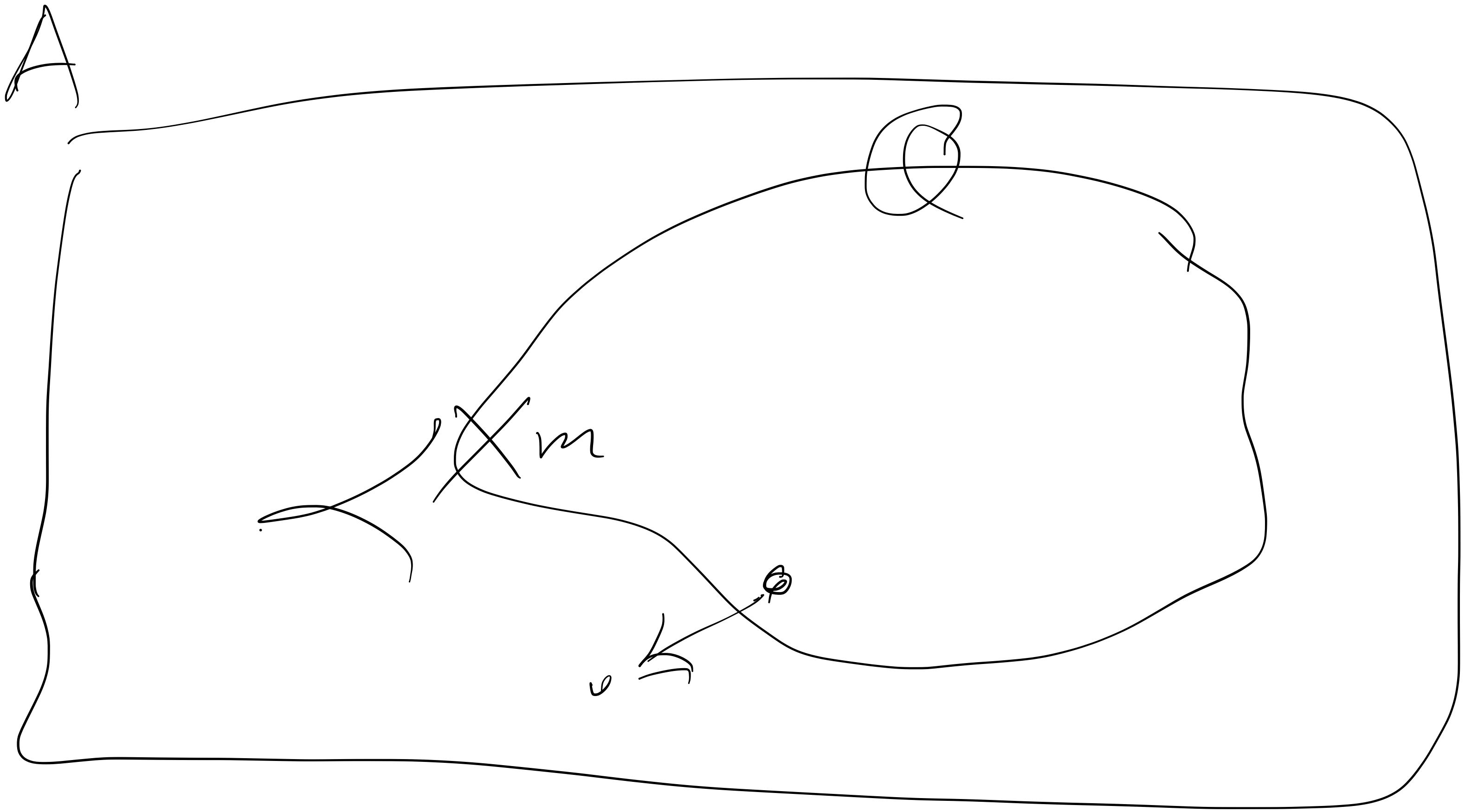
Well-founded relation $\prec$ on A

$\cdots \prec a_4 \prec \cdots \cancel{\prec a_2} \prec a_1 \prec a_0$



An application. For strings u, u' over an alphabet Σ,

$$u' \prec u \quad \text{iff} \quad \exists a \in \Sigma.\ au' = u$$

defines a well-founded relation on strings.

Exercise 1.4 There is no string u over Σ s.t. $au = ub$ for distinct symbols a and b in Σ.

Proof Assume there were (to obtain a contradiction). Then there would be a $\prec$ minimal string u s.t.

$$au = ub$$

But then $u = au'$.

$$\therefore \quad \cancel{a}au' = \cancel{a}u'b$$

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

But $u' \prec u$.

The principle of well-founded induction

Let $\prec$ be well-founded on A.

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

it suffices to prove that for all $a \in A$,

$$\left(\forall b \prec a.\ P(b)\right) \Rightarrow P(a).$$

$$\left(\forall b \in A.\ b \prec a \Rightarrow P(b)\right)$$

Examples

(1) On $\mathbb{N}$ where $m \prec n$ iff $m+1=n$ in $\mathbb{N}$.

(2) On $\mathbb{N}$ where $m \prec n$ iff $m < n$ in $\mathbb{N}$.

(3) On Boolean propositions where $A \prec B$ iff A is a subexpression of B

Examples of definition by well-founded induction (a.k.a. well-founded recursion).

