PSC 2021/22 (375AA, 9CFU)

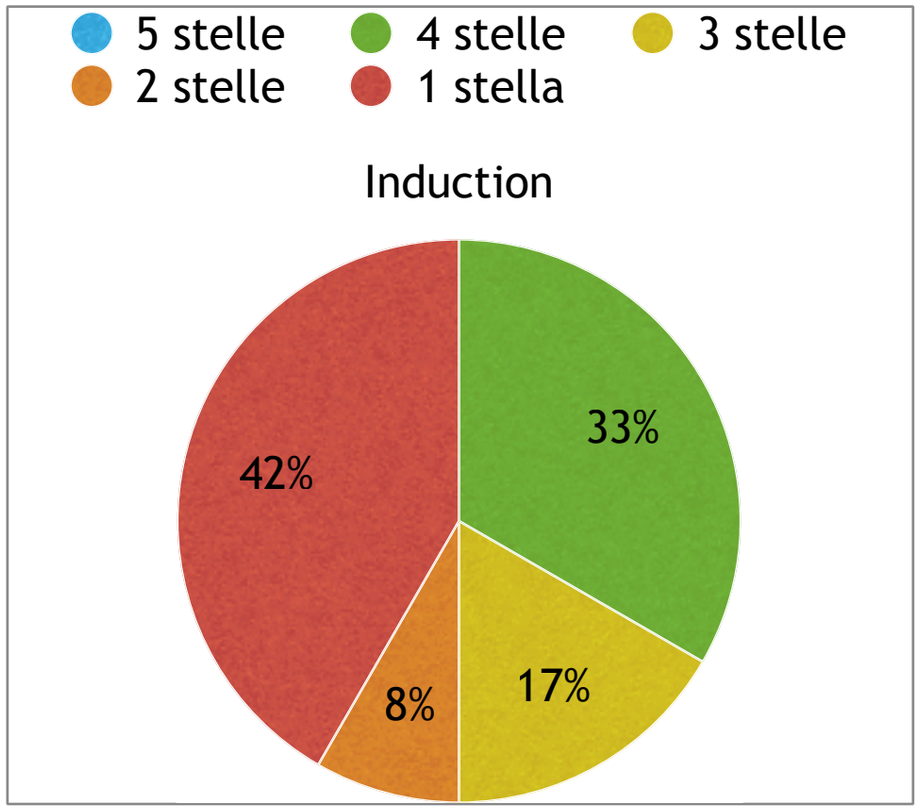
Principles for Software Composition

Roberto Bruni
http://www.di.unipi.it/~bruni/

http://didawiki.di.unipi.it/doku.php/magistraleinformatica/psc/start

05a - Induction

From your forms



(over 12 answers)

Induction everywhere

How to

prove an existential statement? $\exists x.\ P(x)$

exhibit a witness

$\exists n \in \mathbb{N}.\ n^2 \leq n$ $n = 0$

disprove a universal statement? $\neg\forall x.\ P(x) \equiv \exists x.\ \neg P(x)$

exhibit a counterexample to P

$\forall n \in \mathbb{N}.\ n^2 \leq n$ $n = 2$

prove a universal statement? $\forall x.\ P(x)$

use induction!

What is common to

natural numbers

lists

trees

grammar languages

terms of a signature

theorems of a logic system

derivations

computations

generated by
finite applications
of some given rules

base cases

inductive cases

What is common to

	base case	inductive case
natural numbers	0	succ
lists	nil	cons
trees	nil	node
grammar languages	productions with only terminal symbols	productions with non terminal symbols
terms of a signature	constants	operators
theorems of a logic system	axioms	inference rules
derivations	axioms	inference rules
computations	single step	concatenation

A famous proof

Every non prime number greater than 1 can be written as the product of two or more prime numbers

base case ($n = 2$): 2 is prime

inductive case: taken a generic n, we assume the property holds for all numbers from 2 to n and prove it holds for $n + 1$:

- if $n + 1$ is prime we are done;
- otherwise, let $n + 1 = a \cdot b$ for some $1 < a, b \leq n$. By inductive hypothesis, a and b can be written as product of prime numbers. Let $a = p_1 \cdots p_k$ and $b = q_1 \cdots q_h$. Then $n + 1 = p_1 \cdots p_k \cdot q_1 \cdots q_h$ can be written as the product of $k + h$ primes.

