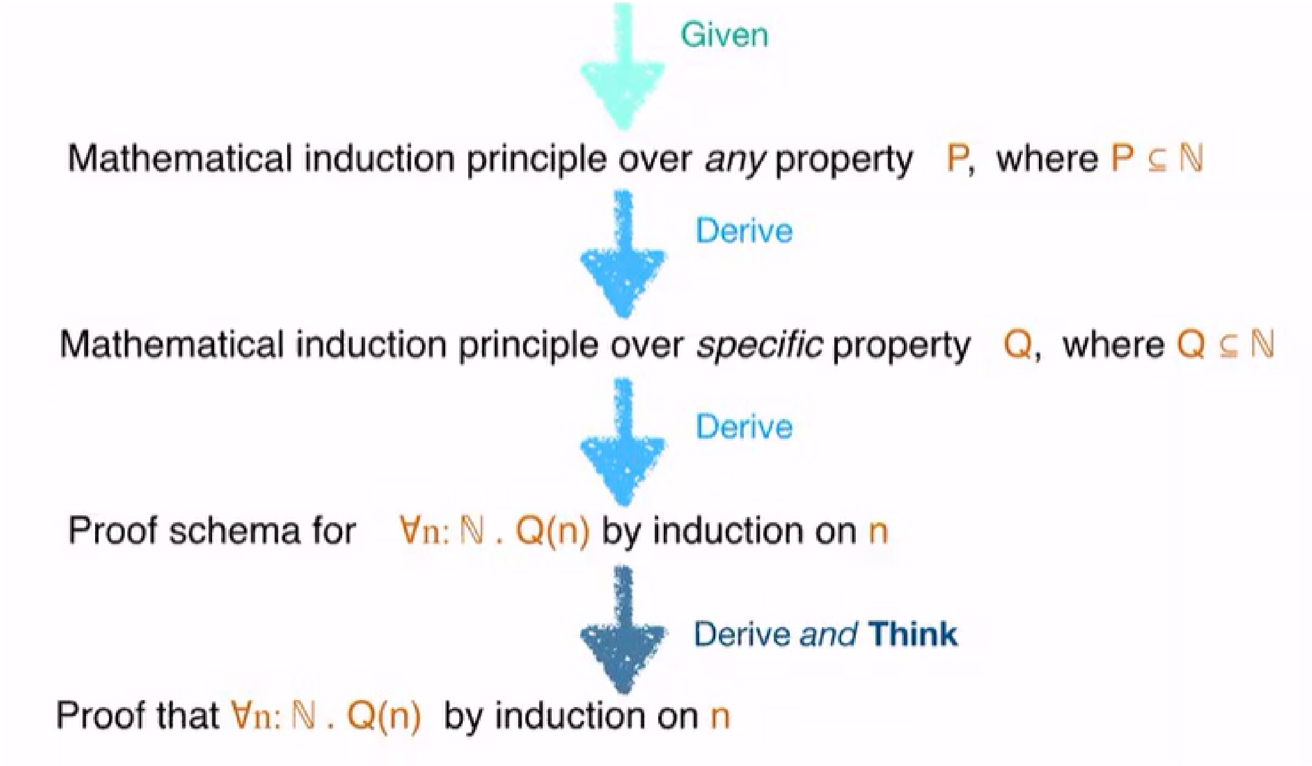
Induction over Numbers

General Plan for every proof



The Rules

Induction can be used to prove statements of the form

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

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

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

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

Example

14:36 Sat 23 Jan 92%

Done Induct.Numbers.1 3 (1 of 21)

