Divergence & Coinduction | Convergence & Induction

Op. semantics usually focus on convergence

$$\langle c, s \rangle \Downarrow s'$$

Mathematical model: transition system $(\Sigma, \longrightarrow)$

Standard practice for $\longrightarrow$

- inductive relation
- syntax-oriented

} presentation via inference rules

$$\frac{\langle c_1, s_1 \rangle \Downarrow s_2 \qquad \langle c_2, s_2 \rangle \Downarrow s_3}{\langle c_1 ; c_2, s_1 \rangle \Downarrow s_3}$$

What are inference rules ?

1. Fix a universe $\mathcal{U}$ of judgments

Ex.

$\langle c, s \rangle \Downarrow s'$

$\Gamma \vdash t : T$

$\Gamma \vdash (\lambda x. t) =_\beta t[s/x]$

$\vdash \varphi \wedge \psi$

$\vdots$

A judgment is a linguistic unity that we assert

2. An inference rule over $\mathcal{U}$ is a pair $(\mathcal{A}, c)$ s.t.

$c \in \mathcal{U}$ is called the conclusion

$\mathcal{A} \subseteq \mathcal{U}$ is the set of premises

Notation.
$$\frac{\mathcal{A}}{c} \qquad \frac{\{a_1, \ldots, a_n\}}{c} \qquad \frac{a_1 \quad \cdots \quad a_n}{c}$$

Ex. For $\mathcal{U} \triangleq \{ \langle c, s \rangle \Downarrow s' \mid c \in Com,\ s, s' \in States \}$

$A \triangleq \{ \langle c_1, s_1 \rangle \Downarrow s_2,\ \langle c_2, s_2 \rangle \Downarrow s_3 \mid \dots \}$

Then $(A, \langle c_1; c_2 \rangle \Downarrow s_3)$ is an inference rule

We call axioms rules of the form $(\emptyset, c)$

③ An inference system is a collection Φ of inference rules

Ex. Op. semantics defines an inference system

How do we prove judgments in a system Φ?

Usually, c provable iff $\exists$ finite proof tree of rules in Φ

$$\underbrace{\dfrac{\dfrac{q_1 \quad \cdots \quad q_m}{p_1} \qquad \cdots \qquad \dfrac{r_1 \quad \cdots \quad r_\ell}{p_n}}{c}}_{\text{The derivation tree is finite}}$$

$\Downarrow$

induction proof principle

s.t. $(\{p_1, \dots, p_n\}, c) \in \Phi$

$(\{q_1, \dots, q_m\}, p_1) \in \Phi$

$\vdots$

How to make all of that precise?

Fixed Point Semantics of Inference Systems

Any inference system Φ gives a function

$$F_\Phi : \mathcal{P}(\mathcal{U}) \to \mathcal{P}(\mathcal{U})$$

$$\underbrace{F_\Phi(T)}_{\text{hypotheses}} \triangleq \{ \underbrace{c \in \mathcal{U} \mid \exists (A, c) \in \Phi \,.\, A \subseteq T}_{\text{conclusion}} \}$$

F_Φ gives the conclusion of <u>one-step</u> of inference

$$F_\Phi(\emptyset) = \text{axioms}$$

$$F_\Phi(F_\Phi(\emptyset)) = \text{depth-1 consequences of axioms}$$

$$F_\Phi(F_\Phi(F_\Phi(\emptyset))) = \text{depth-2 consequences of axioms}$$

Fact. $\mathcal{P}(\mathcal{U})$ is a complete lattice

1. There is a partial order given by subset inclusion

   - $A \subseteq A$
   - $A \subseteq B$ & $B \subseteq C \implies A \subseteq C$
   - $A \subseteq B$ & $B \subseteq A \iff A = B$

2. There are meet and join operators, given by arbitrary intersection $\bigcap_{i \in I} A_i$ and union $\bigcup_{i \in I} A_i$, respectively.