A far less known proof

All cats are the same colour

base case ($n = 1$): trivial

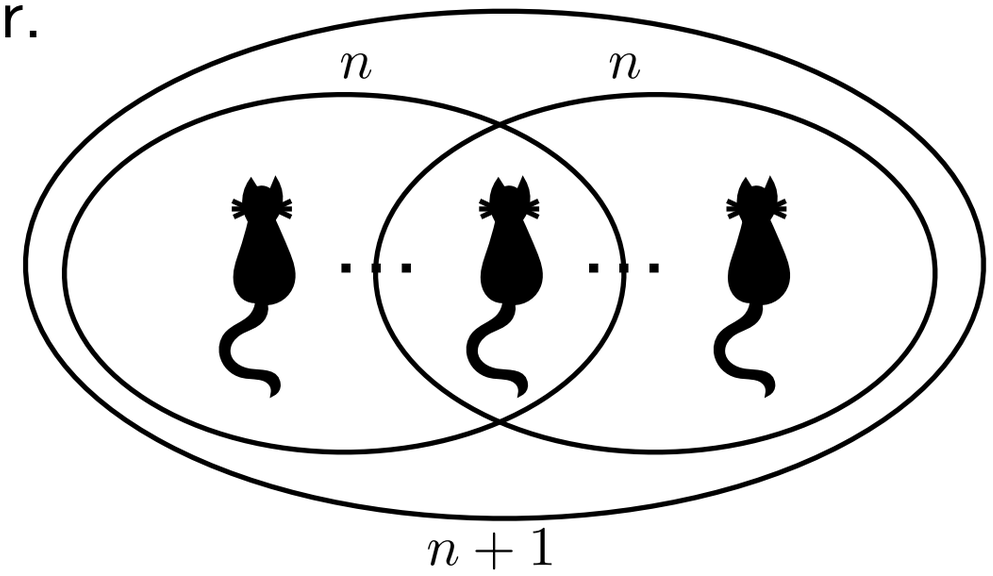
inductive case: taken a generic n, we assume the property holds for all groups with $k \leq n$ cats and prove it holds for any group with $n + 1$ cats as well.

Take $n+1$ cats and place them along a line (this is the hardest part of the proof!).

By inductive hypothesis, the first n cats are the same colour.

By inductive hypothesis, the last n cats are the same colour.

Since the cats in the middle of the line belongs to both groups, by transitivity all $n + 1$ cats are the same colour.



Well founded induction

Ingredients

a set of elements A (possibily infinite)

a predicate $P : A \to \mathbb{B}$

we want to prove $\forall a \in A.\ P(a)$

a binary relation of precedence $\prec \subseteq A \times A$

(not necessarily transitive)

$a \prec b$ reads a precedes b

also written $b \succ a$

also written $a \to b$ (graph notation)

to use induction, we must guarantee to reach some base cases!

