}_{i \in I}$.

The Theory of Observables II

The Abstract Denotational Semantics, defined as

$$
\begin{aligned}
\mathcal{Q}_\alpha[\![\mathsf{G}\ \mathit{in}\ \mathsf{P}]\!] &:= \mathcal{G}_\alpha[\![\mathsf{G}]\!]_{\mathsf{gfp}\,\mathcal{P}_\alpha[\![\mathsf{P}]\!]} \\
\mathcal{G}_\alpha[\![\mathsf{A},\mathsf{G}]\!]_\mathsf{X} &:= \mathcal{A}_\alpha[\![\mathsf{A}]\!]_\mathsf{X} \mathbin{\tilde{\times}} \mathcal{G}_\alpha[\![\mathsf{G}]\!]_\mathsf{X} & \mathcal{G}_\alpha[\![\varnothing]\!]_\mathsf{X} &:= \alpha(\phi_\varnothing) \\
\mathcal{A}_\alpha[\![\mathsf{A}]\!]_\mathsf{X} &:= \mathsf{A} \mathbin{\tilde{\odot}} \mathsf{X} \\
\mathcal{P}_\alpha[\![\{\mathsf{c}\} \cup \mathsf{P}]\!]_\mathsf{X} &:= \mathcal{C}_\alpha[\![\mathsf{c}]\!]_\mathsf{X} \mathbin{\tilde{+}} \mathcal{P}_\alpha[\![\mathsf{P}]\!]_\mathsf{X} & \mathcal{P}_\alpha[\![\emptyset]\!]_\mathsf{X} &:= \alpha(\mathit{Id}_\mathbb{I}) \\
\mathcal{C}_\alpha[\![\mathsf{H}:-\mathsf{B}]\!]_\mathsf{X} &:= \alpha \circ \mathcal{C}[\![\mathsf{H}:-\mathsf{B}]\!] \circ \gamma(\mathsf{X}). \\
\mathcal{F}_\alpha[\![\mathsf{P}]\!] &:= \mathsf{gfp}\,\mathcal{P}_\alpha[\![\mathsf{P}]\!]
\end{aligned}
$$

has the following properties,

- $\alpha(\mathcal{A}[\![\mathsf{A}]\!]_\mathrm{I}) = \mathcal{A}_\alpha[\![\mathsf{A}]\!]_{\alpha(\mathrm{I})}$,
- $\alpha(\mathcal{G}[\![\mathsf{G}]\!]_\mathrm{I}) = \mathcal{G}_\alpha[\![\mathsf{G}]\!]_{\alpha(\mathrm{I})}$,
- $\alpha(\mathcal{C}[\![\mathsf{c}]\!]_\mathrm{I}) = \mathcal{C}_\alpha[\![\mathsf{c}]\!]_{\alpha(\mathrm{I})}$,
- $\alpha(\mathcal{P}[\![\mathsf{P}]\!]_\mathrm{I}) = \mathcal{P}_\alpha[\![\mathsf{P}]\!]_{\alpha(\mathrm{I})}$,
- $\mathcal{P}_\alpha[\![\mathsf{P}]\!]$ is co-continuous on $\mathbb{A}$ and $\mathcal{F}_\alpha[\![\mathsf{P}]\!] = \mathcal{P}_\alpha[\![\mathsf{P}]\!] \downarrow \omega$,
- $\alpha(\mathcal{F}[\![\mathsf{P}]\!]) = \mathcal{F}_\alpha[\![\mathsf{P}]\!]$ and $\alpha(\mathcal{Q}[\![\mathbf{G}\ \mathit{in}\ \mathsf{P}]\!]) = \mathcal{Q}_\alpha[\![\mathbf{G}\ \mathit{in}\ \mathsf{P}]\!]$.

The Semantics Domain I

We want to apply the framework to define a fixpoint semantics modeling finite failure.
The semantics domain: an abstract collection X which associates G the set S of its instances which finitely fail.

