Mathematics, KTH
Bengt Ek
November 2015

Supplementary material for SF2736, Discrete mathematics:

Induction and recursion

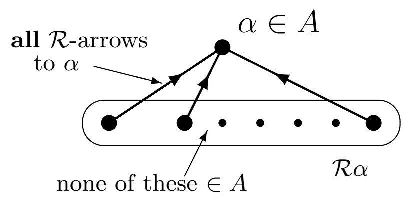
On well-founded binary relations

Let $\mathcal{R}$ be a binary relation on a set $\mathcal{D}$. As usual, we write $\alpha\mathcal{R}\beta$ to express that $\alpha \in \mathcal{D}$ is related to $\beta \in \mathcal{D}$.

We already know the properties **reflexivity**, **symmetry**, and **transitivity** for binary relations. We shall now introduce another important property, that of **well-foundedness**.

Notation:
For $\alpha \in \mathcal{D}$, let $\boldsymbol{\mathcal{R}\alpha = \{\xi \in \mathcal{D} \mid \xi\mathcal{R}\alpha\}}$.

$\boldsymbol{\alpha}$ $\boldsymbol{\mathcal{R}}$-minimal in $\boldsymbol{A}$:



Definition:
The element $\alpha \in A \subseteq \mathcal{D}$ is **$\boldsymbol{\mathcal{R}}$-minimal in $\boldsymbol{A}$** iff there is no $\xi \in A$ with $\xi\mathcal{R}\alpha$, i.e., iff $A \cap \mathcal{R}\alpha = \varnothing$.

Definition:
The relation $\mathcal{R}$ on $\mathcal{D}$ is **well-founded** (Sw. välgrundad) iff
for all $\boldsymbol{A \subseteq \mathcal{D}}$, $\boldsymbol{A \neq \varnothing}$ there is $\alpha \in A$ which is **$\boldsymbol{\mathcal{R}}$-minimal in $\boldsymbol{A}$**.

A **well-order** is the same as a well-founded total order.

Examples of well-founded relations:

- $\mathcal{D} = \mathbb{N}$, $\alpha\mathcal{R}\beta$ means $\beta = \alpha + 1$
- $\mathcal{D} = \mathbb{N}$, $\alpha\mathcal{R}\beta$ means $\alpha < \beta$
- $\mathcal{D} = \mathbb{N}$, $\alpha\mathcal{R}\beta$ means $\alpha \mid \beta$ and $\alpha \neq \beta$
- $\mathcal{D} = \mathcal{P}_{fin}(\mathbb{N})$ (the set of all finite subsets of $\mathbb{N}$), $\alpha\mathcal{R}\beta$ means $\alpha \subset \beta$

$\mathcal{R}$ of the first two examples are well-founded because every non-empty subset of $\mathbb{N}$ has a least element. In the third example, the least non-zero number of a set A (if there is one) is $\mathcal{R}$-minimal in A and if $A = \{0\}$, 0 is $\mathcal{R}$-minimal in A. In the final example, an $\alpha \in A$ with a minimal number of elements is $\mathcal{R}$-minimal in A.
In the second example, there is exactly one $\mathcal{R}$-minimal element in every $A \subseteq \mathcal{D}$, but in the others there are several such elements in some $A \subseteq \mathcal{D}$.

Examples of non-well-founded relations:

- $\mathcal{D} = \mathbb{Z}$, $\alpha \mathcal{R} \beta$ means $\beta = \alpha + 1$
- $\mathcal{D} = \mathbb{Z}$, $\alpha \mathcal{R} \beta$ means $\alpha < \beta$
- $\mathcal{D} = \mathbb{N}$, $\alpha \mathcal{R} \beta$ means $\alpha > \beta$ (so $\mathcal{R}$-minimal means maximal in the ordinary sense)
- $\mathcal{D} = \{x \in \mathbb{Q} \mid 0 \le x\}$, $\alpha \mathcal{R} \beta$ means $\alpha < \beta$
- $\mathcal{D} = \mathcal{P}(\mathbb{N})$, $\alpha \mathcal{R} \beta$ means $\alpha \subset \beta$
- $\mathcal{D} = \{\alpha, \beta, \gamma\}$, $\mathcal{R} = \{\langle \alpha, \beta \rangle, \langle \beta, \gamma \rangle, \langle \gamma, \alpha \rangle\}$

Examples of $A \subseteq \mathcal{D}$, $A \neq \varnothing$, without $\mathcal{R}$-minimal elements in these examples are $\mathcal{D}$, $\mathcal{D}$, $\mathcal{D}$, $\mathcal{D} \setminus \{0\}$, $\{\mathbb{N} \setminus \{0, 1, \ldots, n\} \mid n \in \mathbb{N}\}$ and $\mathcal{D}$.

