Declarative Programming and (Co)Induction

Module 2: inductive and coinductive Prolog

Davide Ancona and Elena Zucca

Università di Genova

PhD Course, DIBRIS, June 26-27, 2014

Part 1
Recursive definitions and fixed points

Induction and coinduction

What induction and coinduction are useful for?

- Induction: definition of and reasoning on sets whose elements can be generated in a finite number of steps
  Natural numbers, finite lists, finite trees
- Coinduction: definition of and reasoning on sets whose elements
  - cannot be generated in a finite number of steps
  - or can be cyclic/defined circularly

  Real numbers, repeating decimals, infinite/circular lists, infinite/circular trees, . . .

Regular coinduction

Useful for defining of and reasoning on finite cyclic entities: graphs, finite automata, context-free grammars, recursive types, repeating decimals, . . .

Recursive definitions (1)

Equation or recursive definition?

Everybody is familiar with algebraic equations

$$x = \frac{1 + x}{2}$$

Even though a bit unusual, the equation above can be also considered as a (recursive) definition.

This is fine, since the equation admits just one solution.

Recursive definitions (2)

Equation or recursive definition?

The following is a recursive definition

```
factorial n = if n > 0 then n * factorial (n-1) else 1
```

but it may be considered an equation as well, with a unique solution

Other examples

```
increment [] = []
increment (x : l) = (x + 1) : increment l

allPosiive [] = True
allPositive (x : l) = x > 0 && allPositive l
```

But here there may be more then one solution ...

Recursive definitions (3)

Equation or recursive definition?

How many solutions does the following equation admit?

$$X = \{0\} \cup X$$

Important observation:

the number of solutions depends on the domain of solutions

Recursive definitions (3)

Equation or recursive definition?

How many solutions does the following equation admit?

$$X = \{0\} \cup X$$

Important observation:

the number of solutions depends on the domain of solutions

- The equation admits the unique solution $\{0\}$ for the power set $\wp(\{0\})$
- The equation admits infinite solutions for the power set of natural numbers $\wp(\mathbb{N})$: all sets $S \in \wp(\mathbb{N})$ s.t. $0 \in S$

Recursive definitions (3)

Equation or recursive definition?

How many solutions does the following equation admit?

$$X = \{0\} \cup X$$

Important observation:

the number of solutions depends on the domain of solutions

- The equation admits the unique solution $\{0\}$ for the power set $\wp(\{0\})$
- The equation admits infinite solutions for the power set of natural numbers $\wp(\mathbb{N})$: all sets $S \in \wp(\mathbb{N})$ s.t. $0 \in S$

However, there exixts a unique solution if we impose some constraint:

- the least solution (inductive definition): $X = \{0\}$
- the greatest solution (coinductive definition): $X = \mathbb{N}$

Recursive definitions, functions and fixed points

Solutions as fixed points

A recursive definition can be easily turned into a function.

For instance $X = \{0\} \cup X$ corresponds to the function $f{:}\wp(\mathbb{N}) \to \wp(\mathbb{N})$ s.t.

$$f(X) = \{0\} \cup X$$

Then X is a solution of our equation iff X is a fixed point of f:

$$f(X) = X$$

In particular:

- $\{0\}$ is the least fixed point of f
- $\mathbb{N}$ is the greatest fixed point of f

Power sets, partial orders and complete lattices (1)

Partial orders

$(\wp(\mathbb{N}), \subseteq)$ is a partial order

- reflexivity: for all $X \in \wp(\mathbb{N})$, $X \subseteq X$
- anti-symmetry: for all $X, Y \in \wp(\mathbb{N})$, $X \subseteq Y$ and $Y \subseteq X$ implies $X = Y$
- transitivity: for all $X, Y, Z \in \wp(\mathbb{N})$, $X \subseteq Y$ and $Y \subseteq Z$ implies $X \subseteq Z$

Supremum (least upper bound) and infimum (greatest lower bound)

Let $S \subseteq \wp(\mathbb{N})$ (S is a set of sets)

