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 $x$, $x$ induces an *observational equivalence* $\approx_x$ on programs.
  $P_1 \approx_x P_2$ if $P_1$ and $P_2$ are indistinguishable according to the property $x$.

• The semantics $S$ is *correct* w.r.t. $x$ if
  $S(P_1) = S(P_2) \Rightarrow P_1 \approx_x P_2$.

• The semantics $S$ is *fully abstract* if
  $P_1 \approx_x P_2 \Rightarrow S(P_1) = S(P_2)$.

• Moreover, the semantics $S$ is *and-compositional* if
  $S(G_1 \land G_2) = S(G_1)S(\land)S(G_2)$.

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?

\[ \text{FF}_P = \{ A \mid A \text{ is ground and } \leftarrow A \text{ has a fair finitely failed SLD-tree in } P \} \]

\text{FF}_P \text{ is not correct w.r.t. } \approx_{ff}. \]

\textbf{Example}

\[ P_1: \; p(f(X)) :- p(X) \]
\[ P_2: \; p(f(X)) :- p(X), p(a) \]

\[ \text{FF}_P = \{ p(a), p(f(a)), p(f(f(a))), \ldots \} \]

\[ \leftarrow p(X) \text{ finitely fails in } P_2 \text{ but not in } P_1. \]

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

\[ \text{NGFF}_P = \{ A \mid \leftarrow A \text{ has a fair finitely failed SLD-tree in } P \} \]

\[ \text{NGFF}_P \text{ is correct, fully abstract and AND-compositional [Gori et al.97].} \]

But \( \text{NGFF}_P \) has no a direct fixpoint characterization.

\[ \downarrow \]

\[ \textbullet \] \( \text{NGFF}_P \) can not be computed by an iterative fixpoint operator.

\[ \textbullet \] 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 ($\alpha(gfp(T)) = gfp(T^a)$) 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.
The Concrete Semantics

- A collection \( D \) is a partial function,
  \[
  D(G) = \{ d \mid d = G \xrightarrow{c_1} \theta_1 \cdots \xrightarrow{c_n} G_n \ldots \}
  \]
  \( d \) is an SLD derivation via a parallel rule

- \( C \) is the domain of collections and \((C \sqsubseteq)\) is the concrete domain, where \( D_1 \sqsubseteq D_2 \) if \( \forall G, D_1(G) \subseteq D_2(G) \).

Denotational semantics

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

\[
\begin{align*}
\eta[\{G \mid P\}] & := \eta[G]_{gfp \eta[P]} \\
\eta[A, G]_I & := A[A]_I \times \eta[G]_I \\
\eta[\emptyset]_I & := \Phi_0 \\
\lambda[A]_I & := A \odot I \\
\eta[c \cup P]_I & := \eta[c]_I + \eta[P]_I \\
\eta[H : - B]_I & := \text{tree}(H : - B) \triangleright \eta[B]_I.
\end{align*}
\]

where

\[
\text{tree}(p(t) : - B) := \Phi \left[ \frac{\{p(x), p(x) \xrightarrow{\{x/t\} \rightarrow B}\}}{p(t) : - B} \right].
\]
Program Denotation

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

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

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

Example

\[
p
q(a) : \neg p(X) \\
p(f(X)) : \neg p(X)
\]

\[
gfp(P[P])(q(X)) = \\
\left( d := q(X) \frac{\{X/X_1\}}{q(a) : \neg p(X_1)} \rightarrow p(X) \frac{\{X_1/f(X_2)\}}{p(f(X_2)) : \neg p(X_2)} \rightarrow p(X) \frac{\{X_2/f(X_3)\}}{p(f(X_3)) : \neg p(X_3)} \rightarrow p(X) \ldots ; \right) \\
\bigcup \text{prefixes}(d)
\]

\[
gfp(P[P])(p(X)) = \\
\left( d' := p(X) \frac{\{X/f(X_1)\}}{p(f(X_1)) : \neg p(X_1)} \rightarrow p(X) \frac{\{X_1/f(X_2)\}}{p(f(X_2)) : \neg p(X_2)} \rightarrow p(X) \frac{\{X_2/f(X_3)\}}{p(f(X_3)) : \neg p(X_3)} \rightarrow p(X) \ldots ; \right) \\
\bigcup \text{prefixes}(d')
\]
The Theory of Observables I

- 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 $p(X)$.

We can observe $\emptyset := \emptyset_1 \cdots \emptyset_n$, where

$$p(X) \xrightarrow{\emptyset_1} G_1 \cdots \xrightarrow{\emptyset_n} G_n \rightarrow \square \in \mathcal{F}[p(X)].$$

$\alpha_{ca}$ is a Galois insertion.

