aglaia norza

Logica Matematica

appunti delle lezioni
libro del corso: tbd

12/11/2025

thisisaglaia@gmail.com
github.com/AglaiaNorza

Contents

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:

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

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

  il caso $0 \to 0$ deve essere vero, perché corrisponde al caso in cui $A \wedge B$ è falso perché B è falso; il caso $0 \to 0$ 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 $\alpha(A) = \alpha(B)$.

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

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

Lemma 1 **Equivalenze**

(1) $T \vDash A$

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

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

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:

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

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 $\alpha(A_1) = f_1(\alpha(p_2), \dots, \alpha(p_n))$, quindi la formula si comporta esattamente come f_1:

$$f(\alpha(p_1), \alpha(p_2), \dots, \alpha(p_n)) = f(1, \alpha(p_2), \dots, \alpha(p_n)) = f_1(\alpha(p_2), \dots, \alpha(p_n)).$$

Quindi, in questo caso, vale

$$\alpha(A) = (\alpha(p_1), \alpha(p_2), \dots, \alpha(p_n))$$

– $\alpha(p_1) = 0$
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:
>
> $$f(x_1, x_2, \dots, x_n) = \begin{cases} f_1(x_2, \dots, x_n) & \text{se } x_1 = 1, \\ f_0(x_2, \dots, x_n) & \text{se } x_1 = 0. \end{cases}$$

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:

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

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 $A, B \in \text{PROP}$ 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	$A \vee (\neg A \wedge B) \equiv A \vee B$ $A \wedge (\neg A \vee B) \equiv A \wedge B$

Table 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 soddisfca 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.

> Colorabilità

1.8. Teorema di compattezza

> Def. 7 **Monotonia della conseguenza logica**
> Si dice che la nozione di conseguenza logica è **monotona**, ovvero che
>
> $$T' \vDash A \wedge T' \subseteq T \ \Rightarrow \ T \vDash A$$
>
> (se $A_1, A_2, \ldots, A_k \vDash A$, allora $T \vDash A$ per ogni teoria T contenente $A_1, A_2, \ldots, A_k$)

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**

$\texttt{FINSAT} \Rightarrow \texttt{SAT}$, 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) $T \in \texttt{SAT} \iff T \in \texttt{FINSAT}$

- ① $\Rightarrow$ ②

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

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

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

- ② $\Rightarrow$ ①

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

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

  Per ②, quindi, $\exists T_0 \; t.c,\; T_0 \overset{fin}{\subseteq} T \vDash p \wedge \neg p$, il che va in contraddizione con $T \in \texttt{FINSAT}$. $\square$

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 $A \in B, C$. Possiamo quindi introdurre $\hat{B} = B \setminus \{A\}$ e $\hat{C} = C \setminus \{A\}$.
> 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. $T \in \texttt{FINSAT} \Rightarrow T \in \texttt{SAT}$.

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 $\texttt{FINSAT}$)

> (la definizione è ben posta per l'estendibilità di $\texttt{FINSAT}$)

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

Definiamo

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

Sappiamo che $T^* \in \texttt{FINSAT}$ 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:

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

> **Claim**: $\alpha^*(T) = 1$
> (avremmo $T \in \texttt{SAT}$, 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 $\{p_{i1}^*, \dots, p_{ik}^*\}$, abbiamo $A^* = A \cup \{p_{i1}^*, \dots, p_{ik}^*\} = \{A, p_{i1}^*, \dots, p_{ik}^*\} \overset{fin}{\subseteq} T^*$.

Dato che $T^* \in \texttt{FINSAT}$, $\exists \beta$ 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 $p_j \neg \in T^*$. 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 4), poiché $p_{i1}, \dots, p_{ik}$ sono le variabili che compongono A, segue che $\alpha(A) = \alpha(B)$.

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 $T \in \texttt{SAT}$ □

(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:

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

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 $\{A, B\} \subseteq T^* \in$ `UNSAT`, quindi $T^* \notin$ `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) $A = \neg B$

  (2) $A = B \wedge C$

  (3) $A = B \vee C$

  (4) $A = B \to C$

  TODO

□

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 $T \vDash A \wedge T \vDash \neg A$, 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 $T \models A \vee B$ 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: $\dfrac{\text{X} \qquad X \to Y}{\text{Y}}$

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**

$$\vdash A \Rightarrow \vDash A$$
$$T \vdash A \Rightarrow T \vDash A$$

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 $T \vdash A \Rightarrow T \vDash A$).

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.

Thm. 9 **Teorema di completezza**

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

idea di dimostrazione ($T \vDash A \Rightarrow T \vdash A$):
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 $\vdash (A_1 \to (A_2 \to \dots (A_n \to A) \dots)) \iff A_1, \dots, A_n \vdash A$.

1.11.1. Dimostrazione del teorema di completezza

Per dimostrare il teorema, ci saranno utili le seguenti proprietà:

(1) $T \vdash A \land T \subseteq S \Rightarrow S \vdash A$

(2) $T \vdash A \iff \exists S \overset{fin}{\subseteq} T \ \ t.c. \ \ S \vdash A$

(3) $T \vdash A \ \land \ (\forall B \in T, \ \ S \vdash B) \Rightarrow S \vdash A$