- S is a downward closed set, i.e., if $G \in S \Rightarrow G\vartheta \in S$.
- *The key point:* S enjoys a kind of "upward closure" property.
  Example
  Assume $\{p(a), p(f(a)), p(f(f(X))), p(f(f(a))), \ldots\} \in S$.
  Which behavior for $p(X)$*?*

  - *Suppose* $p(X)$ *has a successful derivation.*
    $p(X) \xrightarrow[c_1]{\sigma_1} G_1 \xrightarrow[c_2]{\sigma_2}, \ldots, G_{n-1} \xrightarrow[c_n]{\sigma_n} \Box$
    Let $\vartheta = \sigma_1 \cdot \ldots \cdot \sigma_n$.
    $\forall p(t) \in S$, $\nexists \delta = mgu(p(t), p(X)\vartheta)$, *otherwise* $p(t)\delta$

  - *Suppose* $p(X)$ *has an infinite derivation.*
    $p(X) \xrightarrow[c_1]{\sigma_1} G_1 \xrightarrow[c_2]{\sigma_2}, \ldots, G_{n-1} \xrightarrow[c_n]{\sigma_n} \ldots$
    Let $\vartheta_i = \sigma_1 \cdot \ldots \cdot \sigma_i$.
    $\forall p(t) \in S$, $\forall i \ \nexists \delta_i = mgu(p(t), p(X)\vartheta_i)$, *otherwise* $p(t)\delta_i$

$$\Downarrow$$

if $\forall$ *possible sequences* $\vartheta_1 :: \ldots :: \vartheta_n :: \ldots \ p(X)\vartheta_i \leq p(X)\vartheta_{i+1}$

$\exists p(t) \in S$, *s.t.* $\forall i \, \exists \delta_i = mgu(p(t), p(X)\vartheta_i)$,

then

$p(X) \in S$.

The Semantics Domain II

$$\mathrm{up}^{ff}_G(S) = S \cup \{G\vartheta \mid \begin{array}{l} \text{for all (possibly infinite) sequences} \\ \vartheta_1 :: \ldots\ldots :: \vartheta_n :: \ldots, G\vartheta_i \le G\vartheta_{i+1} \\ \exists \bar{G} \in S \text{ s.t.} \\ \forall\, i,\ \bar{G} \text{ unifies with } G\vartheta\vartheta_i \end{array} \}.$$

up^{ff}_G is a closure operator.

S is a downward closed set of instances of a goal G closed also w.r.t. up^{ff}_G.

The finite failure observable

From the all the possible derivations for G in P,

$$\left\{\begin{array}{l} G \xrightarrow[c_1]{\vartheta_1} \ldots \xrightarrow[c_n]{\vartheta_n} G_n; \\ G \xrightarrow[c_1]{\vartheta_1} \ldots \xrightarrow[c_n]{\vartheta_n} \Box; \\ G \xrightarrow[c_1]{\vartheta_1} \ldots \xrightarrow[c_n]{\vartheta_n} G_n \ldots; \\ \vdots \end{array}\right\}$$

$$\Downarrow \quad \alpha$$

$$\{G\vartheta \mid G\vartheta \text{ finitely fails in } P\}$$

Informally, α gives the set of instances of G which can not be rewritten successfully or infinitely.

- $< \alpha, \gamma >$ is a Galois insertion.
- α satisfies the sufficient conditions 1-5.

We can define the optimal abstract operators on the domain for finite failure.

- $A \tilde{\odot} X = \phi\left[{}^{R}/_{A}\right]$ where
  $R := \{A\vartheta \mid A' \leq A, \vartheta = mgu(A, A'')_{|A}\}$.

- $$X_1 \tilde{\times} X_2 = \lambda G.up^{ff}_{G}(\{G\vartheta \mid G = (G_1, G_2),\ G_1\vartheta \in X_1(G_1) \text{ or } G_2\vartheta \in X_2(G_2)\}).$$

- $\widetilde{\prod} X_i = \lambda G.up^{ff}_{G}(\cup(X_i(G)).$

- $\widetilde{\sum} X_i = \lambda G. \cap (X_i(G)).$

$\tilde{\times}$ gives a simpler AND- compositionality result than the one stated in [Gori et al.97].

Example

$$\begin{array}{l} P \\ q(a). \\ p(f(X)). \end{array}$$

Let X^{ff} *the abstract collection for atomic goals only.*

$$X^{ff}(q(X)) = \{\ q(f(a), q(f(X)), \ldots\}$$
$$X^{ff}(p(X)) = \{\ p(a)\}$$

The goal $p(X), q(X)$ *finitely fails in* P

$$p(X), q(X) \in up^{ff}{}_{p(X),q(X)}(p(a), q(a); p(f(a)), q(f(a)); p(f(X)), q(f(X)) : \ldots)$$

