Calcolo dei Sequenti:
Induzione e Regole di Inferenza

damiano.macedonio@univr.it

17 novembre 2010

1 Principio di induzione

L'insieme $\mathbb{N}$ dei naturali è formato dai numeri $\{0, 1, 2, 3, \ldots\}$. 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: $3 = 0+1+1+1$; $4 = 0+1+1+1+1$; $5 = 0+1+1+1+1+1$; $6 = \ldots$

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'intuizione '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.

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

Dimostrazione. 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 $0+1+2+\ldots+n = n(n+1)/2$ sia vero. Allora $0+1+2+\ldots+n+(n+1) = n(n+1)/2+(n+1)$. 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 2. *Consideriamo un nuovo calcolo dei sequenti* S *costituito dal sistema* LJ *privo delle regole strutturali di indebolimento e contrazione, in cui la regola di identità è esteso con la seguente nuova forma di identità:*

$$\frac{}{\Gamma, A \vdash A}\ \textit{(id2)}$$

Mostrare che

$$\textit{se il sequente } \Gamma \vdash C \textit{ è derivabile in } \mathrm{S}\textit{, allora anche il sequente } \Gamma, A \vdash C \textit{ è derivabile in } \mathrm{S}. \tag{1}$$

Dimostrazione. 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 $\bot$. Vediamo in dettaglio.

(i) Se il sequente $\Gamma \vdash C$ è derivato per identità, allora $\Gamma = \Gamma', C$ e la derivazione è:[1]

$$\frac{}{\Gamma', C \vdash C}\ \textit{(id2)}$$

ora, sempre usando l'identità possiamo derivare anche[2]

$$\frac{}{\Gamma', A, C \vdash C}\ \textit{(id2)}$$

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:

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

n.b. Assumendo – come faremo sempre – che i contesti $\Gamma, \Delta, \ldots$ 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 $\bot$ è della forma $\Gamma', \bot \vdash C$ e quindi possiamo considerare ancora l'assioma di $\bot$ per concludere $\Gamma', \bot, A \vdash C$.

[1] Notate che ho proprio scritto una derivazione di altezza 0 nel sistema S.
[2] E questa è una nuova derivazione nel sistema S.

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

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 cha compare in Π è un taglio, allora il sequente è della forma $\Gamma, \Gamma' \vdash C$ e la sua derivazione è

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

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

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

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

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

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

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

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

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

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

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

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 concluder che anche $\Gamma, A \vdash B$ e $\Gamma, A \vdash D$ sono derivabili in S. Per cui

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

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. E abbiamo concluso l'esercizio. $\square$

Assunzione sulle regole di scambio. Per semplificare le derivazioni, diamo la seguente convenzione.

$\boxed{\textit{D'ora in poi considereremo calcoli di sequenti in cui la regola di scambio è implicita.}}$

In pratica, quando scriviamo $\Gamma \vdash \Delta$ intendiamo che Γ e Δ sono sequenze non ordinate di formule ben formate (anche vuote).

Esercizio 3. *Una derivazione che non contiene alcuna applicazione della regola di taglio si dice* cut-free*. Dimostrare che se il sequente $\Gamma \vdash A \wedge B$ è derivabile in LJ con una derivazione cut-free, allora anche i sequenti $\Gamma \vdash A$ e $\Gamma \vdash B$ sono derivabili in LJ con derivazioni cut-free.*

Dimostrazione. Procediamo per induzione sulla struttura della derivazione cut-free del sequente.

Base dell'induzione. La prova cut-free del sequente $\Gamma \vdash A \wedge B$ è una derivazione di altezza 0. Abbiamo tre casi. Il sequente può essere stato derivato con una istanza della identità o una istanza degli assiomi per $\top$ e $\bot$.

(i) Se il sequente $\Gamma \vdash A \wedge B$ è derivato per identità, allora $\Gamma = A \wedge B$ e la derivazione è:

$$\frac{}{A \wedge B \vdash A \wedge B}\ id$$

Ma allora, possiamo semplicemente costruire queste due *nuove* derivazioni:

$$\frac{\dfrac{}{A \vdash A}\ id}{A \wedge B \vdash A}\ \wedge\text{-}rifl \qquad\qquad \frac{\dfrac{}{B \vdash B}\ id}{A \wedge B \vdash A}\ \wedge\text{-}rifl$$

che derivano $\Gamma \vdash A$ e $\Gamma \vdash B$ senza usare tagli.

(ii) Se il sequente $\Gamma \vdash A \wedge B$ è derivato per $\bot$-*ax*, allora $\Gamma = \Gamma', \bot$ e la derivazione è:

$$\frac{}{\Gamma', \bot \vdash A \wedge B}\ \bot\text{-}ax$$

Ma allora, possiamo semplicemente costruire queste due *nuove* derivazioni:

$$\frac{}{\Gamma', \bot \vdash A}\ \bot\text{-}ax \qquad\qquad \frac{}{\Gamma', \bot \vdash B}\ \bot\text{-}ax$$

che derivano $\Gamma \vdash A$ e $\Gamma \vdash B$ senza usare tagli.

(iii) Il caso di $\top$-*ax* *non* è possibile. Infatti, gli unici sequenti derivati come istanza di $\top$-*ax* sono del tipo $\Sigma \vdash \top$, e il sequente $\Gamma \vdash A \wedge B$ non è tra questi.

