Induzione

- Definizione induttiva di insiemi e funzioni
- Principio di induzione strutturale

- Gli insiemi definiti per induzione ricevono una struttura che può servire come base per la definizione induttiva di funzioni su di essi
- Le tecniche induttive sono utili nella verifica dei programmi

Principio di induzione sui numeri naturali

Formulazione I

Per dimostrare che una proprietà P vale per tutti i numeri $n \in Nat$ è sufficiente mostrare che

a. CASO BASE: P vale per 0

b. PASSO INDUTTIVO: Se P vale per un numero $n \in Nat$ allora P vale anche per $n + 1$

Questa formulazione è maggiormente connessa al fatto che i numeri naturali possono essere costruiti iniziando con il numero 0 e aggiungendo ripetutamente un'unità

Principio di induzione sui numeri naturali (ctnd.)

Formulazione II (induzione forte)

Per dimostrare che una proprietà P vale per tutti i numeri $n \in Nat$ è sufficiente mostrare che

a. CASO BASE: P vale per 0

b. PASSO INDUTTIVO: Se $n \in Nat$ e P vale per tutti gli $m \in Nat$ tali che $m < n$, allora P vale anche per n

Questa formulazione ha più a che fare con l'ordinamento dei numeri naturali.

Può essere più conveniente della prima formulazione nel caso di dimostrazioni in cui ci viene più comodo dimostrare il passo induttivo (b) con numeri più piccoli del predecessore del numero in questione

Definizione induttiva di insiemi

Sia $\mathcal{U}$ un insieme detto *universo*, $B \subseteq \mathcal{U}$ un insieme detto *insieme base*

Sia $\mathcal{K}$ un insieme di relazioni $r \subseteq \mathcal{U}^n \times \mathcal{U}$ (dove $n \geq 1$ dipende da r) detto insieme dei costruttori

Un insieme $A \subseteq \mathcal{U}$ viene detto *definito induttivamente* (o *ricorsivamente*) da B e $\mathcal{K}$, quando A è il più piccolo (rispetto all'inclusione insiemistica) di tutti i sottoinsiemi S di $\mathcal{U}$ per cui valgono le seguenti due condizioni:

a. $B \subseteq S$

b. $r(S^n) \subseteq S$ per tutti gli $r \in \mathcal{K}$ cioé se $a_1, \ldots, a_n \in S$ e $((a_1, \ldots, a_n), a) \in r$ allora $a \in S$

Esempio di insieme costruito induttivamente - Termini della logica del I Ordine

L'insieme T_B dei termini del linguaggio del I ordine di base B viene costruito induttivamente

- $x \in Var$, allora $x \in T_B$
- $c \in \mathcal{F}$, allora $c \in T_B$
- $f \in \mathcal{F}$ con arietà $n \geq 1$ e $t_1, \ldots, t_n \in T_B$, allora $f(t_1, \ldots, t_n) \in T_B$

Esempio di insieme costruito induttivamente - Programmi while

Sia $B = (\mathcal{F}, \mathcal{P})$ una base, allora l'insieme L_2^B dei programmi while su B viene definito induttivamente

a. Statement di assegnamento

   Per ogni variabile $x \in Var$ e ogni termine t della logica predicativa

$$x := t \qquad \text{è un programma while}$$

b. Statement composto

   Siano S_1 ed S_2 due programmi while, allora $S_1; S_2$ è un programma while

Esempio di insieme costruito induttivamente - Programmi while

c. Statement condizionale

Siano S_1, S_2 due programmi while ed e una formula della logica predicativa priva di quantificatori,

allora

`if` e `then` S_1 `else` S_2 `fi`

è un programma while

d. While loop

Sia S_1 un programma while ed e una formula della logica predicativa priva di quantificatori,

allora

`while` e `do` S_1 `od` è un programma while

Definizione costruttiva di un insieme definito per induzione

Sia $\mathcal{U}$ un insieme detto *universo*, $B \subseteq \mathcal{U}$ un insieme detto *insieme base*

Sia $\mathcal{K}$ un insieme di relazioni $r \subseteq \mathcal{U}^n \times \mathcal{U}$ (dove $n \geq 1$ dipende da r) detto *insieme dei costruttori*

Una sequenza $u_1, \ldots, u_m$ $(m \geq 1)$ di elementi di $\mathcal{U}$ con $u_m = u$ viene detta una *sequenza di costruzione* per u (da B e $\mathcal{K}$) quando per ogni $i = 1, \ldots, m$, accade che o

a. $u_i \in B$, oppure

b. esiste un costruttore $r \subseteq \mathcal{U}^n \times \mathcal{U}$, $r \in \mathcal{K}$ e $i_1, \ldots, i_n < i$ tali che $((u_{i_1}, \ldots, u_{i_n}), u_i) \in r$

Definizione costruttiva di un insieme definito per induzione (ctnd.)

