Logica Matematica

Sapienza Università di Roma

libro del corso: tbd

aglaia norza

6 gennaio 2026

thisisaglaia@gmail.com | github.com/AglaiaNorza

Indice

1 Logica Proposizionale

1.1. Introduzione

La logica proposizionale è un linguaggio formale con una semplice struttura sintattica basata su proposizioni elementari (atomiche) e sui seguenti connettivi logici:

- *Negazione* ($\neg$): inverte il valore di verità di un enunciato: se un enunciato è vero, la sua negazione è falsa, e viceversa.
- *Congiunzione* ($\wedge$): il risultato è vero se e solo se entrambi i componenti sono veri.
- *Disgiunzione* ($\vee$): il risultato è vero se almeno uno dei componenti è vero.
- *Implicazione* ($\rightarrow$): rappresenta l'enunciato logico "se ... allora". Il risultato è falso solo se il primo componente è vero e il secondo è falso.
- *Equivalenza* ($\leftrightarrow$): rappresenta l'enunciato logico "se e solo se". Il risultato è vero quando entrambi i componenti hanno lo stesso valore di verità, cioè sono entrambi veri o entrambi falsi.

Introduciamo anche il concetto di disgiunzione esclusiva o "XOR" ($\oplus$), il cui risultato è vero solo se gli operandi sono diversi tra di loro (uno vero e uno falso).

Def. 1: **Linguaggio proposizionale**

Un linguaggio proposizionale è un insieme infinito $\mathcal{L}$ di simboli detti **variabili proposizionali**, tipicamente denotato come $\{p_i : i \in I\}$ (con I "insieme di indici").

Def. 2: **Proposizione**

Una **proposizione** in un linguaggio proposizionale è un elemento dell'insieme PROP così definito:

(1) tutte le variabili appartengono a PROP

(2) se $A \in$ PROP, allora $\neg A \in$ PROP

(3) se $A, B \in$ PROP, allora $(A \wedge B), (A \vee B), (A \rightarrow B) \in$ PROP

(4) nient'altro appartiene a PROP (PROP è il più piccolo insieme che contiene le variabili e soddisfa le proprietà di chiusura sui connettivi 1 e 2)

Per facilitare la leggibilità delle formule, definiamo le seguenti regole di *precedenza*: $\neg$ ha precedenza su $\wedge, \vee$, e questi ultimi hanno precedenza su $\rightarrow$.

1.2. Assegnamenti, tavole di verità

Per un linguaggio $\mathcal{L}$, un **assegnamento** è una funzione

$$\alpha : \mathcal{L} \rightarrow \{0, 1\}$$

Estendiamo α ad $\hat{\alpha}$: PROP $\rightarrow \{0, 1\}$ in questo modo:

- $\hat{\alpha}(\neg A) = \begin{cases} 1 & A = 0 \\ 0 & A = 1 \end{cases}$
- $\hat{\alpha}(A \wedge B) = \begin{cases} 1 & \hat{\alpha}(A) = \hat{\alpha}(B) = 1 \\ 0 & altrimenti \end{cases}$
- $\hat{\alpha}(A \vee B) = \begin{cases} 0 & \hat{\alpha}(A) = \hat{\alpha}(B) = 0 \\ 1 & altrimenti \end{cases}$
- $\hat{\alpha}(A \rightarrow B) = \begin{cases} 0 & \hat{\alpha}(A) = 1 \wedge \hat{\alpha}(B) = 0 \\ 1 & altrimenti \end{cases}$

> notazione
>
> Utilizzeremo α al posto di $\hat{\alpha}$ per comodità di notazione.

Osserviamo che è possibile rappresentare gli assegnamenti in modo compatto utilizzando le **tavole di verità**, una presentazione tabulare della funzione di assegnamento.

Per esempio, possiamo riscrivere la definizione di $\alpha(\neg A)$ come segue:

A	$\neg A$
0	1
1	0

Ogni riga di una tavola di verità corrisponde ad un assegnamento α.

Si noti anche che dalla definizione di α segue che un'implicazione può essere vera senza che ci sia connessione causale o di significato tra antecedente e conseguente (per esempio, "se tutti i quadrati sono pari allora π è irrazionale").

In secondo luogo, segue anche che una proposizione è sempre vera se il suo antecedente è falso (il che rispecchia la pratica matematica di considerare vera a vuoto una proposizione ipotetica la cui premessa non si applica).

Questo è giustificabile come segue:

- vogliamo che $(A \wedge B) \rightarrow B$ sia sempre vera
- il caso $1 \rightarrow 1$ deve essere vero, perché corrisponde al caso in cui A e B sono vere;

  il caso $0 \rightarrow 0$ deve essere vero, perché corrisponde al caso in cui $A \wedge B$ è falso perché B è falso; il caso $0 \rightarrow 0$ deve essere vero perché corrisponde al caso in cui $A \wedge B$ è falso perché B è falso;

il caso $0 \to 1$ deve essere vero perché corrisponde al caso in cui $A \wedge B$ è falso perché A è falso ma B è vero;

resta dunque soltanto il caso $1 \to 0$, che non corrisponde a nessun caso di $A \wedge B \to B$.

In più, si vuole che valga, per contrapposizione $(A \to B) \to (\neg B \to \neg A)$.

Osserviamo che, data $A = p_1, p_2, \ldots, p_k$ e due assegnamenti α e β t.c.:

$$\alpha(p_1) = \beta(p_1)$$
$$\ldots$$
$$\alpha(p_k) = \beta(p_k)$$

allora necessariamente $\alpha(A) = \beta(A)$.

soddisfacibilità

Se per una formula A e un assegnamento α si ha $\alpha(A) = 1$, si dice che "A soddisfa α" (o "A è vera sotto α").

- Se A ha almeno un assegnamento che la soddisfa, si dice **soddisfacibile** ($A \in$ `SAT`).
- Se non esiste un assegnamento che la soddisfa, A si dice **insoddisfacibile** ($A \in$ `UNSAT`).
- Se A è soddisfatta da tutti i possibili assegnamenti, si dice **tautologia** (o "verità logica") ($A \in$ `TAUT`).

Introduciamo anche alcune regole che

1.3. Conseguenza logica

Def. 3: **Conseguenza logica**

Sia T una *teoria*, ossia un insieme $\{A_1, \ldots, A_n\}$ proposizioni in un dato linguaggio proposizionale, e sia $A \in$ PROP .

Diciamo che A è **conseguenza logica** di T se

$$\forall \alpha,\ \alpha(T) = 1 \to \alpha(A) = 1$$

ovvero se ogni assegnamento che soddisfa T soddisfa anche A_{n+1}.

Scriviamo in tal caso $T \vDash A_{n+1}$, oppure $A_1, \ldots, A_n \vDash A$.

Si ha che:

- $T \nvDash A$ significa che $\exists \alpha$ t.c. $\alpha(T) = 1 \wedge \alpha(A) = 0$
- $\emptyset \vDash A$ o, equivalentemente $\vDash A \iff A$ è una tautologia
- se $T \vDash A$, allora $T \cup \neg A$è insoddisfacibile
- la conseguenza logica ha la proprietà di **monotonia**: se $T \vDash A$, allora anche $T \cup B \vDash A$
- ha anche la proprietà di transitività: se $T \vDash A$ e $A \vDash B$ allora $T \vDash B$

Lemma 1: **Equivalenze**

(1) $T \vDash A$

(2) $\vDash (A_1 \wedge \cdots \wedge A_n) \to A$

(3) $(A_1 \wedge \cdots \wedge A_n \wedge \neg A) \in \texttt{UNSAT}$

sono equivalenti.

1.4. Completezza funzionale

Data una tavola di verità arbitraria con n argomenti, esiste una proposizione A che ha esattamente quella tavola di verità?

Una proposizione A contenente le n variabili proposizionali $a_1, a_2, \ldots, a_n$ determina una funzione di n argomenti $f : \{0,1\}^n \to \{0,1\}$ ("**funzione di verità**"), tale che il valore di f_A su un argomento $(x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ sia dato da un arbitrario assegnamento α tale che $\alpha(p_k) = x_k$ per $k \in [1, n]$.

Thm. 1: **Teorema**

Sia $f : \{0,1\}^n \to \{0,1\}$ una funzione di verità. Esiste una proposizione A con n variabili proposizionali tale che, per ogni assegnamento α:

$$\alpha(A) = f(\alpha(a_1), \alpha(a_2), \ldots, \alpha(a_n))$$

(per qualsiasi funzione di verità, esiste sempre una proposizione che si comporta esattamente come essa (il valore di verità di A, $\alpha(A)$ è uguale al risultato della funzione f a parità di input))

dimostrazione

Si dimostra per induzione su n.

- **caso base**: $n = 1$ abbiamo quattro possibili f:

$$\begin{aligned} f_1(0) &= 0, \quad f_1(1) = 0 \\ f_2(0) &= 1, \quad f_2(1) = 1 \\ f_3(0) &= 0, \quad f_3(1) = 1 \\ f_4(0) &= 1, \quad f_4(1) = 0 \end{aligned}$$

  Alla funzione f_1 corrisponde la formula $(p \wedge \neg p)$, alla funzione f_2 la formula $(p \vee \neg p)$, alla funzione f_3 la formula p, e alla funzione f_4 la formula $(\neg p)$.

- **caso induttivo**: (assumiamo che il teorema valga per $n-1$ variabili, e dimostriamo che vale per n)

  Se $n > 1$, scriviamo il grafico di

$$f : \{0,1\}^n \to \{0,1\}$$

  in forma di tavola di verità in questo modo:

p_1	p_2	$\cdots$	p_n	$f(p_1,\ldots,p_n)$	
0	$\cdots$	$\cdots$	0	$\cdots$	
$\vdots$			$\vdots$	$\vdots$	grafico di una funzione f_0
0	$\cdots$	$\cdots$	1	$\cdots$	
1	$\cdots$	$\cdots$	0	$\cdots$	
$\vdots$			$\vdots$	$\vdots$	grafico di una funzione f_1
1	$\cdots$	$\cdots$	1	$\cdots$	

Se non consideriamo la prima colonna (p_1), la tavola di verità descrive il grafico di due funzioni, f_0 e f_1, a $n-1$ argomenti.

Sappiamo, quindi, per ipotesi induttiva, che esistono due formule A_0 e A_1 a $n-1$ variabili tali che, per ogni assegnamento α:

$$\alpha(A_0) = f_0(\alpha(p_1), \alpha(p_2), \ldots, \alpha(p_n))$$

$$\alpha(A_1) = f_1(\alpha(p_1), \alpha(p_2), \ldots, \alpha(p_n))$$

Dobbiamo ora combinare le due formule considerando anche la colonna p_1.

Possiamo farlo tramite la formula $A = (\neg p_1 \to A_0) \wedge (p_1 \to A_1)$.

Dimostriamo che A soddisfa il teorem: dobbiamo dimostrare che, dato un assegnamento qualsiasi α, si ha:

$$\alpha(A) = f(\alpha(p_1), \alpha(p_2), \ldots, \alpha(p_n))$$

Distinguiamo i due casi:

- $\alpha(p_1) = 1$
  in questo caso, si ha:
  $$\alpha\Big(\underset{=1}{(\neg p_1} \to A_0) \wedge \underset{=1}{(p_1} \to A_1)\Big)$$
  e la formula vale quindi $1 \iff \alpha(A_1) = 1$.
  Ma $\alpha(A_1) = f_1(\alpha(p_2), \ldots, \alpha(p_n))$, quindi la formula si comporta esattamente come f_1:
  $$f(\alpha(p_1), \alpha(p_2), \ldots, \alpha(p_n)) = f(1, \alpha(p_2), \ldots, \alpha(p_n)) = f_1(\alpha(p_2), \ldots, \alpha(p_n)).$$
  Quindi, in questo caso, vale
  $$\alpha(A) = (\alpha(p_1), \alpha(p_2), \ldots, \alpha(p_n))$$
- $\alpha(p_1) = 0$
  in questo caso, si ha:
  $$\alpha\Big(\underset{=1}{(\neg p_1} \to A_0) \wedge \underset{=1}{(p_1} \to A_1)\Big)$$
  che vale $1 \iff \alpha(A_0) = 1$.
  Quindi si può fare lo stesso ragionamento di sopra, ma per A_1 e f_0.

> Potremmo anche costruire una funzione f che rappresenta il comportamento di A:
>
> $$f(x_1, x_2, \ldots, x_n) = \begin{cases} f_1(x_2, \ldots, x_n) & \text{se } x_1 = 1, \\ f_0(x_2, \ldots, x_n) & \text{se } x_1 = 0. \end{cases}$$

1.5. Forme normali

notazione

Chiamiamo “letterale” una variabile proposizionale o una negazione di una variabile proposizionale

È utile individuare alcune forme normali canoniche.

Def. 4: **Forma Normale Disgiuntiva**

Diciamo che A è in Forma Normale Disgiuntiva (**DNF**, *Disjunctive Normal Form*) se A è una disgiunzione di congiunzioni di letterali, ossia è nella forma seguente:

$$\bigvee_{i \leq n} \bigwedge_{j \leq m_i} A_{ij} = (A_{1,1} \wedge \cdots \wedge A_{1,m_1}) \vee \cdots \vee (A_{n,1} \wedge \cdots \wedge A_{n,m_n})$$

Def. 5: **Forma Normale Congiuntiva**

Diciamo che A è in Forma Normale Congiuntiva (**CNF**, *Conjunctive Normal Form*) se A è una disgiunzione di congiunzioni di letterali, ossia è nella forma seguente:

$$\bigwedge_{i \leq n} \bigvee_{j \leq m_i} A_{ij} = (A_{1,1} \vee \cdots \vee A_{1,m_1}) \wedge \cdots \wedge (A_{n,1} \vee \cdots \vee A_{n,m_n})$$

1.6. Equivalenza Logica

> Def. 6: **Equivalenza logica**
>
> Due formule $A, B \in$ PROP sono logicamente equivalenti ($A \equiv B$) quando, per ogni assegnamento α si ha $\alpha(A) = \alpha(B)$.

Introduciamo alcune regole utili per verificare l'equivalenza tra proposizioni.

Con un piccolo abuso di notazione, definiamo 1 e 0 come le formule per cui $\forall \alpha,\ \alpha(1) = 1$ e $\alpha(0) = 0$.

In questo modo, abbiamo:

Involuzione	$\neg\neg A \equiv A$
Assorbimento (con 0 e 1)	$A \vee 0 \equiv A$ $A \wedge 1 \equiv A$
Cancellazione	$A \vee 1 \equiv 1$ $A \wedge 0 \equiv 0$
Terzo escluso (*tertium non datur*)	$A \vee \neg A \equiv 1$ $A \wedge \neg A \equiv 0$
Leggi di De Morgan	$\neg(A \vee B) \equiv \neg A \wedge \neg B$ $\neg(A \wedge B) \equiv \neg A \vee \neg B$
Commutatività	$A \vee B \equiv B \vee A$ $A \wedge B \equiv B \wedge A$
Associatività	$A \vee (B \vee C) \equiv (A \vee B) \vee C$ $A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$
Distributività	$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$ $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
I teorema di assorbimento	$A \vee (A \wedge B) \equiv A$ $A \wedge (A \vee B) \equiv A$
II teorema di assorbimento	$A \vee (\neg A \wedge B) \equiv A \vee B$ $A \wedge (\neg A \vee B) \equiv A \wedge B$

Tabella 1.1: Principali leggi di equivalenza logica

1.7. Formalizzazioni in logica proposizionale

Il concetto di soddisfacibilità ci permette di usare insiemi di formule proposizionali per catturare determinate strutture matematiche.

Per esempio: sia X un insieme. Consideriamo il linguaggio proposizionale composto dalle variabili $p_{(x,y)}$ per ogni $(x, y) \in X \times X$, e consideriamo il seguente insieme T di proposizioni in questo linguaggio:

(1) $\neg p_{x,x}\ \ \forall x \in X$ (antiriflessività)

(2) $p_{x,y} \to \neg p_{y,x}\ \ \forall x \in X$ (asimmetria)

(3) $(p_{x,y} \wedge p_{y,z}) \to p_{x,z}\ \ \forall x, y, z \in X$ (transitività)

(4) $(p_{x,y} \vee p_{y,x}) \ \forall x \neq y \in X$ (ordine totale)

Usiamo una teoria T per poter gestire anche casi di insiemi infiniti. Infatti, sappiamo che una teoria infinita è soddisfatta se e solo se lo sono tutte le sue proposizioni.

L'insieme $T = T_X$ esprime il concetto di **ordine totale stretto** su X. Infatti, se avessimo un assegnamento α che soddisfa tutte le proposizioni di T, l'ordine indotto da tutte le variabili vere sotto α sarebbe un ordine totale stretto di X.

Se α è un assegnamento, definiamo la relazione $\prec_\alpha$ su X come segue:

$$x \prec_\alpha y \leftrightarrow \alpha(p_{x,y}) = 1$$

Si ha che per ogni assegnamento α che soddisfa T_X, l'ordine $\prec_\alpha$ indotto da α è un ordine totale stretto su X.

Dall'altra parte, se $\prec$ è un ordine totale stretto su X, e $\alpha_\prec$ è l'assegnamento indotto da $\prec$ così definito:

$$\alpha_\prec(p_{x,y}) = 1 \leftrightarrow (x \prec y)$$

Si ha che, per ogni ordine totale stretto $\prec$ su X, l'assegnamento $\alpha_\prec$ indotto da $\prec$ sulle variabili $p_{x,y}$ soddisfa T.

Ovvero, un assegnamento α soddisfa la teoria T_X se e solo se l'ordine indotto da α su X è un ordine totale.

1.7.1. Esempi di formalizzazioni di problemi noti in Logica Proposizionale

Colorabilità

Esempio: 2-colorabilità

Consideriamo il problema di colorare una mappa (grafo) con due colori (Rosso e Blu) in modo che nazioni confinanti abbiano colori diversi.

Per esempio:

- mappa M: Italia (I), Austria (A), Ungheria (U).
- variabili proposizionali: X_C indica che la nazione X ha il colore C.

Per modellare il problema in logica proposizionale, definiamo tre tipi di formule:

(1) *Ogni nazione ha almeno un colore:*

$$(I_R \vee I_B) \wedge (A_R \vee A_B) \wedge (U_R \vee U_B)$$

(2) *Ogni nazione ha al più un colore (unicità):*

$$(I_R \rightarrow \neg I_B) \wedge (A_R \rightarrow \neg A_B) \wedge (U_R \rightarrow \neg U_B)$$

(3) *Nazioni confinanti hanno colori diversi:*

$$(I_R \rightarrow \neg A_R) \wedge (I_B \rightarrow \neg A_B) \wedge (A_R \rightarrow \neg U_R) \wedge (A_B \rightarrow \neg U_B)$$

Esiste una corrispondenza biunivoca tra una colorazione valida e un assegnamento di verità che soddisfa la teoria:

- Una colorazione valida f induce un assegnamento α che soddisfa le formule (es. se I è rossa, $\alpha(I_R) = 1, \alpha(I_B) = 0$).

- Un assegnamento α che soddisfa le formule permette di ricostruire una colorazione valida.

La mappa M è quindi *2-colorabile* se e soltanto se l'insieme delle proposizioni è soddisfacibile.

La formalizzazione completa non è però la più "economica". Il vincolo di unicità del colore (punto 2 sopra) è conseguenza logica degli altri vincoli (punto 1 e punto 3).

$$\text{Vincolo (1)} \wedge \text{Vincolo (3)} \models \text{Vincolo (2)}$$

È quindi possibile omettere il secondo gruppo di formule senza alterare la soddisfacibilità.

Considerando Slovenia (S), Austria (A) e Ungheria (U):

- Queste tre nazioni sono tutte confinanti tra loro (formano un triangolo nel grafo).
- L'insieme delle proposizioni risulta *insoddisfacibile*.

  Infatti, se S è Rossa ($S_R = 1$), allora i vicini devono essere non-rossi ($A_R = 0, U_R = 0$). Poiché devono avere un colore, allora devono essere Blu ($A_B = 1, U_B = 1$). Ma A e U confinano, quindi non possono essere entrambi Blu. Contraddizione.

Formalizzazione della colorabilità di grafi

Sia $G = (V, E)$ un grafo e k il numero di colori disponibili $(1, \ldots, k)$. Definiamo le variabili $P_{v,i}$ che significano "il vertice v ha colore i".

