Reasoning on equivalence of programs

We will follow notes available online by:
- Luke Ong (Oxford)
- Roberto Amadio (IRIF)

Lecture notes by L. Ong: Section 5 (and 6)
Operational methods in semantics by R. Amadio: Chapter 8 (weak reduction strategies) and 9 (simulation).

Equivalence on programs

A notion of equivalence among programs should be natural and usable.

- Contextual equivalence is natural.
- It can be characterized as a certain simulation which is easier to reason about.

Contextual equivalence

Write $M \Downarrow$ and say that $M$ converges if $\exists V \ M \Downarrow V$

We observe the termination of the term placed in a closing context, i.e., contexts $C$ such that $C[M]$ and $C[N]$ are closed terms

$M \leq_{C} N$ if for all closing $C$ ($C[M] \Downarrow$ implies $C[N] \Downarrow$)

Contextual equivalence is derived by defining:

$M =_{C} N$ if $M \leq_{C} N$ and $N \leq_{C} M$

Simulation

Definition 185 (simulation): We say that a binary relation on closed terms $S$ is a simulation if whenever $(M, N) \in S$ we have: (1) If $M \Downarrow$ then $N \Downarrow$ and (2) for all $P$ closed $(MP, NP) \in S$. We shall also use the infix notation $M \leq_{S} N$ for $(M, N) \in S$. We define $\leq_{S}$ as the largest simulation.

(using that the set of binary relations is a complete lattice under set inclusion:

$\leq_{S}$ is the largest fixed point of the following function on binary relations

$f(S) = \{(M, N) \mid M \Downarrow$ implies $N \Downarrow, \forall P$ closed $(MP, NP) \in S\}$

This is a CO-INDUCTIVE DEFINITION

Induction and Co-induction

we make a pause to understand (co-)inductive definitions and the (co-)inductive method
Inductively generated sets

- To define a set $S$ "inductively", we need
  - **Basis**: Specify one or more elements that are in $S$.
  - **Induction Rule**: Give one or more rules telling how to construct a new element from an existing element in $S$.
  - **Closure**: No other elements are in $S$.

Example: the following rules inductively define which subset of $\mathbb{Z}$?

- **Basis**: $3 \in S$
- **Induction rule**: $x \in S$ \& $x \in \mathbb{Z}$ implies $x+4 \in S$

Without closure requirement, lots of sets would satisfy this def. For example, $\mathbb{Z}$ works since $3 \in \mathbb{Z}$ and $x+4 \in \mathbb{Z}$.

Termination (inductive def.)

\[
\begin{align*}
P & \quad \text{Normal form} \\
\downarrow & \\
\quad & \quad \quad \downarrow \\
\vdots & \\
\quad & \quad \quad \quad \downarrow \\
P & \quad P' & P' & P \\
\downarrow & \\
\end{align*}
\]

The smallest set of elements in $S$ that is closed under these rules; i.e., the smallest subset $T \subseteq S$ such that:

- All normal forms are in $T$.
- If there is a step $P \rightarrow P'$ for some $P' \in T$, then also $P \in T$.

Non-termination (co-inductive def.)

\[
\begin{align*}
P & \quad P' \\
\downarrow & \\
\quad & \quad \uparrow \\
P & \quad P' \\
\downarrow & \\
\end{align*}
\]

The largest subset $D \subseteq S$ such that if $P \in D$ then there is $P' \in D$ such that $P \rightarrow P'$

ie, each element in $D$ is the conclusion of a rule whose premises also belongs to $D$.

Start with the set $S$ of all elements. Then repeatedly remove $P$ from the set if $P$ has no reduction step.

In which sense rules define a set?

Consider a set of rule instances of the form

\[
X_1, X_2, \ldots, X_n \quad \text{S set of judgments}
\]

Rules define a set operator

\[
F(B) = \{ X \mid \{X_1, X_2, \ldots, X_n\} \subseteq B \text{ and } X_1, X_2, \ldots, X_n \text{ is a rule instance} \}
\]

Ex Question: Is true that $F$ is monotone?

A set operator $F$ is monotone if $B \subseteq C$ implies $F(B) \subseteq F(C)$.

In which sense $F$ defines a set?

Desirable properties of the set $A \subseteq S$ defined by $F$:

- $A$ is $F$-closed iff $F(A) \subseteq A$.
  - Every element that the rules say should be in $A$ to actually be in $A$.

- $A$ is $F$-consistent iff $A \subseteq F(A)$.
  - Every element of $A$ is the result of applying a rule, all elements that cannot be inferred from $A$ are not in $A$.

The set $A$ is

- Closed: no new judgments can be inferred from $A$.
- Consistent: all judgments that cannot be inferred from $A$ are not in $A$.

In which sense $F$ defines a set?

Desirable properties of the set $A \subseteq S$ defined by $F$:

- $A$ is $F$-closed iff $F(A) \subseteq A$.
  - Every element that the rules say should be in $A$ to actually be in $A$.

- $A$ is $F$-consistent iff $A \subseteq F(A)$.
  - Every element of $A$ is the result of applying a rule, all elements that cannot be inferred from $A$ are not in $A$.

