

## CAPITOLO 8

[indice](#)

## GENERARE I TEOREMI DI TEORIE SEMPLICI

**1. Come costruire un sistema inferenziale corretto**

Sia  $T$  una teoria, cioè un qualunque insieme di formule, ed  $\alpha$  una formula, allora ricordiamo che si dice che  $\alpha$  è una *conseguenza logica* di  $T$ , in breve  $T \vDash \alpha$ , quando ogni modello di  $T$  verifica  $\alpha$ . Ad esempio se  $T$  è la teoria dei gruppi allora  $T \vDash \alpha$  significa che  $\alpha$  è una proprietà che è verificata da tutti i gruppi. Ora se ci poniamo il problema di stabilire effettivamente se  $\alpha$  è una conseguenza logica di  $T$  il procedimento suggerito da tale definizione sembra alquanto difficile da applicare. Infatti dovremmo:

1. prendere tutte le possibili interpretazioni del dato linguaggio
2. considerare solo quelle che sono modelli della teoria  $T$
3. verificare che ciascuno di tali modelli verifichi la formula  $\alpha$ .

E' evidente che una tale impresa risulta impossibile anche perché la classe delle possibili interpretazioni di un linguaggio ha una grandezza che va oltre le capacità umane. Allora è necessario trovare un'altra via e chiedersi se:

*esiste un metodo effettivo capace di stabilire, data una teoria  $T$  ed una formula  $\alpha$ , se  $\alpha$  è una conseguenza logica di  $T$  ?<sup>1</sup>*

Ora esistono strumenti adatti ad un tale scopo che sono utilizzati dagli uomini da tempi immemorabili: sono le dimostrazioni ! Esaminiamo pertanto che cosa è una dimostrazione.

Un matematico quando effettua una dimostrazione di un teorema  $\alpha$  a partire da un sistema di assiomi  $T$  di fatto scrive una sequenza finita  $\alpha_1, \alpha_2, \dots, \alpha_n$  di asserzioni di cui l'ultima è del tipo "pertanto possiamo concludere  $\alpha$ ". Inoltre un matematico "giustifica" implicitamente o esplicitamente ogni asserzione in qualche modo. Ecco un elenco di giustificazioni che vengono di solito date:

- *perché è una assioma della teoria  $T$  ...*

(ad esempio quando faccio affermazioni del tipo "per la proprietà associativa . . .")

- *perché è logicamente vero che ...*

(ad esempio quando affermo "d'altra parte un numero o è pari o non è pari ...")

- *perché segue dalle asserzioni già provate ...*

(ad esempio quando affermo "poiché abbiamo provato che l'ultima cifra di  $n$  è 4 ed abbiamo provato che terminare per 4 implica essere pari allora possiamo asserire che  $n$  è pari).

Quest' ultimo caso corrisponde alla nozione di *regola di inferenza* vista come procedimento con cui da alcune asserzioni se ne ricava un'altra. Tra le regole più antiche e più usate è il "modus ponens", cioè la regola per cui se, a partire dall'insieme di assiomi  $T$ ,

- ho dimostrato la formula  $\alpha \rightarrow \beta$

- ed ho dimostrato  $\alpha$

- allora posso affermare anche  $\beta$ .

Possiamo indicare in breve tale regola al modo seguente:

<sup>1</sup> Non si deve confondere tale domanda con le seguenti, apparentemente simili, domande.

1. Esiste un metodo capace, per ogni teoria  $T$ , di generare effettivamente tutte le conseguenze logiche di  $T$  ?
2. Fissata una struttura del primo ordine e detto  $T$  l'insieme di tutte le asserzioni vere in tale struttura, esiste un metodo per verificare se una formula  $\alpha$  è una conseguenza logiche di  $T$  ?
3. Fissata una struttura e detto  $T$  l'insieme di tutte le asserzioni vere in tale struttura, esiste un metodo per generare tutte le conseguenze logiche di  $T$  ?

$$\frac{\alpha; \alpha \rightarrow \beta}{\beta} \quad (\text{Modus Ponens})$$

Da notare che tale regola è “corretta” nel senso che se le due premesse sono vere in una data interpretazione allora anche il conseguente è vero in tale interpretazione. Un altro esempio di regola corretta è quella che permette di affermare  $\alpha \wedge \beta$  se si sono già dimostrate le formule  $\alpha$  e  $\beta$ . Questa regola prende il nome di “introduzione di  $\wedge$ ”.

$$\frac{\alpha; \beta}{\alpha \wedge \beta} \quad (\text{regola della } \wedge\text{-introduzione})$$

Esistono anche regole relative ai quantificatori.

$$\frac{\alpha}{\forall x(\alpha)} \quad (\text{regola di } \forall\text{-introduzione}) \quad \frac{\forall x(\alpha)}{\alpha(t)} \quad (\text{regola di } \forall\text{-eliminazione})$$

dove  $t$  è un termine chiuso. Queste due regole vengono anche chiamate *generalizzazione* e *particolarizzazione*. Più in generale possiamo dare la seguente definizione.

**Definizione 1.1.** Chiamo *regola di inferenza* una qualunque funzione parziale  $m$ -aria  $r(x_1, \dots, x_m)$  che associa ad ogni  $m$ -pla di formule  $\alpha_1, \dots, \alpha_m$  in cui è definita (le premesse) una formula  $\alpha = r(\alpha_1, \dots, \alpha_m)$  (la conclusione). Diciamo che la regola è *corretta* se, presa una qualunque interpretazione  $I$ , se  $\alpha_1, \dots, \alpha_m$  sono vere in  $I$  allora anche  $\alpha$  è vera in  $I$ .

Naturalmente la scelta delle regole di inferenza corrette è molto ampia e nei diversi approcci alla deduzione vengono proposte regole diverse. Per quanto riguarda le giustificazioni del tipo “è logicamente vero” vuol dire che si ha a disposizione un insieme  $Al$  di formule logicamente vere da cui si può attingere.

**Definizione 1.2.** Un *apparato inferenziale* è definito da un insieme di regole di inferenza e da un insieme  $Al$  di formule dette *assiomi logici*. Sia  $T$  una teoria ed  $\alpha$  una formula. Chiameremo *dimostrazione di  $\alpha$  sotto ipotesi  $T$*  una successione finita di formule  $\alpha_1, \dots, \alpha_n$  con  $\alpha_n = \alpha$  tale che ogni  $\alpha_i$  verifichi almeno una delle seguenti condizioni:

- $\alpha_i$  è un assioma logico, cioè  $\alpha_i \in Al$
- $\alpha_i$  è una ipotesi, cioè  $\alpha_i \in T$
- $\alpha_i$  è stata ottenuta da formule precedenti (cioè con indice minore di  $i$ ) tramite una regola di inferenza.

**Definizione 1.3.** Diremo che  $\alpha$  è *dimostrabile in  $T$* , e scriveremo  $T \vdash \alpha$  se esiste una dimostrazione di  $\alpha$  sotto ipotesi  $T$ . Diremo che  $\alpha$  è *confutabile in  $T$*  se  $T \vdash \neg \alpha$ .

**Esempi.** Assumiamo come regole di inferenza GEN ed MP e come assiomi logici tutte le formule che hanno una delle seguenti tre forme

$$(\alpha \wedge \neg \beta) \rightarrow \neg \beta, \quad (\alpha \wedge \neg \beta) \rightarrow \alpha, \quad (\forall x \alpha(x)) \rightarrow \alpha(t).$$

Sia  $X = \{ \alpha \wedge \neg \beta, \alpha \rightarrow \beta \}$  allora un esempio di dimostrazione di  $\neg \beta$  sotto ipotesi  $X$  è costituita dalla successione

1.  $(\alpha \wedge \neg \beta) \rightarrow \neg \beta$  (perché un assioma logico)
2.  $\alpha \wedge \neg \beta$  (per ipotesi)
3.  $\neg \beta$  (per modus ponens da 1. e 2.)

Una dimostrazione di  $\beta$  è costituita dalla successione

1.  $(\alpha \wedge \neg \beta) \rightarrow \alpha$  (perché un assioma logico)
2.  $\alpha \wedge \neg \beta$  (per ipotesi)
3.  $\alpha$  (per modus ponens da 1. e 2)
4.  $\alpha \rightarrow \beta$  (per ipotesi)
5.  $\beta$  (per modus ponens da 3. e 4.)

**Esempio.** Sia  $X = \{y > 0 \rightarrow (x > 0 \rightarrow x + y > 0), 5 > 0, 7 > 0\}$  allora una dimostrazione della formula  $5 + 7 > 0$  sotto ipotesi  $X$  è costituita dalla successione

- $y > 0 \rightarrow (x > 0 \rightarrow x + y > 0)$  (per ipotesi)
- $\forall y (y > 0 \rightarrow (x > 0 \rightarrow x + y > 0))$  (per la regola di generalizzazione)
- $7 > 0 \rightarrow (x > 0 \rightarrow x + 7 > 0)$  (perché è un assioma logico del tipo  $(\forall x \alpha(x)) \rightarrow \alpha(t)$ )
- $\forall x (7 > 0 \rightarrow (x > 0 \rightarrow x + 7 > 0))$  (per la regola di generalizzazione)
- $7 > 0 \rightarrow (5 > 0 \rightarrow 5 + 7 > 0)$  (perché è un assioma logico del tipo  $(\forall x \alpha(x)) \rightarrow \alpha(t)$ )
- $7 > 0$  (per ipotesi)
- $5 > 0 \rightarrow 5 + 7 > 0$  (per modus ponens)
- $5 > 0$  (per ipotesi)
- $5 + 7 > 0$  (per modus ponens).