L'insieme T di formule che formalizza il problema è:

(1) **Almeno un colore per ogni vertice:**

$$\bigvee_{i=1}^{k} P_{v,i} \quad \text{per ogni } v \in V$$

(2) **Al più un colore per ogni vertice (mutua esclusione):**

$$\neg(P_{v,i} \wedge P_{v,j}) \quad \text{per ogni } v \in V, \text{ con } i \neq j$$

(3) **Vincolo di adiacenza (colori diversi per archi):**

$$\neg(P_{v,i} \wedge P_{w,i}) \quad \text{per ogni arco } \{v, w\} \in E, \text{ per ogni colore } i$$

Teorema: Il grafo G ammette una k-colorazione se e solo se l'insieme di formule T è soddisfacibile. La colorazione è data da $c(v) = i \iff \alpha(P_{v,i}) = 1$.

Pigeonhole Principle

Il Principio dei Cassetti (Pigeonhole Principle, $PHP(m, n)$) afferma che se inseriamo m oggetti (piccioni) in n cassetti, con $m > n$, allora almeno un cassetto deve contenere più di un oggetto.

Consideriamo il caso con m piccioni e n cassetti. Definiamo le variabili proposizionali:

$$p_{i,j} \quad \text{con } i \in \{1, \ldots, m\} \text{ e } j \in \{1, \ldots, n\}$$

Il significato intuitivo di $p_{i,j}$ è: "l'oggetto i è nel cassetto j".

Per formalizzare il problema, costruiamo due tipi di proposizioni:

(1) **Ogni oggetto è in almeno un cassetto (Totalità)**

Per un singolo oggetto i, la disgiunzione di tutti i possibili cassetti deve essere vera:

$$(p_{i,1} \lor p_{i,2} \lor \cdots \lor p_{i,n})$$

Per tutti gli m oggetti, prendiamo la congiunzione:

$$A = \bigwedge_{i=1}^{m} \left(\bigvee_{j=1}^{n} p_{i,j} \right)$$

(2) **Ogni cassetto contiene al più un oggetto (Iniettività)**

Questa condizione esprime che non ci sono collisioni. Se questa condizione è vera, la funzione è iniettiva. Per ogni cassetto k, e per ogni coppia di oggetti distinti i e j, non è possibile che entrambi siano in k:

$$\neg(p_{i,k} \land p_{j,k}) \quad \text{equivalente a} \quad (\neg p_{i,k} \lor \neg p_{j,k})$$

Formalizziamo l'iniettività su tutto il dominio come la congiunzione di questi vincoli:

$$B = \bigwedge_{k=1}^{n} \bigwedge_{1 \le i < j \le m} (\neg p_{i,k} \lor \neg p_{j,k})$$

(3) **Il teorema**

Il principio afferma che se ogni oggetto è assegnato a un cassetto (formula A), allora l'assegnamento *non* può essere iniettivo (non B), dato che $m > n$. La formula che esprime il $PHP(m, n)$ è quindi:

$$A \to \neg B$$

(tautologia)

Spesso, nel contesto SAT, si cerca di dimostrare il principio per assurdo, cercando un assegnamento che renda vera la sua negazione. Cerchiamo cioè una situazione in cui tutti i piccioni sono assegnati (A) **e** l'assegnamento è iniettivo (B):

$$A \land B$$

In forma estesa:

$$\left(\bigwedge_{i=1}^{m} \bigvee_{j=1}^{n} p_{i,j} \right) \land \left(\bigwedge_{k=1}^{n} \bigwedge_{i \neq j} (\neg p_{i,k} \lor \neg p_{j,k}) \right)$$

Se $m > n$, questo insieme di formule è una insoddisfacibile, poiché non esiste alcun modo di mettere m piccioni in n cassetti senza collisioni.

1.8. Teorema di compattezza

Def. 7: Monotonia della conseguenza logica

Si dice che la nozione di conseguenza logica è **monotona**, ovvero che

$$T' \vDash A \land T' \subseteq T \implies T \vDash A$$

(se $A_1, A_2, \dots, A_k \vDash A$, allora $T \vDash A$ per ogni teoria T contenente $A_1, A_2, \dots, A_k$)

Nonostante non sembri intuitivamente vero, vale anche il viceversa:

Thm. 2: Teorema di compattezza v.1

Se $T \vDash A$, esiste un sottoinsieme finito T_0 di T tale che $T_0 \vDash A$

Introduciamo il concetto di una teoria finitamente soddisfacibile:

Def. 8: FINSAT

Una teoria si dice **finitamente soddisfacibile** ($\in$ FINSAT) se *ogni* suo sottoinsieme finito è soddisfacibile.

Possiamo quindi introdurre una nuova versione del teorema di compattezza:

Thm. 3: Teorema di compattezza v.2

FINSAT $\implies$ SAT, ovvero se ogni sottoinsieme di T è soddisfacibile, anche T è soddisfacibile.

Lemma 2: Teorema di compattezza v.1 $\equiv$ v.2

I due punti seguenti (le due versioni del teorema di compattezza) sono equivalenti:

(1) $T \vDash A \iff \exists\, T_0 \overset{fin}{\subseteq} T \; t.c.\; T_0 \vDash A$

(2) $T \in$ SAT $\iff T \in$ FINSAT

- ① $\implies$ ②

  Supponiamo per assurdo che $T \vDash A \implies \exists T_0 \overset{fin}{\subseteq} T \; t.c.\; T_0 \vDash A$, che $T \in$ FINSAT, ma che $T \notin$ SAT ($T \in$ UNSAT).

  Se $T \in$ UNSAT, possiamo dire che $T \vDash p \land \neg p$ (tutto è conseguenza logica di una teoria insoddisfacibile).

  Per ①, quindi, $\exists T_0 \; t.c.,\; T_0 \overset{fin}{\subseteq} T \vDash p \land \neg p$, il che va in contraddizione con $T \in$ FINSAT.

- ② $\implies$ ①

  Supponiamo per assurdo che $T \in$ FINSAT $\implies T \in$ SAT, e che $T \vDash A$ ma che $\forall T_0 \overset{fin}{\subseteq} T,\; T_0 \nvDash A$.

  $T_0 \nvDash A$ significa $T_0 \cup \{\neg A\} \in$ SAT.

  Preso un qualsiasi sottoinsieme finito $S \subseteq (T \cup \{\neg A\})$, questo sarà contenuto in un qualche $T_0 \cup \{\neg A\}$. Dato che ogni $T_0 \cup \{A\} \in$ SAT, anche $S \in$ SAT. Dunque, $T \cup \{\neg A\} \in$ FINSAT.

  Quindi, visto che FINSAT $\implies$ SAT, $T \cup \{\neg A\} \in$ SAT, il che va in contraddizione con l'ipotesi $T \vDash A$. □

Thm. 4: **Estendibilità di SAT**

Se T è soddisfacibile, allora $T \cup \{A\}$ è soddisfacibile oppure $T \cup \{\neg A\}$ è soddisfacibile.

dimostrazione dalle dispense

Sia α un assegnamento che soddisfa T. Se $\alpha(A) = 1$ allora $T \cup \{A\}$ è soddisfacibile. Se $\alpha(A) = 0$, $T \cup \{\neg A\}$ è soddisfacibile.

dimostrazione vista in classe

Supponiamo $T \in \texttt{SAT}$, $T \cup \{A\} \in \texttt{UNSAT}$ e $T \cup \{\neg A\} \in \texttt{UNSAT}$. Avremmo entrambi $T \vDash \{\neg A\}$ e $T \vDash A$, il che è impossibile se $T \in \texttt{SAT}$.

Un concetto analogo vale per FINSAT.

Thm. 5: **Estendibilità di FINSAT**

Sia $T \in \texttt{FINSAT}$. Per ogni formula A, $T \cup \{A\} \in \texttt{FINSAT}$ o $T \cup \{\neg A\} \in \texttt{FINSAT}$

Supponiamo per assurdo che $T \cup \{A\} \notin \texttt{FINSAT}$ e $T \cup \{\neg A\} \notin \texttt{FINSAT}$.

Vuol dire che esistono $B \overset{fin}{\subseteq} T \cup \{A\}$ e $C \overset{fin}{\subseteq} T \cup \{\neg A\}$ insoddisfacibili.

Dato che per ipotesi $T \in \texttt{FINSAT}$, sappiamo che $A \in B$, $\neg A \in C$ (altrimenti non potrebbero essere UNSAT, in quanto sarebbero solo $\subseteq T \in$ FINSAT). Possiamo quindi introdurre $\hat{B} = B \setminus \{A\}$ e $\hat{C} = C \setminus \{\neg A\}$.

Sappiamo che l'insieme $\hat{B} \cup \hat{C} \in \texttt{FINSAT}$, in quanto sottoinsieme finito di T.

Sia α un assegnamento che lo soddisfa. Se $\alpha(A) = 1$, allora soddisfa anche B. Se $\alpha(A) = 0$, soddisfa anche C. In entrambi i casi abbiamo una contraddizione.

1.8.1. Dimostrazione per i linguaggi numerabili

Sia T in un linguaggio numerabile. $T \in \texttt{FINSAT} \implies T \in \texttt{SAT}$.

Supponiamo $\mathcal{L} = \{p_1, p_2, \dots\}$ numerabile.

Definiamo una "catena" di teorie come segue:

- $T_0 = T$
- $T_1 = \begin{cases} T_0 \cup \{p_1\} & T_0 \cup \{p_1\} \in \texttt{FINSAT} \\ T_0 \cup \{\neg p_1\} & T_0 \cup \{\neg p_1\} \in \texttt{FINSAT} \end{cases}$

  $\vdots$
- $T_{n+1} = \begin{cases} T_n \cup \{p_{n+1}\} & T_0 \cup \{p_{n+1}\} \in \texttt{FINSAT} \\ T_n \cup \{\neg p_{n+1}\} & T_0 \cup \{\neg p_{n+1}\} \in \texttt{FINSAT} \end{cases}$

(aggiungiamo quindi proposizioni una alla volta in modo che T_i resti FINSAT)

(la definizione è ben posta per l'estendibilità di FINSAT)

Avremo quindi $T = T_0 \subseteq T_1 \subseteq T_2 \subseteq \dots$

Definiamo

$$T^* = \bigcup_{n \in \mathbb{N}} T_n$$

Sappiamo che $T^* \in$ FINSAT perché $\forall X = \{A_1, A_2, \dots, A_k\} \overset{fin}{\subseteq} T^*$, esiste n^* t.c. $X \subseteq T_{n^*}$.

(T è costruito come una catena crescente, quindi ogni suo sottoinsieme finito è un sottoinsieme di uno degli insiemi della catena - quello con "pedice massimo"; per esempio, se $X = \{A_1, A_2\}$ con $A_1 = \{p_1\},\ A_2 = \{p_3, p_5\}$, avremo $X \subseteq T_5$)

Visto che, per costruzione, $\forall p_n$ vale $(p_n \in T^* \oplus \neg p_n \in T^*)$, possiamo definire un assegnamento:

$$\alpha^*(p_n) = \begin{cases} 1 & p_n \in T^* \\ 0 & p_n \notin T^* \ (\neg p_n \in T^*) \end{cases}$$

Claim: $\alpha^*(T) = 1$

(avremmo $T \in$ SAT, quindi avremmo finito)

Dobbiamo quindi dimostrare che $\forall A \in T, \alpha^*(A) = 1$.

Abbiamo $A = \{p_{i1}, \dots, p_{i_k}\} \in T$.

Introduciamo la notazione: $p_n^* = \begin{cases} p_n & p_n \in T^* \ \ (\alpha^*(p_n) = 1) \\ \neg p_n & \neg p_n \in T^* \ \ (\alpha^*(p_n) = 0) \end{cases}$

Poiché $A \in T \subseteq T^*$ e $\{p_{i1}^*, \dots, p_{ik}^*\} \subseteq T^*$, abbiamo $A^* = A \cup \{p_{i1}^*, \dots, p_{ik}^*\} = \{A, p_{i1}^*, \dots, p_{ik}^*\} \overset{fin}{\subseteq} T^*$.

Dato che $T^* \in$ FINSAT, $\exists \beta$ t.c. $\beta(A^*) = 1$ (il che può succedere solo se $\beta(A) = 1 \ \wedge \ \beta(p_{ij}^*) = 1 \ \forall j \in [k]$).

Ma, poiché $\beta(p_{ij}^*) = 1 \ \forall j \in [k]$, notiamo che necessariamente $\beta(p_j) = 1$ se $p_j \in T^*$ e $\beta(p_j) = 0$ se $p_j \notin T^*$. Dunque, notiamo che β e α^* si comportano allo stesso modo per ogni variabile $p_{i1}, \dots, p_{ik}$.

Da questo (e dall'osservazione a fine pagina 5), poiché $p_{i1}, \dots, p_{ik}$ sono le variabili che compongono A, segue che $\beta(A) = \alpha^*(A)$.

Ma $\beta(A) = 1$ per scelta di β, quindi $\alpha^*(A) = 1$. Visto che possiamo applicare lo stesso ragionamento ad ogni $A \in T$, si ha che $\alpha^*(T) = 1$, ovvero $T \in$ SAT □

(ogni proposizione che va verificata, in quanto finita, riguarda solo un sottoinsieme di T, e crea quindi un "bottleneck")

1.8.2. Dimostrazione per i linguaggi arbitrari

Lemma 3: Lemma di Zorn

Sia X un insieme, e $\leq \subseteq X^2$ una relazione di **ordine parziale** (riflessiva, antisimmetrica e transitiva) su X. Definiamo, in X, i concetti di:

- catena C = sottoinsieme di X i cui elementi sono a due a due confrontabili via $\leq$
- maggiorante = elemento $x \in X$ t.c. $\forall y \in C,\ y \leq x$

Il **lemma di Zorn** afferma che, se per ogni catena C in X esiste un **maggiorante** in X, allora esiste un

elemento $m \in X$ **massimale**.

Il Lemma di Zorn è una forma dell'Assioma della Scelta (che, informalmente, afferma che quando viene data una collezione di insiemi non vuoti si può sempre costruire un nuovo insieme "scegliendo" un singolo elemento da ciascuno di quelli di partenza).

A noi basta considerare come relazione d'ordine l'inclusione insiemistica $\subseteq$ per la quale l'**unione è un maggiorante**.

Usiamo il Lemma di Zorn per dimostrare (il verso non banale de) il Teorema di Compattezza.

Lemma 4: **Lemma di Zorn per famiglie di insiemi**

Sia A un insieme e $\mathcal{P}(A)$ il suo insieme delle parti.

Sia $\mathcal{F} \subseteq \mathcal{P}(A)$ una famiglia di sottinsiemi di A.

Se per ogni **catena** $\mathcal{C}$ in $\mathcal{F}$ (i.e., per ogni famiglia di sottinsiemi di A appartenenti a $\mathcal{F}$ i cui elementi sono due a due confrontabili via $\subseteq$) esiste un **maggiorante** in $\mathcal{F}$ (ossia un sottinsieme S di A in $\mathcal{F}$ tale che per ogni $S' \in \mathcal{C}$ vale $S' \subseteq S$), allora esiste un sottinsieme **massimale** M di A in $\mathcal{F}$ (ossia $M \in \mathcal{F}$ tale che per ogni $S \in \mathcal{F}$, se $M \subseteq S$ allora $S = M$).

> Si osserva facilmente che se $\mathcal{F}$ contiene l'**unione** di ogni sua catena allora soddisfa le condizioni di applicabilità del lemma, in quanto l'unione risulta un maggiorante della catena.

Data $T \in \texttt{FINSAT}$, definiamo $\mathcal{T} = \{\hat{T} \mid T \subseteq \hat{T} \ \wedge \ \hat{T} \in \texttt{FINSAT}\}$, la famiglia di teorie FINSAT che estendono T. Sappiamo che $\mathcal{T} \neq \emptyset$, in quanto contiene almeno T.

Vogliamo verificare che $\mathcal{T}$ verifichi le condizioni per applicare il lemma di Zorn.

Sia $C = (T_i)$ una catena crescente. È evidente che $\bigcup_i T_i$ è un maggiorante, e anche che estende T. Sappiamo anche che è FINSAT. Infatti, se consideriamo un qualsiasi sottoinsieme finito di $\bigcup_i T_i$, ogni sua proposizione sarà un elemento di qualche elemento della catena; questo significa che l'insieme stesso è un sottoinsieme di un elemento della catena, ed è quindi FINSAT.

Applicando quindi il lemma di Zorn, otteniamo che $\mathcal{T}$ contiene un massimale T^*, ovvero una teoria tale che:

- $T \subseteq T^*$
- $T^* \in \texttt{FINSAT}$
- T^* non può essere propriamente esteso mantenendo la condizione di finita soddisfacibilità - ovvero $\forall T' \in \mathcal{T}, \ T^* \subseteq T' \implies T' = T^*$

In quanto massimale, T^* gode di alcune proprietà:

(1) data A, non può essere che $\neg A \in T^*$ e $A \in T^*$

(2) se $A \notin T^*$, necessariamente $\neg A \in T^*$ (altrimenti T^* potrebbe essere estesa con A o $\neg A$ senza perdere la finita soddisfacibilità)

(3) se $A \in T^*$ e $A \vDash B$, si ha $B \in T^*$ (T^* è chiuso per conseguenza logica)

(se $B \notin T^*$, si avrebbe $\neg B \in T^*$, ma dato che $A \vDash B$, si avrebbe $\{A, B\} \subseteq T^* \in \texttt{UNSAT}$, quindi $T^* \notin \texttt{FINSAT}$)

Come per la dimostrazione precedente, definiamo un assegnamento

$$\alpha^*(p_n) = \begin{cases} 1 & p_n \in T^* \\ 0 & \neg p_n \in T^* \end{cases}$$

Claim: $\alpha^*(T) = 1$

Dimostrare che α^* soddisfa T^* basta a dimostrare che soddisfa anche T.

Possiamo dimostrare una proprietà più forte: che $\forall A,\ \alpha(A) = 1 \iff A \in T^*$

Lavoriamo per induzione sulla struttura di A:

- **caso base**: $A = p_n$ - si ha $\alpha^*(p_n) = 1 \iff p_n \in T^*$
- **casi induttivi**:

(1) **NOT:** $A = \neg B$

$$\alpha^*(\neg B) = 1 \iff \alpha^*(B) = 0$$

Per l'ipotesi induttiva su B, sappiamo che $\alpha^*(B) = 0 \iff B \notin T^*$. Sfruttando la proprietà di massimalità di T^* (ogni formula o la sua negazione deve appartenere all'insieme):

$$B \notin T^* \iff \neg B \in T^*$$

Pertanto, $\alpha^*(\neg B) = 1 \iff \neg B \in T^*$.

(2) **AND:** $A = B \wedge C$

Dobbiamo mostrare che $\alpha^*(B \wedge C) = 1 \iff (B \wedge C) \in T^*$.

(⇒) Sia $\alpha^*(B \wedge C) = 1$. Per definizione di valutazione, questo implica $\alpha^*(B) = 1$ e $\alpha^*(C) = 1$. Per l'ipotesi induttiva, abbiamo $B \in T^*$ e $C \in T^*$. Supponiamo per assurdo che $(B \wedge C) \notin T^*$. Per la massimalità, allora $\neg(B \wedge C) \in T^*$. Consideriamo l'insieme finito $\{B, C, \neg(B \wedge C)\} \subseteq T^*$. Questo insieme è insoddisfacibile (UNSAT), il che contraddice il fatto che T^* sia FINSAT (finitamente soddisfacibile). Quindi deve essere $(B \wedge C) \in T^*$.

(⇐) Sia $(B \wedge C) \in T^*$. Dobbiamo mostrare che $B \in T^*$ e $C \in T^*$. Se $B \notin T^*$, allora $\neg B \in T^*$. L'insieme $\{B \wedge C, \neg B\} \subseteq T^*$ sarebbe UNSAT, impossibile. Quindi $B \in T^*$. Analogamente $C \in T^*$. Per ipotesi induttiva, $\alpha^*(B) = 1$ e $\alpha^*(C) = 1$, quindi $\alpha^*(B \wedge C) = 1$.

(3) **OR:** $A = B \vee C$

Dobbiamo mostrare che $\alpha^*(B \vee C) = 1 \iff (B \vee C) \in T^*$.

