Induction

Myrto Arapinis
School of Informatics
University of Edinburgh

October 6, 2014

The principle of (ordinary) induction

Let $P(n)$ be a predicate. If

1. $P(0)$ is true, and
2. $P(n)$ IMPLIES $P(n+1)$ for all non-negative integers n

then

- ▷ $P(m)$ is true for all non-negative integers m

The principle of (ordinary) induction

Let $P(n)$ be a predicate. If

1. $P(0)$ is true, and
2. $P(n)$ IMPLIES $P(n+1)$ for all non-negative integers n

then

- ▷ $P(m)$ is true for all non-negative integers m

1. The first item says that $P(0)$ holds
2. The second item says that $P(0) \rightarrow P(1)$, and $P(1) \rightarrow P(2)$, and $P(2) \rightarrow P(3)$, *etc.*

- ▷ Intuitively, there is a domino effect that eventually shows that $\forall n \in \mathbb{N}.\ P(n)$

Proof by induction

To prove by induction $\forall k \in \mathbb{N}.\ P(k)$ is true, follow these three steps:

Base Case: Prove that $P(0)$ is true

Inductive Hypothesis: Let $k \geq 0$. We assume that $P(k)$ is true

Inductive Step: Prove that $P(k+1)$ is true

Proof by induction

To prove by induction $\forall k \in \mathbb{N}.\ P(k)$ is true, follow these three steps:

Base Case: Prove that $P(0)$ is true

Inductive Hypothesis: Let $k \geq 0$. We assume that $P(k)$ is true

Inductive Step: Prove that $P(k+1)$ is true

Remark

Proofs by mathematical induction do not always start at the integer 0. In such a case, the base case begins at a starting point $b \in \mathbb{Z}$. In this case we prove the property only for integers $\geq b$ instead of for all $n \in \mathbb{N}$

$$\forall k \in \, . \;\; \sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

$\forall k \in \,. \;\; \sum_{i=1}^{k} i = \frac{k(k+1)}{2}$

(By induction) Let $P(k)$ be the predicate "$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$"

Base Case: $\sum_{i=1}^{0} i = 0 = \frac{0(0+1)}{2}$, thus $P(0)$ is true

Inductive Hypothesis: Let $k \geq 0$. We assume that $P(k)$ is true, *i.e.* $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$

Inductive Step:

$$\begin{aligned} \sum_{i=1}^{k+1} i &= \left[\sum_{i=1}^{k} i\right] + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \qquad \text{(by I.H.)} \\ &= \frac{k(k+1)+2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

Thus $P(k+1)$ is true $\square$

$\forall k \in \mathbb{N}.\ k^3 - k$ is divisible by 3

$\forall k \in \mathbb{N}.\ k^3 - k$ is divisible by 3

(By induction) Let $P(k)$ be the predicate "$k^3 - k$ is divisible by 3"

Base Case: Since $0 = 3 \cdot 0$, it is the case that 3 divides $0 = 0^3 - 0$, thus $P(0)$ is true

Inductive Hypothesis: Let $k \geq 0$. We assume that $P(k)$ is true, *i.e.* $k^3 - k$ is divisible by 3

Inductive Step:

$$
\begin{array}{rcll}
(k+1)^3 - (k+1) & = & (k^3 + 3k^2 + 3k + 1) - (k+1) & \\
 & = & k^3 + 3k^2 + 2k & \\
 & = & (k^3 - k) + 3k^2 + 3k & \\
 & = & 3(\ell + k^2 + k) \text{ for some } \ell & \text{(by I.H.)}
\end{array}
$$

Thus $(k+1)^3 - (k+1)$ is divisible by 3. So we can conclude that $P(k+1)$ is true $\square$

$\forall k \geq 4.\ 2^k < k!$

$\forall k \geq 4.\ 2^k < k!$

(By induction) Let $P(k)$ be the predicate "$2^k < k!$"

Base Case: $2^4 = 16 < 24 = 4!$, thus $P(4)$ is true

Inductive Hypothesis: Let $k \geq 4$. We assume that $P(k)$ is true, *i.e.* $2^k < k!$

Inductive Step:
$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &< 2 \cdot k! && \text{(by I.H.)} \\ &< (k+1) \cdot k! && (k \geq 4) \\ &= (k+1)! \end{aligned}$$

Thus $P(k+1)$ is true □

All horses are of the same color

All horses are of the same color

(By induction) Let $P(k)$ be the predicate "in any set of k horses, all the horses are of the same color"

Base Case: In any set of just one horse, all horses obviously have the same color, thus $P(1)$ is true

Inductive Hypothesis: Let $k \geq 1$. We assume that $P(k)$ is true, *i.e.* "in any set of k horses, all the horses are of the same color"