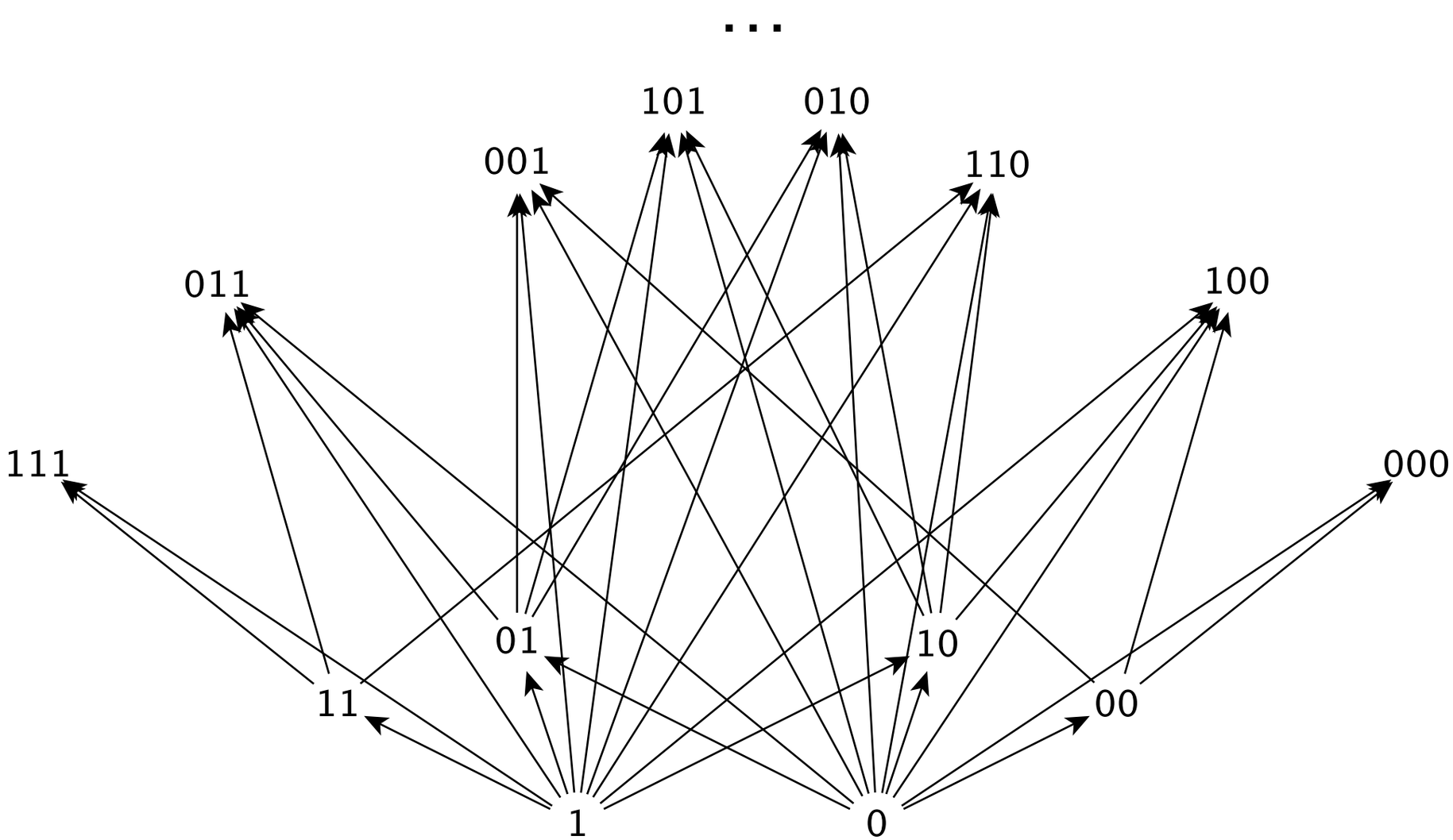
no infinite descending chain is allowed in $\prec$

(well-founded relation)

Graph of a relation

Example:

$A = \mathbb{B}^*$ $\quad u \prec w$ if u appears in w (with $u \neq \epsilon$ and $u \neq w$)



Infinite descending chain

Infinite descending chain

an infinite sequence $\{a_i\}_{i \in \mathbb{N}}$ of elements in A

such that $\forall i \in \mathbb{N}.\ a_i \succ a_{i+1}$

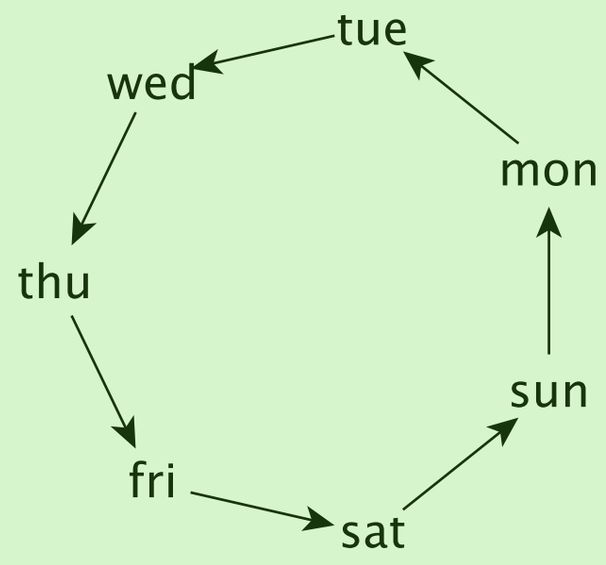
the sequence can also be seen as a function $a : \mathbb{N} \to A$

$$a(n) = a_n$$

Example

$A = \{\mathsf{mon}, \mathsf{tue}, \mathsf{wed}, \mathsf{thu}, \mathsf{fri}, \mathsf{sat}, \mathsf{sun}\}$

