METODI MATEMATICI PER L'INFORMATICA

ANNO ACCADEMICO 2010/2011

1. Calcoli deduttivi formali

Introduciamo una formalizzazione della nozione di dimostrazione. L'interesse di questa formalizzazione non è solo concettuale (formalizziamo l'idea intuitiva di dimostrazione ipotetico-deduttiva) ma anche *algoritmico*.

Per semplificare le induzioni limitiamo il linguaggio ai connettivi $\neg, \rightarrow$. Gli altri connettivi si possono introdurre per definizione (come abbreviazioni). (N.B. Usiamo lo stesso sistema usato nel libro di testo ma diamo una diversa dimostrazione del Teorema di Completezza).

Gli assiomi del Calcolo Proposizionale sono dati dai seguenti schemi (X, Y, Z variano su proposizioni).

Ax 1 $(X \rightarrow (Y \rightarrow X))$
Ax 2 $(X \rightarrow (Y \rightarrow Z) \rightarrow ((X \rightarrow Y) \rightarrow (X \rightarrow Z))$
Ax 3 $(\neg Y \rightarrow \neg X) \rightarrow (X \rightarrow Y)$

Gli assiomi qui sopra sono per la precisione *schemi di assioma*. Ogni formula ottenuta sostituendo X, Y, Z con proposizioni della logica proposizionale è una *istanza* di assioma.

Introduciamo una unica regola di inferenza, che formalmente è una relazione $R(X, Y, Z)$ tra tre proposizioni, dove X, Y sono le premesse e Z la conclusione e si dice che Z *si ottiene* da X, Y applicando la regola R, o che Z *segue* da X, Y per la regola R. La regola che usiamo è il cosidetto Modus Ponens: da X e $(X \rightarrow Y)$ segue Y.

Definizione 1.1 (Deduzione)**.** Una deduzione (o derivazione o prova) è una sequenza finita $F_1, \ldots, F_k$ di proposizioni tale che per ogni $i \in \{1, \ldots, k\}$,

- F_i è una istanza di un assioma, oppure
- F_i si ottiene da due formule precedenti nella sequenza per Modus Ponens, i.e., esistono $m, \ell < k$ tali che F_ℓ è $(F_m \rightarrow F_i)$.

Una formula F è un teorema del calcolo proposizionale se esiste una deduzione la cui ultima formula è F. In tal caso scriviamo $\vdash F$.

Esempio. $\vdash B \rightarrow B$. Cfr. il libro di testo.

Si osserva facilmente che il calcolo appena definito è *corretto* nel senso che ogni teorema è una tautologia.

Proposizione 1.2 (Correttezza)**.** *Se B è un teorema allora B è una tautologia, i.e.*

$$\vdash B \Longrightarrow \models B.$$

Dimostrazione. Ogni istanza di un assioma è una tautologia, e il Modus Ponens conserva la verità: se A è vera e $A \rightarrow B$ è vera, allora B è vera. □

Digressione. L'interesse algoritmico del cacolo deduttivo è il seguente. Gli assiomi che abbiamo introdotto sono stringhe di simboli nel linguaggio formale della logica proposizionale, e sono scelti in modo tale da essere riconoscibili in modo meccanico (algoritmicamente). Inoltre, la regola di deduzione logica che abbiamo introdotto è tale che, date tre proposizioni A, B, C, è possibile riconoscere in modo

Note preparate da Lorenzo Carlucci, carlucci@di.uniroma1.it.

meccanico (algoritmico) se una C è una conseguenza corretta dell'applicazione del Modus Ponens a A e B. In questo modo dal sistema deduttivo è possibile ricavare un algoritmo per *enumerare in modo meccanico tutti e sole le proposizioni che sono dimostrabili nel sistema, i.e., tutti e soli i teoremi.*

Inoltre, per il calcolo proposizionale che abbiamo introdotto vale un teorema di completezza e correttezza analogo a quello visto per i tableau: le proposizioni dimostrabili nel sistema sono tutte e sole le tautologie. Allora abbiamo che

(1) Esiste una algoritmo per enumerare tutti e soli i teoremi, e
(2) I teoremi coincidono con le verità logiche.

Dunque dal calcolo deduttivo formale e dal fatto che valgono i teoremi di Correttezza (sono dimostrabili solo le tautologie) e Compattezza (tutte le tautologie sono dimostrabili), abbiamo che esiste un algoritmo per enumerare tutte e sole le verità logiche.

