Logica per la programmazione

Appunti ad uso degli studenti del I anno
Corso di Laurea in Informatica
Università di Pisa
a.a. 2008/09

Autori: R. Barbuti, P. Mancarella, S.Martini
Editore: F.Turini

Indice

1 Introduzione

Questo corso ha lo scopo di insegnare elementi di base di logica e di tecniche di dimostrazione finalizzate alla programmazione. La logica e i calcoli su essa basati, le tecniche di dimostrazione appunto, giocano un ruolo fondamentale, anzi molti ruoli fondamentali nella programmazione. Il primo ruolo è per la formalizzazione dei requisiti. Raramente un programmatore scrive un programma per risolvere un proprio problema. Di solito un programmatore (un team di programmatori) scrive un programma per risolvere un problema posto da altri. La fase di formalizzazione dei requisiti è quella in cui committente e programmatore concordano le caratteristiche attese per il programma da realizzare. è evidente che più precisi sono i requisiti e più certo sarà il risultato, ovvero più facile saraà la vita del programmatore e più sicura l'accettazione da parte del committente. La logica può aiutare molto in questa fase, consentendo di usare un linguaggio non ambiguo e con una semantica (significato) ben preciso. Un secondo uso della logica è poi quello di poter dimostrare proprietà di programmi mediante l'uso di calcoli logici progettati allo scopo (p.e. la logica di Hoare). C'è poi il capitolo importantissimo della logica, o meglio di particolari logiche, usabili direttamente come linguaggi di programmazione, per esempio il linguaggio Prolog.

Queste note sono state ottenute fondendo insieme note scritte negli anni da colleghi del Dipartimento di Informatica:

Paolo Mancarella, Simone Martini: Logica per la Programmazione

Roberto Barbuti, Paolo Mancarella: Cenni di Logica Matematica

Il mio contributo è stato solo di editor, ovvero di fare la fusione delle due dispense scrivendo qualche pezzo di collegamento.

2 Dimostrazioni

Il modo con cui effettueremo i calcoli (le dimostrazioni) in queste note può essere illustrato con un esempio di algebra elementare certamente ben noto al lettore. Lidentità $(a+b)(a-b) = (a2-b2)$ può essere dimostrata mediante una successione di uguaglianze successive, ciascuna di esse giustificata da qualche legge algebrica o da qualche identità già dimostrata. In genere tali giustificazioni sono così ovvie (o almeno dovrebbero esserlo per lo studente di algebra) da non essere menzionate esplicitamente; nel nostro caso, tuttavia, vogliamo annotarle insieme ad ogni passaggio. Un modo per organizzare la dimostrazione è il seguente:

$(a+b)(a-b)$

$=$ { distributività della moltiplicazione rispetto alladdizione, ovvero, in formule, $(y+z)x = yx+zx$ applicata con a al posto di y, b al posto di z e $(a-b)$ al posto di x }

$a(a-b)+b(a-b)$

$=$ { distributività della moltiplicazione rispetto alla sottrazione, due volte, ovvero, in formule, $x(y-z) = xy-xz$ applicata la prima volta con $x=a, y=a, z=b$ e la seconda con $x=b, y=a, z=b$ }

$(aa-ab)+(ba-bb)$

$=$ { $xx = x^2$, e associatività delladdizione }

$a^2-ab+ba-b^2$

$=$ { commutatività della moltiplicazione, e $-x+x=0$ }

a^2+0-b^2

$=$ { $x+0=x$ }

a^2-b^2

La dimostrazione consiste dunque di una catena di uguaglianze, ciascuna corredata da una giustificazione, sotto la forma di una identità algebrica; si noti come in tutte le uguaglianze eccetto la prima si sia implicitamente utilizzato anche il principio di sostituzione, cioè la possibilità di sostituire parti di espressioni con altre espressioni a loro uguali (nellultima uguaglianza, ad esempio, si è sostituita la sottoespressione a^2+0 con a^2). Tutte le dimostrazioni di queste note si conformeranno a questo formato, con la possibilità, come vedremo, di utilizzare simboli diversi da $=$ nella prima colonna. Per quanto riguarda le giustificazioni, si cercherà, soprattutto allinizio, di essere quanto più possibile precisi. A tal fine, assumeremo le proprietà

algebriche degli operatori aritmetici; luguaglianza (=) è riflessiva ($x = x$), simmetrica (se $x = y$ allora $y = x$) e transitiva (se $x = y$ e $y = z$, allora $x = z$). In virtù della transitività di =, un calcolo della forma:

$$\begin{array}{ll} & E_1 \\ = & \quad \{ \text{ giustificazione}_1 \ \} \\ & E_2 \\ = & \quad \{ \text{ giustificazione}_2 \ \} \\ & \cdots \\ = & \quad \{ \text{ giustificazione}_{k-1} \ \} \\ & E_k \end{array}$$

costituisce una dimostrazione che $E_1 = E_k$. Di quando in quando sarà utile impiegare (sia nelle espressioni che come simbolo nella prima colonna delle dimostrazioni) una relazione di ordinamento ($\leq$ o $\geq$); esse sono riflessive, transitive ed antisimmetriche (se $x \leq y$ e $y \geq ? x$ allora $x = y$). Notiamo subito che mentre un calcolo della forma

$$\begin{array}{ll} & E_1 \\ \geq & \quad \{ \text{ giustificazione}_1 \ \} \\ & E_2 \\ = & \quad \{ \text{ giustificazione}_2 \ \} \\ & \cdots \\ \geq & \quad \{ \text{ giustificazione}_{k-1} \ \} \\ & E_k \end{array}$$

(dove in prima colonna compaiono solo uguaglianze e relazioni dordine dello stesso verso) costituisce una dimostrazione che $E_1 \geq E_k$, un calcolo della forma

$$\begin{array}{ll} & E_1 \\ \geq & \quad \{ \text{ giustificazione}_1 \ \} \\ & E_2 \\ = & \quad \{ \text{ giustificazione}_2 \ \} \\ & \cdots \\ \leq & \quad \{ \text{ giustificazione}_{k-1} \ \} \\ & E_k \end{array}$$

dove relazioni dordine distinte sono presenti in prima colonna non costituisce una dimostrazione valida n che $E_1 \leq Ek$, n che $E_1 \geq E_k$. Oltre agli ordinari operatori algebrici (con le loro leggi), utilizzeremo anche altri operatori, che introdurremo di volta in volta. Siccome non vogliamo rifarci allintuizione per la derivazione di identità che li coinvolgono, ciascuno di essi verrà introdotto insieme ad un gruppo di leggi che ne permette la manipolazione simbolica. Come primo esempio, consideriamo gli operatori binari max e min (intuitivamente: $(amaxb)$ è il massimo tra a e b; $(a \ min \ b)$ è il minimo tra a e b). Tali operatori sono governati dalle leggi seguenti (siccome molte di esse si applicano indipendentemente sia a max che a min, scriveremo m in quelle leggi che si applicano ad entrambi):

$a \ m \ b = b \ m \ a$	(Commutatività)
$a \ m \ (b \ m \ c) = (a \ m \ b) \ m \ c$	(Associatività)
$a \ m \ a = a$	(Idempotenza)
$a + (b \ m \ c) = (a + b) \ m \ (a + c)$	(Distributività di + su m)
$a \ max \ b \geq a$	$(max :\geq)$
$a \ min \ b \leq a$	$(\ min \ :\leq)$
$-a \ min \ -b = -(a \ max \ b)$	$(\ min \ : max)$
$-a \ max \ -b = -(a \ min \ b)$	$(max : \ min \ )$

Utilizzando queste leggi, e seguendo il formato appena introdotto, possiamo dimostrare che $amaxb \geq a \; min \; b$ (si noti luso di $\geq$ in prima colonna):

$a \; max \; b$
$\geq$ { Lunica legge che permette di introdurre il simbolo $\geq$ in presenza di max è $max :\geq$. Applichiamola }
a
$\geq$ { Dobbiamo adesso introdurre min. La scelta ovvia è $min :\leq$ }
$a \; min \; b$

Imbarchiamoci adesso in un esempio meno banale, per mostrare come, nonostante l'apparente complessità, una strategia razionale, guidata dalla struttura delle espressioni in gioco, permette di raggiungere l'obiettivo in modo semplice e naturale (per questo scopo, le giustificazioni comprendono qui come nell'esempio precedente anche le motivazioni informali del perch si è scelto una legge piuttosto che un'altra). Vogliamo dimostrare che

$$(*)(a \; max \; b) + (c \; max \; d) = (a + c) \; max \; (a + d) \; max \; (b + c) \; max \; (b + d)$$

Notiamo subito che il membro destro non è ambiguo solo in virtù della legge (Associatività) per max . Come partiamo nella dimostrazione? Siccome cerchiamo di trasformare un membro nell'altro per mezzo di uguaglianze successive, sembra ragionevole partire dal lato più complicato. Dunque:

$(a + c) \; max \; (a + d) \; max \; (b + c) \; max \; (b + d)$
$=$ { Il nostro obiettivo è una formula più corta di quella di partenza; l'unica legge che accorcia le formule in gioco è (Distributività). La applichiamo due volte }
$(a + (c \; max \; d)) \; max \; (b + (c \; max \; d))$
$=$ { Dobbiamo ancora accorciare la formula. Vorremmo applicare (Distributività), ma prima dobbiamo manipolare la formula. Applichiamo allora due volte la commutatività di + }
$((c \; max \; d) + a) \; max \; ((c \; max \; d) + b)$
$=$ { Distributività }
$(c \; max \; d) + (a \; max \; b)$
$=$ { Commutatività di + }
$(a \; max \; b) + (c \; max \; d)$

Concludiamo notando che, in realtà, abbiamo dimostrato anche che

$$(a \; min \; b) + (c \; min \; d) = (a + c) \; min \; (a + d) \; min \; (b + c) \; min \; (b + d)$$

visto che tutte le leggi che abbiamo impiegato nella dimostrazione valgono anche per min.

2.0.1 Esercizi

Gli esercizi seguenti servono a prendere dimestichezza con il formato di dimostrazione appena introdotto e con l'applicazione rigorosa delle leggi.

1. Si dimostri che $(a \; max \; -a) + (b \; max \; -b) \geq (a + b) \; max \; -(a + b)2$.
2. Si dimostri che $((a + c) \; max \; (b + c)) + ((a - c) \; max \; (b - c)) \geq a + b$.
3. Il valore assoluto di un'espressione è definito come $|a| = a \; max \; -a$. Si dimostri che $|a|+|b| \geq |a+b|$.

3 Calcolo proposizionale

Abbiamo manipolato sinora espressioni aritmetiche, il cui valore, in altre parole, è da intendersi nell'insieme dei numeri interi. Per i nostri scopi è importante introdurre subito un'altra classe di espressioni, il

cui valore è un valore di verità (o valore booleano[1]), vero (T) o falso (F). Le proposizioni sono dunque asserzioni a cui sia assegnabile in modo univoco un valore di verità in accordo ad una interpretazione del mondo a cui si riferiscono. Le proposizioni corrispondono in filosofia a quelli che si chiamano enunciati dichiarativi e che già Aristotele definiva: dichiarativi sono non già tutti i discorsi, ma quelli in cui sussiste una enunciazione vera oppure

falsa. Per esempio, assumendo come interpretazione l'attuale geografia politica e l'aritmetica standard, le seguenti frasi sono proposizioni:

1. Roma è la capitale d'Italia
2. La Francia è unostato asiatico
3. 1+1=2
4. 2+2=3

è infatti possibile assegnare in modo univoco il valore T alla prima e alla terza frase e il valore F alle altre due.

Le seguenti frasi non sono invece proposizioni:

1. che ora è?
2. leggete queste note con attenzione
3. x+1=2

Infatti la prima frase non è una asserzione ma una domanda e la seconda non è una asserzione ma un invito (usa l'imperativo enon l'indicativo). Infine la terza non contiene l'informazione completa per decidere se è vera o falsa in quanto non è noto il valore di x. A dire il vero abbiamo già incontrato espressioni di questo tipo: un'espressione della forma $a = b$ (o $a \leq b$) è infatti da interpretarsi come un'asserzione (una proposizione) su uno stato di cose, cui corrisponde il valore vero se e solo se effettivamente in questo stato di cose a è identico a b (o a è minore o uguale di b). Inoltre, come le espressioni aritmetiche possono essere composte mediante opportune operazioni governate da apposite leggi, così è utile introdurre operatori (che diremo connettivi proposizionali, o connettivi, tout court) che permettono di comporre tra loro proposizioni. Ad esempio le due proposizioni elementari

- oggi piove (*)
- oggi fa freddo (**)

possono dare luogo mediante congiunzione (connettivo and) alla proposizione

- oggi piove and oggi fa freddo (***)

Il valore di verità delle proposizioni (*) e (**) è determinato dall'osservazione della realtà (diremo anche: dallo stato di cose corrente), mentre il valore di verità di (***) viene individuato univocamente dal valore di verità delle proposizioni componenti (*) e (**) e dal significato del connettivo *and*. Ad esempio, nel momento in cui scriviamo, (*) ha valore di verità F mentre (**) ha valore di verità T, e ciò è sufficiente per determinare che (***) ha valore di verità F.

Nel seguito faremo uso dei cinque connettivi di base elencati qui di seguito, dove p e q stanno per proposizioni arbitrarie.

[1] in onore del logico e matematico britannico George Boole (1815-1864) che per primo formalizzo il calcolo proposizionale

connettivo	*forma simbolica*	*operazione*
not	$\neg p$	negazione
and	$p \wedge q$	congiunzione
or	$p \vee q$	disgiunzione
se ... allora	$p \Rightarrow q$	implicazione
se e soltanto se	$p \equiv q$	equivalenza
p se q	$p \Leftarrow q$	consequenza

Il valore di verità di formule costruite mediante connettivi è determinato, come detto in precedenza, in funzione del valore di verità delle formule componenti. Tale associazione può essere descritta informalmente mediante frasi del tipo: La congiunzione di due proposizioni è vera se e soltanto se entrambe le proposizioni sono vere o, meglio, mediante le cosiddette tabelle di verità, che esprimono il valore di una proposizione composta, dati i valori di verità delle proposizioni componenti. La tabella di verità dei cinque connettivi è la seguente:

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \equiv q$	$p \Leftarrow q$
T	T	F	T	T	T	T	T
T	F	F	F	T	F	F	T
F	T	T	F	T	T	F	F
F	F	T	F	F	T	T	T

Si noti come nelle tabelle di verità sia necessario prevedere tutte le possibili combinazioni di valori di verità per le proposizioni componenti.

Una formula del calcolo proposizionale è dunque una costruzione ottenuta a partire da proposizioni elementari e dai connettivi visti. Possiamo esprimere questo fatto fornendo una grammatica libera da contesto il cui linguaggio generato è l'insieme di tutte le formule proposizionali costruibili a partire da un insieme prefissato di proposizioni elementari. Assumiamo tra i connettivi logici i seguenti livelli di precedenza:

operatore	livello di precedenza
$\equiv$	0
$\Rightarrow, \Leftarrow$	1
$\wedge, \vee$	2
$\neg$	3

Formule di interesse particolare ai nostri scopi sono le tautologie e le contraddizioni. Una proposizione è una tautologia se e soltanto se il suo valore di verità rimane T indipendentemente dal valore di verità delle sue componenti elementari. In altre parole, il valore di verità di una tautologia rimane T anche se tutte le occorrenze di proposizione elementare che vi compaiono vengono rimpiazzate da una qualunque proposizione. Viceversa, una formula è una contraddizione se e solo se il suo valore di verità rimane F indipendentemente dal valore di verità delle sue componenti. Un esempio di tautologia è la formula $p \vee \neg p$, come appare evidente dalla tabella di verità seguente:

p	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

Un attimo di riflessione è sufficiente per convincersi che, se p è una tautologia, allora $\neg p$ è una contraddizione.

Abbiamo introdotto le tabelle di verità per fornire una giustificazione intuitiva dell'uso dei connettivi e dare così la possibilità di seguire le manipolazioni formali delle formule con ragionamenti basati sull'intuizione. Non dobbiamo tuttavia dimenticare che il nostro scopo è quello di sviluppare un calcolo formale per le formule proposizionali, che consenta di effettuare dimostrazioni di asserti interessanti attraverso una pura manipolazione simbolica delle formule coinvolte. Nel capitolo precedente abbiamo visto come ciò sia possibile nel caso di espressioni algebriche che coinvolgono operatori governati da leggi, le quali consentono la manipolazione simbolica delle espressioni stesse. In quel caso gli asserti interessanti ai nostri scopi erano identità ($E_1 = E_2$) o diseguaglianze ($E_1 \leq E_2$ oppure $E_1 \geq E_2$). Nel caso invece delle formule proposizionali gli asserti per noi interessanti saranno le cosiddette equivalenze ed implicazioni tautologiche, definite come segue: una proposizione p implica tautologicamente una proposizione q se e soltanto se $p \Rightarrow q$ è una tautologia; p è tautologicamente equivalente a q se e soltanto se $p \equiv q$ è una tautologia [2] A questo scopo, tra tutte le tautologie del calcolo proposizionale è conveniente selezionarne alcune, particolarmente importanti, dalle quali le altre si possano ottenere per manipolazione simbolica (allo stesso modo in cui, tra tutte le identità algebriche, alcune ad esempio associatività, commutatività, ecc. sono assunte come leggi dalle quali le altre sono derivate)6. Le prime leggi che introdurremo riguardano $\equiv$:

$p \equiv p$	(Riflessività)
$(p \equiv q) \equiv (q \equiv p)$	(Simmetria)
$((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))$	(Associatività)
$(p \equiv T) \equiv p$	(Unità)
$se (p \equiv q) e (q \equiv r) allora (p \equiv r)$	(Transitività)

Se osserviamo che $\equiv$, come $=$, è riflessivo, simmetrico e transitivo, possiamo capire come sia opportuno assumere questo operatore come il connettivo principale con cui effettuare dimostrazioni di proposizioni (così come $=$ era l'operatore principale per effettuare dimostrazioni di identità algebriche). Come per l'uguaglianza, assumiamo inoltre per $\equiv$ il seguente principio di sostituzione:

Se vale $p \equiv q$, allora sostituendo in una formula r una qualsiasi occorrenza di p con q si ottiene una formula tautologicamente equivalente ad r.

Se, date le formule p, q ed r, conveniamo di indicare con la notazione r^q_p la formula ottenuta da r rimpiazzando la sottoformula p con q (ad esempio, $(s \Rightarrow (p \wedge q)^q_{p \wedge q})$ è la formula $(s \Rightarrow q)$), possiamo scrivere il principio di sostituzione come:

Se abbiamo stabilito che $p \equiv q$, allora vale anche $r \equiv r^q_p$.