$a(n) = n\text{th day past}$



Well-founded relation

A relation is called well-founded
if it has no infinite descending chain

$\mathbb{N}$	$n \prec m$ if $m = n + 1$	✓
$\mathbb{Z}$	$n \prec m$ if $m = n + 1$	✗
$\mathbb{N}$	$n \prec m$ if $n < m$	✓
$\mathbb{Z}$	$n \prec m$ if $n < m$	✗
$\mathbb{N}$	$n \prec m$ if $n \leq m$	✗
$\mathbb{N}$	$n \prec m$ if $n = m$	✗

Transitive closure

a binary relation $\prec \subseteq A \times A$

its transitive closure $\prec^+ \subseteq A \times A$

is the least relation generated by the following rules

$$\frac{a \prec b}{a \prec^+ b} \qquad \frac{a \prec^+ b \quad b \prec^+ c}{a \prec^+ c}$$

by the first rule, it is obvious that $\prec \subseteq \prec^+$

it can be proved that $(\prec^+)^+ = \prec^+$

Transit. and refl. closure

a binary relation $\prec \subseteq A \times A$

its transitive and reflexive closure $\prec^* \subseteq A \times A$

is the least relation generated by the following rules

$$\frac{a \in A}{a \prec^* a} \qquad \frac{a \prec b}{a \prec^* b} \qquad \frac{a \prec^* b \quad b \prec^* c}{a \prec^* c}$$

it is obvious that $\prec \subseteq \prec^+ \subseteq \prec^*$

it can be proved that $(\prec^*)^* = \prec^*$

Closures and paths

a binary relation $\prec \subseteq A \times A$

$a \prec^+ b$ iff there is a non-empty path from a to b in the graph of $\prec$

$$\exists k > 0, \{c_i\}_{i \in [0,k]}.\ a = c_0 \prec c_1 \prec \cdots \prec c_k = b$$

$a \prec^* b$ iff there is a possibly empty path from a to b in the graph of $\prec$

$$\exists k \geq 0, \{c_i\}_{i \in [0,k]}.\ a = c_0 \prec c_1 \prec \cdots \prec c_k = b$$

Closures

		$\prec^+$	$\prec^*$
$\mathbb{N}$	$n \prec m$ if $m = n + 1$	$n < m$	$n \leq m$
$\mathbb{Z}$	$n \prec m$ if $m = n + 1$	$n < m$	$n \leq m$
$\mathbb{N}$	$n \prec m$ if $n < m$	$n < m$	$n \leq m$
$\mathbb{N}$	$n \prec m$ if $n \leq m$	$n \leq m$	$n \leq m$
$\mathbb{N}$	$n \prec m$ if $n = m$	$n = m$	$n = m$

Get ready for theorems: proofs included

on the right, you see one of the oldest surviving fragments of Euclid's Elements, a textbook used for millennia to teach proof-writing techniques (source: *wikipedia*)

Theorem

A relation is well-founded iff its transitive closure is well-founded

$\prec^+$ w.f. $\Rightarrow \prec$ w.f.

obvious:
any descending chain for $\prec$ is a descending chain for $\prec^+$
and thus it is finite because $\prec^+$ is w.f.

Theorem

A relation is well-founded iff its transitive closure is well-founded

$\prec$ w.f. $\Rightarrow$ $\prec^+$ w.f. $\quad\equiv\quad$ $\neg(\prec^+$ w.f.$)$ $\Rightarrow$ $\neg(\prec$ w.f.$)$

by contraposition:
we assume $\prec^+$ is not w.f. and prove $\prec$ is not w.f.

take an infinite descending chain for $\prec^+$

$$a_0 \succ^+ a_1 \succ^+ a_2 \succ^+ \cdots$$

$a \prec^+ b$ iff there is a non-empty path from a to b in the graph of $\prec$

$$a_0 \succ \cdots \succ a_1 \succ \cdots \succ a_2 \succ \cdots$$

thus we get an infinite descending chain for $\prec$

Acyclic relation

a binary relation $\prec \subseteq A \times A$

$\prec$ has a cycle if $a \prec^+ a$ for some $a \in A$

We say that $\prec$ is acyclic if it has no cycle

note that $\prec$ is acyclic iff $\prec^+$ is such

Theorem

Well-founded relations are acyclic

by contraposition:
we prove that if $\prec$ has a cycle then it is not well-founded

take $a \in A$ such that $a \prec^+ a$

then we have an infinite descending chain for $\prec^+$

$$a \succ^+ a \succ^+ a \succ^+ \dots$$

therefore $\prec^+$ is not w.f.

by the previous theorem, $\prec$ is not w.f.

