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).

1

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.

2

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, ie:

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:*

$M \approx_C N$ *if* $M \leq_C N$ *and* $N \leq_C M$

3

Motivating example: 1+1 = 2 ?

$$one \stackrel{\text{def}}{=} \lambda x.\, \lambda y.\, x\, y$$
$$two \stackrel{\text{def}}{=} \lambda x.\, \lambda y.\, x\, (x\, y)$$
$$succ \stackrel{\text{def}}{=} \lambda n.\, \lambda x.\, \lambda y.\, x\, (n\, x\, y)$$

Is it the case that *succ one* $\Downarrow$ *two* holds? (in weak CbV?)

1. Are the terms *succ one* and *two* contextually equivalent?
2. Does the following statement make sense?

Think of the Church numeral $\underline{n}$ as the procedure that takes a function-input and an argument-input, and applies the function n-times to the argument.

4

Bisimulation

where the idea comes from?

The Reference:

Robin Milner, *Communication and Concurrency*, Prentice Hall, 1989.

5

when two machines have the same behaviour?

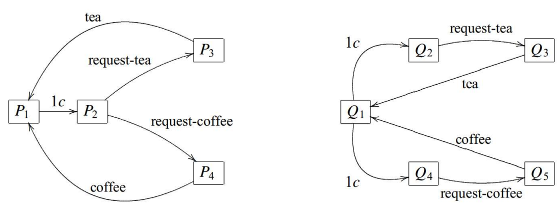


Fig. 1.5 Two vending machines.

Intuitively :
- when we do something with one machine, we must be able to do the same with the other
- the same is again true, on the two states that the machines evolve to.

6

Definition (bisimulation) A relation $\mathcal{R}$ on processes is a **bisimulation** if whenever $P \mathrel{\mathcal{R}} Q$:

1. if $P \xrightarrow{\mu} P'$, then there is Q' such that $Q \xrightarrow{\mu} Q'$ and $P' \mathrel{\mathcal{R}} Q'$.
2. if $Q \xrightarrow{\mu} Q'$, then there is P' such that $P \xrightarrow{\mu} P'$ and $P' \mathrel{\mathcal{R}} Q'$.

P and Q are **bisimilar**, written $P \sim Q$, if $P \mathrel{\mathcal{R}} Q$, for some bisimulation $\mathcal{R}$.

The bisimulation diagram:

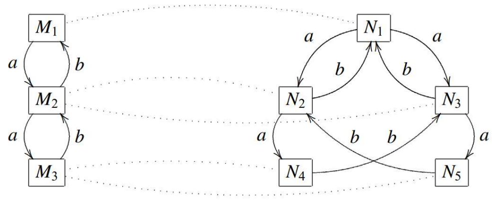
$$\begin{array}{ccc} P & \mathcal{R} & Q \\ \mu \downarrow & & \mu \downarrow \\ P' & \mathcal{R} & Q' \end{array}$$

7

Definition (bisimulation) A relation $\mathcal{R}$ on processes is a **bisimulation** if whenever $P \mathrel{\mathcal{R}} Q$:

1. if $P \xrightarrow{\mu} P'$, then there is Q' such that $Q \xrightarrow{\mu} Q'$ and $P' \mathrel{\mathcal{R}} Q'$.
2. if $Q \xrightarrow{\mu} Q'$, then there is P' such that $P \xrightarrow{\mu} P'$ and $P' \mathrel{\mathcal{R}} Q'$.

P and Q are **bisimilar**, written $P \sim Q$, if $P \mathrel{\mathcal{R}} Q$, for some bisimulation $\mathcal{R}$.



$\{(M_1, N_1), (M_2, N_2), (M_2, N_3), (M_3, N_4), (M_3, N_5)\}$

8

Idea: observing the behaviour of a function

Given a closed term s, the only experiment of depth 1 we can do is to evaluate s and see if it converges to some abstraction (weak head normal form) $\lambda x.p_1$. If it does so, we can continue the experiment to depth 2 by supplying a term t_1 as input to $\lambda x.p_1$, and so on. Note that what the experimenter can observe at each stage is only the *fact* of convergence, not which term lies under the abstraction. We can picture matters thus:

Stage 1 of experiment: $s \Downarrow \lambda x.p_1$;

Stage 2 of experiment: $p_1[t_1/x] \Downarrow \ldots$

9

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* $M\ S\ N$ *for* $(M, N) \in S$. *We define* $\leq_S$ *as the largest simulation.*

10

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* $M\ S\ N$ *for* $(M, N) \in S$. *We define* $\leq_S$ *as the largest simulation.*

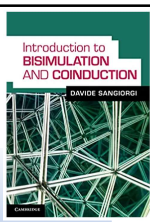
(using that the set of binary relations is a complete lattice under set inclusion:)

$\leq_S$ is the largest fixed point of the following function on binary relations

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

This is a CO-INDUCTIVE DEFINITION

11



Induction and Co-induction

we make a pause to understand

(co-)inductive definitions and the (co-)inductive method

12

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 Z ?