- If both hold, $A$ is a fixed point.
- Does $F$ actually have a fixed point?
- Is the fixed point unique?
Non-termination (co-inductive def.)

Start with the set \( S \) of all elements. Then repeatedly remove \( P \) from the set if \( P \) has no reduction step.

The largest subset \( D \subseteq S \) such that if \( P \in D \) then there is \( P' \in D \) such that \( P \rightarrow P' \)

ie, each element in the closure is the conclusion of a rule whose premises also belongs to the closure.

Simple example (on a finite set)

Simple Finitary Example (co-inductive definition) Let \((S, \rightarrow)\) be a set and \(\rightarrow \subseteq S \times S\) a transition relation. Define \(D\) as the greatest subset of \(S\) such that if \(s \in D\) then \(\exists s' \rightarrow s\) and \(s' \in D\). We take as complete lattice the parts of \(S\) ordered by inclusion.

The monotonic function \(f\) associated with the definition is for \(X \subseteq S\):

\[
f(X) = \{ s \in X \mid \exists s' \rightarrow s \} .
\]

suppose \(S = \{1, 2, 3, 4\}\) with :

\[
\begin{align*}
1 & \rightarrow 2 \\
1 & \rightarrow 3 \\
1 & \rightarrow 4 \\
3 & \rightarrow 1 \\
4 & \rightarrow 4.
\end{align*}
\]

The operator \(f\) has both a least fixed point and a greatest fixed point, which are the smallest closed set and the largest consistent set.

What are they?

Some more examples

Lists over alphabet A

Consider the rules

\[
\begin{align*}
\text{nil} \in \mathcal{L} \\
\ell \in \mathcal{L} \\
a \in A
\end{align*}
\]

\( \text{cons}(\ell, a) \in \mathcal{L} \)

• Is there a smaller set closed under these rules? Is finite?

• Is there a larger set consistent with these rules?

Lists over alphabet A

Consider the rules

\[
\begin{align*}
\text{nil} \in \mathcal{L} \\
\ell \in \mathcal{L} \\
a \in A
\end{align*}
\]

\( \text{cons}(\ell, a) \in \mathcal{L} \)

The set (inductively) generated by these rules, i.e., the smallest set closed under these rules:

finite lists

Inductive proof technique for lists: Let \( P \) be a predicate (a property) on lists. To prove that \( P \) holds on all lists, prove that

- \( \text{nil} \in P \);
- \( \ell \in P \) implies \( \text{cons}(\ell, a) \in P \), for all \( a \in A \).

What is the largest set consistent with these rules?

i.e., the largest \( \mathcal{A} \subseteq \mathcal{F}(\mathcal{A}) \)

“all element that cannot be inferred from \( A \) are not in \( A \)”
Co-induction is not (just) black magic

Lattices

A poset \((P, \leq)\) is a lattice if for any two \(x, y \in P\) the set \(\{x, y\}\) has greatest lower bound and least upper bound.

Definition

A poset \((P, \leq)\) is a complete lattice if for every \(X \subseteq P\) the bounds \(\bigvee X\) and \(\bigwedge X\) exist in \(P\).

Complete Lattices

- If \((P, \sqsubseteq)\) is a complete lattice then \(\operatorname{glb} / \operatorname{lub}\) of \(P\) exist in \(P\),
  \[ \bigcap P = \bot = \bigcup \emptyset \quad \bigcup P = \top = \bigcap \emptyset. \]
- Every finite lattice is complete.

For every set \(X\), the poset \((P(X), \subseteq)\) is a complete lattice.

Fixed points

A monotonic function \(f\) on a partial order \(L\) is a function respecting the order:

\[ \forall x, y \ (x \leq y \implies f(x) \leq f(y)) \]

Let \((P, \leq)\) be a poset and let \(f\) be endofunction over \(P\).

- \(\text{Fix}(f) = \{x \mid f(x) = x\}\) fixed points
- \(\text{Pre}(f) = \{x \mid f(x) \leq x\}\) pre-fixed points
- \(\text{Post}(f) = \{x \mid x \leq f(x)\}\) post-fixed points

Notation:

- \(\mu f\) least fixed point of \(f\)
- \(\nu f\) greatest fixed point of \(f\)

Under which conditions a function has least/greatest fp?
Tarski-Knaster Theorem

Let $f : L \to L$ be a monotone function on a complete lattice. Then $f$ has a greatest and a least fixed point, expressed by:

\[
\sup\{x \mid x \leq f(x)\} \quad \text{and} \quad \inf\{x \mid f(x) \leq x\}.
\]

Proof of (i).

Let $a = \bigsqcup Post(f)$. We have to show:

1. $\forall x \in \text{Fix}(f), x \sqsubseteq a$
2. $f(a) = a$

Suppose $x = f(x)$.

(a) $x \sqsubseteq f(x)$ by weakening

(b) $x \sqsubseteq a$ by def. of upper bound

What we proved?