Proposition:
If the relation $\mathcal{R}$ on $\mathcal{D}$ is well-founded and the relation $\mathcal{R}_1$ on $\mathcal{D}_1 \subseteq \mathcal{D}$ is such that $\alpha \mathcal{R}_1 \beta \Rightarrow \alpha \mathcal{R} \beta$ for all $\alpha, \beta \in \mathcal{D}_1$ (i.e., $\mathcal{R}_1 \subseteq \mathcal{R}$), then $\mathcal{R}_1$ on $\mathcal{D}_1$ is also well-founded.

Pf: If $\varnothing \neq A \subseteq \mathcal{D}_1$ and α is $\mathcal{R}$-minimal in A, α is $\mathcal{R}_1$-minimal in A. $\square$

So, if a relation is not well-founded, it is because "there are too many arrows". If you take away arrows and/or elements from a well-founded relation, the resulting relation is always well-founded.

Proposition:
A relation $\mathcal{R}$ on $\mathcal{D}$ is well-founded iff there is no sequence $\alpha_0, \alpha_1, \alpha_2, \ldots$ with $\alpha_{i+1} \mathcal{R} \alpha_i$ for all $i = 0, 1, 2, \ldots$.

This characterization of well-founded relations is often easier to verify than the definition. The well-founded relations are exactly those without a *cycle* (you can't come back to an element by following arrows backwards from it) or an *infinite backward chain* (if you follow arrows backwards it must come to a stop in a finite number of steps). There may, however, exist infinite forward chains, for instance any infinite ascending sequence in $\mathbb{N}$ with $<$ as $\mathcal{R}$.

Exercises

Wf1) Prove the second proposition above. (To prove "if" a so-called **axiom of choice** is needed, i.e., one has to assume that infinitely many choices can be made to find the α_i.)

Wf2) Let $\mathcal{R}_1$, $\mathcal{R}_2$ be well-founded relations on $\mathcal{D}_1$, $\mathcal{D}_2$ (with $\mathcal{D}_1 \cap \mathcal{D}_2 = \varnothing$). The relation $\mathcal{R}$ on $\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2$ is defined so that if $\alpha \mathcal{R} \beta$ then either $\alpha \in \mathcal{D}_1$ and $\beta \in \mathcal{D}_2$ or $\alpha, \beta \in \mathcal{D}_i$ and $\alpha \mathcal{R}_i \beta$ for $i = 1$ or 2.
Show that $\mathcal{R}$ is well-founded.

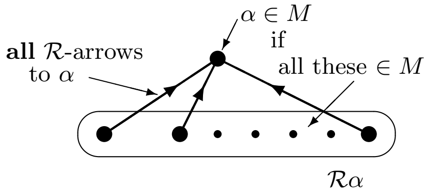
Wf3) Let $\mathcal{R}_1$, $\mathcal{R}_2$ be well-founded relations on $\mathcal{D}_1$, $\mathcal{D}_2$.
The relation $\mathcal{R}$ on $\mathcal{D} = \mathcal{D}_1 \times \mathcal{D}_2 = \{\langle \alpha_1, \alpha_2 \rangle \mid \alpha_i \in \mathcal{D}_i\}$ is given by $\langle \alpha_1, \alpha_2 \rangle \mathcal{R} \langle \beta_1, \beta_2 \rangle$ iff either $\alpha_2 \mathcal{R}_2 \beta_2$ or both $\alpha_2 = \beta_2$ and $\alpha_1 \mathcal{R}_1 \beta_1$.
Show that $\mathcal{R}$ is well-founded.

$\mathcal{R}$-induction and $\mathcal{R}$-recursion

Now for the reason why well-foundedness is such an important property of binary relations. We shall prove that the relation $\mathcal{R}$ can be used for proofs by induction and definitions of functions by recursion iff $\mathcal{R}$ is well-founded.

Definition:
The set $M \subseteq \mathcal{D}$ is called **$\mathcal{R}$-inductive** iff
for all $\boldsymbol{\alpha \in \mathcal{D}}$: $\boldsymbol{\mathcal{R}\alpha \subseteq M \Rightarrow \alpha \in M}$.

***M* $\mathcal{R}$-inductive:**



That means that $M \subseteq \mathcal{D}$ is $\mathcal{R}$-inductive iff
M:s complement $M^c = \{\xi \in \mathcal{D} \mid \xi \notin M\}$
has no $\mathcal{R}$-minimal element.