Avendo definito la nozione di dimostrazione e la conseguente relazione  $\vdash$ , da un buon apparato inferenziale ci si aspetta che valga l'equivalenza

$$T \vdash \alpha \Leftrightarrow T \vDash \alpha.$$

Se non valesse tale equivalenza dovremmo aspettarci ad esempio che pur avendo dimostrato in teoria dei gruppi una asserzione  $\alpha$ , non è detto che tale asserzione valga in tutti i gruppi. Oppure dovremmo aspettarci che pur essendoci una asserzione  $\alpha$  che vale in tutti i gruppi, potrebbe darsi che non esista una dimostrazione di tale asserzione. Questo sarebbe un fortissimo limite alle capacità razionali dell'essere umano. Un primo passo rispetto a tale questione si ottiene supponendo che le regole di inferenza siano corrette e gli assiomi formule logicamente vere.

**Teorema 1.4.** (Correttezza del sistema inferenziale). Consideriamo un sistema inferenziale le cui regole di inferenza siano corrette ed i cui assiomi logici siano formule logicamente vere. Allora se  $T$  è una teoria ed  $\alpha$  una formula, risulta che

$$T \vdash \alpha \Rightarrow T \vDash \alpha.$$

*Dim.* Se  $\alpha$  fosse un assioma logico il teorema sarebbe ovvio poiché gli assiomi logici sono formule logicamente vere. Supponiamo quindi che  $\alpha$  non sia un assioma logico: dobbiamo provare che se  $\pi$  è una dimostrazione di  $\alpha$  sotto ipotesi  $T$  allora  $T \vDash \alpha$ . Procederemo per induzione sulla lunghezza  $n$  di  $\pi$ . Se  $n = 1$ , allora  $\alpha \in T$  ed è evidente che  $T \vDash \alpha$ . Supponiamo che il teorema sia vero per tutti i numeri minori di  $n$  e proviamolo per  $n$ . Se  $\alpha$  è ottenuto per modus ponens da  $\beta \rightarrow \alpha$  e  $\beta$ , allora per ipotesi di induzione risulta  $T \vDash \beta \rightarrow \alpha$  e  $T \vDash \beta$  è ciò comporta che  $T \vDash \alpha$ . Se  $\alpha$  è ottenuto per generalizzazione si procede in modo analogo.  $\square$

Un po' più complicato è trovare un sistema inferenziale per cui valga anche l'implicazione inversa. Rimandiamo la questione e ci occupiamo per il momento di apparati inferenziali che funzionino per teorie molto semplici.

## 2. Teorie con solo regole e fatti: la programmazione logica

Ricordiamo che un *letterale* è una formula atomica (*letterale positivo*) oppure la negata di una formula atomica (*letterale negativo*) e che una *matrice* è una formula priva di quantificatori. Inoltre viene chiamata

- *clausola* ogni formula che sia disgiunzione di letterali;
- *clausola di programma* ogni clausola con almeno un letterale positivo
- *clausola positiva di programma* ogni clausola con esattamente un letterale positivo.
- *fatto* ogni formula atomica chiusa
- *regola* una clausola di programma che non sia un fatto.

**Esempi.** La formula

- $\neg(x \leq y) \vee \neg(y \leq z) \vee (x \leq z)$  è una clausola positiva,
- $\forall x(x \cdot x^{-1} = 1)$  è una clausola positiva;
- $1+1=2$  è un fatto (e quindi una clausola positiva)
- $\neg(2+2=5)$  è un letterale ma non è un fatto (che non è una clausola positiva)
- $\neg(x \leq y) \vee (x \leq y+1) \vee (x \leq y+2)$  è una clausola ma non è una clausola positiva.

La dimostrazione della seguente proposizione è evidente.

**Proposizione 2.1.** Ogni clausola di programma è equivalente ad una formula atomica oppure ad una formula del tipo

$$\alpha_1 \wedge \dots \wedge \alpha_h \wedge \neg \beta_1 \wedge \dots \wedge \neg \beta_k \rightarrow \alpha$$

con  $\alpha_1, \dots, \alpha_h$  e  $\beta_1, \dots, \beta_k$  formule atomiche. Ogni clausola positiva di programma è equivalente ad una formula atomica oppure ad una formula del tipo

$$\alpha_1 \wedge \dots \wedge \alpha_h \rightarrow \beta$$

con  $\alpha_1, \dots, \alpha_h$  e  $\beta$  formule atomiche. Le clausole che non sono clausole di programma sono equivalenti a formule del tipo  $\neg(\alpha_1 \wedge \dots \wedge \alpha_n)$ .

Noi studieremo un particolare tipo di teorie, i programmi (programmi positivi), che sono caratterizzate dall'aver come assiomi solo clausole di programma (clausole positive di programma).

**Definizione 2.2.** Una teoria prende il nome di *programma* se è costituita solo da clausole di programma. Una teoria è chiamata *programma positivo*, se è costituita solo da clausole positive di programma.

Il nome "programma" deriva dal fatto che nel linguaggio di programmazione *Prolog* i programmi degli usuali linguaggi procedurali sono sostituiti da sistemi di assiomi che sono clausole di programma.

**Esempio.** Il seguente sistema di assiomi per l'equivalenza

$$x \equiv x \quad ; \quad (x \equiv y) \rightarrow (y \equiv x) \quad ; \quad (x \equiv z) \wedge (z \equiv y) \rightarrow (x \equiv y)$$

definisce una teoria che è un programma positivo.

**Esempio.** Nel linguaggio dell'ordinamento le formule

$$\neg(x < x) \ ; \ (x < y) \wedge (y < z) \rightarrow (x < z)$$

definiscono la teoria dell'ordinamento stretto che non è un programma in quanto la formula  $\neg(x < x)$  non è una clausola di programma. La teoria dell'ordinamento (non stretto) è espressa dalle seguenti formule

$$x \leq x \quad ; \quad (x \leq y) \wedge (y \leq x) \rightarrow (x = y) \quad ; \quad (x \leq y) \wedge (y \leq z) \rightarrow (x \leq z)$$

(a cui vanno aggiunti gli assiomi per l'identità) ed è pertanto un programma positivo.

Il seguente teorema mostra l'importanza della nozione di programma.

**Teorema 2.3.** Ogni matrice è logicamente equivalente a una congiunzione di clausole. Ne segue che:

- ogni teoria universale è equivalente a un sistema di clausole
- ogni teoria è riducibile a un sistema di clausole.

*Dim.* La prima parte del teorema segue dal fatto che nel capitolo riguardante il calcolo proposizionale abbiamo mostrato che ogni formula si può ridurre a forma normale congiuntiva e quindi a congiunzione di clausole. Lo stesso teorema vale anche nel calcolo dei predicati purché al posto delle variabili proposizionali si considerino le formule atomiche. Pertanto possiamo affermare che ogni matrice è logicamente equivalente ad una congiunzione di clausole. Consideriamo una teoria universale  $T$  e sia  $\forall x_1 \dots x_p (\alpha)$  un suo assioma dove  $\alpha$  è una matrice. Se riduciamo  $\alpha$  a congiunzione di clausole  $\alpha_1 \wedge \dots \wedge \alpha_n$ , la nostra formula sarà equivalente alla formula  $\forall x_1 \dots x_p (\alpha_1 \wedge \dots \wedge \alpha_n)$ . D'altra parte per le leggi distributive dei quantificatori (Proposizione 5.8 del Capitolo 5) risulta che una tale formula è equivalente ad una formula del tipo  $(\forall x_1 \dots \forall x_p \alpha_1) \wedge \dots \wedge (\forall x_1 \dots \forall x_p \alpha_n)$  e quindi all'insieme

$$\{\forall x_1 \dots \forall x_p \alpha_1, \dots, \forall x_1 \dots \forall x_p \alpha_n\}$$

di formule. In conclusione, poiché quando si assume un sistema di assiomi si suppone sempre la quantificazione universale, la teoria  $T$  è equivalente alla teoria che si ottiene sostituendo ogni formula  $\forall x_1 \dots x_p (\alpha)$  con l'insieme  $\{\alpha_1, \dots, \alpha_n\}$  di clausole.

Consideriamo una qualunque teoria  $T$ , allora tramite la skolemizzazione tale teoria risulta riducibile ad una teoria universale (in una opportuna estensione del linguaggio) e questa teoria universale è equivalente ad un sistema di clausole.  $\square$

**Nota.** Non è difficile provare che una formula del tipo  $\alpha_1 \vee \dots \vee \alpha_n \rightarrow \alpha$  è equivalente a  $(\alpha_1 \rightarrow \alpha) \wedge \dots \wedge (\alpha_n \rightarrow \alpha)$ . Pertanto possono essere considerate programmi anche le teorie che contengono, oltre a clausole di programmi, formule del tipo  $\alpha_1 \vee \dots \vee \alpha_n \rightarrow \alpha$  con  $\alpha_i$  congiunzione di atomiche ed  $\alpha$  atomica.

### 3. Un sistema inferenziale per i programmi logici

Se ci si limita alle teorie che sono programmi positivi allora è possibile utilizzare un sistema inferenziale particolarmente semplice. Tale sistema non ha assiomi logici ed utilizza solo la regola di  $\wedge$ -introduzione, quella di particolarizzazione ed  $MP$ . La regola di  $\wedge$ -introduzione la utilizziamo nella forma più generale:

$$\frac{\alpha_1, \dots, \alpha_n}{\alpha_1 \wedge \dots \wedge \alpha_n} \quad (\text{regola della } \wedge\text{-introduzione})$$

Per tale sistema inferenziale esiste un metodo piuttosto semplice ed elegante per produrre teoremi. Per esporlo indichiamo con

- $Fatt(P)$  l'insieme dei fatti che appartengono a  $P$  o che si ottengono dalle regole atomiche di  $P$  per particolarizzazione sostituendo al posto delle variabili libere termini chiusi;
- $Reg(P)$  l'insieme delle clausole chiuse che si ottengono dalle regole non atomiche di  $P$  sostituendo anche in questo caso le variabili con termini chiusi.