In base a tale principio ogni passaggio delle nostre dimostrazioni assumerà la forma

$$\begin{array}{ll} & r \\ \equiv & \quad \{\ p \equiv q\ \} \\ & r^q_p \end{array}$$

dove, almeno per ora, $p \equiv q$ sarà sempre l'istanza di una tautologia. Come primo esempio, possiamo mostrare subito che, in verità, la riflessività di $\equiv$ è conseguenza delle altre leggi:

$$\begin{array}{ll} & p \\ \equiv & \quad \{\ \text{Applicando Simmetria ad Unità si ottiene } p \equiv (p \equiv T)\text{; applicando} \\ & \quad \text{quest'ultima: } \} \\ & p \equiv T \\ \equiv & \quad \{\ \text{Unità } \} \\ & p \end{array}$$

Le prossime leggi che introduciamo riguardano la disgiunzione e la congiunzione:

[2] nel seguito diremo spesso "$p \Rightarrow q$ (risp. $p \equiv q$) vale" intendendo con ciò che $p \Rightarrow q$ (risp. $p \equiv q$) è una implicazione (risp. una equivalenza) tautologica

$$p \vee q \equiv q \vee p \qquad \text{(Commutatività)}$$
$$p \wedge q \equiv q \wedge p$$

$$p \vee (q \vee r) \equiv (p \vee q) \vee r \qquad \text{(Associatività)}$$
$$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$$

$$p \vee p \equiv p \qquad \text{(Idempotenza)}$$
$$p \wedge p \equiv p$$

$$p \wedge T \equiv p \qquad \text{(Unità)}$$
$$p \vee F \equiv p$$

$$p \wedge F \equiv F \qquad \text{(Zero)}$$
$$p \vee T \equiv T$$

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \qquad \text{(Distributività)}$$
$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

Esempio Dimostriamo che $p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$. Siccome si tratta del primo esempio di dimostrazione, saremo un po' pedanti, annotando tutte le leggi che si utilizzano nel corso della dimostrazione. Partiamo dal membro più complesso:

$$\begin{array}{ll} & (p \vee q) \vee (p \vee r) \\ \equiv & \quad \{ \text{ Commutatività } \} \\ & (q \vee p) \vee (p \vee r) \\ \equiv & \quad \{ \text{ Associatività } \} \\ & q \vee (p \vee (p \vee r)) \\ \equiv & \quad \{ \text{ Associatività } \} \\ & q \vee ((p \vee p) \vee r) \\ \equiv & \quad \{ \text{ Idempotenza } \} \\ & q \vee (p \vee r) \\ \equiv & \quad \{ \text{ Associatività } \} \\ & (q \vee p) \vee r \\ \equiv & \quad \{ \text{ Commutavità } \} \\ & (p \vee q) \vee r \\ \equiv & \quad \{ \text{ Associatività } \} \\ & p \vee (q \vee r) \end{array}$$

Osserviamo come si sia dovuto fare spesso ricorso alle leggi di associatività e commutatività, per eseguire manipolazioni intermedie delle formule prima di poter applicare l'idempotenza e poi per ricondurre il risultato nella forma voluta. Come nel caso delle derivazioni algebriche, possiamo semplificare assai formule e dimostrazioni utilizzando implicitamente sia l'associatività (scrivendo ad esempio $p \vee q \vee p \vee r$) che la commutatività. E questo è poprio quello che faremo nel seguito; la dimostrazione precedente assumerà dunque la forma assai più semplice:

$$\begin{array}{ll} & (p \vee q) \vee (p \vee r) \\ \equiv & \quad \{ \text{ Idempotenza } \} \\ & p \vee (q \vee r) \end{array}$$

Questa prima dimostrazione esemplifica proprio l'uso del calcolo logico ovvero l'applicazione per via formale di trasformazioni delle formule per verificare una tautologia. Possiamo anche verificare per via semantica che l'equivalenza dell'esempio sia una tautologia, ovvero qualunque sia l'interpetazione delle proposizioni p, q ed r, costruendo una tabella di verità da cui emerge che il membro sinistro e destro assumono gli stessi valori di verità per ogni combinazione di valori delle proposizioni p, q ed r.

Le prossime due tautologie che dimostreremo, dette leggi di assorbimento, sono molto utili per semplificare determinati calcoli:

$$p \wedge (p \vee q) \equiv p \qquad \text{(Assorbimento)}$$
$$p \vee (p \wedge q) \equiv p$$

Dimostriamo la prima, lasciando l'altra per esercizio:

$$\begin{array}{ll} & p \wedge (p \vee q) \\ \equiv & \quad \{ \text{ Unità } \} \\ & (p \vee F) \wedge (p \wedge q) \\ \equiv & \quad \{ \text{ Distributività } \} \\ & p \vee (F \wedge q) \\ \equiv & \quad \{ \text{ Zero } \} \\ & p \vee F \\ \equiv & \quad \{ \text{ Unità } \} \\ & p \end{array}$$

Passiamo adesso alle leggi che regolano l'unico connettivo unario (cioè ad un solo argomento) del nostro calcolo, la negazione. Come per i connettivi precedenti, avremo bisogno di alcune leggi che ne permettano l'utilizzo da solo, più altre leggi che ne chiariscano l'utilizzo in contesti in cui esso compaia insieme ad altri connettivi.

$$\begin{array}{rr} \neg(\neg p) \equiv p & \text{(Doppia negazione)} \\ p \vee \neg p \equiv T & \text{(Terzo escluso)} \\ p \wedge \neg p \equiv F & \text{(Contraddizione)} \\ \neg p \vee \neg q \equiv \neg(p \wedge q) & \text{(De Morgan)} \\ \neg p \wedge \neg q \equiv \neg(p \vee q) & \\ & \\ \neg T \equiv F & \text{(T:F)} \\ \neg F \equiv T & \end{array}$$

Dimostriamo le leggi di complemento:

$$p \vee (\neg p \wedge q) \equiv p \vee q \qquad \text{(Complemento)}$$
$$p \wedge (\neg p \vee q) \equiv p \wedge q$$

Dimostriamo la prima, lasciando l'altra come esercizio.

$$\begin{array}{ll} & p \vee (\neg p \wedge q) \\ \equiv & \quad \{ \text{ Distributività } \} \\ & (p \vee \neg p) \wedge (p \vee q) \\ \equiv & \quad \{ \text{ Terzo escluso } \} \\ & T \wedge (p \vee q) \\ \equiv & \quad \{ \text{ Unità } \} \\ & (p \vee q) \end{array}$$

Il lettore attento avrà notato come manchi sinora una qualsiasi legge che colleghi efficacemente $\wedge, \vee$ o $\neg$ con l'equivalenza $\equiv$. Per ovviare a questa deficienza, è conveniente introdurre prima la legge che governa l'implicazione e dare poi le relazioni di quest'ultima con l'equivalenza. L'implicazione può essere definita a partire dalla negazione e dalla disgiunzione[3]; l'unica regola per questo connettivo è dunque la sua definizione in termini degli altri connettivi:

[3] ancora una volta non è questo il luogo per discutere della interdefinibilità dei connettivi. Basterà dire che esistono molti insiemi di connettivi *funzionalmente completi*, cioè dai quali si posaano definire tutti glia altri. L'insieme $\{\vee, \neg\}$ è uno di questi, così come $\{\wedge, \neg\}$ e $\{\Rightarrow, \neg\}$.

$$(p \Rightarrow q) \equiv (\neg p \vee q) \qquad \text{(Elim-}\Rightarrow\text{)}$$

Le relazioni con l'equivalenza sono ora date dalla legge:

$$(p \equiv q) \equiv (p \Rightarrow q) \wedge (q \Rightarrow p) \qquad \text{(Elim-}\equiv\text{)}$$

Introduciamo, infine, un nuovo connettivo ausiliario, la conseguenza, con la tautologia

$$(p \Leftarrow q) \equiv (q \Rightarrow p) \qquad \text{(Elim-}\Leftarrow\text{)}$$

Utilizzando le leggi introdotte e le tautologie dimostrate sinora, è possibile dimostrare molte altre leggi (anzi: tutte le tautologie del calcolo proposizionale sono derivabili da questo insieme). Noi ci accontenteremo di vedere qualche altro esempio, lasciando molte leggi quali esercizio per lo studente. Vediamo, a titolo d'esempio, la derivazione del cosiddetto modus ponens:

$$(p \wedge (p \Rightarrow q)) \Rightarrow q \qquad \text{(Modus ponens)}$$

Si noti che le leggi introdotte sin qui riguardano solo equivalenze tautologiche, ovvero asserti in cui il connettivo principale è $\equiv$: finché non avremo a disposizione un bagaglio di leggi che ci permettano di manipolare direttamente formule in cui compaia l'implicazione come connettivo principale, non possiamo far altro che dimostrare il modus ponens (una implicazione tautologica) riducendo l'intera formula a T [4], ovvero mostrando direttamente che è una tautologia. Il primo passo della dimostrazione appare dunque obbligato, non potendo che appellarsi alla definizione dell'implicazione data dalla legge Elim-$\Rightarrow$.

$$\begin{array}{ll} & (p \wedge (p \Rightarrow q)) \Rightarrow q \\ \equiv & \quad \{ \text{ Elim-}\Rightarrow \} \\ & \neg(p \wedge (p \Rightarrow q)) \vee q \\ \equiv & \quad \{ \text{ Elim-}\Rightarrow \} \\ & \neg(p \wedge (\neg p \vee q)) \vee q \\ \equiv & \quad \{ \text{ DeMorgan } \} \\ & \neg p \vee \neg(\neg p \vee q) \vee q \\ \equiv & \quad \{ \text{ DeMorgan } \} \\ & \neg p \vee (\neg\neg p \wedge \neg q) \vee q \\ \equiv & \quad \{ \text{ Complemento } \} \\ & \neg p \vee \neg q \vee q \\ \equiv & \quad \{ \text{ TerzoEscluso } \} \\ & \neg p \vee T \\ \equiv & \quad \{ \text{ Zero } \} \\ & T \end{array}$$

Un'altra importante legge, la cui dimostrazione, lasciata per esercizio, procede su una linea analoga a quella del modus ponens, è:

$$p \wedge q \Rightarrow p \qquad \text{(Sempl.-}\wedge\text{)}$$

Il modus ponens e le leggi che hanno come connettivo principale un'implicazione (come Sempl.-$\wedge$) possono essere fruttuosamente utilizzate per dimostrare tautologie riguardanti una o più implicazioni. La cosa, tuttavia, va affrontata con qualche cautela, il che ci consiglia di dedicare a questo argomento tutto il prossimo paragrafo. Concludiamo con alcune importanti tautologie utili nel calcolo; la loro dimostrazione a partire dalle altre viste sin qui è lasciata per esercizio.

[4] si ricordi che una "legge" non è altro che una tautologia, e dunque deve essere equivalente a T

$(p \Rightarrow \neg p) \equiv \neg p$	(Riduzione ad assurdo)
$(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$	(Controposizione)
$p \wedge q \Rightarrow r \equiv p\ wedge \neg r \Rightarrow \neg q$	(Scambio)
$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$	(Transitività-$\Rightarrow$)
$(p \equiv q) \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$	(Elim-$\equiv$-bis)
$p \Rightarrow p \vee q$	(Intro-$\vee$)

4 Del formato delle dimostrazioni

Le dimostrazioni viste sin qui si basano sul principio di sostituzione, ovvero sostituendo una (sotto-)formula p di una formula r con una (sotto-)formula q equivalente a p, non si cambia il valore di verità di r (ovvero si ottiene una formula tautologicamente equivalente ad r). Con la stessa libertà con la quale avevamo permesso a $\leq$ di comparire nella prima colonna di dimostrazioni riguardanti espressioni algebriche, tuttavia, vorremmo poter utilizzare in prima colonna anche il connettivo $\Rightarrow$. è il modus ponens a permetterlo: se, infatti, abbiamo derivato p, e sappiamo che $p \Rightarrow q$, è appunto questa legge a permetterci di concludere q. Ne consegue che una dimostrazione della forma

r_1
$\equiv$ { giustificazione$_1$ }
...
$\equiv$ { giustificazione$_h$ }
p
$\Rightarrow$ { modus ponens, $p \Rightarrow q$) (* }
q
$\equiv$ { giustificazione$_{h+1}$ }
...
$\equiv$ { giustificazione$_{k-1}$ }
r_k

è una dimostrazione legale di $r_1 \Rightarrow r_k$. Infatti i primi h passi di dimostrazione ci consentono di concludere che $r_1 \equiv p$ e ciò, insieme con il fatto che $p \Rightarrow q$, garantisce che $r_1 \Rightarrow q$; i rimanenti passi infine consentono di dimostrare $q \equiv r_k$ e ciò, insieme con quanto appena dimostrato, ci permette di concludere $r_1 \Rightarrow r_k$. Per l'importanza e l'ubiquità di dimostrazioni di questo genere, ometteremo nel seguito di annotare esplicitamente il modus ponens tra le giustificazioni di un passaggio come (*).

Esempio:

$(p \vee q) \wedge \neg p \Rightarrow q$	(Tollendo Ponens)

Come preannunciato, invece di cercare di ridurre tutta la formula a T, lavoreremo su una delle sue due parti, l'antecedente, mostrando che davvero implica il conseguente (in $p \Rightarrow q$, p è detto l'*antecedente*, mentre q è il *conseguente*).

$(p \vee q) \wedge \neg p$
$\equiv$ { doppia negazione e complemento }
$(q \wedge \neg p)$
$\Rightarrow$ { Sempl.-$\wedge$ }
q

(**Esercizio**: si dimostri la legge del tollendo ponens riducendola a T.) Osserviamo, ora, che nella dimostrazione precedente si è applicata una legge dell'implicazione (Sempl.-$\wedge$: $p \wedge q \Rightarrow p$) ad un'intera formula della dimostrazione (nel caso in esame proprio $q \wedge \neg p$). Una domanda immediata è se, come nel caso dell'equivalenza, si possano applicare leggi riguardanti l'implicazione a sottoformule di una data espressione, ovvero si possa disporre di una sorta di principio di sostituzione anche per l'implicazione, che consenta di introdurre tale connettivo nella prima colonna delle dimostrazioni. Ci si chiede, ad esempio, se sia lecita una derivazione del tipo:

$$
\begin{array}{ll}
 & (p \wedge q) \vee r \\
\Rightarrow & \quad \{ \text{ Sempl.-}\wedge \ \} \\
 & p \vee r
\end{array}
$$

dove, appunto, Sempl.-$\wedge$ è stata applicata alla sottoformula $(p \wedge q)$ della formula in considerazione $(p \wedge q) \vee r$. Per rispondere a questa domanda nel caso in questione, notiamo innanzitutto che la formula, che indicheremo con (**)

$$((p \vee r) \wedge (p \Rightarrow q)) \Rightarrow (q \vee r)$$

è una tautologia (**Esercizio**: lo si dimostri). Inoltre, siccome anche Sempl.-$\wedge$ è una tautologia (ovvero $(p \wedge q \Rightarrow p) \equiv T$), possiamo riscrivere la dimostrazione precedente come

$$
\begin{array}{ll}
 & (p \wedge q) \vee r \\
\equiv & \quad \{ \text{ Unità } \} \\
 & ((p \wedge q) \vee r) \wedge (p \wedge q \Rightarrow p) \\
\Rightarrow & \quad \{ \text{ (**), applicata con } (p \wedge q) \text{ al posto di } p, \text{ e } p \text{ al posto di } q \ \} \\
 & p \vee r
\end{array}
$$

il che ne dimostra la correttezza. L'esempio riuscito, tuttavia, non deve far pensare che il caso generale sia risolto. Mentre, infatti, la dimostrazione

$$
\begin{array}{ll}
 & r \Rightarrow (p \wedge q) \\
\Rightarrow & \quad \{ \text{ Sempl.-}\wedge \ \} \\
 & r \Rightarrow p
\end{array}
$$

è corretta (**Esercizio**: si dimostri la correttezza della deduzione, secondo la linea dell'esempio precedente), la seguente non lo è:

$$
\begin{array}{ll}
 & (p \wedge q) \Rightarrow r \\
\Rightarrow & \quad \{ \text{ Sempl.-}\wedge \ldots \textbf{NO!} \ \} \\
 & p \Rightarrow r
\end{array}
$$

Per vederlo, mostriamo che l'intera formula non è una tautologia, ovvero non è riducibile a T.

$$
\begin{array}{ll}
 & ((p \wedge q) \Rightarrow r) \Rightarrow (p \Rightarrow r) \\
\equiv & \quad \{ \text{ Elim.-}\Rightarrow, \text{ 2 volte } \} \\
 & \neg(p \wedge q \Rightarrow r) \vee \neg p \vee r \\
\equiv & \quad \{ \text{ Elim.-}\Rightarrow, \text{ De Morgan } \} \\
 & \neg(\neg p \vee \neg q \vee r) \vee \neg p \vee r \\
\equiv & \quad \{ \text{ De Morgan } \} \\
 & (p \wedge q \wedge \neg r) \vee \neg p \vee r \\
\equiv & \quad \{ \text{ De Morgan } \} \\
 & (q \wedge \neg(\neg p \vee r)) \vee \neg p \vee r \\
\equiv & \quad \{ \text{ Complemento } \} \\
 & q \vee \neg p \vee r
\end{array}
$$

è facile osservare a questo punto che la formula ottenuta non è una tautologia, rimpiazzando ad esempio q ed r con F e p con T.

Esercizio: Si dimostri che, in realtà, vale l'implicazione inversa:

$$((p \wedge q) \Rightarrow r) \Leftarrow (p \Rightarrow r).$$

Nella ricerca di una tecnica generale per affrontare questo tipo di dimostrazioni, torniamo per un momento alle derivazioni algebriche, e chiediamoci se, anche in quel caso, si possa liberamente agire su sottoespressioni. Un attimo di riflessione mostra subito che, sebbene il calcolo

$$
\begin{array}{ll}
 & a+b-c \\
\leq & \quad \{\ \mathrm{a} \leq \mathrm{d}\ \} \\
 & d+b-c
\end{array}
$$

sia perfettamente legittimo, il calcolo

$$
\begin{array}{ll}
 & a+b-c \\
\leq & \quad \{\ \mathrm{c} \leq \mathrm{d}\ \} \\
 & a+b-d
\end{array}
$$

risulta banalmente scorretto. Il punto cruciale è che, mentre nel primo esempio la maggiorazione avviene in un contesto positivo, nel secondo essa avviene in un contesto negativo (più correttamente: la variabile c occorre in posizione negativa in $a+b-c$) e, quando questo accade, la maggiorazione non è più lecita, a meno di non invertire il verso dell'operatore di relazione utilizzato, ottenendo la dimostrazione, questa volta corretta

$$
\begin{array}{ll}
 & a+b-c \\
\geq & \quad \{\ \mathrm{c} \leq \mathrm{d}\ \} \\
 & a+b-d
\end{array}
$$

La stessa situazione si verifica nel caso proposizionale, dove l'operatore di negazione ($\neg$) introduce contesti negativi. In modo informale, diremo dunque che p occorre positivamente in $p, p \wedge q, p \vee q$ e $q \Rightarrow p$, mentre occorre negativamente in $\neg p$ e $p \Rightarrow q$ (si ricordi, infatti, che $p \Rightarrow q \equiv \neg p \vee q$). Possiamo allora enunciare in modo generale il principio di sostituzione per $\Rightarrow$:

Se abbiamo stabilito $p \Rightarrow q$, e p occorre positivamente in r, allora vale $r \Rightarrow r^q_p$

Si ricordi che r^q_p denota il risultato della sostituzione di q al posto di p in r.

Come nel caso delle espressioni algebriche, l'applicazione di una implicazione tautologica in contesti negativi richiede di invertire il senso dell'implicazione. In altre parole vale il seguente principio di sostituzione per $\Leftarrow$:

Se abbiamo stabilito $p \Rightarrow q$, e p occorre negativamente in r, allora vale $r \Leftarrow r^q_p$

Riassumendo, i passi elementari delle nostre dimostrazioni visti fin qui sono tutte istanze dei seguenti schemi di dimostrazione, che riflettono i tre principi di sostituzione per $\equiv, \Rightarrow$ e $\Leftarrow$:

$$
\begin{array}{ll}
 & r \\
\equiv & \quad \{\ \mathrm{p} \equiv \mathrm{q}\ \} \\
 & r^q_p
\end{array}
$$

$$
\begin{array}{ll}
 & r \\
\Rightarrow & \quad \{\ p \text{ occorre positivamente in } r,\ p \Rightarrow q\ \} \\
 & r^q_p
\end{array}
$$

$$
\begin{array}{ll}
\Leftarrow & \quad \{\ p \text{ occorre negativamente in } r,\ p \Rightarrow q\ \} \\
 & r^q_p
\end{array}
$$

Per economia di notazione, trascureremo nel seguito di menzionare le giustificazioni p occorre positivamente in r o p occorre negativamente in r, assumendole implicitamente ogni volta che applicheremo un passo di dimostrazione come i precedenti.