Theorem

If A is finite and $\prec$ acyclic, then $\prec$ is well-founded

the proof exploits the pigeonhole principle

Pigeonhole principle (aka drawer principle)

If n items are put into $m < n$ slots,

then at least one slot must contain more than one item

in the picture: ten pigeons and nine holes

Theorem

If A is finite and $\prec$ acyclic, then $\prec$ is well-founded

by contraposition:
we prove that if $\prec$ is not well-founded then it has a cycle

take an infinite descending chain for $\prec$

$$a_0 \succ a_1 \succ a_2 \succ \cdots$$

let $k = |A|$ and consider $a_0, ..., a_k$ (they are $k+1$ elements)

by the pigeonhole principle, $a_i = a_j$ for some $0 \leq i < j \leq k$

$$a_i \succ a_{i+1} \succ \cdots \succ a_{j-1} \succ a_j = a_i$$

thus $a_i \prec^+ a_i$ and $\prec$ has a cycle

Minimal elements

a binary relation $\prec \subseteq A \times A$

let $Q \subseteq A$ and $m \in Q$

m is minimal in Q if none of the elements in Q precedes m

$$\forall x \in Q.\ x \not\prec m$$
$$\equiv \neg\exists x \in Q.\ x \prec m$$

Q has no minimal element means $\forall m \in Q.\ \exists x \in Q.\ x \prec m$

Minimal elements

		minimal element?	unique?
$\mathbb{N}, <$	$\varnothing \subset Q \subseteq \mathbb{N}$	✓	✓
$\mathbb{Z}, <$	$\varnothing \subset Q \subseteq \mathbb{Z}$	✓/✗	✓
$\wp(\mathbb{N}), \subset$	$\varnothing \subset Q \subseteq \wp(\mathbb{N})$	✓/✗	✓/✗

Lemma

$\prec$ is w.f. iff any non empty $Q \subseteq A$ has a minimal element

$\equiv$

① $\prec$ has an infinite descending chain iff

② there is a (non empty) $Q \subseteq A$ with no minimal element

① $\Rightarrow$ ② Take an infinite descending chain $\{a_i\}_{i \in \mathbb{N}}$

the set $Q = \{a_i \mid i \in \mathbb{N}\}$ has no minimal element

(if it had one, say a_k, then $a_{k+1} \prec a_k$!)

Lemma

$\prec$ is w.f. iff any non empty $Q \subseteq A$ has a minimal element

$\equiv$

① $\prec$ has an infinite descending chain iff

② there is a (non empty) $Q \subseteq A$ with no minimal element

② $\Rightarrow$ ① Take $\varnothing \subset Q \subseteq A$ with no minimal element

Since $Q \neq \varnothing$ we can pick $a_0 \in Q$

Since a_0 cannot be minimal, we can take $a_1 \in Q$ s.t. $a_1 \prec a_0$

Since a_1 cannot be minimal, we can take $a_2 \in Q$ s.t. $a_2 \prec a_1$

...

Since a_k cannot be minimal, we can take $a_{k+1} \in Q$ s.t. $a_{k+1} \prec a_k$

...

Theorem [w.f. induction]

Let $\prec \subseteq A \times A$ be w.f.

$$(\ \forall a \in A.\ P(a)\ ) \quad \Leftrightarrow \quad (\ \forall a \in A.\ (\forall b \prec a.\ P(b)) \Rightarrow P(a)\ )$$

Set $H(a) \triangleq \forall b \prec a.\ P(b)$ $\qquad$ $S(a) \triangleq H(a) \Rightarrow P(a)$

$$(\ \forall a \in A.\ P(a)\ ) \quad \Leftrightarrow \quad (\ \forall a \in A.\ S(a)\ )$$

① ②

① $\Rightarrow$ ② Assume $\forall a.\ P(a)$ Take a generic $a \in A$

$$S(a) \equiv (H(a) \Rightarrow P(a)) \equiv (\neg H(a) \vee P(a)) \equiv (\neg H(a) \vee \mathbf{tt}) \equiv \mathbf{tt}$$