   Here, I is any set of indexes, and $\{A_i\}_{i \in I}$ is a I-indexed family of sets in $\mathcal{U}$.

$$\underbrace{B \subseteq \bigcap_{i \in I} A_i \iff \forall i \in I.\ B \subseteq A_i}_{\text{Universal property of meet}}$$

$$\underbrace{\bigcup_{i \in I} A_i \subseteq B \iff \forall i \in I.\ A_i \subseteq B}_{\text{Universal property of join}}$$

<u>Remark</u>. Universal properties uniquely define objects.

<u>Ex</u>. UP of meet tells that $\bigcap_i A_i$ is the greatest lower bound of $\{A_i\}_{i \in I}$

greatest $\swarrow$ All lower bounds B of $\{A_i\}_{i \in I}$ (i.e. those s.t. $\forall i \in I.\ B \subseteq A_i$) are smaller than $\bigcap_i A_i$:

$$B \subseteq \bigcap_i A_i$$

lower bound $\searrow$ $\bigcap_i A_i \subseteq A_i \quad (\forall i)$

In fact, since

$$B \subseteq \bigcap_i A_i \iff \forall i \in I.\ B \subseteq A_i \qquad \text{(UP)}$$

We have:

- Lower bound

$$(\text{Reflexivity of } \subseteq) \implies \underbrace{\bigcap_i A_i}_{B} \subseteq \bigcap_i A_i$$

$$\implies \forall i \in I.\ \bigcap_i A_i \subseteq A_i \qquad [\text{By (UP)}]$$

- Greatest: Assume $\forall i \in I.\ B \subseteq A_i$. Then $B \subseteq \bigcap_i A_i$ by UP

- Uniqueness: Suppose we have X satisfying UP. Then $X = \bigcap_i A_i$, i.e. $\bigcap_i A_i \subseteq X$ and $X \subseteq \bigcap_i A_i$

Why is all of that interesting? Because of Knaster-Tarski Theorem

Recall that a function $F: \mathcal{P}(\mathcal{U}) \to \mathcal{P}(\mathcal{U})$ is monotone if

$$A \subseteq B \implies F(A) \subseteq F(B)$$

And that $X \subseteq \mathcal{U}$ is a fixed point of F if

$$F(X) = X$$

In general, F may have none or many fixed points

Ex. $\mathrm{Id}: \mathcal{P}(\mathcal{U}) \to \mathcal{P}(\mathcal{U})$, $A \mapsto A$ Then any $A \subseteq \mathcal{U}$ is a fixed point of Id

$\mathrm{Not}: \mathcal{P}(\mathcal{U}) \to \mathcal{P}(\mathcal{U})$, $A \mapsto \mathcal{U} \setminus A$ Then $\neg \exists X \subseteq \mathcal{U}.\ \mathrm{Not}(X) = X$

Theorem (Knaster-Tarski). If $F : \mathcal{P}(\mathcal{U}) \to \mathcal{P}(\mathcal{U})$ is monotone, then F has both least and greatest fixed points

$$lfp(F) = \bigcap \{ X \mid F(X) \subseteq X \}$$ Inductively-defined sets

$$gfp(F) = \bigcup \{ X \mid X \subseteq F(X) \}$$ CoInductively-defined sets

Consequently, we have

$$F(A) \subseteq A \implies lfp(F) \subseteq A$$ induction proof principle

$$A \subseteq F(A) \implies A \subseteq gfp(F)$$ coinduction proof principle

Back to F_Φ ...