(⇒) Sia $\alpha^*(B \vee C) = 1$. Allora $\alpha^*(B) = 1$ oppure $\alpha^*(C) = 1$. Per ipotesi induttiva, $B \in T^*$ oppure $C \in T^*$. Supponiamo WLOG che $B \in T^*$. L'insieme $\{B, \neg(B \vee C)\}$ è insoddisfacibile. Poiché T^* è FINSAT e $B \in T^*$, non può contenere $\neg(B \vee C)$. Per massimalità, deve contenere $(B \vee C)$.

(⇐) Sia $(B \vee C) \in T^*$. Supponiamo per assurdo che $\alpha^*(B \vee C) = 0$. Questo implicherebbe $\alpha^*(B) = 0$ e $\alpha^*(C) = 0$. Per ipotesi induttiva, $B \notin T^*$ e $C \notin T^*$. Per massimalità, $\neg B \in T^*$ e $\neg C \in T^*$. Consideriamo l'insieme finito $\{(B \vee C), \neg B, \neg C\} \subseteq T^*$. Questo insieme è chiaramente insoddisfacibile, contraddicendo la proprietà `FINSAT`di T^*. Quindi l'ipotesi che la valutazione sia 0 è falsa, pertanto $\alpha^*(B \vee C) = 1$.

(4) **IMPLICAZIONE:** $A = B \to C$

Dobbiamo mostrare che $\alpha^*(B \to C) = 1 \iff (B \to C) \in T^*$.

($\Leftarrow$) Sia $(B \to C) \in T^*$. Se $\alpha^*(B \to C) = 0$, allora $\alpha^*(B) = 1$ e $\alpha^*(C) = 0$. Per ipotesi induttiva, $B \in T^*$ e $C \notin T^*$ (quindi $\neg C \in T^*$). Consideriamo l'insieme finito $\{(B \to C), B, \neg C\} \subseteq T^*$. Questo insieme è `UNSAT`(Modus Ponens contraddetto). Poiché T^* è `FINSAT`, non possiamo avere questa configurazione. Quindi $\alpha^*(B \to C)$ deve essere 1.

($\Rightarrow$) Sia $\alpha^*(B \to C) = 1$. Questo accade se $\alpha^*(B) = 0$ oppure $\alpha^*(C) = 1$.

- Se $\alpha^*(B) = 0 \implies B \notin T^* \implies \neg B \in T^*$. L'insieme $\{\neg B, \neg(B \to C)\}$ è `UNSAT`. Quindi $(B \to C) \in T^*$.
- Se $\alpha^*(C) = 1 \implies C \in T^*$. L'insieme $\{C, \neg(B \to C)\}$ è `UNSAT`. Quindi $(B \to C) \in T^*$.

Conclusione

Abbiamo mostrato che per ogni A, $\alpha^*(A) = 1 \iff A \in T^*$. Poiché $T \subseteq T^*$ e per ogni $A \in T^*$ vale $\alpha^*(A) = 1$, ne consegue che α^* soddisfa tutte le formule in T. Dunque T è soddisfacibile (`SAT`).

1.9. Applicazioni del teorema di compattezza

1.10. Decidibilità

Dato il potere espressivo della logica proposizionale, è naturale chiedersi se sia possibile automatizzare la risposta alla domanda "$T \vDash A$".

Se $T = \{A_1, \dots, A_n\}$ è una **teoria finita**, la risposta è banalmente "sì", in quanto sappiamo che $T \vDash A \iff (A_1 \wedge \dots \wedge A_n) \to A \in \texttt{TAUT}$ (il che è facilmente verificabile tramite tavole di verità).

> Def. 9: **Decidibilità**
>
> Dato uno spazio X di possibili input, chiamiamo un *problema* un qualsiasi sottoinsieme $S \subseteq X$.
>
> Diciamo che S è **algoritmicamente decidibile** se esiste un algoritmo tale che $\forall\ x \in X$, se $x \in S$, l'algoritmo su input x termina in tempo finito e risponde "sì", e se $x \in S$, l'algoritmo su input x termina in tempo finito e risponde "no".

Se invece T è una teoria **infinita numerabile**, potremmo usare il *teorema di compattezza* per fare un ragionamento del genere:

- Sappiamo che $T \vDash A \iff \exists\, T_0 \overset{fin}{\subseteq} T \ \ t.c.\ \ T_0 \vDash A$
- Indicando con $Fin(T)$ l'insieme dei sottoinsiemi finiti di T, sappiamo che $Fin(T)$ è numerabile (in quanto T lo è).
- Se potessimo quindi produrre algoritmicamente un'enumerazione di $Fin(T)$ del tipo $S_1, S_2, S_3, \dots$, poiché, grazie al teorema di compattezza, sappiamo che $\exists i \in \mathbb{N} \ \ t.c.\ \ S_i \vDash A$, potremmo seguire questa procedura:

  partendo da $i = 1$, ci chiediamo se $S_i \vDash A$. Poiché S_i è finito, si può rispondere algoritmicamente. Se la risposta è "sì", terminiamo la procedura e rispondiamo "sì". Altrimenti, ripetiamo con $i + 1$.

Se l'enumerazione di $Fin(T)$ si può produrre algoritmicamente, allora tutta la procedura è algoritmica. Notiamo però che, mentre nel caso in cui $T \vDash A$ sicuramente l'algoritmo terminerà e darà la risposta esatta, nel caso in cui $T \nvDash A$, esso non terminerà mai (visto che T è infinita).

Chiamiamo questo tipo di problema semi-decidibile.

> Def. 10: **Problema semi-decidibile**
>
> Dato uno spazio ambiente X e un problema $S \subseteq X$, diciamo che S è **semi-decidibile** se esiste un algoritmo tale che $\forall\ x \in X$, se $x \in S$, l'algoritmo (su input x) termina e risponde "sì"; se invece $x \notin S$, l'algoritmo (su input x) continua all'infinito (*diverge*).

> Def. 11: **Problema computabilmente enumerabile**
>
> Un insieme infinito per cui esiste una procedura algoritmica di enumerazione di tutti e soli i suoi elementi è detto **computabilmente enumerabile**.

(Notiamo che $\neg$(numerabile $\to$ computabilmente enumerabile))

> Thm. 6
>
> Se T è computabilmente enumerabile, allora il problema $T \vDash A$ è semi-decidibile.

Notiamo quindi che, se lo spazio X dei possibili input è computabilmente enumerabile, allora:

- ogni problema decidibile è anche semi-decidibile

- un problema è semi-decidibile se e solo se è computabilmente numerabile

Possiamo stabilire delle proprietà di T che ci garantiscano la decidibilità? La risposta è sì.

Consideriamo la procedura introdutta poco fa ed estendiamola in questo modo:

- ad ogni passo, controlliamo non solo $S_i \vDash A$, ma anche $S_i \vDash \neg A$
- se $S_i \vDash A$, terminiamo e rispondiamo "sì"; se $S_i \vDash \neg A$, terminiamo e rispondiamo "no"

Escludiamo le teorie per cui si ha $T \vDash A \land T \vDash \neg A$, in quanto sono "**incoerenti**" (ed insoddisfacibili).

Ci restano quindi tre casi:

(1) **Caso 1**: $T \models A$ e $T \not\models \neg A$: la procedura applicata a A termina e risponde affermativamente mentre la procedura applicata a $\neg A$ diverge. Possiamo concludere che $T \models A$.

(2) **Caso 2**: $T \not\models A$ e $T \models \neg A$: la procedura applicata a A diverge e la procedura applicata a $\neg A$ termina e risponde affermativamente. Possiamo comunque concludere che $T \models \neg A$. Se T non è insoddisfacibile, non può essere che $T \models A$. Dunque possiamo concludere e rispondere che $T \models A$.

(3) **Caso 3**: $T \not\models A$ e $T \not\models \neg A$: La procedura diverge quando viene applicata sia ad A che a $\neg A$. Questo caso esiste, ma vogliamo escluderlo.

Def. 12: Teoria semanticamente completa

Una teoria T è detta **semanticamente completa** se $\forall\ A$ nel linguaggio di T, vale esattamente una tra $T \vDash A$ e $T \vDash \neg A$.

Da questo possiamo derivare che:

Thm. 7

Se T è computabilmente enumerabile e semanticamente completa, allora $T \vDash A?$ è decidibile algoritmicamente $\forall\ A$.

Notiamo che le proprietà seguenti sono equivalenti:

(1) T è semanticamente completa.

(2) Per ogni formula A, vale $T \models A \iff T \not\models \neg A$.

(3) T è soddisfacibile e per ogni formula A se $T \not\models A$ allora $T \models \neg A$.

(4) T ha un unico modello.

(5) Per ogni formula A, B vale $T \models A \lor B$ se e solo se $T \models A$ oppure $T \models B$.

(6) Per ogni formula A, B vale $T \not\models A \to B$ se e solo se $T \models A$ e $T \models \neg B$.

1.11. Calcoli deduttivi formali

Una dimostrazione rigorosa è una successione ordinata e finita di asserzioni, ognuna delle quali può essere giustificata richiamandosi a una verità assunta come ipotesi (assioma), o a una regola di ragionamento corretta che permette di ottenerla da altre proposizioni.

La regola che utilizziamo nel nostro sistema di dimostrazioni ("alla Hilbert") è il **Modus Ponens**: da $X \wedge (X \to Y)$ segue Y.

Lo scriviamo in questo modo: $\dfrac{\mathrm{X} \qquad X \to Y}{\mathrm{Y}}$

> Def. 13: **Dimostrazione**
>
> Una **dimostrazione** / deduzione è una *successione finita* $F_1, \dots, F_k$ di proposizioni t.c., $\forall\, i \in [k]$:
>
> - F_i è un'istanza di un assioma, oppure
> - F_i si ottiene da due formule precedenti tramite regole di inferenza

Nel nostro sistema (in cui limitiamo il linguaggio ai connettivi $\neg$ e $\to$), scegliamo come assiomi:

> (1) $X \to (Y \to X)$
>
> (2) $(X \to (Y \to Z)) \to$
> $((X \to Y) \to (X \to Z))$
> (se X implica $Y \to Z$, allora $X \to Y$ implica $X \to Z$ (una sorta di transitività))
>
> (3) $(\neg Y \to \neg X) \to (X \to Y)$

Abbiamo scelto questo sistema perché vogliamo la completezza rispetto alla conseguenza logica. Vogliamo quindi che $\vDash A \iff A$ è dimostrabile da queste regole di inferenza e ipotesi in T.

> Def. 14: **Dimostrazione nel calcolo proposizionale**
>
> Una **dimostrazione** / deduzione di A da T nel C.P. è una *successione finita* $F_1, \dots, F_k$ di proposizioni t.c.:
>
> - $F_k = A$
> - $\forall\, i \in [k]$:
> - F_i è un'istanza di **assioma**
> - $F_i \in T$
> - $\exists\, p, q < i \quad t.c. \quad \dfrac{F_q \qquad F_p = F_q \to F_i}{F_i}$
> (è un'istanza del M.P.)

> Def. 15: **Teorema**
>
> A è un teorema se:
>
> $$\vdash A$$
>
> ovvero A è dimostrabile a partire "semplicemente" dagli assiomi.

Thm. 8: **Correttezza**

$$\vdash A \implies \vDash A$$
$$T \vdash A \implies T \vDash A$$

La dimostrazione è semplice: $\vdash A$ significa che A è dimostrabile a partire dagli assiomi logici (che sono verità logiche), e il Modus Ponens preserva le verità logiche (e il discorso è facilmente estendibile per $T \vdash A \implies T \vDash A$).

Se scriviamo $Teor(T) = \{A : T \vdash A\}$, la Correttezza si esprime insiemisticamente in questo modo:

$$Teor(T) \subseteq Cons(T)$$

ovvero, il nostro sistema permette di derivare formalmente dalle ipotesi di T solo *conseguenze logiche* di T.

1.12. Teorema di completezza

Thm. 9: **Teorema di completezza**

$$\vdash A \iff \vDash A$$
$$T \vdash A \iff T \vDash A$$

idea di dimostrazione ($T \vDash A \implies T \vdash A$):

Dal teorema di compattezza sappiamo che

$$\begin{aligned} T \vDash A &\iff \exists\{A_1, \dots, A_n\} \subseteq T \ \ t.c. \ \ A_1, \dots, A_n \vDash A \\ &\iff \vDash (A_1 \to (A_2 \to \dots (A_n \to A) \dots)) \end{aligned}$$

Dimostreremo che tutte le tautologie sono teoremi del calcolo proposizionale, e che quindi

$$\exists\{A_1, \dots, A_n\} \subseteq T \ \ t.c. \ \ \vdash (A_1 \to (A_2 \to \dots (A_n \to A) \dots))$$

Da questo vogliamo ottenere $T \vdash A$.

Lo faremo verificando che $\vdash (A_1 \to (A_2 \to \dots (A_n \to A) \dots)) \iff A_1, \dots, A_n \vdash A$.

1.12.1. Completezza Semplice

L'obiettivo di questa sezione è dimostrare che le verità logiche (tautologie) sono dimostrabili nel calcolo proposizionale.

$$\vDash B \implies \vdash B$$

Per farlo, utilizziamo un lemma fondamentale che collega la verità semantica (valutazioni α) alla dimostrabilità sintattica.

Lemma 5: **Lemma principale**

Sia B una formula contenente le variabili proposizionali $p_1, \dots, p_k$. Sia α un assegnamento di verità.

Definiamo la formula B^α come:

$$B^\alpha = \begin{cases} B & \text{se } \alpha(B) = 1 \\ \neg B & \text{se } \alpha(B) = 0 \end{cases}$$

(e analogamente per le variabili p_j^α). Allora vale sempre:

$$p_1^\alpha, \ldots, p_k^\alpha \vdash B^\alpha$$

Si procede per **induzione** sul numero n di connettivi logici $(\neg, \rightarrow)$ in B.

Base ($n = 0$): B è una variabile atomica p_i. La tesi diventa $p_i \vdash p_i$ (se $\alpha(p_i) = 1$) oppure $\neg p_i \vdash \neg p_i$ (se $\alpha(p_i) = 0$). Entrambe sono banalmente vere.

Passo Induttivo ($n > 0$): Supponiamo il lemma vero per formule con meno connettivi. Analizziamo la forma di B:

- **Caso $B = \neg C$:**
  - Se $\alpha(C) = 0$, allora $\alpha(B) = 1$. Per ipotesi induttiva $\Gamma \vdash C^\alpha$ cioè $\Gamma \vdash \neg C$. Ma B^α è B (cioè $\neg C$). Quindi $\Gamma \vdash B^\alpha$.
  - Se $\alpha(C) = 1$, allora $\alpha(B) = 0$. Per ipotesi induttiva $\Gamma \vdash C$. Dobbiamo dimostrare $\Gamma \vdash \neg B$ (cioè $\neg\neg C$). Usiamo il teorema $\vdash C \rightarrow \neg\neg C$.
- **Caso $B = C \rightarrow D$:** Si analizzano i valori di verità di C e D. Ad esempio, se $\alpha(C) = 1$ e $\alpha(D) = 0$, allora $\alpha(B) = 0$. Per ipotesi induttiva abbiamo $\Gamma \vdash C$ e $\Gamma \vdash \neg D$. Dobbiamo dimostrare $\Gamma \vdash \neg(C \rightarrow D)$. Questo segue dal teorema $C \rightarrow (\neg D \rightarrow \neg(C \rightarrow D))$.

Thm. 10: **Teorema di Completezza Semplice**

Se B è una tautologia, allora $\vdash B$.

Sia B una tautologia con variabili $p_1, \ldots, p_k$. Poiché è una tautologia, per *ogni* assegnamento α vale $\alpha(B) = 1$, quindi $B^\alpha = B$. Dal Lemma precedente segue che per ogni assegnamento α:

$$p_1^\alpha, \ldots, p_k^\alpha \vdash B$$

Consideriamo due assegnamenti α e β che differiscono solo per il valore di p_k:

- $\alpha(p_k) = 1 \implies p_1^\alpha, \ldots, p_{k-1}^\alpha, p_k \vdash B$
- $\beta(p_k) = 0 \implies p_1^\alpha, \ldots, p_{k-1}^\alpha, \neg p_k \vdash B$

Applicando il Teorema di Deduzione a entrambi:

$$\Gamma \vdash p_k \rightarrow B \quad \text{e} \quad \Gamma \vdash \neg p_k \rightarrow B$$

(dove $\Gamma = \{p_1^\alpha, \ldots, p_{k-1}^\alpha\}$).

Utilizzando il teorema noto $(A \rightarrow B) \rightarrow ((\neg A \rightarrow B) \rightarrow B)$, otteniamo:

$$p_1^\alpha, \ldots, p_{k-1}^\alpha \vdash B$$

Abbiamo eliminato la dipendenza da p_k. Iterando il procedimento per $k-1, k-2, \ldots, 1$, eliminiamo tutte le premesse e otteniamo infine:

$$\vdash B$$

1.12.2. Teorema di Deduzione

Il passaggio chiave per collegare la soddisfacibilità alla dimostrabilità è il Teorema di Deduzione, che ci permette di spostare le premesse all'interno della formula sotto forma di implicazione.

Thm. 11: **Teorema di Deduzione [Herbrand, 1930]**

Sia T un insieme di formule e A, B due formule. Allora:

$$T, B \vdash A \iff T \vdash (B \to A)$$

dim

Dobbiamo dimostrare la doppia implicazione.

Direzione 1: $T \vdash (B \to A) \implies T, B \vdash A$
Questa direzione è immediata.

(1) Sia $(G_1, \ldots, G_m)$ una derivazione di $B \to A$ a partire da T.

(2) Aggiungiamo B come nuova ipotesi (poiché ora lavoriamo in $T \cup \{B\}$).

(3) Avendo B e $B \to A$, per Modus Ponens otteniamo A.

(4) Dunque $T, B \vdash A$.

Direzione 2: $T, B \vdash A \implies T \vdash (B \to A)$
Sia $(F_1, \ldots, F_n)$ una derivazione di A (quindi $F_n = A$) a partire dalle premesse $T \cup \{B\}$. Dobbiamo dimostrare per induzione sull'indice i (lunghezza della derivazione) che $T \vdash (B \to F_i)$ per ogni $i = 1, \ldots, n$.

Base dell'induzione ($i = 1$): F_1 è l'inizio della derivazione. Ci sono tre casi:

- **Caso 1:** F_1 è un assioma logico oppure $F_1 \in T$.
  In questo caso $T \vdash F_1$ (senza bisogno di B). Utilizziamo l'assioma logico $F_1 \to (B \to F_1)$. Per Modus Ponens, otteniamo $T \vdash B \to F_1$.
- **Caso 2:** F_1 è proprio la formula B.
  Dobbiamo dimostrare $T \vdash B \to B$. Sappiamo che $\vdash B \to B$ è un teorema logico (già dimostrato precedentemente o verificabile dagli assiomi). Quindi a maggior ragione $T \vdash B \to B$.

Passo induttivo ($i > 1$): Supponiamo che la tesi valga per tutti i passi $k < i$. Analizziamo F_i:

- Se F_i è un assioma, un elemento di T o B, si procede come nel caso base.
- **Caso 3:** F_i è ottenuto per **Modus Ponens**.
  Significa che esistono $m, l < i$ tali che F_l è la formula $F_m \to F_i$. Per **ipotesi induttiva** sappiamo che:

  $$1)\ T \vdash B \to F_m$$
  $$2)\ T \vdash B \to (F_m \to F_i) \quad (\text{poiché } F_l = F_m \to F_i)$$

  Utilizziamo l'Assioma 2 (distributività dell'implicazione):

  $$(B \to (F_m \to F_i)) \to ((B \to F_m) \to (B \to F_i))$$

  Applicando il Modus Ponens due volte (usando le ipotesi induttive 1 e 2), concludiamo:

  $$T \vdash B \to F_i$$

Poiché $F_n = A$, l'induzione prova che $T \vdash B \to A$.

1.12.3. Conclusione del Teorema di Completezza

Grazie al Teorema di Deduzione, possiamo ora completare la strategia descritta all'inizio:

(1) Dal Teorema di Compattezza: $T \vDash A \implies \exists\{A_1, \dots, A_n\} \subseteq T$ tale che $A_1, \dots, A_n \vDash A$.