- Basis: 3 ∈ S
- Induction rule: $\dfrac{x \in S \quad \& \quad x \in Z}{x+4 \in S}$

- inductive definition of S = {3,7,11,15,19,23,…}
- **Without closure requirement**, lots of sets would satisfy this def. For example, Z works since 3∈Z and x+4∈Z.

13

Termination (inductive def.)

$$\frac{P \quad \text{Normal form}}{P\downarrow} \qquad \frac{P \longrightarrow P' \qquad P'\downarrow}{P\downarrow}$$

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* $P \to P'$ for some $P' \in T$, then also $P \in T$.

14

Non-termination (co-inductive def.)

$$\frac{P \longrightarrow P' \qquad P'\uparrow}{P\uparrow}$$

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

15

In which sense rules define a set?

considered a set of *rule instances* of the form

$$\frac{X_1 \; X_2 \; \ldots \; X_n}{X},$$

where X and the X_i are members of some set S.

S set of judgments

Rules define a set operator

$$\mathsf{F}(B) \triangleq \{X \mid \{X_1, X_2, \ldots, X_n\} \subseteq B \text{ and } \frac{X_1 \; X_2 \; \ldots \; X_n}{X} \text{ is a rule instance}\}.$$

Ex Question: Is true that F is monotone?

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

16

In which sense F defines a set?

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

- A is F-*closed if*: $\mathsf{F}(A) \subseteq A$.
  Every element that the rules say should be in A to actually be in A.
- A is F-*consistent if*: $A \subseteq \mathsf{F}(A)$.
  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*.

17

In which sense F defines a set?

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

- A is F-*closed if*: $\mathsf{F}(A) \subseteq A$.
  Every element that the rules say should be in A to actually be in A.
- A is F-*consistent if*: $A \subseteq \mathsf{F}(A)$.
  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?

18

Non-termination (co-inductive def.)

$$\frac{P \longrightarrow P' \qquad P' \upharpoonright}{P \upharpoonright}$$

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

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

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

19

Simple example (on a finite set)

Simple Finitary Example (**co-inductive definition**) *Let* $(S, \to)$ *be a set and* $\to \subseteq S \times S$ *a transition relation. Define* D *as the greatest subset of* S *such that if* $s \in D$ *then:* $\exists s'\ s \to s'$ *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* $X \subseteq S$*:*

$$f(X) = \{s \in X \mid \exists s'\ s \to s'\} \ .$$

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

- 1 -> 2 *1-> 3* *1-> 4*
- 3 -> 1
- 4 -> 4.

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?

20

Some more examples

21

Lists over alphabet A

Consider the rules

$$\frac{}{\texttt{nil} \in \mathcal{L}} \qquad \frac{\ell \in \mathcal{L} \qquad a \in A}{\texttt{cons}(a, \ell) \in \mathcal{L}}$$

- Is there a smaller set closed under these rules? Is finite?
- Is there a larger set consistent with these rules?

22

Lists over alphabet A

Consider the rules

$$\frac{}{\texttt{nil} \in \mathcal{L}} \qquad \frac{\ell \in \mathcal{L} \qquad a \in A}{\texttt{cons}(a, \ell) \in \mathcal{L}}$$

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

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

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

23

Lists over alphabet A

Consider the rules

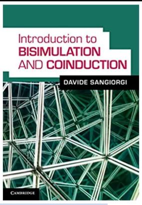
$$\frac{}{\texttt{nil} \in \mathcal{L}} \qquad \frac{\ell \in \mathcal{L} \qquad a \in A}{\texttt{cons}(a, \ell) \in \mathcal{L}}$$

What is the largest set consistent with these rules ?

i.e. the largest $A \subseteq F(A)$
"all element that cannot be inferred from A are not in A"

24

Slides by Giovanni Bernardi (stages possibles!)



