Structural Induction

J.-F. Monin

Univ. Joseph Fourier and
LIAMA, Tsinghua Univ. , Beijing

Tsinghua, August 2010

Making a property inductive by strengthening

- $fib\ 0 = 1$
- $fib\ 1 = 1$
- $fib\ (S\ (S\ n)) = fib\ n + fib\ (S\ n)$
- $gfib\ a\ b\ 0 = a$
- $gfib\ a\ b\ 1 = b$
- $gfib\ a\ b\ (S\ (S\ n)) = gfib\ a\ b\ n + gfib\ a\ b\ (S\ n)$

Prove $\forall n, gfib\ 1\ 1\ n = fib\ n$ by obvious (?) induction

- $gfib\ 1\ 1\ 0 = 1 = fib 0$
- Assume $gfib\ 1\ 1\ n = fib\ n$, $gfib\ 1\ 1\ (S\ n) = ?$
  2 cases
  - $n = 0$: $gfib\ 1\ 1\ (S\ 0) = 1 = fib(S\ 0)$
  - $n = S\ p$: $gfib\ 1\ 1\ (S\ (S\ p)) = \underbrace{gfib\ 1\ 1\ p}_{NOK} + \underbrace{gfib\ 1\ 1\ (S\ p)}_{OK}$

Need to prove simultaneously $P\ n$ and $P\ (S\ n)$

Making a property inductive by strengthening

- $\mathit{fib}\ 0 = 1$
- $\mathit{fib}\ 1 = 1$
- $\mathit{fib}\ (S\ (S\ n)) = \mathit{fib}\ n + \mathit{fib}\ (S\ n)$
- $\mathit{gfib}\ a\ b\ 0 = a$
- $\mathit{gfib}\ a\ b\ 1 = b$
- $\mathit{gfib}\ a\ b\ (S\ (S\ n)) = \mathit{gfib}\ a\ b\ n + \mathit{gfib}\ a\ b\ (S\ n)$

Prove $\forall n, \mathit{gfib}\ 1\ 1\ n = \mathit{fib}\ n\ \wedge\ \mathit{gfib}\ 1\ 1\ (S\ n) = \mathit{fib}\ (S\ n)$

- $\mathit{gfib}\ 1\ 1\ 0 = 1 = \mathit{fib}0$, $\mathit{gfib}\ 1\ 1\ (S\ 0) = 1 = \mathit{fib}\ (S\ 0)$
- Assume $\mathit{gfib}\ 1\ 1\ n = \mathit{fib}\ n$ and $\mathit{gfib}\ 1\ 1\ (S\ n) = \mathit{fib}\ (S\ n)$, then
  - $\mathit{gfib}\ 1\ 1\ (S\ n) = \mathit{fib}\ (S\ n)$ by 2nd induction hyp
  - $\mathit{gfib}\ 1\ 1\ (S\ (S\ n)) = \mathit{gfib}\ 1\ 1\ n + \mathit{gfib}\ 1\ 1\ (S\ n) = \mathit{fib}\ n + \mathit{fib}\ (S\ n) = \mathit{fib}\ (S\ (S\ n))$
    using the 2 induction hyps

Abstracting this reasoning scheme

$$\frac{P\,0 \qquad P\,1 \qquad \forall n, P\ n \Rightarrow P(S\ n) \Rightarrow P\,(S\,(S\ n))}{\forall n, P\ n}$$

Can be proved from $\mathbb{N}$ along the same lines

Pose $Q\ n \stackrel{\text{def}}{=\!=} P\ n\ \wedge\ P\,(S\ n)$

- $Q\,0$: using $P\,0$ and $P\,1$
- Assume $Q\ n$, prove $Q\,(S\ n)$
  - $Q\ n$ provides $P\ n$ and $P\,(S\ n)$
  - We want $Q\ n$, that is $P\,(S\ n)$ and $P\,(S\,(S\ n))$
  - $P\,(S\ n)$: by first induction hypothesis
  - $P\,(S\,(S\ n))$: using $\forall n, P\ n \Rightarrow P(S\ n) \Rightarrow P\,(S\,(S\ n))$ and the 2 induction hypotheses

Drawing dependencies

For

- plus
- add
- fib
- gfib

Still stronger

$$\frac{P\,0 \qquad P\,1 \qquad \forall n, P\ n\ \wedge\ P\,(S\ n) \Rightarrow P\,(S\,(S\ n))}{\forall n, P\ n}$$

$$\frac{P\,0 \qquad \forall n, (\forall m, m \leq n \Rightarrow P\ m) \Rightarrow P\,(S\ n)}{\forall n, P\ n}$$

By (basic) induction on $Q\ n \stackrel{\text{def}}{=\!=} \forall m, m \leq n \Rightarrow P\ m$