- $\sup S = \min\{X \in \wp(\mathbb{N}) \mid Y \subseteq X \text{ for all } Y \in S\}$
- $\inf S = \max\{X \in \wp(\mathbb{N}) \mid X \subseteq Y \text{ for all } Y \in S\}$

Suprema and infima are unique

Power sets, partial orders and complete lattices (2)

Complete lattices

$(\wp(\mathbb{N}), \subseteq)$ is a particular partial order called complete lattice

- every $S \subseteq \wp(\mathbb{N})$ has supremum and infimum

Examples:

- If $S = \{X \in \wp(\mathbb{N}) \mid 0 \in X\}$ then $\sup S = \mathbb{N}$, $\inf S = \{0\}$
- If $S = \{X \in \wp(\mathbb{N}) \mid 0 \notin X\}$ then $\sup S = \mathbb{N} \setminus \{0\}$, $\inf S = \emptyset$
- If $S = \{X \in \wp(\mathbb{N}) \mid X \text{ finite}\}$ then $\sup S = \mathbb{N}$, $\inf S = \emptyset$

Though we will mainly deal with power sets $\wp(U)$ over a given set U, called universe, the results that follow apply to any complete lattice.

Exercise: relation between sup and inf

$\inf S = \sup\{X \mid X \subseteq Y \text{ for all } Y \in S\}$
Proof:

Let $T = \{X \mid X \subseteq Y \text{ for all } Y \in S\}$
$\inf S \subseteq Y$ for all $Y \in S$ (def. of inf)
$\inf S \in T$ (def. of T)
$\inf S \subseteq \sup T$ (def. of sup)
$X \subseteq Y$ for all $X \in T$ and $Y \in S$ (def. of T)
$\sup T \subseteq Y$ for all $Y \in S$ (def. of sup)
$\sup T \subseteq \inf S$ (def. of inf)
$\inf S = \sup T$ (symmetry)

f-closed and f-dense sets

Monotone function $f{:}\wp(U) \to \wp(U)$

For all $X, Y \in \wp(U)$, $X \subseteq Y$ implies $f(X) \subseteq f(Y)$

- $X \in \wp(U)$ is f-closed iff $f(X) \subseteq X$
- $X \in \wp(U)$ is f-dense (or f-justified, or f-consistent) iff $X \subseteq f(X)$
- $X \in \wp(U)$ is a fixed point of f iff $f(X) = X$

X fixed point of f iff X both f-closed and f-dense

Examples

If $f : \wp(\mathbb{N}) \to \wp(\mathbb{N})$ and $f(X) = \{0\} \cup \{x + 2 \mid x \in X\}$ then

- $\mathbb{N}$ is f-closed, but not f-dense
- $\emptyset$ is f-dense, but not f-closed
- $\{2x \mid x \in \mathbb{N}\}$ is a fixed point of f (which is unique in this particular case)

Tarski-Knaster theorem (1)

Lemma

Let $f:\wp(U) \to \wp(U)$ be monotone

1. $\sup\{X \mid X\ f\text{-dense}\}$ is f-dense
2. $\inf\{X \mid X\ f\text{-closed}\}$ is f-closed

Proof of lemma

1. Let $Y = \sup\{X \mid X \subseteq f(X)\}$
   for all X f-dense, $X \subseteq Y$ (def. of sup)
   for all X f-dense, $f(X) \subseteq f(Y)$ (f monotone)
   for all X f-dense, $X \subseteq f(X) \subseteq f(Y)$ (def. of f-dense)
   for all X f-dense, $X \subseteq f(Y)$ (transitivity)
   $Y \subseteq f(Y)$ (def. of sup)
   Y is f-dense (def. f-dense)
2. Obtained from 1 by duality (replacing sup with inf and $\subseteq$ with $\supseteq$)

Tarski-Knaster theorem (2)

Claim

Let $f{:}\wp(U) \to \wp(U)$ be monotone

1. $f(\sup\{X \mid X\ f\text{-dense}\}) = \sup\{X \mid X\ f\text{-dense}\}$
2. $f(\inf\{X \mid X\ f\text{-closed}\}) = \inf\{X \mid X\ f\text{-closed}\}$

