15/03

CHIARIMENTO SU SE/ALLORA

Quando la proposizione "se x allora y" $(x \Rightarrow y)$? Essa è falsa solo se A è vero mentre B è falso.
Quindi se A è falso, la relazione rimane vera !!

RELAZIONI

Una relazione è un sottoinsieme del prodotto cartesiano.

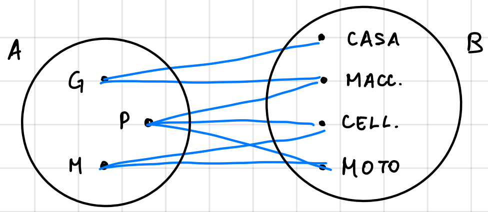
Prodotto Cartesiano

Si definisce prodotto cartesiano di $A_1, \dots, A_n$ insiemi $A_1 \times \dots \times A_n = \{(a_1, \dots, a_n) : a_1 \in A_1 \cdots a_n \in A_n\}$
Nota bene: $\{a, b\}$ è una coppia non ordinata; $(a,b) := \{a, \{b\}\}$ è una coppia ordinata (definizione data da Kuratowski)

Relazioni

Definiamo una relazione n-aria su $A_1, \dots, A_n$ $R \subseteq A_1 \times \dots \times A_n$. Di conseguenza una relazione 1-aria sarà $R \subseteq A$.

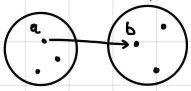
D'ora in poi parleremo principalmente di relazioni binarie $R \subseteq A_1 \times A_2$.



Notazioni:

- $R \subseteq T$ se $(a,b) \in R \Rightarrow (a,b) \in T$
- $R = T$ se $R \subseteq T$ e $T \subseteq R$
- $R \cap T = \{(a,b) \in A_1 \times A_2 : (a,b) \in R \wedge (a,b) \in T\}$
- $R \cap T = \{$ " " : " $\vee$ " $\}$
- $(a,b) \in R = aRb$

Come rappresentiamo una relazione binaria?

1) A e B sono insiemi finiti $(|A||B| < +\infty)$
   - grafo di adiacenza:  disegno la freccia se aRb

   - matrice di adiacenza: fissiamo un ordinamento di $A_1 = \{\overset{I}{G}, \overset{II}{P}, \overset{III}{M}\}$ e $A_2 = \{\overset{I}{CA}, \overset{II}{MA}, \overset{III}{CE}, \overset{IV}{MO}\}$ e definisco una matrice $A \in Mat(|A_1| \times |A_2|, \{0,1\})$ di cui gli elementi saranno

$$a_{ij} = \begin{cases} 1 & \text{se } (a_i, a_j) \in R \\ 0 & \text{altrimenti} \end{cases} \Rightarrow M_R = \begin{array}{c} \\ G \\ P \\ M \end{array} \begin{array}{c} \begin{array}{cccc} CA & MA & CE & MO \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

Come si comporta la matrice di adiacenza in presenza di unione ed intersezione?
- intersezione: vengono presi gli 1 presenti in entrambe le matrici $\Rightarrow (M_{R\cap T})_{ij} = (M_R)_{ij} (M_T)_{ij}$
- unione: vengono presi tutti gli 1 $\Rightarrow (M_{R \cup T})_{ij} = M_R \oplus M_T$ → somma booleana

Prodotto di relazioni

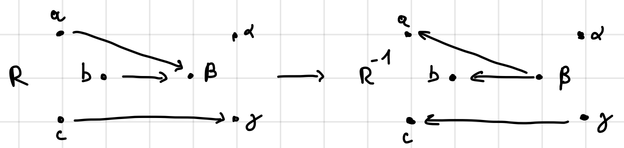
Prendiamo due relazioni $R \subseteq A_1 \times \underline{A_2}$ e $T \subseteq \underline{A_2} \times A_3$ definiamo allora il prodotto
$R \cdot T \subseteq A_1 \times A_3 = \{(a,c) \in A_1 \times A_3 : \exists b \in A_2 : (a,b) \in R \wedge (b,c) \in T\}$

Supponiamo di conoscere $M_R \in Mat(|A_1|\times|A_2|, \{0,1\})$ e $M_T \in Mat(|A_2|\times|A_3|, \{0,1\})$, posso scrivere $(M_R M_T)_{ij} = \sum_{k=1}^{|A_2|} (M_R)_{ik}(M_T)_{kj}$
Il valore di $(M_R M_T)_{ij}$ rappresenta il numero di cammini possibili tra i nodi i e j degli insiemi di arrivo e partenza.
Se eseguiamo $M_R M_T$ ponendo tutti gli elementi maggiori di zero pari a 1, otteniamo la matrice d'adiacenza di $R \cdot T$.