So, the definition of well-foundedness can be formulated thus:

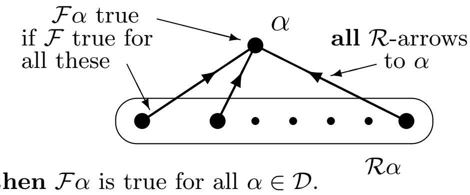
Theorem:
$\mathcal{R}$ is well-founded iff $\mathcal{D}$ is **the only $\mathcal{R}$-inductive** subset of $\mathcal{D}$.

By taking M as the set of $\alpha \in \mathcal{D}$ with a property $\mathcal{F}$ we get

Theorem ($\mathcal{R}$-induction):
If $\mathcal{R}$ is well-founded **and** for all $\alpha \in \mathcal{D}$:
$$\mathcal{F}\beta \text{ for all } \beta \in \mathcal{R}\alpha \Rightarrow \mathcal{F}\alpha$$
then $\mathcal{F}\alpha$ is true for all $\alpha \in \mathcal{D}$.

To prove $\mathcal{F}\alpha$ for all $\alpha \in \mathcal{D}$, one can always assume $\mathcal{F}\beta$ for all $\beta \in \mathcal{R}\alpha$!

$\mathcal{R}$-induction:
If for all $\alpha \in \mathcal{D}$:



then $\mathcal{F}\alpha$ is true for all $\alpha \in \mathcal{D}$.

Conversely, if $\mathcal{R}$ is not well-founded, there is a set $M \subseteq \mathcal{D}$, $M \neq \varnothing$ without an $\mathcal{R}$-minimal element. If $\mathcal{F}$ is true iff $\alpha \in M^c$, it is true for all $\alpha \in \mathcal{D}$ that $\mathcal{F}\beta$ for all $\beta \in \mathcal{R}\alpha \Rightarrow \mathcal{F}\alpha$, but if $\alpha \in M \neq \varnothing$, then $\mathcal{F}\alpha$ is false.

So, $\mathcal{R}$ is well-founded **iff** $\mathcal{R}$-induction works for all properties $\mathcal{F}$ on $\mathcal{D}$.

Examples of $\mathcal{R}$-induction:

- $\mathcal{D} = \mathbb{N}$, $\alpha\mathcal{R}\beta$ means $\beta = \alpha + 1$, gives "ordinary" induction over $\mathbb{N}$. To prove a statement one shows it to be true for 0 (since it certainly is true for all α with $\alpha\mathcal{R}0$) and that it is true for $k + 1$ if it is true for k.
- $\mathcal{D} = \mathbb{N}$, $\alpha\mathcal{R}\beta$ means $\alpha < \beta$, gives so-called "strong induction" over $\mathbb{N}$. To prove the statement for n one may assume it for all $k < n$.
- $\mathcal{D} = \mathbb{Q}$, the rational numbers, $\alpha\mathcal{R}\beta$ means $\alpha < \beta$. $\mathcal{R}$ is not a well-ordered relation and the property $\mathcal{F}\alpha :\ \alpha \leq 0$ satisfies that $\mathcal{F}\beta$ for all $\beta < \alpha \Rightarrow \mathcal{F}\alpha$ for all $\alpha \in \mathcal{D}$, but $\mathcal{F}\alpha$ is not true for all $\alpha \in \mathcal{D}$.

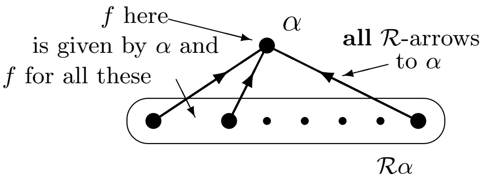
As usual **induction** (to prove statements) is closely related to **recursion** (to define functions). To decide if statements are true or false is to define a function which takes truth values, so induction can be considered a special case of recursion. On the other hand, induction is used to prove the theorem below about recursion.

Let $g(\alpha, h)$ be defined for $\alpha \in \mathcal{D}$ and $h : \mathcal{R}\alpha \to Y$.

Definition:
$f : \mathcal{D} \to Y$ is **$\boldsymbol{\mathcal{R}}$-recursive** (with g) iff for all $\alpha \in \mathcal{D}$

$$\boldsymbol{f(\alpha) = g(\alpha, f|_{\mathcal{R}\alpha})}.$$

***f* $\boldsymbol{\mathcal{R}}$-recursive** if for all $\alpha \in \mathcal{D}$:



$f|_{\mathcal{R}\alpha} : \mathcal{R}\alpha \to Y$ is the **restriction** of f to $\mathcal{R}\alpha$, defined by
$f|_{\mathcal{R}\alpha}(\xi) = f(\xi)$, all $\xi \in \mathcal{R}\alpha$.