Per la logica proposizionale le tavole di verità e i tableau semantici sono due metodi meccanici (algoritmici) che già permettono di decidere se una qualunque formula proposizionale è una verità logica o no, quindi l'esistenza di un algoritmo che enumera tutte e sole le verità logiche non ci dice niente di nuovo.

Per l'estensione della logica proposizionale in cui si considerano anche i quantificatori $\forall$ e $\exists$ (detta *logica predicativa*) esiste una nozione rigorosa di verità logica (analoga a quella di tautologia proposizionale) ma *non esiste un metodo algoritmico per decidere se una certa proposizione è una verità logica o no.* Vale però una proprietà più debole: *esiste un algoritmo che enumera tutte e sole le (infinite) proposizioni che sono verità logiche*, e questa proprietà si dimostra defininendo un calcolo deduttivo formale e dimostrando che soddisfa un adeguato teorema di completezza e correttezza.

Possiamo estendere la nozione di deduzione appena definita in modo da formalizzare una dimostrazione condotta in base a un insieme di ipotesi che non sono assiomi della logica. Se $\mathcal{S}$ è un insieme di proposizioni (anche infinito), e F è una formula, diciamo che F è deducibile dalle premesse $\mathcal{S}$ se esiste una sequenza finita di formula $F_1, \ldots, F_k$ tale che per ogni $i \in \{1, \ldots, k\}$,

- F_i è un assioma, oppure
- F_i è in $\mathcal{S}$, oppure
- F_i si ottiene per Modus Ponens da due formule che la precedono nella sequenza.

In tal caso scriviamo $\mathcal{S} \vdash F$. Per semplicità, per un insieme $\mathcal{S}$ e formule $A_1, \ldots, A_n, B$, scriviamo $\mathcal{S}, A_1, \ldots, A_n \vdash B$ invece di usare la notazione più corretta $\mathcal{S} \cup \{A_1, \ldots, A_n\} \vdash B$ e analogamente se $\mathcal{S}_1, \ldots, \mathcal{S}_n$ sono insiemi e B è una formula scriviamo $\mathcal{S}_1, \ldots, \mathcal{S}_n \vdash B$ per $\mathcal{S}_1 \cup \cdots \cup \mathcal{S}_n \vdash B$. Ricordiamo che questo è sempre un asserto esistenziale, che dice: esiste una successione finita di formule con certe proprietà la cui ultima formula è F. La proposizione seguente è una conseguenza immediata delle definizioni.

Proposizione 1.3 (Proprietà fondamentali di $\mathcal{S} \vdash F$)**.**

(1) *Se $\mathcal{S} \vdash F$ e $\mathcal{S} \subseteq \mathcal{S}'$ allora $\mathcal{S}' \vdash F$.*
(2) *$\mathcal{S} \vdash F$ se e solo se esiste un sottinsieme finito $\mathcal{U} \subseteq \mathcal{S}$ tale che $\mathcal{U} \vdash F$.*
(3) *Se $\mathcal{S} \vdash F$ e per ogni $A \in \mathcal{S}$ vale $\mathcal{U} \vdash A$, allora $\mathcal{U} \vdash F$.*

Il Teorema seguente (dovuto a Herbrand, intorno al 1930) semplifica notevolmente manipolazione delle derivazioni. Dice che se da una insieme di premesse $\mathcal{S} \cup \{B\}$ derivo una formula C, allora dalle sole premesse $\mathcal{S}$ derivo la formula $(B \to C)$. Notare che $\mathcal{S}, B \vdash C$ dice che esiste una seguenza finita $C_1, \ldots, C_n$ di formule tale che C_n è C e ogni formula C_i è nella sequenza o perché è un assioma o perché è in $\mathcal{S}$, o perché è B o perché si ottiene per Modus Ponens da formule precedenti. Invece $\mathcal{S} \vdash (B \to C)$ dice che esiste una seguenza finita $D_1, \ldots, D_m$ di formule tale che D_m è $(B \to C)$ e ogni formula D_i è nella sequenza o perché è un assioma o perché è in $\mathcal{S}$, o perché si ottiene per Modus Ponens da formule precedenti. La dimostrazione del Teorema descrive implicitamente un algoritmo per *trasformare* una deduzione $C_1, \ldots, C_n$ in una $D_1, \ldots, D_m$.

