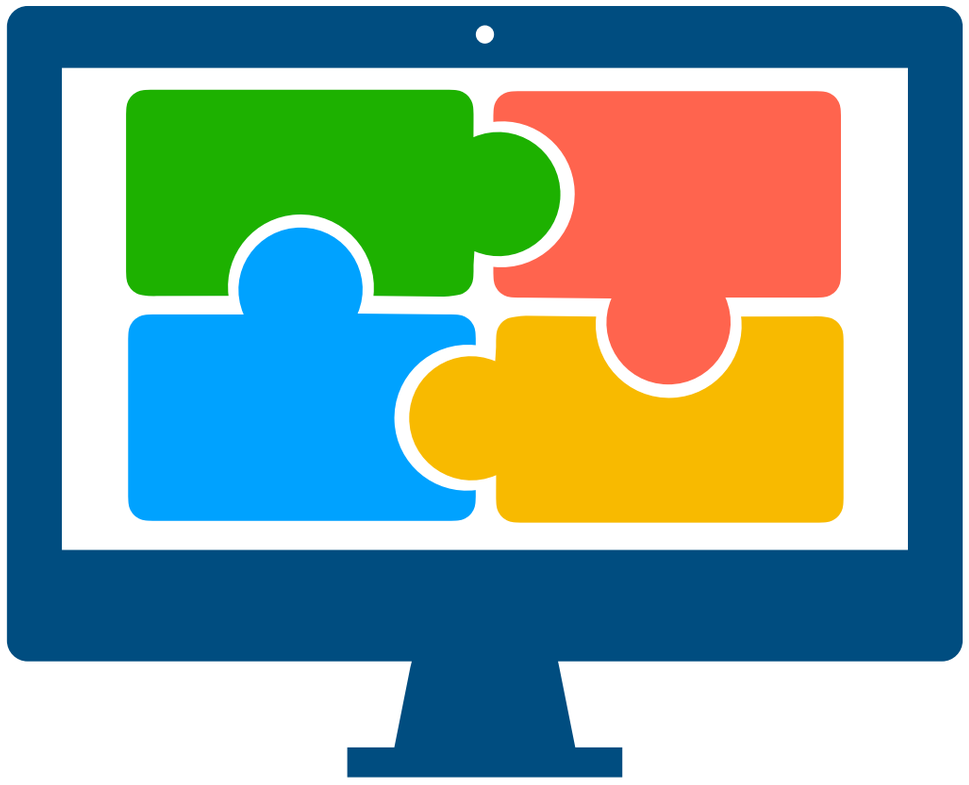


Linguaggi di Programmazione

Roberta Gori

Induzione 3-4

Induzione

Come facciamo a

dimostrare un'affermazione esistenziale? $\exists x.\ P(x)$

mostriamo un testimone

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

confutare un'affermazione universale? $\neg \forall x.\ P(x) \equiv \exists x.\ \neg P(x)$

mostriamo un controesempio a P

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

dimostrare un'affermazione universale? $\forall x.\ P(x)$

usiamo l'induzione!

Cosa hanno in comune

numeri naturali

liste

alberi

grammatiche

termini di una segnatura

teoremi di un sistema logico

derivazioni

computazioni

sono generati da un numero finito di applicazioni di regole

caso base

caso induttivo

Cosa hanno in comune

	caso base	caso induttivo
numeri naturali	0	succ
liste	nil	cons
alberi	nil	node
grammatiche di linguaggi	produzioni con solo simboli terminali	produzioni con simboli non terminali
termini della segnatura	costanti	functor
teoremi di un sistema logico	assiomi	regole di inferenza
derivazioni	assiomi	regole di inferenza
computazioni	passo singolo	concatenazione di passi

Una dimostrazione famosa

Ogni numero maggiore di 1 o e' primo o può essere scritto come il prodotto di due o più numeri primi

caso base $(n = 2)$**:** 2 è primo

caso induttivo: preso un generico n, assumiamo che la proprietà valga per tutti i numeri da 2 a n e proviamo a dimostrarla per $n + 1$:

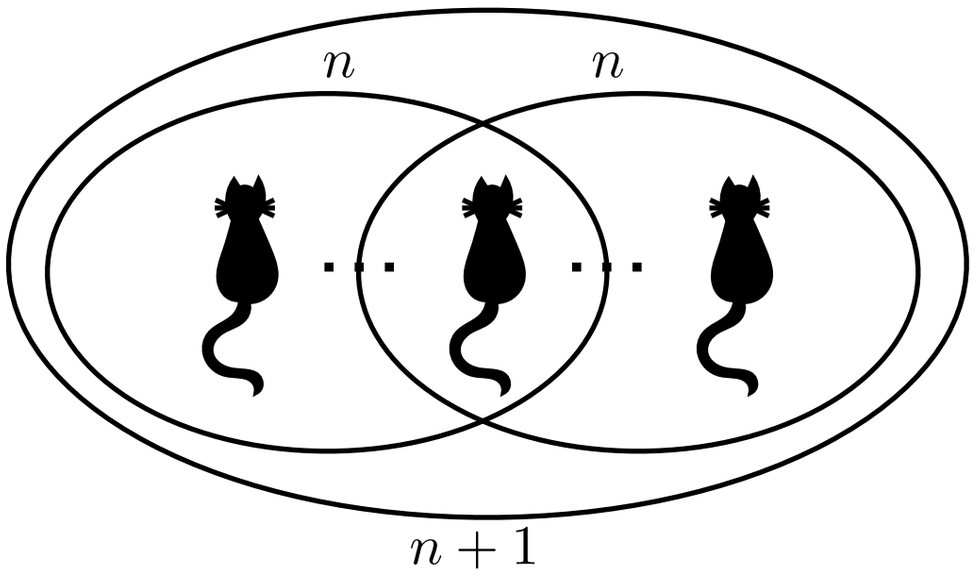
- se $n + 1$ è primo abbiamo finito;
- altrimenti, sia $n + 1 = a \cdot b$ per qualche $1 < a$ e $b <= n$. Per ipotesi induttiva a e b possono essere riscritti come prodotto di numeri primi. Sia $a = p_1 \cdot ... \cdot p_k$ e $b = q_1 \cdot ... \cdot q_h$. Allora $n+1 = a \cdot b = p_1 \cdot ... \cdot p_k \cdot q_1 \cdot ... \cdot q_h$ puo' essere riscritto come prodotto di $k + h$ numeri primi.

Una prova meno conosciuta

Tutti i gatti sono dello stesso colore

caso base (n=1): ovvio

caso induttivo: preso un generico n, assumiamo che la proprietà valga per tutti i gruppi con $k \leq n$ gatti e proviamo a dimostrarla per un gruppo di $n+1$ gatti:
Prendiamo $n+1$ e mettiamoli su una linea.
Per ipotesi induttiva i primi $n-1$ gatti sono tutti dello stesso colore.
Per ipotesi induttiva gli ultimi $n-1$ gatti sono tutti dello stesso colore.
Dal momento che i gatti nel mezzo appartengono a entrambi i gruppi, per transitività tutti i gatti sono dello stesso colore.



Induzione ben fondata

Ingredienti

un insieme di elementi A (possibilmente infinito)

un predicato $P : A \to \mathcal{B}$

vogliamo provare $\forall a \in A.P(a)$

una relazione binaria di precedenza $\prec \subseteq A \times A$

(non necessariamente transitiva)