$\bar{A}$ viene detto *definito induttivamente* da B e da $\mathcal{K}$ quando $\bar{A}$ è costituito da tutti quegli elementi $u \in \mathcal{U}$, per cui esiste una sequenza di costruzione da B e da $\mathcal{K}$

Di particolare interesse è il caso in cui questo processo di costruzione descrive in modo non ambiguo come ottenere un elemento dell'insieme

Definizione induttiva libera

La definizione induttiva di un insieme mediante un insieme base B ed un insieme di costruttori $\mathcal{K}$ viene detta *libera* se per ogni elemento $a \in A$, accade che o

- $a \in B$, oppure
- c'è soltanto un costruttore $r \in \mathcal{K}$, e solo una n-tupla di elementi $a_1, \ldots, a_n \in A$ tali che $((a_1, \ldots, a_n), a) \in r$

Principio di induzione strutturale

Sia $A \subseteq \mathcal{U}$ definito induttivamente mediante l'insieme base B e l'insieme dei costruttori $\mathcal{K}$.

Per dimostrare che una proprietà P vale per tutti gli $a \in A$ è sufficiente notare che

a) CASO BASE: P vale per tutti gli $a \in B$

b) PASSO INDUTTIVO: Se P vale per $a_1, \ldots, a_n \in A$ (ipotesi induttiva) e $((a_1, \ldots, a_n), a) \in r$ per qualche $r \in \mathcal{K}$, allora P vale anche per a

Principio di induzione strutturale (ctnd 1.)

Dim:

Sia $C \subseteq A$ l'insieme degli elementi di A per cui la proprietà P vale.

Bisogna mostrare che $a)$ e $b)$ implicano che P vale per tutti gli $a \in A$, cioé $A \subseteq C$.

Da $a)$ si ha che $B \subseteq C$, mentre da $b)$ si ha che se $a_1, \ldots, a_n \in C$ e $((a_1, \ldots, a_n), a) \in r$ per qualche $r \in \mathcal{K}$, allora $a \in C$.

Dunque $C \supseteq A$, e poiché per hp. $C \subseteq A$, si ha che $C = A$.

Principio di induzione strutturale (ctnd 2.)

Una dimostrazione per induzione strutturale può essere sempre sostituita con una dimostrazione per induzione sui naturali

Il "trucco" è cambiare la dimostrazione in modo che essa diventi per induzione sulla *profondità* degli elementi

Quando l'insieme A viene definito induttivamente dall'insieme base B e dall'insieme dei costruttori $\mathcal{K}$, esiste almeno una sequenza di costruzione per ogni $a \in A$

$$d(a) = \min\{m \in Nat | u_1, \ldots, u_m \text{ è una sequenza di costruzione di a}\} - 1$$

Principio di induzione strutturale (ctnd 3.)

Sia P una proprietà e definiamo Q come

"P vale per tutti gli $a \in A$ di profondità $d(a) = n$"

Le due asserzioni
"P vale per tutti gli $a \in A$ "
e
"Q vale per tutti gli $n \in Nat$"

sono equivalenti

Principio di induzione strutturale (ctnd 4.)

Una dimostrazione per induzione strutturale di P può essere tradotta in una dimostrazione di Q con l'induzione sui naturali

- $d(a) = 0$ se e solo se $a \in B$
- $d(a) > d(a_i)$, $i = 1, \ldots, n$ quando $((a_1, \ldots, a_n), a) \in r$ per qualche $r \in \mathcal{K}$

NOTA: l'induzione strutturale non è più potente dell'induzione su Nat.

Definizione di funzioni per induzione

Sia $A \subseteq \mathcal{U}$ definito induttivamente dalla base B e dall'insieme di costruttori $\mathcal{K}$.
Sia V un insieme arbitrario.