(2) Questo equivale a dire che $\vDash (A_1 \to (\cdots \to A) \dots)$ è una tautologia.

(3) Per la **Completezza Semplice** (le tautologie sono teoremi), abbiamo:

$$\vdash (A_1 \to (A_2 \to \dots (A_n \to A) \dots))$$

(4) Applicando n volte il **Teorema di Deduzione** (nella direzione $\Longleftarrow$), "scarichiamo" le premesse una alla volta:

$$A_1, A_2, \dots, A_n \vdash A$$

(5) Poiché $\{A_1, \dots, A_n\} \subseteq T$, per la proprietà di monotonia concludiamo:

$$T \vdash A$$

2 Logica Predicativa

2.1. Introduzione

Abbiamo visto come la logica proposizionale ci permette di modellare alcuni tipi di problemi facilmente. Tuttavia, per altri tipi di problemi è necessario un maggiore potere espressivo.

> Def. 16: **Struttura relazionale**
>
> Una struttura relazionale è una tupla $\mathcal{A} = (A,\ R_1, \ldots, R_n,\ f_1, \ldots, f_n,\ c_1, \ldots, c_n)$, dove:
>
> - A rappresenta un insieme di elementi (tipicamente non vuoto) (*dominio*)
> - $R_1, \ldots, R_n$ sono *relazioni* su A (anche unarie), ossia suoi sottoinsiemi
> - $f_1, \ldots, f_n$ sono *funzioni* su A
> - $c_1, \ldots, c_k$ sono *costanti* su A

Esempio: un esempio di struttura è quella di gruppo.

Un gruppo è definito da un insieme A (di elementi del gruppo), un elemento $e \in A$ (l'elemento neutro) e un'operazione binaria $\circ : A \times A \to A$, che soddisfa le seguenti proprietà:

(1) Per ogni $a \in A$, $a \circ e = e \circ a = a$

(2) Per ogni $a \in A$ esiste un $b \in A$ tale che $a \circ b = b \circ a = e$

(3) Per ogni $a, b, c \in A$: $a \circ (b \circ c) = (a \circ b) \circ c$.

(Un gruppo è inoltre abeliano se soddisfa: per ogni $a, b \in A$ si ha $a \circ b = b \circ a$.)

> Def. 17: **Linguaggio predicativo**
>
> Un **linguagggio predicativo** $\mathcal{L}$ è una collezione (finita o infinita) di simboli di tre tipi:
>
> - simboli di *relazioni*, con la loro arietà
> - simboli di *funzioni*, con la loro arietà
> - simboli di *costanti* (di arietà 0)
>
> Inoltre, assumiamo sempre un insieme numerabile di *variabili* $v_1, v_2, \ldots$

Esempio: per continuare con l'esempio di sopra, un linguaggio adeguato per la teoria dei ruppi è $\mathcal{L}_G = \{\cdot, e\}$, dove $\cdot$ è un simbolo di funzione binaria per l'operazione di gruppo, e e è una costante per l'elemento neutro.

> Nota bene
>
> Nella logica dei predicati, si può quantificare solo sugli *elementi* delle strutture e non sulle strutture stesse (si chiama, per questo, Logica di Primo Ordine o FOL, First-Order Logic).
>
> Per quantificare sulle strutture, esiste la Logica di Secondo Ordine (non trattata in questo corso).

Def. 18: Termini

I **termini** sono ottenuti partendo dalle variabili e dalle costanti e chiudendo sotto applicazione dei simboli di funzione.

Un termine che non contiene variabili è un **termine chiuso**.

Per formulare proposizioni nel linguaggio $\mathcal{L}$, si usano i seguenti simboli logici:

- **connettivi**: $\wedge, \vee, \rightarrow, \neg$
- **quantificatori**: $\exists, \forall$
- il simbolo di **eguaglianza**: $=$

Def. 19: Formule

Una **formula atomica** è una stringa del tipo $R(t_1, \ldots, t_k)$, dove R è un simbolo di relazione di arità k e $t_1, \ldots, t_k$ sono termini, oppure una stringa del tipo $t = s$, dove t e s sono termini.

Le **formule** sono ottenute partendo dalle formule atomiche e chiudendo sotto connettivi proposizionali e quantificatori universali ed esistenziali.

Nelle formule $(\forall v)F$ e $(\exists v)F$, F è detto il **dominio** (o *scope*) del quantificatore e v la variabile quantificata. Se v non occorre in F, possiamo identificare le due formule quantificate con F.

Un'occorrenza di una variabile x in una formula F è **vincolata** se e solo se:

- l'occorrenza di x è la variabile quantificata di un quantificatore, oppure
- l'occorrenza di x è nel dominio di un quantificatore con variabile quantificata

Tutte le altre occorrenze di x sono dette **libere**.

Un **enunciato** è una formula senza variabili libere.

Se F è una formula e $x_1, \ldots, x_n$ sono variabili distinte, indichiamo con $F(x_1, \ldots, x_n)$ il fatto che le variabili libere di F sono contenute nell'insieme $\{x_1, \ldots, x_n\}$.

Def. 20: Termine libero

Un termine t è **libero per una variabile** v in una formula F se nessuna occorrenza libera di v in F è nel dominio di un quantificatore $\forall y$ o $\exists y$ con y una variabile in t.

(ovvero, se si sostituisce v con t nella formula, nessuna delle variabili di t viene legata da un quantificatore presente in F)

Per esempio, se F è $\exists y(x = y + y)$, nessun termine contenente y è libero per x in F.

2.2. Semantica

Vogliamo poter definire il concetto di **verità logica** nella logica dei predicati (analogo a quello di tautologia nella logica proposizionale). A tale scopo, ci serve definire la nozione di verità di una formula della logica predicativa.

La verità di una formula della logica predicativa dipende dalla scelta dell'ambiente in cui decidiamo di interpretare i simboli del linguaggio. Un tale ambiente è detto **struttura**.

Def. 21: Struttura per un linguaggio $\mathcal{L}$

Dato un linguaggio $\mathcal{L}$, una **struttura** (o interpretazione) $\mathcal{A}$ per il linguaggio $\mathcal{L}$ consiste di:

- un insieme A non vuoto, detto **dominio**
- per ogni simbolo R_i di arietà d, una relazione di arietà d sul dominio A, che denotiamo con $R_i^{\mathcal{A}}$ dove $R_i^{\mathcal{A}} \subseteq A^d$
- per ogni simbolo f_j di arietà d, una funzione a d argomenti sul dominio A, che denotiamo con $f_i^{\mathcal{A}}$ dove $f_j^{\mathcal{A}} : A^d \to A$
- per ogni $k \in K$, un elemento di A che denotiamo con $c_k^{\mathcal{A}}$

Un **assegnamento** α in $\mathcal{A}$ è una mappa che associa ad ogni variabile un elemento di A, i.e.:

$$\alpha : \{v_n : n \in \mathbb{N}\} \to A$$

Un assegnamento si estende in modo univoco ai termini ponendo:

- $\alpha(c) = c^{\mathcal{A}}$
- $\alpha(f(t_1, \ldots, t_k)) = f^{\mathcal{A}}(\alpha(t_1), \ldots, \alpha(t_k))$.

Indichiamo con $\alpha\binom{x}{a}$ l'assegnamento che differisce da α solo perché associa l'elemento a alla variabile x.

Def. 22: Soddisfazione

Definiamo la relazione $\mathcal{A} \vDash F[\alpha]$, che significa "la formula F è soddisfatta nella struttura $\mathcal{A}$ relativamente all'assegnamento α"

La definiamo per induzione sulla complessità di F (semantica Tarskyana):

- $\mathcal{A} \vDash R(t_1, \ldots, t_k)[\alpha]$ se e solo se $(\alpha(t_1), \ldots, \alpha(t_k)) \in R^{\mathcal{A}}$, dove $t_1, \ldots, t_k$ sono termini e R è un simbolo di relazione di varietà k.
- $\mathcal{A} \vDash (t = s)[\alpha]$ se e solo se $\alpha(t) = \alpha(s)$, dove t e s sono termini.
- $\mathcal{A} \vDash \neg G[\alpha]$ se e solo se non vale $\mathcal{A} \vDash G[\alpha]$.
- $\mathcal{A} \vDash (G \wedge H)[\alpha]$ se e solo se $\mathcal{A} \vDash G[\alpha]$ e $\mathcal{A} \vDash H[\alpha]$.
- $\mathcal{A} \vDash (G \vee H)[\alpha]$ se e solo se $\mathcal{A} \vDash G[\alpha]$ o $\mathcal{A} \vDash H[\alpha]$.
- $\mathcal{A} \vDash (G \to H)[\alpha]$ se e solo se: se $\mathcal{A} \vDash G[\alpha]$ allora $\mathcal{A} \vDash H[\alpha]$.
- $\mathcal{A} \vDash (\exists x G)[\alpha]$ se e solo se esiste $a \in \mathcal{A}$ tale che $\mathcal{A} \vDash G[\alpha(x/a)]$.
- $\mathcal{A} \vDash (\forall x G)[\alpha]$ se e solo se per ogni $a \in \mathcal{A}$ vale $\mathcal{A} \vDash G[\alpha(x/a)]$.

Osservazione

Il fatto che valga $\mathcal{A} \vDash F[\alpha]$ dipende solo dai valori di α sulle variabili libere che appaiono in F. Quindi, come già visto in maniera simile per la logica proposizionale, se α e β sono due assegnamenti che coincidono sui valori assegnati alle variabili $x_1, \ldots, x_n$, allora $\mathcal{A} \vDash F[\alpha] \iff \mathcal{A} \vDash F[\beta]$.

Da questo segue che, se F è un **enunciato**, allora $\mathcal{A} \vDash F[\alpha]$ vale **per tutti gli assegnamenti o per nessuno**.

Def. 23: **Soddisfacibilità, Validità**

Se $\exists \alpha \;\; t.c. \;\; \mathcal{A} \vDash F[\alpha]$, diciamo che α *soddisfa* un enunciato E in $\mathcal{A}$. In questo caso, E è detto **soddisfacibile** in $\mathcal{A}$.

Diciamo che una formula F è **vera** in una struttura se *è soddisfatta da tutti gli assegnamenti* in quella struttura.

> Una formula F è vera in una struttura se e solo se l'enunciato
>
> $$\forall x_1, \ldots \forall x_n \; F(x_1, \ldots, x_n)$$
>
> (dove $x_1, \ldots, x_n$ sono tutte e sole le variabili libere di F) è vero nella struttura.

Un enunciato E è **valido** se è vero in tutte le strutture (ossia se $\forall \mathcal{A}, \; \mathcal{A} \vDash E$). In tal caso, scriviamo $\vDash E$.

Dualmente, E è *insoddisfacibile* se non esiste una struttura in cui è vero.

2.3. Teorie

Dato un linguaggio $\mathcal{L}$, ci interessa introdurre questi insiemi degni di nota:

- **Teoria** - una teoria è un insieme T di enunciati in $\mathcal{L}$
- **Modello** - un modello di una teoria è una struttura per $\mathcal{L}$ che *soddisfa tutti gli elementi di* T.

  scriviamo $\mathcal{A} \vDash T$

  e definiamo quindi $Mod(T) = \{\mathcal{A} : \mathcal{A} \vDash T\}$

  (nota: una teoria si dice *soddisfacibile* se ha un modello)
- **Conseguenza logica di una teoria** - E t.c. E è vero in tutti i modelli di T (diciamo che T *implica logicamente* E)

  definiamo coerentemente $Conseq(T) = \{E : T \vDash E\}$

Esempio: teoria dei gruppi

Un esempio è la teoria formata dagli assiomi di gruppo scritti in un linguaggio predicativo $\mathcal{L}_G = \mathcal{L}_{\text{Gruppi}}\{\circ, e\}$, dove $\circ$ è un simbolo di funzione di arietà due ed e è un simbolo di costante.

Gli assiomi della teoria di gruppo si esprimono con i seguenti enunciati:

$$\forall v_1 \forall v_2 \forall v_3 ((v_1 \circ v_2) \circ v_3 = v_1 \circ (v_2 \circ v_3))$$
$$\forall v_1 ((v_1 \circ e = v_1) \wedge (e \circ v_1 = v_1))$$
$$\forall v_1 \exists v_2 ((v_1 \circ v_2 = e) \wedge (v_2 \circ v_1 = e))$$

che formano la teoria dei gruppi T_G.

I modelli della teoria dei gruppi sono le strutture che chiamiamo gruppi, quindi si ha che $Mod(T_G) =$ insieme di tutti e soli i gruppi.

Gli enunciati che sono veri in qualunque gruppo formano l'insieme delle conseguenze logiche della teoria T_{Gruppi}, ossia $\{E : T_{\text{Gruppi}} \models E\}$. Le proprietà di un singolo gruppo G formano la "teoria di G" $\{E : G \models E\}$.

Si osserva facilmente che la teoria di una singola struttura $\mathcal{M}$ è sempre completa.

D'altra parte, l'insieme delle conseguenze logiche di una teoria T non è necessariamente completo (nel senso di contenere E o $\neg E$ per ogni possibile enunciato E). Per esempio, le conseguenze degli assiomi di gruppo (ossia la teoria T_{Gruppi}) non formano un insieme completo: dato che esistono gruppi abeliani e gruppi non-abeliani e dato che la proprietà di essere abeliano è esprimibile nel linguaggio dei gruppi con un enunciato predicativo ($C = \forall v_1 \forall v_2 (v_1 \circ v_2 = v_2 \circ v_1)$), esistono modelli di T_{Gruppi} che soddisfano C e modelli di T_{Gruppi} che non soddisfano C (ossia soddisfano $\neg C$). Dunque né C né $\neg C$ sono in $\text{Conseq}(T_{\text{Gruppi}})$ (né l'essere abeliano né l'essere non abeliano sono conseguenze degli assiomi di gruppo).

La teoria T_{Gruppi} è dunque incompleta.

2.4. Isomorfismi tra strutture

Se esiste un isomorfismo tra due strutture $\mathcal{A}$ e $\mathcal{B}$, significa che queste sono "indistinguibili", ovvero che hanno le stesse proprietà. È dunque vero che $\mathcal{A} \cong \mathcal{B} \implies \mathcal{A}$ e $\mathcal{B}$ soddisfano gli stessi enunciati? La risposta è sì (nel linguaggio per cui sono isomorfe).

Thm. 12: **Isomorfismo tra due strutture**

$\mathcal{A} \cong \mathcal{B} \implies \mathcal{A}$ e $\mathcal{B}$ **soddisfano le stesse formule**.

Sia h l'isomorfismo. Si ha quindi $\forall F(x_1, \dots, x_n),\ \forall (a_1, \dots, a_n) \in A^n$

$$\mathcal{A} \vDash F(x_1, \dots, x_n)[a_1, \dots, a_n] \iff \mathcal{B} \vDash F(x_1, \dots, x_n)[h(a_1), \dots, h(a_n)]$$

Lo dimostriamo per le formule, che sono una struttura induttiva (così che valga anche per gli enunciati).

- **caso base**:

  (1) $t_1 \leq t_2$

  $$\begin{gathered} \mathcal{A} \vDash (x \leq y)[a_1, a_2] \iff \mathcal{B} \vDash (x \leq y)[h(a_1), h(a_2)] \\ (a_1, a_2) \in \leq_A \iff (h(a_1), h(a_2)) \in \leq_B \\ \text{vero per def. di isomorfismo} \end{gathered}$$

  (2) $t_1 = t_2$

  $$\begin{gathered} \mathcal{A} \vDash (x = y)[a_1, a_2] \iff \mathcal{B} \vDash (x = y)[h(a_1), h(a_2)] \\ a_1 = a_2 \iff h(a_1) = h(a_2) \\ \text{vero per def. di isomorfismo} \end{gathered}$$

- **passo induttivo:** Assumiamo che la proprietà valga per le formule ϕ e ψ.

Sia $\vec{a} = (a_1, \ldots, a_n)$ la sequenza degli elementi in A e $h(\vec{a}) = (h(a_1), \ldots, h(a_n))$ la sequenza in B.

(1) **negazione ($\neg$)**:

$$\begin{aligned} &\mathcal{A} \models \neg\phi[\vec{a}] \\ \iff &\mathcal{A} \not\models \phi[\vec{a}] \quad \text{(def. di } \neg) \\ \iff &\mathcal{B} \not\models \phi[h(\vec{a})] \quad \text{(ip. ind. su } \phi) \\ \iff &\mathcal{B} \models \neg\phi[h(\vec{a})] \quad \text{(def. di } \neg) \end{aligned}$$

(2) **congiunzione ($\wedge$)**:

$$\begin{aligned} &\mathcal{A} \models (\phi \wedge \psi)[\vec{a}] \\ \iff &\mathcal{A} \models \phi[\vec{a}] \text{ e } \mathcal{A} \models \psi[\vec{a}] \quad \text{(def. di } \wedge) \\ \iff &\mathcal{B} \models \phi[h(\vec{a})] \text{ e } \mathcal{B} \models \psi[h(\vec{a})] \quad \text{(ip. ind. su } \phi \text{ e } \psi) \\ \iff &\mathcal{B} \models (\phi \wedge \psi)[h(\vec{a})] \quad \text{(def. di } \wedge) \end{aligned}$$

(3) **quantificazione ($\exists$)**: Sia ϕ con variabile libera y in aggiunta a $x_1, \ldots, x_n$.

$$\begin{aligned} &\mathcal{A} \models (\exists y\phi)[\vec{a}] \\ \iff &\exists c \in A \text{ tale che } \mathcal{A} \models \phi[\vec{a}, c] \quad \text{(def. di } \exists) \\ \iff &\exists c \in A \text{ tale che } \mathcal{B} \models \phi[h(\vec{a}), h(c)] \quad \text{(ip. ind. su } \phi) \end{aligned}$$

Poiché h è suriettiva, l'insieme $\{h(c) \mid c \in A\}$ è uguale all'insieme base B. Posto $b = h(c)$:

$$\begin{aligned} &\iff \exists b \in B \text{ tale che } \mathcal{B} \models \phi[h(\vec{a}), b] \\ &\iff \mathcal{B} \models (\exists y\phi)[h(\vec{a})] \quad \text{(def. di } \exists) \end{aligned}$$

(Il caso per $\forall$ segue da $\forall y\phi \equiv \neg\exists y\neg\phi$).

□

Passiamo ad un caso ancora più generale. Vogliamo mostrare che un isomorfismo tra due strutture

$$\begin{aligned} \mathcal{A} &= (A, \{R_i^A\}_{i\in I}, \{f_j^A\}_{j\in J}, \{c_k^A\}_{k\in K}) \\ \mathcal{B} &= (B, \{R_i^B\}_{i\in I}, \{f_j^B\}_{j\in J}, \{c_k^B\}_{k\in K}) \end{aligned}$$

preserva *l'intera struttura*.

