1.1 Mathematical Induction

Motivation: The game of frogs

With thanks to Bartosz D. Wozniak

The game of frogs takes place on a plank of n meters length, where $n : \mathbb{N}$. It starts with m frogs at different positions on the plank (where $m : \mathbb{N}$).

The frogs move from reft to right or from right to left. They all have different, non-zero speeds. When they collide, the frog with the highest speed continues his journey, while the rest flip direction.

When a frog reaches the edge of the plank, it falls off the plank, and morphs into a prince.

Is there some initial configuration for which in all future steps there will be at least one frog left on the plank?

"In the 'Game of Frogs', you swim or die."

For all initial configurations eventually all frogs will have been turned to princes. This can be proven by mathematical induction over the number of frogs on the plank.

Slide 45

Motivation-2: Beetles eating cactuses

A beetle eats the leaves of a cactus, but when it does so, the cactus grows back. The question is whether the beetle will consume the cactus.

In more detail: The cactus corresponds to a tree. When the beetle eats one of the leaves of that tree, then the leaf (lf) is removed from the tree. Moreover, if lf is not a child of the root, then, the cactus will grow back as follows:
Let T_{lf} be the subtree with root $parent(lf)$ and after lf has been removed. Add k copies of T_{lf} under $parent(parent(lf))$, where k is an arbitrary natural number.

The cactus is *consumed* when it consists of the root only.

- Is there a cactus which no beetle can consume?
- Can the beetle avoid ever consuming the cactus?

For the first question, ne can show that for all possible cacti, the beetle has a strategy whereby to consume the whole cactus. For this you need to show that the betle has a strategy whereby it decreases the depth of the tree, and if the tree has depth 1, then the beetle can consume it – ie a more sophisticated proof by induction. For the second question, the answer is that no matter what the beetle does, it cannot keep the cactus alive. The proof requires a more sophisticated form of structural induction, and we shall probably not have time to discuss it in the course. But you can find out more under Hydra and Hercules.

Induction in general

Induction can be used to prove statements of the form

$$\forall x : S.P(x)$$

where S is an enumerable set, and $P \subseteq S$.

Examples of properties of enumerable sets.

- $\forall n : \mathbb{N}.(7^n + 5$ is exactly divisible by 3)
- $\forall n : \mathbb{N}.\forall m : \mathbb{N}.$ Given a plank of length n and with m frogs, eventually there will only be princes left.
- $\forall$`xs:[a]`.$\forall$`ys:[a]`.
  `length(xs ++ ys)` $=$ `length(xs) + length(ys)`

$P \subseteq S$ means that P is a property of of elements of the set S. For example, $pos \subset \mathbb{Z}$.

Examples of enumerable sets are the natural numbers ($\mathbb{N}$), sequences, strings, or Haskell data structures such as lists, trees, etc. $\mathbb{R}$ is *not* an enumerable set.

Slide 47

Principle of mathematical induction

For any $P \subseteq \mathbb{N}$:

$$P(0) \quad \land \quad \forall k : \mathbb{N}.[\, P(k) \rightarrow P(k+1)\,] \quad \longrightarrow \quad \forall n : \mathbb{N}.P(n)$$

Slide 48

Mathematical induction principle for $\sum_{i=0}^{n} i = \frac{n*(n+1)}{2}$

$$\sum_{i=0}^{0} i = \frac{0*(0+1)}{2}$$

$$\land$$

$$\forall k : \mathbb{N}. \;\; [\; \sum_{i=0}^{k} i = \frac{k*(k+1)}{2} \;\; \rightarrow \;\; \sum_{i=0}^{k+1} i = \frac{(k+1)*(k+1+1)}{2} \;]$$

$$\rightarrow$$

$$\forall n : \mathbb{N}. \sum_{i=0}^{n} i = \frac{n*(n+1)}{2}$$

Slide 49

Proof schema for $\forall n : \mathbb{N}. \sum_{i=0}^{n} i = \frac{n*(n+1)}{2}$ by math. ind. over n

Base Case

To Show $\sum_{i=0}^{0} i = \frac{0*(0+1)}{2}$

...

Inductive Step

Take k arbitrary

Inductive Hypothesis $\sum_{i=0}^{k} i = \frac{k*(k+1)}{2}$

To Show $\sum_{i=0}^{k+1} i = \frac{(k+1)*(k+1+1)}{2}$

...

Slide 50

Proof Style - remember

1. Write what is given and what you want to prove.
2. Make proof steps explicit.
3. Justify each proof step, indicating properties, assumptions or lemmas used for particular step.
4. Give names to intermediate results, and refer to these when using them later.
5. When proving by induction, say on which variable you apply the induction principle.
6. Vary granularity of proof steps according to confidence, and circumstances.

Aim to write proofs that *others* can check.

Slide 51

Base Case of proof of $\forall n. \sum_{i=0}^{n} i = \frac{n*(n+1)}{2}$

Base Case, To Show : $\sum_{i=0}^{0} i = \frac{0*(0+1)}{2}$

$$
\begin{aligned}
& \textstyle\sum_{i=0}^{0} i \\
= \;& 0 && \text{by definition of } \textstyle\sum \\
= \;& \tfrac{0*(1)}{2} && \text{by arithmetic} \\
= \;& \tfrac{0*(0+1)}{2} && \text{by arithmetic}
\end{aligned}
$$

Slide 52

Inductive step of proof of $\forall n. \sum_{i=0}^{n} i = \frac{n*(n+1)}{2}$

Inductive Step

Take a $k \in \mathbb{N}$, arbitrary.