Theorem [w.f. induction]

Let $\prec \subseteq A \times A$ be w.f.

$$S(a) \triangleq H(a) \Rightarrow P(a)$$
$$H(a) \triangleq \forall b \prec a.\ P(b)$$

$$\textcircled{1}\ (\ \forall a \in A.\ P(a)\ ) \quad \Leftrightarrow \quad (\ \forall a \in A.\ S(a)\ )\ \textcircled{2}$$

$\textcircled{2} \Rightarrow \textcircled{1} \quad \equiv \quad \neg\textcircled{1} \Rightarrow \neg\textcircled{2}$

Assume $\exists a \in A.\ \neg P(a)$

Take $Q \triangleq \{q \in A \mid \neg P(q)\} \neq \varnothing$

Since $\prec$ is w.f., then Q has a minimal element $m \in Q$

Obviously $\neg P(m)$ (because $m \in Q$)

Since m is minimal, $\forall b \prec m.\ b \notin Q$

i.e. $\forall b \prec m.\ P(b) \quad \equiv \quad H(m)$

Thus $H(m) \wedge \neg P(m) \quad \equiv \quad \neg(H(m) \Rightarrow P(m)) \quad \equiv \quad \neg S(m)$

i.e. $\exists a \in A.\ \neg S(a)$

w.f. induction principle

a w.f. relation $\prec \subseteq A \times A$

$$\frac{\forall a \in A.\ (\ (\forall b \prec a.\ P(b)) \Rightarrow P(a)\ )}{\forall a \in A.\ P(a)}$$

Advantage: when proving $P(a)$ for a generic a,

we can exploit the assumption $\forall b \prec a.\ P(b)$!

Weak mathematical induction

$$\frac{\forall a \in A.\ (\ (\forall b \prec a.\ P(b)) \Rightarrow P(a)\ )}{\forall a \in A.\ P(a)}$$

$A = \mathbb{N}$

$\prec = \{(n, n+1) \mid n \in \mathbb{N}\}$ (immediate precedence relation)

- if $a = 0$, then there is no $b \prec 0$, hence $(\forall b \prec 0.\ P(b)) \equiv \mathbf{tt}$ and $(\ (\forall b \prec 0.\ P(b)) \Rightarrow P(0)\ ) \equiv \mathbf{tt} \Rightarrow P(0) \equiv P(0)$

- if $a = n + 1$, then there is only one b such that $b \prec n + 1$, namely $b = n$ then
$(\ (\forall b \prec n + 1.\ P(b)) \Rightarrow P(n + 1)\ ) \equiv P(n) \Rightarrow P(n + 1)$

Weak mathematical induction principle

$$\frac{P(0) \qquad \forall n \in \mathbb{N}.\ (\ P(n) \Rightarrow P(n+1)\ )}{\forall n \in \mathbb{N}.\ P(n)}$$

Weak: we can exploit $P(n)$,

for proving $P(n+1)$!

Weak induction: example

Prove that: $\forall n \in \mathbb{N}.\ \exists k \in \mathbb{N}.\ n^3 - n = 3k$

Let $P(n) \triangleq \exists k \in \mathbb{N}.\ n^3 - n = 3k$

Prove $P(0) \triangleq \exists k \in \mathbb{N}.\ 0^3 - 0 = 3k$ trivial: take $k = 0$

Prove $\forall n \in \mathbb{N}.\ (P(n) \Rightarrow P(n+1))$ Take a generic $n \in \mathbb{N}$

Assume $P(n) \triangleq \exists k_1 \in \mathbb{N}.\ n^3 - n = 3k_1$

Prove $P(n+1) \triangleq \exists k \in \mathbb{N}.\ (n+1)^3 - (n+1) = 3k$

Observe
$$\begin{aligned}(n+1)^3 - (n+1) &= n^3 + 3n^2 + 3n + 1 - n - 1 \\ &= (n^3 - n) + 3n^2 + 3n \\ &= 3k_1 + 3n^2 + 3n \quad \text{(by } P(n)\text{)} \\ &= 3(k_1 + n^2 + n)\end{aligned}$$

Take $k = k_1 + n^2 + n$

Strong mathematical induction principle

$$\frac{\forall a \in A.\ (\ (\forall b \prec a.\ P(b)) \Rightarrow P(a)\ )}{\forall a \in A.\ P(a)}$$