Ad esempio se  $P$  consiste nelle clausole

$$\begin{aligned} &r(a,b). \\ &r(b,c). \\ &r(X,X). \\ &r(X,Y) \rightarrow r(Y,X) \end{aligned}$$

allora

$$\begin{aligned} Fatt(P) &= \{r(a,b), r(b,c), r(a,a), r(b,b), r(c,c)\} \\ Reg(P) &= \{r(a,a) \rightarrow r(a,a), r(a,b) \rightarrow r(b,a), r(a,c) \rightarrow r(c,a), \\ &\quad r(b,a) \rightarrow r(a,b), r(b,b) \rightarrow r(b,b), r(b,c) \rightarrow r(c,b) \\ &\quad r(c,a) \rightarrow r(a,c), r(c,b) \rightarrow r(b,c), r(c,c) \rightarrow r(c,c)\}. \end{aligned}$$

L'insieme dei fatti che si possono dimostrare a partire da un programma positivo può essere ottenuto al modo seguente.

**Definizione 3.1.** Dato un programma positivo  $P$ , definiamo l'operatore  $T : P(B_{\mathcal{L}}) \rightarrow P(B_{\mathcal{L}})$  ponendo, per ogni sottoinsieme  $X$  di  $B_{\mathcal{L}}$

$$T(X) = X \cup Fatt(P) \cup \{ \alpha \mid \alpha_1 \wedge \dots \wedge \alpha_n \rightarrow \alpha \in Reg(P), \alpha_1 \in X, \dots, \alpha_n \in X \}. \quad (3.1)$$

Il significato dell'operatore  $T$  è che se ad un certo passo del processo inferenziale è stato dimostrato un insieme  $X$  di fatti al passo successivo è possibile dimostrare l'insieme  $T(X)$  di fatti.

**Teorema 3.2.** L'operatore  $T$  è algebrico. Detto  $X$  un sottoinsieme di  $B_{\mathcal{L}}$ , indichiamo con  $D(X)$  il minimo punto fisso di  $T$  contenente  $X$ . Allora risulta che

$$P \vdash \alpha \Leftrightarrow \exists n \alpha \in T^n(\emptyset).$$

e quindi

$$\{ \alpha \in B_{\mathcal{L}} : P \vdash \alpha \} \Leftrightarrow \alpha \in D(\emptyset).$$

*Dim.* Per provare che  $T$  è algebrico dobbiamo provare che se  $\alpha \in T(X)$  allora esiste  $F$  finito tale che  $F \subseteq X$  e  $\alpha \in T(F)$ . Ora nel caso  $\alpha \in X$  abbiamo che  $\alpha \in T(\{\alpha\})$ , nel caso  $\alpha \in Fatt(P)$ ,  $\alpha \in T(\emptyset)$ , nel caso che  $\alpha \in T(X)$  perché esiste  $\alpha_1 \wedge \dots \wedge \alpha_n \rightarrow \alpha \in Reg(P)$  tale che  $\alpha_1 \in X, \dots, \alpha_n \in X$ , allora  $\alpha \in T(\{\alpha_1, \dots, \alpha_n\})$ .

Per provare l'equivalenza, cominciamo a provare, per induzione su  $n$ , che

$$\alpha \in T^n(\emptyset) \Rightarrow \text{esiste una dimostrazione } \pi \text{ di } \alpha \text{ con ipotesi in } P.$$

Per  $n = 0$  abbiamo che  $T^0(\emptyset) = Fatt(P)$  e quindi è evidente che  $P \vdash \alpha$ . Supponiamo l'implicazione vera per  $n$  e che  $\alpha \in T^{n+1}(X) = T(T^n(X))$ . Allora per la definizione di  $T$  sono possibili i seguenti casi.

- $\alpha \in T^n(X)$ , allora l'esistenza di  $\pi$  è assicurata dall'ipotesi di induzione
- esistono  $\alpha_1 \in T^n(X), \dots, \alpha_m \in T^n(X)$  con  $\alpha_1 \wedge \dots \wedge \alpha_m \rightarrow \alpha \in Reg(P)$ . In tale caso per ipotesi di induzione esistono dimostrazioni  $\pi_1, \dots, \pi_m$  di  $\alpha_1, \dots, \alpha_m$ . E' evidente che, con ovvio significato dei simboli la successione di formule

$$\begin{array}{l} \pi_1 \\ \cdot \\ \cdot \\ \cdot \\ \pi_m \\ \alpha_1 \wedge \dots \wedge \alpha_m \quad (\wedge\text{-introduzione}) \\ \gamma_1 \wedge \dots \wedge \gamma_m \rightarrow \gamma \quad (\text{regola in } P \text{ di cui } \alpha_1 \wedge \dots \wedge \alpha_m \rightarrow \alpha \text{ è una particolarezzazione,}) \\ \alpha_1 \wedge \dots \wedge \alpha_m \rightarrow \alpha \quad (\text{per particolarezzazione}) \\ \alpha \quad (\text{per MP}) \end{array}$$

otteniamo una dimostrazione  $\pi$  di  $\alpha$ .

In maniera analoga si prova per induzione su  $n$  che

$$\text{esiste una dimostrazione } \pi \text{ di } \alpha \text{ di lunghezza } n \Rightarrow \alpha \in D(X). \quad \square$$

**Esempio.** Sia  $P = \{r(a,b), r(c,d), r(x,y) \rightarrow s(x,y), r(y,x) \rightarrow s(x,y)\}$ , allora  $U(\mathcal{L}) = \{a,b,c,d\}$ .

Inoltre,

$$T(\emptyset) = \text{Fatt}(P) = \{r(a,b), r(c,d)\};$$

$$T_2(\emptyset) = \{r(a,b), r(c,d)\} \cup \{s(a,b), s(c,d), s(b,a), s(d,c)\};$$

$$T^3(\emptyset) = T_2(\emptyset).$$

Pertanto  $T_2(\emptyset) = \{r(a,b), r(c,d)\} \cup \{s(a,b), s(c,d), s(b,a), s(d,c)\}$  è l'insieme dei fatti che si possono provare a partire dal programma  $P$ .

**Problema.** Aggiungere al programma precedente la formula  $r(x,x)$  (oppure la formula  $s(x,x)$ ) e calcolare l'insieme dei fatti dimostrabili in tale nuovo programma.

**Esempio.** Supponiamo di avere un linguaggio  $\mathcal{L}$  con costanti  $a,b,c,d$  ed una relazione binaria "eq". Inoltre sia  $P$  la teoria dell'equivalenza, cioè la teoria i cui assiomi sono:

$$eq(x,x) \quad ; \quad eq(x,y) \rightarrow eq(y,x) \quad ; \quad eq(x,z) \wedge eq(z,y) \rightarrow eq(x,y).$$

Tale teoria è un programma positivo e risulta

$$T(\emptyset) = \{eq(a,a), eq(b,b), eq(c,c), eq(d,d)\}; \quad T^2(\emptyset) = T(\emptyset),$$

pertanto  $T(\emptyset)$  è direttamente l'insieme dei fatti provabili.

**Problema.** Aggiungere al programma dell'esempio precedente gli assiomi  $eq(a,c)$  e  $eq(d,c)$  e calcolare l'insieme dei fatti provabili.

**Esempio.** Consideriamo un linguaggio con una costante  $a$ , un simbolo per una funzione  $s$  ed un nome di predicato "dispari". Consideriamo il programma positivo

$$dispari(a).$$

$$dispari(X) \rightarrow dispari(s(s(X))).$$

Allora

$$T(\emptyset) = \{dispari(a)\}$$

$$T^2(\emptyset) = \{dispari(a)\} \cup \{dispari(s(s(a)))\}$$

$$T^3(\emptyset) = \{dispari(a), dispari(s(s(a)))\} \cup \{dispari(s(s(s(s(a))))\}$$

...

In tale esempio tutti i  $T^n(\emptyset)$  sono diversi tra loro e l'insieme dei fatti dimostrabili coincide con l'insieme dei fatti del tipo  $dispari(s(\dots s(a)))$  dove  $s$  compare un numero pari di volte.

#### 4. Modelli di Herbrand: mondi costruiti con parole

Per i programmi positivi non solo l'apparato inferenziale è particolarmente semplice ma anche la costruzione di modelli non presenta eccessive difficoltà. Per mostrare questo fatto seguiremo una delle principali idee della logica matematica cioè che:

*è possibile costruire modelli di una teoria a partire dal linguaggio stesso in cui è espressa la teoria.*

Tale idea è in accordo con il punto di vista secondo cui la matematica è solo un sistema per manipolare dei segni:

$$\text{matematica} \Leftrightarrow \text{segni} + \text{regole per manipolare segni.}$$

Più precisamente per costruire un modello assumiamo che:

si possa considerare come dominio di interpretazione l'insieme dei "nomi che si possono formulare nel linguaggio  $\mathcal{L}$ ".

Con la parola "nome" intendiamo un'espressione linguistica che determina univocamente un elemento del dominio di interpretazione. Pertanto i nomi sono sia le costanti (in un certo

sensu i nomi propri) sia ciò che si può ottenere dalle costanti e dai nomi di operazioni, cioè i termini chiusi.

**Definizione 4.1.** Sia  $\mathcal{L}$  un linguaggio del primo ordine contenente almeno una costante, allora l'universo di Herbrand è l'insieme  $U(\mathcal{L})$  di tutti i termini chiusi di  $\mathcal{L}$ .

Ad esempio se nel linguaggio ho una costante 1 ed un nome di operazione +, allora l'universo di Herbrand sarà costituito dai termini chiusi

$$1, 1+1, (1+1)+1, 1+(1+1), \dots$$

Se nel linguaggio ho anche il simbolo 0, allora l'universo di Herbrand sarà costituito dai termini del tipo

$$0, 1, 1+1, 0+1, 1+0, (1+1)+1, 1+(1+1), \dots$$

Se nel linguaggio ho solo il simbolo  $\leq$  allora non esistono termini e l'universo di Herbrand è vuoto. Se il linguaggio contiene solo i nomi "Maria" e "Carlo" allora l'universo di Herbrand si riduce all'insieme  $\{Maria, Carlo\}$ . Se oltre a questi due nomi si introduce anche il nome di funzione *padre\_di*, allora nell'universo di Herbrand sarà costituito dagli infiniti termini

$$\begin{aligned} & Maria, Carlo, \\ & padre\_di(Maria), padre(Carlo), \\ & padre\_di(padre\_di(Maria)), padre\_di(padre(Carlo)), \\ & \dots \end{aligned}$$

**Proposizione 4.2.** Se non vi sono nomi di funzioni in  $\mathcal{L}$  l'universo di Herbrand  $U(\mathcal{L})$  coincide con l'insieme delle costanti ed è quindi, in generale, finito. Se vi è il nome di almeno una funzione allora  $U(\mathcal{L})$  è infinito.

