Discrete Mathematics, Chapter 5: Induction and Recursion

Richard Mayr

University of Edinburgh, UK

Outline

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 wrt. R.

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

- In ZFC this is equivalent to the property that 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.
- A partial order relation is called well-founded iff the corresponding strict order (i.e., without the reflexive part) is well-founded.

Well-founded Relations: Examples

Clicker

Which of these relations is well-founded? (Why?)

1. $<$ on $\mathbb{R}^+$
2. $<$ on $\mathbb{Z}$
3. $<$ on $\mathbb{Z}^+ \times \mathbb{Z}^+$
4. $<$ on $\mathbb{R}^+ - \mathbb{Q}$
5. $<$ on $\mathbb{Q}^+ - \mathbb{Z}$

Well-founded Relations: Examples

Clicker

Which of these relations is well-founded? (Why?)

1. $<$ on $\mathbb{R}^+$
2. $<$ on $\mathbb{Z}$
3. $<$ on $\mathbb{Z}^+ \times \mathbb{Z}^+$
4. $<$ on $\mathbb{R}^+ - \mathbb{Q}$
5. $<$ on $\mathbb{Q}^+ - \mathbb{Z}$

Which of these relations is **not** well-founded? (Why?)

1. $\{(x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid x|y \wedge x \neq y\}$
2. $\subsetneq$ on $2^{\mathbb{N}}$
3. $\in$ on $2^{\mathbb{R}}$
4. Cardinality of sets on $2^{\mathbb{N}}$
   $\{(A, B) \mid A, B \subseteq \mathbb{N} \wedge |A| < |B|\}$

Well-founded Induction

- Given a well-founded relation R on X, and a property P of elements of X.
- We want to show that P holds for all elements $x \in X$, i.e., $\forall x \in X.\, P(x)$.
- It suffices to show the following:
  If $x \in X$ and $P(y)$ is true for all y such that yRx (i.e., for all "smaller" y), then $P(x)$ must also be true.
  Formally

$$\forall x \in X\, [(\forall y \in X\, (y\, R\, x \rightarrow P(y))) \rightarrow P(x)] \rightarrow \forall x \in X\, P(x)$$

- Why is that correct?
  If you negate the formula above, you could construct an infinite decreasing chain $\dots x_3 R x_2 R x_1 R x_0$ with $\forall i.\, \neg P(x_i)$.
  This contradicts the well-foundedness of R.

Examples of well-founded relations

- $(\mathbb{N}, <)$. The strict order on the natural numbers.
- $\mathbb{Z}^+$ where $x\,R\,y$ is defined by $x|y$ and $x \neq y$.
- Σ^*, the set of all finite strings over a fixed alphabet Σ, with $x\,R\,y$ 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".

Special case: Mathematical Induction

Here we have $R = \{(n, n+1) \mid n \in \mathbb{N}\}$ well-founded on $\mathbb{N}$.

Principle of Mathematical Induction: To prove that $P(n)$ is true for all $n \in \mathbb{N}$, we complete these steps:

Basis Step: Show that $P(0)$ is true.
(In the instantiation of the formula for well-founded induction this is the only case where there are no R-“smaller” elements y.)

Inductive Step: Show that $P(k) \rightarrow P(k+1)$ is true for all $k \in \mathbb{N}$.

To complete the inductive step, we assume the inductive hypothesis that $P(k)$ holds for an arbitrary integer k, and then, under this assumption, show that $P(k+1)$ must be true.

Note: Proofs by mathematical induction do not always start at the integer 0. In such a case, the basis step begins at a starting point b where b is an integer. In this case we prove the property only for integers $\geq b$ instead of for all of $\mathbb{N}$.

Proving a Summation Formula by Mathematical Ind.

Show that the following property $P(n)$ that

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

is true for all $n \geq 1$.

Basis step: $P(1)$ is true since $1 = 1(1+1)/2$.

Inductive step: Assume that $P(k)$ is true, i.e., the inductive hypothesis

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

Under this assumption we have

$$\begin{aligned} \sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} i + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1)+2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

Proving Inequalities by Mathematical Induction

Example: Use mathematical induction to prove that $2^n < n!$ for every integer $n \geq 4$.
Solution: Let $P(n)$ be the proposition that $2^n < n!$.
Basis step: $P(4)$ is true since $2^4 = 16 < 4! = 24$.
Inductive step: Assume $P(k)$ holds, i.e., $2^k < k!$ for an arbitrary integer $k \geq 4$. To show that $P(k+1)$ holds:

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &< 2 \cdot k! \quad \text{by the inductive hypothesis} \\ &< (k+1)k! \\ &= (k+1)! \end{aligned}$$

Therefore, $2^n < n!$ holds, for every integer $n \geq 4$.
Note that the basis step is $P(4)$, since $P(0), \ldots, P(3)$ are all false.