Then for each g we have the important

Theorem ($\boldsymbol{\mathcal{R}}$-recursion):
If $\mathcal{R}$ is well-founded there is **exactly one** $\mathcal{R}$-recursive (with g) function on $\mathcal{D}$.

The idea of the proof is to use $\mathcal{R}$-induction over α to prove that $f(\alpha)$ is determined uniquely by the reursion condition. To make that meaningfull, we need

Definition:
$A \subseteq \mathcal{D}$ is said to be **$\boldsymbol{\mathcal{R}}$-hereditary** (Sw. ärftlig) iff for all $\alpha \in A$, $\mathcal{R}\alpha \subseteq A$.

We note that:

- Arbitrary unions of $\mathcal{R}$-hereditary sets are $\mathcal{R}$-hereditary.
  If $\alpha \in \bigcup_\iota A_\iota$, where A_ι are all $\mathcal{R}$-hereditary, $\alpha \in A_\kappa$ for some κ, so $\mathcal{R}\alpha \subseteq A_\kappa$ and thus $\mathcal{R}\alpha \subseteq \bigcup_\iota A_\iota$. □
- Arbitrary intersections of $\mathcal{R}$-hereditary sets are $\mathcal{R}$-hereditary.
  If $\alpha \in \bigcap_\iota A_\iota$, where A_ι are all $\mathcal{R}$-hereditary, $\alpha \in A_\iota$ for all ι, so $\mathcal{R}\alpha \subseteq A_\iota$, all ι, and thus $\mathcal{R}\alpha \subseteq \bigcap_\iota A_\iota$. □
- If for every $\beta \in \mathcal{R}\alpha$ there is an $\mathcal{R}$-hereditary set A_β with $\beta \in A_\beta$, $A_\alpha = \{\alpha\} \cup \bigcup_{\beta \in \mathcal{R}\alpha} A_\beta$ is an $\mathcal{R}$-hereditary set with $\alpha \in A_\alpha$.
  For all $\gamma \in A_\beta$ for some $\beta \in \mathcal{R}\alpha$, $\mathcal{R}\gamma \subseteq A_\alpha$ (since A_β is $\mathcal{R}$-hereditary) and $\mathcal{R}\alpha \subseteq A_\alpha$ (by the construction of A_α and since $\beta \in A_\beta$). □

Proof of the theorem on $\mathcal{R}$-recursion:
Given are a well-founded relation $\mathcal{R}$ on $\mathcal{D}$ and a function $g(\alpha, h)$.
1. **Uniqueness:** If $A \subseteq \mathcal{D}$ is $\mathcal{R}$-hereditary and f_1 and f_2 are functions $A \to Y$ which for all $\alpha \in A$ satisfy

$$f(\alpha) = g(\alpha, f|_{\mathcal{R}\alpha}), \qquad (*)$$

then $f_1(\alpha) = f_2(\alpha)$ for all $\alpha \in A$. (($*$) is meningfull, since A is $\mathcal{R}$-hereditary.)
That is proved by $\mathcal{R}$-induction (since $\mathcal{R}$ is well-founded on A): If $\alpha \in A$ och $f_1(\beta) = f_2(\beta)$ for all $\beta \in \mathcal{R}\alpha$, we have $f_1(\alpha) = g(\alpha, f_1|_{\mathcal{R}\alpha}) = g(\alpha, f_2|_{\mathcal{R}\alpha}) = f_2(\alpha)$.
2. **Amalgamation:** If $f_\iota : A_\iota \to Y$ satisfy ($*$) on the $\mathcal{R}$-hereditary $A_\iota \subseteq \mathcal{D}$, then there is a function $f_\cup : \bigcup_\iota A_\iota \to Y$ which satisfies ($*$) for all $\alpha \in \bigcup_\iota A_\iota$.
Every pair of the functions take the same values in points where they are both defined, because f_{ι_1} and f_{ι_2} both satisfy ($*$) on the $\mathcal{R}$-hereditary $A_{\iota_1} \cap A_{\iota_2}$, so by 1. $f_{\iota_1}(\alpha) = f_{\iota_2}(\alpha)$ for all $\alpha \in A_{\iota_1} \cap A_{\iota_2}$. Then for $\alpha \in \bigcup_\iota A_\iota$ we can define