*Dim.* La prima parte è ovvia. Supponiamo che esista un nome di operazione  $n$ -aria  $f$  e sia  $c$  una costante del linguaggio, allora posto

$$t_1 = f(c, \dots, c), t_2 = f(t_1, \dots, t_1), t_3 = f(t_2, \dots, t_2), \dots$$

si ottiene una successione infinita di termini chiusi e quindi di elementi di  $U(\mathcal{L})$ .  $\square$

**Esempio.** Sia  $\mathcal{L}$  un linguaggio per la teoria degli insiemi ordinati contenente le costanti 0 ed 1, allora  $U(\mathcal{L})$  è l'insieme finito  $\{0,1\}$ . Sia  $\mathcal{L}$  un linguaggio con una sola costante  $c$  ed un solo nome di funzione unaria  $f$  allora

$$U(\mathcal{L}) = \{c, f(c), f(f(c)), \dots\}.$$

Se invece in  $\mathcal{L}$  vi è anche la costante  $b$  allora

$$U(\mathcal{L}) = \{a, b, f(a), f(b), f(f(a)), f(f(b)), \dots\}.$$

Se invece di  $f$  vi è il nome di una operazione binaria +, allora

$$U(\mathcal{L}) = \{c, b, c+c, c+b, (b+b)+b, (c+b)+c, \dots\}.$$

Da notare che  $c+c$  viene considerato diverso da  $c$ ,  $c+b$  diverso da  $b+c$  e così via.

Possiamo considerare l'universo di Herbrand  $U(\mathcal{L})$  come una struttura algebrica.

**Definizione 4.3.** Chiamiamo *algebra libera dei termini chiusi* la struttura che ha l'universo di Herbrand  $U(\mathcal{L})$  come dominio e che ha come operazioni le operazioni ottenute definendo, per ogni nome di operazione  $n$ -aria  $o$ , l'operazione  $n$ -aria  $o' : U(\mathcal{L})^n \rightarrow U(\mathcal{L})$  tale che

$$o'(t_1, \dots, t_n) = o(t_1, \dots, t_n).$$

L'insieme  $C$  delle costanti è un sistema di generatori di tale struttura algebrica.

**Definizione 4.3.** Una interpretazione  $(D, I)$  di  $\mathcal{L}$  viene detta *interpretazione di Herbrand o modello di Herbrand* (in breve *H-interpretazione* o *H-modello*) se:

- a) il dominio  $D$  è l'universo di Herbrand di  $\mathcal{L}$ , cioè  $D = U(\mathcal{L})$ ;
- b) ogni costante viene interpretata con se stessa:  $I(c) = c$
- c) ogni nome di funzione  $n$ -aria  $h$  viene interpretata come la funzione che associa ai termini chiusi  $t_1, \dots, t_n$  il termine chiuso  $h(t_1, \dots, t_n)$ :

$$I(h)(t_1, \dots, t_n) = h(t_1, \dots, t_n).$$

Da notare che due differenti  $H$ -interpretazioni di un dato linguaggio differiscono solo per le interpretazioni dei predicati.

**Esempio.** Ad esempio, supponiamo che il nostro linguaggio  $\mathcal{L}$  contenga i nomi propri (cioè le costanti) *maria*, *mario*, *luigi*, *carlo*, ed il predicato *Amico*( $x, y$ ) da interpretare con la relazione di amicizia. Allora una interpretazione di tale linguaggio si ottiene, ad esempio, considerando un insieme  $D$  di persone, associando alle costanti *maria*, *mario*, *luigi* e *carlo* delle particolari persone in  $D$  ed interpretando *Amico* come un particolare relazione binaria  $I(\text{Amico}) \subseteq D \times D$  che esprime la relazione di amicizia. Naturalmente niente esclude che oltre le quattro persone che sono denotate con particolari nomi ci siano anche molte altre persone in  $D$ . Noi siamo interessati ad interpretazioni che siano le più piccole possibile e quindi in cui  $D$  abbia solo quattro elementi che permettano di interpretare i quattro nomi di persona utilizzati. Ma, se si vuole questo, tanto vale identificare questi quattro elementi con quattro foglietti con i nomi degli elementi o, addirittura con i quattro nomi di persona coinvolti. Si pone allora  $D = \{\text{maria, mario, luigi, carlo}\}$  cioè  $D$  uguale all'universo di Herbrand  $U_{\mathcal{L}}$ . Una interpretazione si ottiene assegnando al predicato *Amico* un insieme di coppie, cioè un elemento di  $P(D \times D)$ . Ad esempio potremmo mettere

$$I(\text{Amico}) = \{(\text{mario, carlo}), (\text{carlo, luigi}), (\text{luigi, carlo})\}.$$

Poiché  $D \times D$  ha cardinalità 16,  $P(D \times D)$  ha cardinalità  $2^{16} = 65536$ . Questo significa che esistono 65536  $H$ -interpretazioni possibili di  $\mathcal{L}$ .

Supponiamo di aggiungere al linguaggio il nome di funzione *padre* che interpretiamo come la funzione che associa ad ogni persona il relativo padre. Allora l'universo di Herbrand diventa subito infinito poiché sarà costituito da

$$U_{\mathcal{L}} = \{\text{maria, mario, luigi, carlo, padre(maria), padre(mario), padre(luigi), padre(carlo), padre(padre(maria)), padre(padre(mario)), \dots}\}.$$

Ancora una volta si ottiene una interpretazione di Herbrand associando ad *Amico* un opportuno insieme di coppie, cioè un opportuno sottoinsieme  $U_{\mathcal{L}} \times U_{\mathcal{L}}$ . Ne segue che esistono tante interpretazioni diverse quanti sono gli elementi di  $P(U_{\mathcal{L}} \times U_{\mathcal{L}})$ . In definitiva, essendo  $U_{\mathcal{L}}$  un insieme numerabile, l'insieme delle possibili interpretazioni di Herbrand ha la potenza del continuo.

**Problema.** Sia  $\mathcal{L}$  un linguaggio con costanti  $a, b, c$  ed un unico predicato unario  $r$ . Dire quante  $H$ -interpretazioni di  $\mathcal{L}$  esistono.

La seguente proposizione si dimostra per induzione sulla complessità del termine  $t$ .

**Proposizione 4.5.** Detta  $I$  una interpretazione di Herbrand e  $t$  un termine le cui variabili sono comprese tra  $x_1, \dots, x_n$ , allora  $I(t) : U(\mathcal{L})^n \rightarrow U(\mathcal{L})$  è la funzione che associa ai termini chiusi  $t_1, \dots, t_n$  il termine che si ottiene sostituendo in  $t$  a ciascun  $x_i$  il termine  $t_i$ . In altre parole:

$$I(t)(t_1, \dots, t_n) = t(x_1/t_1, \dots, x_n/t_n).$$

Ad esempio, se  $\mathcal{L}$  contiene la costante  $c$  ed una operazione binaria  $+$ , allora il termine  $t = ((x_1+x_2)+a)+x_1$  determina la funzione  $I(t)$  che associa ad ogni coppia  $t_1, t_2$  di termini chiusi il termine chiuso  $((t_1+t_2)+a)+t_1$ .

La seguente proposizione si prova per induzione sulla complessità della formula  $\alpha$ .

**Proposizione 4.6.** Detta  $I$  una interpretazione di Herbrand risulta che, per ogni formula  $\alpha$ ,

$$I \models \alpha [t_1, \dots, t_n] \Leftrightarrow I \models \alpha(t_1, \dots, t_n).$$

In particolare,

$$I \models \exists x_i \alpha(x_i) \Leftrightarrow \text{esiste } t \in U(\mathcal{L}) \text{ tale che } I \models \alpha(x_i/t).$$

### 5. Un teorema di punto fisso per costruire modelli

Due differenti  $H$ -interpretazioni di uno stesso linguaggio differiscono solo per il modo come sono stati interpretati i predicati. Questo fatto può essere utilizzato per definire in modo semplice un  $H$ -modello.

**Definizione 5.1.** Prende il nome di *base di Herbrand* l'insieme  $B_{\mathcal{L}}$  di tutti i possibili fatti, cioè formule atomiche che non contengono variabili.

Ciò significa che in  $B_{\mathcal{L}}$  vi sono tutte e sole le formule del tipo  $r(t_1, \dots, t_n)$  con  $r$  nome di relazione e  $t_1, \dots, t_n$  elementi dell'universo di Herbrand. La seguente proposizione mostra che possiamo associare ad ogni insieme di fatti  $S$  una interpretazione di Herbrand  $I_S$  definita dal porre, per ogni nome di relazione  $n$ -aria  $r$ ,

$$I_S(r) = \{(t_1, \dots, t_n) \mid r(t_1, \dots, t_n) \in S\}. \quad (5.1)$$

Tale interpretazione può essere vista come la più piccola  $H$ -interpretazione in cui tutti i fatti in  $S$  risultano veri. Possiamo anche procedere in modo inverso poiché possiamo associare ad ogni  $H$ -interpretazione  $I$  il sottoinsieme  $S_I$  di  $B_{\mathcal{L}}$  costituito dai fatti che sono veri in  $I$ :

$$S_I = \{r(t_1, \dots, t_n) \in B_{\mathcal{L}} \mid I \models r(t_1, \dots, t_n)\}. \quad (5.2)$$

**Proposizione 5.2.** La corrispondenza che associa ad ogni  $H$ -interpretazione  $I$  il sottoinsieme  $S_I$  di  $B_{\mathcal{L}}$  è biettiva e la sua inversa è l'applicazione che associa ad ogni sottoinsieme  $S$  di  $B_{\mathcal{L}}$  l' $H$ -interpretazione  $I_S$ .

