Ch. 6

Well-founded induction

answers:

What is necessary to support induction principles?

Eg. important for showing termination of programs.

Definition

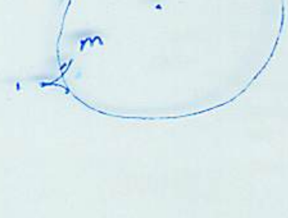
A relation $\prec$ on a set A is **well-founded** iff there are **no** infinite descending chains

$$\cdots \prec a_n \prec \cdots \prec a_1 \prec a_0 .$$

Proposition 6.1 Let $\prec \subseteq A \times A$.

$\prec$ is well-founded iff every non-empty subset $Q \subseteq A$ has a **minimal** element m

i.e. $\quad m \in Q$ and $\forall b \prec m.\ b \notin Q$.



Well-founded relations:

Examples

$m \prec n$ iff $m+1 = n$ on $\mathbb{N}_0$ (or $\mathbb{N}$)

$m \prec n$ iff $m < n$ on $\mathbb{N}_0$ (or $\mathbb{N}$)

$A \prec B$ iff A is an immediate subproposition of B in Boolean propns.

Non-example

$\mathbb{Z}$ with $<$

For strings $u, u' \in \Sigma^*$

$u' < u$ iff $\exists a \in \Sigma.\ au' = u.$

determines a wfd relation on Σ^*.

Exercise 6.3

There is no $u \in \Sigma^*$ s.t. $au = ub$ for symbols $a \neq b$.

For strings $u, u' \in \Sigma^*$

$u' \prec u$ iff $\exists a \in \Sigma.\ au' = u.$

determines a wfd relation on Σ^*.

Exercise 6.3

There is no $u \in \Sigma^*$ s.t. $au = ub$ for symbols $a \neq b$.

Proof. Assume there was. Then would be a $\prec$-minimal string u s.t.

$$au = ub.$$

But then

For strings $u, u' \in \Sigma^*$

$u' \prec u$ iff $\exists a \in \Sigma$: $au' = u$.

determines a wfd relation on Σ^*.

Exercise 6.3

There is no $u \in \Sigma^*$ s.t. $au = ub$ for symbols $a \neq b$.

Proof. Assume there was. Then would be a $\prec$-minimal string u s.t.

$$au = ub. \quad (\dagger)$$

But then $u = au'$ for some $u' \in \Sigma^*$.

$$\therefore \cancel{a}au' = \cancel{a}u'b \quad \text{by } (\dagger).$$

$$\therefore au' = u'b$$

But $u' \prec u$. Contradiction. $\square$

The principle of well-founded induction

Let $\prec$ be wfd on A.

To prove $\forall a \in A.\ P(a)$

it suffices to prove that

for all $a \in A$

$$\big(\forall b \prec a.\ P(b)\big) \Rightarrow P(a).$$

Proposition 6.9

(a) $\mathrm{hcf}(m,n) = \mathrm{hcf}(m, n-m)$ $\qquad m<n$

(b) $\mathrm{hcf}(m,n) = \mathrm{hcf}(m-n, n)$ $\qquad n<m$

(c) $\mathrm{hcf}(m,m) = m$

Recall

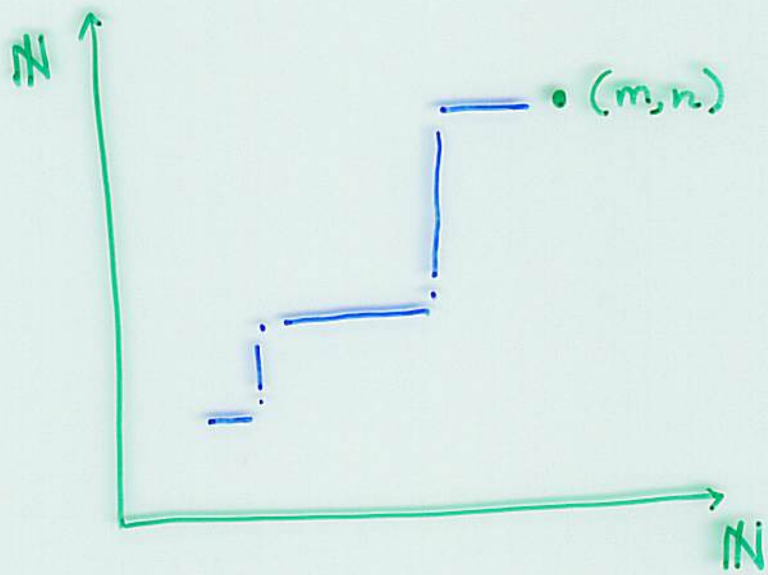
- $\mathrm{hcf}(m,n) \mid m$ & $\mathrm{hcf}(m,n) \mid n$
- $k \mid m$ & $k \mid n \Rightarrow k \mid \mathrm{hcf}(m,n)$