Inductive Hypothesis: $\sum_{i=0}^{k} i = \frac{k*(k+1)}{2}$

To Show: $\sum_{i=0}^{k+1} i = \frac{(k+1)*(k+1+1)}{2}$

$$
\begin{aligned}
& \textstyle\sum_{i=0}^{k+1} i \\
= \;& \textstyle\sum_{i=0}^{k} i + (k+1) && \text{by definition of } \textstyle\sum \ldots. \\
= \;& (\tfrac{k*(k+1)}{2}) + (k+1) && \textbf{by induction hypothesis} \\
= \;& \tfrac{k^2+k+2*k+2}{2} && \text{by arithmetic} \\
= \;& \tfrac{k^2+3*k+2}{2} && \text{by arithmetic} \\
= \;& \tfrac{(k+1)*(k+2)}{2} && \text{by arithmetic}
\end{aligned}
$$

Slide 53

Proof by mathematical induction, second example

We want to prove

$(*) \quad \forall n : \mathbb{N}.(7^n + 5 \text{ is exactly divisible by } 3)$

by mathematical induction over n.

We reformulate $(*)$ as

$(**) \quad \forall n : \mathbb{N}.\exists m : \mathbb{N}.\ 7^n + 5 = 3 * m.$

Slide 54

Mathematical induction principle for (**) $\forall n : \mathbb{N}.\exists m : \mathbb{N}.\ 7^n + 5 = 3 * m$

$$\exists m : \mathbb{N}.\ 7^0 + 5 = 3 * m$$

$$\wedge$$

$$\forall k : \mathbb{N}.\ [\ \exists m : \mathbb{N}.\ 7^k + 5 = 3 * m \ \rightarrow\ \exists m' : \mathbb{N}.\ 7^{k+1} + 5 = 3 * m'\ ]$$

$$\longrightarrow$$

$$\forall n : \mathbb{N}.\exists m : \mathbb{N}.\ 7^n + 5 = 3 * m$$

Slide 55

Proving (**) by math. ind. over n - schema

Base Case

To Show $\exists m : \mathbb{N}.\ 7^0 + 5 = 3 * m.$

...

Inductive Step

Take a $k \in \mathbb{N}$, arbitrary.

Inductive Hypothesis $\exists m : \mathbb{N}.\ 7^k + 5 = 3 * m.$

To Show $\exists m' : \mathbb{N}.\ 7^{k+1} + 5 = 3 * m'.$

...

Slide 56

Base Case for (**)

Base Case, To Show : $\exists m : \mathbb{N}.\ 7^0 + 5 = 3 * m.$

We first manipulate the term $7^0 + 5$.

$$\begin{array}{rcll} 7^0 + 5 & = & 1 + 5 & \text{by arithmetic} \\ & = & 6 & \text{by arithmetic} \\ & = & 3 * 2 & \text{by arithmetic} \end{array}$$

Therefore, $\exists m : \mathbb{N}.\ 7^0 + 5 = 3 * m.$

Slide 57

Inductive Step for (**)

Inductive Step

Take a $k \in \mathbb{N}$, arbitrary.

Inductive Hypothesis: $\exists m : \mathbb{N}.\ 7^k + 5 = 3 * m$.

To Show: $\exists m' : \mathbb{N}.\ 7^{k+1} + 5 = 3 * m'$.

(A) $7^k + 5 = 3 * m1$. by ind. hyp., for some $m1 : \mathbb{N}$.

Moreover,

$$
\begin{array}{lll}
7^{k+1} + 5 & = 7 * 7^k + 5 & \text{by arithmetic} \\
 & = (6 + 1) * 7^k + 5 & \text{by arithmetic} \\
 & = (6 * 7^k + 7^k) + 5 & \text{by arithmetic} \\
 & = 3 * (2 * 7^k) + (7^k + 5) & \text{by arithmetic} \\
 & = 3 * (2 * 7^k) + 3 * m1 & \text{by (A)} \\
 & = 3 * (2 * 7^k + m1) & \text{by arithmetic}
\end{array}
$$

Take $m2$ as $m2 = 2 * 7^k + m1$, and thus obtain
$\exists m' : \mathbb{N}.\ 7^{k+1} + 5 = 3 * m'$.

Slide 58

Why does induction work?

Intuitively, and informally

- Base case: $P(0)$ holds
- Inductive Step: $P(k) \to P(k+1)$ for all $k \geq 0$
  - $P(0) \to P(1)$ so $P(1)$ holds
  - $P(1) \to P(2)$ so $P(2)$ holds
  - $P(2) \to P(3)$ so $P(3)$ holds
  - $P(3) \to P(4)$ so $P(4)$ holds
  - ...

and so $P(n)$ holds for all $n \geq 0$.

Slide 59

A cautionary tale

We will show a proof by induction that

All people in a room have the same age.

Take $P(n) \equiv$ in any room with n people, every person has the same age".

We will prove $\forall n : \mathbb{N}.P(n)$.

Slide 60

All people in a room have same age - base case

Base Case, To Show : Everybody in a room with 0 people has same age.

obvious

Slide 61

All people in a room have same age - inductive step

Inductive Step

Take $k : \mathbb{N}$, arbitrary.