<u>Lemma</u>. For any system Φ, $F_\Phi : \mathcal{P}(\mathcal{U}) \to \mathcal{P}(\mathcal{U})$ is monotone

$lfp(F_\Phi)$: inductively-defined sets of Φ-provable judgments

$c \in lfp(F_\Phi) \iff \exists$ finite derivation / finite proof-tree of c (in Φ)

<u>Moral</u>. Whenever we define something as finitary provability via a set of rules, we are giving $lfp(F_\Phi)$

<u>Induction</u> $F_\Phi(T) \subseteq T \implies lfp(F_\Phi) \subseteq T$

Think about T has a property on judgments, then induction states:

- To conclude that all provable judgments have property T
  ($lfp(F_\Phi) \subseteq T$)

  show that:

  For any rule $(A, c) \in \Phi$,

  $$\underbrace{A \subseteq T}_{\text{all premises satisfy } T} \implies \underbrace{c \in T}_{\text{conclusion satisfies } T} \qquad \left(F_\Phi(T) \subseteq T \right)$$

This is the usual induction on derivation trees

Ex. $\mathcal{U} = \{ \langle c, s\rangle \Downarrow s' \mid c \in Com,\ s, s' \in States \}$

Φ = rules of operational semantics

$lfp(F_\Phi) = \{ \langle c, s\rangle \Downarrow s' \mid \langle c, s\rangle \Downarrow s' \text{ is derivable} \}$

$\approx$ set of commands c that on initial state s, terminates on state s'.

In practice, when we write $\langle c, s\rangle \Downarrow s'$ we usually mean provable $\langle c, s\rangle \Downarrow s'$, i.e. $\langle c, s\rangle \Downarrow s'$ ranges over $lfp(F_\Phi)$.

Claim (Termination). If $\langle c, s\rangle \Downarrow s'$, then $\underbrace{(c, s) \to^* (skip, s')}_{\text{defined by a } \Phi' \ldots}$

Proof. By rule-induction / induction on $\langle c, s\rangle \Downarrow s'$. ...

...

Formally, we need to show

$$\underbrace{\text{If } \langle c,s\rangle \Downarrow s' \text{ is provable}}_{\forall\, \underbrace{\langle c,s\rangle \Downarrow s'}_{j} \,\in\, lfp(F_{\mathbb{B}})}, \quad \underbrace{\text{Then } (c,s) \to^* (skip, s')}_{j \,\in\, \underbrace{\{\langle c,s\rangle \Downarrow s' \mid (c,s) \to^* (skip,s')\}}_{T}}$$

$$\underbrace{\forall\, j \in lfp(F_{\mathbb{B}}) \implies j \in T}_{lfp(F_{\mathbb{B}}) \subseteq T}$$

We do that by induction:

$$F_{\mathbb{B}}(T) \subseteq T$$

Ex. (Syntax). Recall the syntax of arithmetic expressions

$$e ::= c_n \mid e + e$$

This is an inductive definition.

We are inductively defining a set $\mathcal{E}$ using rules

$$\frac{}{c_n \in \mathcal{E}} \qquad \frac{e_1 \in \mathcal{E} \qquad e_2 \in \mathcal{E}}{e_1 + e_2 \in \mathcal{E}}$$

This is an inference system Φ

Judgments: e (or e exp)

Rules $(\emptyset, c_n)$, $(\{e_1, e_2\}, e_1 + e_2)$

Then $\mathcal{E} = lfp(F_\Phi)$

Induction on syntax / Structural induction

$$\frac{(\forall n)\ c_n \in P \qquad \forall e_1, e_2.\ P(e_1) \,\&\, P(e_2) \Longrightarrow P(e_1 + e_2)}{\forall e \in \mathcal{E}.\ P(e)}$$

For $P \subseteq \mathcal{E} = \mathrm{lfp}\,(F_\Phi)$, we see that

- $\forall e \in \mathcal{E}.\ P(e)$ means $\mathrm{lfp}\,(F_\Phi) \subseteq P$
- Hypothesis means $F_\Phi(P) \subseteq P$

E.g. $P = \{ e \in \mathcal{E} \mid [\![e]\!] \geq 0 \}$

The main inductive property we are interested in is termination

$\langle c, s\rangle \Downarrow s'$

$t \Downarrow v$ $\longleftarrow$ $\left\{ \begin{array}{l} t ::= x \mid \lambda x.t \mid t\,t \\ v ::= x \mid \lambda x.t \\ \dfrac{}{v \Downarrow v} \qquad \dfrac{t \Downarrow \lambda x.t' \quad s \Downarrow v' \quad t'[v'/x] \Downarrow v}{t\,s \Downarrow v} \end{array} \right.$

$\vdots$

Correctness requires to deal with divergence, too. How to do that?