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

- Moreover if $\alpha, \gamma$ and the concrete operators satisfy also the following conditions

  1. $\alpha(A \odot D) = \alpha(A \odot (\gamma \circ \alpha)D),$
  2. $\alpha(D \times D') = \alpha((\gamma \circ \alpha)D \times (\gamma \circ \alpha)D'),$
  3. $\alpha(D \triangleright D') = \alpha(D \triangleright (\gamma \circ \alpha)D').$
  4. $\alpha(\prod\{P\downarrow i\}_{i \in I}) = \alpha(\prod(\gamma \circ \alpha)\{P\downarrow i\}_{i \in I}),$
  5. $\alpha(\prod \gamma(\{X_i\}_{i \in I})) = \text{glb}\{X_i\}_{i \in I}.$
The Theory of Observables II

The Abstract Denotational Semantics, defined as

\[ \Omega_\alpha[\mathbb{G \ in \ P}] := \mathcal{G}_\alpha[\mathbb{G}]_{\text{gfp} \mathcal{P}_\alpha[P]} \]
\[ \mathcal{G}_\alpha[A, \mathbb{G}]_X := \mathcal{A}_\alpha[A]_X \sim \mathcal{G}_\alpha[\mathbb{G}]_X \]
\[ \mathcal{G}_\alpha[\emptyset]_X := \alpha(\phi_\emptyset) \]
\[ \mathcal{A}_\alpha[A]_X := A \sim X \]
\[ \mathcal{P}_\alpha[\{c\} \cup P]_X := \mathcal{C}_\alpha[c]_X \sim \mathcal{P}_\alpha[P]_X \]
\[ \mathcal{P}_\alpha[\emptyset]_X := \alpha(\text{Id}_\emptyset) \]
\[ \mathcal{C}_\alpha[H : - B]_X := \alpha \circ \mathcal{C}[H : - B] \circ \gamma(X) \]
\[ \mathcal{F}_\alpha[P] := \text{gfp} \mathcal{P}_\alpha[P] \]

has the following properties,

- \( \alpha(\mathcal{A}[A]_I) = \mathcal{A}_\alpha[A]_{\alpha(I)} \),
- \( \alpha(\mathcal{G}[\mathbb{G}]_I) = \mathcal{G}_\alpha[\mathbb{G}]_{\alpha(I)} \),
- \( \alpha(\mathcal{C}[c]_I) = \mathcal{C}_\alpha[c]_{\alpha(I)} \),
- \( \alpha(\mathcal{P}[P]_I) = \mathcal{P}_\alpha[P]_{\alpha(I)} \),
- \( \mathcal{P}_\alpha[P] \) is co-continuous on \( \mathcal{A} \) and \( \mathcal{F}_\alpha[P] = \mathcal{P}_\alpha[P] \downarrow \omega \),
- \( \alpha(\mathcal{F}[P]) = \mathcal{F}_\alpha[P] \) and \( \alpha(\Omega[\mathbb{G \ in \ P}]) = \Omega_\alpha[\mathbb{G \ in \ P}] \).
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 $G \in S \Rightarrow G\emptyset \in S$.
- 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.
  \[ p(X) \xrightarrow{\sigma_1} G_1 \xrightarrow{\sigma_2} \ldots, G_{n-1} \xrightarrow{\sigma_n} \Box \]
  Let $\emptyset = \sigma_1 \cdot \ldots \cdot \sigma_n$.
  $\forall p(t) \in S, \not\exists \delta = \text{mgu}(p(t), p(X)\emptyset)$, otherwise $p(t)\emptyset$

- Suppose $p(X)$ has an infinite derivation.
  \[ p(X) \xrightarrow{\sigma_1} G_1 \xrightarrow{\sigma_2} \ldots, G_{n-1} \xrightarrow{\sigma_n} \ldots \]
  Let $\emptyset_i = \sigma_1 \cdot \ldots \cdot \sigma_i$.
  $\forall p(t) \in S, \forall i \not\exists \delta_i = \text{mgu}(p(t), p(X)\emptyset_i)$, otherwise $p(t)\emptyset_i$

\[ \downarrow \]

if $\forall$ possible sequences $\emptyset_1 :: \ldots :: \emptyset_n :: \ldots p(X)\emptyset_i \leq p(X)\emptyset_{i+1}$

$\exists p(t) \in S, s.t. \forall i \exists \delta_i = \text{mgu}(p(t), p(X)\emptyset_i)$,

then

$p(X) \in S$. 

A fixpoint semantics for reasoning about finite failure
The Semantics Domain II

\[ u_{G}^{ff}(S) = S \cup \{ G \theta \mid \text{for all (possibly infinite) sequences } \theta_1 :: \ldots :: \theta_n :: \ldots, G \theta_i \leq G \theta_{i+1} \exists \tilde{G} \in S \text{ s.t. } \forall i, \tilde{G} \text{ unifies with } G \theta \theta_i \} \]

\[ u_{G}^{ff} \] is a closure operator.

\( S \) is a downward closed set of instances of a goal \( G \) closed also w.r.t. \( u_{G}^{ff} \).
The finite failure observable

From the all the possible derivations for $G$ in $P$,

\[
\begin{align*}
G \xrightarrow{c_1} \cdots \xrightarrow{c_n} G_n; \\
G \xrightarrow{c_1} \cdots \xrightarrow{c_n} \Box; \\
G \xrightarrow{c_1} \cdots \xrightarrow{c_n} G_n \cdots; \\
\vdots
\end{align*}
\]

\[\downarrow \alpha\]

\{G\theta \mid G\theta \text{ finitely fails in } P\}

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

- $< \alpha, \gamma >$ is a Galois insertion.