Quindi

$$\begin{aligned} \mathcal{A} \cong \mathcal{B} \iff &\exists h : A \hookrightarrow\!\!\!\!\rightarrow B \text{ t.c.} \\ &\forall i \in I, j \in J, \ \forall (a_1, \ldots, a_t) \in A^t \\ \forall (a_1, \ldots, a_t) \in A^t, \ (a_1, \ldots, a_t) \in R_i^A &\iff (h(a_1), \ldots, h(a_t)) \in R_i^B \\ &h(f_j^A(a_1, \ldots, a_t)) = f_j^B(h(a_1), \ldots, h(a_t)) \end{aligned}$$

Vogliamo dimostrare che, per ogni termine t e ogni assegnazione α, il valore del termine t in $\mathcal{A}$ con assegnazione α, quando mappato dall'isomorfismo h, è uguale al valore del termine t in $\mathcal{B}$ con assegnazione $h(\alpha)$:

$$h(t^{\mathcal{A},\alpha}) = t^{\mathcal{B},h(\alpha)}$$

Si dimostra per induzione sulla struttura del termine t.

proof

(1) **Caso 1: t è una variabile ($t = x$)**

$$\begin{aligned} h(x^{\mathcal{A},\alpha}) &= h(\alpha(x)) && \text{(per def. di valutazione: } x^{\mathcal{A},\alpha} = \alpha(x)) \\ x^{\mathcal{B},h(\alpha)} &= h(\alpha)(x) && \text{(per def. di valutazione in } \mathcal{B} \text{ con assegnazione } h(\alpha)) \end{aligned}$$

Per definizione dell'assegnazione $h(\alpha)$, si ha $h(\alpha)(x) = h(\alpha(x))$. Quindi, l'uguaglianza è soddisfatta:

$$h(x^{\mathcal{A},\alpha}) = h(\alpha(x)) = h(\alpha)(x) = x^{\mathcal{B},h(\alpha)}$$

(2) **Caso 2: t è una costante ($t = c$)**

(in questo caso α non ha impatto - non ci sono assegnazioni)

$$\begin{aligned} h(c^{\mathcal{A},\alpha}) &= h(c^{\mathcal{A}}) && \text{(la valutazione di } c \text{ è l'interpretazione } c^{\mathcal{A}}) \\ &= c^{\mathcal{B}} && \text{(poiché } h \text{ è un isomorfismo, preserva le costanti)} \\ c^{\mathcal{B},h(\alpha)} &= c^{\mathcal{B}} && \text{(la valutazione di } c \text{ è l'interpretazione } c^{\mathcal{B}}) \end{aligned}$$

Quindi, l'uguaglianza è soddisfatta:

$$h(c^{\mathcal{A},\alpha}) = c^{\mathcal{B}} = c^{\mathcal{B},h(\alpha)}$$

(3) **Caso 3: t è una funzione ($t = f(t_1, \ldots, t_p)$)**

$$\begin{aligned} h(t^{\mathcal{A},\alpha}) &= h(f(t_1, \ldots, t_p)^{\mathcal{A},\alpha}) \\ &= h(f^{\mathcal{A}}(t_1^{\mathcal{A},\alpha}, \ldots, t_p^{\mathcal{A},\alpha})) && \text{(def. di valutazione di termine funzione)} \\ &= f^{\mathcal{B}}(h(t_1^{\mathcal{A},\alpha}), \ldots, h(t_p^{\mathcal{A},\alpha})) && (h \text{ isomorfismo, preserva la funzione } f) \\ &= f^{\mathcal{B}}(t_1^{\mathcal{B},h(\alpha)}, \ldots, t_p^{\mathcal{B},h(\alpha)}) \\ &= f(t_1, \ldots, t_p)^{\mathcal{B},h(\alpha)} && \text{(def. di valutazione di termine funzione in } \mathcal{B}) \\ &= t^{\mathcal{B},h(\alpha)} \end{aligned}$$

La proprietà è dimostrata per tutti i termini. □

Corollary for Thm. 12: Equivalenza elementare

Si ha quindi che $\mathcal{A} \cong \mathcal{B} \implies \mathcal{A} \equiv \mathcal{B}$ ("elementarmente equivalenti")

ovvero, $\mathcal{A}$ e $\mathcal{B}$ soddisfano gli stessi enunciati.

Thm. 13: **Equivalenza elementare su domini finiti**

In generale, non vale $\mathcal{A} \equiv \mathcal{B} \implies \mathcal{A} \cong \mathcal{B}$. Vale però se $\mathcal{A}$ e $\mathcal{B}$ finite e $\mathcal{L}$ ha solo simboli di relazione.

dim grafi

2.5. La teoria DLO

2.5.1. Numeri razionali

Prendiamo la struttura $\mathcal{Q} = (\mathbb{Q}, \leq)$. Le proprietà di questa struttura si possono esprimere in enunciati predicativi nel linguaggio $\mathcal{L} = \{\leq (x, y)\}$, per il quale, per comodità, usiamo la notazione infissa $x \leq y$.

Aggiungiamo anche $x < y$ come abbreviazione di $(x \leq y) \wedge \neg(x = y)$.

Le proprietà di $Q, \leq$ sono le seguenti:

(1) (A1 - Riflessività) $\forall x\ (x \leq x)$,

(2) (A2 - Transitività) $\forall x \forall y \forall z\ ((x \leq y \wedge y \leq z \to x \leq z)$,

(3) (A3 - Antisimmmetria) $\forall x \forall y\ ((x \leq y \wedge y \leq x) \to y = x)$,

(4) (A4 - Totalità) $\forall x \forall y\ (x \leq y \vee x \leq y)$,

(5) (A4 - Illimitato a destra) $\forall x \exists y\ (x < y)$,

(6) (A5 - Illimitato a sinistra) $\forall x \exists y\ (y < x)$,

(7) (A6 - Densità) $\forall x \forall y (x < y \to \exists z (x < z \wedge z < y))$.

Chiamiamo questa teoria **DLO** (*Dense Linear Order*).

Thm. 14: Q e DLO

$\mathbb{Q}$ è l'*unico ordine lineare denso numerabile senza estremi* a meno di isomorfismi.

2.5.1.1. Isomorfismo: caso numerabile

Thm. 15: Isomorfismo: caso numerabile

Sia $\mathcal{B} = (B, \leq_B)$ una struttura con dominio B numerabile e $\leq_B$ un ordine totale denso senza estremi su B. Allora esiste un isomorfismo tra $\mathcal{B}$ e $\mathcal{Q}$.

Vogliamo dimostrare che *ogni struttura* dove B è numerabile e $\preceq$ è un ordine totale denso senza estremi su A è isomorfa a $(\mathbb{Q}, \leq)$.

È naturale definire l'isomorfismo così: $\mathcal{B} \cong \mathcal{Q} \iff \exists h : \mathbb{Q} \hookrightarrow\!\!\!\!\rightarrow B$ t.c. $\forall q, q' \in \mathbb{Q}$

$$q \leq q' \iff h(q) \leq_B h(q')$$

$$q = q' \iff h(q) = h(q')$$

La dimostrazione usa un metodo chiamato *Back-and-Forth*.

proof

Vogliamo costruire un isomorfismo tra $\mathcal{B}$ e $\mathcal{Q}$.

Entrambe hanno un dominio numerabile, quindi fissiamo una enumerazione di B $(b_0, b_1, b_2, \dots)$ e una enumerazione di $\mathbb{Q}$ $(q_0, q_1, q_2, \dots)$.

Definiremo ricorsivamente una enumerazione $p_1, p_2, p_3, \dots$ e una enumerazione $d_1, d_2, d_3, \dots$ in modo tale che la mappa $p_i \mapsto d_i$ sia un isomorfismo tra $\mathcal{B}$ e $\mathcal{Q}$.

Per induzione:

- Poniamo $p_0 = b_0$ e $d_0 = q_0$.
- Consideriamo un n generico e assumiamo che $p_0, \dots, p_n$ e $d_0, \dots, d_n$ siano definiti.

  Distinguiamo due casi:

  (1) Caso **pari**: scegliamo un elemento p_{n+1} in $B \setminus \{p_0, \dots, p_n\}$ con indice minimo in $(b_0, b_1, b_2, \dots)$. Compariamo questo elemento agli elementi già scelti.
  Abbiamo tre casi:
  - (Prima di tutti gli altri elementi)
    Per ogni $m \leq n$, $p_{n+1} < p_m$. In questo caso scelgo un q_{n+1} in $\mathbb{Q}$ tale che per ogni $m \leq n$ abbiamo $d_{n+1} < d_m$. Questo elemento esiste perché $\mathbb{Q}$ soddisfa gli assiomi che asseriscono la *non esistenza di estremi* nell'ordine.
    (Scelgo un elemento da $\mathbb{Q}$ che sia anch'esso prima di tutti gli altri)
  - (Dopo tutti gli altri elementi)
    Per ogni $m \leq n$, $d_{n+1} > d_m$. In questo caso scelgo un q_{n+1} in $\mathbb{Q}$ tale che per ogni $m \leq n$ valga $d_{n+1} > d_m$. Questo elemento esiste perché $\mathbb{Q}$ soddisfa l'assioma che *esclude l'esistenza di un estremo destro* nell'ordine.
    (Scelgo un elemento da $\mathbb{Q}$ che sia anch'esso dopo tutti gli altri)
  - (Da qualche parte nel mezzo)
    Nessuno dei primi due casi. Allora esistono $m_0, m_1 \leq n$ tali che $p_{m_0} < p_{n+1} < p_{m_1}$ e nessun altro elemento di $\{p_0, p_1, \dots, p_n\}$ è nell'intervallo $[p_{m_0}, d_{m_1}]$. In questo caso scelgo un elemento d_{n+1} in $\mathbb{Q}$ tale che $d_{m_0} < d_{n+1} < d_{m_1}$. Questo elemento esiste perché $\mathbb{Q}$ soddisfa l'assioma di *densità*.
    (Scelgo un elemento da $\mathbb{Q}$ che sia anch'esso in mezzo agli altri)

  (2) Caso **dispari**: procediamo allo stesso modo, ma partendo da un elemento $q_{n+1} \in \mathbb{Q} \setminus \{q_0, \dots, q_n\}$.

Grazie alla separazione in passi pari e dispari (poiché scegliamo sia a partire da B che da $\mathbb{Q}$), non ci saranno "buchi" nelle nostre scelte di elementi.

Notiamo che nella dimostrazione non servono proprietà di $\mathbb{Q}$ se non quelle di DLO (e l'ipotesi di numerabilità del dominio). Il teorema si può quindi generalizzare.

Thm. 16: **Teorema di isomorfismo di Cantor**

Siano $\mathcal{A} = (A, \leq_A)$ e $\mathcal{B} = (B, \leq_B)$ t.c. A, B sono entrambi numerabili e $\mathcal{A} \vDash$ DLO e $\mathcal{B} \vDash$ DLO. Allora, $\mathcal{A} \cong \mathcal{B}$.

2.6. DLO: caso generale

Ci chiediamo: data una struttura $\mathcal{D} = (D, \leq_D) \vDash$ DLO con D più che numerabile, $\mathcal{D} \overset{?}{\equiv} \mathcal{Q}$ - ovvero, per esempio, esiste un enunciato nel linguaggio degli ordini vero in $\mathbb{Q}$ e falso in $\mathbb{R}$? (Se potessimo scrivere la completezza di $\mathbb{R}$ in linguaggio degli ordini, allora questo sarebbe sicuramente vero (in quanto $\mathbb{Q}$ non è completo) - ma non è possibile farlo).

Vogliamo quindi individuare un **criterio sufficiente** a concludere $\mathcal{Q} \equiv \mathcal{R}$.

2.6.1. Sottostrutture, proprietà del testimone

Introduciamo come prima cosa il concetto di sottostruttura:

Def. 24: Sottostruttura

Date due strutture $\mathcal{A}$ e $\mathcal{B}$, $\mathcal{A}$ si dice **sottostruttura** di $\mathcal{B}$ ($\mathcal{A} \subseteq \mathcal{B}$) se e solo se si ha:

- $A \subseteq B$
- per ogni simbolo R di relazione, $R^{\mathcal{A}} = R^{\mathcal{B}} \cap A^n$ (dove n arità di R)
- per ogni simbolo di costante, $c^{\mathcal{B}} \in A$ e $c^{\mathcal{A}} = c^{\mathcal{B}}$
- per ogni simbolo di funzione, $f^{\mathcal{A}} = f^{\mathcal{B}}|_A^n$ (con n arietà di f)

Def. 25: Sottostruttura elementare

Date due strutture $\mathcal{A}$ e $\mathcal{B}$, $\mathcal{A}$ si dice **sottostruttura elementare** di $\mathcal{B}$ ($\mathcal{A} \prec \mathcal{B}$) se e solo se si ha:

$$A \subseteq B \ \wedge \ \forall F, \forall \vec{a} \in A, \ \ \mathcal{A} \vDash F[\vec{a}] \iff \mathcal{B} \vDash F[\vec{a}]$$

(ovvero $\mathcal{A} \subseteq \mathcal{B}$ e $\mathcal{A} \equiv \mathcal{B}$).

Notiamo che $\mathcal{Q} \subseteq \mathcal{R}$.

Data una formula F, è naturale che se α è un assegnamento in $\mathbb{Q}$ e $\mathcal{Q} \vDash \exists x F[\alpha]$, allora $\mathcal{R} \vDash \exists x F[\alpha]$.

Non è però detto che valga l'inverso, ossia:

Thm. 17: Proprietà del testimone tra $\mathcal{R}$ e $\mathcal{Q}$

Per ogni formula F con x variabile libera, *per ogni assegnamento* α in $\mathbb{Q}$, se

$$\mathcal{R} \vDash \exists x \ F(x)[\alpha]$$

allora $\exists q \in \mathbb{Q}$ tale che:

$$\mathcal{R} \vDash F(x)[\alpha \left(\begin{smallmatrix} x \\ q \end{smallmatrix}\right)]$$

(quindi, abbiamo una formula F con tutte le variabili in $\mathbb{Q}$ tranne una; presumiamo che sia vera con l'ultima variabile assegnata in $\mathbb{R}$ - allora vogliamo che $\exists q \in \mathbb{Q}$ (da assegnare all'ultima variabile) che la soddisfi)

La proprietà del testimone è la condizione sufficiente per dedurre $\mathcal{Q} \equiv \mathcal{R}$.

Come già visto, conviene dimostrare la proprietà per le formule (così che valga anche per gli enunciati).

Corollary for Thm. 17: Conseguenza della proprietà del testimone

Se vale la proprietà del testimone tra $\mathcal{R}$ e $\mathcal{Q}$, allora $\forall F, \forall \alpha$ su Q,

$$\mathcal{Q} \vDash F[\alpha] \iff \mathcal{R} \vDash F[\alpha]$$

proof

Si dimostra per induzione su F.

- **caso base**: F è di tipo $(x \leq y)$.

$$\mathcal{Q} \vDash (x \leq y)[\alpha] \iff \mathcal{R} \vDash (x \leq y)[\alpha]$$
$$\alpha(x) \leq_{\mathbb{Q}} \alpha(y) \iff \alpha(x) \leq_{\mathbb{R}} \alpha(y)$$

  (argomento analogo per $(x = y)$)

- **booleani**:

$$\mathcal{Q} \vDash A \wedge B[\alpha] \iff \mathcal{R} \vDash A \wedge B[\alpha]$$
$$\mathcal{Q} \vDash A[\alpha] \wedge \mathcal{Q} \vDash B[\alpha] \iff \mathcal{R} \vDash A[\alpha] \wedge \mathcal{R} \vDash B[\alpha]$$

  Vero per ipotesi induttiva su A e B:

$$\mathbb{Q} \models A[\alpha] \iff \mathbb{R} \models A[\alpha] \quad \text{e} \quad \mathbb{Q} \models B[\alpha] \iff \mathbb{R} \models B[\alpha]$$

  (argomento analogo per gli altri connettivi booleani)

- **esistenziale**:

  Sia $F \equiv \exists x\, F(x)$. Assumiamo che la tesi valga per la formula $F(x)$ (I.I.). Dobbiamo mostrare che:

$$\mathbb{Q} \vDash \exists x\, F(x)[\alpha] \iff \mathbb{R} \vDash \exists x\, F(x)[\alpha]$$

  Direzione $\Longrightarrow$ *:* Assumiamo $\mathbb{Q} \vDash \exists x\, F(x)[\alpha]$. Per definizione, vale sse esiste un elemento $q \in \mathbb{Q}$ tale che $\mathbb{Q} \vDash F(x)[\alpha\,(\,{}^{x}_{q}\,)]$. Poiché l'assegnazione $\alpha\,(\,{}^{x}_{q}\,)$ è in $\mathbb{Q}$, per I.I. applicata a $F(x)$:

$$\mathbb{Q} \vDash F(x)[\alpha\,(\,{}^{x}_{q}\,)] \iff \mathbb{R} \vDash F(x)[\alpha\,(\,{}^{x}_{q}\,)]$$

  Poiché $q \in \mathbb{Q}$ e $\mathbb{Q} \subseteq \mathbb{R}$, q è un elemento di $\mathbb{R}$. Per definizione di soddisfacibilità in $\mathbb{R}$:

$$\mathbb{R} \vDash \exists x\, F(x)[\alpha]$$

  Direzione $\Longleftarrow$ *:* Assumiamo $\mathbb{R} \vDash \exists x\, F(x)[\alpha]$, con α assegnamento in $\mathbb{Q}$. Per definizione, vale sse $\exists r \in \mathbb{R}$ t.c. $\mathcal{R} \vDash F(x)\,(\,{}^{x}_{r}\,)$ Per la *proprietà del testimone*, se $\mathbb{R} \vDash \exists x\, F(x)[\alpha]$, allora esiste un testimone $q \in \mathbb{Q}$ tale che $\mathbb{R} \vDash F(x)[\alpha\,(\,{}^{x}_{q}\,)]$. Per ipotesi induttiva su F, questo vale sse $\exists q \in \mathbb{Q}$ t.c. $\mathcal{Q} \vDash F(x)[\alpha\,(\,{}^{x}_{q}\,)]$. Ovvero:

$$\mathbb{R} \vDash F(x)[\alpha\,(\,{}^{x}_{q}\,)] \iff \mathbb{Q} \vDash F(x)[\alpha\,(\,{}^{x}_{q}\,)]$$

  Quindi $\mathbb{Q} \vDash F(x)[\alpha\,(\,{}^{x}_{q}\,)]$. Poiché esiste un $q \in \mathbb{Q}$ che soddisfa $F(x)$ in $\mathbb{Q}$, per definizione (di soddisfacibilità):

$$\mathbb{Q} \vDash \exists x\, F(x)[\alpha]$$

□

Corollary for Thm. 17: Altra conseguenza della proprietà del testimone

Quindi, se vale la proprietà del testimone tra $\mathcal{Q}$ e $\mathcal{R}$, per ogni enunciato E nel linguaggio degli ordini si ha:

$$\mathcal{Q} \vDash E \iff \mathcal{R} \vDash E$$

ovvero $\mathcal{Q} \equiv \mathcal{R}$, e quindi $\mathcal{Q} \prec \mathcal{R}$.

2.6.2. Equivalenza tra $\mathcal{R}$ e $\mathcal{Q}$

Per dimostrare $\mathcal{Q} \equiv \mathcal{R}$, definiamo $\mathcal{A} = (A, \leq_A)$ t.c. $\mathcal{Q} \subseteq \mathcal{A} \subseteq \mathcal{R}$ e A numerabile.

Seguiremo quindi questi passi:

(1) dimostreremo la proprietà del testimone tra $\mathcal{A}$ e $\mathcal{R}$, ottenendo $\mathcal{A} \equiv \mathcal{R}$

(2) visto che $\mathcal{R} \vDash$ DLO e (1), si ha $\mathcal{A} \vDash$ DLO

(3) da (2) e A numerabile, applicando il Teorema di Cantor (p.34) si ottiene $\mathcal{A} \cong \mathcal{Q}$

(4) visto che $\cong \implies \equiv$, si ha $\mathcal{A} \equiv \mathcal{Q}$

(5) per transitività, $\mathcal{R} \equiv \mathcal{Q}$.

Costruiamo quindi $\mathcal{A}$ partendo da $\mathcal{Q}$.

Sia F una formula del linguaggio DLO e siano x_1, x_2, y le sue variabili libere.

Se $\mathcal{R} \vDash \exists y F(x_1, x_2, y) \begin{bmatrix} x_1 & x_2 \\ q_1 & q_2 \end{bmatrix}$, per definizione di soddisfacibilità sappiamo che

$\exists r \in \mathbb{R}$ t.c. $\mathcal{R} \vDash F(x_1, x_2, y) \begin{bmatrix} x_1 & x_2 & y \\ q_1 & q_2 & r \end{bmatrix}$. Ne scegliamo uno in modo canonico (usiamo implicitamente l'assioma della scelta).

> Def. 26: **Funzione di Skolem**
>
> Chiamiamo **funzione di Skolem** (da Thoralf Skolem) della formula F relativamente ad y la funzione
>
> $$f_{F,y} : \mathcal{Q}^n \to \mathcal{R}$$
>
> che associa ad ogni scelta di $(q_1, \ldots, q_n)$ un tale $r \in \mathbb{R}$ in modo canonico.

Dato $\mathcal{F} = \{\text{funzioni di Skolem}\}$, chiudiamo $\mathbb{Q}$ sotto $\mathcal{F}$.

Otteniamo $A_1 = \mathbb{Q} \cup \{b \in \mathbb{R} \mid b = f(q_1, \ldots, q_n) \text{ con } f \in \mathcal{F},\ (q_1, \ldots, q_n) \in Q^n\}$.