Induction, co-induction, and fixed points

Co-induction is not (just) black magic

25

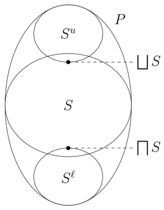
memo

A relation $\mathcal{R} \subseteq X \times X$ is a

preorder if it is reflexive and transitive

partial order if it is reflexive, antisymmetric, and transitive

equivalence if is reflexive, symmetric, and transitive



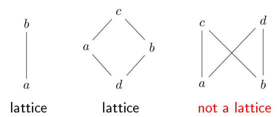
Sup (S) = least upper bound

Inf (S) = greatest lower bound

26

Lattices

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



Definition

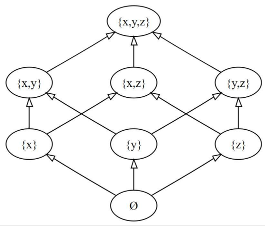
A poset $\langle P, \leq \rangle$ is a *complete lattice* if for every $X \subseteq P$ the bounds $\bigvee X$ and $\bigwedge X$ exist in P.

27

Complete Lattices

- If $\langle P, \sqsubseteq \rangle$ is a complete lattice then glb/lub of P exist in P,
  $\bigsqcap P = \bot = \bigsqcup \emptyset \qquad \bigsqcup P = \top = \bigsqcap \emptyset.$
- Every finite lattice is complete.

For every set X, the poset $\langle \mathcal{P}(X), \subseteq \rangle$ is a complete lattice.



28

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

$$\forall x, y \ (\ x \leq y \ implies \ f(x) \leq f(y) \ )$$

29

Fixed points

Let $\langle P, \leq \rangle$ be a poset and let f be endofunction over P. $f : P \to P$

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

notation:

- μf least fixed point of f
- νf greatest fixed point of f

Under which conditions a function has least/greatest fp ?

30

Tarski-Knaster

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

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

31

Theorem

Let $\langle L, \sqsubseteq \rangle$ be a complete lattice and $f : L \to L$ be a monotone function.

(i) $\nu f = \bigsqcup\{\, x \mid x \sqsubseteq f(x) \,\}$, *coinduction*

(ii) $\mu f = \bigsqcap\{\, x \mid f(x) \sqsubseteq x \,\}$. induction

Proof of (i).

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

(a) $\forall x \in Fix(f).\, x \sqsubseteq a$

(b) $f(a) = a$

(a)

Suppose $x = f(x)$.

$x \sqsubseteq f(x)$ by weakening

$x \sqsubseteq a$ by def. of upper bound

32

Recall $a = \bigsqcup Post(f) = \bigsqcup\{\, x \mid x \sqsubseteq f(x) \,\}$.

(b) We obtain $f(a) = a$ by anti-simmetry if we show

1. $a \sqsubseteq f(a)$

$\forall x \in Post(f).\, x \sqsubseteq a$	by def. upper bound
$\forall x \in Post(f).\, f(x) \sqsubseteq f(a)$	by monotonicity
$\forall x \in Post(f).\, x \sqsubseteq f(a)$	by transitivity
$f(a)$ upper bound of $Post(f)$	
$a \sqsubseteq f(a)$	by def. least upper bound

2. $f(a) \sqsubseteq a$

$a \sqsubseteq f(a)$	by previous point
$f(a) \sqsubseteq f(f(a))$	by monotonicity of f
$f(a) \in Post(f)$	by def. of $Post(f)$
$f(a) \sqsubseteq a$	by def. of upper bound

□

33

What we proved?

Given a set of *rule, ie pairs* (B, x), where
x ∈ *U* is the conclusion of the rule and *B* ⊆ *U* is the set of its premises

The operator F is defined by
F(A) = {x ∈ U | ∃B ⊆ A such that *(B, x) is a rule instance}*

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

A is $\quad$ *closed* if $F(A) \subseteq A$
$\quad\quad\;$ *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** and the **largest consistent set**:

$$lfp(F) = \bigcap\{A \mid F(A) \subseteq A\};$$
$$gfp(F) = \bigcup\{A \mid A \subseteq F(A)\}.$$

34

Inductive and co-inductive interpretation of rules

$$lfp(F) = \bigcap\{A \mid F(A) \subseteq A\};$$
$$gfp(F) = \bigcup\{A \mid A \subseteq F(A)\}.$$

- **Induction principle**: to prove that all judgments in the inductive interpretation belong to a set A, show that A is F-closed.
- **Coinduction principle**: to prove that all judgments in a set A belong to the coinductive interpretation, show that A is F-consistent.

$$A \subseteq F(A) \Longrightarrow A \in \{B \mid B \subseteq F(B)\}$$
$$\Longrightarrow A \subseteq \bigcup\{B \mid B \subseteq F(B)\} = gfp(F).$$

35

Non-termination (co-inductive def.)

$$\frac{P \to P' \qquad P' \uparrow}{P \uparrow}$$

The largest subset D ⊆ *S* such that (**) if *P* ∈ *D* then there is *P'* ∈ *D* such that *P* → *P'*

Suppose that program Ω reduces to itself, that is Ω -> Ω .
To see that Ω contained in D,
Consider set X = {Ω } .
Since X satisfies (**), then X⊆D, as D is the greatest such set.
Hence Ω is a member of D.