Guidelines: Mathematical Induction Proofs

Template for Proofs by Mathematical Induction

1. Express the statement that is to be proved in the form "for all $n \geq b$, $P(n)$" for a fixed integer b.
2. Write out the words "Basis Step." Then show that $P(b)$ is true, taking care that the correct value of b is used. This completes the first part of the proof.
3. Write out the words "Inductive Step."
4. State, and clearly identify, the inductive hypothesis, in the form "assume that $P(k)$ is true for an arbitrary fixed integer $k \geq b$."
5. State what needs to be proved under the assumption that the inductive hypothesis is true. That is, write out what $P(k+1)$ says.
6. Prove the statement $P(k+1)$ making use the assumption $P(k)$. Be sure that your proof is valid for all integers k with $k \geq b$, taking care that the proof works for small values of k, including $k = b$.
7. Clearly identify the conclusion of the inductive step, such as by saying "this completes the inductive step."
8. After completing the basis step and the inductive step, state the conclusion, namely that by mathematical induction, $P(n)$ is true for all integers n with $n \geq b$.

Strong Induction

Here we have $R = <$, the usual "strictly smaller than" ordering on $\mathbb{N}$.

To prove that $P(n)$ is true for all $n \geq 0$, complete two steps:

Basis Step: Verify that the proposition $P(0)$ is true.

Inductive Step: Show the conditional statement
$[P(0) \wedge P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$
holds for all integers $k \geq 0$.

Note: Compared to mathematical induction, strong induction has a stronger induction hypothesis. You assume not only $P(k)$ but even $[P(0) \wedge P(1) \wedge P(2) \wedge \cdots \wedge P(k)]$ to then prove $P(k+1)$.

Again the base case can be above 0 if the property is proven only for a subset of $\mathbb{N}$.

Proof of the Fundamental Theorem of Arithmetic, using Strong Induction

Show that if n is an integer ≥ 2, then n can be written as the product of primes.

Solution: Let $P(n)$ be the proposition that n can be written as a product of primes.

Basis step: $P(2)$ is true since 2 itself is prime.

Inductive step: The inductive hypothesis is that $P(j)$ is true for all integers j with $2 \leq j \leq k$.

To show that $P(k+1)$ must be true under this assumption, two cases need to be considered:

- If $k+1$ is prime, then $P(k+1)$ is trivially true.
- Otherwise, $k+1$ is composite and can be written as the product of two positive integers a and b with $2 \leq a \leq b < k+1$.
  By the inductive hypothesis a and b can be written as the product of primes and therefore $k+1$ can also be written as the product of those primes.

Recursively Defined Functions

Definition

A recursive or inductive definition of a function consists of two steps.

Basis step: Specify the value of the function at zero.

Recursive step: Give a rule for finding its value at an integer from its values at smaller integers.

A function $f : \mathbb{N} \to \mathbb{N}$ corresponds to sequence $a_0, a_1, \ldots$ where $a_i = f(i)$. (Remember the recurrence relations in Chapter 2.4.).

Example: Give a recursive definition of the factorial function $n!$.

Recursively Defined Functions

Definition

A recursive or inductive definition of a function consists of two steps.

Basis step: Specify the value of the function at zero.

Recursive step: Give a rule for finding its value at an integer from its values at smaller integers.

A function $f : \mathbb{N} \rightarrow \mathbb{N}$ corresponds to sequence $a_0, a_1, \ldots$ where $a_i = f(i)$. (Remember the recurrence relations in Chapter 2.4.).

Example: Give a recursive definition of the factorial function $n!$.

$$\begin{aligned} f(0) &= 1 \\ f(n+1) &= (n+1) \cdot f(n) \end{aligned}$$

Recursively Defined Functions

Definition

A recursive or inductive definition of a function consists of two steps.

Basis step: Specify the value of the function at zero.

Recursive step: Give a rule for finding its value at an integer from its values at smaller integers.

A function $f : \mathbb{N} \to \mathbb{N}$ corresponds to sequence $a_0, a_1, \ldots$ where $a_i = f(i)$. (Remember the recurrence relations in Chapter 2.4.).

Example: Give a recursive definition of the factorial function $n!$.

$$\begin{aligned} f(0) &= 1 \\ f(n+1) &= (n+1) \cdot f(n) \end{aligned}$$

Example: Fibonacci numbers. $f(0) = 0$, $f(1) = 1$ and $f(n+2) = f(n+1) + f(n)$.