Given a set of rules, pairs $(B, x)$, where $x \in U$ is the conclusion of the rule and $B \subseteq U$ is the set of its premises

The operator $F$ is defined by:

\[ F(A) = \{x \in U \mid \exists B \subseteq A \text{ such that } (B, x) \text{ is a rule instance}\} \]

$F(A)$ is the set of judgements that can be inferred in one step from the judgements in $A$ by using the rules.

$A$ is

- closed if $F(A) \subseteq A$
- consistent if $A \subseteq F(A)$

The rules operator has both a least fixed point and a greatest fixed point, which are

- the smallest closed set
- the largest consistent set

The inductive and co-inductive interpretation of rules:

\[
\begin{align*}
\text{Inductive interpretation:} & \quad \text{if } A \subseteq F(A) \Rightarrow A \subseteq F(A) \\
\text{Co-inductive interpretation:} & \quad \text{if } A \subseteq F(A) \Rightarrow A \subseteq F(A)
\end{align*}
\]

The operator $F$ has both a least fixed point and a greatest fixed point, which are

- the smallest closed set
- the largest consistent set

What are they?

And if we remove the first rule?
Finite list (inductive method)

\[\begin{align*}
\text{nil} & \in \mathcal{L} \\
\ell \in \mathcal{L} \quad \alpha \in A \\
\text{cons}(\alpha, \ell) & \in \mathcal{L}
\end{align*}\]

\[\mathcal{F}(S) \overset{\text{def}}{=} \{\text{nil}\} \cup \{\text{cons}(\alpha, s) : \alpha \in A, s \in S\}\]

Proving \(\mathcal{F}(\mathcal{P}) \subseteq \mathcal{P}\) requires proving
- \(\text{nil} \in \mathcal{P}\);
- \(\ell \in \mathcal{P}\) implies \(\text{cons}(\alpha, \ell) \in \mathcal{P}\), for all \(\alpha \in A\).

This is the same as the familiar induction technique for lists.

EX Lists (coinductive method)

\[\begin{align*}
\text{nil} & \in \mathcal{L} \\
\ell \in \mathcal{L} \quad \alpha \in A \\
\text{cons}(\alpha, \ell) & \in \mathcal{L}
\end{align*}\]

\[\mathcal{F}(S) \overset{\text{def}}{=} \{\text{nil}\} \cup \{\text{cons}(\alpha, s) : \alpha \in A, s \in S\}\]

Show that the infinite list \(s_1 = b c b c b \ldots\) is in the set coinductively defined by the two rules above, assuming \(c, b \in A\).

1. Let us try \(T = \{s_1\}\) and check that \(T\) is consistent with the rules, i.e., \(T \subseteq \mathcal{F}(T)\).
2. We strengthen the hypothesis. Take \(s_2 = b c b \ldots\).
   - Let us try \(T = \{s_1, s_2\}\), and check that \(T \subseteq \mathcal{F}(T)\).

Therefore, \(\{s_1, s_2\} \subseteq \text{gfp } \mathcal{F}\) for a given \(T\), if for all \(s \in T\) there is a rule \((s, x) \in \mathcal{R}\) with \(S \subseteq T\), then \(T \subseteq \text{gfp } \mathcal{F}\).

Constructing the fixpoint

A function \(\mathcal{F}\) on a complete lattice is EX.

- **continuous** if for all sequences \(a_0, a_1, \ldots\) of increasing points in the lattice (i.e., \(a_i \leq a_{i+1}\), for \(i \geq 0\)) we have \(\mathcal{F}(\bigcup_{i} a_i) = \bigcup_{i} \mathcal{F}(a_i)\).
- **cocontinuous** if for all sequences \(a_0, a_1, \ldots\) of decreasing points in the lattice (i.e., \(a_i \geq a_{i+1}\), for \(i \geq 0\)) we have \(\mathcal{F}(\bigcap_{i} a_i) = \bigcap_{i} \mathcal{F}(a_i)\).

**Theorem 3.85 (Continuity/Cocontinuity Theorem)**: Let \(\mathcal{F}\) be an endofunction on a complete lattice, in which \(\bot\) and \(\top\) are the bottom and top elements. If \(\mathcal{F}\) is continuous, then
- \(\mathcal{F}(\bot) = F_{\infty}(\bot)\).
- If \(\mathcal{F}\) is cocontinuous, then
  \[\mathcal{F}(\top) = F_{\infty}(\top)\].

The sequence \(F_{\infty}(\bot), F_{\infty}(\bot), \ldots\) is increasing, whereas \(F_{\infty}(\top), F_{\infty}(\top), \ldots\) is decreasing.
Ex 1. Co-continuity

Ex
i. Prove that if $F$ is co-continuous (or continuous), then it is also monotone.
(Hint: take $x \geq y$, and the sequence $x, y, y, y, \ldots$)

ii. Prove co-continuity Theorem

Point ii is more important

Simulation

Back where we started... (to be continued next week)

Homework

Ex 2 Consider the strings over an alphabet $\Sigma$

- Consider the set $S$ co-inductively defined by the following rules (where $\Sigma$ is an alphabet)

- Consider the relation on elements of $S$ co-inductively defined by the rules (where $\Sigma$ is an alphabet)

EX. Prove that $\text{aaaaa} \preceq \text{baaaa}$... (the two strings are infinite)