$a \prec b$ si legge a precede b

scritto anche come $b \succ a$

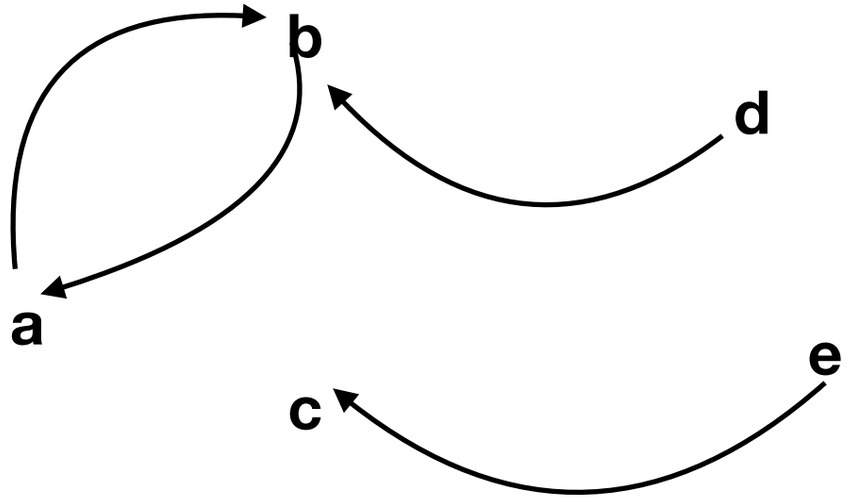
non sono ammesse catene discendenti infinite in $\prec$

relazione ben fondata

Grafo di una relazione

- A={a,b,c,d,e}

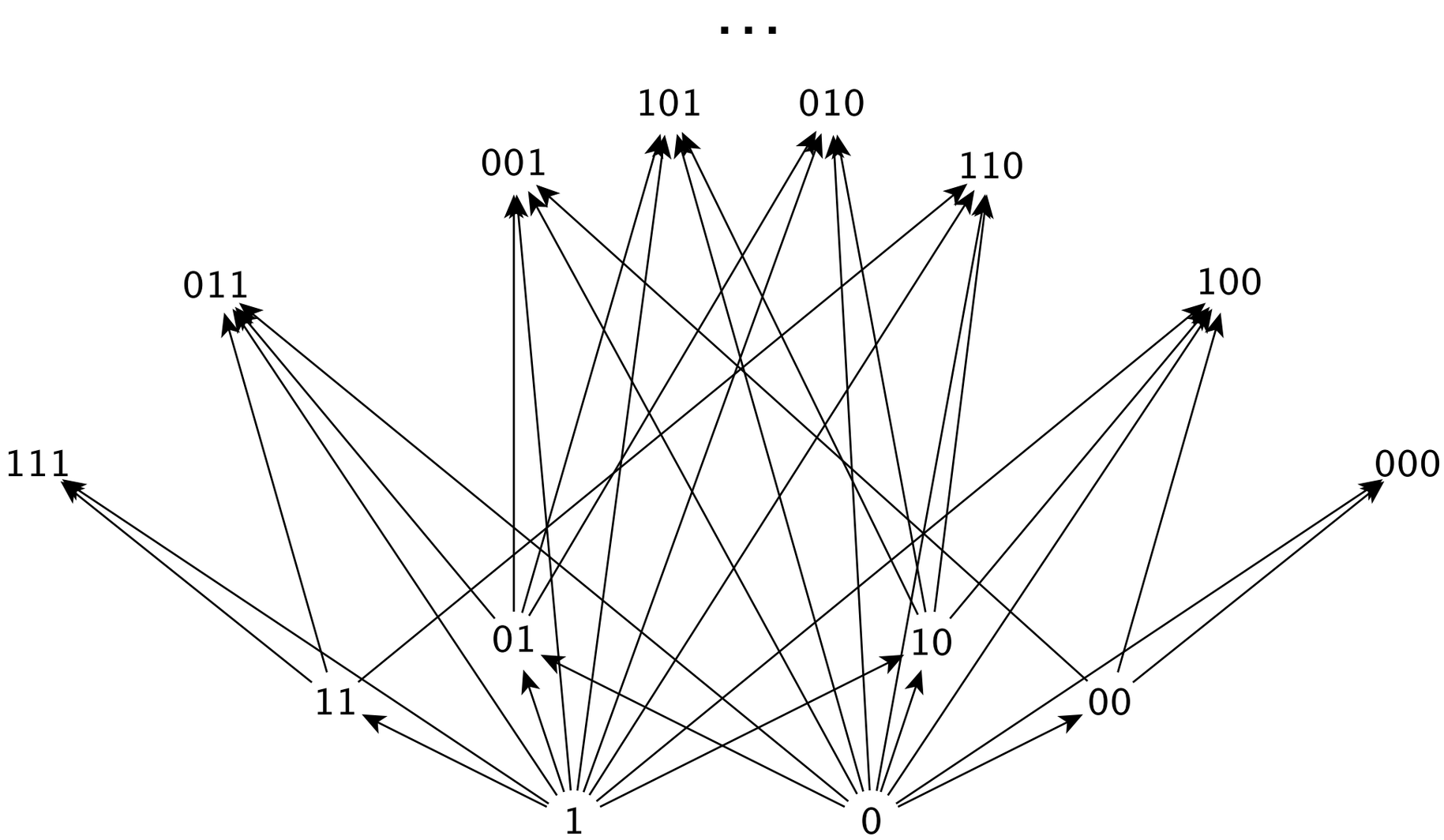
$$a \prec b,\ b \prec a,\ d \prec b \text{ e } e \prec c$$