Proposizione 1.4 (Teorema di Deduzione)**.** *Se $\mathcal{S}, B \vdash C$ allora $\mathcal{S} \vdash (B \to C)$.*

Dimostrazione. Sia $C_1, \ldots, C_n$ una deduzione di C dall'insieme $\mathcal{S} \cup \{B\}$. Per induzione su $j \in \{1, \ldots, n\}$ mostriamo $\mathcal{S} \vdash (B \to C_j)$.

(Caso $j = 1$) C_1 è un assioma o un elemento di $\mathcal{S} \cup \{B\}$. Sia C_1 è un assioma o un elemento di $\mathcal{S}$. $C_1 \to (B \to C_1)$ è un'istanza dell'Assioma 1. Per Modus Ponens otteniamo $(B \to C_1)$.

Sia C_1 la formula B. Sappiamo già che $(B \to B)$ è un teorema. Dunque a maggior ragione $\mathcal{S} \vdash (B \to B)$.

(Caso $j > 1$) Per ipotesi induttiva per ogni $k < j$, $\mathcal{S} \vdash (B \to C_k)$. Se C_j è un Assioma, un elemento di $\mathcal{S}$ oppure B, si ragiona come prima. Se C_j è ottenuta per Modus Ponens esistono $m, \ell < j$ tali che C_ℓ e C_m tale che C_m è $(C_\ell \to C_j)$. Per ipotesi induttiva sappiamo che $\mathcal{S} \vdash (B \to C_\ell)$ e $\mathcal{S} \vdash (B \to C_m)$. Con due applicazioni di Modus Ponens dalla seguente istanza dell'Assioma 2 otteniamo la conclusione desiderata.

$$(B \to (C_\ell \to C_j)) \to ((B \to C_\ell) \to (B \to C_j)).$$

□

Corollario 1.5.

(1) $B \to C, C \to D \vdash B \to D$
(2) $B \to (C \to D), C \vdash B \to D$

Dimostrazione. Semplice esercizio, applicando il Teorema di Deduzione e usando gli Assiomi. □

Nella dimostrazione del Teorema di Completezza facciamo uso di un piccolo numero di teoremi del Calcolo dei Predicati. I teoremi in questione sono i seguenti e le dimostrazioni le trovate nel libro di testo eccetto l'ultima che è lasciata per esercizio.

Proposizione 1.6.

(1) $\vdash (B \to \neg\neg B)$
(2) $\vdash \neg C \to (C \to D)$
(3) $\vdash C \to (\neg D \to \neg(C \to D))$
(4) $\vdash (B \to C) \to ((\neg B \to C) \to C)$.

Proposizione 1.7. *Sia B una formula e siano $p_1, \dots, p_k$ le variabili proposizionali che compaiono in B. Sia v un assegnamento. Definiamo p_j^v e B^v come segue.*

$$p_j^v = \begin{cases} p_j & \text{se } v(p_j) = 1 \\ \neg p_j & \text{se } v(p_j) = 0. \end{cases} \qquad B^v = \begin{cases} B & \text{se } v(B) = 1 \\ \neg B & \text{se } v(B) = 0. \end{cases}$$

Allora

$$p_1^v, \dots, p_k^v \vdash B^v.$$

Prima di dimostrare la Proposizione precedente vediamo come da essa si ottiene facilmente che ogni tautologia ha una dimostrazione nel calcolo proposizionale.

Corollario 1.8 (Teorema di Completezza)**.** *Se B è una tautologia allora B è un teorema. Ossia*

$$\models B \Longrightarrow \vdash B.$$

Dimostrazione. Sia B una tautologia e siano $p_1, \dots, p_k$ le variabili proposizionali che compaiono in B. Per ogni assegnamento v, $v(B) = 1$. Dalla Proposizione 1.7 abbiamo che $p_1^v, \dots, p_k^v \vdash B$. Siano w, u due assegnamenti tali che

$$w(p_1) = u(p_1), \dots, w(p_{k-1}) = u(p_{k-1}),$$

e

$$w(p_k) = 1; \quad u(p_k) = 0.$$

Allora $p_1^w = p_1^u, \dots, p_{k-1}^w = p_{k-1}^u$ e dalla Proposizione 1.7 applicata a w segue

$$p_1^w, \dots, p_{k-1}^w, p_k \vdash B,$$

mentre dalla Proposizione 1.7 applicata a u segue

$$p_1^w, \dots, p_{k-1}^w, \neg p_k \vdash B.$$

Dal teorema $(B \to C) \to ((\neg B \to C) \to C)$ (Proposizione 1.6, (4)) segue allora

$$p_1^w, \dots, p_{k-1}^w \vdash B.$$

Abbiamo così eliminato p_k dalle premesse. Iterando l'argomento di sopra possiamo analogamente eliminare $p_{k-1}, \dots, p_2, p_1$. Otteniamo allora che $\vdash B$. □

Dimostriamo ora la Proposizione 1.7.