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

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

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

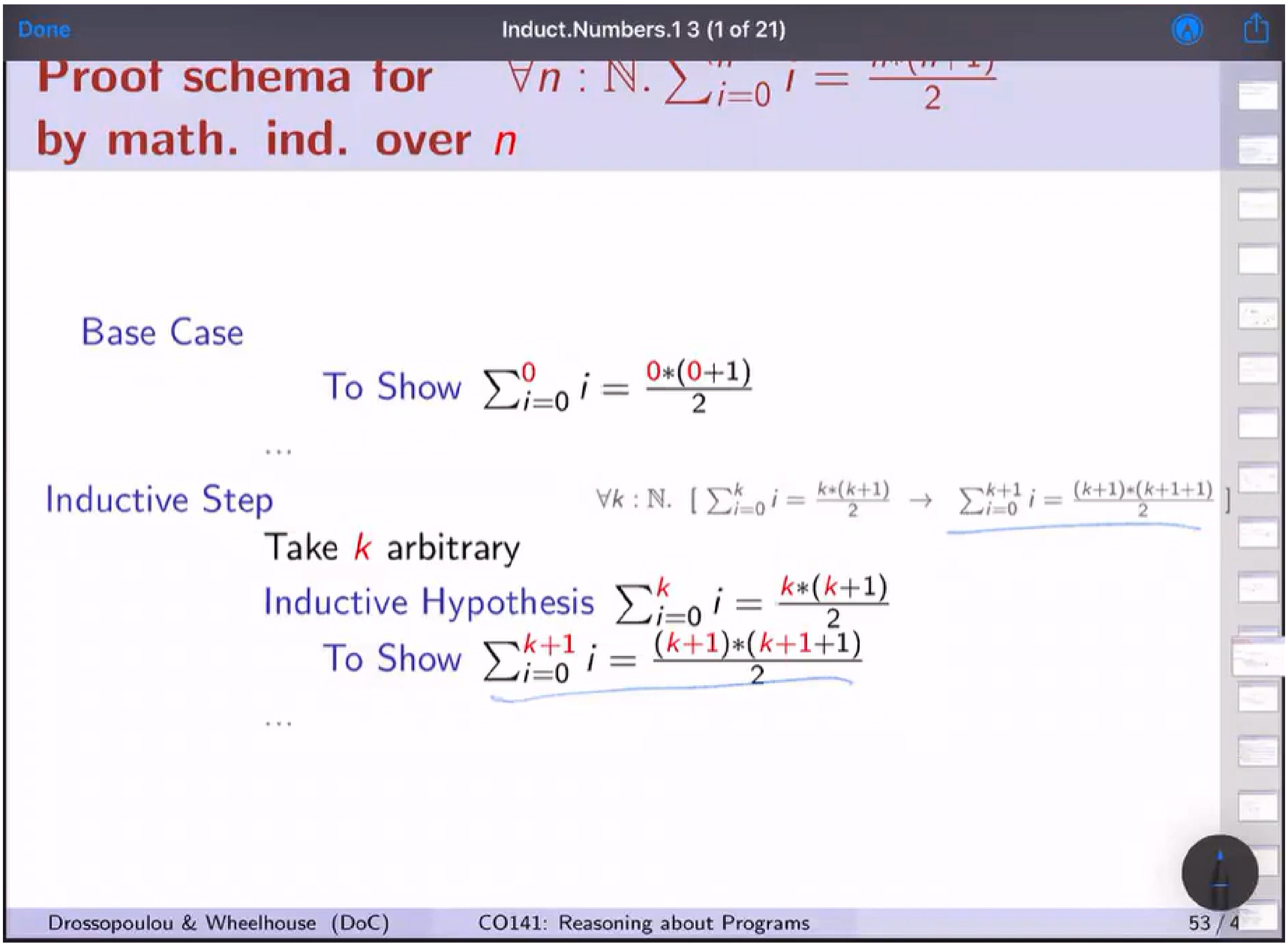
$$\wedge$$

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

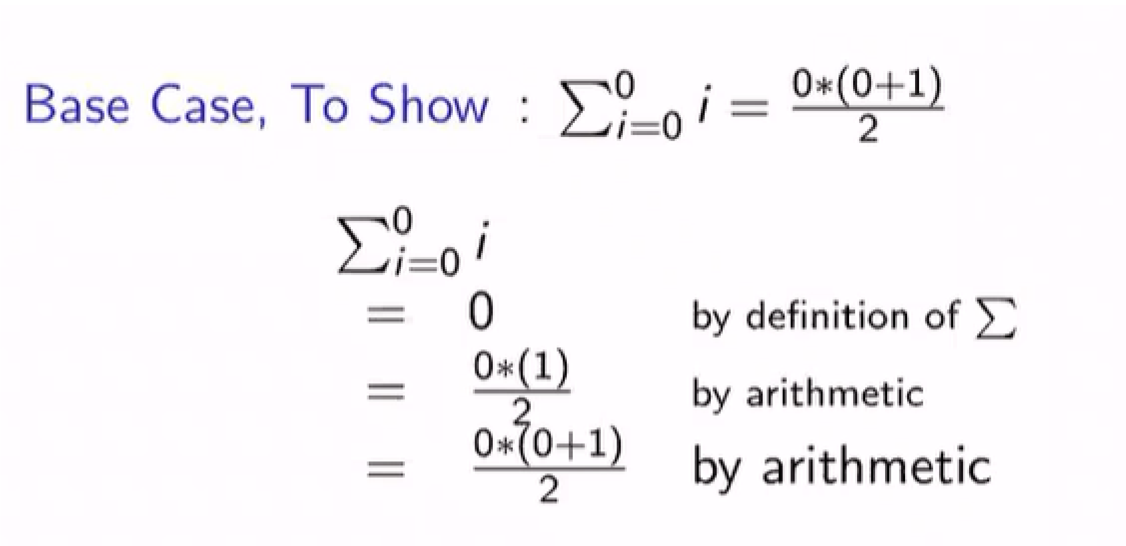
$$\rightarrow$$

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

Drossopoulou & Wheelhouse (DoC) CO141: Reasoning about Programs 52 / 4



Base Case of Proof



Inductive Step Of Proof

Inductive Step

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

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

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

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

Good Proof Style

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.

Example 2

We want to prove

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

by mathematical induction over n.

We reformulate (*) as

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

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

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

$$\wedge$$

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

$$\longrightarrow$$

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

Base Case

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

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

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

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

Inductive Step

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,

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

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

> ⚠ **Warning**
>
> Justify Every Step!

New Technique of Mathematical 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 $\mathtt{f}\ 0$ is undefined; therefore "base case" cannot be stated.

3 Possible Approaches

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

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

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

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

3rd Approach is best.

3rd Approach: Technique of Mathematical Induction

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

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

Example

To Prove:

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

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

$$\texttt{f}\ 1 = \frac{1}{1+1}$$
$$\land$$
$$\forall k \geq 1.\ [\ \texttt{f}\ k = \frac{k}{k+1}\ \to\ \texttt{f}\ (k+1) = \frac{k+1}{k+2}\ ]$$
$$\longrightarrow$$
$$\forall n \geq 1. \texttt{f}\ n = \frac{n}{n+1}$$

Proof Schema

$\forall k \geq 1.$

—

$\forall n \geq 1.\texttt{f}$

Base Case

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

...

Inductive Step

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

Assume that $\boldsymbol{k} \geq 1$.