Inductive Hypothesis: Everybody in a room with k people has same age

To Show: Everybody in a room with $k+1$ people has same age

1. Take room with $k+1$ people, and arbitrary persons A and B.
2. Remove A. Now the induction hypothesis is applicable. Therefore, B has same age as all other people in the room.
3. Bring A back in the room and remove B. Induction hypothesis is applicable.
   Therefore, A has same age as all other people in the room.
4. Therefore A and B have the same age as everybody else in the room.
5. Therefore, everybody in the room has the same age.

Slide 62

Is induction flawed?

Conclusion:

Justify each proof step

From the previous argument, step 4 was flawed. Namely, the step only works if the original room has at least 3 people, ie only if $k \geq 2$. So, we have a proof, where the base case (for $k = 0$ or even $k = 1$) holds, and the inductive step holds only for $k \geq 2$. Therefore the step is not applicable on the base case, and the inductive chain is broken.

New technique of math. induction

For example, given

```
f :: Int -> Ratio Int
-- SPEC ∀n ≥ 1.f n = n/(n+1)
f 1 = 1/2
f n =  1/(n*(n+1)) + f (n-1)
```

Math. induct. principle. not *directly* applicable on $\forall n \geq 1.\mathtt{f}\ n = \frac{n}{n+1}$, because

a) The conclusion has different shape.

b) The term `f 0` is undefined; therefore "base case" cannot be stated.

Slide 63

Slide 64

Part I: Reasoning About Haskell Programs — Mathematical Induction

Three Approaches to proving $\forall n \geq 1.\texttt{f}\ n = \frac{n}{n+1}$

In order to prove $\forall n \geq 1.\texttt{f}\ n = \frac{n}{n+1}$, we can

1st Approach Prove, instead $\forall n : \mathbb{N}.\boldsymbol{n \geq 1} \longrightarrow \texttt{f}\ n = \frac{n}{n+1}$

2nd Approach Prove, instead $\forall n : \mathbb{N}.\texttt{f}\ (n\ \boldsymbol{+1}) = \frac{n\ \boldsymbol{+1}}{n\ \boldsymbol{+2}}$

3rd Approach Apply the Mathematical Induction **"Technique"**

Drossopoulou & Wheelhouse (DoC) Reasoning about Programs 64 / 396

In the next slides we will be explaining the induction technique.

Before that, as an exercise, we will study the first approach from above.

1st Approach - Math. Induct. Principle on $\forall n : \mathbb{N}.[n \geq 1 \ \rightarrow \ \texttt{f}\ n = \frac{n}{n+1}]$

Application of the induction principle on the property from above gives

$$\left(\ 0 \geq 1 \ \longrightarrow \ \texttt{f}\ 0 = \tfrac{0}{0+1}\ \right)$$
$$\wedge$$
$$\forall k : \mathbb{N}.\ [\ \ (k \geq 1 \ \rightarrow \ \texttt{f}\ k = \tfrac{k}{k+1}) \ \rightarrow \ (k+1 \geq 1 \ \rightarrow \ \texttt{f}\ k+1 = \tfrac{k+1}{k+1+1} 0)\ \ ]$$
$$\longrightarrow$$
$$\forall n : \mathbb{N}.\ [\ n \geq 1 \ \rightarrow \ \texttt{f}\ n = \tfrac{n}{n+1}\ ]$$

Proof

The principle thus leads to the following proof:

Base Case

To Show: $0 \geq 1 \ \longrightarrow \ \texttt{f}\ 0 = \frac{0}{0+1}$

Holds trivially by contradiction, as $0 \geq 1$ is false.

Inductive Step

Take a $k : \mathbb{N}$, arbitrary.

Inductive Hypothesis $k \geq 1 \longrightarrow \texttt{f}\ k = \frac{k}{k+1}$

To Show $k+1 \geq 1 \longrightarrow \texttt{f}\ (k+1) = \frac{k+1}{k+2}$

1st Case: $k = 0$.

Then, $k+1 = 1$. We will apply definition of $\texttt{f}\ 1$.

(1)	$1 = k+1 \geq 1$	by case
(2)	$\texttt{f}\ k+1 = \frac{1}{2}$	by def. of $\texttt{f}$, and (1).
(3)	$\frac{k+1}{k+2} = \frac{1}{2}$	by (1).
(4)	$\texttt{f}\ k+1 = \frac{k+1}{k+2}$	by (2) and (3)

Note that we did *not* use the induction hypothesis!

2nd Case: $k \neq 0$.

Then, we have

(1)	$k \geq 1$	by case
(2)	$k+1 \geq 2$	by (1) and arithm.
(4)	$\texttt{f}\ (k+1) = \frac{1}{(k+1)*(k+2)} + \texttt{f}\ k$	by (2), and def. of $\texttt{f}$.
(5)	$\texttt{f}\ (k+1) = \frac{1}{(k+1)*(k+2)} + \frac{k}{k+1}$	by (4), and ind. hypothesis
(6)	$\texttt{f}\ (k+1) = \frac{1}{(k+1)*(k+2)} + \frac{k*(k+2)}{(k+1)*(k+2)}$	by (5), and arithmetic
(7)	$\texttt{f}\ (k+1) = \frac{k+1}{k+2}$	by (6), and arithmetic

Some of you will have seen such proofs where you used two or more base cases. But note that there is no need for such a construction. In all flavours of mathematical induction there is only one base case.