Grafo di una relazione

Esempio:

$A = \mathbb{B}^*$ $\quad u \prec w$ se u appare in w (con $u \neq \epsilon$ e $u \neq w$)



Catene discendenti infinite

Catene discendenti infinite

una sequenza infinita $\{a_i\}_{i\in\mathbb{N}}$ di elementi di A
tali che $\forall i \in \mathbb{N}. a_i \succ a_{i+1}$

la sequenza puo' essere anche vista come una funzione $a : \mathbb{N} \to A$

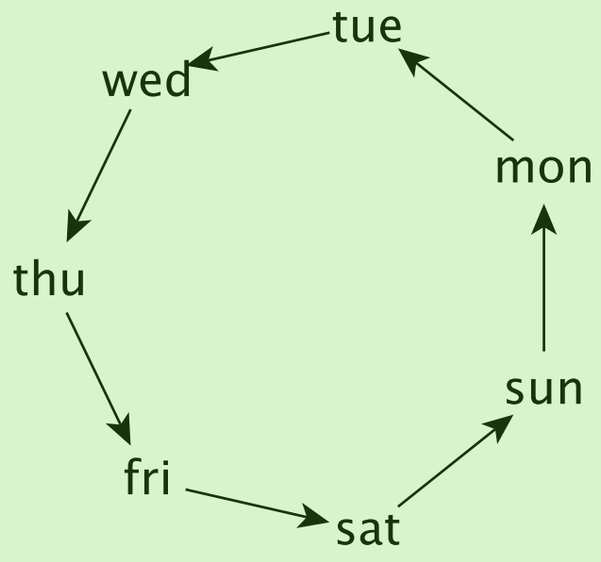
$$a(n) = a_n$$

$$a(0) \succ a(1) \succ a(2)....$$

Esempio

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

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



Relazioni ben fondate

Una relazione si dice ben fondata
se non ha catene discendenti infinite

$\mathbb{N}$	$n \prec m$ 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 $n = m$	✗

Chiusura transitiva

una relazione binaria $\prec \subseteq A \times A$

la sua chiusura transitiva $\prec^+ \subseteq A \times A$

e' la piu' piccola relazione generata dalle regole

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

dalla prima regola, e' ovvio che $\prec \subseteq \prec^+$

si puo' dimostrare che $(\prec^+)^+ = \prec^+$

Chiusura transitiva e riflessiva

una relazione binaria $\prec \subseteq A \times A$

la sua chiusura transitiva e riflessiva $\prec^* \subseteq A \times A$

e' la piu' piccola relazione generata dalle regole

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

e' ovvio che $\prec \subseteq \prec^+ \subseteq \prec^*$

si puo' dimostrare che $(\prec^*)^* = \prec^*$

Chiusure e cammini

una relazione binaria $\prec \subseteq A \times A$

$a \prec^+ b$ sse c'è un cammino non vuoto da a a b nel grafo di $\prec$

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

$a \prec^* b$ sse c'è un cammino eventualmente vuoto da a a b nel grafo di $\prec$