5 Complementi di calcolo proposizionale

Concludiamo la trattazione del calcolo proposizionale con ulteriori esempi e con la trattazione delle forme normali, un concetto spesso utile per la manipolazione di formule ribelli ad altri trattamenti.

$$((p \Rightarrow q) \wedge \neg q) \Rightarrow \neg p \qquad \text{(Tollendo Tollens)}$$

$$\begin{array}{ll} & (p \Rightarrow q) \wedge \neg q \\ \equiv & \quad \{ \text{ Elim-}\Rightarrow \} \\ & (\neg p \vee q) \wedge \neg q \\ \equiv & \quad \{ \text{ Complemento } \} \\ & \neg q \wedge \neg p \\ \Rightarrow & \quad \{ \text{ Sempl.-}\wedge \} \\ & \neg p \end{array}$$

$$\begin{array}{ll} (p \Rightarrow q) \wedge (p \Rightarrow r) \equiv (p \Rightarrow q \wedge r) & \text{(Sempl.Destra-}\Rightarrow\text{)} \\ (p \Rightarrow q) \vee (p \Rightarrow r) \equiv (p \Rightarrow q \vee r) & \end{array}$$

Dimostriamo la prima, lasciando la seconda per esercizio.

$$\begin{array}{ll} & (p \Rightarrow q) \wedge (p \Rightarrow r) \\ \equiv & \quad \{ \text{ Elim.-}\Rightarrow, \text{ 2 volte } \} \\ & (\neg p \vee q) \wedge (\neg p \vee r) \\ \equiv & \quad \{ \text{ Distributività } \} \\ & \neg p \vee (q \wedge r) \\ \equiv & \quad \{ \text{ Elim.-}\Rightarrow \} \\ & p \Rightarrow q \wedge r \end{array}$$

Si noti l'uso della legge distributiva per raccogliere $\neg p$, nonchè l'uso della legge di eliminazione del $\Rightarrow$ per introdurre l'implicazione.

$$\begin{array}{ll} (p \Rightarrow r) \vee (q \Rightarrow r) \equiv (p \wedge q \Rightarrow r) & \text{(Sempl.Sinistra-}\Rightarrow\text{)} \\ (p \Rightarrow r) \wedge (q \Rightarrow r) \equiv (p \vee q \Rightarrow r) & \end{array}$$

Dimostriamo la seconda, lasciando la prima per esercizio.

$$\begin{array}{ll} & (p \Rightarrow r) \wedge (q \Rightarrow r) \\ \equiv & \quad \{ \text{ Elim.-}\Rightarrow, \text{ 2 volte } \} \\ & (\neg p \vee r) \wedge (\neg q \vee r) \\ \equiv & \quad \{ \text{ Distributività } \} \\ & (\neg p \wedge \neg q) \vee r \\ \equiv & \quad \{ \text{ De Morgan } \} \\ & \neg(p \vee q) \vee r \\ \equiv & \quad \{ \text{ Elim.-}\Rightarrow \} \\ & p \vee q \Rightarrow r \end{array}$$

Una variante della prima legge Sempl.Sinistra-$\Rightarrow$ è la seguente:

$$p \Rightarrow (q \Rightarrow r) \equiv (p \wedge q \Rightarrow r) \qquad \text{(Sempl.Sinistra-}\Rightarrow\text{)}$$

anche la sua sua dimostrazione è lasciata per esercizio.

$$(p \Rightarrow q) \wedge (r \Rightarrow s) \Rightarrow (p \wedge r \Rightarrow q \wedge s) \qquad \text{(Sempl.-}\Rightarrow\text{)}$$

Per dimostrare questa legge, utilizziamo una nuova tecnica di prova suggerita dalla legge di controposizione. Osserviamo infatti che

$$
\begin{array}{ll}
 & (p \Rightarrow q) \wedge (r \Rightarrow s) \Rightarrow (p \wedge r \Rightarrow q \wedge s) \\
\equiv & \quad \{ \text{ Controposizione } \} \\
 & \neg(p \wedge r \Rightarrow q \wedge s) \Rightarrow \neg((p \Rightarrow q) \wedge (r \Rightarrow s))
\end{array}
$$

Una dimostrazione di quest'ultima implicazione è dunque anche una prova di Sempl.-$\Rightarrow$.

$$
\begin{array}{ll}
 & \neg(p \wedge r \Rightarrow q \wedge s) \\
\equiv & \quad \{ \text{ Elim.-}\Rightarrow \} \\
 & \neg(\neg(p \wedge r) \vee (q \wedge s)) \\
\equiv & \quad \{ \text{ De Morgan, Doppia Negazione } \} \\
 & (p \wedge r) \wedge \neg(q \wedge s) \\
\equiv & \quad \{ \text{ De Morgan } \} \\
 & (p \wedge r) \wedge (\neg q \vee \neg s) \\
\equiv & \quad \{ \text{ Distributività } \} \\
 & (p \wedge r \wedge \neg q) \vee (p \wedge r \wedge \neg s) \\
\Rightarrow & \quad \{ \text{ Sempl-}\wedge, \text{ 2 volte } \} \\
 & (p \wedge \neg q) \vee (r \wedge \neg s) \\
\equiv & \quad \{ \text{ De Morgan } \} \\
 & \neg(\neg p \vee q) \vee \neg(\neg r \vee s) \\
\equiv & \quad \{ \text{ Elim.}\Rightarrow, \text{ 2 volte } \} \\
 & \neg(p \Rightarrow q) \vee \neg(r \Rightarrow s) \\
\equiv & \quad \{ \text{ De Morgan } \} \\
 & \neg((p \Rightarrow q) \wedge (r \Rightarrow s))
\end{array}
$$

L'ultima legge che abbiamo visto è particolarmente utile in quanto giustifica la seguente tecnica di prova:

Per dimostrare che $p \wedge r \Rightarrow q \wedge s$ è sufficiente fornire due prove separate per $p \Rightarrow q$ e per $r \Rightarrow s$.

5.1 Forme Normali

Spesso è desiderabile semplificare, mediante l'uso di tautologie, formule complicate fino a portarle in una forma più semplice, in cui compaiono solo alcuni dei connettivi visti. Tali forme sono dette forme normali e le più comuni tra di esse sono la forma normale congiuntiva e la forma normale disgiuntiva. Una formula è in forma normale congiuntiva se è del tipo

$$(p_1 \vee p_2 \vee \ldots) \wedge (q_1 \vee q_2 \vee \ldots) \wedge \ldots$$

dove $p_1, p_2, \ldots, q_1, q_2, \ldots$ sono lettere proposizionali (cioè identificatori) o la negazione di lettere proposizionali. Analogamente una formula è in forma normale disgiuntiva se è del tipo

$$(p_1 \wedge p_2 \wedge \ldots) \vee (q_1 \wedge q_2 \wedge \ldots) \vee \ldots$$

Le forme normali forniscono un meccanismo per verificare, tra l'altro, se una data formula è o meno una tautologia. Ad esempio la seguente formula in forma normale disgiuntiva è una tautologia in quanto contiene due elementi della disgiunzione che sono l'uno il negato dell'altro (terzo escluso):

$$p \vee (q \wedge r \wedge p) \vee \neg p \vee (\neg r \wedge q \wedge t)$$

. Le forme normali possono essere utilizzate anche per verificare se due formule sono equivalenti. Si considerino ad esempio le due formule

$$\neg((p \Rightarrow q) \wedge (r \Rightarrow p))$$

$$\neg(\neg q \Rightarrow \neg p) \vee \neg(r \Rightarrow p)$$

La prima può essere portata in forma normale disgiuntiva come segue:

$\neg((p \Rightarrow q) \wedge (r \Rightarrow p))$
$\equiv$ { De Morgan }
$\neg(p \Rightarrow q) \vee \neg(r \Rightarrow p)$
$\equiv$ { Elim.-$\Rightarrow$, 2 volte }
$\neg(\neg p \vee q) \vee \neg(\neg r \vee p)$
$\equiv$ { De Morgan, 2 volte, e doppia negazione }
$(p \wedge \neg q) \vee (r \wedge \neg p)$

Analogamente, la seconda può essere portata in forma normale disgiuntiva:

$\neg(\neg q \Rightarrow \neg p) \vee \neg(r \Rightarrow p)$
$\equiv$ { Elim.-$\Rightarrow$, 2 volte, e doppia negazione }
$\neg(q \vee \neg p) \vee \neg(\neg r \vee p)$
$\equiv$ { De Morgan, e doppia negazione }
$(\neg q \wedge p) \vee (r \wedge \neg p)$

Le due forme normali (a meno di commutatività) sono uguali e ciò ci autorizza, per transitività, a dire che le due formule di partenza sono equivalenti.

5.2 Altri esempi

$(p \vee q) \wedge (\neg p \vee r) \Rightarrow (q \vee r)$ (Risoluzione)

$(p \vee q) \wedge (\neg p \vee r)$
$\equiv$ { Elim-$\Rightarrow$, 2 volte }
$(\neg q \Rightarrow p) \wedge (p \Rightarrow r)$
$\Rightarrow$ { Transitività-$\Rightarrow$ }
$\neg q \Rightarrow r$
$\equiv$ { Elim-$\Rightarrow$ }
$q \vee r$

La legge di risoluzione consente di semplificare forme normali congiuntive: se infatti una forma normale congiuntiva è del tipo

$$\ldots \wedge (p \vee q_1 \vee \ldots \vee q_n) \wedge (\neg p \vee r_1 \vee \ldots \vee r_m) \wedge \ldots$$

si può ottenere mediante risoluzione la formula seguente che è implicata dalla precedente:

$$\ldots \wedge (q_1 \vee \ldots \vee q_n \vee r_1 \vee \ldots \vee r_m) \wedge \ldots$$

Come si può notare la seconda forma normale congiuntiva contiene un fattore in meno della precedente.

Esempio: Dimostrare che $((r \Rightarrow p) \wedge (q \Rightarrow r) \wedge r \wedge q \wedge \neg p) \Rightarrow F$ è una tautologia.

$(r \Rightarrow p) \wedge (q \Rightarrow r) \wedge r \wedge q \wedge \neg p$
$\equiv$ { Elim.-$\Rightarrow$, 2 volte }
$(\neg r \vee p) \wedge (\neg q \vee r) \wedge r \wedge q \wedge \neg p$
$\Rightarrow$ { Risoluzione applicata a $(\neg r \vee p)$ e r (si noti che entrambi occorrono positivamente) }
$p \wedge (\neg q \vee r) \wedge q \wedge \neg p$
$\equiv$ { Contraddizione }
$F \wedge (\neg q \vee r) \vee q$
$\equiv$ { zero }
F

5.2.1 Esercizi

Dimostrare le seguenti tautologie:

1. $p \Rightarrow T \equiv T$
2. $(p \Rightarrow (q \wedge \neg q)) \equiv \neg p$
3. $(\neg p \Rightarrow (p \wedge q)) \equiv p$
4. $(\neg p \wedge (p \vee q)) \Rightarrow q$
5. $(\neg q \wedge (p \Rightarrow q)) \Rightarrow \neg p$
6. $p \Rightarrow (q \Rightarrow (p \wedge q))$
7. $(p \vee q) \wedge (p \vee \neg q) \equiv p$
8. $((p \vee q) \Rightarrow r) \Rightarrow (p \Rightarrow r)$
9. $((p \vee q) \wedge (p \Rightarrow r) \wedge (q \Rightarrow s)) \Rightarrow (r \vee s)$
10. $((p \equiv q) \vee r) \equiv (p \vee r \equiv q \vee r)$
11. $((p \equiv q) \vee \neg r) \equiv (p \wedge r \equiv q \wedge r)$
12. $((p \Rightarrow q) \vee r) \equiv (p \vee rq \vee r)$
13. $(p \Rightarrow q) \vee \neg r) \equiv (p \wedge r \Rightarrow q \wedge r)$
14. $((p \wedge q) \vee (q \wedge r) \vee (r \wedge p)) \equiv ((p \vee q) \wedge (q \vee r) \wedge (r \vee p))$
15. $(p \equiv q) \equiv ((\neg p \vee q) \wedge (\neg q \vee p))$, senza introdurre $\Rightarrow$

Dire quali delle seguenti formule sono tautologie, quali contraddizioni e quali né le une né le altre (senza usare tabelle di verità):

1. $(q \wedge p) \vee (q \wedge \neg p) \wedge (q \Rightarrow r)$
2. $p \Rightarrow (p \wedge q)$
3. $(p \Rightarrow q) \vee (q \Rightarrow (p \wedge r))$
4. $((\neg q \Rightarrow p) \vee (q \Rightarrow (\neg p \wedge \neg r))) \Rightarrow r$
5. $p \wedge (p \Rightarrow r) \wedge (r \Rightarrow \neg p)$
6. $\neg p \vee q \vee ((p \vee q) \wedge (\neg p \vee \neg q))$

6 Del formato delle dimostrazioni (II)

è giunto ormai il momento di trattare in piena generalità il modo di scrivere le dimostrazioni che abbiamo adottato. Dato un connettivo *conn* (finora abbiamo utilizzato $\Rightarrow, \equiv$ e $\Leftarrow$) l'interpretazione intuitiva di un singolo passo di dimostrazione come

$$\begin{array}{ll} & P \\ conn & \{\ \mathrm{G}\ \} \\ & Q \end{array}$$

è che, nell'ipotesi G, vale P *conn* Q. Più precisamente, allora, un passo di dimostrazione non è che un modo conveniente di stabilire che l'implicazione

$$G \Rightarrow (P\ conn\ Q)$$

è una tautologia. Analogamente, una sequenza di passi della forma

$$
\begin{array}{ll}
& P \\
conn_1 & \{\ \mathrm{G}_1\ \} \\
& Q \\
conn_2 & \{\ \mathrm{G}_2\ \} \\
& R
\end{array}
$$

è un modo alternativo di esprimere il fatto che

$$(G_1 \Rightarrow (P\ conn_1 Q)) \wedge (G_2 \Rightarrow (Q\ conn_2 R))(*)$$

è una tautologia. Osserviamo, adesso, che finora abbiamo sempre utilizzato tautologie come giustificazioni (cioè, lo ricordiamo, $G \equiv G1 \equiv G2 \equiv T$). Utilizzando questo fatto, una tautologia come la (*) stabilisce che

$$(T \Rightarrow (P\ conn_1 Q)) \wedge (T \Rightarrow (Q\ conn_2 R))$$

o, equivalentemente, visto che $(T \Rightarrow P) \equiv P$,

$$(P\ conn_1 Q) \wedge (Q\ conn_2 R)$$

Se, infine, $conn_1$ e $conn_2$ sono lo stesso connettivo $conn$ e tale connettivo è transitivo, cosa che è sempre stata negli esempi da noi fatti, da ciò segue

$$P\ conn\ R$$

cioè la conclusione che intuitivamente abbiamo sempre avuto in mente.

Ora che la struttura ed il significato delle dimostrazioni sono chiari, tuttavia, niente toglie di fornire, come giustificazione, una formula che non è una tautologia. Se, infatti, vogliamo dimostrare una certa proprietà, diciamo Q, nell'ipotesi che valga un'altra proprietà P, abbiamo a disposizione due strade. La prima, più ovvia, è quella di mostrare direttamente che $P \Rightarrow Q$ è una tautologia o (equivalentemente, grazie alla legge di Controposizione) che $\neg Q \Rightarrow \neg P$ è una tautologia; la seconda, spesso più conveniente soprattutto se Q è una formula complessa è quella di lavorare su Q ed usare P come giustificazione di qualche passaggio. Ciò è giustificato intuitivamente dal significato stesso dell'implicazione: immaginiamo infatti di dimostrare l'asserto $P \Rightarrow Q$ ragionando per casi sui possibili valori di verità che può assumere P. In accordo alla tabella di verità del connettivo $\Rightarrow$, non c'è nulla da dimostrare nel caso in cui il valore di verità di P sia F (se l'antecedente è falso l'implicazione è comunque vera). Se invece assumiamo che P abbia valore di verità T, dobbiamo allora garantirci che anche il valore di verità di Q sia T, altrimenti l'intera implicazione avrebbe valore F. Ma assumere $P \equiv T$ significa anche poter utilizzare P come eventuale giustificazione nella dimostrazione di Q. Detto altrimenti, dimostrare $P \Rightarrow Q$ significa dimostrare che, sotto l'ipotesi che P vale, anche Q vale.

A titolo d'esempio vogliamo dimostrare con questa tecnica la legge:

$$\boxed{p \Rightarrow (p \wedge q \equiv q)}$$

Nella dimostrazione mostriamo l'equivalenza $p \wedge q \equiv q$ utilizzando l'ipotesi p come giustificazione.

$$
\begin{array}{ll}
& p \wedge q \\
\equiv & \quad \{\ \textbf{Ip}\text{: } p\text{, ovvero } p \equiv T\ \} \\
& T \wedge q \\
\equiv & \quad \{\ \text{Unità}\ \} \\
& q
\end{array}
$$

L'annotazione **Ip** nel primo passo di derivazione serve a ricordare che la giustificazione p non è di per s una tautologia (come è invece, ad esempio, Unità nel secondo passo), ma costituisce una assunzione locale alla dimostrazione stessa. Tale annotazione servirà a ricordare che l'ipotesi fatta va tenuta in considerazione al momento in cui si vogliano tirare le conclusioni su quello che si è dimostrato: in altre parole quella sopra non è, come succedeva fino ad ora, una dimostrazione di $(p \wedge q \equiv q)$, quanto piuttosto una dimostrazione che quest'ultimo asserto è implicato tautologicamente da p, l'ipotesi fatta. Per la frequenza di (porzioni di) dimostrazioni come quella precedente, consentiremo di abbreviarle come segue

$$
\begin{array}{ll}
 & p \wedge q \\
\equiv & \quad \{\ \textbf{Ip}\text{: } p\ \} \\
 & q
\end{array}
$$

Vediamo un ulteriore esempio, mostrando con questa tecnica l'implicazione $(P \Rightarrow (Q \equiv X)) \Rightarrow (P \wedge X \Rightarrow Q)$: dimostriamo che vale $P \wedge X \Rightarrow Q$, facendo uso, nella dimostrazione, dell'ipotesi $P \Rightarrow (Q \equiv X)$, laddove ciò si renda utile.

$$
\begin{array}{ll}
 & P \wedge X \\
\Rightarrow & \quad \{\ \textbf{Ip}\text{: } P \Rightarrow (Q \equiv X)\ \} \\
 & (Q \equiv X) \wedge X \\
\equiv & \quad \{\ \text{Elim-}\equiv\ \} \\
 & (Q \Rightarrow X) \wedge (X \Rightarrow Q) \wedge X \\
\Rightarrow & \quad \{\ \text{modus ponens}\ \} \\
 & (Q \Rightarrow X) \wedge Q \\
\Rightarrow & \quad \{\ \text{Elim-}\wedge\ \} \\
 & Q.
\end{array}
$$

Abbiamo pertanto dimostrato che $(P \Rightarrow (Q \equiv X)) \Rightarrow (P \wedge X \Rightarrow Q)$ è una tautologia, in modo assai più semplice che attaccare direttamente l'intera formula.

La tecnica che abbiamo appena visto si generalizza facilmente al caso in cui le assunzioni fatte nel corso di una dimostrazione siano più d'una. A titolo d'esempio, mostriamo come la prova:

$$
\begin{array}{ll}
 & P \\
\Rightarrow & \quad \{\ \textbf{Ip}\text{: } \mathrm{G}_1\ \} \\
 & R \\
\Rightarrow & \quad \{\ \textbf{Ip}\text{: } \mathrm{G}_2\ \} \\
 & Q
\end{array}
$$

sia un modo conveniente per dimostrare

$$(G_1 \wedge G_2 \Rightarrow (P \Rightarrow Q)) \quad (*)$$

Ricordiamo a questo proposito che, per quanto visto sino ad ora, questa è, per definizione, una prova di $(G_1 \Rightarrow (P \Rightarrow R)) \wedge (G_2 \Rightarrow (R \Rightarrow Q))$. Ci basta allora dimostrare che quest'ultima formula implica (*) e a questo scopo utilizziamo una dimostrazione standard, che utilizza cioè solo tautologie come giustificazioni.

$$
\begin{array}{ll}
 & (G_1 \Rightarrow (P \Rightarrow R)) \wedge (G_2 \Rightarrow (R \Rightarrow Q)) \\
\equiv & \quad \{\ \text{Sempl.Sinistra-}\Rightarrow\text{, 2 volte}\ \} \\
 & (G_1 \wedge P \Rightarrow R) \wedge (G_2 \wedge R \Rightarrow Q) \\
\equiv & \quad \{\ \text{Elim-}\Rightarrow\text{, 2 volte}\ \} \\
 & (\neg(G_1 \wedge P) \vee R) \wedge (\neg(G_2 \wedge R) \vee Q) \\
\equiv & \quad \{\ \text{De Morgan, 2 volte}\ \} \\
 & (\neg G_1 \vee \neg \vee P \vee R) \wedge (\neg G_2 \vee \neg R \vee Q) \\
\Rightarrow & \quad \{\ \text{Risoluzione}\ \} \\
 & \neg G_1 \vee \neg P \vee \neg G_2 \vee Q \\
\equiv & \quad \{\ \text{De Morgan}\ \} \\
 & \neg(G_1 \wedge P \wedge G_2) \vee Q \\
\equiv & \quad \{\ \text{Elim-}\Rightarrow\ \} \\
 & G_1 \wedge P \wedge G_2 \Rightarrow Q \\
\equiv & \quad \{\ \text{Sempl.Sinistra-}\Rightarrow\ \} \\
 & G_1 \wedge G_2 \Rightarrow (P \Rightarrow Q)
\end{array}
$$

Vediamo un esempio di applicazione di quanto appena visto, dimostrando la legge del sillogismo disgiuntivo.