Passo induttivo. Consideriamo un naturale n maggiore di 0. Dobbiamo assumere che la proposizione 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

Ip. induttiva: *Se $\Sigma \vdash C \wedge D$ è derivabile in LJ con una derivazione cut-free lunga al più n, allora anche $\Sigma \vdash C$ e $\Sigma \vdash D$ sono derivabili in LJ con derivazioni cut-free.* (3)

Sia ora $\Gamma \vdash A$ derivabile in LJ con una derivazione cut-free Π di altezza $n+1$. Dobbiamo distinguere vari casi a seconda dell'ultima regola applicata nella derivazione Π.

Facciamo intanto due semplici osservazioni:

- L'ultima regola applicata non può essere un taglio (Π è cut-free!).
- L'ultima regola applicata *non* può essere una di queste: $\vee$-*rifl*, $\to$-*form*, $\neg$-*form*. Il motivo è che nella conclusione non comparirebbe una formula come $A \wedge B$ a destra del sequente.

Ora non ci resta che verificare tutti gli altri casi.
(i) Se l'ultima regola cha compare in Π è una istanza di $\wedge$-*form*, allora la derivazione Π è

$$\dfrac{\dfrac{\Pi'}{\Gamma \vdash A} \quad \dfrac{\Pi''}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}$$

con Π' e Π'' cut-free (perché Π lo è). Ma allora possiamo direttamente concludere che $\Gamma \vdash A$ e $\Gamma \vdash B$ possono essere derivati senza usare tagli (Π' è una derivazione cut-free per $\Gamma \vdash A$, Π'' è una derivazione cut-free per $\Gamma \vdash B$).
(ii) Se l'ultima regola cha compare in Π è una istanza di $\rightarrow$ *-rifl*, allora $\Gamma = \Gamma', E \rightarrow F$ e la derivazione Π è

$$\dfrac{\dfrac{\Pi'}{\Gamma' \vdash E} \quad \dfrac{\Pi''}{\Gamma', F \vdash A \wedge B}}{\Gamma', E \rightarrow F \vdash A \wedge B}$$

con Π' e Π'' cut-free e di altezza al più n. In particolare Π'' è una derivazione cut-free per di altezza al più n per $\Gamma', F \vdash A \wedge B$. Posso quindi applicare l'ipotesi induttiva sia su Π' che su Π'' per concludere che esistono due derivazioni Π''_1 e Π''_2 cut-free e tali che

$$\dfrac{\Pi''_1}{\Gamma', F \vdash A} \qquad\qquad \dfrac{\Pi''_2}{\Gamma', F \vdash B}$$

Ma allora posso combinare le derivazioni e ottengo:

$$\dfrac{\dfrac{\Pi'}{\Gamma' \vdash E} \quad \dfrac{\Pi''_1}{\Gamma', F \vdash A}}{\Gamma', E \rightarrow F \vdash A} \qquad\qquad \dfrac{\dfrac{\Pi'}{\Gamma' \vdash E} \quad \dfrac{\Pi''_2}{\Gamma', F \vdash B}}{\Gamma', E \rightarrow F \vdash B}$$

ovvero $\Gamma \vdash A$ e $\Gamma \vdash B$ sono derivabili senza usare tagli, come volevasi.
(iii) Se l'ultima regola cha compare in Π è una istanza di $\vee$-*form*, allora $\Gamma = \Gamma', E \vee F$ e la derivazione Π è

$$\dfrac{\dfrac{\Pi'}{\Gamma', E \vdash A \wedge B} \quad \dfrac{\Pi''}{\Gamma', F \vdash A \wedge B}}{\Gamma', E \vee F \vdash A \wedge B}$$

con Π' e Π'' cut-free e di altezza al più n. Posso quindi applicare l'ipotesi induttiva, ovvero la proprietà (3), per dire che esistono quattro derivazioni Π'_1 e Π'_2, Π''_1 e Π''_2 cut-free e tali che

$$\dfrac{\Pi'_1}{\Gamma', E \vdash A} \qquad \dfrac{\Pi'_2}{\Gamma', E \vdash B} \qquad \dfrac{\Pi''_1}{\Gamma', F \vdash A} \qquad \dfrac{\Pi''_2}{\Gamma', F \vdash B}$$

Posso ancora combinare le derivazioni e ottenere:

$$\dfrac{\dfrac{\Pi'_1}{\Gamma', E \vdash A} \quad \dfrac{\Pi''_1}{\Gamma', F \vdash A}}{\Gamma', E \vee F \vdash A} \qquad\qquad \dfrac{\dfrac{\Pi'_1}{\Gamma', E \vdash B} \quad \dfrac{\Pi''_1}{\Gamma', F \vdash B}}{\Gamma', E \vee F \vdash B}$$

ovvero $\Gamma', E \vee F \vdash A$ e $\Gamma', E \vee F \vdash B$ sono derivabili senza usare tagli, come volevasi.
(iv) ... Vi lascio da verificare i restanti casi: le regole strutturali, $\wedge$-*rifl* e $\neg$-*rifl* (!!attenzione!! in questo ultimo caso non serve utilizzare l'ipotesi induttiva, basta semplicemente "modificare" la prova...)
Dopo aver verificato tutti gli altri casi, il principio di induzione ci permette di affermare che la proposizione vale. $\square$

Esercizio 4 (consigliato). *Sia $\Gamma \vdash \Delta$ un sequente le cui formule sono tutte costruite usando* solo *i connettivi $\vee$ e $\wedge$, partendo da formule atomiche (e non dalle costanti logiche $\bot$ e $\top$)*[3]*. Se tale sequente è derivabile in LJ, allora Γ è non vuoto.*

[3]Per intenderci: le formule in Γ e Δ sono generate dalla seguente produzione: P, Q, R sono formule accettabili; inoltre se A e B sono formule accettabili allora lo sono anche $A \wedge B$ e $A \vee B$