Theorem 77 (Fundamental Theorem of Arithmetic) *For every positive integer* n *there is a unique finite ordered sequence of primes* $(p_1 \leq \cdots \leq p_\ell)$ *with* $\ell \in \mathbb{N}$ *such that*

$$n = \prod(p_1, \ldots, p_\ell) \ .$$

aka "smallest counterexample!"

PROOF: Use the least number principle:

A non-empty subset of $\mathbb{N}$ has a least element.

(The least number principle is equivalent to math. ind.)

Proof by contradiction. Assume there is pos. int. without a unique decomposition.

Then, $n = p_1 \cdot \cdots \cdot p_\ell = q_1 \cdot \cdots \cdot q_k$ for different sequences of primes $p_1 \leq \cdots \leq p_\ell$ and $q_1 \leq \cdots \leq q_k$, and is the least such.

Note $p_1 \mid n$. As p_1 is prime $p \mid q_i$ for some i.

But q_i is prime $\therefore$ $p_1 = q_i$. $\therefore$ $q_1 \leq p_1$.

Symmetrically $p_1 \leq q_1$. $\therefore$ $p_1 = q_1$.

So dividing n by p_1 $(= q_1)$,

$$p_2 \cdot \cdots \cdot p_\ell = q_2 \cdot \cdots \cdot q_k$$

two distinct decompositions of a smaller no. than n. $\times$

$\boxtimes$

Euclid's infinitude of primes

Theorem 80 *The set of primes is infinite.*

PROOF: Proof by contradiction:

Assume the set of primes is finite i.e. $\{p_1, \ldots \; p_k\}$. Define

$$n = p_1 \cdot \ldots \cdot p_k + 1$$

There is prime q s.t. $q \mid n$.

But $q = p_i$ some i. So q gives a remainder 1. $\times\!\!\times$

$\boxtimes$

Structural Induction

Syntax of Boolean propositions:

$$A, B, \ldots ::= a, b, c, \ldots \mid T \mid F \mid A \wedge B \mid A \vee B \mid \neg A$$

To prove $P(A)$ for all Boolean props. A

it suffices to prove

Base case $\quad P(a),\ P(b),\ P(c), \ldots P(T),\ P(F)$

Induction step

$$P(A) \ \& \ P(B) \implies P(A \wedge B)$$

$$P(A) \ \& \ P(B) \implies P(A \vee B)$$

$$P(A) \implies P(\neg A)$$

for all Boolean expressions A, B.

Definitions by structural induction

(1) We can define the length of a Boolean proposition by structural induction:

$$|a| = |b| = |c| = \dots = 1$$

$$|T| = 1 \qquad |F| = 1$$

$$|A \wedge B| = |A| + |B| + 1$$

$$|A \vee B| = |A| + |B| + 1$$

$$|\neg A| = |A| + 1$$

(2) $\vee$ elimination:

$$tr(a) = a \qquad tr(T) = T \qquad tr(F) = F$$

$$tr(A \wedge B) = tr(A) \wedge tr(B)$$

$$tr(A \vee B) = \neg(\neg tr(A) \wedge \neg tr(B))$$

$$tr(\neg A) = \neg\, tr(A).$$

Exercise 1.1 Prove by structural induction on Boolean propositions that

$$|tr(A)| \leq 3|A| - 1$$

for all Boolean propositions A.

Well-founded Induction

A very general induction principle, important for example in proving the termination of programs.

Well-founded relations

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 A relation $\prec$ on a set A is well-founded iff every non-empty subset Q of A has a minimal element m

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

Examples of well-founded relations

(1) $m < n$ iff $m+1 = n$ in $\mathbb{N}$

(2) $m < n$ iff $m < n$ in $\mathbb{N}$

(3) $A < B$ iff A is an immediate sub-expression of B in Boolean propositions.

Non-example

$\mathbb{Z}$ with $<$.

$\ldots \quad -3 \quad -2 \quad -1 \quad 0$

Proposition A relation $\prec$ on a set A is well-founded iff every non-empty subset Q has a minimal element m,

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

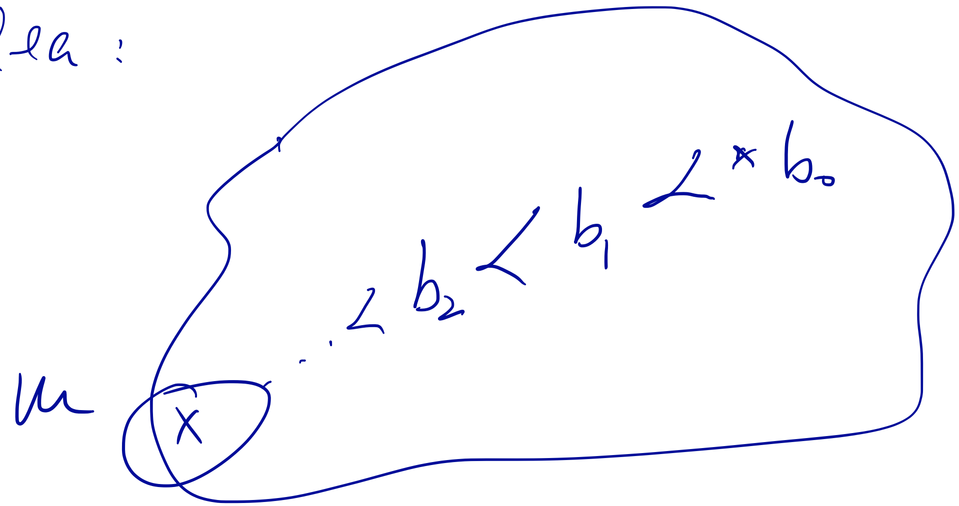
Assume

Proof. "if": Proof by contradiction. Assume $\prec$ is not well-fdd.

i.e. $\cdots \prec a_n \prec \cdots \prec a_2 \prec a_1 \prec a_0$ for some $a_0, a_1, \ldots \in A$.

Take $Q = \{a_0, a_1, \ldots, a_n, \ldots\}$. Fails.

"only if": Idea:



$Q \neq \emptyset$

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

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

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.

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

$$au = ub$$

But then $u = au'$.

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

$$\therefore \quad au' = u'b \qquad \text{But } u' \prec u. \ \times$$

$\boxtimes$