Slide 65

"Technique" of mathematical induction

For any $P \subseteq \mathbb{Z}$, and any $m : \mathbb{Z}$

$$P(m) \quad \wedge \quad \forall k \geq m . [\, P(k) \rightarrow P(k+1) \,] \quad \longrightarrow \quad \forall n \geq m . P(n)$$

Slide 66

Induct. Technique applied to $\forall n \geq 1 . \texttt{f}\ n = \frac{n}{n+1}$

$$\texttt{f}\ 1 = \frac{1}{1+1}$$

$$\wedge$$

$$\forall k \geq 1 .\ [\ \texttt{f}\ k = \frac{k}{k+1} \ \rightarrow\ \texttt{f}\ k+1 = \frac{k+1}{k+2}\ ]$$

$$\longrightarrow$$

$$\forall n \geq 1 . \texttt{f}\ n = \frac{n}{n+1}$$

Slide 67

Proving $\forall n \geq 1.\texttt{f}\ n = \frac{n}{n+1}$ - the schema

Base Case

To Show $\texttt{f} \ = \frac{1}{1+1}$

...

Inductive Step

Take $k : \mathbb{Z}$, arbitrary.
Assume that $\boldsymbol{k \geq 1}$.

Inductive Hypothesis $\texttt{f}\ k = \frac{k}{k+1}$

To Show $\texttt{f}\ (k+1) = \frac{k+1}{k+2}$.

...

Slide 68

Base Case

Base Case, To Show : $\texttt{f}\ 1 = \frac{1}{1+1}$

$$
\begin{array}{lll}
\texttt{f}\ 1 & & \\
= & 1/2 & \text{by definition} \\
= & \frac{1}{1+1} & \text{because } 1+1=2
\end{array}
$$

Slide 69

Inductive step

Inductive Step
Take $k : \mathbb{Z}$, arbitrary.
(**Ass1**) Assume that $k \geq 1$.
Inductive Hypothesis: $\texttt{f}\ k = \frac{k}{k+1}$
To Show: $\texttt{f}\ (k+1) = \frac{k+1}{k+2}$.

$$
\begin{aligned}
&\texttt{f}\ (k+1) \\
&= \frac{1}{(k+1)*(k+2)} + (\texttt{f}\ k) && \text{by def. of } \texttt{f}, \ \textbf{and} \text{ because of } (\textbf{Ass1}). \\
&= \frac{1}{(k+1)*(k+2)} + \frac{k}{k+1} && \text{by induction hypothesis} \\
&= \frac{1}{(k+1)*(k+2)} + \frac{k*(k+2)}{(k+1)*(k+2)} && \text{by arithmetic} \\
&= \frac{1+k^2+2k}{(k+1)*(k+2)} && \text{by arithmetic} \\
&= \frac{(k+1)*(k+1)}{(k+1)*(k+2)} && \text{by arithmetic} \\
&= \frac{k+1}{k+2} && \text{by arithmetic}
\end{aligned}
$$

Slide 70

Comparing the principle and the technique

Principle:

$$P(0) \quad \wedge \quad \forall k : \mathbb{N}.[\, P(k) \rightarrow P(k+1)\,] \quad \rightarrow \quad \forall n : \mathbb{N}.P(n)$$

Technique:
$\forall m \in \mathbb{Z}:$

$$P(m) \quad \wedge \quad \forall k \geq m.[\, P(k) \rightarrow P(k+1)\,] \quad \rightarrow \quad \forall n \geq m.P(n)$$

What is the difference between the two? No difference! In fact, they are equivalent!

The proof that the principle and the technique are equivalent is quite interesting and clever. Here it is.

Technique implies Principle This follows by $\forall$-elimination, by substituting m by 0, and because $\forall n \geq 0.P(n) \equiv \forall n.P(n)$ and because $\forall k \geq m.[\,P(k) \rightarrow P(k+1)\,] \equiv \forall k : \mathbb{N}.[\,P(k) \rightarrow P(k+1)\,]$.

Principle implies Technique We are given the inductive which says, that for any predicate $R \subseteq \mathbb{N}$:

IP $\quad R(0) \quad \wedge \quad \forall k : \mathbb{N}.\ [\ R(k) \rightarrow R(k+1)\ ] \quad \longrightarrow \quad \forall n : \mathbb{N}.R(n)$

Take any predicate $P \subseteq \mathbb{Z}$, and any integer $m : \mathbb{Z}$ such that

(1) $P(m) \quad \wedge \quad \forall k \geq m\ [\,P(k) \rightarrow P(k+1)]\,]$

To Show: $\forall n \geq m.P(n)$

In order to be able to apply the inductive principle we need a predicate which holds at 0, and which is related to P. We therefore define predicate $Q \subseteq \mathbb{N}$ as: $Q(n) \equiv P(n+m)$. Then we obtain:

(2) $Q(0)$ by definition of Q, and **1**

(3) $\forall k : \mathbb{N}.(Q(k) \rightarrow Q(k+1))$ by definition of Q, and **1**