$(p \vee q) \wedge (p \Rightarrow r) \wedge (q \Rightarrow s) \Rightarrow (r \vee s)$ (Sillogismo disgiuntivo)

$$
\begin{array}{ll}
 & p \vee q \\
\Rightarrow & \quad \{\ \textbf{Ip}\colon\ p \Rightarrow r\ \} \\
 & r \vee q \\
\Rightarrow & \quad \{\ \textbf{Ip}\colon\ q \Rightarrow s\ \} \\
 & r \vee s
\end{array}
$$

In realtà, questa è una prova di

$$(p \Rightarrow r) \wedge (q \Rightarrow s) \Rightarrow (p \vee q) \Rightarrow (r \vee s)$$

che, grazie alla legge Sempl.Sinistra-$\Rightarrow$, è equivalente al sillogismo disgiuntivo. (**Esercizio**: si dimostri il sillogismo disgiuntivo senza fare uso di giustificazioni che non sono tautologie; si dimostri poi la legge Sempl-$\Rightarrow$ facendo uso di giustificazioni che non sono tautologie).

Il prossimo esempio, seppur semplice, mette in luce un ulteriore uso delle ipotesi come giustificazioni: vediamo perch quella che segue è una dimostrazione di $((P \vee Q) \wedge R) \Rightarrow (R \wedge S) \equiv S)$.

$$
\begin{array}{ll}
 & R \wedge S \\
\equiv & \quad \{\ \textbf{Ip}\colon\ R\ \} \\
 & S
\end{array}
$$

Secondo quanto visto sinora, abbiamo dimostrato in realtà l'implicazione $R \Rightarrow (R \wedge S) \equiv S)$; osserviamo però che, grazie alla legge Sempl-$\wedge$, vale $((P \vee Q) \wedge R) \Rightarrow R$ e, facendo appello alla transitività dell'implicazione, possiamo concludere che quella precedente può anche essere vista come una dimostrazione dell'asserto di partenza, ovvero di $((P \vee Q) \wedge R) \Rightarrow (R \wedge S) \equiv S)$.

Più in generale, una qualunque dimostrazione di $(G \Rightarrow P)$, è anche una dimostrazione di $(G' \Rightarrow P)$, purch $(G' \Rightarrow G)$ sia una tautologia (o, a maggior ragione, purch $G' \equiv G$ sia una tautologia).

Consentiremo dunque di utilizzare dimostrazioni come

$$
\begin{array}{ll}
 & R \wedge S \\
\Rightarrow & \quad \{\ \textbf{Ip}\colon\ (P \vee Q) \wedge R, ((P \vee Q) \wedge R) \Rightarrow R\ \} \\
 & S
\end{array}
$$

o, più brevemente, come

$$
\begin{array}{ll}
 & R \wedge S \\
\Rightarrow & \quad \{\ \textbf{Ip}\colon\ (P \vee Q) \wedge R\ \} \\
 & S
\end{array}
$$

che sottintendono le considerazioni appena viste. Nel primo caso, la giustificazione evidenzia non solo l'ipotesi fatta, $(P \vee Q) \wedge R$, ma anche l'implicazione il cui conseguente è quanto utilizzato effettivamente nel passo di dimostrazione. Nel secondo caso, invece, tale implicazione (una semplice istanza di Sempl-$\wedge$) è stata omessa per brevità. Sarà il buon senso, di volta in volta, a suggerirci che cosa si debba esplicitare o meno nelle giustificazioni.

Riassumendo quanto detto finora, possiamo dare il seguente schema generale di dimostrazione. Sia:

$$
\begin{array}{ll}
 & r_1 \\
conn_1 & \{\ \mathrm{G}_1\ \} \\
 & r_2 \\
conn_2 & \{\ \mathrm{G}_2\ \} \\
 & \ldots \\
conn_{k-1} & \{\ \mathrm{G}_{k-1}\ \} \\
 & r_k
\end{array}
$$

una sequenza di passi di dimostrazione che, grazie alle proprietà dei connettivi $conn_1$, ..., $conn_k$ consente di concludere

$$r_1\ conn\ r_k$$

Si possono allora presentare i due casi seguenti:

- Se le giustificazioni $G_1, G_2, \ldots, G_{k-1}$ sono tutte tautologie note, abbiamo una dimostrazione di $r_1 connr_k$,
- Se invece alcune delle giustificazioni, siano esse $G_{i_1}, \ldots, G_{i_h}$, non sono tautologie ma ipotesi, abbiamo una dimostrazione di $G_{i_1} \wedge \ldots \wedge G_{i_h} \Rightarrow (r_1 connr_k)$.

Se poi, per qualche formula G, vale $G \Rightarrow G_{i_1} \wedge \ldots \wedge G_{i_h}$(o, a maggior ragione, $G \equiv G_{i_1} \wedge \ldots \wedge G_{i_h}$) abbiamo anche una dimostrazione di $G \Rightarrow (r_1 connr_k)$.

6.1 Altre tecniche di dimostrazione

In questo paragrafo vediamo alcune tecniche di dimostrazione molto utili in pratica. La prima, detta dimostrazione per assurdo, deriva dalla legge

$$(\neg p \Rightarrow F) \equiv p$$

la cui dimostrazione è banale. Tale legge suggerisce la seguente tecnica di prova.
Per dimostrare P è sufficiente dimostrare l'implicazione $\neg P \Rightarrow F$

Si noti che, se P è una formula del tipo $Q \Rightarrow R$, la dimostrazione per assurdo ci conduce a dimostrare $Q \wedge \neg R \Rightarrow F$. Vediamo come esempio la dimostrazione per assurdo di $((p \vee q) \Rightarrow r) \Rightarrow (p \Rightarrow r)$.

$$\begin{array}{ll} & ((p \vee q) \Rightarrow r) \wedge \neg(p \Rightarrow r) \\ \equiv & \quad \{ \text{ Elim-}\Rightarrow, \text{ De Morgan } \} \\ & (\neg(p \vee q) \vee r) \wedge (p \vee r) \\ \Rightarrow & \quad \{ \text{ Risoluzione } \} \\ & (\neg(p \vee q) \wedge p) \\ \equiv & \quad \{ \text{ De Morgan } \} \\ & \neg p \wedge \neg q \wedge p \\ \equiv & \quad \{ \text{ Contraddizione } \} \\ & F \end{array}$$

Un'altra tecnica di dimostrazione utile ci è suggerita dalla seguente legge (la cui dimostrazione è lasciata per esercizio):

$$((q \Rightarrow p) \wedge (\neg q \Rightarrow p)) \equiv p$$

Questa tautologia suggerisce la cosiddetta dimostrazione per casi.
Per dimostrare P è sufficiente dimostrare separatamente le due implicazioni

- $\neg Q \Rightarrow P$
- $Q \Rightarrow P$

dove Q è una formula arbitraria.

In altre parole, per dimostrare che P è una tautologia, possiamo dimostrarlo, separatamente, nell'ipotesi in cui vale Q e nell'ipotesi in cui vale $\neg Q$; naturalmente converrà scegliere Q in modo che le due dimostrazioni risultino facilitate. Vediamo, come esempio, la dimostrazione per casi di $((p \vee q) \Rightarrow r) \Rightarrow (p \Rightarrow r)$.

$$\begin{array}{ll} & (p \vee q) \Rightarrow r \\ \equiv & \quad \{ \textbf{Ip}\text{: } q, \text{ Zero } \} \\ & T \Rightarrow r \\ \equiv & \quad \{ \text{ Elim-}\Rightarrow, \text{ Unità } \} \\ & r \\ \Rightarrow & \quad \{ \text{ Intro-}\vee, \text{ Elim-}\Rightarrow \} \\ & p \Rightarrow r \end{array}$$

Abbiamo dunque dimostrato che vale $q \Rightarrow (((p \vee q) \Rightarrow r) \Rightarrow (p \Rightarrow r))$.

$$\begin{array}{ll} & (p \vee q) \Rightarrow r \\ \equiv & \quad \{ \textbf{Ip}\text{: } \neg q \text{ (ovvero } q \Rightarrow F\text{), Unità } \} \\ & p \Rightarrow r \end{array}$$

Si noti che quest'ultima è in realtà una dimostrazione di

$$\neg q \Rightarrow (((p \vee q) \Rightarrow r) \equiv (p \Rightarrow r))$$

e dunque anche di $\neg q \Rightarrow (((p \vee q) \Rightarrow r) \equiv (p \Rightarrow r))$, la seconda parte della nostra dimostrazione per casi.

6.1.1 Esercizi

1. Si dimostri che la prova

$$\begin{array}{ll} & P \\ \Rightarrow & \quad \{ \textbf{Ip}\text{: } Q \} \\ & R \end{array}$$

è un modo conveniente per organizzare una dimostrazione della formula $P \wedge Q \Rightarrow R$.

2. Si dimostri che la prova

$$\begin{array}{ll} & R \\ \equiv & \quad \{ \textbf{Ip}\text{: } P \} \\ & S \\ \equiv & \quad \{ \textbf{Ip}\text{: } Q \} \\ & T \end{array}$$

è un modo conveniente per organizzare una dimostrazione del fatto che $P \wedge Q \Rightarrow R$ (si dimostri, cioè, che la prova data stabilisce una formula che implica $P \wedge Q \Rightarrow R$).

3. Perch la prova

$$\begin{array}{ll} & R \\ \equiv & \quad \{ \textbf{Ip}\text{: } P \} \\ & S \end{array}$$

è anche una dimostrazione di $P \Rightarrow (R \Rightarrow S)$?

7 Il concetto di conseguenza logica e di dimostrazione

Nella nostra vita quotidiana, siamo abituati ad accettare argomentazioni razionali che, a partire da alcune premesse, ci portano a derivare delle conclusioni. Ad esempio siamo pronti a definire come "legittimo" il seguente ragionamento[5]:

premessa 1:	tutti gli uomini sono mortali
premessa 2:	Socrate è un uomo
conclusione:	Socrate è mortale.

[5]Si tratta del classico sillogismo "Tutti gli uomini sono mortali, Socrate è un uomo quindi Socrate è mortale".

Si noti che nella precedente argomentazione non vi è alcun riferimento al fatto che le premesse coinvolte siano asserti *veri* o asserti *falsi*. Ad esempio, qualcuno potrebbe essere convinto della propria immortalità e dunque potrebbe non accettare come vera la prima premessa. Ciò, tuttavia, non inficia il ragionamento fatto, che può essere rifrasato nel seguente modo: se è *vero* che tutti gli uomini sono mortali e che Socrate è un uomo, allora è *vero* che Socrate è mortale. In altre parole, non è possibile che la conclusione del ragionamento sia falsa se sono vere le due premesse.

Analogamente siamo pronti ad accettare come legittimo il seguente ragionamento:

premessa 1:	tutti i numeri pari maggiori di 2 non sono numeri primi
premessa 2:	4 è un numero pari maggiore di 2
conclusione:	4 non è un numero primo.

Vediamo ora un esempio di argomentazione che non siamo in grado di accettare come legittima.

premessa 1:	tutti gli uomini sono mortali
premessa 2:	Socrate è mortale
conclusione:	Socrate è un uomo.

Che dire nel caso in cui Socrate si riferisce ad un simpatico cagnolino e non al noto filosofo? Le due premesse sono ragionevolmente vere (chi scrive non è al corrente dell'esistenza di cani immortali ...), ma la conclusione non lo è.

Le prime due argomentazioni (valide) possono essere ricondotte ad un medesimo procedimento *deduttivo* basato sull'uso di regole *deduttive* o *regole di inferenza*. Una regola di inferenza è una legge che permette di derivare da uno o più *asserti* un altro asserto. Per adesso accontentiamoci di definire un "asserto" come una frase in italiano.

Come primo esempio di regola di inferenza, diamo quella che permette di concludere che un elemento di una collezione (insieme) di individui gode di una certa proprietà se tutti gli elementi della collezione godono della medesima proprietà. Adottiamo la convenzione di indicare con le ultime lettere minuscole dell'alfabeto x, y, z generici elementi di un insieme, con le prime lettere minuscole dell'alfabeto a, b, c, ecc. specifici elementi dell'insieme e con lettere maiuscole quali P, Q, R generici asserti. Spesso scriveremo $P(x)$, $P(a)$ ecc. ad indicare che l'asserto P predica sul generico elemento x o sullo specifico elemento a dell'insieme[6].

La precedente regola di inferenza si può allora scrivere come segue.

regola 1

Dall'asserto "per tutti gli x vale $P(x)$"
si può derivare l'asserto "$P(a)$"

Si noti che nella precedente regola P è un asserto qualsiasi e non vi è alcun riferimento al fatto che P valga o meno sugli elementi dell'insieme in questione (insieme, peraltro, non specificato). Si noti inoltre che $P(a)$ sta per l'asserto P riferito allo specifico elemento a.

Un altro esempio di regola di inferenza è il seguente:

regola 2

Dagli asserti "da Q segue R" e "Q"
si può derivare l'asserto "R"

[6] Queste convenzioni verranno meglio formalizzate in seguito.

Questa regola può essere rifrasata come segue: se è vero che l'asserto R è conseguenza dell'asserto Q ed è vero l'asserto Q, allora è vero anche l'asserto R.

Proviamo ad applicare queste regole di inferenza al primo esempio visto in precedenza, dove utilizziamo gli asserti $uomo(x)$ e $mortale(x)$ sull'insieme degli esseri umani e indichiamo con *socrate* un particolare essere umano.

Osserviamo innanzitutto che la prima premessa è un asserto del tipo "per tutti gli x vale $P(x)$", dove $P(x)$ è a sua volta l'asserto "da $uomo(x)$ segue $mortale(x)$". Le due premesse dell'esempio possono allora essere riscritte come segue:

asserto 1 per tutti gli x da $uomo(x)$ segue $mortale(x)$.

asserto 2 $uomo(socrate)$.

Quella che segue è una *dimostrazione* dell'asserto $mortale(socrate)$ a partire dagli asserti 1 e 2 e dalle regole di inferenza 1 e 2.

per tutti gli x da $uomo(x)$ segue $mortale(x)$. (asserto 1)
applicando la regola 1, con *socrate* per a
da $uomo(socrate)$ segue $mortale(socrate)$. (asserto 3)
applicando la regola 2 all'asserto 3 e all'asserto 2
$mortale(socrate)$. (asserto 4)

L'applicazione di una regola di inferenza ad uno o più asserti dati è un *passo* di dimostrazione. Una *dimostrazione* è una sequenza di passi. Nell'esempio abbiamo applicato dapprima la regola 1 all'asserto 1 ottenendo l'asserto 3 e quindi la regola 2 agli asserti 2 e 3 ottenendo l'asserto 4.

Anche il secondo esempio visto può essere riformulato come sopra. Gli asserti di partenza sono i seguenti:

asserto 1 per tutti gli x da $numero\_pari(x)$ e $x > 2$ segue $non\_primo(x)$.

asserto 2 $numero\_pari(4)$ e $4 > 2$.

È facile costruire la dimostrazione.

per tutti gli x da $numero\_pari(x)$ e $x > 2$ segue $non\_primo(x)$. (asserto 1)
applicando la regola 1, considerando 4 come la costante a
da $numero\_pari(4)$ segue $non\_primo(4)$. (asserto 3)
applicando la regola 2 all'asserto 3 e all'asserto 2
$non\_primo(4)$. (asserto 4)

La cosa che balza all'occhio è che, nonostante si parli nella prima di uomini e nella seconda di numeri naturali, le due dimostrazioni hanno esattamente la stessa struttura. In entambi i casi, a partire da un insieme di asserti dati, successive applicazioni delle regole di inferenza ci hanno consentito di derivare (*dimostrare*) un nuovo asserto. Il fatto che si parli di cose diverse è solamente indotto dal nome che abbiamo dato alle proprietà coinvolte, ad esempio il fatto di essere "uomo" o essere "numero pari". In realtà potremmo non farci condizionare dalle parole e scrivere gli asserti semplicemente come:

asserto 1 per tutti gli x da $P(x)$ segue $Q(x)$.

asserto 2 $P(a)$.

Ancora, la seguente sarebbe una dimostrazione

per tutti gli x da $P(x)$ segue $Q(x)$. (asserto 1)

applicando la regola 1

da $P(a)$ segue $Q(a)$. (asserto 3)

applicando la regola 2 all'asserto 3 e all'asserto 2

$Q(a)$. (asserto 4)

Si noti che quest'ultima è una dimostrazione dell'asserto $Q(a)$ del tutto indipendente dal "significato" dei simboli coinvolti (in particolare dell'asserto Q e dell'oggetto a). Questa è la prima importante caratteristica delle dimostrazioni: la loro indipendenza da qualsiasi "interpretazione", ovvero dal significato attribuito ai simboli che compaiono negli asserti coinvolti. Una dimostrazione è una pura sequenza di trasformazioni "simboliche" di asserti ottenute attraverso l'applicazione meccanica di regole di inferenza. In gergo informatico, si può dire che la dimostrazione è un concetto puramente "sintattico".

Quale è allora il *significato* di una dimostrazione, vista la sua natura di pura manipolazione simbolica di asserti (come messo particolarmente in luce dall'ultimo esempio)? Al concetto sintattico corrisponde un significato comunemente indicato come *semantica*. La semantica di un asserto viene data attraverso il concetto di *interpretazione*. Un'interpretazione attribuisce un significato alle componenti degli asserti. Rifacendoci agli esempi visti, nell'asserto $P(a)$ una interpretazione può stabilire che il simbolo P sta per "essere uomo" e che il simbolo a sta per il noto filosofo greco Socrate, mentre un'altra interpretazione può stabilire che P sta per "essere uomo" mentre a sta per un simpatico cagnolino. Nel primo caso l'asserto $P(a)$ è vero, nel secondo è falso. Ancora, un'interpretazione può stabilire che P sta per "essere numero pari" e a sta per il numero naturale usualmente indicato con il simbolo 4.

Occorre poi notare che non tutte le interpretazioni hanno un ovvio significato intuitivo: ad esempio possiamo avere un'interpretazione in cui il significato di P è la funzione

$$f(x) = \begin{cases} vero & \text{se } x \text{ è un numero naturale primo} \\ falso & \text{altrimenti} \end{cases}$$

ed il significato del simbolo a è il numero naturale (non primo) 8. In questa interpretazione, l'asserto $P(a)$ è falso.

Quindi, dato un insieme di asserti, ci sono interpretazioni che li rendono veri ed altre no. La cosa non ci disturba perché faremo sempre riferimento alle interpretazioni che rendono veri *tutti* gli asserti che abbiamo. Dato un insieme di asserti Γ, un'interpretazione in cui tutti gli elementi di Γ sono veri è detta *modello* di Γ. E' evidente come il concetto di conseguenza logica sia una estensione del concetto di tautologia visto per il calcolo proposizionale. Quando un asserto Q è vero in tutti i modelli di un insieme di asserti Γ si dice che Q è *conseguenza logica* di Γ. In altre parole, non è possibile interpretare i simboli coinvolti in modo da rendere falso Q e veri tutti gli asserti in Γ. Si noti come il concetto di conseguenza logica corrisponda al concetto di "ragionamento legittimo" che abbiamo introdotto informalmente negli esempi iniziali di questo paragrafo, laddove gli asserti in Γ sono le premesse e l'asserto Q è la conclusione del ragionamento stesso.