Inductive Step: Let $\{H_1, H_2, \ldots, H_{k+1}\}$ be a set of $k+1$ horses. Then, by I.H., all the horses in $\{H_1, H_2, \ldots, H_k\}$ have the same color. Similarly, by I.H., all the horses in $\{H_2, \ldots, H_{k+1}\}$ have the same color. Thus $col(H_1) = col(H_2) = col(H_{k+1})$. But this implies that all the $k+1$ horses are of the same color. Thus, $P(k+1)$ is true. $\square$

All horses are of the same color

(By induction) Let $P(k)$ be the predicate "in any set of k horses, all the horses are of the same color"

Base Case: In any set of just one horse, all horses obviously have the same color, thus $P(1)$ is true

Inductive Hypothesis: Let $k \geq 1$. We assume that $P(k)$ is true, *i.e.* "in any set of k horses, all the horses are of the same color"

Inductive Step: Let $\{H_1, H_2, \ldots, H_{k+1}\}$ be a set of $k+1$ horses. Then, by I.H., all the horses in $\{H_1, H_2, \ldots, H_k\}$ have the same color. Similarly, by I.H., all the horses in $\{H_2, \ldots, H_{k+1}\}$ have the same color. Thus $col(H_1) = col(H_2) = col(H_{k+1})$. But this implies that all the $k+1$ horses are of the same color. Thus, $P(k+1)$ is true. $\square$

!!!The inductive step is not true for k=1!!!

The principle of strong induction

Let $P(n)$ be a predicate. If

1. $P(0)$ is true, and
2. $P(0) \land \cdots \land P(n)$ IMPLIES $P(n+1)$ for all non-negative integers n

then

- ▷ $P(m)$ is true for all non-negative integers m

- Intuitively, there is a domino effect that eventually shows that $\forall n \in \mathbb{N}.\ P(n)$
- Strong induction sometimes makes the proof of the inductive step much easier since we assume a stronger statement

Every natural number $k > 1$ can be written as a product of primes

(By induction) Let $P(k)$ be the predicate "k can be written as a product of primes"

Base Case: Since 2 is a prime number, $P(2)$ is true

Inductive Hypothesis: Let $k \geq 1$. We assume that $P(k)$ is true, *i.e.* "k can be written as a product of primes"

Inductive Step: We distinguish two cases: *(i)* Case $k + 1$ is a prime, then $P(k + 1)$ is true; *(ii)* Case $k + 1$ is not a prime. Then by definition of primality, there must exist $1 < n, m < k + 1$ such that $k + 1 = n \cdot m$. But then we know by I.H. that n and m can be written as a product of primes (since $n, m \leq k$). Therefore, $k + 1$ can also be written as a product of primes. Thus, $P(k + 1)$ is true

□

Every natural number $k > 1$ can be written as a product of primes

(By induction) Let $P(k)$ be the predicate "k can be written as a product of primes"

Base Case: Since 2 is a prime number, $P(2)$ is true

Inductive Hypothesis: Let $k \geq 1$. We assume that $P(k)$ is true, *i.e.* "k can be written as a product of primes"

Inductive Step: We distinguish two cases: *(i)* Case $k + 1$ is a prime, then $P(k + 1)$ is true; *(ii)* Case $k + 1$ is not a prime. Then by definition of primality, there must exist $1 < n, m < k + 1$ such that $k + 1 = n \cdot m$. But then we know by I.H. that n and m can be written as a product of primes (since $n, m \leq k$). Therefore, $k + 1$ can also be written as a product of primes. Thus, $P(k + 1)$ is true
$\square$

$\longrightarrow$ If we had only assumed $P(k)$ to be true, then we could not apply our I.H. to n and m

Well-founded relations

Definition

A binary relation $R \subseteq X \times X$ is well-founded iff every non-empty subset $S \subseteq X$ has a minimal element *w.r.t.*

$$\forall S \subseteq X.\ (S \neq \emptyset \rightarrow \forall s \in S.\ (s, m) \in R)$$

- Intuitively, R does not contain any infinite descending chains (However, it may still contain infinite increasing chains)
- Note that in the general definition above the relation R does not need to be transitive.

Examples of well-founded relations

- $(\mathbb{N}, <)$ - The strict order on the natural numbers
- $\mathbb{Z}^+$ where xRy is defined by $x|y$ and $x \neq y$
- Σ^* - The set of all finite strings over a fixed alphabet Σ, with xRy defined by the property that x is a proper substring of y
- The set $\mathbb{N} \times \mathbb{N}$ of pairs of natural numbers, with $(n_1, n_2)R(m_1, m_2)$ if and only if $n_1 < m_1$ and $n_2 < m_2$
- The set of trees with R defined as "is a proper subtree of"
- Recursively-defined data structures with R defined as "is used as a part in the construction of"

Well-founded induction principle

- Idea of ordinary and strong induction: from properties of "smaller" elements, we prove properties of "larger" elements
- Idea of well-founded relations: generalise induction to well-founded sets

Let R be a well-founded relation on X, and let $P(x)$ be a predicate over elements in X
If $\forall x \in X.\ ((\forall y \in X.\ yRx \rightarrow P(y)) \rightarrow P(x))$
Then $\forall x \in X.\ P(x)$