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

36

Finite list (inductive method)

$$\frac{}{\texttt{nil} \in \mathcal{L}} \qquad \frac{\ell \in \mathcal{L} \quad a \in A}{\texttt{cons}(a,\ell) \in \mathcal{L}}$$

$$\mathcal{F}(S) \triangleq \{\texttt{nil}\} \cup \{\texttt{cons}(a,s) \ : \ a \in A, s \in S\}$$

Proving $\mathcal{F}(\mathcal{P}) \subseteq \mathcal{P}$ requires proving

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

This is the same as the familiar induction technique for lists

37

Lists (inductive method)

$$\frac{}{\texttt{nil} \in \mathcal{L}} \qquad \frac{\ell \in \mathcal{L} \quad a \in A}{\texttt{cons}(a,\ell) \in \mathcal{L}}$$

$$\mathcal{F}(S) \triangleq \{\texttt{nil}\} \cup \{\texttt{cons}(a,s) \ : \ a \in A, s \in S\}$$

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

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

38

EX Lists (coinductive method)

$$\frac{}{\texttt{nil} \in \mathcal{L}} \qquad \frac{\ell \in \mathcal{L} \quad a \in A}{\texttt{cons}(a,\ell) \in \mathcal{L}}$$

$$\mathcal{F}(S) \triangleq \{\texttt{nil}\} \cup \{\texttt{cons}(a,s) \ : \ a \in A, s \in S\}$$

Show that the infinite list $s1$ = **c b c b c …**
is in the set coinductively defined by the two rules above, assuming ***c, b*** ∈ *A*

1. Let us try *T* = {*s*1} and check that *T* is consistent with the rules, ie T ⊆ F(T)
2. We strengthen the hypothesis. Take s2 = **b c b c b …**
   Let us try *T* = {s_1,s_2}, and check that T ⊆ F(T)

Therefore, {s1,s2} ⊆ gfp F

for a given T,
if for all $x \in T$ *there is a rule* $(S,x) \in \mathcal{R}$ *with* $S \subseteq T$,
then $T \subseteq \texttt{gfp}(\Phi_{\mathcal{R}})$

39

Constructing the fixpoint

40

A function F on a complete lattice is

- *continuous* if for all sequences $\alpha_0, \alpha_1, \ldots$ of increasing points in the lattice (i.e., $\alpha_i \leq \alpha_{i+1}$, for $i \geq 0$) we have $F(\bigcup_i \alpha_i) = \bigcup_i F(\alpha_i)$;
- *cocontinuous* if for all sequences $\alpha_0, \alpha_1, \ldots$ of decreasing points in the lattice (i.e., $\alpha_i \geq \alpha_{i+1}$, for $i \geq 0$) we have $F(\bigcap_i \alpha_i) = \bigcap_i F(\alpha_i)$. □

EX.
If *F* is co-continuous (or continuous), then it is also monotone.
(Hint: take *x* ≥ *y*, and the sequence *x, y, y, y, . . .*)

41

$$F^0(x) \stackrel{\text{def}}{=} x,$$
$$F^{n+1}(x) \stackrel{\text{def}}{=} F(F^n(x)).$$

$$F^{\cup\omega}(x) \stackrel{\text{def}}{=} \bigcup_{n\geq 0} F^n(x),$$
$$F^{\cap\omega}(x) \stackrel{\text{def}}{=} \bigcap_{n\geq 0} F^n(x).$$

Theorem 2.8.5 (Continuity/Cocontinuity Theorem) *Let F be an endofunction on a complete lattice, in which $\bot$ and $\top$ are the bottom and top elements. If F is continuous, then*

$$\texttt{lfp}(F) = F^{\cup\omega}(\bot);$$

if F is cocontinuous, then

$$\texttt{gfp}(F) = F^{\cap\omega}(\top).$$

□

The sequence $F^0(\bot), F^1(\bot), \ldots$ is increasing, whereas $F^0(\top), F^1(\top), \ldots$ is decreasing.