$A = \mathbb{N}$

$\prec\ =\ <$ (strictly-less-than relation)

- if $a = 0$, as before, then there is no $b \prec 0$, hence $(\ (\forall b \prec 0.\ P(b)) \Rightarrow P(0)\ ) \equiv P(0)$
- if $a = n + 1$, then $(\forall b \prec n + 1.\ P(b)) \equiv P(0) \wedge P(1) \wedge \cdots \wedge P(n)$ and $(\ (\forall b \prec n + 1.\ P(b)) \Rightarrow P(n + 1)\ ) \equiv (P(0) \wedge \cdots \wedge P(n)) \Rightarrow P(n + 1)$

Strong mathematical induction

$$\frac{P(0) \qquad \forall n \in \mathbb{N}.\ (\ (P(0) \wedge \cdots \wedge P(n)) \Rightarrow P(n+1)\ )}{\forall n \in \mathbb{N}.\ P(n)}$$

Strong: we can exploit more hypotheses than $P(n)$, for proving $P(n+1)$!

Strong induction: example

Prove that: $\forall n \geq 8.\ \exists a, b \in \mathbb{N}.\ n = 3a + 5b$

Let $P(n) \triangleq \exists a, b \in \mathbb{N}.\ n = 3a + 5b$

Prove $P(8) \triangleq \exists a, b \in \mathbb{N}.\ 8 = 3a + 5b$ trivial: take $a = 1, b = 1$

Prove $\forall n \geq 8.\ (P(8) \wedge \cdots \wedge P(n) \Rightarrow P(n+1))$

Assume $P(8) \wedge \cdots \wedge P(n)$

Prove $P(n+1) \triangleq \exists a, b \in \mathbb{N}.\ n + 1 = 3a + 5b$

Observe $n + 1 = (n + 1 - 3) + 3 = (n - 2) + 3$

$$\overset{\text{(by } P(n-2)\text{)}}{=} (3a_1 + 5b_1) + 3$$

$$= 3(a_1 + 1) + 5b_1$$

Take $a = a_1 + 1, b = b_1$

but... did we miss something? Prove $P(9)$ and $P(10)$!

Structural induction

Immediate subterms

a signature $\{\Sigma_n\}_{n\in\mathbb{N}}$

Take $A = T_\Sigma$ (closed terms)

$$\prec = \{(t_i, f(t_1, ..., t_n)) \mid f \in \Sigma_n, i \in [1, n]\}$$

(immediate subterm relation)

Example

$\Sigma_0 = \{0\}$ $\Sigma_1 = \{\mathsf{succ}\}$ $\Sigma_2 = \{\mathsf{plus}\}$

$$0 \prec \mathsf{succ}(0) \prec \mathsf{plus}(0, \mathsf{succ}(0))$$

$$0 \prec \mathsf{plus}(0, \mathsf{succ}(0))$$

$$0 \not\prec \mathsf{plus}(\mathsf{succ}(0), \mathsf{succ}(0))$$

Lemma

$T_\Sigma, \prec$ is w.f.

Let $depth : T_\Sigma \to \mathbb{N}$ defined as:

$$depth(c) \quad \triangleq \quad 1 \qquad \text{if } c \in \Sigma_0$$

$$depth(f(t_1, ..., t_n)) \quad \triangleq \quad 1 + \max_{i \in [1,n]} depth(t_i) \quad \text{if } f \in \Sigma_n$$

By definition, if $t \prec t'$ then $depth(t) < depth(t')$

Any descending chain in $\prec$ induces a descending chain in $<$

Since $<$ is w.f., so is $\prec$

Structural induction principle

$$\frac{\forall n \in \mathbb{N}.\ \forall f \in \Sigma_n.\ \forall t_1, ..., t_n \in T_\Sigma.\ (P(t_1) \wedge \cdots \wedge P(t_n)) \Rightarrow P(f(t_1, ..., t_n))}{\forall t \in T_\Sigma.\ P(t)}$$

Corollary

$T_\Sigma, \prec^+$ is w.f.