(Structural) Induction over binary trees

Trees are a fundamental data structure in computer science: databases, graphics, compilers, editors, optimization, game-playing

Definition (Full binary tree)

Let A be a set of atoms. We recursively define full binary trees ($\mathcal{T}$) as follows:

- Every atom is a tree - $\forall a \in A.\ a \in \mathcal{T}$
- Consing any two trees gives a tree - $\forall t_1, t_2 \in \mathcal{T}.\ (t_1 \bullet t_2 \in \mathcal{T})$

where $n(t)$ is the number of

(Structural) Induction over binary trees

Trees are a fundamental data structure in computer science: databases, graphics, compilers, editors, optimization, game-playing

Definition (Full binary tree)

Let A be a set of atoms. We recursively define full binary trees ($\mathcal{T}$) as follows:

- Every atom is a tree - $\forall a \in A.\ a \in \mathcal{T}$
- Consing any two trees gives a tree - $\forall t_1, t_2 \in \mathcal{T}.\ (t_1 \bullet t_2 \in \mathcal{T})$

where $n(t)$ is the number of

Full binary tree induction

For any predicate $P(t)$,
If $\forall a \in A.\ P(a)$
And $\forall t_1, t_2 \in \mathcal{T}.\ (P(t_1) \wedge P(t_2) \rightarrow P(t_1 \bullet t_2))$
Then $\forall t \in \mathcal{T}.\ P(t)$

Functions on full binary trees

Definition ($h(t)$)

The height $h(t)$ of a full binary tree $t \in \mathcal{T}$ is defined recursively as follows:

- The height of a full binary tree t consisting of only a root r is $h(t) = 0$
- If t_1 and t_2 are full binary trees, then the full binary tree $t = t_1 \bullet t_2$ has height $h(t) = 1 + \max(h(t_1), h(t_2))$

Definition ($n(t)$)

The number of vertices $n(t)$ of a full binary tree t is defined recursively as follows:

- The number of vertices $n(t)$ of a full binary tree t consisting of only a root r is $n(t) = 1$
- If t_1 and t_2 are full binary trees, then the full binary tree $t = t_1 \bullet t_2$ has number of vertices $n(t) = 1 + n(t_1) + n(t_2)$

(Structural) Induction over binary trees

Theorem

If t is a full binary tree, then $n(T) \leq 2^{h(t)+1} - 1$

Proof by structural induction

Base Case: The result holds for a full binary tree t consisting only of a root by definition: $n(t) = 1 \leq 2^1 - 1 = 1$

Recursive step: We assume $(t_1)2h^{(t_1)+1} - 1$ and also $(t_2)2h^{(t_2)+1} - 1$ whenever t_1 and t_2 are full binary trees. Let $t = t_1 \bullet t_2$

$$
\begin{aligned}
n(t) &= 1 + n(t_1) + n(t_2 2) && \text{(by definition of } n(t)\text{)} \\
&\leq 1 + (2^{h(t_1)+1} - 1) + (2^{h(t_2)+1} - 1) && \text{(by I.H.)} \\
&\leq 2 \cdot \max(2^{h(t_1)+1}, 2^{h(t_2)+1}) - 1 \\
&= 2 \cdot 2^{\max(h(t_1), h(t_2))+1} - 1 \\
&= 2 \cdot 2^{h(t)} - 1 && \text{by definition of } h(t) \\
&= 2^{h(t)+1} - 1
\end{aligned}
$$

Example

Let S be the set defined as follows:

- Basis step: $(0, 0) \in S$
- Recursive Step: If $(x, y) \in S$, then $(x, y + 1) \in S$, $(x + 1, y + 1) \in S$, and $(x + 2, y + 1) \in S$

Prove that $\forall (a, b) \in S.\ a \leq 2b$

Proof (by (strong) structural induction) We consider the lexicographic oreder on pairs.
Base Case: $0 \leq 2 \cdot 0$
Recursive Case: Let $(a, b) \in S$. We assume that for all $(a', b') \in S$, $a' \leq 2 \cdot b'$. By definition of S we know that if $(a, b) \in S$, then there exists $(a', b') \in S$ such that (a, b) is obtained by applying one of the three possibilities to (a', b'). We distinguish these three possibilities.

Example (continued)

Case $(a, b) = (a', b' + 1)$. By inductive hypothesis, we know that $a' \leq 2b'$, but then it must be that $a' \leq 2b' + 1 < 2b' + 2 = 2b$

Case $(a, b) = (a' + 1, b' + 1)$. By inductive hypothesis, we know that $a' \leq 2b'$, but then it must be that
$a = a' + 1 \leq 2b' + 1 < 2b' + 2 = 2b$

Case $(a, b) = (a' + 2, b' + 1)$. By inductive hypothesis, we know that $a' \leq 2b'$, but then it must be that $a = a' + 2 \leq 2b' = 2b$