*Dim.* Se  $I$  e  $I'$  sono due diverse  $H$ -interpretazioni, allora esiste  $r$  tale che  $I(r) \neq I'(r)$  e quindi esistono  $t_1, \dots, t_n$  in  $U(\mathcal{L})$  tali che, ad esempio,  $t_1, \dots, t_n$  sono nella relazione  $I(r)$  ma non sono nella relazione  $I'(r)$ . Ciò comporta che  $r(t_1, \dots, t_n)$  appartiene ad  $S_I$  ma non appartiene a  $S_{I'}$  e quindi che  $S_I \neq S_{I'}$ . Il fatto che tale corrispondenza sia suriettiva deriva dal fatto che se  $S$  è un sottoinsieme di  $B_{\mathcal{L}}$  detta  $I$  l'interpretazione definita da

$$I(r) = \{(t_1, \dots, t_n) \mid r(t_1, \dots, t_n) \in S\}$$

risulta che  $S_I = S$ . La rimanente parte della proposizione è immediata.  $\square$

Queste due corrispondenze mostrano che:

la classe delle interpretazioni di Herbrand si può identificare con la classe  $P(B_{\mathcal{L}})$  dei sottoinsiemi di  $B_{\mathcal{L}}$ .

**Esempio.** Sia  $\mathcal{L}$  il linguaggio le cui costanti sono  $a, b, c$  ed avente un unico predicato binario  $r$ . Le  $H$ -interpretazioni si ottengono interpretando  $r$  come sottoinsieme di  $U(\mathcal{L}) \times U(\mathcal{L}) = \{a, b, c\} \times \{a, b, c\}$ . Se si considera un qualunque sottoinsieme  $S$  di  $B_{\mathcal{L}}$ , ad esempio  $S = \{r(a, a), r(c, b), r(b, c)\}$  allora viene definita l'interpretazione  $I_S$  per cui  $I_S(r) = \{(a, a), (c, b), (b, c)\}$ . Si osservi che se  $\mathcal{L}$  contiene l'uguaglianza  $=$  ed  $S$  è un qualunque insieme di fatti, allora non è detto che  $I_S$  interpreti  $=$  con una congruenza e che quindi  $(U(\mathcal{L}), I)$  sia un modello della teoria con uguaglianza. Ad esempio se  $S = \{a = b, c = d, r(a, a), r(c, b), r(b, c)\}$  allora  $I(=)$  è la relazione  $\{(a, b), (c, d)\}$  e tale relazione non è nemmeno di equivalenza.

**Problema.** Elencare un certo numero di clausole vere nell'interpretazione  $I_S$  dell'esempio precedente.

**Problema.** Dire quante  $H$ -interpretazioni del linguaggio dell'esempio precedente sono possibili.

**Problema.** Consideriamo un linguaggio con un nome di predicato binario  $r$  e le costanti  $a, b, c$ . Descrivere il modello di Herbrand associato all'insieme  $\{r(a, b), r(a, a), r(c, a)\}$  di fatti.

**Proposizione 5.3.** Sia  $S$  un sottoinsieme di  $B_{\mathcal{L}}$  ed  $\alpha$  una clausola di programma positivo, allora

- se  $\alpha$  è un fatto

$$I_S \models \alpha \Leftrightarrow \alpha \in S$$

(cioè un fatto è vero in un modello di Herbrand se e solo se appartiene a tale modello)

- se  $\alpha$  è una regola atomica le cui variabili sono tra  $x_1, \dots, x_p$ , allora

$$I_S \models \alpha [t_1, \dots, t_p] \Leftrightarrow \alpha(t_1, \dots, t_p) \in S$$

dove  $\alpha(t_1, \dots, t_p)$  denota il fatto che si ottiene sostituendo ciascun termine chiuso  $t_i$  al posto della variabile  $x_i$ ;

- se  $\alpha$  è una regola del tipo  $\gamma_1 \wedge \dots \wedge \gamma_n \rightarrow \gamma$ , allora

$$I_S \models \alpha [t_1, \dots, t_p] \Leftrightarrow \text{da } \gamma_1(t_1, \dots, t_p) \in S, \dots, \gamma_n(t_1, \dots, t_p) \in S \text{ segue } \gamma(t_1, \dots, t_p) \in S.$$

*Dim.* Se  $\alpha$  è il fatto  $r(t_1, \dots, t_n)$  allora

$$I_S \models r(t_1, \dots, t_n) \Leftrightarrow (t_1, \dots, t_n) \in I(r) \Leftrightarrow r(t_1, \dots, t_n) \in S.$$

Se  $\alpha$  è la regola atomica  $r(\underline{t}_1, \dots, \underline{t}_n)$  le cui variabili libere sono tra  $x_1, \dots, x_p$  allora ricordiamo che  $I(\underline{t}_i)(t_1, \dots, t_p)$  è il termine  $\underline{t}_i(t_1, \dots, t_p)$  che si ottiene sostituendo in  $\underline{t}_i(x_1, \dots, x_p)$  alle variabili  $x_1, \dots, x_p$  i termini  $t_1, \dots, t_p$ . Pertanto

$$\begin{aligned} I_S \models r(\underline{t}_1, \dots, \underline{t}_n) [t_1, \dots, t_p] &\Leftrightarrow (I_S(\underline{t}_1)(t_1, \dots, t_p), \dots, I_S(\underline{t}_n)(t_1, \dots, t_p)) \in I_S(r) \\ &\Leftrightarrow (\underline{t}_1(t_1, \dots, t_p), \dots, \underline{t}_n(t_1, \dots, t_p)) \in I_S(r) \Leftrightarrow r(\underline{t}_1(t_1, \dots, t_p), \dots, \underline{t}_n(t_1, \dots, t_p)) \in S. \end{aligned}$$

Se  $\alpha$  è una regola del tipo  $\gamma_1 \wedge \dots \wedge \gamma_n \rightarrow \gamma$  le cui variabili libere sono tra  $x_1, \dots, x_p$ , allora

$$\begin{aligned} I_S \models \gamma_1 \wedge \dots \wedge \gamma_n \rightarrow \gamma [t_1, \dots, t_p] &\Leftrightarrow I_S \models \gamma_1 [t_1, \dots, t_p], \dots, I_S \models \gamma_n [t_1, \dots, t_p] \text{ implica } I_S \models \gamma [t_1, \dots, t_p] \\ &\Leftrightarrow \text{da } \gamma_1(t_1, \dots, t_p) \in S, \dots, \gamma_n(t_1, \dots, t_p) \in S \text{ segue } \gamma(t_1, \dots, t_p) \in S. \end{aligned}$$

□

Dato un programma positivo  $P$  abbiamo già visto che definendo opportunamente un operatore  $T$  possiamo produrre tutti i fatti che sono dimostrabili a partire da  $P$ .

**Teorema 5.4.** Sia  $P$  un programma positivo e sia  $T$  l'operatore definito in (3.1). Allora sono punti uniti di  $T$  tutti e soli gli  $H$ -modelli di  $P$  (nel senso che  $S$  è punto unito se e solo se  $I_S$  è un modello di  $P$ ).

*Dim.* Supponiamo che  $S$  sia un punto unito di  $T$ , cioè che  $T(S) \subseteq S$  e che  $\alpha_1 \wedge \dots \wedge \alpha_n \rightarrow \alpha \in \text{Reg}(P)$  e  $\alpha_1, \dots, \alpha_n$  sono elementi di  $S$ , allora  $\alpha \in S$ . Allora dalla proposizione 3.3 segue che  $S$  è un modello di  $P$ .

Viceversa, supponiamo che  $S$  sia un  $H$ -modello di  $P$  e dimostriamo che è un punto unito di  $T$ , cioè che  $S$  contiene  $T(S)$ . Ora, per la proposizione 3.3 il fatto che  $S$  sia modello di  $P$  comporta che  $S$  contiene ogni fatto di  $P$  ed ogni fatto che si ottiene da una formula atomica di  $P$ . Pertanto  $S$  contiene  $F(P)$ . D'altra parte supponiamo che  $\alpha_1 \wedge \dots \wedge \alpha_n \rightarrow \alpha$  appartenga a  $\text{Reg}(P)$ , precisamente che sia stata ottenuta dalla regola  $\gamma_1 \wedge \dots \wedge \gamma_n \rightarrow \gamma$  di  $P$  sostituendo alle variabili  $x_1, \dots, x_n$  i termini chiusi  $d_1, \dots, d_p$  e che  $\alpha_1 = \gamma_1(d_1, \dots, d_p), \dots, \alpha_n = \gamma_n(d_1, \dots, d_p)$  siano elementi di  $S$ . Allora sempre per la proposizione 3.3 abbiamo che  $\alpha = \gamma(d_1, \dots, d_p)$  appartiene ad  $S$ . In conclusione

$$S \supseteq \{ \alpha \mid \alpha_1 \wedge \dots \wedge \alpha_n \rightarrow \alpha \in \text{Reg}(P), \alpha_1 \in X, \dots, \alpha_n \in X \}$$

e pertanto  $T(S) \subseteq S$ . □

Si osservi che in particolare da tale teorema segue che ogni programma positivo  $P$  è una teoria soddisfacibile ed ammette come modello l' $H$ -modello banale l'insieme di tutti i fatti  $B_{\mathcal{L}}$ .

**Definizione 5.5.** L' $H$ -modello di un programma positivo che si ottiene come intersezione di tutti gli  $H$ -modelli di  $P$  viene detto *modello minimo di Herbrand di  $P$*  e viene denotato con  $M_P$ .