Il concetto di conseguenza logica, di per sé, non suggerisce alcun metodo pratico per mostrare che una formula Q è o non è conseguenza di un insieme Γ di formule, o, detto altrimenti, per mostrare che è o meno "legittimo" concludere Q dalle premesse Γ. Per mostrare che una conclusione non è conseguenza logica di un insieme di premesse, un metodo ragionevole sembra quello di mostrare che esiste un modello delle premesse in cui la conclusione è falsa. Ciò è quanto abbiamo fatto nell'esempio del cagnolino Socrate. Più problematico è invece stabilire che una formula Q è conseguenza logica di un insieme di formule Γ date. Non possiamo certo sperare di farlo analizzando ogni possibile modello di Γ per assicurarci che in esso Q sia vera: si pensi solo al fatto che i modelli di una formula o di un insieme di formule sono, in generale, infiniti! È proprio nel concetto di dimostrazione che sta la risposta a questo quesito: la dimostrazione (sintattica) di un asserto Q a partire da una collezione di asserti dati Γ mostra che Q è conseguenza logica di Γ. A patto di individuare un insieme di regole di inferenza sufficientemente "potenti" è possibile ricondurre il concetto semantico di conseguenza logica al concetto puramente sintattico di dimostrazione. Si noti che una dimostrazione, come quelle viste negli esempi, è una sequenza di passi di pura manipolazione simbolica degli asserti in gioco, ciascuno corrispondente alla

applicazione di una delle regole di inferenza. Intuitivamente, i vari passi di dimostrazione consentono di trarre una serie di conclusioni (conseguenze) intermedie fino ad arrivare alla conclusione desiderata. Il problema che si pone è allora quello di individuare un insieme di regole di inferenza che:

- siano "corrette": l'applicazione di una regola ad un insieme di premesse deve garantire che la conclusione che se ne trae è effettivamente conseguenza logica di tali premesse.
- siano "complete": se una formula è effettivamente conseguenza logica di un insieme di premesse, l'insieme di regole deve garantire l'esistenza di una dimostrazione di tale fatto.

8 Sintassi dei linguaggi del primo ordine

Il primo aspetto da affrontare è quello puramente sintattico, ovvero stabilire quale è il linguaggio che adottiamo per esprimere ciò che abbiamo finora chiamato asserto e che abbiamo espresso come frase in italiano. La necessità di introdurre un *linguaggio formale* a questo scopo è dovuto alla natura spesso imprecisa e ambigua dei linguaggi naturali come appunto l'italiano. Tuttavia il linguaggio deve essere sufficientemente espressivo per poter descrivere, pur se con una struttura diversa, asserti come quelli che abbiamo utilizzato negli esempi del primo paragrafo.

A partire da un insieme di simboli, detto *alfabeto*, il linguaggio che introduciamo consente di costruire frasi, che chiameremo *formule*, attraverso delle semplici regole di costruzione, in modo analogo a quanto succede con le regole grammaticali dei linguaggi naturali attraverso cui si costruiscono frasi corrette almeno da un punto di vista puramente sintattico[7].

Vediamo quali sono le componenti sintattiche del linguaggio, indicato dai qui in poi con $\mathcal{L}$. Tale linguaggio deve innanzitutto consentire di:

- riferire oggetti specifici, intesi come gli "individui" che popolano il dominio di interesse sul quale si vogliono definire asserti. Negli esempi del primo paragrafo, abbiamo usato a questo scopo simboli quali *Socrate*, 2, ecc. lasciando così intendere il "significato" di tali simboli. Spesso useremo invece nomi puramente simbolici, utilizzando le prime lettere minuscole dell'alfabeto, quali a, b, c, ecc. Quali che siano i simboli utilizzati per indicare gli oggetti del dominio di interesse, essi sono detti le *costanti* del linguaggio.
- esprimere "proprietà" o "relazioni" tra gli oggetti del dominio di interesse. Come nel caso delle costanti, utilizzeremo spesso nomi puramente simbolici, quali p, q, r, ecc. ad indicare tali proprietà: tali simboli sono detti *predicati*. I predicati possono esprimere proprietà di singoli oggetti o relazioni tra oggetti: nel primo caso avremo a che fare con predicati ad un argomento, ad esempio $p(a)$, nel secondo predicati a due o più argomenti, ad esempio $q(b, a), r(a, b, c)$. Ma possiamo avere anche predicati senza argomenti, ad esempio p, al fine di esprimere proprietà che non sono riferite ad oggetti del dominio di interesse (si pensi all'asserto "piove"): questi ultimi verrano detti *lettere proposizionali*. Assumeremo sempre la presenza delle lettere proposizionali $\mathbf{t}$ e $\mathbf{f}$, il cui significato intuitivo è, rispettivamente, quello dell'asserto sempre *vero* e sempre *falso*.

Con gli elementi sintattici visti sino ad ora siamo in grado di costruire asserti semplici sugli elementi del dominio di interesse, che chiameremo formule *atomiche*. Alle formule atomiche possiamo applicare i connettivi già usati per le proposizioni e riassunti nella seguente tabella. Nella tabella seguente sono riportati i cinque connettivi di $\mathcal{L}$, indicando per ciascuno il simbolo utilizzato per rappresentarlo e l'operazione corrispondente:

[7] In questo paragrafo non ci occupiamo del *significato* di una frase, ma solo della sua struttura: frasi come "Il bimbo mangia la mela" e "La mela mangia il bimbo" sono entrambe corrette dal punto di vista sintattico, anche se la seconda può non avere alcun significato di senso comune.

connettivo	*forma simbolica*	*operazione*
non	$\neg p(a)$	negazione
e	$p(a) \wedge q(b,c)$	congiunzione
oppure	$p(a) \vee q(b,c)$	disgiunzione
se ... allora	$p(a) \Rightarrow q(b,c)$	implicazione
se e soltanto se	$p(a) \equiv r(a)$	equivalenza

Gli esempi riportati in tabella non devono far pensare erroneamente che i connettivi possono essere applicati solo per comporre tra di loro formule atomiche: si pensi ad un asserto del tipo "se Paolo ama il teatro e Giuseppe ama il teatro allora Paolo e Giuseppe hanno un interesse in comune". Tale asserto è del tipo $P \Rightarrow Q$ dove a sua volta P è un asserto del tipo $P_1 \wedge P_2$.

Con gli ingredienti sintattici visti sino ad ora è possibile costruire frasi anche complicate che però possono stabilire proprietà e relazioni tra specifici oggetti del dominio di interesse: non è invece possibile costruire asserti più generali che esprimono proprietà riferite a tutti gli elementi del dominio di interesse o ad alcuni di essi, quali ad esempio "*tutti* gli uomini sono mortali", "*qualche* politico è corrotto" e così via. A questo scopo $\mathcal{L}$ consente di utilizzare simboli ausiliari, le *variabili*, che denotano generici elementi del dominio di interesse e che indicheremo con le ultime lettere minuscole dell'alfabeto (x, y, z, ecc.). Le variabili possono essere utilizzate, analogamente alle costanti, come argomenti di predicati, ad esempio $pari(x)$, $q(a,y)$, ecc. Anche se, come vedremo, il linguaggio consente di utilizzare liberamente le variabili, considereremo solo formule in cui le variabili vengono "introdotte" attraverso un simbolo di quantificazione. Il linguaggio prevede a questo scopo due simboli:

- il quantificatore *universale* $\forall$. Possiamo ad esempio scrivere $(\forall x.p(x))$ per esprime l'asserto "per ogni oggetto x vale la proprieta p";
- il quantificatore *esistenziale* $\exists$. Possiamo ad esempio scrivere $(\exists x.q(x))$ per esprimere l'asserto "per qualche oggetto x vale la proprieta q".

I quantificatori possono essere utilizzati anche per "quantificare" formule complicate, come ad esempio $(\forall x.uomo(x) \Rightarrow mortale(x))$ oppure $(\exists x.politico(x) \wedge corrotto(x))$. Si noti l'uso delle parentesi per indicare la formula su cui "agisce" il quantificatore. Nel seguito useremo alcune utili abbreviazioni per annidamenti di quantificatori: scriveremo ad esempio $(\forall x, y.P)$ anziché $(\forall x.(\forall y.P))$. Più in generale:

- $(\forall x_1.(\forall x_2.(\ldots(\forall x_n.P))))$ viene abbreviata con $(\forall x_1, x_2, \ldots, x_n.P)$
- $(\exists x_1.(\exists x_2.(\ldots(\exists x_n.P))))$ viene abbreviata con $(\exists x_1, x_2, \ldots, x_n.P)$

Vediamo qui di seguito alcuni esempi di formalizzazione di asserti nel linguaggio introdotto. Negli esempi, utilizziamo simboli di predicato e di costante "significativi", ma deve essere chiaro che ciò ha il solo scopo di rendere più leggibili le formule ottenute.

1. "Tutti i multipli di 9 sono anche multipli di 3"
   $(\forall x.multiplo(x,9) \Rightarrow multiplo(x,3))$
2. "C'è almeno un numero naturale che non è un numero primo"
   $(\exists x.naturale(x) \wedge \neg primo(x))$
3. "Qualche politico non è corrotto" $(\exists x.politico(x) \wedge \neg corrotto(x))$
4. "Luigi ammira tutti coloro che suonano il pianoforte o il flauto"
   $(\forall x.(suona(x, pianoforte) \vee suona(x, flauto)) \Rightarrow ammira(luigi, x))$

5. "Hanno diritto allo sconto solo i pensionati e i bambini"
   $(\forall x.sconto(x) \equiv (pensionato(x) \vee bambino(x)))$

Il linguaggio introdotto fino ad ora consente di riferire oggetti del dominio di interesse solo attraverso simboli di costante e, in formule quantificate, di variabile. Spesso è utile riferire oggetti che sono "funzione" di altri oggetti del dominio. Si pensi al seguente asserto sui numeri naturali: "Il successore di ogni numero pari è un numero dispari". In esso, sono riferiti due oggetti del dominio di interesse, un generico naturale ed il suo successore: il secondo è chiaramente "funzione" del primo. Per rappresentare situazioni di questo tipo, il linguaggio mette a disposizione un'ulteriore categoria di simboli, i simboli di *funzione*, che denoteremo spesso con le lettere f, g, h e che scriveremo in notazione prefissa. Ogni funzione ha una arietà, ovvero un numero che rappresenta gli argomenti della funzione stessa. Ad esempio, se f ha arietà 2, potremo scrivere $f(a, b)$ ad indicare l'oggetto del dominio ottenuto dagli oggetti a e b attraverso la funzione f. Nel seguito utilizzeremo spesso gli usuali simboli di funzione $+$,$-$, $/$, $\cdot$, ecc. ad indicare le comuni operazioni di somma, sottrazione, divisione e moltiplicazione tra numeri. Inoltre, per queste funzioni utilizzeremo l'usuale notazione infissa, scrivendo ad esempio $3 + 4$ e non $+(3, 4)$.

Vediamo altri esempi di formalizzazioni che utilizzano simboli di funzione.

1. "Il successore di ogni numero pari è un numero dispari"
   $(\forall x.pari(x) \Rightarrow dispari(x + 1))$

2. "Ogni numero naturale maggiore di 25 può essere espresso come somma di un multiplo di 2 e di un multiplo di 3"
   $(\forall x.x > 25 \Rightarrow (\exists y.(\exists z.x = y \cdot 2 + z \cdot 3)))$

3. "Un numero è pari se e solo se è multiplo di 2"
   $(\forall x.pari(x) \equiv (\exists y.x = 2 \cdot y))$.

8.1 Il linguaggio $\mathcal{L}$

In questo paragrafo riassumiamo gli elementi sintattici di $\mathcal{L}$ ed introduciamo un po' di terminologia utilizzata nel seguito. I linguaggi come $\mathcal{L}$ sono detti in logica linguaggi del *prim'ordine*.

Alfabeto

L'alfabeto di $\mathcal{L}$ è costituito da:

(i) un insieme $\mathcal{C}$ di simboli di costante;

(ii) un insieme $\mathcal{F}$ di simboli di funzione;

(iii) un insieme $\mathcal{V}$ di simboli di variabile;

(iv) un insieme $\mathcal{P}$ di simboli di predicato;

(v) i simboli $\neg, \wedge, \vee, \Rightarrow, \equiv$;

(vi) i simboli $\forall$ e $\exists$;

(vii) i simboli "(", ")", "," e ".".

Termini

I termini del linguaggio sono sequenze di simboli che possono comparire come argomenti di predicati. In pratica, un termine è un oggetto sintattico che rappresenta un elemento del dominio di interesse. I termini sono tutte e sole le sequenze ottenibili mediante le seguenti regole.

(T1) ogni costante è un termine;

(T2) ogni variabile è un termine;

(T3) se f è un simbolo di funzione a n argomenti e $t_1, \ldots, t_n$ sono termini, allora $f(t_1, \ldots, t_n)$ è un termine.

Mostriamo che, ad esempio, $f(a, g(b), x)$ è un termine, supponendo che a, b siano simboli di costante in $\mathcal{C}$, f e g siano simboli di funzione in $\mathcal{F}$, rispettivamente a tre e un argomento, e x sia una variabile in $\mathcal{V}$.

1.	b è un termine	(T1)
2.	$g(b)$ è un termine	(T3) applicata a 1 utilizzando g
3.	a è un termine	(T1)
4.	x è un termine	(T2)
5.	$f(a, g(b), x)$ è un termine	(T3) applicata a 2, 3, 4 utilizzando f.

Formule

Le formule sono le frasi del linguaggio utilizzate per descrivere asserti e sono tutte e sole quelle ottenibili mediante le seguenti regole.

(F1) se p è un simbolo di predicato a n argomenti e $t_1, \ldots, t_n$ sono termini, allora $p(t_1, \ldots, t_n)$ è una formula[8]

(F2) se P è una formula, allora $\neg P$ è una formula;

(F3) se P, Q sono formule allora $P \wedge Q$ è una formula;

(F4) se P, Q sono formule allora $P \vee Q$ è una formula;

(F5) se P, Q sono formule allora $P \Rightarrow Q$ è una formula;

(F6) se P, Q sono formule allora $P \equiv Q$ è una formula;

(F7) se P è una formula e x una variabile, allora $(\forall x.P)$ è una formula;

(F8) se P è una formula e x una variabile, allora $(\exists x.P)$ è una formula;

(F9) se P è una formula, allora (P) è una formula.

Mostriamo che, ad esempio, $(\forall x.p(x) \wedge q(a, x))$ è una formula, supponendo che x sia una variabile in $\mathcal{V}$, a sia una costante in $\mathcal{C}$ e p, q siano due predicati in $\mathcal{P}$, rispettivamente ad uno e due argomenti.

1.	x è un termine	(T2)
2.	$p(x)$ è una formula	(F1) applicata a 1 utilizzando p
3.	a è un termine	(T1)
4.	$q(a, x)$ è una formula	(F1) applicata a 1 e 3 utilizzando q
5.	$p(x) \wedge q(a, x)$ è una formula	(F3) applicata a 2 e 4
6.	$(\forall x.p(x) \wedge q(a, x))$ è una formula	(F7) applicata a 5 utilizzando x.

Si noti che le regole di costruzione delle formule consentono di ottenere asserti in cui alcune variabili non vengono introdotte da quantificatori (come ad esempio la formula del passo 5). Tali variabili sono dette *libere* e formule che contengono variabili libere sono dette formule *aperte*, mentre quelle che contengono solo variabili quantificate si dicono chiuse[9]. Nel seguito ci occuperemo sostanzialmente di dare un significato alle sole formule chiuse, in cui cioè ogni variabile viene introdotta mediante un quantificatore. Senza entrare nei dettagli, vediamo il perché di tale scelta attraverso un esempio. Supponiamo di definire asserti sui numeri naturali e consideriamo la formula aperta $multiplo(x, 3)$, dove il significato del predicato *multiplo* è quello ovvio. Non siamo in grado di dire che tale formula è vera né che essa è falsa, a meno che non si dica che la variabile x sta per un particolare numero naturale. Ma anche in questo caso la

[8] Si noti che questa regola, per $n = 0$, definisce anche p come formula atomica, con p lettera proposizionale.

[9] È possibile definire in modo preciso il concetto di formula aperta e chiusa, ma ciò esula dai nostri scopi.

stessa formula può essere in un caso vera (ad esempio se x sta per 9) o falsa (ad esempio se x sta per 8). Consideriamo invece la formula chiusa $(\forall x.multiplo(x, 3))$: possiamo affermare che, nel dominio dei numeri naturali, essa è falsa, poiché vi sono numeri che non sono multipli di 3. Analogamente, la formula chiusa $(\exists x.multiplo(x, 3))$ è vera. Come si vede da questi esempi le variabili quantificate hanno il solo scopo di "segnalare" i punti di azione dei quantificatori che le introducono.

Per semplicità nella trattazione, nel seguito tratteremo solo formule in cui ogni quantificatore introduce una variabile diversa. Così, saremo autorizzati a scrivere $(\forall x.p(x)) \wedge (\exists y.q(y))$ ma non $(\forall x.p(x)) \wedge (\exists x.q(x))$. È bene precisare, tuttavia, che anche questa seconda formula è assolutamente lecita, anzi è possibile stabilire che ha lo stesso significato della prima in qualsivoglia interpretazione.

8.2 Alcuni esempi di formalizzazione

Operazioni su insiemi

In questo paragrafo vediamo come si possono formalizzare le comuni operazioni su insiemi (unione, intersezione, differenza, ecc.) ed alcune proprietà di tali operazioni nel linguaggio della logica che abbiamo introdotto sin qui.

Un *insieme* è semplicemente una collezione di elementi. Di solito, è utile far riferimento ad un *universo* $\mathcal{U}$ (a sua volta un insieme) dal quale si prendono gli elementi. Tipici esempi di insiemi sono:

- i numeri pari, ovvero l'insieme dei numeri naturali divisibili per 2 (in questo caso $\mathcal{U}$ è l'insieme $\mathbf{N}$);
- una retta, ovvero l'insieme dei punti nel piano cartesiano allineati a due punti assegnati (in questo caso $\mathcal{U}$ è il piano cartesiano);
- una circonferenza, ovvero l'insieme dei punti nel piano equidistanti da un punto assegnato (di nuovo $\mathcal{U}$ è il piano cartesiano).

Quale che sia l'universo $\mathcal{U}$ di riferimento, è possibile definire tutta una serie di operazioni e di proprietà sugli insiemi di oggetti in $\mathcal{U}$. Introduciamo, a questo scopo, un linguaggio del prim'ordine mediante il quale formalizziamo operazioni e proprietà attraverso una collezione di formule. Il linguaggio deve consentire innanzitutto di esprimere il fatto che un oggetto dell'universo è elemento di un insieme: ad esempio deve consentire di dire che "4 è elemento dell'insieme dei numeri pari". Il simbolo comunemente usato a questo scopo è $\in$: potremo scrivere ad esempio, $a \in A$ (si legge a "appartiene" ad A) ad indicare che l'oggetto a "fa parte" della collezione A. Osserviamo subito l'importanza di poter distinguere tra *oggetti* ed *insiemi* di oggetti. Formalmente, il linguaggio potrebbe mettere a disposizione due simboli di predicato ad un argomento, ad esempio *obj* e *set*, la cui interpretazione "intesa" è che *obj* vale per elementi dell'universo, mentre *set* vale per insiemi di elementi dell'universo. Per semplificare le formule che scriveremo, useremo invece una semplice convenzione: le lettere minuscole indicano oggetti dell'universo e lettere maiuscole indicano insiemi di oggetti. Quindi, ad esempio, la scrittura $a \in A$ lascia intendere che a sta per un oggetto e A per un insieme[10].

Le usuali operazioni tra insiemi vengono rappresentate attraverso i seguenti simboli di funzione, che introduciamo insieme alla loro definizione formale.

- $\cup$ è l'unione tra due insiemi: $A \cup B$ è l'insieme costituito dagli elementi di A e dagli elementi di B

$$(\forall x, A, B.x \in A \cup B \equiv (x \in A \vee x \in B))$$

- $\cap$ è l'intersezione tra due insiemi: $A \cap B$ è l'insieme costituito dagli elementi che stanno sia in A che in B

$$(\forall x, A, B.x \in A \cap B \equiv (x \in A \wedge x \in B))$$

[10] Senza questa convenzione saremmo invece costretti a scrivere una formula del tipo $obj(a) \wedge set(A) \wedge a \in A$.