Il prodotto di relazioni è associativo, ma non commutativo. Esso, inoltre, è anche compatibile con l'inclusione:
se $R \subseteq T \subseteq A_1 \times A_2$, $S \subseteq U \subseteq A_2 \times A_3$ allora $R \cdot S \subseteq T \cdot U$.

Inversa di una relazione

Data una relazione $R \subseteq A_1 \times A_2$, l'inversa della relazione è $R^{-1} \subseteq A_2 \times A_1 = \{(b,a) \in A_2 \times A_1 : (a,b) \in R\}$



Se M_R è la matrice d'incidenza di R, quella di R^{-1} sarà $M_{R^{-1}} = M_R^T$. Inoltre, è lecito scrivere che $R \cdot R^{-1} \subseteq A_1 \times A_1$ e $R^{-1} \cdot R \subseteq A_2 \times A_2$.

Relazioni binarie su di un unico insieme ($R \subseteq A \times A$)

Le relazioni binarie su un unico insieme hanno matrice di adiacenza quadrata. Di conseguenza, il prodotto di relazioni è sempre possibile e possiamo definire le potenze di relazioni (valgono le solite proprietà delle potenze).
Delle relazioni notevoli di questo tipo sono:
- La relazione vuota $\emptyset$
- La relazione identità I_A (nota: $R^0 = I_A$)
- La relazione universale ω_A

Estendendo l'osservazione sul prodotto matriciale effettuata prima, possiamo affermare che $(M_R^K)_{ij}$ è il numero di percorsi di lunghezza K tra i e j

Una relazione binaria ha delle interessanti proprietà:
- si definisce seriale una relazione che soddisfa: $\forall a \in A \ \exists b \in A \ (a,b) \in R$ (ogni riga di M_R ha un 1)
- " " riflessiva " " " " : $\forall a \in A \ (a,a) \in R$ (la diagonale di M_R ha solo 1)
- " " simmetrica " " " " : $\forall a,b \in A$ se $(a,b) \in R \Rightarrow (b,a) \in R$ (M_R è simmetrica)
- " " antisimmetrica " " " " : $\forall a,b \in A$ se $(a,b) \in R$ e $(b,a) \in R \Rightarrow a = b$
- " " transitiva " " " " : $\forall a,b,c \in A$ se $(a,b) \in R$ e $(b,c) \in R \Rightarrow (a,c) \in R$ (R è transitiva $\Leftrightarrow R^2 \subseteq R$)
  - se una relazione è transitiva, per ogni percorso abbiamo una connessione tra inizio e fine.

Quasi nessuna di queste proprietà implica le altre: Seriale $\not\Rightarrow$ Riflessiva; Antisimmetrica $\not\Rightarrow$ Non simmetrica
Transitiva e simmetrica $\not\Rightarrow$ riflessiva. Però abbiamo che Riflessiva $\Rightarrow$ Seriale e Transitività, simmetria, serialità $\Rightarrow$ riflessiva

Come si comportano unione, intersezione, prodotto e inversione rispetto alle proprietà precedenti?

	$\cap$	$\cup$	$\cdot$	-1
SERIALE	✗	✓	✓	✗
RIFLESSIVA	✓	✓	✓	✓
SIMMETRICA	✓	✓	✗	✓
ANTISIMMETR.	✓	✗	✗	✓
TRANSITIVA	✓	✗	✗	✓

Chiusura di una relazione

Dato P un insieme di proprietà, la P-chiusura di $R \subseteq A \times A$ è una relazione $T \subseteq A \times A$ se $R \subseteq T$ e T è la più piccola relazione che soddisfa P.

Conseguenza della definizione è che $\forall S \subseteq A \times A$ che soddisfa P e $R \subseteq S$, $T \subseteq S$. Quindi la P-chiusura è unica.
DIMOSTRAZIONE: Prendiamo T_1 come P-chiusura e T_2 anch'essa P-chiusura. Per le proprietà sopra otteniamo $T_1 \subseteq T_2$ e $T_2 \subseteq T_1 \Rightarrow T_1 = T_2$.