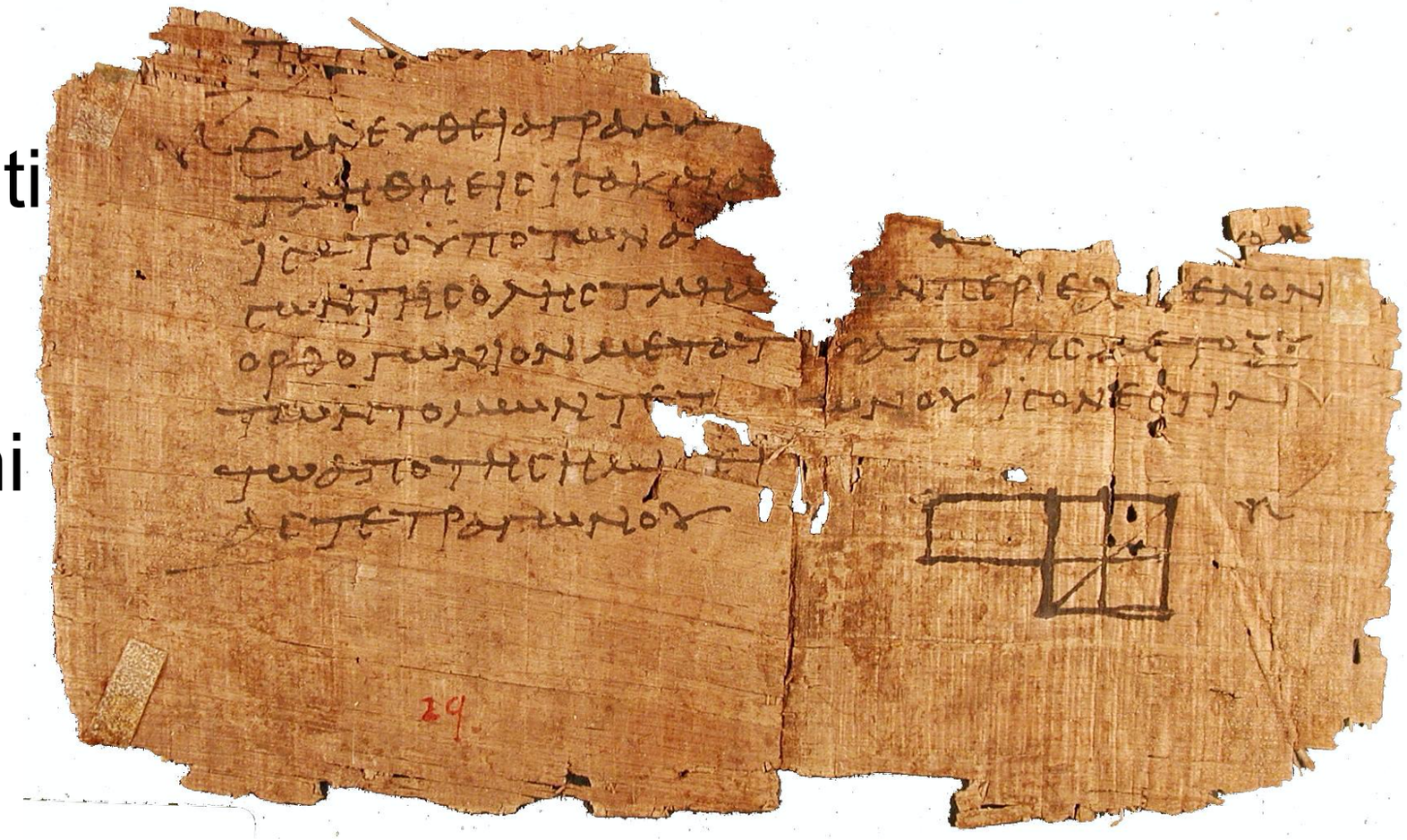
$$\exists k \geq 0, \{c_i\}_{i \in [0,k]}.\ a = c_0 \prec c_1 \prec \cdots \prec c_k = b$$