- $\setminus$ è la differenza tra insiemi: $A \setminus B$ è l'insieme degli elementi che stanno in A ma non in B

$$(\forall x, A, B.x \in A \setminus B \equiv (x \in A \wedge x \notin B))$$

  dove $x \notin B$ è l'usuale abbreviazione per $\neg(x \in B)$.

Introduciamo ora alcuni simboli di predicato che permettono di esprimere le usuali relazioni tra insiemi. Tra questi gioca un ruolo importante il simbolo $=$: la sua interpretazione "intesa" è che due insiemi A e B sono uguali se contengono esattamente gli stessi elementi.

- $(\forall A, B.(A = B \equiv (\forall x.x \in A \equiv x \in B)))$

Abbiamo poi le seguenti relazioni:

- $\subseteq$ è la relazione di sottinsieme: $A \subseteq B$ (si legge A è contenuto o uguale a B) se ogni elemento di A è anche elemento di B

$$(\forall A, B.A \subseteq B \equiv (\forall x.x \in A \Rightarrow x \in B))$$

- $\subset$ è la relazione di sottinsieme proprio: $A \subset B$ (si legge A è strettamente contenuto in B) se ogni elemento di A è anche elemento di B, ma c'è almeno un elemento di B che non è elemento di A.

$$(\forall A, B.A \subset B \equiv ((\forall x.x \in A \Rightarrow x \in B) \wedge (\exists y.y \in B \wedge y \notin A))).$$

Osserviamo come la precedente relazione si possa anche formalizzare, utlizzando le precedenti, come segue:

$$(\forall A, B.A \subset B \equiv (A \subseteq B \wedge A \neq B))$$

dove $A \neq B$ è l'usuale abbreviazione per $\neg(A = B)$.

Il simbolo di costante $\emptyset$ viene di solito utilizzato per rappresentare l'insieme *vuoto*, che non contiene cioè alcun elemento: in formule

$$(\forall x.x \notin \emptyset)$$

Relazioni di equivalenza

Dato un insieme $\mathcal{I}$, il suo prodotto cartesiano è l'insieme di tutte le coppie di elementi in $\mathcal{I}$, e viene di solito rappresentato con $\mathcal{I} \times \mathcal{I}$. Ad esempio, con $\mathcal{I} = \{a, b, c\}$,

$$\mathcal{I} \times \mathcal{I} = \{a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}.$$

Una relazione R su $\mathcal{I}$ è un sottinsieme di $\mathcal{I} \times \mathcal{I}$. Ad esempio, $\{a, b), (b, c)\}$ è una relazione sull'insieme $\{a, b, c\}$. Esempi tipici di relazioni sono la relazione $<$ tra numeri naturali, la relazione di parentela tra esseri umani e così via, la relazione di inclusione tra sottinsiemi di un dato insieme, e così via. Per analogia con le relazioni numeriche, rappresentiamo una generica relazione R su un insieme in notazione infissa, scrivendo, ad esempio, aRb ad indicare che $(a, b) \in R$. Una relazione R è detta relazione di equivalenza se soddisfa alcune proprietà, che formalizziamo nel seguito:

- proprietà riflessiva: ogni elemento è in relazione con se stesso

$$(\forall x.xRx)$$

- proprietà simmetrica: se un elemento è in relazione con un altro elemento, vale anche il viceversa

$$(\forall x, y.xRy \Rightarrow yRx)$$

- proprietà transitiva: se un elemento a è in relazione con un elemento b e quest'ultimo è in relazione con c, anche a è in relazione con c

$$(\forall x, y, z.xRy \wedge yRz \Rightarrow xRz)$$

9 Semantica

La semantica di una formula è un *valore di verità*. Nel seguito utilizzeremo *tt* per indicare il valore *vero* e *ff* per indicare il valore *falso*. Per quanto riguarda le formule chiuse, la loro semantica dipende da un'*interpretazione* che stabilisce il significato dei simboli che vi compaiono. Consideriamo ad esempio la formula $(\forall x.p(x) \vee q(x))$: se il dominio di interesse è quello degli esseri umani, il significato di p è "essere maschio" e quello di q è "essere femmina" la formula può essere interpretata come "Ogni essere umano è maschio o femmina" ed è dunque vera; se invece il dominio di interesse è quello dei numeri naturali, il significato di p è "essere numero primo" e quello di q è "essere numero pari", la formula può essere interpretata come "Ogni numero naturale è primo o è pari" ed è dunque falsa.

Un'interpretazione deve stabilire:

- il dominio di interesse;
- a quali elementi del dominio corrispondono i simboli in $\mathcal{C}$;
- a quali funzioni sul dominio corrispondono i simboli in $\mathcal{F}$;
- a quali proprietà o relazioni corrispondono i simboli in $\mathcal{P}$.

Con ciò l'interpretazione consente di stabilire il significato delle formule atomiche chiuse: il significato delle formule chiuse non atomiche viene poi ottenuto a partire da quello delle sue componenti. Vediamo subito un esempio. Consideriamo un linguaggio in cui $\mathcal{C}$ contiene i simboli a, b e c, non vi sono simboli di funzione e $\mathcal{P}$ contiene il simbolo p a un argomento. Consideriamo le interpretazioni $\mathcal{I}_1$ e $\mathcal{I}_2$ seguenti:

- il dominio di interesse di $\mathcal{I}_1$ è l'insieme delle città {Milano, Roma, Taormina}; a sta per Milano, b sta per Roma e c sta per Taormina; p sta per la seguente funzione:

$$f(x) = \begin{cases} tt & \text{se } x \text{ è capoluogo di provincia} \\ ff & \text{altrimenti} \end{cases}$$

- il dominio di interesse di $\mathcal{I}_2$ è l'insieme di numeri $\{5, 10, 25\}$; a sta per 5, b per 10 e c per 25. Il significato di p è la seguente funzione:

$$g(x) = \begin{cases} tt & \text{se } x \text{ è multiplo di 5} \\ ff & \text{altrimenti} \end{cases}$$

Consideriamo ora alcune formule ed il loro *valore di verità*, ovvero il loro significato, nelle due interpretazioni.

Formula	Valore in $\mathcal{I}_1$	valore in $\mathcal{I}_2$
$p(a)$	vero	vero
$p(b)$	vero	vero
$p(c)$	falso	vero
$p(a) \wedge p(c)$	falso	vero
$(\exists x.p(x))$	vero	vero
$(\forall x.p(x))$	falso	vero
$(\exists x.p(x)) \wedge (\exists y.\neg p(y))$	vero	falso

Il valore di verità delle tre formule atomiche $p(a), p(b)$ e $p(c)$ è direttamente stabilito dall'interpretazione di p. Il valore di verità della congiunzione $p(a) \wedge p(c)$ viene invece "calcolato" a partire dal valore dei due membri della congiunzione. Osserviamo infine che il significato intuitivo dell'ultima formula in tabella è:

> nell'insieme {Milano, Roma, Taormina} c'è sia una città che è capoluogo di provincia che una città che non lo è (vero);
>
> nell'insieme $\{5, 10, 25\}$ c'è sia un numero che è multiplo di 5 che un numero che non lo è (falso).

Consideriamo ora una nuova interpretazione, $\mathcal{I}_3$ in cui: il dominio di interesse è l'insieme di tutte le città d'Italia; a sta per Milano, b sta per Roma, c sta per Napoli e p ha lo stesso significato dato in $\mathcal{I}_1$. Vediamo quale è il valore di verità in $\mathcal{I}_3$ di alcune formule:

Formula	Valore in $\mathcal{I}_3$
$(\forall x.p(x))$	falso
$(\exists x.p(x)) \wedge (\exists y.\neg p(y))$	vero

Si noti che, nonostante le città corrispondenti ad a, b e c siano tutte capoluoghi di provincia, il valore di $(\forall x.p(x))$ è falso: infatti, tra *tutte* le città d'Italia esistono anche città che non sono capoluoghi di provincia. Analogamente la formula $(\exists x.p(x)) \wedge (\exists y.\neg p(y))$ è vera in quanto tra *tutte* le città d'Italia vi sono sia capoluoghi di provincia che non.

Come accennato in conclusione del precedente paragrafo, per stabilire il significato di formule aperte (ovvero che contengono variabili libere) non basta stabilire quello dei simboli di costante, funzione e predicato che vi compaiono, ma bisogna anche stabilire quali oggetti sono associati alle varibili libere. Ad esempio non basta dire che il dominio di interesse è quello dei numeri naturali e che il simbolo p sta per "essere pari" per dare semantica alla formula aperta $p(x)$: bisogna anche dire per quale numero naturale sta x. Quando avremo a che fare con formule aperte, affiancheremo ad una interpretazione un *assegnamento* per le variabili libere, ovvero una associazione tra queste ultime e gli elementi del dominio di interesse.

9.1 Interpretazioni

Dato un linguaggio $\mathcal{L}$, una *interpretazione* $\mathcal{I}$ è costituita da:

(i) un insieme $\mathcal{D}_\mathcal{I}$, detto *dominio* dell'interpretazione. Tale insieme costituisce quello che abbiamo finora chiamato formalmente il "dominio di interesse".

(ii) una associazione $\alpha_\mathcal{I}$ che:

- ad ogni simbolo di costante c in $\mathcal{C}$ associa un elemento in $\mathcal{D}_\mathcal{I}$. L'elemento associato a c viene rappresentato da $\alpha_\mathcal{I}(c)$.
- ad ogni simbolo di funzione f ad n argomenti in $\mathcal{F}$ associa una funzione $\alpha_\mathcal{I}(f)$ che, data una n-upla di elementi in $\mathcal{D}_\mathcal{I}$ restituisce un elemento in $\mathcal{D}_\mathcal{I}$. Formalmente:

$$\alpha_\mathcal{I}(f) : \underbrace{\mathcal{D}_\mathcal{I} \times \ldots \times \mathcal{D}_\mathcal{I}}_{n \text{ volte}} \longrightarrow \mathcal{D}_\mathcal{I}$$

- ad ogni lettera proposizionale in p in $\mathcal{P}$ associa un valore di verità $\alpha_\mathcal{I}(p)$, ovvero $\alpha_\mathcal{I}(p) = tt$ o $\alpha_\mathcal{I}(p) = ff$. In particolare, $\alpha_\mathcal{I}(\mathbf{t}) = tt$ e $\alpha_\mathcal{I}(\mathbf{f}) = ff$.
- ad ogni simbolo di predicato p ad n argomenti in $\mathcal{P}$ associa una funzione $\alpha_\mathcal{I}(p)$ che, data una n-upla di elementi in $\mathcal{D}_\mathcal{I}$ restituisce un valore di verità. Formalmente:

$$\alpha_\mathcal{I}(p) : \underbrace{\mathcal{D}_\mathcal{I} \times \ldots \times \mathcal{D}_\mathcal{I}}_{n \text{ volte}} \longrightarrow \{tt, ff\}$$

Nel seguito scriveremo spesso $\mathcal{I} = (\mathcal{D}, \alpha)$ ad indicare che $\mathcal{D}$ è il dominio di $\mathcal{I}$ e α è l'associazione definita da $\mathcal{I}$.
Vediamo subito un esempio. Sia $\mathcal{L}$ un linguaggio in cui:

- $\mathcal{C}$ contiene il solo simbolo a;
- $\mathcal{F}$ contiene i simboli f, g entrambi ad un solo argomento;
- $\mathcal{P}$ contiene il solo simbolo p a due argomenti.

Una possibile interpretazione per tale linguaggio è costituita dal dominio $\mathbf{N}$ dei numeri naturali e dalla seguente associazione α:

- $\alpha(a)$ è 0;
- $\alpha(f)$ è la funzione *successore*, ovvero, dato un numero naturale n, $\alpha(f)(n) = n + 1$;
- $\alpha(p)$ è l'usuale relazione $>$ tra numeri naturali. Ad esempio $\alpha(p)(3, 2) = tt$ mentre $\alpha(p)(7, 12) = ff$

Semantica dei termini chiusi

Data una interpretazione $\mathcal{I} = (\mathcal{D}, \alpha)$, è possibile associare ad ogni termine chiuso (ovvero senza variabili) t del linguaggio un elemento, denotato da $\alpha(t)$, del dominio dell'interpretazione, utilizzando le seguenti regole:

(R1) se t è una costante c, allora $\alpha(t) = \alpha(c)$;

(R2) se t è il termine $f(t_1, \ldots, t_n)$ e $d_1, \ldots, d_n$ sono, rispettivamente $\alpha(t_1), \ldots, \alpha(t_n)$, allora $\alpha(t) = \alpha(f)(d_1, \ldots, d_n)$.

Utilizzando l'esempio precedente, mostriamo che $\alpha(f(f(a))) = 2$.

1. $\alpha(a) = 0$ (R1) e definizione di α
2. $\alpha(f(a)) = 1$ (R2) utilizzando 1. e la definizione di $\alpha(f)$
3. $\alpha(f(f(a))) = 2$ (R2) utilizzando 2. e la definizione di $\alpha(f)$.

Assegnamento

Dato un dominio $\mathcal{D}$, un *assegnamento* è una funzione ρ che associa a ciascuna variabile in $\mathcal{V}$ un elemento di $\mathcal{D}$. Formalmente:

$$\rho : \mathcal{V} \longrightarrow \mathcal{D}.$$

Se d è l'emento di $\mathcal{D}$ associato da ρ alla variabile x, scriveremo, nella usuale notazione funzionale, $\rho(x) = d$. Inoltre, se ρ è un assegnamento, d un elemento del dominio e x una variabile, con la scrittura $\rho[{}^{d}/_{x}]$ indichiamo un nuovo assegnamento che associa alla variabile x l'elemento d e che si comporta come ρ in corrispondenza di ogni altra variabile diversa da x. Più formalmente:

$$\rho[{}^{d}/_{x}](v) = \begin{cases} d & \text{se } v = x \\ \rho(v) & \text{altrimenti} \end{cases}$$

Consideriamo, ad esempio, l'insieme di variabili $\{x, y, z, \ldots\}$, il dominio $\mathbf{N}$ dei numeri naturali ed un assegnamento ρ che associa alla variabile x il numero 0, alla variabile y il numero 3 e alla variabile z il numero 1, ovvero $\rho(x) = 0$, $\rho(y) = 3$ e $\rho(z) = 1$. Se ρ' è l'assegnamento $\rho[{}^{15}/_{z}]$ avremo che: $\rho'(x) = 0$, $\rho'(y) = 3$ e $\rho'(z) = 15$.

Semantica dei termini

Data un'interpretazione $\mathcal{I} = (\mathcal{D}, \alpha)$ ed un assegnamento ρ la semantica di un termine (eventualmente non chiuso) t è ottenuta estendendo semplicemente le regole (R1) e (R2) viste sopra per ottenere l'oggetto in $\mathcal{D}$ rappresentato da t, che denoteremo con $\alpha_\rho(t)$ per evidenziarne la dipendenza sia da α che da ρ.

(R0) se t è la variabile x, allora $\alpha_\rho(t) = \rho(x)$;

(R1) se t è la costante c, allora $\alpha_\rho(t) = \alpha(c)$;

(R2) se t è il termine $f(t_1, \ldots, t_n)$ e $d_1, \ldots, d_n$ sono, rispettivamente $\alpha_\rho(t_1), \ldots, \alpha_\rho(t_n)$, allora $\alpha_\rho(t) = \alpha(f)(d_1, \ldots, d_n)$.

Ancora in riferimento all'esempio precedente, mostriamo che, dato un assegnamento ρ in cui $\rho(x) = 4$, $\alpha_\rho(f(f(x))) = 6$.

1. $\alpha_\rho(x) = 4$ (R0) e definizione di ρ
2. $\alpha(f(x)) = 5$ (R2) utilizzando 1. e la definizione di $\alpha(f)$
3. $\alpha(f(f(x))) = 6$ (R2) utilizzando 2. e la definizione di $\alpha(f)$.

Semantica delle formule

Come detto in precedenza, il nostro scopo è quello di definire la semantica delle formule *chiuse* del linguaggio. Tuttavia, come apparirà più chiaramente nel seguito, la presenza dei quantificatori ci costringe a dover definire anche il significato di formule aperte, che dipende anche da un assegnamento. Siano dunque $\mathcal{I}$ un'interpretazione, ρ un assegnamento e φ una formula (chiusa o aperta) del linguaggio: nel seguito definiamo il significato di φ nell'interpretazione $\mathcal{I}$ sotto l'assegnamento ρ, che denotiamo con $\mathcal{I}_\rho(\varphi)$. Tale significato sarà chiaramente un valore di verità, tt o ff.

Semantica delle formule atomiche

Il caso più semplice è quello delle formule atomiche chiuse.

(S1) se φ è la formula atomica $p(t_1, \ldots, t_n)$ e $\alpha_\rho(t_1) = d_1, \ldots, \alpha_\rho(t_n) = d_n$, allora $\mathcal{I}_\rho(\varphi) = \alpha(p)(d_1, \ldots, d_n)$

Un caso particolare di tale regola, con $n = 0$, definisce anche il significato di formule atomiche costituite da una lettera proposizionale:

se φ è la lettera proposizionale p, allora $\mathcal{I}_\rho(p) = \alpha(p)$

Semplice è anche il caso di una formula φ del tipo (P): il suo significato è lo stesso di P, ovvero:

(S2) se φ è la formula (P) allora $\mathcal{I}_\rho(\varphi) = \mathcal{I}_\rho(P)$

Questa regola mette in luce come le parentesi costituiscano semplicemente un mezzo sintattico per evidenziare la struttura di una formula o per imporre una precisa struttura alla formula stessa. Ad esempio, una formula del tipo $p \wedge q \vee r$ può essere interpretata come la disgiunzione tra r e la congiunzione $p \wedge q$, oppure come la congiunzione tra p e la disgiunzione $q \vee r$. Nel primo caso è bene allora scriverla come $(p \wedge q) \vee r$, nel secondo come $p \wedge (q \vee r)$.

Semantica dei connettivi

Il valore di verità di negazioni, congiunzioni, disgiunzioni, implicazioni ed equivalenze si ottiene in maniera standard dal valore di verità delle sottoformule che le compongono.

(S3) se φ è la formula $\neg P$, allora $\mathcal{I}_\rho(\varphi) = \overline{\mathcal{I}_\rho(P}$, dove $\overline{tt} = ff$ e $\overline{ff} = tt$

(S4) se φ è la formula $P \wedge Q$, allora $\mathcal{I}_\rho(\varphi) = tt$ se $\mathcal{I}_\rho(P) = tt$ e $\mathcal{I}_\rho(Q) = tt$; altrimenti $\mathcal{I}_\rho(\varphi) = ff$

(S5) se φ è la formula $P \vee Q$, allora $\mathcal{I}(_\rho\varphi) = ff$ se $\mathcal{I}_\rho(P) = ff$ e $\mathcal{I}_\rho(Q) = ff$; altrimenti $\mathcal{I}_\rho(\varphi) = tt$

(S6) se φ è la formula $P \Rightarrow Q$, allora $\mathcal{I}_\rho(\varphi) = ff$ se $\mathcal{I}_\rho(P) = tt$ e $\mathcal{I}_\rho(Q) = ff$; altrimenti $\mathcal{I}_\rho(\varphi) = tt$

(S7) se φ è la formula $P \equiv Q$, allora $\mathcal{I}_\rho(\varphi) = tt$ se $\mathcal{I}_\rho(P) = \mathcal{I}_\rho(Q)$; altrimenti $\mathcal{I}_\rho(\varphi) = ff$

Si noti come le precedenti regole stabiliscano una volta per tutte, ed in modo non ambiguo, il significato dei connettivi. Ciò non accade nei linguaggi naturali, come l'italiano. Si pensi ad esempio alla disgiunzione: mentre è chiaro il significato di una frase del tipo "Dormo o son desto" (dal momento che non è possibile dormire ed essere svegli contemporaneamente), può non esserlo quello della frase "Carlo mangia carne *o* insalata": dobbiamo arguire da ciò che Carlo non mangia sia la carne che l'insalata? Oppure dobbiamo arguire che mangia l'una, l'altra, o *entrambe*? La semantica che abbiamo appena introdotto interpreta la frase nel secondo modo, come appare evidente dalla regola (v).