Naturalmente

$$M_P = \bigcup_{n \in \mathbb{N}} T^n(\emptyset)$$

dove:

$$T^1(\emptyset) = \text{Fatt}(P);$$

$$T^2(\emptyset) = \text{Fatt}(P) \cup \{ \beta \mid (\beta_1 \wedge \dots \wedge \beta_n \rightarrow \beta) \in \text{Reg}(P), \beta_1 \in \text{Fatt}(P), \dots, \beta_n \in \text{Fatt}(P) \};$$

$$T^3(\emptyset) = T_2(\emptyset) \cup \{ \beta \mid (\beta_1 \wedge \dots \wedge \beta_n \rightarrow \beta) \in \text{Reg}(P), \beta_1 \in T_2(\emptyset), \dots, \beta_n \in T_2(\emptyset) \};$$

...

$$T^{n+1}(\emptyset) = T^n(\emptyset) \cup \{ \beta \mid (\beta_1 \wedge \dots \wedge \beta_n \rightarrow \beta) \in \text{Reg}(P), \beta_1 \in T^n(\emptyset), \dots, \beta_n \in T^n(\emptyset) \}.$$

Se nel linguaggio esistono solo un numero finito di costanti e non esistono nomi di funzioni, essendo la base di Herbrand  $B_{\mathcal{L}}$  finita, tale catena di sottoinsiemi di  $B_{\mathcal{L}}$  non può crescere indefinitamente. Esisterà quindi un elemento massimo che coincide con il modello minimo  $M_P$ .

**Esempio.** Sia  $P = \{ r(a,b), r(c,d), r(x,y) \rightarrow s(x,y), r(y,x) \rightarrow s(x,y) \}$ , allora  $U(\mathcal{L}) = \{ a,b,c,d \}$ .

Inoltre,

$$T(\emptyset) = \text{Fatt}(P) = \{ r(a,b), r(c,d) \};$$

$$T^2(\emptyset) = \{ r(a,b), r(c,d) \} \cup \{ s(a,b), s(c,d), s(b,a), s(d,c) \};$$

$$T^3(\emptyset) = T_2(\emptyset).$$

Pertanto  $M_P = T_2(\emptyset)$  o, se si vuole, l' $H$ -modello minimo di  $P$  interpreta  $r$  come la relazione  $I(r) = \{ (a,b), (c,d) \}$  ed  $s$  come la relazione  $I(s) = \{ (a,b), (c,d), (b,a), (d,c) \}$ .

**Problema.** Aggiungere al programma precedente la formula  $r(x,x)$  (oppure la formula  $s(x,x)$ ) e calcolare il modello minimo.

**Esempio.** Supponiamo di avere un linguaggio  $\mathcal{L}$  con costanti  $a,b,c,d$  ed una relazione binaria "eq". Inoltre sia  $P$  la teoria dell'equivalenza, cioè la teoria i cui assiomi sono:

$$eq(x,x) \quad ; \quad eq(x,y) \rightarrow eq(y,x) \quad ; \quad eq(x,z) \wedge eq(z,y) \rightarrow eq(x,y) .$$

Tale teoria è un programma positivo e risulta

$$T(\emptyset) = \{eq(a,a), eq(b,b), eq(c,c), eq(d,d)\} ; T^2(\emptyset) = T(\emptyset),$$

pertanto l' $H$ -modello minimo  $M_P$  coincide con  $T(\emptyset)$  ed interpreta "eq" come identità:

$$I(eq) = \{(a,a), (b,b), (c,c), (d,d)\}.$$

Naturalmente esistono anche altri  $H$ -modelli di  $P$ , è sufficiente interpretare  $eq$  con una qualunque relazione di equivalenza in  $\{a, b, c, d\}$ . Il più "grosso" ovviamente è quello in cui  $eq$  viene interpretata come la relazione  $U(\mathcal{L}) \times U(\mathcal{L})$  che sussiste tra due qualunque elementi.

**Problema.** Aggiungere al programma dell'esempio precedente gli assiomi  $eq(a,c)$  e  $eq(d,c)$  e trovare il relativo  $H$ -modello minimo.

**Esempio.** Consideriamo un linguaggio con una costante  $a$ , un simbolo per una funzione  $s$  ed un nome di predicato "dispari". Consideriamo il programma

$$dispari(a).$$

$$dispari(X) \rightarrow dispari(s(s(X))).$$

Allora  $U_{\mathcal{L}} = \{a, s(a), s(s(a)), \dots\}$

$$T(\emptyset) = \{dispari(a)\}$$

$$T^2(\emptyset) = \{dispari(a)\} \cup \{dispari(s(s(a)))\}$$

$$T^3(\emptyset) = \{dispari(a), dispari(s(s(a)))\} \cup \{dispari(s(s(s(s(a))))\}$$

...

In tale esempio tutti i  $T^n(\emptyset)$  sono diversi tra loro ed il modello minimo di Herbrand coincide con l'insieme dei fatti del tipo  $dispari(s(\dots s(a)))$  dove  $s$  compare un numero pari di volte.

## 6. Ad ogni interpretazione è possibile associare una interpretazione di Herbrand

Per poter provare che il sistema inferenziale proposto per i programmi positivi è sufficientemente potente, mostriamo prima che ad ogni struttura matematica è associata una interessante interpretazione di Herbrand.

**Definizione 6.1.** Data una interpretazione  $(D,I)$  di un linguaggio  $\mathcal{L}$ , chiamiamo  $H$ -interpretazione di  $\mathcal{L}$  associata a  $(D,I)$  l'interpretazione di Herbrand  $(U(\mathcal{L}) I^*)$  definita dal seguente insieme di fatti

$$S_I = \{\alpha \in B_{\mathcal{L}} \mid I \models \alpha\}.$$

In altri termini,  $I^*$  è l'interpretazione in cui il dominio è l'universo di Herbrand e tale che per ogni nome di relazione  $r$ ,

$$(t_1, \dots, t_n) \text{ sono nella relazione } I^*(r) \Leftrightarrow \text{la formula atomica } r(t_1, \dots, t_n) \text{ è vera in } I.$$

**Esempio.** Sia  $\mathcal{L} = \{\leq, 0, 1\}$  il linguaggio per le strutture ordinate e consideriamo l'interpretazione  $(D,I)$  di tale linguaggio tale che:

$$D = \mathcal{P}(S),$$

$$I(\leq) \text{ è la relazione di inclusione,}$$

$$I(0) = \emptyset$$

$$I(1) = S.$$

Allora l' $H$ -interpretazione associata a  $(\mathcal{P}(S), \subseteq, \emptyset, S)$  è la relazione d'ordine nel dominio  $U(\mathcal{L}) = \{0, 1\}$ , in cui 0 ed 1 si interpretano ancora con 0 ed 1 e  $I^*(\leq) = \{(0,1), (0,0), (1,1)\}$ .

La seguente proposizione mostra che il modello di Herbrand associato ad un'interpretazione  $I$  è, in un certo senso, un sottomodello di  $I$ . Infatti il suo quoziente normale è isomorfo al sottomodello di  $I$  generato dall'insieme delle interpretazioni dei termini chiusi.

**Proposizione 6.2.** Sia  $(D, I)$  una interpretazione ed  $(U(\mathcal{L}), I^*)$  la relativa  $H$ -interpretazione. Consideriamo la funzione  $f : U(\mathcal{L}) \rightarrow D$  che associa ad ogni termine chiuso  $t \in U(\mathcal{L})$  la sua interpretazione  $I(t)$  in  $D$ . Allora tale funzione risulta essere un omomorfismo pieno di  $(U(\mathcal{L}), I^*)$  in  $(D, I)$ . Inoltre il quoziente normale di  $(U(\mathcal{L}), I^*)$  è isomorfo alla sotto-interpretazione di  $(D, I)$  il cui dominio è  $h(D)$ .

*Dim.* Per provare che la funzione  $f$  è un omomorfismo osserviamo che, per ogni nome di operazione  $n$ -aria  $h$ , risulta

$$f(h(t_1, \dots, t_n)) = I(h(t_1, \dots, t_n)) = I(h)(I(t_1), \dots, I(t_n)) = I(h)(f(t_1), \dots, f(t_n)).$$

**Esempio.** Consideriamo il linguaggio per la teoria degli anelli che supponiamo contenga le costanti 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, tre nomi di operazioni +, - e  $\cdot$  ed il simbolo di uguaglianza =. In tale linguaggio siamo interessati a termini di un particolare tipo che si riferiscono alla rappresentazione decimale di un numero. Infatti, oltre alle costanti, consideriamo:

- il termine 10 che indichiamo con  $10^1$
- il termine  $10 \cdot 10$  che indichiamo con  $10^2$
- il termine  $(10 \cdot 10) \cdot 10$  che indichiamo con  $10^3$
- ...
- il termine  $a_0 + a_1 \cdot 10 + \dots + a_n \cdot 10^n$  che indichiamo con  $a_0 a_1 \dots a_n$
- il termine  $-(a_0 + a_1 \cdot 10 + \dots + a_n \cdot 10^n)$  che indichiamo con  $-a_0 a_1 \dots a_n$

Naturalmente  $a_0, \dots, a_n$  denotano elementi in  $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ . Consideriamo poi una particolare interpretazione di tale linguaggio, ad esempio quella usuale determinata da campo  $R$  dei numeri reali. Allora, il modello di Herbrand associato ad  $R$  ha come dominio l'insieme dei termini chiusi del tipo  $(1+1) \cdot (1+1)$ ,  $0 \cdot 1$ ,  $-(0+1)$ ,  $0+1$  . . . L'interpretazione dell'unico predicato = viene definita dall'insieme delle equazioni  $t_1 = t_2$  che sono verificate in  $R$  (l'unica relazione è l'uguaglianza). Ad esempio in tale insieme ci saranno le equazioni

$$1=1, (1-1) \cdot 1 = 1 \cdot 1 - 1 \cdot 1, (1+1) \cdot 1 = (1+1) \cdot 1, 1 + 0 = 1, 0 - (1+1) = (0-1) - 1 \dots$$

Questo significa che il simbolo = viene interpretato da una relazione  $\equiv$  tra termini che si ottiene ponendo  $t_1 \equiv t_2$  se e solo se  $t_1$  e  $t_2$  denotano lo stesso elemento in  $R$ . E' evidente che  $\equiv$  risulta essere una congruenza. La corrispondenza  $h : U(\mathcal{L}) \rightarrow R$  che associa ad ogni termine  $t$  la relativa interpretazione  $I(t) \in R$  è un omomorfismo pieno il cui codominio è l'anello dei numeri interi relativi. Il nucleo di tale omomorfismi è proprio  $\equiv$ . Questo significa che l'anello degli interi relativi può essere ottenuto come opportuno quoziente dell'algebra dei termini.