Small-step : $\langle c, s\rangle \Uparrow$:ff $\underbrace{\neg \exists}_{\text{negation}} n \geq 0, s'. \ \langle c, s\rangle \longrightarrow^{n} \langle \text{skip}, s'\rangle$

Non-constructive

Big-step : ??? Divergence seems beyond the scope of big-step semantics

Solution

Coinductive reasoning

- Dual to induction

Induction	Coinduction
finitary constructions	infinitary objects
E.g. list (A)	E.g. stream (A)

- Coinduction gives a "constructive" account of infinitary behaviours
  ↳ Bisimulation in concurrency theory

Inductive Set

- Least set constructed via rules.
- Everything in the set must be the result of finite construction (finite derivation tree)

Coinductive Set

- Largest set consistent with rules
- Elements in the set must be the result of a possibly infinite derivation
- Something is in the set if there is no finitary refutation for that

Given an inference system Φ,

$gfp(F_\Phi)$

contains all $c \in \mathcal{U}$ s.t. $\exists (A, c) \in \Phi$ and $A \subseteq gfp(F_\Phi)$ } This clause is circular

$$\frac{a_1 \quad \cdots \quad a_n}{c}$$

Coinduction Proof Principle

$$T \subseteq F_\Phi(T) \implies T \subseteq gfp(F_\Phi)$$

To prove that T is contained in the coinductively defined set $gfp(F_\Phi)$, show that $\forall c \in T.\ \exists (A, c) \in \Phi.\ A \subseteq T$

Example

Given an TS $(\mathcal{S}, \to)$, define the set $\Uparrow$ as the largest set s.t

$s \in \Uparrow$ implies $\exists s'.\ s \to s'$ & $s' \in \Uparrow$

$$\frac{s \to s' \qquad s' \Uparrow}{s \Uparrow}$$

Formally :

$\mathcal{U} = \mathcal{S}$

$\Phi = \{ (\{s\}, s') \mid s \to s' \}$

Then

$F_\Phi(A) = \{ s' \mid \exists s.\ s \to s' \ \&\ s \in A \}$

Hence, $T \subseteq F_{\Uparrow}(T)$ means

$$\forall s \in T.\ \exists s'.\ s' \to s \ \&\ s' \in T$$

Therefore $\Uparrow = \mathrm{gfp}(F_{\Uparrow})$

<u>Ex.</u> Consider the TS of IMP. Show that

$$\langle \underbrace{\text{while true do skip}}_{w}, s\rangle \in \Uparrow$$

Intuition: we build an infinite proof of $\langle w, s\rangle \Uparrow$.

$$\dfrac{\langle w,s\rangle \to \langle \text{skip}; w, s\rangle \qquad \dfrac{\langle \text{skip}; w, s\rangle \to \langle w,s\rangle \qquad \langle w,s\rangle \Uparrow}{\langle \text{skip}; w,s\rangle \Uparrow}}{\langle w,s\rangle \Uparrow}$$

Formally, we need to find T s.t.

1. $\langle w, s\rangle \in T$
2. $T \subseteq F_{\Phi}(T)$

<u>Guess 1</u>. $T = \{ \langle w, s \rangle \}$

Stack because $\langle w, s\rangle \to \langle skip; w, s\rangle$

but $\langle skip; w, s \rangle \notin T$

<u>Guess 2</u>. $T = \{ \langle w, s\rangle, \langle skip; w, s \rangle \}$

Do we have $F_{\Phi}(T) \subseteq T$?

<u>Exercise</u>