Apply **IP** on **(2)** and **(3)** from above, and obtain

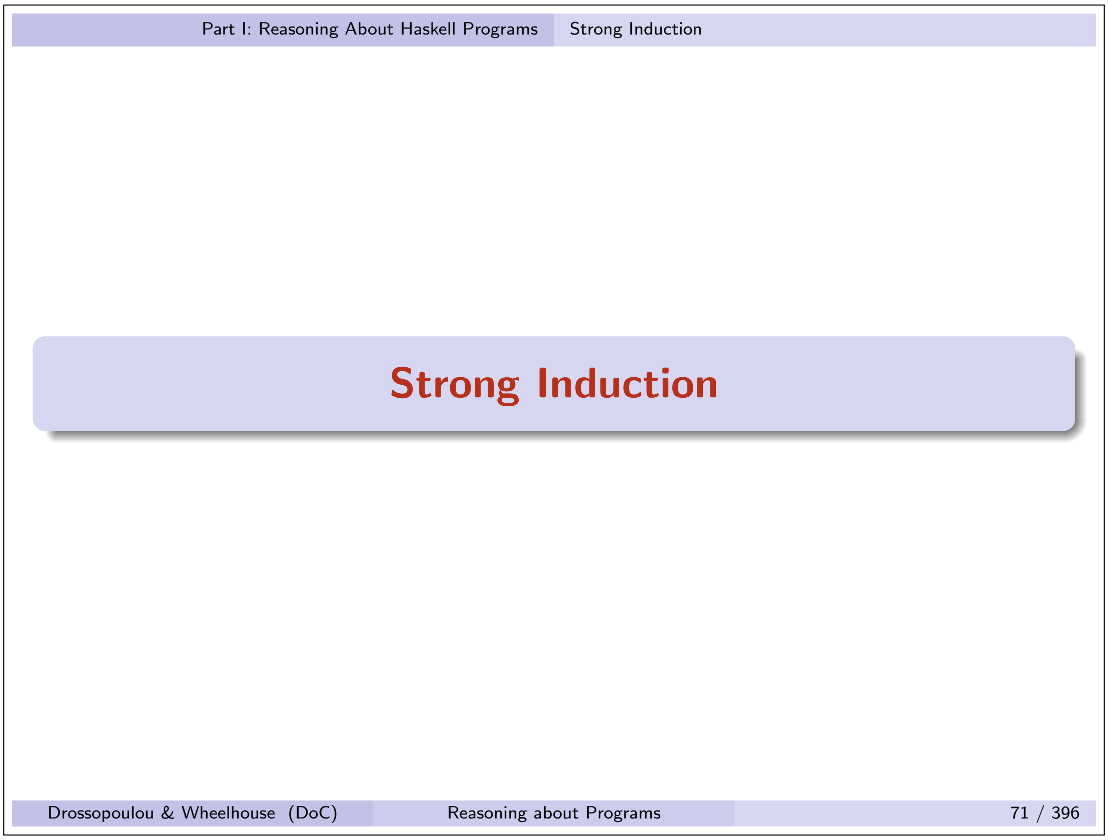
(4) $\forall n : \mathbb{N}.Q(n)$.

(5) $\forall n : \mathbb{N}.Q(n) \equiv \forall n \geq m.P(n)$, by definition of Q.

(6) $\forall n \geq m.P(n)$, by **(4)** and **(5)**.

1.2 Strong Induction

Slide 71



Mathematical Induction allows the inductive step $(k+1)$, to refer to the *direct* predecessor (k).

Strong induction allows the inductive step $(k + 1)$, to refer to *any* predecessor (e.g., to $k - 1$ or $k - 2$).

In some cases we need to use strong induction.

Our plan

- discuss an example that require strong induction
- prove this example
- discuss the relationship between strong and mathematical induction

Strong Induction is also known as "Course-of-Values Induction".

Slide 72

Motivation for strong induction

Does the function g

```
   g :: Int -> Int
   -- SPEC ∀n : ℕ. g n = 3^n − 2^n
  g 0 = 0
  g 1 = 1
  g n = ( 5 * g(n-1) ) - ( 6*g(n-2) )
```

satisfy the property SPEC?

Naive application of mathematical induction is insufficient to prove that $\forall n : \mathbb{N}.\ g\ n = 3^n - 2^n$. We can see that in the following part of the proof

Induction Step

Take $k : \mathbb{N}$, arbitrary.

Induction Hypothesis: $g\ k = 3^k - 2^k$

to Show: $g\ (k+1) = 3^{k+1} - 2^{k+1}$

$$
\begin{array}{lll}
 & g\ (k+1) & \\
 = & (\ 5 * g(k)\ ) - (\ 6*g(k-1)\ ) & \text{by definition} \\
 = & 5 * (3^k - 2^k) - (\ 6*g\ (k-1)\ ) & \text{by ind. hypo. on } k \\
 = & ??? &
\end{array}
$$

But now we are stuck! We would like to apply the induction hypothesis to $k - 1$. But are we allowed to do that?