Non tutte le teorie universali ammettono modelli, ad esempio la teoria universale costituita dalla sola formula  $\forall x(\alpha \wedge \neg \alpha)$  non ammette modelli. Tuttavia la seguente proposizione mostra che se una teoria universale ammette un modello, allora ammette anche un  $H$ -modello.

**Teorema 6.3.** Esistono teorie che pur se ammettono modelli non ammettono  $H$ -modelli. Pertanto se  $T$  è una teoria e  $(D, I)$  un suo modello, non è detto che l'interpretazione di Herbrand associata a  $(D, I)$  sia ancora un modello di  $T$ .

*Dim.* Consideriamo la teoria  $T = \{r(a), r(b), \exists x(\neg r(x))\}$ , considerata in un linguaggio che ha come costanti  $a, b$  ed " $r$ " come simbolo di relazione binaria. Tale teoria non è universale ed è soddisfacibile in quanto basta considerare come modello quello definito da un insieme  $D$  e da una interpretazione in cui  $I(r) \neq D$  mentre  $I(a) \in I(r)$  e  $I(b) \in I(r)$ . Non esiste però un  $H$ -modello per  $T$  perché il dominio di ogni  $H$ -modello è  $U(T) = \{a, b\}$  ed in tutti gli  $H$ -modelli di  $T$  essendo  $I(r) = \{a, b\}$  risulterà  $\forall x(r(x))$ .

**Teorema 6.4.** Se una teoria  $T$  è universale e  $(D, I)$  è un modello di  $T$ , allora l'interpretazione di Herbrand associata a  $(D, I)$  è ancora un modello di  $T$ . Ne segue che se  $T$  è universale allora:

$$T \text{ soddisfacibile} \Leftrightarrow T \text{ ammette un modello di Herbrand.}$$

*Dim.* Supponiamo che  $T$  sia una teoria universale, sia  $(D, I)$  un modello di  $T$  e sia  $(U(\mathcal{L}), I^*)$  il modello di Herbrand associato. Poiché la funzione  $h : U(\mathcal{L}) \rightarrow D$  è un omomorfismo pieno di  $I^*$  in  $I$ , tutte le formule universali che valgono in  $I$  valgono anche in  $I^*$ . Ciò prova, in particolare, che  $(U(\mathcal{L}), I^*)$  è un modello di  $T$ .  $\square$

**Teorema 6.5.** Ogni teoria  $T$  che ammette un modello ammette un modello di Herbrand in una opportuna estensione del linguaggio  $\mathcal{L}$ . Ne segue anche che ogni teoria che ammette un modello ammette anche un modello finito o numerabile (anche se ci si riferisce ai modelli normali).

*Dim.* Si ricordi che tramite la riduzione a forma normale prenessa e la successiva Skolemizzazione è possibile trasformare tutte le formule di  $T$  in formule universali equivalenti. In questo modo si ottiene una teoria universale  $T^*$ . Allora il fatto che esiste un modello di  $T$  implica che esiste un modello di  $T^*$  e quindi, per la proposizione 4.7, esiste un modello di Herbrand di  $T^*$ . Questo modello è anche un modello di  $T$ .

Per provare la seguente parte della proposizione basta osservare che l'universo di Herbrand nel caso in cui non esistono nomi di funzioni è un insieme finito, altrimenti è un insieme numerabile. Quando si effettua il quoziente di tale insieme modulo la congruenza determinata dall'identità, si ottiene ancora un insieme finito o numerabile.  $\square$

Ad esempio consideriamo la teoria  $T = \{r(a), r(b), \exists x(\neg r(x))\}$  descritta all'inizio della dimostrazione del Teorema 5.3. Possiamo eliminare il quantificatore esistenziale nel terzo assioma introducendo una costante  $c$  e sostituendo  $\exists x(\neg r(x))$  con  $\neg r(c)$ . In tale caso l'universo di Herbrand coincide con  $\{a, b, c\}$ , ed un  $H$ -modello di  $T^* = \{r(a), r(b), \neg r(c)\}$  si ottiene ponendo  $I(r) = \{a, b\}$ .

Un tale teorema, che verrà dimostrato nuovamente quando proveremo il teorema di completezza, ha un significato filosofico fondamentale. Infatti dice che appena si formula una teoria coerente  $T$  relativa ad una data realtà o fenomeno, si riesce a costruire un modello costituito da solo materiale linguistico di tale fenomeno. Tale modello formale costituisce un modello matematico di tale teoria.

**Teorema 6.6.** Sia  $P$  un programma positivo allora il suo  $H$ -modello minimo  $M_P$  è costituito dall'insieme dei fatti che sono conseguenze logiche di  $P$ :

$$M_P = \{\alpha \in B_{\mathcal{L}} \mid P \vDash \alpha\}.$$

Pertanto, per ogni fatto  $\alpha$ ,

$$P \models \alpha \Leftrightarrow P \vdash \alpha$$

*Dim.* Supponiamo che  $\alpha \notin M_P$  ed ammettiamo per assurdo che  $\alpha$  non sia conseguenza logica di  $P$ ; allora esisterebbe un modello di  $P$  in cui  $\alpha$  è falsa, e quindi un modello della teoria  $P \cup \{\neg\alpha\}$ . Essendo  $\neg\alpha$  senza quantificatori la teoria  $P \cup \{\neg\alpha\}$  è universale (pur non essendo un programma positivo), pertanto per la proposizione 4.5 esiste un suo  $H$ -modello e quindi di un  $H$ -modello di  $P$  in cui  $\alpha$  è falsa. Ciò è assurdo in quanto, appartenendo  $\alpha$  a  $M_P$ , appartiene a tutti gli  $H$ -modelli di  $P$  ed è quindi vera in tutti gli  $H$ -modelli di  $P$ . Viceversa, supponiamo che  $\alpha$  sia una conseguenza logica di  $P$ ; allora  $\alpha$  è vera in tutti gli  $H$ -modelli di  $P$  ed in particolare anche nel modello minimo  $M_P$ . Quindi  $\alpha$  appartiene a  $M_P$ .  $\square$

Tale teorema afferma, in sostanza, che il modello minimo di un programma positivo  $P$  è costituito da quei fatti che sono veri in tutti i possibili modelli di  $P$ .

### 7. Varietà algebriche e strutture algebriche libere.

In questo paragrafo ci riferiamo alle strutture algebriche e quindi a linguaggi che siano forniti di nomi di funzioni e di costanti ma aventi come unico nome di relazione il simbolo  $=$  di eguaglianza. Le teorie (per meglio dire i programmi) che considereremo nel seguito conterranno sempre gli assiomi per l'uguaglianza i quali sono clausole di programma positivo. Pertanto nei modelli di Herbrand di tali teorie l'interpretazione di  $=$  deve essere una congruenza nell'universo di Herbrand (che viene visto come struttura algebrica).

**Definizione 7.1.** Chiamiamo *algebra di Herbrand* una interpretazione di Herbrand di un linguaggio algebrico che verifichi gli assiomi di eguaglianza. Chiamiamo *algebra normale di Herbrand* il quoziente normale di una algebra di Herbrand.

Allora un algebra di Herbrand si ottiene considerando l'algebra dei termini chiusi più una congruenza in tale algebra. La corrispondente algebra quoziente ha come elementi le classi complete di equivalenza.

Ricordiamo che abbiamo chiamato *varietà* la classe dei modelli (normali) di una teoria con solo equazioni. Ad esempio la classe dei gruppi e quella degli anelli costituiscono varietà. Poiché ogni equazione è una clausola di programma positivo, possiamo considerare i modelli di Herbrand costruiti nel paragrafo precedente.

**Definizione 7.2.** Sia  $\mathcal{L}$  un linguaggio,  $S$  una teoria equazionale ed  $A$  un insieme. Indichiamo con  $\mathcal{L}(A)$  il linguaggio che si ottiene aggiungendo gli elementi di  $A$  alle costanti di  $\mathcal{L}$ . Allora chiameremo *struttura algebrica libera* su  $A$  di  $S$  il quoziente normale del modello di Herbrand minimo del programma positivo che si ottiene aggiungendo ad  $S$  gli assiomi dell'uguaglianza nel linguaggio  $\mathcal{L}(A)$ .

Per capire un po' meglio questa definizione, consideriamo qualche esempio.

**Monoide.** Ricordiamo che si chiama *monoide* una struttura algebrica con una operazione binaria associativa ed un elemento neutro. In altre parole sia  $\mathcal{L}$  il linguaggio con un nome " $\cdot$ " per una operazione binaria, una costante  $1$  ed il simbolo " $=$ ". Allora un monoide è una interpretazione normale di  $\mathcal{L}$  che verifica il seguente sistema di assiomi.

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

$$x \cdot 1 = x$$

$$1 \cdot x = x.$$

Sia  $A = \{a, b\}$ . Allora l'universo di Herbrand di  $\mathcal{L}(A)$  è costituito da infiniti termini del tipo  $a, b, a \cdot b, (a \cdot b) \cdot b, a \cdot 1, 1 \cdot b, a \cdot (a \cdot b), \dots$ .