Un connettivo la cui semantica può non risultare ovvia, se confrontata con il suo significato nel ragionamento comune, è il connettivo di implicazione ($\Rightarrow$). Supponiamo di avere due formule atomiche *piove* e *porto l'ombrello* e di considerare la formula *piove* $\Rightarrow$ *porto l'ombrello* ottenuta dalle precedenti mediante il connettivo di implicazione.

È chiaro che in una interpretazione in cui *piove* e *porto l'ombrello* sono entrambe vere, l'intera formula deve essere vera, mentre in una in cui *piove* è vera e *porto l'ombrello* è falsa, l'implicazione deve essere falsa: se in una giornata piovosa di fine autunno, bagnato fradicio, sprovvisto di qualsiasi protezione, affermo "se piove allora porto l'ombrello", sto dicendo una falsità.

La semantica del connettivo rispecchia questo ragionamento: $tt \Rightarrow tt$ ha valore tt, mentre $tt \Rightarrow ff$ ha valore ff.

Quale è, però, il valore di *piove* $\Rightarrow$ *porto l'ombrello* in una interpretazione in cui *piove* è falso? Se siamo in un'assolata giornata di piena estate e affermo: "se piove allora porto l'ombrello", si può dire o meno se ho detto la verità? Usando il ragionamento comune, diremmo che quello che ho affermato "è possibile". Purtroppo in logica matematica non esiste il valore di verità "è possibile": in una interpretazione data, una formula può solamente essere vera o falsa. Si stabilisce quindi, convenzionalmente, di dare valore di verità tt a tutte le implicazioni "possibili". Questo corrisponde a dire che una implicazione $P \Rightarrow Q$ è vera in una interpretazione che assegna valore ff a P, indipendentemente dal valore di Q. Come vedremo questa scelta ci permette di avere molte proprietà interessanti.

Semantica dei quantificatori

Veniamo infine alle formule quantificate il cui significato, seppure chiaro intuitivamente, necessita di un bagaglio formale piuttosto complicato. Consideriamo una semplice formula del tipo $(\exists x.p(x))$, dove p è un simbolo di predicato ad un argomento. Ciò che vorremmo esprimere attraverso una regola nello stile delle regole S0 $\div$ S8 è che, data un'interpretazione $\mathcal{I} = (\mathcal{D}, \alpha)$, tale formula è vera se e soltanto se "c'è un elemento in $\mathcal{D}$ che soddisfa la proprietà $\alpha(p)$". Un primo tentativo (errato) di formalizzazione è la regola

$\alpha((\exists x.p(x))) = tt$ se esiste d tale che $\alpha(p(d)) = tt$; $\alpha((\exists x.p(x))) = ff$ altrimenti.

Il problema è che l'oggetto d in questione potrebbe non essere associato tramite α ad alcun termine del linguaggio. Si pensi di nuovo all'esempio del linguaggio che prevede le sole costanti a, b e c ed il simbolo di predicato p ad un argomento, e all'interpretazione $\mathcal{I} = (\mathcal{D}, \alpha)$, in cui: $\mathcal{D}$ è l'insieme delle città italiane, $\alpha(a)$ = Taormina, $\alpha(b)$ = Assisi, $\alpha(c)$ = Volterra e p è la proprietà "essere capoluogo di provincia". La formula $(\exists x.p(x))$ è vera in questa interpretazione: ad esempio Milano è un capoluogo di provincia. Purtroppo nessuna delle città che è capoluogo di provincia è associata ad una costante del linguaggio (non possiamo ad esempio scrivere p(Milano)).

La soluzione a questo problema si ottiene utilizzando il concetto di assegnamento: la formula $(\exists x.p(x))$ è vera in un'interpretazione $\mathcal{I}$ e in un assegnamento ρ, se c'è almeno un elemento del dominio d tale che $\mathcal{I}_{\rho[^d/_x]}(p(x)) = tt$. Nell'esempio, tale elemento potrebbe essere quello che associa alla variabile x la città Milano. Analogamente, la formula $(\forall x.p(x))$ è vera in $\mathcal{I}$ e nell'assegnamento ρ se, per qualunque oggetto d del dominio, si ha che $\mathcal{I}_{\rho[^d/_x]}(p(x)) = tt$. Nell'esempio, abbiamo che $(\forall x.p(x))$ è falsa: basta considerare l'assegnamento $\rho' = \rho[^{Taormina}/_x]$ per ottenere che $\mathcal{I}_{\rho'}(p(x)) = ff$.

La generalizzazione di quanto visto negli esempi precedenti ci conduce alle regole per il quantificatore universale ed esistenziale.

(S8) se φ è la formula $(\forall x.P)$, allora $\mathcal{I}_\rho(\varphi) = tt$ se $\mathcal{I}_{\rho[^d/_x]}(P) = tt$ per qualunque d in $\mathcal{D}$; altrimenti $\mathcal{I}_\rho(\varphi) = ff$

(S9) se φ è la formula $(\exists x.P)$, allora $\mathcal{I}_\rho(\varphi) = tt$ se c'è almeno un elemento d in $\mathcal{D}$ per cui $\mathcal{I}_{\rho[^d/_x]}(P) = tt$; altrimenti $\mathcal{I}_\rho(\varphi) = ff$

Prima di vedere qualche esempio è importante sottolineare che, nel caso di formule chiuse, la semantica *non* dipende da alcun assegnamento per le variabili ma solo dall'interpretazione, che corrisponde a quanto mostrato intuitivamente al termine del precedente paragrafo. Questo importante risultato, la cui dimostrazione formale esula dai nostri scopi, può essere formalmente enunciato come segue:

Data un'interpretazione $\mathcal{I}$ ed una formula chiusa φ, quali che siano ρ e ρ' si ha

$$\mathcal{I}_\rho(\varphi) = \mathcal{I}_{\rho'}(\varphi)$$

9.2 Modelli

Dato un linguaggio ed una formula φ, vi sono, in generale, interpretazioni in cui la formula è vera ed altre in cui la formula è falsa, come abbiamo visto negli esempi.

Sia allora $\mathcal{I}$ un'interpretazione e φ una formula: se φ è vera in $\mathcal{I}$ si dice che $\mathcal{I}$ è un *modello* per φ. Per questa importante nozione, introduciamo una apposita notazione

$$\mathcal{I} \models \varphi.$$

Questa notazione verrà utilizzata anche per rappresentare il fatto che una interpretazione è modello per un insieme Γ di formule: scriveremo cioè

$$\mathcal{I} \models \Gamma$$

ad indicare che, per ciascuna formula φ in Γ, si ha $\mathcal{I} \models \varphi$. Inoltre indicheremo con $\mathcal{I} \not\models \varphi$ (risp. $\mathcal{I} \not\models \Gamma$) ad indicare che l'interpretazione $\mathcal{I}$ *non* è modello di φ (risp. Γ).

Se una formula è vera in almeno una interpretazione si dice che essa è *soddisfacibile*, mentre una formula falsa in qualunque interpretazione è detta *insoddisfacibile*. Inoltre le formule vere in qualunque interpretazione si dicono *valide*.

Ecco alcuni esempi:

$(p(a)$	soddisfacibile
$p(a) \vee \neg p(a)$	valida
$p(a) \wedge \neg p(a)$	insoddisfacibile

Se φ è una formula valida, scriviamo $\models \varphi$ per sottolineare il fatto che la verità di φ è indipendente dall'interpretazione.

9.3 Conseguenza logica

La nozione di modello ci consente di formalizzare il concetto di conseguenza logica visto nell'introduzione a queste note.

Sia Γ un insieme di formule e φ una formula. Si dice che φ è *conseguenza logica* di Γ se e soltanto se φ è una formula vera in qualunque modello di Γ. I simboli $\models$ e $\not\models$ verranno utilizzati anche per rappresentare il fatto che una formula è o meno conseguenza logica di un insieme di formule: scriveremo cioè $\Gamma \models \varphi$ (risp. $\Gamma \not\models \varphi$) ad indicare che φ è (risp. non è) conseguenza logica di Γ.

9.4 Esempi

Consideriamo il seguente insieme di formule *Ins*, introdotte nel paragrafo 8.2.

$(\forall x, A, B.x \in A \cup B \equiv (x \in A \vee x \in B))$	(unione
$(\forall x, A, B.x \in A \cap B \equiv (x \in A \wedge x \in B))$	(intersezione
$(\forall x, A, B.x \in A \setminus B \equiv (x \in A \wedge x \notin B))$	(differenza
$(\forall A, B.(A = B \equiv (\forall x.x \in A \equiv x \in B)))$	(uguaglianza
$(\forall A, B.A \subseteq B \equiv (\forall x.x \in A \Rightarrow x \in B))$	(inclusione
$(\forall x.x \notin \emptyset)$	(vuoto

Un modello di questo insieme di formule è chiaramente un'intepretazione in cui il dominio di interesse è costituito da $\mathbf{N}$ e da $2^{\mathbf{N}}$ (l'insieme i cui elementi sono tutti i possibili sottinsiemi di $\mathbf{N}$) e i simboli di funzione e predicato sono interpretati nel modo ovvio. Ma anche un'interpretazione in cui il dominio è costuito da un qualunque insieme di oggetti $\mathbf{A}$ e da $2^{\mathbf{A}}$ ed i simboli sono interpretati nel modo ovvio è modello delle formule date.

Vediamo invece un'interpretazione che non è modello delle formule precedenti. Consideriamo il dominio costituito dagli oggetti $\bullet, \dagger$ e dagli insiemi $\{\}$ (l'insieme vuoto), $\{\bullet\}$, $\{\dagger\}$ e $\{\bullet, \dagger\}$ ed in cui, ad esempio, il simbolo $\cup$ è interpretato dalla seguente funzione $\uplus$:

$$\uplus(A, B) = \begin{cases} \{\ \} & \text{se } A = B \\ A & \text{altrimenti} \end{cases}$$

Tale interpretazione non è modello della formula (unione).

10 Sistemi di dimostrazione

10.1 La necessità di un calcolo formale

Nell'introduzione a queste note abbiamo già osservato come il concetto semantico di conseguenza logica debba essere affiancato da un metodo di calcolo che consenta di "dimostrare" che una formula è o meno conseguenza logica di un insieme di formule. Ad esempio è facile convincersi che la formula

$$(\forall A, B. A \cup B = B \cup A)$$

è conseguenza logica delle formule *Ins* del paragrafo 9.4. In altre parole, in tutti i modelli di *Ins* l'operazione di unione è commutativa.

L'idea di base della teoria della dimostrazione (*proof theory*) è di identificare un insieme di *regole di inferenza* che consentano di organizzare una dimostrazione attraverso una sequenza di semplici passi di dimostrazione. Ogni passo di dimostrazione corrisponde alla applicazione di una singola regola di inferenza, che consente di derivare una conclusione φ a partire da una serie di premesse Γ. Un *sistema di dimostrazione* (*proof system*) $\mathcal{S}$ è dunque una collezione di regole di inferenza. Una *dimostrazione* in $\mathcal{S}$ di una formula φ a partire da un insieme di premesse Γ è una sequenza di formule $\varphi_1, \varphi_2, \ldots, \varphi_n$ in cui:

(1) ogni formula φ_i è un elemento di Γ oppure è ottenuta applicando una regola di inferenza di $\mathcal{S}$ a partire dalle premesse Γ e $\varphi_1, \ldots, \varphi_{i-1}$

(2) φ_n è proprio φ

La (1) mette in luce il fatto che, in una dimostrazione, le premesse che si possono utilizzare in un passo sono non solo le premesse date Γ ma anche tutte le formule derivate nei passi di dimostrazione precedenti. Nel seguito indichiamo con $\Gamma \vdash_{\mathcal{S}} \varphi$ il fatto che la formula φ è dimostrabile in $\mathcal{S}$ a partire dalle premesse Γ.

Un sistema di dimostrazione deve essere *corretto*, ovvero consentire di derivare conclusioni che sono effettivamente conseguenze delle premesse date: se $\Gamma \vdash_{\mathcal{S}} \varphi$ allora $\Gamma \models \varphi$. Un sistema è anche *completo* se permette di dimostrare una formula a partire da un insieme di premesse se la prima è conseguenza logica del secondo: se $\Gamma \models \varphi$ allora $\Gamma \vdash_{\mathcal{S}} \varphi$.

10.2 Un calcolo formale

Nella logica classica esistono molti sistemi di dimostrazione che godono delle proprietà di correttezza e completezza. In queste note, presenteremo un calcolo orientato alla dimostrazione di formule con una particolare struttura: le equivalenze e le implicazioni. Presentiamo cioè un frammento di sistema che consente di dimostrare formule del tipo $\phi \equiv \psi$ e $\phi \Rightarrow \psi$ attraverso un bagaglio di regole di inferenza piuttosto ristretto. Il nostro scopo è solo quello di orientare lo studente alla comprensione delle dimostrazioni formali che incontrerà spesso nel corso degli studi e di prendere dimestichezza con tali dimostrazioni. Il calcolo che presentiamo ha una forte analogia con il calcolo algebrico che consente di dimostrare semplici identità e disuguaglianze in algebra elementare.

10.3 Dimostrazioni di equivalenze

Come nel caso del calcolo algebrico, la prima regola di inferenza che adottiamo nel calcolo logico è quella che consente di sostituire, in una formula, una sottoformula con una ad essa equivalente. Definiamo prima in modo preciso il concetto di *rimpiazzamento* in una formula.

Rimpiazzamento
Siano P, Q e R formule: allora P_R^Q è la formula ottenuta da P rimpiazzando un'occorrenza della sottoformula R con la formula Q.

Ad esempio:

$(p(x,y) \wedge q(z))_{q(z}^{r(x}$ è la formula $p(x,y) \wedge r(x)$

Il principio di sostituzione per $\equiv$ stabilisce che, se un'equivalenza $Q \equiv R$ fa parte delle premesse, allora possiamo concludere che vale anche l'equivalenza $P \equiv P_R^Q$, dove P è una qualunque formula. Questo principio può essere enunciato nel seguente formato:

$$\boxed{\begin{array}{c}\text{Principio di sostituzione per } \equiv \\ \\ \dfrac{(Q \equiv R) \in \Gamma}{\Gamma \vdash P \equiv P_R^Q}\end{array}}$$

Vediamo un primo esempio di dimostrazione che utilizza il principio di sostituzione. Le premesse che utilizziamo sono, in realtà, *schemi* di premesse: ad esempio, una premessa del tipo

$$(p \vee \neg p) \equiv \mathbf{t}$$

sta per una qualunque formula, detta *istanza* dello schema, ottenuta rimpiazzando tutte le occorrenze del simbolo p con una formula del linguaggio. Per esempio, $((P \wedge Q) \vee \neg(P \wedge Q)) \equiv \mathbf{t}$, oppure $((P \Rightarrow (Q \wedge R)) \vee \neg(P \Rightarrow (Q \wedge R))) \equiv \mathbf{t}$, oppure $((3 > 2) \vee \neg(3 > 2)) \equiv \mathbf{t}$ e così via, sono tutte istanze dello schema precedente. Negli schemi di assioma utilizzeremo le lettere minuscole p, q, r ecc. per indicare generiche formule.

Sia allora Γ il seguente insieme di (schemi di) premesse: ad ogni schema è affiancato il nome che useremo nelle giustificazioni che lo utilizzano.

$$\boxed{\begin{array}{rr}(p \vee (q \wedge r)) \equiv ((p \vee q) \wedge (p \vee r)) & \text{(distributività)} \\ (p \vee \neg p) \equiv \mathbf{t} & \text{(terzo escluso)} \\ (\mathbf{t} \wedge p) \equiv p & \text{(unità)}\end{array}}$$

Dimostriamo l'equivalenza:

$$(p \vee (\neg p \wedge q)) \equiv (p \vee q).$$

Anche in questa formula i simboli p, q stanno per "generiche" formule.

$$\begin{array}{ll} & (p \vee (\neg p \wedge q)) \\ \equiv & \quad \{ \text{ distributività } \} \\ & (p \vee \neg p) \wedge (p \vee q) \\ \equiv & \quad \{ \text{ terzo escluso } \} \\ & \mathbf{t} \wedge (p \vee q) \\ \equiv & \quad \{ \text{ unità } \} \\ & (p \vee q) \end{array}$$

Come nel caso dell'uguaglianza algebrica, anche l'equivalenza logica è transitiva e questo ci permette di concludere che quella precedente è una dimostrazione di $(p \vee (\neg p \wedge q)) \equiv (p \vee q)$ e dunque che tale formula è conseguenza logica delle premesse date.

10.4 Leggi generali e ipotesi

Le premesse utilizzate nell'esempio precedente sono in realtà *leggi generali* che rappresentano formule *valide*: più precisamente, ogni loro istanza è una formula valida, cioè vera in qualunque interpretazione. Da ciò possiamo concludere che anche la formula dimostrata è valida, e cioè vera in qualunque interpretazione. In generale, sia Γ un insieme di formule valide e sia φ una formula dimostrabile a partire da Γ, ovvero $\Gamma \vdash \varphi$. Abbiamo allora:

$\Gamma \vdash \varphi$

per la correttezza di $\vdash$

$\Gamma \models \varphi$

per definizione di $\models$

φ è vera in ogni modello di Γ

ogni interpretazione è modello di Γ

φ è vera in ogni interpretazione

definizione di formula valida

φ è una formula valida.

Dunque una dimostrazione di φ che utilizzi come premesse solo formule valide è una dimostrazione che anche φ è una formula valida: come nel caso del simbolo $\models$, scriveremo semplicemente

$$\vdash \varphi$$

ad indicare che, in realtà, la dimostrazione dipende solo da premesse che sono formule valide.

Vediamo invece un esempio di dimostrazione che utilizza, tra le altre, anche una premessa non valida. Sia Γ il seguente insieme di premesse

$(p \vee p) \equiv p$	(idempotenza)
$(p \vee \neg p) \equiv \mathbf{t}$	(terzo escluso)
$\neg P \equiv Q$	(ipotesi)

Nella terza premessa abbiamo volutamente utilizzato lettere maiuscole, ad indicare che P e Q non stanno per formule arbitrarie, ma per formule particolari. Detto altrimenti, non possiamo liberamente rimpiazzare P e Q con altre formule ed essere sicuri di ottenere una formula vera: si pensi al caso in cui si rimpiazza P con $\mathbf{t}$ e Q con $\mathbf{t}$.

Dimostriamo che da tali premesse si può concludere l'equivalenza:

$$((\neg P \vee Q) \vee \neg Q) \equiv \mathbf{t}$$

$$\begin{array}{ll} & (\neg P \vee Q) \vee \neg Q \\ \equiv & \quad \{ \text{ ipotesi } \} \\ & (Q \vee Q) \vee \neg Q \\ \equiv & \quad \{ \text{ idempotenza } \} \\ & Q \vee \neg Q \\ \equiv & \quad \{ \text{ terzo escluso } \} \\ & \mathbf{t} \end{array}$$

Vediamo cosa possiamo concludere da questa dimostrazione (indicando con φ la conclusione della dimostrazione stessa):

$\Gamma \vdash \varphi$

per la correttezza di $\vdash$

$\Gamma \models \varphi$

per definizione di $\models$

φ è vera in ogni modello di Γ

ogni interpretazione è modello di (idempotenza) e (terzo escluso

φ è vera in ogni modello di (ipotesi)

definizione di conseguenza logica

$\neg P \equiv Q \models \varphi$

Possiamo dunque concludere che, in una dimostrazione, le formule valide possono essere comunque utilizzate come premesse, senza che la conclusione della dimostrazione stessa "dipenda" da esse.

Nel seguito metteremo in luce quanto appena discusso direttamente nelle dimostrazioni, scrivendo una giustificazione come

$$\{\textbf{Ip:} \ldots\}$$

se la giustificazione *non* è costituita da una legge generale. Quindi, ad esempio, l'ultima dimostrazione presentata viene scritta come segue:

$(\neg P \vee Q) \vee \neg Q$
$\equiv$ { **Ip:** $\neg P \equiv Q$ }
$(Q \vee Q) \vee \neg Q$
$\equiv$ { idempotenza }
$Q \vee \neg Q$
$\equiv$ { terzo escluso }
$\mathbf{t}$

In generale, dunque, data una dimostrazione di una formula φ saremo autorizzati a concludere che $\Gamma \vdash \varphi$, dove Γ è l'insieme delle giustificazioni etichettate con **Ip**.