Chiusure

		$\prec^+$	$\prec^*$
$\mathbb{N}$	$n \prec m$ 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 $n = m$	$n = m$	$n = m$

Teoremi incluse le prove

sulla destra, si vede uno dei più antichi frammenti sopravvissuti degli Elementi di Euclide, un libro di testo usato per millenni per insegnare le tecniche di scrittura di prove
(source: *wikipedia*)



Teorema

Una relazione è ben fondata sse (se e solo se) la sua chiusura transitiva è ben fondata

$\prec^+$ è ben fondata $\Rightarrow$ $\prec$ è ben fondata

ovvio:
ogni catena discendente per $\prec$ è anche una catena discendente per $\prec^+$ ed è finita perchè $\prec^+$ è ben fondata

Teorema

Una relazione è ben fondata sse (se e solo se) la sua chiusura transitiva è ben fondata

$\prec$ è ben fondata $\Rightarrow$ $\prec^+$ è ben fondata $\quad \equiv \neg(\prec^+ \text{ b.f.}) \Rightarrow \neg(\prec \text{ b.f.})$

per contrapposizione: assumiamo che $\prec^+$ non sia ben fondata e proviamo che neanche $\prec$ lo è. Consideriamo una catena discendente infinita per $\prec^+$

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

per definizione, $a \prec^+ b$ sse esiste un cammino non vuoto da a a b nel grafo di $\prec$

$$a_0 \succ ... \succ a_1 \succ ... \succ a_2 \succ ...$$

quindi abbiamo che anche la catena di $\prec$ è discendente infinita

Relazioni Acicliche

una relazione binaria $\prec \subseteq A \times A$

$\prec$ ha un ciclo se $a \prec^+ a$ per qualche $a \in A$

Diciamo che $\prec$ è aciclica se non ha cicli

Notate che $\prec$ è aciclica sse $\prec^+$ lo è

Teorema

Se una relazione e' ben fondata allora e' acicliche

Per contrapposizione:
proviamo che se $\prec$ ha un ciclo allora non è ben fondata. Consideriamo $a \in A$ tale che $a \prec^+ a$ allora abbiamo una catena discendente infinita per $\prec^+$

$$a \succ^+ a \succ^+ a \succ^+ ...$$

quindi abbiamo che $\prec^+$ non è ben fondata
per il teorema precedente neanche $\prec$ è ben fondata.

Teorema

Se A è finito e $\prec$ è aciclica allora $\prec$ è ben fondata

La prova utilizza il principio dei piccioni

Il principio dei piccioni

Se n oggetti sono posti in $m < n$ slots,
allora almeno uno slot contiene piú di un oggetto

nella figura: 10 piccioni e nove slots

Teorema

Se A è finito e $\prec$ è aciclica allora $\prec$ è ben fondata

Per contrapposizione:
proviamo che se $\prec$ non è ben fondata allora ha un ciclo. Consideriamo una catena discendente infinita per $\prec$,

$$a_0 \succ a_1 \succ a_2 \succ ...$$

$k = |A|$ e prendiamo i primi $k+1$ elementi della catena discendente

$$a_0 \succ a_1 \succ a_2 \succ ... \succ a_k$$

per il principio dei piccioni, $a_i = a_j$ per qualche $0 \leq i < j \leq k$,

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

quindi $a_i \prec^+ a_i$ e $\prec$ ha un ciclo.