A well-founded relation on $\mathbb{N} \times \mathbb{N}$

$$(m', n') < (m, n)$$

iff

$$(m', n') \neq (m, n) \ \& \ m' \leq m \ \& \ n' \leq n .$$



Euclid's algorithm for hcf

A reduction relation $\xrightarrow[E]{}$ on $\mathbb{N} \times \mathbb{N}$:

$$(m, n) \xrightarrow[E]{} (m, n-m) \quad \text{if} \quad m < n$$

$$(m, n) \xrightarrow[E]{} (m-n, n) \quad \text{if} \quad n < m$$

Theorem 6.10 For all $m, n \in \mathbb{N}$

$$(m, n) \xrightarrow[E]{}^{*} (hcf(m,n),\ hcf(m,n)).$$

Euclid's algorithm for hcf

A reduction relation $\xrightarrow[E]{}$ on $\mathbb{N} \times \mathbb{N}$:

$$(m, n) \xrightarrow[E]{} (m, n-m) \quad \text{if} \quad m < n$$

$$(m, n) \xrightarrow[E]{} (m-n, n) \quad \text{if} \quad n < m$$

Theorem 6.10 For all $m, n \in \mathbb{N}$

$$\underbrace{(m, n) \xrightarrow[E]{}^{*} (hcf(m,n),\ hcf(m,n))}_{P(m,n) \overset{def}{\Longleftrightarrow}}.$$

$P(m,n) \overset{def}{\Longleftrightarrow}$

Prove $\forall m, n \in \mathbb{N}.\ P(m,n)$

by wfd induction w.r.t. $\prec \subseteq \mathbb{N} \times \mathbb{N}$

Building well-founded relations

Fundamental wfd relations

From inductive definitions

Transitive closure

If $\prec$ is wfd on A, then

$\prec^+$ is wfd on A.

Inverse image

Let $f : A \to B$.

If $\prec_B$ is wfd on B, then

$\prec_A$ is wfd on A, where

$$a' \prec_A a \;\overset{}{\underset{\text{def}}{\Longleftrightarrow}}\; f(a') \prec_B f(a) \,.$$

Defn. by well-founded induction
(Well-founded recursion)

Examples

- Defn. by mathl. induction:

$$f(0) = \sim\sim\sim$$
$$f(n+1) = \sim\sim\sim f(n) \sim\sim\sim$$

- Defn. by structural induction:

$$\mathrm{length}(a) = 1$$
$$\mathrm{length}(A \vee B) = \mathrm{length}(A) + \mathrm{length}(B) + 1$$
$$\vdots$$

- Defn. by wfd. induction on $<$ on $\mathbb{N}$

Fibonacci $\quad fib(1) = 1, \quad fib(2) = 1,$

$$fib(n) = fib(n-1) + fib(n-2) \text{ for } n > 2.$$

[cf. course-of-values induction]

Let $\prec_A$ be wfd on A, $\prec_B$ wfd on B.

Product

$\prec$ is wfd on $A \times B$ where

$$(a', b') \preccurlyeq (a, b) \overset{\text{def}}{\Leftrightarrow} \underbrace{a' \preccurlyeq_A a}_{a' \prec_A a \text{ or } a' = a} \;\&\; b' \preccurlyeq_B b.$$

Lexicographic product

$\prec_{lex}$ is wfd on $A \times B$ where

$$(a', b') \prec_{lex} (a, b) \overset{\text{def}}{\Leftrightarrow}$$

$$a' \prec_A a \text{ or } (a' = a \;\&\; b' \prec_B b).$$

Ackermann's function

$$ack : \mathbb{N}_0 \times \mathbb{N}_0 \longrightarrow \mathbb{N}_0$$

$$ack(0,n) = n+1$$

$$ack(m,0) = ack(m-1, 1) \quad \text{if } m>0$$

$$ack(m,n) = ack(m-1, ack(m,n-1)) \quad \text{if } m,n>0$$

i.e. $ack(m-1,k)$ where $k = ack(m,n-1)$

Ackermann's function

$$ack : \mathbb{N}_0 \times \mathbb{N}_0 \longrightarrow \mathbb{N}_0$$

$$ack(0,n) = n+1$$

$$ack(m,0) = ack(m-1,\ 1) \quad \text{if } m>0$$

$$ack(m,n) = ack(m-1,\ ack(m,n-1)) \quad \text{if } m,n>0$$

i.e. $ack(m-1,k)$ where $k = ack(m,n-1)$

- ack is defined because

$$(m,n-1) <_{lex} (m,n)$$

$$(m-1,k) <_{lex} (m,n)$$

$<_{lex}$ is lex. product of $<$ and $<$ on $\mathbb{N}_0$.

Well-founded recursion P. 92

$\prec$ wfd on A

$$f(x) = \sim\sim f(x_1) \sim\sim f(x_2) \sim\sim \ldots \in B$$

where $x_1 \prec x$, $x_2 \prec x$, $\cdots$

defines a unique function

$$f : A \longrightarrow B.$$

[NB. x etc. can be a pair, or tuple.]

Examinable material = what's been lectured

$\boxed{\text{lecture plan P.2}}$ = slides available from course web page soon.
REVISED SOON