We therefor introduce another, stronger, principle of induction over $\mathbb{N}$, called strong induction. It allows the application of the induction

Slide 73

Principle of strong induction

$$P(0) \quad \wedge \quad \forall k:\mathbb{N}.[\ \forall j \in \{0..k\}.P(j) \ \longrightarrow\ P(k+1)\ ] \ \rightarrow\ \forall n:\mathbb{N}.P(n)$$

Slide 74

Strong induction principle applied on $\mathtt{g\ n} = 3^{\mathtt{n}} - 2^{\mathtt{n}}$

$$\mathtt{g}\ 0 = 3^0 - 2^0$$

$$\wedge$$

$$\forall \mathtt{k}.[\ \forall \mathtt{j} \in \{0..\mathtt{k}\}.\ \mathtt{g\ j} = 3^{\mathtt{j}} - 2^{\mathtt{j}} \ \rightarrow\ \mathtt{g}\ (\mathtt{k+1}) = 3^{\mathtt{k+1}} - 2^{\mathtt{k+1}}\ ]$$

$$\longrightarrow$$

$$\forall \mathtt{n}:\mathbb{N}.\ \mathtt{g\ n} = 3^{\mathtt{n}} - 2^{\mathtt{n}}$$

Slide 75

Proving $\forall n:\mathbb{N}.\ g\ n = 3^n - 2^n$ by strong ind. over *n* - schema

Base Case

To Show $g\ 0 = 3^0 - 2^0$

...

Inductive Step

Take $k:\mathbb{N}$, arbitrary.

Inductive Hypothesis $\forall j \in \{0..k\}.\ g\ j = 3^j - 2^j$

To Show $g\ (k+1) = 3^{k+1} - 2^{k+1}$

...

Slide 76

Base case of proof of $\forall n:\mathbb{N}.\ g\ n = 3^n - 2^n$

Base Case, To Show : $g\ 0 = 3^0 - 2^0$

$$
\begin{array}{lll}
g\ 0 & & \\
= & 0 & \text{by definition of } g \\
= & 1 - 1 & \text{by arithmetic} \\
= & 3^0 - 2^0 & \text{by arithmetic}
\end{array}
$$

We have shown the base case. Note that the following proof for the inductive step *is* *flawed*:

Inductive Step

Take an arbitrary `k` : $\mathbb{N}$

Inductive Hypothesis: $\forall \mathtt{j} \in \{0..\mathtt{k}\}.\ (\ \mathtt{g\ j} = 3^{\mathtt{j}} - 2^{\mathtt{j}}\ )$

To Show: $\mathtt{g\ (k+1)} = 3^{\mathtt{k+1}} - 2^{\mathtt{k+1}}$

`g(k+1)`

$=$	`5 * g(k) - 6*g(k-1)`	by definition
$=$	$5 * (3^{\mathtt{k}} - 2^{\mathtt{k}}) - 6 * (3^{\mathtt{k-1}} - 2^{\mathtt{k-1}})$	by ind. hyp. on `k`, `k-1`
$=$	$5 * (3 * 3^{\mathtt{k-1}} - 2 * 2^{\mathtt{k-1}}) - 6 * (3^{\mathtt{k-1}} - 2^{\mathtt{k-1}})$	by arithmetic
$=$	$15 * 3^{\mathtt{k-1}} - 6 * 3^{\mathtt{k-1}} - 10 * 2^{\mathtt{k-1}} + 6 * 2^{\mathtt{k-1}}$	by arithmetic
$=$	$9 * 3^{\mathtt{k-1}} - 4 * 2^{\mathtt{k-1}}$	by arithmetic
$=$	$3^{\mathtt{k+1}} - 2^{\mathtt{k+1}}$	by arithmetic

What is wrong with the proof of the inductive step? - 1

- Informally, and comparing the code with the proof we notice that
  - we never used the second case in the definition of `g`/
- Formally, just looking at the proof we notice
  - The inductive hypothesis is only applicable when `t` $\in\ 0..k$

What is wrong with the proof of the inductive step? - 2

The first step is flawed:

Inductive Step:

Take an arbitrary `k` : $\mathbb{N}$

Inductive Hypothesis: $\forall \mathtt{j} \in \{0..\mathtt{k}\}.\ (\ \mathtt{g\ j} = 3^{\mathtt{j}} - 2^{\mathtt{j}}\ )$

To Show: $\mathtt{g\ (k+1)} = 3^{\mathtt{k+1}} - 2^{\mathtt{k+1}}$

`g(k+1)`

$=$ `5 * g(k) - 6*g(k-1)`   by definition of `g`

Namely, in the above we applied the third case (line 5) of the definition of `f`. But, this case is not applicable, when $\mathtt{k} + 1 = 1$, or $\mathtt{k} + 1 = 0$. Notice that the case when when $\mathtt{k} + 1 = 0$ is not problematic.

What is wrong with the proof of the inductive step? - 3

The second step is also flawed:

Inductive Step:

Take an arbitrary $\mathtt{k} : \mathbb{N}$

Inductive Hypothesis: $\forall \mathtt{j} \in \{0..\mathtt{k}\}.\ (\ \mathtt{g\ j} = 3^{\mathtt{j}} - 2^{\mathtt{j}}\ )$

To Show: $\mathtt{g\ (k+1)} = 3^{\mathtt{k+1}} - 2^{\mathtt{k+1}}$

$$
\begin{array}{lll}
\ldots & & \\
= & \mathtt{5\ *\ g(k)\ -\ 6*g(k-1)} & \ldots \\
= & 5 * (3^{\mathtt{k}} - 2^{\mathtt{k}}) - 6 * (3^{\mathtt{k-1}} - 2^{\mathtt{k-1}}) & \text{by ind. hyp. twice}
\end{array}
$$

In the proof step above, we applied the inductive hypothesis to obtain that $g(k-1) = 3^{k-1} - 2^{k-1}$. However, the inductive hypothesis is only applicable if $k-1 \in \{0..k\}$, i.e. if $k-1 \geq 0$. The latter is equivalent with requiring that $k \geq 1$.