Elementi Minimali

una relazione binaria $\prec \subseteq A \times A$

Sia $Q \subseteq A$ e $m \in Q$

m e' minimale in Q se nessun di Q precede m

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

Q non ha elementi minimali sse $\forall m \in Q.\ \exists x \in Q.\ x \prec m$

Elementi Minimali

		Elemento Minimale ?	Unico?
$\mathbb{N}, <$	$\varnothing \subset Q \subseteq \mathbb{N}$	✓	✓
$\mathbb{Z}, <$	$\varnothing \subset Q \subseteq \mathbb{Z}$	✓/✗	✓
$\wp(\mathbb{N}), \subset$	$\varnothing \subset Q \subseteq \wp(\mathbb{N})$	✓/✗	✓/✗

Lemma

$\prec$ è b.f. sse ogni $\emptyset \neq Q \subseteq A$ ha un elemento minimale

$\equiv$

① $\prec$ ha una catena discendente infinita sse

② $\exists Q \subseteq A$ non vuoto che non ha elementi minimali

① $\Rightarrow$ ②

Consideriamo l'insieme $Q = \{a_i \mid i \in \mathbb{N}\}$. Q non ha elementi minimali. Se ne avesse uno, diciamo a_k, avremmo che $a_{k+1} \succ a_k$.

Lemma

$\prec$ è b.f. sse ogni $\emptyset \neq Q \subseteq A$ ha un elemento minimale

$\equiv$

① $\prec$ ha una catena discendente infinita sse

② $\exists Q \subseteq A$ non vuoto che non ha elementi minimali

② $\Rightarrow$ ①

Considera $\emptyset \neq Q \subseteq A$ che non ha un elemento minimale.

Dal momento che $\emptyset \neq Q$ scegliamo un $a_0 \in Q$.

Dal momento che a_0 non è minimale, possiamo considerare $a_1 \in Q$ tale che $a_1 \prec a_0$

Dal momento che a_1 non è minimale, possiamo considerare $a_2 \in Q$ tale che $a_2 \prec a_1$

....

Dal momento che a_k non è minimale, possiamo considerare $a_{k+1} \in Q$ tale che $a_{k+1} \prec a_k$

....

Teorema [induzione b.f.]

Sia $\prec \subseteq A \times A$ b.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 $\forall a.\ P(a)$ $\qquad$ Take a generic $a \in A$

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

Teorema [induzione b.f.]

Sia $\prec \subseteq A \times A$ b.f.

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

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

② ⇒ ① ≡ ¬① ⇒ ¬②

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

perche' almeno a appartiene a Q

Prendiamo $Q = \{q \in A \mid \neg P(q)\} \neq \emptyset$
Dal momento che $\prec$ è b.f., sappiamo che Q ha un elemento minimale $m \in Q$

Ovviamente, $\neg P(m)$ (perchè $m \in Q$)
m è minimale, quindi $\forall b \prec m.b \notin Q$
cioè $\forall b \prec m.P(b) \ \equiv \ H(m)$

Thus $H(m) \wedge \neg P(m) \ \equiv \ \neg(H(m) \Rightarrow P(m)) \ \equiv \ \neg S(m)$
cioè $\exists a \in A.\neg S(a)$

Principio di induzione b.f.

una relazione b.f. $\prec \subseteq A \times A$

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

Vantaggio: quando proviamo $P(a)$ per un a generico, possiamo usare l'assunzione $\forall b \prec a.P(b)$!

Deriviamo il principio di induzione matematica debole

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

$A = \mathbb{N}$

$\prec = \{(n, n+1) \mid n \in \mathbb{N}\}$ (relazione di precedenza immediata)

- se $a = 0$, allora non esiste un $b \prec 0$, per cui $(\forall b \prec 0.P(b)) \equiv tt$ e $((\forall b \prec 0.P(b)) \Rightarrow P(0)) \equiv tt \Rightarrow P(0) \equiv P(0)$

- se $a = n + 1$, allora esiste un solo b tale che $b \prec n + 1$, ovvero $b = n$ allora $((\forall b \prec n + 1.P(b)) \Rightarrow P(n + 1)) \equiv P(n) \Rightarrow P(n + 1)$

Principio di Induzione matematica debole

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

Debole: possiamo assumere P(n) per provare P(n+1)!