Poiché l'unico nome di relazione è  $=$  i fatti sono tutti del tipo  $t = t'$  con  $t$  e  $t'$  elementi di  $U(\mathcal{L})$  e quindi un modello di Herbrand minimo sarà costituito da un insieme di equazioni di tale tipo. In particolare, per la Proposizione 4.5, il minimo modello di Herbrand sarà definito da

$$S = \{t = t' \mid t = t' \text{ è vera in ogni monoide}\}.$$

Tale modello minimo non è normale. Ad esempio, pur essendo  $(a \cdot b) \cdot a \equiv a \cdot (b \cdot a)$ , il termine  $(a \cdot b) \cdot a$  è differente da  $a \cdot (b \cdot a)$ . Siano  $x_1, \dots, x_n$  costanti, come al solito, ometteremo il punto e scriveremo  $x_1 x_2 \dots x_n$  per denotare il termine  $(x_1 \cdot (x_2 \cdot (\dots x_n)))$ . Ora, ricordiamo che la relazione di eguaglianza determina una equivalenza in cui, valendo la proprietà associativa, ogni termine chiuso sarà equivalente ad un termine del tipo  $x_1 \dots x_n$ . Ad esempio il termine  $(a \cdot (1 \cdot b)) \cdot (a \cdot a)$  è equivalente ad  $a \cdot ((1 \cdot b) \cdot (a \cdot a))$  che è equivalente ad  $a \cdot (1 \cdot (b \cdot (a \cdot a)))$  e quindi ad  $a1baa$ . In altre parole valendo la proprietà associativa l'uso delle parentesi non ha importanza. D'altra parte, poiché tra gli assiomi vi è anche l'affermazione che  $1$  è elemento neutro, ogni termine in cui compare  $1$  è equivalente ad un termine in cui  $1$  viene cancellato. In definitiva possiamo identificare un qualunque termine diverso dalla costante  $1$  con una parola nell'alfabeto  $\{a, b\}$  (che chiameremo "forma normale"). L'operazione di prodotto nell'insieme di tali parole sarà la corrispondenza che associa ad ogni coppia  $s, t$  di termini chiusi di  $\mathcal{L}(A)$  l'elemento  $(s) \cdot (t)$ . Ad esempio il prodotto di  $a \cdot (a \cdot b)$  per  $(b \cdot b) \cdot a$  è la parola  $(a \cdot (a \cdot b)) \cdot ((b \cdot b) \cdot a)$ . Con le notazioni semplificate, ciò significa che il prodotto di due parole coincide con la giustapposizione delle due parole e che quindi il prodotto di  $aab$  per  $bba$  è la parola  $aabbba$ . Otteniamo pertanto la nota definizione di monoide libero con generatori  $\{a, b\}$ .

**Monoidi commutativi.** Naturalmente possiamo fissare anche altre equazioni ed ottenere teorie più forti di quella dei monoidi liberi. Ad esempio aggiungendo  $x_1 x_2 = x_2 x_1$  otterremo la teoria dei monoidi commutativi ed in corrispondenza i monoidi commutativi liberi. Ciò significa ad esempio che la parola  $abab$  risulta equivalente alla parola  $aabb$ . Più in generale, è immediato che ogni parola è equivalente ad una parola del tipo  $a^n b^m$  con  $n$  ed  $m$  interi positivi (chiameremo *forme normali* i termini di tale tipo). Il prodotto sarà definito pertanto tramite

$$(a^n b^m) \cdot (a^p b^q) = a^{n+p} b^{m+q}.$$

**Problema.** Descrivere la struttura libera della teoria che si ottiene aggiungendo l'equazione  $a \cdot b = 1$ , oppure l'equazione  $x^2 = 1$ , oppure l'equazione  $a = 1$ , oppure l'equazione  $x^3 = 1$ , oppure l'equazione  $x^2 = x$ .

**Gruppi.** La teoria dei gruppi abeliani si ottiene aggiungendo un simbolo  $^{-1}$  per l'operazione di inverso e gli assiomi  $xx^{-1} = 1$  e  $x^{-1}x = 1$ . Naturalmente al nuovo simbolo per l'inverso corrisponde l'operazione che associa al termine  $t$  il termine  $t^{-1}$ , ad esempio alla parola  $ab$  è associata la parola  $(ab)^{-1}$ . Se, come al solito, si pone  $x^0 = 1$  e  $x^n = x(x^{n-1})$ , non è difficile vedere che ogni elemento di  $U(\mathcal{L})$  è equivalente ad una parola del tipo  $a^n b^m$  con  $m$  ed  $n$  interi relativi. Ad esempio, il termine chiuso  $(ab)(abb)^{-1}$  è equivalente a  $a^0 b^{-1}$  perché in ogni gruppo abeliano risulta che  $(xy)^{-1} = y^{-1}x^{-1}$  e quindi

$$(ab)(abb)^{-1} = abb^{-1}b^{-1}a^{-1} = ab^{-1}a^{-1} = a^0 b^{-1}.$$

D'altra parte è possibile rappresentare ogni classe completa di equivalenza tramite un suo elemento rappresentativo (forma normale). Pertanto il gruppo libero abeliano con due generatori può essere definito come l'insieme delle parole del tipo  $a^n b^m$ , con  $n, m$  interi relativi ed in cui l'operazione di prodotto è definita ponendo:

$$(a^n b^m)(a^{n'} b^{m'}) = a^{n+n'} b^{m+m'}.$$

**Problema.** Aggiungere agli assiomi della teoria dei gruppi abeliani l'assioma  $x^2 = 1$  e supporre che  $A = \{a, b\}$ . Studiare i modelli minimali normali corrispondenti.  $\square$

Abbiamo visto che spesso una struttura algebrica può essere ottenuta come quoziente di un'algebra  $U(\mathcal{L})$  di termini tramite una opportuna congruenza. D'altra parte è evidente che non si possono fare calcoli con classi ed è più conveniente individuare in ogni classe un particolare rappresentante che chiameremo "forma normale". Fatto questo si decide di lavorare con le forme normali invece che con le classi. In tale caso un calcolo consiste nel passare da forme normali a forme normali.

**Esempio.** Nell'insieme delle espressioni aritmetiche, cioè espressioni del tipo  $(3+5) \cdot 37 + 1$  possiamo chiamare forma normale la forma decimale in cui un intero è rappresentato da una somma di potenze di dieci. Allora quando si esegue una operazione, ad esempio il prodotto, il problema consiste nel passare dalla forma normale di due numeri  $x$  ed  $y$  alla forma normale di  $x \cdot y$ . Ad esempio, il prodotto di 234 per 11 viene visto come riduzione a forma normale dell'espressione  $(2 \cdot (10 \cdot 10) + 3 \cdot 10 + 4) \cdot (10 + 1)$  riduzione che porta alla espressione  $2 \cdot (10 \cdot 10) + 5 \cdot 10 + 7$ . Lo stesso "calcolo delle espressioni" che si studia a scuola non è altro che una riduzione di una espressione a forma normale.

**Esempio.** Nell'insieme delle formule della logica del primo ordine possiamo considerare l'equivalenza logica. La riduzione in forma normale prenessa permette di individuare in ogni classe di equivalenza un relativo rappresentante.

I sistemi di "calcolo simbolico" come Derive o Mathematica consistono nella riduzione di un termine (rappresentante una classe) alla sua forma canonica. La teoria generale che tratta tali tipi di problematiche prende il nome teoria dei "sistemi di riduzione" o dei "sistemi di riscrittura" che abbiamo già visto nel capitolo 4.

## 9. Il metodo di risoluzione ed il Prolog (da scrivere)

### 10. Logica induttiva: teorie scientifiche come compressione dell'informazione

Abbiamo visto che ad ogni programma positivo  $P$  è possibile associare in modo effettivo il relativo modello minimo di Herbrand  $M_P$ , cioè l'insieme dei fatti che si possono provare a partire da  $P$ . In generale  $P$  ha una cardinalità molto inferiore a quella di  $M_P$  e questo rende preferibile la programmazione logica ad altri sistemi per trattare informazione (ad esempio i data-base relazionali). In altre parole la programmazione logica può essere vista anche come un modo di compattare l'informazione. Ad esempio se si deve conservare in memoria l'informazione "essere coniugati" tramite un predicato  $coniugati(X,Y)$ , allora la possibilità di usare la regola

$$coniugati(X,Y) \rightarrow coniugati(Y,X)$$

permette di risparmiare metà memoria conservando una informazione del tipo  $coniugato(mario, maria)$  ma non l'informazione  $coniugato(maria, mario)$  che invece viene dedotta.

Possiamo anche considerare il processo inverso supponendo di avere un insieme  $M$  di fatti e cercando di trovare un programma (finito)  $P$  tale che  $M_P = M$ . Se la cardinalità di  $P$  è molto più piccola di quella di  $M$  allora risolvere un tale problema significa compattare l'informazione disponibile.

Ad esempio supponiamo di avere l'insieme di 8 fatti

$$M = \{ama(mario, maria), ama(maria, mario), ama(luigi, anna), ama(anna, luigi), \\ ama(maria, maria), ama(mario, mario), ama(luigi, luigi), ama(anna, anna)\}.$$

-Tale insieme può essere rappresentato dal programma positivo  $P$

$ama(X,Y) \rightarrow ama(Y,X).$

$ama(X,X).$

$ama(mario, maria).$

$ama(luigi, anna).$

nel senso che  $M = M_P$ . Da notare che tale programma contiene solo 4 formule. Il programma è stato prodotto osservando le regolarità della base di dati di partenza.

E' possibile riguardare l'insieme dei fatti come osservazioni che un ricercatore effettua nello studiare un fenomeno e la costruzione della teoria  $P$  come la ricerca di una teoria scientifica che giustifichi i fatti (cioè che consenta di dedurre i fatti da pochi principi generali). Tali tipi di ricerca appartengono alla "logica induttiva" che studia come costruire teorie a partire da un dato insieme di fatti. La logica "deduttiva" invece studia come, fissata una teoria, si possano derivare da essa i fatti che interessano. Ovviamente la logica induttiva è tipica di un fisico o di un chimico mentre la logica deduttiva è tipica di un matematico.