But the requirement that $k \geq 1$ has nor appeared anywhere in the proof so far. In order to be able to ask that $k \geq 1$, we will to consider the cases where $k = 0$ and $k > 0$ separately.

Repairing the proof

How can we repair the proof?

Treat the case where $\mathtt{k} = 0$ separately.

Slide 77

Part I: Reasoning About Haskell Programs | Strong Induction

Inductive step of proof of $\forall \mathtt{n} : \mathbb{N}.\ \mathtt{g\ n} = 3^{\mathtt{n}} - 2^{\mathtt{n}}$

Inductive Step

Take an arbitrary $\mathtt{k} : \mathbb{N}$

Inductive Hypothesis: $\forall \mathtt{j} \in \{0..\mathtt{k}\}.\ (\ \mathtt{g\ j} = 3^{\mathtt{j}} - 2^{\mathtt{j}}\ )$

To Show: $\mathtt{g\ (k+1)} = 3^{\mathtt{k+1}} - 2^{\mathtt{k+1}}$

1st Case, $\mathtt{k} = 0$

To show: $\mathtt{g\ (1)} = 3^{1} - 2^{1}$.

$\mathtt{g\ (1)}$

$$
\begin{array}{lll}
= & 1 & \text{by line 4 in definition of } \mathtt{g} \\
= & \ldots & \text{rest as exercise}
\end{array}
$$

Drossopoulou & Wheelhouse (DoC) | Reasoning about Programs | 77 / 396

Note that we did not use the inductive hypothesis for this case.

Slide 78

Inductive step of proof of $\forall n : \mathbb{N}.\ g\ n = 3^n - 2^n$ - continued

Inductive Hypothesis: $\forall j \in \{0..k\}.\ (\ g\ j = 3^j - 2^j\ )$

To Show: $g\ (k+1) = 3^{k+1} - 2^{k+1}$

2nd Case, $k \neq 0$

(A) $k \geq 1$ because $k : \mathbb{N}$ and $k \neq 0$ by case.

(B) $k, k-1 \in \{0..k\}$ because $k : \mathbb{N}$ and $k \neq 0$.

$g\ (k+1)$

$=$	`5 * g(k) - 6*g(k-1)`	By (A), line 5 of defn. g applies
$=$	$5 * (3^k - 2^k) - 6 * (3^{k-1} - 2^{k-1})$	By (B), and induction hypothesis
$=$	$5 * (3 * 3^{k-1} - 2 * 2^{k-1}) - 6 * (3^{k-1} - 2^{k-1})$	by arithmetic
$=$	...	....
$=$	$3^{k+1} - 2^{k+1}$	by arithmetic

Slide 79

Compare mathematical and strong induction

Mathematical Induction

$$P(0) \quad \wedge \quad \forall k : \mathbb{N}.[\ P(k) \rightarrow P(k+1)\ ] \quad \longrightarrow \quad \forall n : \mathbb{N}.P(n)$$

Strong Induction

$$P(0) \quad \wedge \quad \forall k{:}\mathbb{N}.[\ \forall j{\in}\{0..k\}.P(j) \ \rightarrow\ P(k+1)\ ] \quad \longrightarrow \quad \forall n{:}\mathbb{N}.P(n)$$

The two principles are equivalent.

The proof idea is the same as that for showing the mathematic principle and the "technique" are equivalent.

Proving that Strong Induction implies Mathematical Induction

Take any predicate P, such that
A: $P(0)$
B: $\forall k:\mathbb{N}.P(k) \rightarrow P(k+1)$

To show: $\forall n:\mathbb{N}.P(n)$ using *strong* induction.

We will prove that $\forall k:\mathbb{N}.(\forall j \in \{0..k\}.P(j)) \rightarrow P(k+1)$.

Namely, take arbitrary $k:\mathbb{N}$.

(ass1)	$\forall j \in \{0..k\}.P(j)$	assumption
1	$P(k)$	by $\forall$-elimination on (ass1), choosing $j = k$.
2	$P(k+1)$	from B, and 1.

Therefore, we have

C: $\forall k:\mathbb{N}.(\forall j \in \{0..k\}.P(j)) \rightarrow P(k+1)$

We apply the strong induction principle on A and C, and obtain $\forall n:\mathbb{N}.P(n)$.

Proving that Mathematical Induction implies Strong Induction

Take any predicate P, such that

A: $P(0)$

B: $\forall k.\ (\forall j \in \{0..k\}.P(j)) \ \rightarrow \ P(k+1)$

To show: $\forall n:\mathbb{N}.P(n)$ using *mathematical* induction.

We define a new predicate Q as: $Q(n) \ \equiv \ \forall i \in \{0..n\}.P(i)$.

Then we can prove that

C: $Q(0)$ (because $P(0)$ holds, and because $Q(0) \leftrightarrow P(0)$).