- $\alpha$ satisfies the sufficient conditions 1-5.
The Abstract Optimal Operators

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

- \( A \bowtie X = \phi^{[R/A]} \) where
  \( R := \{ A \theta \mid A' \leq A, \theta = \text{mgu}(A, A'') \}_A \).

- \( X_1 \bowtie X_2 = \lambda G. \text{up}^f_G(\{ G \theta \mid G = (G_1, G_2), G_1 \theta \in X_1(G_1) \) or \( G_2 \theta \in X_2(G_2) \}) \).

- \( \prod X_i = \lambda G. \text{up}^f_G(\cup(X_i(G))) \).

- \( \sum X_i = \lambda G. \cap(X_i(G)) \).

\( \bowtie \) gives a simpler AND-compositionality result than the one stated in [Gori et al. 97].

Example

\[
\begin{align*}
  P & \quad q(a). \\
  & \quad p(f(X)).
\end{align*}
\]

Let \( X^f \) the abstract collection for atomic goals only.

\[
\begin{align*}
  X^f(q(X)) & = \{ q(f(a), q(f(X)), \ldots \} \\
  X^f(p(X)) & = \{ p(a) \}
\end{align*}
\]

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

\[
p(X), q(X) \in \text{up}^f_{p(X), q(X)}(p(a), q(a); p(f(a)), q(f(a)); p(f(X)), q(f(X)) : \ldots)
\]
The Fixpoint Operator

\[ \mathcal{P}_a[\mathcal{P}]_x = \lambda p(x). \{ \text{p}(t) \mid \text{for every clause defining the procedure } p, \]
\[ \text{p}(t) : -B \in \mathcal{P} \]
\[ \text{p}(\mathcal{\tilde{t}}) \in up_{p,x}^{ff}(\text{Unif}_{p(x)}(\text{p}(t)) \cup \{ \text{p}(t)\mathcal{\tilde{t}} \mid \mathcal{\tilde{t}} \text{ is a relevant for } \text{p}(t), \]
\[ B\mathcal{\tilde{t}} \in up_B^{ff}(\{B\sigma \mid B = (B_1, \ldots, B_n)\theta \exists B_i\theta \sigma \in X(B_i))) \]

• \( \mathcal{P}_a[\mathcal{P}] \) is co-continuous \( \Rightarrow \) \( gfp(\mathcal{P}_a[\mathcal{P}]) = up_{p,x}^{ff}(\cup_{i<\omega} \mathcal{P}_a[\mathcal{P}] \downarrow i) \)

Example

\begin{align*}
q(a) & : -p(X) \\
p(f(X)) & : -p(X)
\end{align*}

\[ \mathcal{P}_a[\mathcal{P}] \downarrow 1(q(X)) = \{ q(f(X)), q(f(f(X))), \ldots \}
\[ \mathcal{P}_a[\mathcal{P}] \downarrow 1(p(X)) = \{ p(a) \}
\]

\[ \mathcal{P}_a[\mathcal{P}] \downarrow 2(q(X)) = \mathcal{P}_a[\mathcal{P}] \downarrow 1(q(X))
\]

\[ \mathcal{P}_a[\mathcal{P}] \downarrow 2(p(X)) = \{ p(a), p(f(a)) \}
\]

\[ \vdots \]

\[ \mathcal{P}_a[\mathcal{P}] \downarrow \omega(q(X)) = \mathcal{P}_a[\mathcal{P}] \downarrow 1(q(X))
\]

\[ \mathcal{P}_a[\mathcal{P}] \downarrow \omega(p(X)) = \{ p(a), p(f(a)), p(f(f(a))), \ldots \}
\]

\[ p(X) \not\in up_{p,x}^{ff}(\mathcal{P}_a[\mathcal{P}] \downarrow \omega(p(X))) \text{ since } \]

\[ \exists \theta_1 = \{X/f(Y)\} :: \theta_2 = \{X/f(f(Y))\} :: \theta_3 = \{X/f(f(f(Y)))\} :: \ldots , \]

\[ \text{and } \forall p(t) \in \mathcal{P}_a[\mathcal{P}] \downarrow \omega(p(X)) \forall \theta \exists \delta_i = \text{mg}u(p(t), p(X)\theta_i). \]

\[ \downarrow \]

\[ q(a) \not\in \mathcal{P}_a[\mathcal{P}] \downarrow \omega + 1(q(X)) \]
Relation to other Semantics

Lassez and Maher in [Lassez and al.84] introduced the following direct fixpoint characterization for $\mathbb{F}_p$.

- $F_p = \bigcup_{d \geq 1} F_p^d$

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

For every finite $k$.

$$\bigcup_{p(x)\text{ground}}(\mathcal{P}_\alpha[P] \downarrow k (p(x))) = F_p^k.$$

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 $\mathcal{P}_\alpha[P]$.

- $\mathcal{P}_\alpha[P]$ 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 $\mathcal{P}_\alpha[P]$.

- 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.