Deriviamo il principio di induzione matematica forte

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

$A = \mathbb{N}$

$\prec = <$ (minore stretto)

- come prima se $a = 0$, allora non esiste un $b \prec 0$, per cui $(\forall b \prec 0.P(b)) \equiv tt$
  e
  $((\forall b \prec 0.P(b)) \Rightarrow P(0)) \equiv P(0)$
- se $a = n + 1$, allora $((\forall b \prec n + 1.P(b)) = P(0) \wedge P(1) \wedge ... \wedge P(n)$
  allora $((\forall b \prec n+1.P(b)) \Rightarrow P(n+1)) \equiv P(0) \wedge P(1) \wedge ... \wedge P(n) \Rightarrow P(n+1)$

Principio di induzione matematica forte

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

Forte: possiamo assumere piu' di P(n) per provare P(n+1)!

Induzione Strutturale

Relazione di sottotermine immediato

$$\text{una segnatura } \{\Sigma_n\}_n \in \mathbf{N}$$

$$\text{prendiamo } A = T_\Sigma \text{ (termini chiusi)}$$

senza variabili!

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

(relazione di sottotermine immediato)

Esempio

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

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

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

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

Lemma

$T_\Sigma, \prec$ è b.f.

Definiamo $depth : T_\Sigma \to \mathbb{N}$

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

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

Per definizione, se $t \prec t'$ allora $depth(t) < depth(t')$

Ogni catena discendente in $\prec$ induce una catena discendente in $<$

Dal momento che $<$ è b.f. anche $\prec$ è b.f.

Principio di induzione strutturale

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

Corollario

T_Σ, $\prec^+$ è b.f.

Perchè $\prec^+$ è la chiusura transitiva di una relazione b.f.

Esempio

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

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

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

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

Terminazione di espressioni aritmetiche

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

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

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

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

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

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

Principio di induzione strutturale

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

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

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

Caso Base

$\forall x \in \mathsf{Ide}.\ P(x)$ Prendiamo un generico $x \in Ide$

Vogliamo provare $P(x) \triangleq \forall \sigma.\ \exists m.\ \langle x, \sigma \rangle \longrightarrow m$

la sola variabile

Prendiamo un generico $\sigma \in \mathbf{M}$ e consideriamo il goal $\langle x, \sigma \rangle \to m$

Dalla regola $\dfrac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)}$ abbiamo $\langle x, \sigma \rangle \longrightarrow m \nwarrow_{[m=\sigma(x)]} \square$

Abbiamo finito (considerando $m = \sigma(x)$)

Caso Base

$\forall n \in \mathbb{Z}.\ P(n)$ Prendiamo un generico $n \in Z$

Vogliamo provare $P(n) \triangleq \forall \sigma.\ \exists m.\ \langle n, \sigma \rangle \longrightarrow m$

Prendiamo un generico $\sigma \in \mathbf{M}$ e consideriamo il goal $\langle n, \sigma \rangle \to m$

Dalla regola $\dfrac{}{\langle n, \sigma \rangle \longrightarrow n}$ abbiamo $\langle n, \sigma \rangle \longrightarrow m \nwarrow_{[m=n]} \square$

Abbiamo finito (considerando $m = n$)

Caso Induttivo

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

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

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

Vogliamo provare $P(a_0 \text{ op } a_1) \triangleq \forall \sigma.\ \exists m.\ \langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow m$

Caso Induttivo (cont.)

Prendiamo un generico $\sigma \in \mathbf{M}$ e consideriamo il goal $\langle a_0\, op\, a_1, \sigma\rangle \to m$

Per la regola $\dfrac{\langle a_0, \sigma\rangle \longrightarrow n_0 \quad \langle a_1, \sigma\rangle \longrightarrow n_1}{\langle a_0 \text{ op } a_1, \sigma\rangle \longrightarrow n_0\ op\ n_1}$ abbiamo

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

Per ipotesi induttiva, esistono m_0, m_1 tali che
$\langle a_0, \sigma\rangle \to m_0$ e $\langle a_1, \sigma\rangle \to m_1$

Abbiamo finito (considerando $m = m_0\, op\, m_1$)