D: $\forall k.\ Q(k) \rightarrow Q(k+1)$

Namely, $Q(k)$ implies

1	$\forall i \in \{0..k\}.P(i)$	by definition of Q
2	$P(k+1)$	by **B** and 1
3	$\forall i \in \{0..k{+}1\}.P(i)$	by 1 and 2
4	$Q(k+1)$	by definition of Q

We apply the *mathematical* induction principle on (C) and (D), and obtain $\forall n : \mathbb{N}.Q(n)$. This is equivalent with $\forall n : \mathbb{N}.P(n)$.

q.e.d.

1.3 Two more cautionary tales

Two more cautionary tales

We shall prove that

- $\forall n \in \mathbb{N}.\ \sum_{i=2}^{n} i = \frac{n*(n+1)}{2}$
- $\forall n \in \mathbb{N}.\ Even(fib\ n)$.

Remember that

```
fib :: Int -> Int
fib 0 = 0
fib 1 = 1
fib n =  fib (n-1)  +  fib (n-2)
```


Slide 80

Slide 81

Bogus proof that $\forall n. \sum_{i=2}^{n} i = \frac{n*(n+1)}{2}$

Base Case, To Show : $\sum_{i=2}^{0} i = \frac{0*(0+1)}{2}$

$$
\begin{array}{rcll}
\sum_{i=0}^{0} i & = & 0 & \text{by def. of } \sum \quad (1)\\
& = & \frac{0*(0+1)}{2} & \text{by arithmetic} \quad (2)
\end{array}
$$

Inductive Step

Take a $k \in \mathbb{N}$, arbitrary.

Inductive Hypothesis: $\sum_{i=2}^{k} i = \frac{k*(k+1)}{2}$

To Show: $\sum_{i=2}^{k+1} i = \frac{(k+1)*(k+1+1)}{2}$

$$
\begin{array}{rcll}
\sum_{i=2}^{k+1} & = & \sum_{i=2}^{k} i + (k+1) & \text{by def. of } \sum \text{....} \quad (3)\\
& = & (\frac{k*(k+1)}{2}) + (k+1) & \textbf{by ind. hypo} \quad (4)\\
& = & \frac{(k+1)*(k+1+1)}{2} & \text{by arithmetic} \quad (5)
\end{array}
$$

Slide 82

Bogus proof that $\forall n. Even(fib\ n)$

Base Case, To Show : $Even(fib\ 0)$

$$
\begin{array}{rcll}
Even(fib\,0) & \equiv & Even(0) & \text{by def. of } fib \quad (1)\\
& \equiv & true & \text{by def. of } Even \quad (2)
\end{array}
$$

Inductive Step

Take a $k \in \mathbb{N}$, arbitrary.

Inductive Hypothesis: $\forall j \in \{0..k\}. Even(fib\,j)$

To Show: $Even(fib\,(k+1))$

$$
\begin{array}{ll}
fib\,(k+1) = fib\,k \ + \ fib\,(k-1) & \text{by def. of } fib \quad (3)\\
Even(fib\,k) & \text{by ind. hypo.} \quad (4)\\
Even(fib\,(k-1)) & \text{by ind. hypo.} \quad (5)\\
Even(fib\,(k+1)) & \text{(3), (4), (5), and}\\
& \text{because sum of even is even} \quad (6)
\end{array}
$$

What went wrong?

- What is wrong in the proof of $\forall n \in \mathbb{N}.\ \sum_{i=2}^{n} i = \frac{n*(n+1)}{2}$.
- What is wrong in the proof of $\forall n \in \mathbb{N}.\ Even(fib\, n)$.

In the proof of $\forall n \in \mathbb{N}\ \sum_{i=2}^{n} i = \frac{n*(n+1)}{2}$, step (3) is illegal. Namely, the equation $\sum_{i=2}^{k+1} = \sum_{i=2}^{k} i + (k+1)$ does not hold when $k = 0$. In in the induction step we took an *arbitrary* $k \in \mathbb{N}$.

On the other hand, in the proof of $\forall n \in \mathbb{N}.\, Even(fib\, n)$., steps (3) and (5) are illegal. Namely, $fib\,(k+1) = fib\, k + fib\,(k-1)$ does not hold when $k = 0$. Also, the induction hypothesis is not applicable when $k = 0$ because then $k - 1 \notin \{0..k\}$ and therefore the induction hypothesis cannot be used to obtain that $Even(fib(k-1))$.

1.4 Summary

Slide 84

Summary

We have seen three, equivalent, forms of induction over $\mathbb{Z}$.

The proof schemas are an implication of the corresponding induction principle and the proof planning rules from week 2 (slide 37).

The proofs are an implication of the proof schemas and the proof planning and construction rules from week 2 (slides 36 and 37).

Slide 85

Summary - 2

Mathematical Induction

$$P(0) \quad \wedge \quad \forall k:\mathbb{N}.[\ P(k) \rightarrow P(k+1)\ ] \quad \longrightarrow \quad \forall n:\mathbb{N}.P(n)$$

Technique, for any $m:\mathbb{Z}$:

$$P(m) \quad \wedge \quad \forall k \geq m.[\ P(k) \rightarrow P(k+1)\ ] \quad \longrightarrow \quad \forall n \geq m.P(n)$$

Strong Induction

$$P(0) \quad \wedge \quad \forall k:\mathbb{N}.[\ \forall j \in \{0..k\}.P(j) \ \rightarrow \ P(k+1)\ ] \quad \longrightarrow \quad \forall n:\mathbb{N}.P(n)$$