

Calcolo dei Sequenti: Induzione e Regole di Inferenza

mace@dsi.unive.it

10 ottobre 2007

1 Principio di induzione

L'insieme \mathbb{N} dei naturali è formato dai numeri $\{0, 1, 2, 3, \dots\}$. Esso può essere direttamente definito partendo dallo 0 e sfruttando la funzione successore “*somma 1*”. Il naturale 1 è ottenuto da $0 + 1$; sommando 1 si ottiene $2 = 0 + 1 + 1$ e così via: $3 = 0 + 1 + 1 + 1$; $4 = 0 + 1 + 1 + 1 + 1$; $5 = 0 + 1 + 1 + 1 + 1 + 1$; $6 = \dots$

Il *principio di induzione* sfrutta questo fatto e dice che *se sono verificate queste due condizioni*

Base dell'induzione – *una proprietà P vale per 0*

Passo induttivo – *assumendo che la proprietà P sia valida per un qualsiasi naturale n si riesce a dimostrare che P è valida anche per $n + 1$*

allora possiamo concludere che la proprietà P vale per tutti i naturali.

In pratica il passo induttivo è una procedura che trasforma una prova del fatto che P vale per n in una prova del fatto che P vale per $n + 1$. La base dell'induzione è il punto di partenza del ragionamento: dopo che si è provato che P vale per 0, applicando la procedura del passo induttivo si ottiene che P vale anche per 1, quindi applicando ancora la stessa procedura si ottiene che P vale per 2, poi ancora per 3, per 4 e così via considerando ogni naturale.

Per avere un'intuizione¹ ‘informatica’ si può pensare al principio di induzione come ad un programma che parte dimostrando che la proprietà P vale in 0 e poi fa partire un ciclo `for` che ad ogni iterazione sfrutta il fatto che P vale in n per dimostrare che P vale anche in $n + 1$. Visto che la procedura chiamata ad ogni iterazione è sempre la stessa, basta che essa sia verificata una sola volta (per un n generale). Scritto in pseudo-codice il principio di induzione funziona più o meno così:

Verifica P in m :

1. Prova P per $n:=0$;
2. `for` $x:=0$ `to` $m-1$ `do` ‘sapendo che P vale in x prova che P vale in $x+1$ ’
3. hai provato che P vale in m !

Noi dobbiamo solo dimostrare la riga 1 del codice, ovvero la base dell'induzione, e trovare un metodo per passare da x a $x+1$ alla riga 2 del codice, ovvero il passo induttivo.

Ci sarà utile anche il *principio di induzione generalizzato* che dice che *se sono verificate queste due condizioni*

Base dell'induzione – *una proprietà P vale per 0*

Passo induttivo – *assumendo che la proprietà P sia valida per tutti i naturali fino ad un certo n si riesce a dimostrare che P è valida anche per $n + 1$*

allora possiamo concludere che la proprietà P vale per tutti i naturali.

¹Grazie a Samuel Rota Bulò per l'osservazione.

Esercizio. *Mostrare che per ogni naturale m vale $0 + 1 + 2 + \dots + m = m(m + 1)/2$*

Procediamo per induzione. La base dell'induzione dice di verificare che $0 = 0(0 + 1)/2$ e questo si vede facilmente. Per il passo induttivo, fissiamo un naturale n e supponiamo che $0 + 1 + 2 + \dots + n = n(n + 1)/2$ sia vero. Allora $0 + 1 + 2 + \dots + n + (n + 1) = n(n + 1)/2 + (n + 1)$. Ora portando tutto a denominatore comune: $n(n + 1)/2 + (n + 1) = [n(n + 1) + 2(n + 1)]/2 = (n + 1)(n + 2)/2$. E questo ci dice proprio che la proprietà richiesta vale anche per $n + 1$. Il principio di induzione ci fa concludere che la proprietà considerata vale per tutti i naturali.

2 Induzione e derivazioni

Con un semplice esercizio mostriamo come sfruttare il principio di induzione quando studiamo le derivazioni nel calcolo dei sequenti.

Esercizio. *Consideriamo un nuovo calcolo dei sequenti S costituito dal sistema LJ privo delle regole strutturali di indebolimento e contrazione, in cui l'assioma di identità è esteso con la seguente nuova forma di identità:*

$$\Gamma, A \vdash A \quad (id2)$$

Mostrare che

$$\text{se il sequente } \Gamma \vdash C \text{ è derivabile in } S, \text{ allora anche il sequente } \Gamma, A \vdash C \text{ è derivabile in } S. \quad (1)$$

Questa proprietà si prova per induzione sulla lunghezza delle derivazioni. Spesso questo tipo di dimostrazione viene chiamato 'per induzione sulla struttura delle prove'. In pratica si prende un sequente $\Gamma \vdash C$ derivabile in S e si considera la lunghezza della sua derivazione, ovvero l'altezza dell'albero di derivazione.

Base dell'induzione. Dobbiamo mostrare che la proprietà (1) vale per tutti i sequenti che sono derivabili con una derivazione di altezza 0, ovvero una derivazione che usa regole senza premesse. Le regole possibili sono: l'identità e gli assiomi per il \top e \perp . Vediamo in dettaglio.