Associamo

- ad ogni elemento $a \in B$ un elemento $h(a) \in V$
- ad ogni costruttore $r \subseteq \mathcal{U}^n \times \mathcal{U} \in \mathcal{K}, (n \geq 1)$, una funzione $h(r) : V^n \rightarrow V$

Definizione di funzioni per induzione (ctnd.)

Una definizione induttiva di una funzione $g : A \to V$ viene data da

a) $g(a) = h(a)$ per ogni elemento $a \in B$

b) $g(a) = h(r)(g(a_1), \ldots, g(a_n))$
cioé $(a, h(r)(b_1, \ldots, b_n)) \in g$ se $(a_1, b_1), \ldots, (a_n, b_n) \in g$ per tutti gli $r \subseteq \mathcal{U}^n \times \mathcal{U}$, e $a_1, \ldots, a_n \in A$ con $((a_1, \ldots, a_n), a) \in r$

Questa definizione è consistente solo se ad ogni $a \in A$ viene assegnato esattamente un valore mediante a) oppure b) (cioé se g è una funzione)

Se questa condizione viene soddisfatta diciamo che g è ben definita

Definizione di funzioni per induzione (ctnd 1.)

Teorema di ricorsione

Se la definizione induttiva di un insieme A mediante l'insieme base B e l'insieme dei costruttori $\mathcal{K}$ è libera, allora la funzione $g : A \to V$ definita induttivamente come nella definizione precedente è ben definita

Esempio

Sia $B = (\mathcal{F}, \mathcal{P})$ una base. Dato un programma while $S \in \mathrm{L}_2^B$, costruire un programma flowchart $fc(S) \in \mathrm{L}_1^B$ tale che, comunque io scelga un'interpretazione $\boldsymbol{\mathcal{I}}$,

$$\boldsymbol{\mathcal{M}}_{\boldsymbol{\mathcal{I}}}(S)(\sigma) = \boldsymbol{\mathcal{M}}_{\boldsymbol{\mathcal{I}}}(fc(S))(\sigma)$$

per ogni $\sigma \in \Sigma_{\boldsymbol{\mathcal{I}}}$

Svolgimento

Costruiamo induttivamente la funzione $fc : \mathrm{L}_2^B \to \mathrm{L}_1^B$

- S è il programma $x := t$

  Poniamo $fc(S) = begin : x := t; \mathtt{goto}\, end$.

Esempio

Allora, comunque scelgo $\boldsymbol{\mathcal{I}}$ e σ

$(x := t, \sigma) \Rightarrow (\epsilon, \sigma[x/\boldsymbol{\mathcal{I}}(t)(\sigma)])$
$(begin, \sigma) \Rightarrow (end, \sigma[x/\boldsymbol{\mathcal{I}}(t)(\sigma)])$

- S è il programma $S_1; S_2$

$$fc(S) = fc(S_1)\{end/l_{new}\} \; fc(S_2)'\{begin/l_{new}\}$$

dove $fc(S_2)'$ è ottenuto da $fc(S_2)$ tramite la ridenominazione delle etichette e $l_{new} \notin \mathtt{Lab}(fc(S_1)) \cup \mathtt{Lab}(fc(S_2)')$

Esempio

- S è il programma

  $\texttt{if } e \texttt{ then } S_1 \texttt{ else } S_2 \texttt{ fi}$

  $$fc(S) = begin : \texttt{if } e \texttt{ then goto } l_{new_1} \texttt{ else goto } l_{new_2} \texttt{ fi}$$
  $$fc(S_1)\{begin/l_{new_1}\}$$
  $$fc(S_2)'\{begin/l_{new_2}\}$$

  dove $fc(S_2)'$ è ottenuto da $fc(S_2)$ tramite la ridenominazione delle etichette e $l_{new_1}, l_{new_2} \notin \texttt{Lab}(fc(S_1)) \cup \texttt{Lab}(fc(S_2)')$

Esempio

- S è il programma

  `while` e `do` S_1 `od`

  $$fc(S) = begin : \texttt{if } e \texttt{ then goto } l_{new} \texttt{ else goto } end \texttt{ fi}$$
  $$fc(S_1)\{begin/l_{new}\}\{end/begin\}$$

  dove $l_{new} \notin \texttt{Lab}(fc(S_1))$