Proof of theorem

1. Let $Y = \sup\{X \mid X \subseteq f(X)\}$
   $Y \subseteq f(Y)$ (previous lemma)
   $f(Y) \subseteq f(f(Y))$ (f monotone)
   $f(Y)$ f-dense (def. f-dense)
   $f(Y) \subseteq Y$ (def. sup)
   $f(Y) = Y$ (anti-symmetry)
2. Obtained from 1 by duality

Greatest and least fixed points

Since X fixed point of f implies X both f-closed and f-dense

- $\sup\{X \mid X\ f\text{-dense}\}$ greatest fixed point of f (denoted by gfp f)
- $\inf\{X \mid X\ f\text{-closed}\}$ least fixed point of f (denoted by lfp f)

Kleene fixed point theorem (1)

How can lfp f and gfp f be constructed?

Continuous function $f{:}\wp(U) \to \wp(U)$

- f preserves sup and inf:
  for all $S \subseteq \wp(U)$
  - $f(\sup S) = \sup\{f(X) | X \in S\}$
  - $f(\inf S) = \inf\{f(X) | X \in S\}$

Property

Continuous functions are always monotone.
$X \subseteq Y$ implies $\sup\{X, Y\} = Y$ implies $f(Y) = \sup\{f(X), f(Y)\}$ implies $f(X) \subseteq f(Y)$

Iterated applications of f

$f^0(X) = X$
$f^{n+1}(X) = f(f^n(X))$ for all $n \in \mathbb{N}$

Kleene fixed point theorem (2)

Claim

Let $f{:}\wp(U) \to \wp(U)$ be continuous.

1. $\text{lfp}\ f = \sup\{f^n(\emptyset) \mid n \in \mathbb{N}\}$
2. $\text{gfp}\ f = \inf\{f^n(U) \mid n \in \mathbb{N}\}$

Proof

1. $f(\sup\{f^n(\emptyset) \mid n \in \mathbb{N}\}) = \sup\{f^{n+1}(\emptyset) \mid n \in \mathbb{N}\}$ (f continuous)
   $\sup\{f^{n+1}(\emptyset) \mid n \in \mathbb{N}\} = \sup\{f^n(\emptyset) \mid n \in \mathbb{N}\}$ ($f^0(\emptyset) = \emptyset$, def. of sup)
   $\text{lfp}\ f \subseteq \sup\{f^n(\emptyset) \mid n \in \mathbb{N}\}$ (def. of lfp f)
   $f^0(\emptyset) \subseteq \text{lfp}\ f$ ($f^0(\emptyset) = \emptyset$)
   $f^n(\emptyset) \subseteq \text{lfp}\ f$ implies $f^{n+1}(\emptyset) \subseteq \text{lfp}\ f$ (f is monotone, def. of lfp f)
   $f^n(\emptyset) \subseteq \text{lfp}\ f$ for all $n \in \mathbb{N}$ (induction over n)
   $\sup\{f^n(\emptyset) \mid n \in \mathbb{N}\} \subseteq \text{lfp}\ f$ (def. of sup)
   $\text{lfp}\ f = \sup\{f^n(\emptyset) \mid n \in \mathbb{N}\}$ (symmetry)
2. Obtained from 1 by duality

Kleene fixed point theorem with weaker assumption

Ascending and descending chains

- if $f: \wp(U) \rightarrow \wp(U)$ is monotone, then by induction over n:
  - $f^0(\emptyset) \subseteq f^1(\emptyset) \subseteq \ldots f^n(\emptyset) \subseteq f^{n+1}(\emptyset) \subseteq \ldots$ ascending chain
  - $f^0(U) \supseteq f^1(U) \supseteq \ldots f^n(U) \supseteq f^{n+1}(U) \supseteq \ldots$ descending chain
- least fixed point
  - f monotone, f preserves sup of ascending chains
  - even weaker: f monotone, f preserves sup of ascending chain $f^0(\emptyset) \subseteq \ldots \subseteq f^n(\emptyset) \subseteq$
- greatest fixed point
  - f monotone, f preserves inf of descending chains
  - even weaker: f monotone, f preserves inf of descending chain $f^0(U) \supseteq \ldots \supseteq f^n(U) \supseteq$
- Remark: the underlying lattice does not need to be complete, it is only required to be bounded