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

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

Base Case

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

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

Inductive Step

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

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

In Summary

Principle:

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

Technique:
For any arbitrary $m \in \mathbb{Z}$:

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

Strong Induction

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

Example

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

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

$$\land$$

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

$$\longrightarrow$$

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

Proof Schema

$\longrightarrow$

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

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

...

Base Case

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

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

Inductive Step

Inductive Step

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

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

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

1st Case, $k = 0$

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

$g\ (1)$

$= \quad 1 \qquad$ by line 4 in definition of g

$= \quad \ldots \qquad$ rest as exercise

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

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

$g\ (k+1)$

$= \quad 5 * g(k) - 6 * g(k-1) \qquad$ By (A), line 5 of defn. g applies

$= \quad 5 * (3^k - 2^k) - 6 * (3^{k-1} - 2^{k-1}) \qquad$ By (B), and induction hypothesis

$= \quad 5 * (3 * 3^{k-1} - 2 * 2^{k-1}) - 6 * (3^{k-1} - 2^{k-1}) \qquad$ by arithmetic

$= \quad \ldots \qquad$ ....

$= \quad 3^{k+1} - 2^{k+1} \qquad$ by arithmetic

In Summary

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

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

Strong Induction Principle

For any $Q \subseteq \mathbb{Z}$, and $m \in \mathbb{Z}$

$$Q(m) \quad \wedge \quad \forall k : \mathbb{Z}.[\ \forall j \in [m..k].Q(j) \rightarrow Q(k+1)\ ] \quad \longrightarrow \quad \forall n \geq m.Q(n)$$

$\forall n \geq m.Q(n)$ is a shorthand for $\forall n : \mathbb{Z}.[n \geq m \rightarrow Q(n)]$

> ⚠ **Warning**
>
> Write Proof Schemas! You will get marks!

Final Summary

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 $m \in \mathbb{Z}$:

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

Strong Induction:

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

Strong Induction, for $m \in \mathbb{Z}$:

$$P(m) \quad \wedge \quad \forall k \geq m.[\ \forall j \in \underline{[m..k]}.P(j) \ \rightarrow \ P(k+1)\ ] \quad \longrightarrow \quad \forall n \geq m.P(n)$$