Rephrasing

$$\frac{\forall n, (\forall m, m < n \Rightarrow P\ m) \Rightarrow P\ n}{\forall n, P\ n}$$

Well-founded induction on $(\mathbb{N}, <)$

Well-founded induction

Material:

- S: a set, called the domain of the induction
- R: a relation on S
- R is well-founded

$$\frac{\forall x, (\forall y, R\ y\ x \Rightarrow P\ y) \Rightarrow P\ x}{\forall x, P\ x}$$

Two equivalent views on *well-founded*

- any decreasing chain eventually stops
- all elements of S are accessible

An element is accessible $\stackrel{\text{def}}{=\!=}$ all its predecessors are accessible

Important application

Theorem of chocolate tablets

Statement

Let us take a tablet containing n tiles
and cut it into pieces along grooves

How many shots are needed for reducing the tablet into tiles?

Answer

$n - 1$

It does not depend on successive choices of grooves!

Proof

By well-founded induction on $(\mathbb{N}, <)$

Construction of well-founded relations

E.g. the lexicographic ordering of two well-founded relations is well-founded.

Structural induction

A very natural generalisation of induction

On lists

$$\frac{P\ nil \qquad \forall n \forall l, P\ l \Rightarrow P(n :: l)}{\forall l, P\ l}$$

Examples: stuttering list, associativity of append, reverse

On binary trees

$$\frac{P\ leaf \qquad \forall n \forall t_l t_r, P\ t_l \Rightarrow P\ t_r \Rightarrow P\ (Node\ t_l\ n\ t_r)}{\forall t, P\ t}$$

Examples: number of keys and of leaves, algorithms on binary search trees

Induction on a inductive predicate

```
Inductive even (n: nat) :=
  | E0 : even 0
  | E2:  forall n:nat, even n -> even (S (S n)).
```

$$\frac{P\,0 \qquad \forall n, \mathit{even}\ n \Rightarrow P\ n \Rightarrow P\,(S\,(S\ n))}{\forall n, \mathit{even}\ n \Rightarrow P\ n}$$

Rem: we use Coq syntax, up to something to be introduced in later lectures – indicating the type of *even* n.

Lists of consecutive even numbers

```
Inductive list :=
  | E : list
  | C :  nat -> list -> list.
```

$$\frac{P\ E \qquad \forall n \forall l, P\ l \Rightarrow P (C\ n\ l)}{\forall l, P\ l}$$

```
Inductive evl (n: nat) :=
  | E0 : evl 0
  | E2:  forall n:nat, evl n -> evl (S (S n)).
```

$$\frac{P\ E0 \qquad \forall n \forall l, P\ l \Rightarrow P (E2\ n\ l)}{\forall l, P\ l}$$

$$\frac{P\ 0\ E0 \qquad \forall n \forall l, P\ n\ l \Rightarrow P\ (S\ (S\ n))\ (E2\ n\ l)}{\forall n l, P\ n\ l}$$

Lists of consecutive even numbers (cont'd)

```
Inductive evl (n: nat) :=
  | E0 : evl 0
  | E2:  forall n:nat, evl n -> evl (S (S n)).
```

$$\frac{P\ 0\ E0 \qquad \forall n \forall l, P\ n\ l \Rightarrow P\ (S\ (S\ n))\ (E2\ n\ l)}{\forall n l, P\ n\ l}$$

Take for P a predicate which does not depend on its second argument: $P\ n\ l \stackrel{\mathrm{def}}{=\!=} Q\ n$

$$\frac{Q\ 0 \qquad \forall n\, \forall (l : evl\ n), Q\ n \Rightarrow Q\ (S\ (S\ n))}{\forall n (l : evl\ n), Q\ n}$$

$$\frac{Q\ 0 \qquad \forall n, evl\ n \Rightarrow Q\ n \Rightarrow Q\ (S\ (S\ n))}{\forall n, evl\ n \Rightarrow Q\ n}$$

Now, evl reads just *even*

Application: accessibility on (S, R)

Already available:

- a type S representing the domain of induction
- a binary relation R on S

```
Inductive accessible : S -> Prop :=
  AccIntro :
    (forall y, R y x -> accessible y) ->
    accessible x
```

$$\frac{\forall x, (\forall y, R\ y\ x \Rightarrow P\ y) \Rightarrow P\ x}{\forall x, \mathit{accessible}\ x \Rightarrow P\ x}$$

Definition. The relation R is well-founded when all elements of S are accessible. If R is well-founded, well-founded induction can be derived:

$$\frac{\forall x, (\forall y, R\ y\ x \Rightarrow P\ y) \Rightarrow P\ x}{\forall x, P\ x}$$

In short

Trees everywhere!

- Very intuitive objects
- Suitable for structural induction, a natural and simple generalisation of basic induction on natural numbers
- All forms of induction are special cases of structural induction
  (infinitely branching trees may enter into the picture)