Application of the Kleene theorem (1)

Example 1

$$f_1 : \wp(\mathbb{Q}) \to \wp(\mathbb{Q}) \text{ ($\mathbb{Q}$ is the set of rational numbers)}$$

$$f_1(X) = \{0\} \cup \{x + 1 \mid x \in X\}$$

$f_1(\emptyset) = \{0\}$
$f_1^2(\emptyset) = \{0, 1\}$
...
$f_1^n(\emptyset) = \{x \leq n - 1 \mid x \in \mathbb{N}\}$ for all $n \geq 1$
lfp $f_1 = \sup\{f_1^n(\emptyset) \mid n \in \mathbb{N}\} = \mathbb{N}$

$f_1(\mathbb{Q}) = \mathbb{Q}$
...
$f_1^n(\mathbb{Q}) = \mathbb{Q}$
gfp $f_1 = \mathbb{Q}$

Exercise: show that if $f_1 : \wp(S) \to \wp(S)$, where S is the set of non negative rational numbers, then the fixed point is unique, and compute it.

Application of the Kleene theorem (2)

Example 2

Let $[0,1]$ be the closed interval of real numbers

$$f_2 : \wp([0,1]) \to \wp([0,1])$$

$$f_2(X) = \{0\} \cup \{\tfrac{x}{2} \mid x \in X\} \cup \{\tfrac{1+x}{2} \mid x \in X\}$$

$f_2(\emptyset) = \{0\}$
$f_2^2(\emptyset) = \{0, \frac{1}{2}\}$
...
$f_2^n(\emptyset) = \{\sum_{i=1}^{i<n} \frac{b_i}{2^i} \mid b_i \in \{0,1\}\}$
$\text{lfp } f_2 = \sup\{f_2^n(\emptyset) \mid n \in \mathbb{N}\} = \{\sum_{i=1}^{i<n} \frac{b_i}{2^i} \mid n \in \mathbb{N}, b_i \in \{0,1\}\}$

$f_2([0,1]) = [0,1]$
...
$f_2^n([0,1]) = [0,1]$
$\text{gfp } f_2 = \inf\{f_2^n([0,1]) \mid n \in \mathbb{N}\} = [0,1]$

Application of the Kleene theorem (3)

Example 3

$$f_3 : \wp(\mathbb{N}) \to \wp(\mathbb{N})$$

$$f_3(X) = \{x - x \mid x \in X, x > 0\} \cup \{x + 1 \mid x \in X, x > 0\}$$

$f_3(\emptyset) = \emptyset$
$f_3^2(\emptyset) = \emptyset$
...
$f_3^n(\emptyset) = \emptyset$
lfp $f_3 = \emptyset$

$f_3(\mathbb{N}) = \{0\} \cup \{x \geq 2 \mid x \in \mathbb{N}\}$
$f_3^2(\mathbb{N}) = \{0\} \cup \{x \geq 3 \mid x \in \mathbb{N}\}$
...
$f_3^n(\mathbb{N}) = \{0\} \cup \{x \geq n + 1 \mid x \in \mathbb{N}\}$
$\inf\{f_3^n(\mathbb{N}) \mid n \in \mathbb{N}\} = \{0\}$
but $f_3(\{0\}) = \emptyset$, hence gfp $f_3 = \emptyset$, and f_3 does not preserve inf

Application of the Kleene theorem (4)

Remarks on the examples

- lfp $f_i \subsetneq$ gfp f_i for $i = 1, 2$
- gfp f_i depends on the fixed universe
  For instance, in example 2 if $U = [0, 1] \cap \mathbb{Q}$, then
  $f_2(U) = U$ and gfp $f_2 = [0, 1] \cap \mathbb{Q}$