Recursively Defined Sets and Structures

Recursive definitions of sets have two parts:

- The basis step specifies an initial collection of elements.
- The recursive step gives the rules for forming new elements in the set from those already known to be in the set.

Sometimes the recursive definition has an exclusion rule, which specifies that the set contains nothing other than those elements specified in the basis step and generated by applications of the rules in the recursive step.
We will always assume that the exclusion rule holds, even if it is not explicitly mentioned.
We will later develop a form of induction, called structural induction, to prove results about recursively defined sets.

Recursively Defined Sets and Structures

Example: A subset of Integers S:

Basis step: $3 \in S$.

Recursive step: If $x \in S$ and $y \in S$, then $x + y \in S$.

Initially 3 is in S, then $3 + 3 = 6$, then $3 + 6 = 9$, etc.

Example: The natural numbers $\mathbb{N}$.

Basis step: $0 \in \mathbb{N}$.

Recursive step: If $n \in \mathbb{N}$ then $n + 1 \in \mathbb{N}$.

Example: The set Σ^* of strings over alphabet Σ.

Basis step: $\lambda \in \Sigma^*$. (λ is the empty string.)

Recursive step: If $w \in \Sigma^*$ and $x \in \Sigma$ then $wx \in \Sigma^*$.

Well-Formed Formulae in Propositional Logic

Define the set of well-formed formulae in propositional logic involving T, F, propositional variables, and operators from the set $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$.

Basis step: T, F, and s, where s is a propositional variable, are well-formed formulae.

Recursive step: If E and F are well formed formulae, then $(\neg E)$, $(E \wedge F)$, $(E \vee F)$, $(E \rightarrow F)$, $(E \leftrightarrow F)$, are well-formed formulae.

Example: $((p \vee q) \rightarrow (q \wedge F))$ is a well-formed formula.
$pq\wedge$ is not a well-formed formula.

Full Binary Trees

Definition

The set of full binary trees can be defined recursively by these steps.

Basis step: There is a full binary tree consisting of only a single vertex r.

Recursive step: If T_1 and T_2 are disjoint full binary trees, there is a full binary tree, denoted by $T_1 \cdot T_2$, consisting of a root r together with edges connecting the root to each of the roots of the left subtree T_1 and the right subtree T_2.

Structural Induction

Here we instantiate well-founded induction with a relation R defined as "is used as a part in the recursive step of the construction of".

To prove a property of the elements of a recursively defined set, we use structural induction.

Basis step: Show that the property holds for all elements specified in the basis step of the recursive definition.

Recursive step: Show that if the property is true for each of the parts used to construct new elements in the recursive step of the definition, then the property also holds for these new elements.

Functions on Full Binary Trees

Definition

The **height** $h(T)$ of a full binary tree T is defined recursively as follows:

Basis step: The height of a full binary tree T consisting of only a root r is $h(T) = 0$.

Recursive step: If T_1 and T_2 are full binary trees, then the full binary tree $T = T_1 \cdot T_2$ has height $h(T) = 1 + \max(h(T_1), h(T_2))$.

Definition

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

Basis step: The number of vertices $n(T)$ of a full binary tree T consisting of only a root r is $n(T) = 1$.

Recursive step: If T_1 and T_2 are full binary trees, then the full binary tree $T = T_1 \cdot T_2$ has number of vertices $n(T) = 1 + n(T_1) + n(T_2)$.

Structural Induction on Binary Trees

Theorem

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

Proof by structural induction.
Basis step: The result holds for a full binary tree consisting only of a root. $n(T) = 1$ and $h(T) = 0$. Hence, $n(T) = 1 \leq 2^{0+1} - 1 = 1$.
Recursive step: By induction hypothesis we assume $n(T_1) \leq 2^{h(T_1)+1} - 1$ and also $n(T_2) \leq 2^{h(T_2)+1} - 1$ whenever T_1 and T_2 are full binary trees.

$$\begin{aligned}
n(T) &= 1 + n(T_1) + n(T_2) \quad \text{(by the recursive formula of n(T))} \\
&\leq 1 + (2^{h(T_1)+1} - 1) + (2^{h(T_2)+1} - 1) \quad \text{(by inductive hypothesis)} \\
&\leq 2 \cdot \max(2^{h(T_1)+1}, 2^{h(T_2)+1}) - 1 \\
&= 2 \cdot 2^{max(h(T_1),h(T_2))+1} - 1 \\
&= 2 \cdot 2^{h(T)} - 1 \quad \text{by the recursive definition of } h(T) \\
&= 2^{h(T)+1} - 1
\end{aligned}$$