- $$\mathrm{rem}(m,n) = \begin{cases} \mathrm{rem}(m-n,n) & \text{if } m \geq n \\ m & \text{if } m < n \end{cases}$$

w.r.t. $\prec$ on $\mathbb{N} \times \mathbb{N}$ where $(m',n') \prec (m,n)$ iff $m' < m$.

- $$\gcd(m,n) = \begin{cases} n & \text{if } n \mid m \\ \gcd(n, \mathrm{rem}(m,n)) & \text{otherwise} \end{cases}$$

w.r.t. $\prec$ on $\mathbb{N} \times \mathbb{N}$ where $(m',n') \prec (m,n)$ iff $n' < n$.

- Factorial function $$n! = \begin{cases} 1 & \text{if } n = 0 \\ n \cdot (n-1)! \end{cases}$$

- Fibonacci numbers $f(0) = 0 \quad f(1) = 1$

  $f(n) = f(n-1) + f(n-2) \quad n > 1$

Definition by well-founded recursion

Suppose $\prec$ is a well-founded relation on B.

Suppose $F(b, c_1, \cdots, c_k, \cdots) \in C$, a set,

for all $b \in B$, $c_1, \cdots, c_k, \cdots \in C$.

Then a recursive definition, for all $b \in B$,

$$f(b) = F(b, f(b_1), \cdots, f(b_k), \cdots),$$

with $b_1, \cdots, b_k, \cdots \prec b$, determines

a unique function f from B to C.

Theorem (1) $\gcd(m,n) \mid m$ and $\gcd(m,n) \mid n$

(2) $\forall d \in \mathbb{N}.\ d \mid m\ \&\ d \mid n \Rightarrow d \mid \gcd(m,n)$

for all $m, n > 0$ in $\mathbb{N}$.

Proof By well-founded induction w.r.t.

$$(m', n') \prec (m, n) \text{ iff } n' < n$$

for $m', n', m, n \geq 0$ in $\mathbb{N}$. Clearly $\prec$ is well-fdd.

We take as induction hypothesis

$$P(m,n) \text{ iff (1) and (2) hold of } m, n > 0 \text{ in } \mathbb{N}.$$

To apply well-founded induction R.T.P

$$\forall m, n > 0 \text{ in } \mathbb{N}.\ \left(\forall (m', n') \prec (m, n).\ P(m', n')\right) \Rightarrow P(m,n).$$

Let $m, n > 0$ in $\mathbb{N}$. Assume $\forall (m', n') < (m, n).\ P(m', n')$.

RTP $P(m, n)$, i.e. (1) & (2) for m, n.

Case $n \mid m$

(1) Then $\gcd(m, n) = n$ by definition.

Hence $\gcd(m, n) \mid n, m$ directly

(Recall if $k \mid n$ & $n \mid m$ then $k \mid m$)

(2) Suppose $d \in \mathbb{N}$ and $d \mid m, n$. Then,

$d \mid n = \gcd(m, n)$.

Case $n \nmid m$. Then by defn, $\gcd(m,n) = \gcd(n, \mathrm{rem}(m,n))$

As $(n, \mathrm{rem}(m,n)) \prec (m,n)$ — recall $0 \leq \mathrm{rem}(m,n) < n$ —

we have $P(n, \mathrm{rem}(m,n))$.

by IH

(1) Hence $\gcd(m,n) = \gcd(n, \mathrm{rem}(m,n)) \mid n, \mathrm{rem}(m,n)$

$\therefore \gcd(m,n) \mid m, n$ by Cor. 57(1).

(2) Let $d \mid m, n$. Then, from $P(n, \mathrm{rem}(m,n))$,

$d \mid \gcd(n, \mathrm{rem}(m,n)) = \gcd(m,n)$.

I.e. $P(m,n)$.

By well-founded induction we conclude

$\forall m, n > 0 \text{ in } \mathbb{N}.\ P(m,n)$. $\boxtimes$

Instead of Cor 57 (1):

$g \mid n, \ \mathrm{rem}(m,n)$

$$\boxed{\text{RTP:} \quad g \mid m, n.}$$

$$m = q \cdot n + \mathrm{rem}(m,n)$$

Have $g \mid n$ $\quad g \mid \mathrm{rem}(m,n)$

$$\therefore \ g \mid m.$$

$$\therefore \ g \mid m, \ n.$$

Ackermann's function from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$

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

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

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

$$[= ack(m-1, k) \text{ where } k = ack(m, n-1).]$$

- Why is this a good definition of a function?
- Why does its evaluation terminate?
- What is the well-founded relation w.r.t. which pairs on the r.h.s. are decreasing?

Answer: the lexicographic product of $<$ and $<$ where $<$ is "less than" on $\mathbb{N}$.

The lexicographic product of relations

Let $<_A$ be well-founded on A.

Let $<_B$ be well-founded on B. Then,

$<_{lex}$ is well-founded on $A \times B$ where

$$(a', b') <_{lex} (a, b) \quad \text{iff}$$

$$a' <_A a \quad \text{or} \quad (a = a' \ \& \ b' <_B b).$$

To see $<_{lex}$ is well-founded consider

$$\ldots <_{lex} (a_n, b_n) \ \ldots <_{lex} (a_2, b_2) <_{lex} (a_1, b_1) <_{lex} (a_0, b_0)$$