Because $\prec^+$ is the transitive closure of a w.f. relation

Example

$\Sigma_0 = \{0\} \quad \Sigma_1 = \{\mathsf{succ}\} \quad \Sigma_2 = \{\mathsf{plus}\}$

$$0 \prec^+ \mathsf{succ}(0) \prec^+ \mathsf{plus}(0, \mathsf{succ}(0))$$

$$0 \prec^+ \mathsf{plus}(0, \mathsf{succ}(0))$$

$$0 \prec^+ \mathsf{plus}(\mathsf{succ}(0), \mathsf{succ}(0))$$

Termination of arithmetic expressions

$$a ::= x \mid n \mid a \text{ op } a$$

$$x \in \text{Ide} \qquad \text{op} \in \{+, \times, -\}$$

$$n \in \mathbb{Z} \qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : \text{Ide} \to \mathbb{Z}\}$$

$$\frac{}{\langle x, \sigma\rangle \longrightarrow \sigma(x)} \qquad \frac{}{\langle n, \sigma\rangle \longrightarrow n} \qquad \frac{\langle a_0, \sigma\rangle \longrightarrow n_0 \quad \langle a_1, \sigma\rangle \longrightarrow n_1}{\langle a_0 \text{ op } a_1, \sigma\rangle \longrightarrow n_0 \; op \; n_1}$$

$$P(a) \triangleq \forall \sigma \in \mathbb{M}.\ \exists m \in \mathbb{Z}.\ \langle a, \sigma\rangle \longrightarrow m$$

$$\forall a.\ P(a)\ ?$$

Structural induction principle

$$\frac{\forall a_0, a_1.\ P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \ \mathsf{op}\ a_1)}{\forall a.\ P(a)}$$

$\forall x \in \mathsf{Ide}.\ P(x)$ $\qquad$ $\forall n \in \mathbb{Z}.\ P(n)$

Base case

$\forall x \in \mathsf{Ide}.\ P(x)$ Take a generic $x \in \mathsf{Ide}$

We want to prove $P(x) \triangleq \forall \sigma.\ \exists m.\ \langle x, \sigma \rangle \longrightarrow m$

Take a generic $\sigma \in \mathbb{M}$ and consider the goal $\langle x, \sigma \rangle \longrightarrow m$ (the only variable)

By rule $\dfrac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)}$ we have $\langle x, \sigma \rangle \longrightarrow m \nwarrow_{[m=\sigma(x)]} \square$

And we are done (taking $m = \sigma(x)$)

Base case

$\forall n \in \mathbb{Z}.\ P(n)$ Take a generic $n \in \mathbb{Z}$

We want to prove $P(n) \triangleq \forall \sigma.\ \exists m.\ \langle n, \sigma \rangle \longrightarrow m$

Take a generic $\sigma \in \mathbb{M}$ and consider the goal $\langle n, \sigma \rangle \longrightarrow m$

the only variable

By rule $\dfrac{}{\langle n, \sigma \rangle \longrightarrow n}$ we have $\langle n, \sigma \rangle \longrightarrow m \nwarrow_{[m=n]} \square$

And we are done (taking $m = n$)

Inductive case

$\forall a_0, a_1.\ P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \text{ op } a_1)$ Take generic a_0, a_1

We assume $P(a_0) \triangleq \forall \sigma.\ \exists m_0.\ \langle a_0, \sigma \rangle \longrightarrow m_0$

$P(a_1) \triangleq \forall \sigma.\ \exists m_1.\ \langle a_1, \sigma \rangle \longrightarrow m_1$

We want to prove $P(a_0 \text{ op } a_1) \triangleq \forall \sigma.\ \exists m.\ \langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow m$

Inductive case (ctd)

Take a generic $\sigma \in \mathbb{M}$ and consider the goal $\langle a_0 \text{ op } a_1, \sigma\rangle \longrightarrow m$

By rule $\dfrac{\langle a_0, \sigma\rangle \longrightarrow n_0 \quad \langle a_1, \sigma\rangle \longrightarrow n_1}{\langle a_0 \text{ op } a_1, \sigma\rangle \longrightarrow n_0 \; op \; n_1}$ we have

$\langle a_0 \text{ op } a_1, \sigma\rangle \longrightarrow m \nwarrow_{[m=m_0 \, op \, m_1]} \langle a_0, \sigma\rangle \longrightarrow m_0 \, , \, \langle a_1, \sigma\rangle \longrightarrow m_1$

By inductive hypotheses, there are m_0, m_1 s.t.
$\langle a_0, \sigma\rangle \longrightarrow m_0$ and $\langle a_1, \sigma\rangle \longrightarrow m_1$

And we are done (taking $m = m_0 \; op \; m_1$)