42

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

43

Simulation

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

44

CbN Simulation

We consider weak call-by-name λ *calculus*. We write $\Downarrow$ for $\Downarrow^n$

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* $M\ S\ N$ *for* $(M, N) \in S$. *We define* $\leq_S$ *as the largest simulation.*

(recall 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*

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

CO-INDUCTIVE DEFINITION

45

Ex. CbN Simulation

To prove that $M \leq_S N$ (M, N closed) it suffices to find a relation S which is a simulation and such that $M\ S\ N$.

EX
i. Show that $\leq_S$ is a preorder over Λ ie a reflexive and transitive binary relation

ii. Is the union of two simulations a simulation ?

iii. *If* $M \Downarrow V$ *and* $N \Downarrow V$, M, N *closed, then* $M =_S N$. Prove it.

46

Homework

47

Ex. 1 Consider the strings over an alphabet Σ

- Consider the set S coinductively defined by the following rules (where Σ is an alphabet)

$$\frac{}{\epsilon \in S} \qquad \frac{s \in S \quad \sigma \in \Sigma}{\sigma s \in S}$$

The largest set S such that $\epsilon \in S'$ and that if $\sigma s \in S$, then $s \in S$ (and $\sigma \in \Sigma$).

- Consider the relation on elements of S co-inductively defined by the rules

(where ≤ is th

$$\frac{}{\epsilon \leqslant \epsilon} \qquad \frac{\sigma_1 \leq \sigma_2 \qquad s_1 \leqslant s_2}{\sigma_1 s_1 \leqslant \sigma_2 s_2}$$

$$F(X) = \{(\epsilon, \epsilon)\} \cup \{(\sigma_1 s_1, \sigma_2 s_2) \mid \sigma_1 \leq \sigma_2 \wedge (s_1, s_2) \in X\}$$

EX. Prove that aaaaa$\cdots \leqslant$ baaaa... (the two strings are infinite)

48

Ex. 2 CbN Simulation

To prove that $M \leq_S N$ (M, N closed) it suffices to find a relation S which is a simulation and such that $M \; S \; N$.

EX

i. Show that $\leq_S$ is a preorder over Λ ie a reflexive and transitive binary relation

ii. Is the union of two simulations a simulation ?

iii. *If* $M \Downarrow V$ *and* $N \Downarrow V$, M, N *closed, then* $M =_S N$. Prove it.

49

Inductive and co-inductive methos

50

Induction and co-induction principle

A set *R* of rules on yields a monotone operator

$$\Phi_{\mathcal{R}}(T) = \{x \mid (T', x) \in \mathcal{R} \text{ for some } T' \subseteq T\}$$

$$\text{if } \Phi_{\mathcal{R}}(T) \subseteq T \text{ then } \mathtt{lfp}(\Phi_{\mathcal{R}}) \subseteq T,$$
$$\text{if } T \subseteq \Phi_{\mathcal{R}}(T) \text{ then } T \subseteq \mathtt{gfp}(\Phi_{\mathcal{R}}).$$

51

Induction

A set T being a pre-fixed point of $\Phi_{\mathcal{R}}$ (i.e., the hypothesis $\Phi_{\mathcal{R}}(T) \subseteq T$) means that:

for all rules $(S, x) \in \mathcal{R}$, *if* $S \subseteq T$, *then also* $x \in T$.

The Fixed-point Theorem tells us that the least fixed point is the least pre-fixed point: the set inductively defined by the rules is therefore the smallest set closed.

Let T be a property

for a given T,
if for all rules $(S, x) \in \mathcal{R}, S \subseteq T$ *implies* $x \in T$
then $\mathtt{lfp}(\Phi_{\mathcal{R}}) \subseteq T$.

if we have a property T, and we wish to prove that all elements in the set inductively defined by Φ have the property, we have to show that T is a pre-fixed point of Φ

52

Co-Induction

In the case of coinduction, the hypothesis is that T is a post-fixed of $\Phi_{\mathcal{R}}$

for all $x \in T$, *there is a rule* $(S, x) \in \mathcal{R}$ *with* $S \subseteq T$.

That is, each element of T is conclusion of a rule whose premises are satisfied in T.

for a given T,
if for all $x \in T$ *there is a rule* $(S, x) \in \mathcal{R}$ *with* $S \subseteq T$,
then $T \subseteq \mathtt{gfp}(\Phi_{\mathcal{R}})$

53