Sappiamo che $\mathcal{Q} \subseteq \mathcal{A}_1 = (A_1, \leq_A) \subseteq \mathcal{R}$.

È però vero che se x_1, x_2 sono assegnati in A_1 come a_1, a_2 allora esiste un $a \in A_1$ t.c.
$\mathcal{R} \vDash F(x_1, x_2, y) \begin{bmatrix} x_1 & x_2 & y \\ a_1 & a_2 & a \end{bmatrix}$? Non necessariamente. Infatti, se $a_1, a_2 \in \mathbb{Q}$, sicuramente sì.

Ma, se $a_1, a_2 \in \mathcal{A}_1 \setminus \mathcal{Q}$, non possiamo saperlo per certo. Dobbiamo quindi chiudere nuovamente sotto $\mathcal{F}$.

Non ci basta però chiudere un'altra volta, in quanto il problema si ripropone. Dobbiamo ripetere l'operazione $\forall i \geq 0$.

Abbiamo quindi

$$A_{i+1} = A_i \cup \mathcal{F}(A_i)$$

(utilizziamo la notazione $\mathcal{F}(A)$ per indicare la chiusura di A su F)

Definiamo

$$A = \bigcup_{i \in \mathbb{N}} A_i$$

Si vede che A è chiuso sotto funzione di Skolem.
Infatti, se $a_1, \ldots, a_n \in A_k$ e $f \in \mathcal{F}$ allora $f(a_1, \ldots, a_n) \in A_{k+1}$.

$\mathcal{A} = (A = \bigcup_{i \in \mathbb{N}} A_i, \leq_A)$ ha anche la Proprietà del Testimone relativamente ad $\mathcal{R}$.

Ovvero, se

$$\mathcal{R} \vDash \exists y F(x_1, x_2, y) \begin{bmatrix} x1 & x2 \\ a_1 & a_2 \end{bmatrix} \quad a_1, a_2 \in A$$

allora $\exists a \in A$ t.c.

$$\mathcal{R} \vDash F(x_1, x_2, y) \begin{bmatrix} x1 & x2 & y \\ a_1 & a_2 & a \end{bmatrix}$$

[caso generale: $\forall F, \forall \alpha \in A$, se:

$$\mathcal{R} \vDash \exists x F(x)[a]$$

allora $\exists a \in A$ t.c.:

$$\mathcal{A} \vDash F(x)\,[\alpha\,(\,{}^{x}_{a}\,)]$$

]

Possiamo quindi concludere che $\mathcal{A} \equiv \mathcal{R}$.

Possiamo anche verificare che $\mathcal{A}$ è numerabile:

- $\mathcal{F}$ è numerabile (perché esiste una funzione per ogni scelta di formula del linguaggio e di variabile libera, entrambe da insiemi numerabili)
- ogni A_k è numerabile ($A_1 = \mathbb{Q}$ è numerabile, e ogni A_{k+1} è l'unione di un A_k numerabile con la sua chiusura sotto un altro insieme numerabile)

Abbiamo quindi dimostrato la seguente proposizione

> **Prop. 1**
>
> Esiste una sottostruttura numerabile $\mathcal{A}$ di $\mathcal{R}$ che contiene $\mathbb{Q}$ e soddisfa esattamente gli stessi enunciati di $\mathcal{R}$ nel linguaggio degli ordini.

$\mathcal{A}$ è anche un modello numerabile di DLO, perché $\mathcal{R} \vDash$DLO.

Dunque $\mathcal{A} \cong \mathcal{Q}$. Dunque $\mathcal{Q} \equiv \mathcal{R}$ (nel linguaggio degli ordini).

2.6.3. Generalizzazione della dimostrazione

La dimostrazione è generale - si può ricostruire in maniera equivalente partendo non da $\mathcal{R}$ ma da un qualunque $\mathcal{B}$ modello non-numerabile di DLO.

La Proprietà del Testimone si esprime non relativamente a $\mathcal{Q}$ ma ad una sottostruttura numerabile $\mathcal{X}$ di $\mathcal{B}$ del tipo $(X, \leq^{\mathcal{X}})$ con $X \subseteq B$ e $\leq^{\mathcal{A}} = \leq^{\mathcal{B}} \cap (A \times A)$.

Si parte da un sottoinsieme numerabile X di $\mathcal{B}$ (che ha sicuramente), e si procede per chiusura sotto funzioni di Skolem allo stesso modo.

Si costruisce così $\mathcal{X} = \bigcup_{i \in \mathbb{N}} X_i$. Si ha $\mathcal{X} \vDash$DLO, e quindi $\cong$ e $\equiv \mathcal{Q}$.

> **Thm. 18**
>
> Si ha quindi che **tutti i modelli di DLO** (numerabili o meno) soddisfano esattamente gli stessi enunciati di $\mathcal{Q}$.
>
> i.e. $\mathcal{B} \vDash$ DLO $\implies \mathcal{B} \equiv \mathcal{Q}$
>
> DLO "identifica" quindi $(\mathcal{Q}, \leq) : Th(\mathcal{Q}) = Th(\mathcal{B})$

Corollary for Thm. 18:

DLO è una teoria completa.

(ossia, $\forall$ enunciato E, DLO $\vDash E$ oppure DLO $\vDash \neg E$ (e DLO ha almeno un modello)).

> Un modello di DLO soddisfa esattamente gli stessi enunciati di $\mathcal{Q}$. Dunque, $Cons(\text{DLO})$ sono esattamente gli enunciati veri nella singola struttura di $\mathcal{Q}$, che è una teoria completa.

2.7. Criterio di Tarski-Vaught

Per stabilire se una sottostruttura è anche una **sottostruttura elementare** ($\mathcal{A} \preceq \mathcal{B}$), possiamo quindi utilizzare la *Proprietà del Testimone*, che chiamiamo anche "criterio di Tarski-Vaught".

Def. 27: **Proprietà del Testimone (generale)**

Sia $\mathcal{A} \subseteq \mathcal{B}$. Diciamo che $\mathcal{A}$ soddisfa la **Proprietà del Testimone** rispetto a $\mathcal{B}$ se, per ogni formula del tipo $\exists x F(x)$ e per ogni assegnamento α in A, se

$$\mathcal{B} \models \exists x F(x)[\alpha]$$

allora $\exists a \in A$ tale che:

$$\mathcal{B} \models F(x)\,[\alpha\,(\tfrac{x}{a})]$$

(se in $\mathcal{B}$ esiste una soluzione (un testimone) per una certa proprietà parametrizzata da elementi di A, dobbiamo essere in grado di trovare quel testimone già dentro A)

Thm. 19

Sa $\mathcal{A}$ è una sottostruttura di $\mathcal{B}$ che **soddisfa la Proprietà del Testimone** rispetto a $\mathcal{B}$, allora $\mathcal{A}$ è una **sottostruttura elementare** di $\mathcal{B}$.

$$\mathcal{A} \subseteq \mathcal{B} \text{ e Testimone} \implies \mathcal{A} \preceq \mathcal{B}\ (\implies \mathcal{A} \equiv \mathcal{B})$$

Quindi, iniziamo a vedere che partendo da un arbitrario modello $\mathcal{B}$ infinito, ne esiste sempre uno numerabile (purché il linguaggio sia numerabile).

Prendiamo $\mathcal{B} \models T$ con $|\mathcal{B}| = \infty$ e $X \subseteq B$ con X numerabile.

Facciamo la solita chiusura per funzioni di Skolem.

Immaginiamo una successione di insiemi $X_0 \subseteq X_1 \subseteq X_2 \ldots$.

Definiamo:

$$A = \bigcup_{i \in \mathbb{N}} X_i$$

Definiamo la struttura $\mathcal{A}$ in questo modo:

- Per ogni simbolo di relazione: $R^{\mathcal{A}} = R^{\mathcal{B}} \cap A^n$

- Per ogni funzione: $f^{\mathcal{A}} = f^{\mathcal{B}}\big|_{A^n}$

NB: Ci manca la proprietà sulle costanti. Dobbiamo avere $c^{\mathcal{B}} \in A$. Potremmo far sì che le costanti siano "teste" di funzioni 0-arie di Skolem, garantendo la loro inclusione nella chiusura.

La struttura risultante è:

$$\mathcal{A} = \left(\bigcup_{i \in \mathbb{N}} X_i, \{c_i^{\mathcal{A}}\}, \{R_j^{\mathcal{A}}\}, \{f_k^{\mathcal{A}}\} \right)$$

$\mathcal{A}$ è una sottostruttura per definizione e ha la proprietà del test (Tarski-Vaught).

$$\implies \mathcal{A} \equiv \mathcal{B} \quad \text{(elementarmente equivalenti)}$$

Quindi, $\mathcal{A} \models T$.

2.8. Teorema di Löwenheim-Skolem (All'in giù)

Thm. 20: Teorema di Löwenheim-Skolem all'in giù

Sia $\mathcal{B}$ una struttura infinita adeguata per un linguaggio numerabile $\mathcal{L}$. Sia $X \subseteq B$ un sottoinsieme del suo dominio. Esiste una struttura $\mathcal{A}$ tale che:

(1) $X \subseteq A$

(2) $\mathcal{A} \preceq \mathcal{B}$ (è sottostruttura elementare)

(3) Se il linguaggio $\mathcal{L}$ e l'insieme X sono numerabili, allora **A** è numerabile.

Essenzialmente, **ogni teoria in un linguaggio numerabile che ammette un modello infinito ($\mathcal{B}$), ammette un "sotto-modello" numerabile** ($\mathcal{A}$) che è una sottostruttura elementare di $\mathcal{B}$.

La dimostrazione procede quasi analogamente a quella vista sopra.

Corollary for Thm. 20:

Non esiste una teoria T in un linguaggio $\mathcal{L}$ numerabile (predicativo) che possa forzare i suoi modelli ad essere "più che numerabili".

$$\mathcal{B} \models T \implies |B| > \aleph_0 \quad \text{(Falso in generale)}$$

Corollary for Thm. 20: "Paradosso" di Skolem

La teoria assiomatica degli insiemi (ZFC) (se ha un modello) ha modelli numerabili.

(Il linguaggio ha un solo simbolo di relazione binaria ($\in$) ed è numerabile).

Il "paradosso" (non un vero paradosso) nasce dal fatto che:

- In ZFC si dimostra l'esistenza di insiemi non numerabili (es. l'insieme dei reali $\mathbb{R}$). Formalmente:

$$\text{ZFC} \vdash \exists x (\text{“}x \text{ è non numerabile”})$$

- Se ZFC ha un modello $\mathcal{V}$, allora per il Teorema di Löwenheim-Skolem deve averne anche un modello numerabile $\mathcal{M}$.

- Quindi esiste una struttura numerabile in cui è soddisfatto l'enunciato "esiste un insieme non-numerabile".

2.9. Teorie categoriche (ω-categoricità)

L'argomento usato per dimostrare la completezza di DLO si può generalizzare.

Def. 28: ω-categoricità)

Una teoria T si dice **ω-categorica** se tutti i suoi modelli **numerabili** sono isomorfi tra loro.

(ricordiamo che se due modelli sono isomorfi, allora sono necessariamente elementarmente equivalenti)

Sia T una teoria in un linguaggio numerabile che soddisfa le seguenti tre proprietà:

(1) T è **soddisfacibile** (ha almeno un modello).

(2) T **non ha modelli finiti** (ha solo modelli infiniti).

(3) T è **ω-categorica** (ha un solo modello numerabile a meno di isomorfismo).

Possiamo concludere che T è una teoria **completa**.

proof

Supponiamo che T non sia completa.

1. Se T non è completa, esiste un enunciato E nel linguaggio tale che T non dimostra né E né $\neg E$.

$$T \nvdash E \quad \text{e} \quad T \nvdash \neg E$$

2. Questo implica che esistono due modelli $\mathcal{B}$ e $\mathcal{C}$ tali che:

$$\mathcal{B} \models T \cup \{\neg E\} \quad \text{e} \quad \mathcal{C} \models T \cup \{E\}$$

3. Per l'ipotesi (2), T non ha modelli finiti, quindi $\mathcal{B}$ e $\mathcal{C}$ sono entrambi infiniti.

4. Applichiamo il Teorema di Löwenheim-Skolem a entrambi i modelli:
   - Esiste $\mathcal{B}_0 \preceq \mathcal{B}$ con $\mathcal{B}_0$ numerabile. Poiché $\mathcal{B} \models \neg E$, allora $\mathcal{B}_0 \models \neg E$.
   - Esiste $\mathcal{C}_0 \preceq \mathcal{C}$ con $\mathcal{C}_0$ numerabile. Poiché $\mathcal{C} \models E$, allora $\mathcal{C}_0 \models E$.

5. Ora abbiamo due modelli numerabili di T, $\mathcal{B}_0$ e $\mathcal{C}_0$. Per l'ipotesi (3) di **ω-categoricità**, tutti i modelli numerabili sono isomorfi:

$$\mathcal{B}_0 \cong \mathcal{C}_0$$

6. Se due strutture sono isomorfe, soddisfano gli stessi enunciati:

$$\mathcal{B}_0 \equiv \mathcal{C}_0$$

Tuttavia, abbiamo stabilito al punto 4 che $\mathcal{B}_0 \models \neg E$ e $\mathcal{C}_0 \models E$ (contraddizione) □

2.10. Calcolo dei Predicati

Introduciamo ora il calcolo dei predicati (con identità) "alla Hilbert". Ad ogni linguaggio $\mathcal{L}$ possiamo associare un calcolo dei predicati del I ordine.

Def. 29: **Dimostrabilità**

Si ha $T \vdash A$ se e solo se esiste una sequenza $(A_1, A_2, \dots, A_n)$ di formule tali che:

- $A_n = A$
- $\forall 1 \leq i \leq n$:
  - $A_i \in T$, oppure
  - A_i assioma, oppure
  - A_i segue dai precedenti per regole di inferenza

Gli assiomi logici sono i seguenti:

(1) Tutti gli assiomi proposizionali (illustrati a p.21)

Gli assiomi predicativi:

(2) $\forall x F \to F[x/t]$ con t termine libero per x in F (per "libero" vedi p.27)

da questa regola deriva anche: $\dfrac{F[x/t]}{\exists x\ F}$

(3) $\forall x(F \to G) \to (F \to \forall x\ G)$, con F senza occorrenze libere di x (si dice "F non parla di x")

Gli assiomi dell'identità:

(4) Per ogni simbolo di relazione R:

$$\forall x_1 \dots x_n,\ \forall y_1, \dots y_n,\ \left(\bigwedge_{i=1}^{n}(x_i = y_i)\right) \to \big(R(x_1, \dots, x_n) \leftrightarrow R(y_1, \dots, y_n)\big)$$

(5) Per ogni simbolo di funzione f:

$$\forall x_1 \dots x_n,\ \forall y_1, \dots y_n,\ \left(\bigwedge_{i=1}^{n}(x_i = y_i)\right) \to \big(f(x_1, \dots, x_n) = f(y_1, \dots, y_n)\big)$$

(6) (uguaglianza e transitività)

$$\forall x\ y\ z\Big((x = x) \wedge \big((x = y) \to (y = x)\big) \wedge \big(((x = y) \wedge (y = z)) \to (x = z)\big)\Big)$$

(valgono $(x = x)$ e $(x = y \to y = x)$ e $((x = y \wedge y = z) \to x = z)$)

Le **regole di inferenza** che utilizziamo nel calcolo predicativo sono:

(1) *Modus Ponens*: $\dfrac{X \qquad X \to Y}{Y}$

(2) *Generalizzazione*: $\dfrac{F}{\forall x\ F}$

(attenzione ! non è come dire che se una formula F vale in un caso, allora vale $\forall x$ - stiamo dicendo che, se ho *dimostrato in maniera generica* F, allora essa è vera $\forall x$)

2.10.1. Proprietà fondamentali del Calcolo dei Predicati

Il calcolo dei predicati mantiene molte delle proprietà del calcolo proposizionale, come:

- il **teorema di correttezza**: $T \vdash A \implies T \vDash A$ (anche qui tutti gli assiomi sono verità logiche e le regole di inferenza preservano le verità logiche)
- $T \vdash A \land T \subseteq S \implies S \vdash A$
- se $\vdash A$, A è detto "teorema"
- $\dfrac{T \vdash A \qquad A \vdash B}{T \vdash B}$
- $\dfrac{T \vdash A \qquad S \vdash B}{T \cup S \vdash A \land B}$

> Thm. 21: **Teorema di deduzione per il calcolo predicativo**
>
> Sia E un enunciato, A una formula e Γ un insieme di formule. Vale:
>
> $$\Gamma, E \vdash A \iff T \vdash (E \to A)$$

Altre proprietà:

- Ogni istanza di tautologia proposizionale è una verità nel Calcolo dei Predicati

2.10.2. Teorema di completezza per la logica predicativa

Come per la logica proposizionale, vogliamo dimostrare $T \vDash A \iff T \vdash A$.

Esiste però un'altra definizione equivalente per il teorema di completezza.

> Def. 30: **Coerenza**
>
> Una teoria T è **coerente** (o non-contraddittoria) $\iff \neg\exists$ enunciato A t.c. $T \vdash A \land T \vdash \neg A$

> Il Calcolo dei Predicati è coerente, ossia per nessuna formula vale $\vdash F \land \vdash \neg F$.

> Def. 31: **Teorema di completezza v.2**
>
> $$T \text{ coerente} \iff T \text{ ha un modello } (\in \texttt{SAT})$$

Notiamo facilmente che T incoerente come testimoniato da A (ovvero $T \vdash A \land T \vdash \neg A$) implica necessariamente T insoddisfacibile.

Infatti, $T \vdash A \implies T \vDash A$ e $T \vdash \neg A \implies T \vDash \neg A$, e se valgono sia $T \vDash A$ che $T \vDash \neg A$ sappiamo che T è insoddisfacibile ($Mod(T) = \emptyset$).

Ci manca da dimostrare T coerente $\implies Mod(T) \neq \emptyset$.

Thm. 22: **Equivalenza tra le due forme di teorema di completezza**

Si ha che (1) $T \vDash A \iff T \vdash A \equiv T$ coerente $\iff T$ ha un modello $(\in \texttt{SAT})$ (2)

proof

(1) Assumiamo (2) e dimostriamo $T \vDash A \implies T \vdash A$

Sappiamo che $T \vDash A$. Ci sono due opzioni:

- $T \in \texttt{UNSAT}$: $T \vDash A$ è vera $\forall A$, quindi T incoerente
  (se $\exists B$ t.c. $T \vdash B \land T \vdash \neg B$, possiamo dimostrare una qualsiasi affermazione A in questo modo: $\vdash B \to (\neg B \to A)$)
  quindi $T \vdash A$
- $T \in \texttt{SAT}$: se $T \in \texttt{SAT}$ e $T \vDash A$, sappiamo che $T \cup \neg A \in \texttt{UNSAT}$.
  Per (2), quindi, $T \cup \neg A$ è incoerente, quindi $T \vdash A$
  $T \cup \neg A$ incoerente significa $T \cup \neg A \vdash \bot$, quindi (x deduzione) $T \vdash \neg A \to \bot$;
  per reductio ad absurdum ($(\neg A \to \bot) \vdash A$), si ha quindi $T \vdash A$.

(2) Assumiamo (1) e dimostriamo T coerente $\implies T$ ha un modello

Presumiamo che T non abbia un modello. Questo implica logicamente qualsiasi cosa ($T \vdash A$ e $T \vdash \neg A$). Per (1), quindi, $T \vDash A$ e $T \vDash \neg A$, quindi T incoerente (per contrapposizione, otteniamo l'implicazione originale).

2.10.3. Estensioni di teorie

Vogliamo dimostrare coerenza $\implies$ soddisfacibilità. Per farlo, introduciamo il concetto di *estensione*.

Def. 32: **Estensione**

Diciamo che una teoria T' **estende** una teoria T se $T \subseteq T'$.

Def. 33: **Teoria sintatticamente completa**

Una teoria T si dice **sintatticamente completa** se per ogni enunciato E nel linguaggio di T, vale $T \vdash E$ oppure $T \vdash \neg E$.

Lemma 6: **Lemma di Lindenbaum**

Ogni teoria coerente (in un linguaggio numerabile) ammette un'estensione coerente e completa.