(i) Se il sequente $\Gamma \vdash C$ è derivato per identità, allora $\Gamma = \Gamma', C$ e la derivazione è:²

$$\Gamma', C \vdash C$$

ora, sempre usando l'identità possiamo derivare anche³

$$\Gamma', A, C \vdash C$$

e concludere, con la regola di scambio, derivando il sequente $\Gamma', C, A \vdash C$ che è proprio il sequente $\Gamma, A \vdash C$ cercato. Per essere espliciti, la derivazione di $\Gamma, A \vdash C$, sapendo che $\Gamma = \Gamma', C$, è:

$$\frac{\frac{\Gamma', A, C \vdash C}{\Gamma', C, A \vdash C} id2}{\Gamma, A \vdash C} sc$$

n.b. Assumendo – come faremo sempre – che i contesti Γ, Δ, \dots rappresentano *sequenze non ordinate*, possiamo direttamente dire che $\Gamma', C, A \vdash C$ si deriva come istanza dell'assioma di identità (*id2*).

(ii) Un sequente $\Gamma \vdash C$ prodotto dall'assioma di \perp è della forma $\Gamma', \perp \vdash C$ e quindi possiamo considerare ancora l'assioma di \perp per concludere $\Gamma', \perp, A \vdash C$.

(iii) Il caso che $\Gamma \vdash C$ sia prodotto dall'assioma di \top è analogo.

²Notate che ho proprio scritto una derivazione di altezza 0 nel sistema S .

³E questa è una nuova derivazione nel sistema S .

Passo induttivo. Consideriamo un naturale n maggiore di 0. Dobbiamo assumere che la proprietà (1) sia verificata per tutti i sequenti che hanno una derivazione di altezza minore o uguale a n e provare che essa vale anche per i sequenti con una derivazione di altezza $n + 1$. Formalmente assumiamo

Ipotesi induttiva: *se il sequente $\Gamma \vdash C$ è derivabile in S con una derivazione lunga al più n , allora anche il sequente $\Gamma, A \vdash C$ è derivabile in S .* (2)

Consideriamo ora un sequente $\Gamma \vdash C$ derivabile in S con una derivazione lunga $n + 1$ e sia Π una sua derivazione lunga $n + 1$. Dobbiamo distinguere vari casi a seconda della regola che è stata applicata per ultima in Π .

(i) Se l'ultima regola che compare in Π è un taglio, allora il sequente è della forma $\Gamma, \Gamma' \vdash C$ e la sua derivazione è

$$\frac{\frac{\Pi'}{\Gamma' \vdash B} \quad \frac{\Pi''}{B, \Gamma'' \vdash C}}{\Gamma', \Gamma'' \vdash C}$$

Ora, le due derivazioni Π' e Π'' hanno altezza minore o uguale a n , quindi possiamo applicare l'ipotesi induttiva (2) su $\Gamma' \vdash B$ e concludiamo che anche $\Gamma', A \vdash B$ è derivabile in S . Per cui

$$\frac{\vdots \quad \frac{\Pi''}{B, \Gamma'' \vdash C}}{\Gamma', \Gamma'', A \vdash C}$$

e concludiamo che anche $\Gamma, A \vdash C$ è derivabile in S .

(ii) Se l'ultima regola che compare in Π è \wedge -rifl. *espl.*, allora il sequente è della forma $\Gamma', B \wedge D \vdash C$ e la sua derivazione è

$$\frac{\frac{\Pi'}{\Gamma', B \vdash C}}{\Gamma', B \wedge D \vdash C}$$

Ora, la derivazione Π' ha altezza minore o uguale a n , quindi possiamo applicare l'ipotesi induttiva (2) su $\Gamma', B \vdash C$ e concludiamo che anche $\Gamma', B, A \vdash C$ è derivabile in S . Per cui

$$\frac{\vdots}{\frac{\Gamma', B, A \vdash C}{\Gamma', B \wedge D, A \vdash C}}$$

e concludiamo che anche $\Gamma, A \vdash C$ è derivabile in S .

(iii) Se l'ultima regola che compare in Π è \wedge -form., allora il sequente è della forma $\Gamma \vdash B \wedge D$ e la sua derivazione è

$$\frac{\frac{\Pi'}{\Gamma \vdash B} \quad \frac{\Pi''}{\Gamma \vdash D}}{\Gamma \vdash B \wedge D}$$

Ora, le due derivazioni Π' e Π'' hanno altezza minore o uguale a n , quindi possiamo applicare l'ipotesi induttiva (2) su $\Gamma \vdash B$ e $\Gamma \vdash D$ per concludere che anche $\Gamma, A \vdash B$ e $\Gamma, A \vdash D$ sono derivabili in S . Per cui

$$\frac{\frac{\vdots}{\Gamma, A \vdash B} \quad \frac{\vdots}{\Gamma, A \vdash D}}{\Gamma, A \vdash B \wedge D}$$

e concludiamo che anche $\Gamma, A \vdash C$ è derivabile in S .

(iv) ... Tutti gli altri casi sono analoghi, ma devono essere verificati *tutti* per poter affermare che la proprietà (1) vale! Vi lascio verificare i casi per: \vee , \rightarrow , \neg . Ricordate di assumere implicitamente la regola di scambio.

Dopo aver verificato tutti gli altri casi, il principio di induzione ci permette di affermare che la proprietà (1) vale per tutti i sequenti derivabili in S .