10.5 Leggi generali per l'equivalenza

Presentiamo alcune leggi generali ed il nome che utilizzeremo per esse nelle giustificazioni.

$p \equiv p$	(riflessività)
$(p \equiv q) \equiv (q \equiv p)$	(simmetria)
$(p \vee p) \equiv p$	(idempotenza)
$(p \wedge p) \equiv p$	
$(p \vee \neg p) \equiv \mathbf{t}$	(terzo escluso)
$(p \wedge \neg p) \equiv \mathbf{f}$	(contraddizione)
$(p \wedge q) \equiv (q \wedge p)$	(commutatività)
$(p \vee q) \equiv (q \vee p)$	
$(p \equiv \mathbf{t}) \equiv p$	(unità)
$(p \wedge \mathbf{t}) \equiv p$	
$(p \vee \mathbf{f}) \equiv p$	
$(p \wedge \mathbf{f}) \equiv \mathbf{f}$	(zero)
$(p \vee \mathbf{t}) \equiv \mathbf{t}$	

$((p \vee q) \vee r) \equiv (p \vee (q \vee r))$ $((p \wedge q) \wedge r) \equiv (p \wedge (q \wedge r))$	(associatività)
$(p \wedge (q \vee r)) \equiv ((p \wedge q) \vee (p \wedge r))$ $(p \vee (q \wedge r)) \equiv ((p \vee q) \wedge (p \vee r))$	(distributività)
$\neg\neg p \equiv p$	(doppia negazione)
$\neg(p \wedge q) \equiv (\neg p \vee \neg q)$ $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$	(De Morgan)
$(p \Rightarrow q) \equiv (\neg p \vee q)$	(eliminazione-$\Rightarrow$)
$(p \equiv q) \equiv ((p \Rightarrow q) \wedge (q \Rightarrow p))$ $(p \equiv q) \equiv ((p \wedge q) \vee (\neg p \wedge \neg q))$	(eliminazione-$\equiv$)
$p \Rightarrow (q \Rightarrow r) \equiv (p \wedge q) \Rightarrow r$	(semplificazione-$\Rightarrow$)

10.6 Dimostrazioni di implicazioni

Richiamiamo innanzitutto il significato di un'implicazione. Consideriamo il valore di verità di un'implicazione $\phi \Rightarrow \psi$ in una generica interpretazione: se l'antecedente ϕ è falso in tale interpretazione, l'impicazione è vera, indipendentemente dal valore di verità del conseguente. Se invece ϕ è vera, l'intera implicazione è vera se lo è il conseguente, falsa altrimenti. Dunque, l'unico caso "interessante" nel determinare il valore di verità di un'implicazione è quando l'antecedente è vero.

La dimostrazione di implicazioni del tipo $\phi \Rightarrow \psi$ avviene, nel nostro calcolo, attraverso l'uso di una regola simile al principio di sostituzione dell'equivalenza, che consente di applicare leggi riguardanti l'implicazione a sottoformule di una data formula e di introdurre il connettivo di implicazione nella prima colonna delle dimostrazioni. Ad esempio, una dimostrazione del tipo

$$\begin{array}{ll} & (p \wedge q) \vee r \\ \Rightarrow & \quad \{\ (p \wedge q) \Rightarrow p\ \} \\ & p \vee r \end{array}$$

dove, appunto, è stata applicata la legge $(p \wedge q) \Rightarrow p)$ (che, come vedremo, è una formula valida) alla sottoformula $(p \wedge q)$ della formula iniziale.

Purtroppo, tale principio non si può applicare liberamente come nel caso dell'equivalenza, ma solo con alcune restrizioni. Ad esempio, la seguente dimostrazione

$$\begin{array}{ll} & \neg(p \wedge q) \\ \Rightarrow & \quad \{\ (p \wedge q) \Rightarrow p\ \} \\ & \neg p \end{array}$$

non è lecita! È facile convincersi che la premessa $(p \wedge q) \Rightarrow p$ (pur valida) non giustifica l'implicazione $\neg(p \wedge q) \Rightarrow \neg p$. Ad esempio, se p e q vengono interpretate, rispettivamente, come *tt* e *ff*, l'implicazione $\neg(p \wedge q) \Rightarrow \neg p$ è falsa!
Per capire la ragione di ciò, facciammo appello ancora una volta alle analogie con il calcolo algebrico. Prendiamo come esempio l'espressione algebrica $a + b - c$ e la proposizione $b > d$. Possiamo chiaramente concludere che $(a + b - c) > (a + d - c)$, ovvero costruire il calcolo:

$$\begin{array}{ll} & a + b - c \\ > & \quad \{\ b > d\ \} \\ & a + d - c \end{array}$$

Consideriamo ora la stessa espressione ma la proposizione $c > d$: è facile convincersi che il seguente calcolo

$$
\begin{array}{ll}
 & a+b-c \\
> & \quad \{\ c > d\ \} \\
 & a+b-d
\end{array}
$$

è scorretto. Il punto cruciale è che, mentre nel primo esempio la maggiorazione avviene in un contesto positivo, nel secondo essa avviene in un contesto negativo (più correttamente: la variabile c occorre in posizione negativa in $a+b-c$) e, quando questo accade, la maggiorazione non è più lecita, a meno di non invertire il verso dell'operatore di relazione utilizzato, ottenendo la dimostrazione, questa volta corretta

$$
\begin{array}{ll}
 & a+b-c \\
< & \quad \{\ c > d\ \} \\
 & a+b-d
\end{array}
$$

La stessa situazione si verifica nel calcolo logico, dove il connettivo $\neg$ introduce contesti negativi. Nell'esempio precedente, è corretta la dimostrazione

$$
\begin{array}{ll}
 & \neg(p \wedge q) \\
\Leftarrow & \quad \{\ (p \wedge q) \Rightarrow p\ \} \\
 & \neg p
\end{array}
$$

in cui abbiamo "invertito" il verso dell'implicazione. Per mantenere il verso dell'implicazione, dobbiamo applicare il principio di sostituzione per l'implicazione solo a sottoformule che occorrono in un contesto non negativo. Ad esempio, p occorre positivamente in p, $p \vee q$, $p \wedge q$ e $q \Rightarrow p$, mentre occorre negativamente in $\neg p$ e $p \Rightarrow q$ (si ricordi, infatti, che $(p \Rightarrow q) \equiv (\neg p \vee q)$).

Possiamo allora enunciare il principio di sostituzione per $\Rightarrow$ come segue:

Principio di sostituzione per $\Rightarrow$

$$\frac{(Q \Rightarrow R) \in \Gamma \qquad Q \text{ occorre positivamente in } P}{\Gamma \vdash P \Rightarrow P^R_Q}$$

Principio di sostituzione per $\Rightarrow$

$$\frac{(Q \Rightarrow R) \in \Gamma \qquad Q \text{ occorre negativamente in } P}{\Gamma \vdash P^R_Q \Rightarrow P}$$

Si noti che una stessa sottoformula può occorrere sia positivamente che negativamente in una data formula (ad esempio, la sottoformula P occorre sia positivamente che negativamente in $P \vee \neg P$) e dunque, nell'applicare il principio di sostituzione per $\Rightarrow$, si deve prestare attenzione alla *singola* occorrenza della formula che si sta rimpiazzando. Vediamo alcuni esempi che mettono in luce questo punto.

Corrette		Scorrette	
$(P \vee R) \wedge \neg P$		$(P \vee R) \wedge \neg P$	
$\Rightarrow$ $\{\mathbf{Ip}\text{: } P \Rightarrow Q\}$		$\Leftarrow$ $\{\mathbf{Ip}\text{: } P \Rightarrow Q\}$	
$(Q \vee R) \wedge \neg P$		$(Q \vee R) \wedge \neg P$	
$(P \vee R) \wedge \neg P$		$(P \vee R) \wedge \neg P$	
$\Leftarrow$ $\{\mathbf{Ip}\text{: } P \Rightarrow Q\}$		$\Rightarrow$ $\{\mathbf{Ip}\text{: } P \Rightarrow Q\}$	
$(P \vee R) \wedge \neg Q$		$(P \vee R) \wedge \neg Q$	
		$(P \vee R) \wedge \neg P$	
		$\Rightarrow$ $\{\mathbf{Ip}\text{: } P \Rightarrow Q\}$	
		$(Q \vee R) \wedge \neg Q$	
		$(P \vee R) \wedge \neg P$	
		$\Rightarrow$ $\{\mathbf{Ip}\text{: } P \Rightarrow Q\}$	
		$(Q \vee R) \wedge \neg Q$	

10.7 Teorema di deduzione

Le dimostrazioni di implicazioni possono essere fatte in modo semplice utilizzando un importante risultato che va sotto il nome di *teorema di deduzione*, e che possiamo riformulare con la seguente regola.

Teorema di deduzione
$\Gamma \vdash P \Rightarrow Q$
se e soltanto se
$\Gamma, P \vdash Q$

dove Γ, P indica un insieme di premesse costituito da tutte le premesse in Γ e dalla premessa P. Il teorema di deduzione ci permette, dunque, di affermare che una dimostrazione del tipo

$$\begin{array}{ll} & P \\ \mathit{conn} & \{\ \mathbf{Ip}\text{: } R\ \} \\ & Q \end{array}$$

è anche una dimostrazione di $R \Rightarrow (P\ \mathit{conn}\ Q)$.

Come esempio, mostriamo la dimostrazione della formula

$$P \Rightarrow ((P \wedge Q) \equiv Q)$$

attraverso una dimostrazione del fatto che l'equivalenza $(P \wedge Q) \equiv Q$ segue logicamente da P.

$$\begin{array}{ll} & P \wedge Q \\ \equiv & \quad \{\ \mathbf{Ip}\text{: } P\ \} \\ & \mathbf{t} \wedge Q \\ \equiv & \quad \{\ \text{unità}\ \} \\ & Q \end{array}$$

Si noti che, nel primo passo di dimostrazione, abbiamo rimpiazzato P con $\mathbf{t}$ grazie all'ipotesi P (ovvero $P \equiv \mathbf{t}$).

10.8 Leggi generali per l'implicazione

Presentiamo alcune leggi generali che riguardano l'implicazione.

$$((p \equiv q) \wedge (q \equiv r)) \Rightarrow (p \equiv r) \qquad \text{(transitività)}$$
$$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$$

$$(p \wedge (p \Rightarrow q)) \Rightarrow q \qquad \text{(modus ponens)}$$

$$p \wedge q \Rightarrow q \qquad \text{(semplificazione-}\wedge\text{)}$$

$$p \Rightarrow p \vee q \qquad \text{(introduzione-}\vee\text{)}$$

$$(p \vee q) \wedge (\neg p \vee r) \Rightarrow (q \vee r) \qquad \text{(risoluzione)}$$

$$((p \Rightarrow q) \wedge (p \Rightarrow r)) \Rightarrow (p \Rightarrow q \wedge r)$$

$$(p \vee q \Rightarrow r) \Rightarrow ((p \Rightarrow r) \vee (q \Rightarrow r))$$

10.9 Leggi per i quantificatori

Le dimostrazioni di formule che coinvolgono quantificatori richiedono spesso leggi particolari che riflettono l'intuizione sul significato dei quantificatori stessi. Una semplice legge è quella che corrisponde alla regola 1 vista nell'introduzione a queste note. Nel nostro calcolo questa regola si riflette nella seguente legge:

$$(\forall x.P) \Rightarrow P[^{t}/_{x}] \qquad \text{(eliminazione-}\forall\text{)}$$

dove t è un termine e $P[^{t}/_{x}]$ indica la formula ottenuta da P rimpiazzando con t tutte le occorrenze della variabile x in P "legate" dal quantificatore universale. Ad esempio

$$\begin{array}{ll} & (\forall x.pari(x) \wedge x > 2 \Rightarrow \neg primo(x)) \\ \Rightarrow & \quad \{ \text{ elim.-}\forall \text{ } \} \\ & pari(4) \wedge 4 > 2 \Rightarrow \neg primo(4) \end{array}$$

e

$$\begin{array}{ll} & (\forall x.pari(x) \wedge x > 2 \Rightarrow \neg primo(x)) \\ \Rightarrow & \quad \{ \text{ elim.-}\forall \text{ } \} \\ & pari(3) \wedge 3 > 2 \Rightarrow \neg primo(3) \end{array}$$

sono dimostrazioni corrette che utilizzano la legge appena introdotta.

Per il quantificatore esistenziale, una legge intuitiva che ne riflette il significato è la seguente:

$$P[^{t}/_{x}] \Rightarrow (\exists x.P) \qquad \text{(introduzione-}\exists\text{)}$$

Intuitivamente, tale legge consente di dedurre l'esistenza di un elemento del dominio che soddisfa una proprietà, a partire dal fatto che tale proprietà vale su un particolare elemento. Ad esempio:

$$\begin{array}{ll} & pari(4) \wedge 4 > 2 \\ \Rightarrow & \quad \{ \text{ intro.-}\exists \text{ } \} \\ & (\exists x.pari(x) \wedge x > 2) \end{array}$$

Si noti che, come intuizione vuole, la legge (eliminazione-$\forall$) ci consente anche di utilizzare, come giustificazione di un passo di dimostrazione, una qualsivoglia istanza di una premessa del tipo $(\forall x.P)$ ottenuta rimpiazzando x con un termine. Ad esempio, la seguente è una dimostrazione corretta di $(\forall x.P(x)) \vdash (Q(a) \Rightarrow P(a))$.

$$
\begin{array}{ll}
 & Q(a) \Rightarrow P(a) \\
\equiv & \quad \{ \textbf{Ip: } P(a) \} \\
 & Q(a) \Rightarrow \mathbf{t} \\
\equiv & \quad \{ \text{elim.-}\Rightarrow \} \\
 & \neg Q(a) \vee \mathbf{t} \\
\equiv & \quad \{ \text{zero} \} \\
 & \mathbf{t}
\end{array}
$$

Altre leggi utili che coinvolgono formule quantificate sono le seguenti.

$$
\begin{array}{lr}
\neg(\exists x.P) \equiv (\forall x.\neg P) & \text{(De Morgan)} \\
\neg(\forall x.P) \equiv (\exists x.\neg P) & \\
 & \\
(\forall x.(\forall y.P)) \equiv (\forall y.(\forall x.P)) & \text{(annidamento)} \\
(\exists x.(\exists y.P)) \equiv (\exists y.(\exists x.P)) &
\end{array}
$$

$$
\begin{array}{lr}
(\forall x.P \wedge Q) \equiv (\forall x.P) \wedge (\forall x.Q) & (\forall : \wedge) \\
(\exists x.P \vee Q) \equiv (\exists x.P) \vee (\exists x.Q) & (\exists : \vee) \\
 & \\
(\forall x.P) \equiv P \qquad \text{se } x \text{ non occorre in } P & \text{(costante)} \\
(\exists x.P) \equiv P \qquad \text{se } x \text{ non occorre in } P & \\
 & \\
(\exists x.P \wedge Q) \Rightarrow ((\exists x.P) \wedge (\exists x.Q)) & \\
((\forall x.P) \vee (\forall x.Q)) \Rightarrow (\forall x.P \vee Q) & \\
 & \\
(\forall x.P) \Rightarrow (\forall x.P \vee Q) & \\
(\exists x.P) \Rightarrow (\exists x.P \vee Q) & \\
 & \\
(\forall x.P \wedge Q) \Rightarrow (\forall x.P) & \\
(\exists x.P \wedge Q) \Rightarrow (\exists x.P) &
\end{array}
$$

Il predicato di uguaglianza

Molto spesso le formule che si utilizzano coinvolgono il predicato di uguaglianza $=$. Di norma, in una qualunque interpretazione una formula del tipo $t = t'$, dove t e t' sono termini del linguaggio, è vera se e soltanto se t e t' denotano lo stesso oggetto del dominio di interesse. Dal momento che questa sarà sempre la nostra interpretazione del predicato $=$, diamo nel seguito due leggi utili che riguardano il comportamento di formule logiche rispetto all'uguaglianza.

$$x = y \Rightarrow (P \equiv P_x^y) \qquad \text{(Leibniz)}$$
$$(x = y \wedge P) \equiv (x = y \wedge P_x^y)$$
$$(x = y \wedge P) \Rightarrow P_x^y$$

$$(\forall x.x = y \Rightarrow P) \equiv P_x^y \qquad \text{(singoletto)}$$
$$(\exists x.x = y \wedge P) \equiv P_x^y$$

Le due leggi (Leibniz) corrispondono all'intuizione che, sapendo che due oggetti x e y sono in realtà lo stesso oggetto, asserire P in funzione di x è la stessa cosa che asserire P in funzione di y.

Ad esempio, nel dominio dei numeri naturali, $pari(15)$ e $pari(12 + 3)$ sono formule equivalenti (entrambe false, se *pari* è interpretato nel modo usuale). Infatti:

$pari(15)$
$\equiv$ { $15 = 12 + 3$, (Leibniz }
$pari(12 + 3)$

10.10 La regola della generalizzazione

Oltre alle precedenti leggi, per costruire dimostrazioni che coinvolgono formule quantificate, è possibile utilizzare la seguente regola di inferenza. Per dimostrare una formula del tipo $(\forall x.P)$ è possibile rimpiazzare la variabile quantificata x con un *nuovo* simbolo di costante, sia esso d, e dimostrare $P[^d/_x]$. Se tale dimostrazione ha successo, si può *generalizzare* la dimostrazione alla formula originaria $(\forall x.P)$. Intuitivamente, il ruolo della nuova costante è quello di rappresentare un *generico* elemento del dominio, sul quale non è possibile fare alcuna assunzione.

Generalizzazione Universale

$$\frac{\Gamma \vdash P[^d/_x], \text{ con } d \text{ nuova costante}}{\Gamma \vdash (\forall x.P)}$$

Vediamo alcuni esempi. Siano p e q predicati ad un argomento e sia Γ il seguente insieme di premesse:

$$(\forall x.p(x) \Rightarrow q(x)) \qquad (\forall x.p(x))$$

Vogliamo dimostrare che $(\forall x.q(x))$ è conseguenza logica di Γ: lo facciamo, per generalizzazione universale, dimostrando $\Gamma \vdash q(d)$, con d nuova costante.

$(\forall x.p(x) \Rightarrow q(x) \wedge (\forall x.p(x))$
$\Rightarrow$ { elim.-$\forall$), d nuova costante }
$(p(d) \Rightarrow q(d)) \wedge p(d)$
$\Rightarrow$ { modus ponens }
$q(d)$

Un'altra dimostrazione, più concisa, è la seguente:

$p(d)$
$\Rightarrow$ { **Ip:** $p(d) \Rightarrow q(d)$ }
$q(d)$

Come esempio più complesso, mostriamo che dall'insieme di premesse *Ins* del paragrafo 8.2 segue logicamente

$$(\forall A, B.A \cup B = B \cup A).$$

Dimostriamo $Ins \vdash C \cup D = D \cup C$, con C, D nuove costanti.

$C \cup D = D \cup C$

$\equiv$ { istanza di (uguaglianza), con d nuova costante }

$d \in C \cup D \equiv d \in D \cup C$

$\equiv$ { unione }

$(d \in C \vee d \in D) \equiv (d \in D \vee d \in C)$

$\equiv$ { commutatività }

$(d \in C \vee d \in D) \equiv (d \in C \vee d \in D)$

$\equiv$ { riflessività }

t

Vediamo infine la dimostrazione di un'altra ben nota proprietà delle operazioni su insiemi:

$$(\forall A, B, C.A \cup (B \cap C) = (A \cup B) \cap (A \cup C))$$

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$\equiv$ { uguaglianza }

$d \in A \cup (B \cap C) \equiv d \in (A \cup B) \cap (A \cup C)$

$\equiv$ { unione), (intersezione }

$(d \in A \vee d \in B \cap C) \equiv d \in (A \cup B) \wedge d \in (A \cup C)$

$\equiv$ { unione), (intersezione }

$(d \in A \vee (d \in B \wedge d \in C)) \equiv ((d \in A \vee d \in B) \wedge (d \in A \vee d \in C))$

$\equiv$ { distributività }

$(d \in A \vee (d \in B \wedge d \in C)) \equiv (d \in A \vee (d \in B \wedge d \in C))$

$\equiv$ { riflessività }

t