(Sia T coerente. Allora $\exists S$ teoria nel linguaggio di T t.c.:

- $T \subseteq S$
- S è coerente
- S è sintatticamente completa

)

proof

Fissiamo un'enumerazione $\{E_1, E_2, \dots\}$ di tutti gli enunciati di T.

Definiamo una successione di teorie in quessto modo:

- $S_0 = T$
- $S_{n+1} = \begin{cases} S_n \cup \{E_{n+1}\} & \text{se } S_n \cup \{E_{n+1}\} \text{ coerente (ovvero } S_n \nvdash \neg E_{n+1}) \\ S_n & \text{altrimenti (ovvero } S_n \vdash \neg E_{n+1}) \end{cases}$

  nel secondo caso non serve aggiungere $\{\neg E_{n+1}\}$ perché si ha già $S_n \vdash \neg E_{n+1}$ (sarebbe superfluo)

Sia $S = \bigcup_{n \in \mathbb{N}} S_n$.

(1) S è **coerente**

S è coerente significa che $\nexists E$ per cui $\exists \{A_1, A_2, \dots, A_t\}, \{B_1, B_2, \dots, B_t\} \subseteq S$ t.c. $A_1, A_2, \dots, A_t \vdash E$ e $B_1, B_2, \dots, B_t \vdash \neg E$.

Si nota facilmente che questo è impossibile, in quanto, per costruzione, entrambi gli insiemi di enunciati apparterrebbero a un S_m per qualche m (vista la costruzione "a catena" di S), e si avrebbe $S_m \vdash E$ e $S_m \vdash \neg E$, quindi S_m incoerente (ma per costruzione, $\forall i$ S_i è coerente).

(2) S è sintatticamente **completa**

Scegliamo di dimostrarlo nella forma $S \nvdash \neg E \implies S \vdash E$

Sia $E = E_{n+1}$ per un qualche n. Sappiamo che $\forall i$ e in particolare per n, $S_n \nvdash \neg E_{n+1}$.

Quindi, per costruzione $S_{n+1} = S_n \cup \{E_{n+1}\} \implies S_{n+1} \vdash E_{n+1} \overset{S_{n+1} \subseteq S}{\implies} S \vdash E_{n+1}$.

Se invece di T coerente avessimo ipotizzato T soddisfacibile, la conclusione sarebbe stata banale perché si sarebbe definita S facilmente come (dato $\mathcal{A}$ modello di T) $S = Th(\mathcal{A}) = \{E \mid \mathcal{A} \vDash E\}$, evidentemente coerente e completo.

Il teorema di completezza mostra che le due cose sono equivalenti.

Abbiamo quindi dimostrato che T coerente $\implies \exists S \supseteq T$ coerente e completa.
Vogliamo però T coerente $\implies T$ soddisfacibile.

Il passo successivo è dimostrare che S è già quasi un modello.

Cerchiamo quindi un modello $\mathcal{M} = (M, \mathcal{R}^{\mathcal{M}}, f_j^{\mathcal{M}}, c_i^{\mathcal{M}})$

Per definirlo, facciamo alcune assunzioni.

Assumiamo di lavorare con un linguaggio $\mathcal{L} = \{R_i, f_j, c_k\}$ che contenga almeno una costante e una funzione (nota bene: se ci sono una costante e una funzione, ci sono infiniti termini chiusi).

Definiamo $\mathcal{M}$ (detto **modello di Henkin** dei termini di S):

- $M = \{\text{termini chiusi di } \mathcal{L}\}$

  es. $\mathcal{L}_1 = \{0, 1, +\}$, $M = \{0, 1, 0+0, 0+1, 1+0, \dots\}$

- $c_k^{\mathcal{M}} = c_k \in M$

  l'interpretazione della costante c è data dalla costante c stessa

  es. $\mathcal{L}_2 = \{e, *\}, M_2 = \{e, e*e, \dots\}$ - come interpretazione di $c_0 = e$ prendo $e \in M_2$

- l'interpretazione di un simbolo di relazione $\mathcal{R}$ è data dall'insieme dei termini chiusi di cui S dimostra che soddisfano la relazione - ovvero $(\mathcal{M}_1, \dots, \mathcal{M}_n) \in \mathcal{R}_i^{\mathcal{M}} \iff S \vdash \mathcal{R}_i(t_1, \dots, t_n)$

- l'interpretazione di un simbolo di funzione f è l'associazione $t_1, \dots, t_n \mapsto f(t_1, \dots, t_n)$ - $f_j^{\mathcal{M}} : M^n \to M$ è t.c. $f_j^{\mathcal{M}}(t_1, \dots, t_n) := f_j(t_1, \dots, t_n)$

  es. $+^{\mathcal{M}}(0,1) = \underbrace{+(0,1)}_{t}$

Osserviamo che l'interpretazione in $\mathcal{M}$ di un termine chiuso t coincide con il termine stesso ($t^{\mathcal{M}} = t$).

Vogliamo dimostrare $\mathcal{M} \vDash S$. Per farlo (come spesso accade) ci è più comodo dimostrare un'affermazione più forte: $\forall E \; \mathcal{M} \vDash E \iff S \vdash E$.

proof

Dimostriamo per casi (su E):

- E è $\neg G$

  se $\mathcal{M} \nvDash E$, per ipotesi induttiva si ha $S \nvdash G$ e da S completa segue $S \vdash \neg G$.

  se $\mathcal{M} \vDash E$, allora per ipotesi induttiva $S \vdash G$ e da S coerente segue $S \nvdash \neg G$

- $\mathcal{M} \vDash G \wedge H \iff S \vdash G \wedge H$

  ($\implies$) supponiamo $\mathcal{M} \vDash G \wedge H$;

  allora, $\mathcal{M} \vDash G \; \wedge \mathcal{M} \vDash H$

  per ipotesi induttiva, abbiamo $S \vdash G \; \wedge S \vdash H$, e usando la tautologia $G \to (H \to (G \wedge H))$ ottengo $S \vdash G \wedge H$

  ($\impliedby$) supponiamo $S \vdash G \wedge H$;

  per la tautologia $G \wedge H \to G$, otteniamo $S \vdash G \; \wedge \; S \vdash H$

  per ipotesi induttiva, segue $S \vDash G \; \wedge \; S \vDash H$, da cui $S \vDash G \wedge H$

- se E è un enunciato atomico $R(t_1, \dots, t_k)$, abbiamo che $\mathcal{M} \; \vDash \; R(t_1, \dots, t_n)$ per definizione $\iff \; (t_1^{\mathcal{M}}, \dots t_n^{\mathcal{M}}) \in \mathbb{R}^{\mathcal{M}}$ e, per l'osservazione sui termini, $\iff \; (t, \dots, t_n) \in R^{\mathcal{M}}$, il che per definizione equivale a $S \vdash R(t_1, \dots, t_n)$

- se E è del tipo $\forall x F$

  sappiamo $\iff \forall m \in M \mathcal{M} \vDash F \begin{bmatrix} x \\ m \end{bmatrix}$

  e qui vale $\mathcal{M} \vDash F \begin{bmatrix} x \\ m \end{bmatrix} \iff \mathcal{M} \vDash F[x/m]$

  per ipotesi induttiva, abbiamo che $\forall m \in M, \; S \vdash F[x/m]$, ma non abbiamo il $\iff$.

  sappiamo $S \vdash \forall x F \implies S \vdash F[x/t]$, ma non l'altro verso (è come dire che sappiamo che per ogni numero c'è una dimostrazione, ma vogliamo che ci sia una dimostrazione per ogni numero)

Possiamo definire una teoria che ci aiuta nella dimostrazione.

Def. 34: **Teoria con testimoni**

Una **teoria con testimoni**, o **teoria di Henkin** (o "scapegoat theory") soddisfa la seguente proprietà:

- $\forall$ formula F con un'unica variabile libera x, $\exists$ un termine chiuso t t.c.

$$T \vdash \exists x \neg F(x) \to \neg F(t)$$

(t è un testimone dell'enunciato $\exists x \neg F(x)$)

(un testimone è un termine specifico (t) che la teoria "nomina" per concretizzare un'affermazione esistenziale - normalmente, se diciamo $\exists x P(x)$, non sappiamo chi sia x per cui P vale; se siamo in una teoria con testimoni, invece, abbiamo $\exists x P(x) \to P(t)$, sappiamo esattamente chi sia t)

Vediamo come una teoria con testimoni ci aiuta a dimostrare il caso $\forall x F(x)$ con $F(x)$ aperta.

(Dimostriamo che, se $\mathcal{M} \vDash \forall x F$ allora $T \vdash \forall x F$)

Per assurdo, supponiamo $\mathcal{M} \vDash \forall x F$ e $T \nvdash \forall x F$.

Per completezza di T vale $T \vdash \neg E$, ovvero $T \vdash \exists x \neg F(x)$. Dato che T è una teoria con testimoni, esiste un termine chiuso t tale che $T \vdash \exists x \neg F(x) \to \neg F(t)$.

Dunque $T \vdash \neg F(t)$.

Per ipotesi induttiva, $\mathcal{M} \vDash \neg F(t)$. Ma da $\mathcal{M} \vDash \forall x F(x)$, e da $\mathcal{M} \vDash \forall x F(x)$, vale, per qualsiasi termine chiuso $\mathcal{M} \vDash F(x) \to F(t)$.

Dunque, $\mathcal{M} \vDash F(t)$, il che contraddice $\mathcal{M} \vDash \neg F(t)$. □

Se T coerente, T si può estendere a $T^* \supseteq T$ che sia coerente e con testimoni (in un $\mathcal{L}$ che estende $\mathcal{L}_T$ con un insieme numerabile di costanti.

Thm. 23

Per ogni teoria T coerente esiste una teoria T' tale che:

- T' è un'estensione di T
- T' è una teoria con testimoni
- il linguaggio di T' è numerabile ed estende quello di T
- T' è coerente

proof

Sia T coerente.

Sia $T_0 = T \cup \{\text{istanze degli assiomi logici nel linguaggio esteso}\}$.

Fissiamo un'enumerazione delle formule in $\mathcal{L}$ con una variabile libera: $F_1(x_1), F_2(x_2), \dots$

Sia $B = \{b_1, b_2, b_3, \dots\}$ un insieme di nuovi simboli di costante. Fissiamone un'enumerazione $b_{j1}, b_{j2}, \dots$, in cui b_{jk} è il primo (per indice) t.c.

- b_{jk} non appare in $F_1(x_1), \dots, F_k(x_k)$
- b_{jk} è diverso da $b_{j1}, \dots, b_{j_{k-1}}$

quindi b_{j1} è la prima costante $\notin F_1$, b_{j2} la prima che non compare in F_2 e non è già stata usata (quindi $\neq b_{j1}$), ecc

Sia W_k il seguente enunciato:

$$\exists x_k \neg F_k(x_k) \to \neg F_k(b_{jk})$$

Sia $T_n = T_0 \cup \{W_1, \dots, W_n\}$, e sia $T_\infty = \bigcup_n T_n$.

claim: $T^* = \bigcup_{n \in \mathbb{N}} T$ è di Henkin, coerente ed estende T.

di Henkin: $\forall n \exists t = b_{j_n}$ t.c. $T^* \ni \exists x_n \neg F_n(x_n) \to \neg F_n(b_{j_n})$ è vero per costruzione

- Dimostriamo che T_∞ è coerente (basta dimostrare che $\forall n\ T_n$ coerente)

per induzione:

- **C.B.**: T_0 è coerente

  "banale", T coerente e abbiamo aggiunto a T solo assiomi

  $T_0 \vdash \bot \implies T \cup A = \{A_1, \dots, A_t\} \vdash \bot \implies T \vdash A \to \bot$ - visto che A assiomi, $T \vdash A$ e per MP, $T \vdash \bot$ - ma questo è impossibile perché T coerente)

- **P.I.**: assumiamo T_{n-1} coerente

  per assurdo, sia T_n incoerente;

  allora, si ha $T_n \vdash \bot$, e $\bot \to B \implies T_n \vdash B\ \forall B$; quindi $T_n \vdash \neg W_n$;

  ma $T_n = T_{n-1} \cup \{W_n\}$, quindi (per deduzione) $T_{n-1} \vdash W_n \to \neg W_n$;

  $\neg W_n$ è una negazione di un'implicazione (quindi verifica la premessa $\exists x_n \neg F_n(x_n)$ e falsifica la conseguenza $\neg F_n(b_{j_n})$) quindi $T_{n-1} \vdash \exists x_n \neg F) n(x_n)$ e $T_{n-1} \vdash F_n(b_{j_n})$.

  Per costruzione, sappiamo che $T_{n-1} = T_0$ $(= T \cup$ assiomi$) \cup \{W_1, \dots, W_{n-1}\}$; abbiamo scelto b_{j_n} e quindi sappiamo che:

  - esso non compare in $W_1, \dots, W_{n-1}$;
  - per definizione, non compare in T;

  Dovrà quindi far parte degli assiomi logici.

  Notiamo che quindi, sostituendo b_{j_n} con una nuova variabile, la formula restante rimarrà un assioma logico.

  Sia quindi y una variabile che non compare nella dimostrazione δ (di $F_n(b_{j_n})$).

  claim: $\delta^y = \delta[b_{j_n}/y] = (D_1^y, \dots, D_n^y)$ è ancora una dimostrazione.

  Infatti:

  - gli assiomi rimangono tali (o non dicono niente su b_{j_n}) o dicono cose sempre vere, quindi sostituendo non cambia nulla
  - le ipotesi $T_{n-1}, W_1, \dots, W_n$ non cambiano, in quanto $\not\ni b_{j_n}$
  - il Modus Ponens è preservato
  - la Generalizzazione non viene mai applicata su b_{j_n} (vorrebbe dire che una formula $\forall y H(y)$ sarebbe stata ottenuta da una formula $H(b_{j_n})$ (ricordiamo che b_{j_n} è una costante specifica), il che è impossibile)

  Ora - se è vero $T_{n-1} \vdash F_n(y)$, per Generalizzazione si ha anche $T_{n-1} \vdash \forall y F_n(y)$. Ma abbiamo anche $T_{n-1} \vdash \exists x \neg F_n(x)$. Le due cose sono chiaramente contraddittorie, quindi T_{n-1} è incoerente. □

Quindi, possiamo formalizzare i seguenti teoremi:

Thm. 24

Sia T una teoria con testimoni e coerente in un linguaggio numerabile. Allora, T ha un modello numerabile.

Thm. 25: **Esistenza del modello**

Ogni teoria coerente (in un linguaggio numerabile) ha un modello numerabile.

proof

Partiamo da T coerente (in $\mathcal{L}$)

- $\overset{\text{Henkin}}{\Longrightarrow}$ $T^* \supseteq T$ coerente con testimoni (in $\mathcal{L}^*$ numerabile $\supseteq \mathcal{L}$)
- $\overset{\text{Lindenbaum}}{\Longrightarrow}$ $\hat{T} \supseteq T^*$ coerente e completa con testimoni (in $\mathcal{L}^*$)

  (la proprietà di essere con testimoni è preservata perché il lemma di Lindenbaum non cambia il linguaggio)
- $\Longrightarrow$ $\mathcal{M}_{\hat{T}} \vDash T$ (il modello dei termini di $\hat{T}$ è un modello numerabile di T)

nota bene !

logica con identità

La dimostrazione sopra descritta si limita alla logica di primo ordine senza identità.

Per il modello sopra definito, $\mathcal{M} \vDash (t_1 = t_2) \iff t$ ed s sono esattamente lo stesso termine (quindi, per esempio, $(1+1) \neq 2$).

Per risolvere questo problema, basta quozientare sulla seguente relazione:

$$t \sim s \iff T \vdash (t = s)$$

- notiamo che $\sim$ è una relazione di equivalenza

Definiamo quindi il modello dei termini $\mathcal{M}/\sim$ in questo modo:

- il dominio è $M/\sim = \{[t]_\sim \mid t \text{ termine chiuso}\}$
- $c^{\mathcal{M}/\sim} = [c]_\sim$
- $f^{\mathcal{M}/\sim}([t_1]_\sim, \dots, [t_n]_\sim) = [f(t_1, \dots, t_n)]_\sim$
- $([t_1]_\sim, \dots, [t_n]_\sim) \in R^{\mathcal{M}/\sim}$ se e solo se $T \vdash R(t_1, \dots, t_n)$

La dimostrazione $\mathcal{M}/\sim \vDash E \iff T \vdash E$ procede esattamente come quella di $\mathcal{M}$. Inoltre, se $\mathcal{M}$ ha cardinalità numerabile, anche $\mathcal{M}/\sim$ ha cardinalità numerabile.

2.11. Teorema di compattezza

Il teorema di compattezza si può riformulare in diversi modi:

Thm. 26: **Teorema di compattezza, versioni equivalenti**

- Un insieme di enunciati è coerente se e solo se ogni suo sottinsieme finito è coerente.
- Un insieme di enunciati ha un modello se e soltanto se ogni suo sottoinsieme finito ha un modello.
- $T \vDash E$ se e solo se esiste un sottoinsieme finito $T_0 \subseteq T$ tale che $T_0 \vDash E$.

2.11.1. Applicazione: (non) assiomatizzabilità

Data una proprietà P di strutture, è utile chiedersi se possa essere espressa da enunciati del primo ordine, ovvero se esista un insieme di enunciati T che soddisfa, per ogni struttura $\mathcal{A}$, la seguente equivalenza:

$$\mathcal{A} \vDash T \iff \mathcal{A} \text{ ha la proprietà } P$$

Se un tale T esiste, diciamo che **assiomatizza** o *definisce* la proprietà P.

Ha ancora più senso chiedersi, nello specifico, data una classe di strutture $\mathcal{C}$ e un linguaggio predicativo $\mathcal{L}$, se esista una teoria in $\mathcal{L}$ tale che la proprietà s opra sia soddisfatta.

Se esiste una teoria T che assiomatizza una proprietà P, ci si può chiedere se esiste un *insieme finito di enunciati* che assiomatizza P. Questo è equivalente a chiedersi se esiste un singolo enunciato E (l'AND tra tutti gli enunciati) tale che, per ogni struttura $\mathcal{A}$ nella classe $\mathcal{C}$,

$$A \vDash E \iff \mathcal{A} \text{ ha la proprietà } P$$

In questo caso, diciamo che P è **finitamente assiomatizzabile** relativamente alla classe $\mathcal{C}$.

Esempio 1: finitezza

- $P =$ "avere dominio finito";
- $\mathcal{C} =$ tutte le strutture;

Partiamo da $P_n =$ "avere dominio di cardinalità $\geq n$".

Possiamo assiomatizzare questa proposizione con un linguaggio $\mathcal{L}$ "vuoto" (senza relazioni specifiche) in questo modo:

$$\exists x_1, \dots, x_n \left(\bigwedge_{i \neq j,\ 1 \leq i \leq n} \neg(x_i = x_j) \right)$$

Possiamo assiomatizzare anche la proprietà "avere dominio di cardinalità n" in questo modo:

$$\exists x_1, \dots, x_n \left(\bigwedge_{i \neq j,\ 1 \leq i \leq n} \neg(x_i = x_j) \wedge \forall y \left(\bigvee_{i=1}^{n} (y = x_i) \right) \right)$$

> Prop. 2: **Assiomatizzazione di "avere un dominio finito / infinito"**
>
> La proprietà "avere dominio infinito" è assiomatizzabile ma non finitamente assiomatizzabile.
>
> La proprietà "avere dominio finito" non è assiomatizzabile.

Consideriamo $T = \{P_n \mid n \in \mathbb{N}\}$ ("avere dominio di cardinalità almeno n" per ogni n). La teoria T assiomatizza "avere un dominio infinito" (se si ha dominio almeno n per ogni n)

Sia per assurdo F una teoria che assiomatizza $P =$ "avere dominio finito".

Consideriamo $F \cup T$. $F \cup T$ non può avere modelli (in quanto parla di essere finito e infinito allo stesso tempo).

Se ne prendo un qualsiasi pezzo finito $T_0 \subseteq F \cup T$, noto però che esso ha un modello (in quanto descrive, "alla peggio", l'avere dominio finito (da F) e l'avere almeno n elementi (da T)).

Visto che T_0 ha un modello, per compattezza tutta la teoria dovrebbe avere un modello (`FINSAT` $\implies$ `SAT`), il che è impossibile. □

Vediamo anche che è impossibile che "avere dominio infinito" sia *finitamente* assiomatizzabile.