$f_\cup(\alpha) = f_\kappa(\alpha)$ if $\alpha \in A_\kappa$ (it will be independent of the choice of such a κ). $f_\cup$ then satisfies $(*)$, since all the f_ι do so.
3. **Local existence:** We use $\mathcal{R}$-induction to prove that for all $\alpha \in \mathcal{D}$ there is an $\mathcal{R}$-hereditary set $A_\alpha \subseteq \mathcal{D}$, with $\alpha \in A_\alpha$, and a function $f_\alpha : A_\alpha \to Y$ satisfying $(*)$.
So suppose that such A_β and f_β exist for all $\beta \in \mathcal{R}\alpha$. Then on the $\mathcal{R}$-hereditary $A_\alpha = \{\alpha\} \cup \bigcup_{\beta\in\mathcal{R}\alpha} A_\beta$, define the function f_α by 2. on $\bigcup_{\beta\in\mathcal{R}\alpha} A_\beta$ and then $f_\alpha(\alpha) = g(\alpha, f_\alpha|_{\mathcal{R}\alpha})$. f_α then satisfies $(*)$ and the $\mathcal{R}$-induction is done.
4. **Existence:** By 2. all f_α can be amalgamated to f satisfying $(*)$ on all $\bigcup_{\alpha\in\mathcal{D}} A_\alpha = \mathcal{D}$. □

Answers and hints for the exercises

Wf1) If there is such a sequence $\alpha_0, \alpha_1, \alpha_2, \ldots$, the set $\{\alpha_0, \alpha_1, \alpha_2, \ldots\}$ has no $\mathcal{R}$-minimal element (since $\alpha_{i+1}\mathcal{R}\alpha_i$, all $i = 0, 1, 2, \ldots$), so $\mathcal{R}$ is not well-founded. This proves "only if".
If $\mathcal{R}$ is not well-founded, there is an $A \subseteq \mathcal{D}$, $A \neq \varnothing$ with no $\mathcal{R}$-minimal element. Take $\alpha_0 \in A$. Since α_0 is not $\mathcal{R}$-minimal in A, there is $\alpha_1 \in A$ with $\alpha_1\mathcal{R}\alpha_0$. But α_1 is also not $\mathcal{R}$-minimal in A, so there is $\alpha_2 \in A$ with $\alpha_2\mathcal{R}\alpha_1$ and so on. At every step we choose one α_i in the sequence $\alpha_0, \alpha_1, \alpha_2, \ldots$ (where the elements do not all have to be distinct) with $\alpha_{i+1}\mathcal{R}\alpha_i$, all $i = 0, 1, 2, \ldots$ This proves "if".
Wf2) Let $A \subseteq \mathcal{D}$, $A \neq \varnothing$.
If $A_1 = A \cap \mathcal{D}_1 \neq \varnothing$, A_1 has an $\mathcal{R}_1$-minimal element $\alpha \in A_1$ (since $\mathcal{R}_1$ is well-founded). α is then also $\mathcal{R}$-minimal in A, since if $\beta\mathcal{R}\alpha$, $\beta \in A$, (by the definition of $\mathcal{R}$) $\beta\mathcal{R}_1\alpha$, $\beta \in A_1$.
If $A \cap \mathcal{D}_1 = \varnothing$, $A \subseteq \mathcal{D}_2$, $A \neq \varnothing$, so ($\mathcal{R}_2$ is well-founded) there is an $\alpha \in A$ which is $\mathcal{R}_2$-minimal in A. α is then also $\mathcal{R}$-minimal in A, because $\beta\mathcal{R}\alpha$, $\beta \in A \subseteq \mathcal{D}_2$ would imply $\beta\mathcal{R}_2\alpha$, $\beta \in A$.
In both cases A has an $\mathcal{R}$-minimal element, so $\mathcal{R}$ is well-founded.
Wf3) Let $A \subseteq \mathcal{D}$, $A \neq \varnothing$.
Also let $A_2 = \{\alpha_2 \in \mathcal{D}_2 \mid \langle\alpha_1, \alpha_2\rangle \in A \text{ for some } \alpha_1 \in \mathcal{D}_1\}$. Then $A_2 \neq \varnothing$ (because $A \neq \varnothing$), so there is an $\mathcal{R}_2$-minimal element α_2^* in A_2.
Let $A_1 = \{\alpha_1 \in \mathcal{D}_1 \mid \langle\alpha_1, \alpha_2^*\rangle \in A\}$. Then $A_1 \subseteq \mathcal{D}_1$, $A_1 \neq \varnothing$, so there is an $\mathcal{R}_1$-minimal element $\alpha_1^* \in A_1$. Then (by the assumptions on $\mathcal{R}$, $\mathcal{R}_1$, $\mathcal{R}_2$) $\langle\alpha_1^*, \alpha_2^*\rangle$ is an $\mathcal{R}$-minimal element in A, so $\mathcal{R}$ is well-founded.