The Fixpoint Operator

$$\mathcal{P}_\alpha[\![P]\!]_X = \lambda p(x).\{\, p(\tilde{t}) \mid \text{for every clause defining the procedure } p,$$
$$p(t) :- B \in P$$
$$p(\tilde{t}) \in up^{ff}_{p(x)}(Nunif_{p(x)}(p(t)) \cup$$
$$\{p(t)\tilde{\vartheta} \mid \tilde{\vartheta} \text{ is a relevant for } p(t),$$
$$B\tilde{\vartheta} \in up^{ff}_B(\{B\sigma \mid B = (B_1, \ldots, B_n)\vartheta\ \exists B_i\vartheta\sigma \in X(B_i)\}\})\}$$

- $\mathcal{P}_\alpha[\![P]\!]$ is co-continuous $\Rightarrow gfp(\mathcal{P}_\alpha[\![P]\!]) = up^{ff}_{p(x)}(\cup_{i<\omega} \mathcal{P}_\alpha[\![P]\!] \downarrow i)$

Example where $\top^{ff} = \lambda p(x).\emptyset$

P

$q(a) :- p(X)$

$p(f(X)) :- p(X)$

$$\begin{aligned}
\mathcal{P}_\alpha[\![P]\!] \downarrow 1(q(X)) &= \{\ q(f(X)), q(f(f(X))), \ldots \\
&\qquad q(f(a)), q(f(f(a))), \ldots\ \} \\
\mathcal{P}_\alpha[\![P]\!] \downarrow 1(p(X)) &= \{\ p(a)\ \} \\
\\
\mathcal{P}_\alpha[\![P]\!] \downarrow 2(q(X)) &= \mathcal{P}_\alpha[\![P]\!] \downarrow 1(q(X)) \\
\mathcal{P}_\alpha[\![P]\!] \downarrow 2(p(X)) &= \{\ p(a), p(f(a))\ \} \\
&\vdots \\
\mathcal{P}_\alpha[\![P]\!] \downarrow \omega(q(X)) &= \mathcal{P}_\alpha[\![P]\!] \downarrow 1(q(X)) \\
\mathcal{P}_\alpha[\![P]\!] \downarrow \omega(p(X)) &= \{\ p(a), p(f(a)), p(f(f(a))), \ldots\}
\end{aligned}$$

$p(X) \notin up^{ff}_{p(X)}(\mathcal{P}_\alpha[\![P]\!] \downarrow \omega(p(X)))$ *since*

$\exists \vartheta_1 = \{X/f(Y)\} :: \vartheta_2 = \{X/f(f(Y))\} :: \vartheta_3 = \{X/f(f(f(Y)))\} :: \ldots,$

and $\forall p(t) \in \mathcal{P}_\alpha[\![P]\!] \downarrow \omega(p(X))\ \forall i\ \ \nexists \delta_i = mgu(p(t), p(X)\vartheta_i)$.

$$\Downarrow$$

$$q(a) \notin \mathcal{P}_\alpha[\![P]\!] \downarrow \omega + 1(q(X))$$

Relation to other Semantics

Lassez and Maher in [Lassez and al.84] introduced the following direct fixpoint characterization for FF_P.

- $F_P = \cup_{d \geq 1} F_P^d$

We can relate $\mathcal{P}_\alpha[\![P]\!] \downarrow k$ and F_P^k.

For every finite k.

$$\cup_{p(x)} \mathtt{ground}(\mathcal{P}_\alpha[\![P]\!] \downarrow k\ (p(x))) = F_P^k.$$

Moreover $\mathcal{P}_\alpha[\![P]\!]$ is co-continuous.

Conclusions and Future Work

- We have defined a fixpoint semantics correctly modeling finite failure, based on a co-continuous operator $\mathcal{P}_\alpha[\![\mathsf{P}]\!]$.
- $\mathcal{P}_\alpha[\![\mathsf{P}]\!]$ is not finitary however for analysis and verification purposes, we are interested in its finitely computable approximations.
- Finitely computable approximations giving a subset or a superset of $\mathsf{NGFF_P}$ can be easily defined starting from $\mathcal{P}_\alpha[\![\mathsf{P}]\!]$.
- We believe that other interesting semantics can be derived from the concrete semantics. We are now currently working on the definition of a new fixpoint semantics modeling "exact answers" of infinite derivations based on a co-continuous operator.

  Some computable abstractions of this semantics could be useful for the analysis of termination of logic programs.
- Finally, our results are a nice example which shows that abstract interpretation is useful for defining new fixpoint semantics. Note that a fixpoints semantics for finite failure was hard to define in a direct way.