Infatti, se esistesse S finita t.c. $\mathcal{A} \vDash S \iff \mathcal{A}$ ha dominio infinito, avremmo che $\neg S$ assiomatizzerebbe "avere dominio finito" (impossibile). □

Lemma 7

Sia P assiomatizzabile. Se $\neg P$ non è assiomatizzabile, allora P non è finitamente assiomatizzabile.

Per contrapposizione, se $P, \neg P$ sono assiomatizzabili, allora P è finitamente assiomatizzabile.

Lemma 8

Se P è assiomatizzabile da T e P è finitamente assiomatizzabile, allora $\exists T_0 \subseteq T$ che assiomatizza P.

Lemma 9

Se T ha modelli finiti arbitrariamente grandi (per ogni n c'è un modello con almeno n elementi), allora T ha anche modelli infiniti.

(Non) assiomatizzazione di "essere un grafo connesso"

Consideriamo i grafi, con linguaggio $\mathcal{L} = \{E(x, y)\}$, e la proprietà $P =$ "essere un grafo connesso".

Possiamo scrivere la proprietà $D_n =$ "essere a distanza $\geq n$" in questo modo:

$$\neg(\exists x_1, \ldots, x_n \left(\bigwedge_{i \neq j} \neg(x_i = x_j) \wedge E(c, x_1) \wedge E(x_1, x_2) \wedge \cdots \wedge E(x_n, d) \right))$$

Supponiamo che P sia assiomatizzabile da una teoria C.

Consideriamo $C \cup \{D_n \mid n \geq 0\}$ - questa teoria non può avere un modello.

Come prima, consideriamo un pezzo finito $T_0 \subseteq C \cup \{D_n \mid n \geq 0\}$.

Come prima, questo sottoinsieme ha un modello (un grafo connesso con vertici a distanza $>$ del massimo n). Come prima, avremmo `FINSAT` $\implies$ `SAT`, e per questo si ha che P non è assiomatizzabile. □

2.11.2. Modelli non standard dell'aritmetica

Dato $\mathcal{N} = (\mathbb{N}, 0, 1, +, *, \leq)$, possiamo definire la sua teoria $T = Th(\mathcal{N}) = \{E \mid \mathbb{N} \vDash E\}$.

Sia $\mathcal{A} \vDash Th(\mathcal{N})$. Quanto assomiglia $\mathcal{A}$ ad $\mathbb{N}$?

Noi vorremmo $\mathcal{A} \cong \mathcal{N}$, ma in realtà esistono molti modelli di $\mathcal{N}$ molto differenti dai numeri naturali che conosciamo.

Consideriamo per esempio una nuova costante c e la teoria:

$$T \cup \{A_n \mid n \in \mathbb{N}\}$$

con $A_n = \underbrace{1 + \cdots + 1}_{n} < c$.

Un sottooinsieme qualsiasi $T_0 \subseteq T \cup \{A_n \mid n \in \mathbb{N}\}$ ha un modello - basta dare un'interpretazione alla costante c.

Per esempio, $\mathcal{A} = (\mathbb{N}, +^{\mathcal{N}}, x^{\mathcal{N}}, 0^{\mathcal{N}}, 1^{\mathcal{N}}, c^{\mathcal{A}} = max(a_1, \ldots, a_k) + 1)$ è un modello di T_0.

Per compattezza, quindi, $T \cup \{A_n \mid n \in \mathbb{N}\}$ ha un modello.

Ma come interpretiamo $c^{\mathcal{A}}$ in questo modello? Deve esserci un unico c tale che, $\forall n, \underbrace{1 + \cdots + 1}_{n} <^{\mathcal{A}} c^{\mathcal{A}}$.

Deve quindi esserci un c maggior di tutti gli elementi di $\mathbb{N}$.

Questo modello è molto diverso da $\mathbb{N}$.$\mathcal{A}$ è quello che si dice **modello non-standard** dell'aritmetica, e $c^{\mathcal{A}}$ è un *naturale non-standard*.

Inizia infatti con $\mathbb{N}$, ma contiene almeno un elemento maggiore di tutti i numeri standard. Inoltre, se $a \in \mathcal{A}$ è un numero non-standard, allora anche il suo predecessore è un numero non-standard. Un elemento non-standard ha quindi infiniti predecessori e successori, nessuno dei quali può essere standard.

Intorno a $c^{\mathcal{A}}$ si sviluppa quindi una copia isomorfa a $\mathbb{Z}$.

Si esclude quindi che si possa definire una teoria T che assiomatizzi $Th(\mathcal{N})$ in modo che valga, come per DLO< che tutti i modelli numerabili di T sono isomorfi. Resta aperta però la possibilità di trovare un insieme di assiomi T con insieme di teoremi computabilmente enumerabili che coincida con la "vera" Teoria dei Numeri $Th(\mathcal{N})$.Una tale teoria sarebbe completa e dunque decidibile e fornirebbe un algoritmo per decidere automaticamente se un enunciato E è un teorema della Teoria dei Numeri o no.

3

I teoremi di Gödel

3.1. Funzioni calcolabili (algoritmiche)

Esistono diverse definizioni di algoritmo. Le principali ci vengono date da Gödel, Herbrand e Kleene (in chiave matematica), da Turing (attraverso le TM), e da Church (nel λ-calcolo).

Def. 35: Funzioni calcolabili

La classe $\mathcal{C}$ delle funzioni parziali calcolabili è la minima classe di funzioni del tipo $\mathbb{N}^k \to \mathbb{N}$ (con $k \in N$) t.c.:

- $+, * \in \mathcal{C}$
- $i(x,y) = \begin{cases} 1 & \text{se } x = y \\ 0 & \text{se } x \neq y \end{cases}$
- $\prod_i^n (x_1, \ldots, x_n) = x_i$ (proiezione)

e $\mathcal{C}$ chiusa sotto composizione - date $\theta_1, \ldots, \theta_n : \mathbb{N}^k \to \mathbb{N}, \psi : \mathbb{N}^m \to \mathbb{N}$, la composta ϕ è definita come segue:

$$\phi(x_1, \ldots, x_n) = \psi(\theta_1(x_1, \ldots, x_n), \ldots, \theta_n(x_1, \ldots, x_k))$$

$\mathcal{C}$ è chiusa anche sotto *minimalizzazione*: data $g(\vec{x}, y)$, la funzione $h(\vec{x})$ è definita come $h(\vec{x}) = min\ z$ t.c.

- i valori $g(\vec{x}, 0), g(\vec{x}, 1), \ldots, g(\vec{x}, z-1)$ sono definiti e $\neq 0$
- $g(\vec{x}, z) = 0$
- (se un tale z non esiste, la funzione non è definita)

Prop. 3

Si ha che $f \in \mathcal{C} \implies f$ calcolabile.

- Nella composizione di funzioni $h(g_1, \ldots, g_m)$:
  - Se tutte le g_i e h fossero totali, si applicherebbero semplicemente le g_i e poi h sul risultato.
  - Se una delle g_i è indefinita, il calcolo procede comunque secondo la logica algoritmica: il programma semplicemente non termina (non si arriva mai ad applicare h).
    (anche se il risultato è indefinito, il processo rimane algoritmico).

Per calcolare una composizione come $h(g_1(\vec{x}), g_2(\vec{x}), \dots)$, è necessario stabilire un ordine di esecuzione:

- Non si possono far partire le funzioni in parallelo; devono essere eseguite in ordine sequenziale.

  se si procedesse in parallelo, si potrebbe trovare un risultato per g_2 mentre g_1 sta ancora calcolando (o è in loop infinito).

- Per definizione, se un argomento è indefinito, l'intera composizione deve esserlo. Procedendo in ordine, se ci si "ferma" su g_1, il calcolo si arresta correttamente senza produrre risultati parziali o errati basati sugli altri argomenti.

(Anche $g(\vec{x}, y)$ è algoritmica perché lo è $h(\vec{x})$)

Prop. 4: **Calcolabilità**

- Una funzione $\varphi : \mathbb{N}^k \to \mathbb{N}$ è calcolabile $\iff \varphi \in \mathcal{C}$.
- $R \subseteq \mathbb{N}^k$ si dice calcolabile se la sua **funzione caratteristica** χ_R è calcolabile.

$$\chi_R(\vec{x}) = \begin{cases} 1 & \text{se } \vec{x} \in R \\ 0 & \text{se } \vec{x} \notin R \end{cases}$$

3.2. Teorema di Definibilità

Def. 36: **Definibilità**

Diciamo che φ è **rappresentabile** in $\mathcal{N}$ da una formula $F(x_1, \dots, x_k, y)$ se per ogni tupla di numeri naturali $(a_1, \dots, a_k, b) \subseteq \mathbb{N}^{k+1}$, vale l'equivalenza:

$$\varphi(a_1, \dots, a_k) = b \iff \mathcal{N} \models F\left[\binom{x_1,\dots,x_k,y}{a_1,\dots,a_k,b}\right]$$

i.e. se le k+1-ple $(a_1, \dots, a_k, b)$ appartenenti al grafo di φ sono esattamente quelle che soddisfano in $\mathcal{N}$ la formula $F(x_1, \dots, x_k, y)$ assegnando a_i a x_i e b a y.

(la formula è vera nel modello standard $\mathcal{N}$ se e solo se la funzione, calcolata sugli input a_i, restituisce b).

Nel linguaggio dell'aritmetica, ogni numero naturale $n \in \mathbb{N}$ ha un nome canonico (**numerale**) costituito dalla somma di n volte la costante 1.

Quindi, vale che:

$$\mathcal{N} \models F\left[\binom{x_1,\dots,x_k,y}{a_1,\dots,a_k,b}\right] \iff \mathcal{N} \vdash F(\bar{a_1}, \dots, \bar{a_k}, \bar{b})$$

Thm. 27: **Teorema di Definibilità**

Le funzioni calcolabili sono definibili in $\mathcal{N}$.

per induzione

- **C.B.**: le funzioni di base sono definibili in $\mathcal{N}$

  L'addizione è definita dalla formula $F(x, y, z) := ((x + y) = z)$, la moltiplicazione dalla formula $G(x, y, z) := ((x \times y) = z)$, la proiezione $\pi_i^n(x_1, \dots, x_n) = x_i$ (dove $i \in [1, n]$) è definibile dalla formula $H(x_1, \dots, x_n, z) := (x_1 = x_1 \wedge \dots \wedge x_i = z \wedge \dots \wedge x_n = x_n)$, la funzione caratteristica dell'uguaglianza dalla formula $I(x, y, z) := (x = y \wedge z = 1) \vee (x \neq y \wedge z = 0)$. □

- **chiusura per composizione**: le funzioni definibili in $\mathcal{N}$ sono chiuse per composizione

  Siano:

  $$\begin{aligned} H_1(x_1, \dots, x_k, y_1) &\quad \text{che rappresenta } \vartheta_1 \\ H_2(x_1, \dots, x_k, y_2) &\quad \text{che rappresenta } \vartheta_2 \\ &\vdots \\ H_m(x_1, \dots, x_k, y_m) &\quad \text{che rappresenta } \vartheta_m \end{aligned}$$

  E sia:

  $$G(y_1, \dots, y_m, z) \quad \text{che rappresenta } \Psi$$

  Voglio una formula $F(x_1, \dots, x_k, w)$ che rappresenti la funzione composta $\Psi(\vartheta_1, \dots, \vartheta_m)$.

  Quand'è che $(x_1, \dots, x_k, w) \in$ grafico composta$(\Psi, \vartheta_1, \dots, \vartheta_m)$? Se W è il valore di Ψ con argomenti = m valori di $\vartheta_1, \dots, \vartheta_m$ applicate a $(x_1, \dots, x_k)$.

  La formula è:

  $$\exists y_1 \dots y_m \quad \text{(se esistono gli } m \text{ valori intermedi)}$$

  tale che:

  $$H_1(x_1 \dots x_k, y_1) \wedge H_2(x_1 \dots x_k, y_2) \wedge \dots \wedge H_m(x_1 \dots x_k, y_m)$$
  $$\wedge \quad G(y_1, \dots, y_m, W) \quad \text{(valore } G(y_1 \dots y_m))$$

  NB: Questo finisce nel grafico della composta se $\exists y_1 \dots$ (se le intermedie sono indefinite, anche la composta lo è).

  Si vede che questa formula è soddisfatta $\iff$ l'elemento appartiene al grafico della composta.

  siano

- **chiusura per minimo**: le funzioni definibili in $\mathcal{N}$ sono chiuse per minimo

  Sia $H(x_1, \dots, x_k, y, z)$ una formula che rappresenta $\vartheta(x_1, \dots, x_k, y)$.

  Voglio G con variabili $(x_1, \dots, x_k, S)$ dove S è il minimo tale che:

  $$\vartheta(x_1, \dots, x_k, S) \downarrow = 0 \quad \wedge \quad \forall w \ (0 \leq w < S, \ \vartheta(x_1, \dots, x_k, w) \downarrow \neq 0)$$

  La formula risultante è:

  $$H(x_1, \dots, x_k, S, 0) \wedge \forall w (w < S \to \exists z (H(x_1, \dots, x_k, w, z) \wedge z \neq 0))$$

Def. 37: Calcolabilità e rappresentabilità di una relazione

Una relazione $R \subseteq N^n$ è calcolabile se e solo se la sua funzione caratteristica è calcolabile.

Una relazione R è rappresentabile in $\mathcal{N}$ se e solo se $\exists F(x_1, \dots, x_k)$ t.c. $\forall n_1, \dots, n_k \in \mathbb{N}$:

$$\begin{aligned} (n_1, \dots, n_k) \in R &\implies \mathcal{N} \vDash F(\bar{n_1}, \dots, \bar{n_k}) \\ (n_1, \dots, n_k) \notin R &\implies \mathcal{N} \vDash \neg F(\bar{n_1}, \dots, \bar{n_k}) \end{aligned}$$

Thm. 28: Rappresentabilità di relazioni

Tutte le relazioni calcolabili sono rappresentabili in $\mathcal{N}$

R è calcolabile se e solo se $\chi_R \in \mathcal{C}$.

Sia $F(x_1, \dots, x_k, y)$ che rappresenta χ_R.

Questo significa che $\chi_R(n_1, \dots, n_k) = b \iff \mathcal{N} \vDash F(\bar{n_1}, \dots, \bar{n_k}, \bar{b})$. Abbiamo che $b \in \{0, 1\}$.

I vettori che appartengono a R sono quelli che danno 1 (per come definiamo χ_R), quindi $F(x_1, \dots, x_k, 1)$ rappresenta R.

Ovvero, presi $(n_1, \dots, n_k) \in R$, $\chi_R(n_1, \dots, n_k) = 1 \implies \mathcal{N} \models F(\bar{n}_1, \dots, \bar{n}_k, 1)$

Se invece $(n_1, \dots, n_k) \notin R$, $\chi_R(n_1, \dots, n_k) = 0 \implies \mathcal{N} \models F(\bar{n}_1, \dots, \bar{n}_k, 0) \implies \mathcal{N} \models \neg F(\bar{n}_1, \dots, \bar{n}_k, 1)$

> L'implicazione finale vale perché:
>
> - $\mathcal{N} \models \neg(0 = 1)$
> - $\mathcal{N} \models$ "F è funzionale"
>
> (dato che F rappresenta una funzione, non ci possono essere 2 valori diversi per cui sia vera sullo stesso parametro)

Osservazione: notiamo che tutte le funzioni calcolabili hanno una simile struttuta sintattica: sono formate da quantificatori esistenziali seguiti da una formula in cui non compaiono quantificatori o essi appaiono solo "limitati" (es. $\forall x(x \leq 7 \to \dots)$) - queste formule vengono dette $\sum_1^0$.

3.3. I numeri di Gödel

Vogliamo mostrare che $Th(\mathcal{N})$ non è calcolabile mostrando che non è rappresentabile in $\mathcal{N}$.

Funzioni e relazioni calcolabili hanno come argomenti numeri naturali. Ci serve quindi poter codificare funzioni e relazioni su altri tipi di oggetti.

Gödel inventa una codifica $code$: $\{$enunciati aritmetici$\} \to \mathbb{N}$ tale che:

- ad ogni simbolo di base del linguaggio (parentesi, connettivi, variabili, simboli di funzione/relazione, costanti) viene associato un **intero positivo dispari**
- ogni formula ben formata è una sequenza $u_0, u_1, \dots, u_n$ di simboli di base, che viene codificata in questo modo:

  $$code(u_0, u_1, \dots, u_n) = 2^{code(u_0)} \cdot 3^{code(u_1)} \cdot \dots \cdot p_n^{code(u_n)}$$

- ogni derivazione è una sequenza $e_0, e_1, \dots, e_n$ di formule, che viene codificata in questo modo:

  $$code(e_0, e_1, \dots, e_n) = 2^{code(e_0)} \cdot 3^{code(e_1)} \cdot \dots \cdot p_n^{code(e_n)}$$

La funzione $code$ è iniettiva e permette di distinguere algoritmicamente tra codici di simboli di base (pari), "formule" (pari con primo esponene dispari) e "derivazioni" (pari con primo esponente pari).

Quando si parla dell'esprimibilità di un insieme di enunciati in una teoria, si intende l'esprimibilità dell'insieme dei codici numerici enunciati.

Ci chiediamo quindi se $\{cod(E) \mid \mathcal{N} \vDash E\}$ sia rappresentabile in $\mathcal{N}$ (non lo è).

3.3.1. Indecidibilità algoritmica dell'aritmetica (Tarski)

Thm. 29: **Teorema di indefinibilità di Tarski**

La verità aritmetica non può essere definita all'interno dell'aritmetica.

(L'insieme delle verità aritmetiche $Th(\mathcal{N}) = \{E \mid \mathcal{N} \vDash E\}$ non è rappresentabile in $\mathcal{N}$.)

Supponiamo per assurdo che $Th(\mathcal{N})$ sia rappresentabile. Si tratta di un insieme, quindi è descritto da una formula con una variabile libera.

Sia $T(x)$ la formula che lo rappresenta.

- $E \in Th(\mathcal{N}) \implies \mathcal{N} \vDash T(\overline{code(E)})$
- $E \notin Th(\mathcal{N}) \implies \mathcal{N} \vDash \neg T(\overline{code(E)})$

Introduciamo una nuova funzione $\delta : \mathbb{N} \to \mathbb{N}$. Dato $p \in \mathbb{N}$, δ controlla se p è il codice numerico di una formula $A(x)$ una variabile libera. Se lo è, $\delta(p) =$ codice di $A(x/\bar{p})$.

(dato p, controllo se codifica una FML $A(x)$ - se sì, scrivo $A(p)$ (metto il numerale p al posto della variabile (quindi do alla formula il suo stesso codice)), codifico la nuova stringa e restituisco il suo codice numerico q)

δ è evidentemente calcolabile (uso la tesi di Church-Turing - ogni funzione descrivibile tramite un algoritmo è calcolabile da una TM - per non doverlo dimostrare esplicitamente). In quanto calcolabile, $\delta \in \mathcal{C}$, e quindi δ rappresentabile.

Quindi, sia $D(x, y)$ una formula che rappresenta δ in $\mathcal{N}$, ovvero tale che:

$$\delta(a) = b \iff \mathcal{N} \vDash D(\bar{a}, \bar{b})$$

Consideriamo la formula

$$\forall y(D(x, y) \to \neg T(y))$$

(che dichiara "per ogni y valore di $\delta(x)$ (quindi formula $A(y/\bar{x})$ in cui $x = code(A)$), y non è un enunciato vero in $\mathcal{N}$)

Questa formula è una formula con una variabile libera x (chiamiamola $A(x)$). (In quanto tale può essere codificata).

Sia p il codice di $A(x)$.

Consideriamo $A(x/\bar{p})$, ovvero

$$\forall y(D(\bar{p}, y) \to \neg T(y))$$

(che dichiara che ogni y valore di $\delta(p)$ non è un enunciato vero in $\mathcal{N}$)

Sia q il suo codice (quindi $\delta(p) = q$).

Notiamo subito che la formula genera una contraddizione: la formula dichiara che ogni numero che sia $= \delta(p)$ non è vero in $\mathcal{N}$, ma essa stessa è uno di quei numeri (quindi sta dichiarando di "mentire" (di non essere vera)).