Dimostrazione della Proposizione 1.7. La dimostrazione è per induzione sul numero n dei simboli $\neg$ e $\rightarrow$ in B.

(Caso $n = 0$) Allora B è una variabile proposizionale e l'argomento è banale perché la tesi da dimostrare è che $p_1 \vdash p_1$ e $\neg p_1 \vdash \neg p_1$.

(Caso $n > 0$) Per ipotesi induttiva per ogni $j < n$ vale la tesi. Distinguiamo due casi a seconda della forma di B.

Sia B è di forma $\neg C$. Distinguiamo due casi a seconda del valore che l'assegnamento v assegna a C.

Se $v(C) = 0$, allora $v(B) = 1$, $C^v = \neg C$ e $B^v = B$. Vogliamo allora dimostrare $p_1^v, \ldots, p_k^v \vdash B$. Per ipotesi induttiva su C abbiamo $p_1^v, \ldots, p_k^v \vdash C^v$, ossia $p_1^v, \ldots, p_k^v \vdash \neg C$, e abbiamo concluso perché B è $\neg C$!

Se $v(C) = 1$, allora $v(B) = 0$, $C^v = C$ e $B^v = \neg B$. Vogliamo allora dimostrare $p_1^v, \ldots, p_k^v \vdash \neg B$. Per ipotesi induttiva su C abbiamo $p_1^v, \ldots, p_k^v \vdash C^v$, ossia $p_1^v, \ldots, p_k^v \vdash C$. Usando il fatto che $\vdash (C \rightarrow \neg\neg C)$ (Proposizione 1.6, (1)) e il Modus Ponens otteniamo $p_1^v, \ldots, p_k^v \vdash \neg\neg C$, ossia $p_1^v, \ldots, p_k^v \vdash \neg B$.

Se B è di forma $(C \rightarrow D)$. Per ipotesi induttiva abbiamo $p_1^v, \ldots, p_k^v \vdash C^v$ e $p_1^v, \ldots, p_k^v \vdash D^v$.

Se $v(C) = 0$ allora $v(B) = 1$, $C^v = \neg C$ e $B^v = B$. Voglio dimostrare $p_1^v, \ldots, p_k^v \vdash B$. $p_1^v, \ldots, p_k^v \vdash C^v$ è $p_1^v, \ldots, p_k^v \vdash \neg C$. Usando il teorema $\vdash \neg C \rightarrow (C \rightarrow D)$ (Proposizione 1.6, (2)) otteniamo il risultato desiderato.

Se $v(D) = 1$ allora $v(B) = 1$, $D^v = D$ e $B^v = B$. Voglio dimostrare $p_1^v, \ldots, p_k^v \vdash B$, ossia $p_1^v, \ldots, p_k^v \vdash (C \rightarrow D)$. Per l'ipotesi induttiva su D ho in questo caso che $p_1^v, \ldots, p_k^v \vdash D$. Usando l'ipotesi induttiva $p_1^v, \ldots, p_k^v \vdash D$, l'istanza $D \rightarrow (C \rightarrow D)$ dell'Assioma 1 otteniamo il risultato desiderato.

Se $v(C) = 1$ e $v(D) = 0$ allora $v(B) = 0$, $C^v = C$, $D^v = \neg D$ e $B^v = \neg B$. Voglio dimostrare $p_1^v, \ldots, p_k^v \vdash B$, ossia $p_1^v, \ldots, p_k^v \vdash \neg(C \rightarrow D)$. Usando le ipotesi induttive $p_1^v, \ldots, p_k^v \vdash C$, $p_1^v, \ldots, p_k^v \vdash \neg D$, il teorema $(C \rightarrow (\neg D) \rightarrow (C \rightarrow D))$ (Proposizione 1.6, (3)) otteniamo il risultato desisderato.

□