Un'altra conseguenza è che se R stesso rispetta P, allora esso sarà chiusura di sé stesso.

Il seguente teorema descrive le condizioni per l'esistenza della P-chiusura di R:

Consideriamo $R \subseteq A \times A$ e fissiamo P l'insieme di proprietà. Se:
1. $\exists H \subseteq A \times A$ che soddisfa P e $R \subseteq H$
2. L'intersezione di relazioni che soddisfano P è a sua volta una relazione che soddisfa P

allora esiste la P-chiusura di R.

Usando il teorema sopra, possiamo affermare che per $P \subseteq \{$Riflessiva, Transitiva, Simmetrica$\}$ esiste sempre la P-chiusura di $R \subseteq A \times A$ e viene indicata $\bar{R}^P$. Le altre proprietà, in generale, non possono essere chiuse.

Chiusura riflessiva

Per chiudere riflessivamente una relazione R, basta aggiungere tutti cappi mancanti: $\bar{R}^{RIFL.} = R \cup I_A$ $(M_R \oplus I)$

Chiusura simmetrica

Per chiudere simmetricamente una relazione R, basta aggiungere tutte le frecce al contrario: $\bar{R}^{SIMM} = R \cup R^{-1}$ $(M_R \oplus M_R^T)$

Chiusura transitiva

Per chiudere transitivamente R, bisogna fare:
- $\bar{R}^{TR} = \bigcup_{K \geq 1} R^K$ dove K è la lunghezza del percorso più lungo
- $M_{\bar{R}^{TR}} = M_R \oplus M_R^2 \oplus M_R^3 \oplus \cdots \oplus M_R^i$ dove i è il piccolo indice soddisfa $M_R^{i+1} \subseteq M_R \oplus \cdots \oplus M_R^i$

DIMOSTRAZIONE: Sia $H = \bigcup_{K>0} R^K$. Dimostriamo che H è chiusura di R:

1) $R \subseteq H$
2) È transitiva: $(a,b),(b,c) \in H \Rightarrow (a,b) \in R^i$ $(b,c) \in R^{i+j} \Rightarrow (a,c) \in R^{i+j} \subseteq H$
3) Sia S una relazione $R \subseteq S$ ed è transitiva. Avremo che $R \subseteq S \Rightarrow R^2 \subseteq SR$ e $R \subseteq S \Rightarrow SR \subseteq S^2$ e quindi $R^2 \subseteq S^2$
Siccome S è transitiva otteniamo che $R^2 \subseteq S^2 \subseteq S \Rightarrow R^2 \subseteq S$. Consideriamo $R^3 = R^2 \cdot R \subseteq SR \subseteq S^2 \subseteq S$, quindi $R^3 \subseteq S$.
Continuando così, possiamo affermare che $H = \bigcup_{K>0} R^K \subseteq S$. Quindi H è la più piccola relazione transitiva che contiene R.

Chiusura riflessiva + simmetrica

$$\bar{R}^{R+S} = R \cup R^{-1} \cup I_A$$

$$M_{\bar{R}^{R+S}} = M_R \oplus M_R^T \oplus I$$

Chiusura riflessiva + transitiva

$$\bar{R}^{R+T} = \bigcup_{K>0} R^K \cup I_A = \bigcup_{K \geq 0} R^K$$

Chiusura simmetrica + transitiva

$$\overline{R}^{S+T} = \bigcup_{K>0} (R \cup R^{-1})^K$$!! Prima chiudo simmetricamente poi transitivamente

Chiusura simmetrica + riflessiva + transitiva

$$\overline{R}^{RST} = \bigcup_{K\geq 0} (R \cup R^{-1})^K$$!! Prima chiudo simmetricamente poi transitivamente.

Relazione d'equivalenza

Si dice una relazione d'equivalenza una relazione che è simmetrica, riflessiva e transitiva. La chiusura d'equivalenza esiste sempre in quanto si può sempre chiudere riflessivamente, simmetricamente e transitivamente.

Con il grafo d'adiacenza di una relazione la chiusura equivalente è immediata: basta saturare ogni connessione in ogni sezione connessa.

Se $R, T \subseteq A\times A$, avremo che $R\cap T$ è ancora d'equivalenza, R^{-1} è transitiva, $R\cup T$ e $R\cdot T$ in generale non sono transitivi

ESEMPIO: Relazione modulo $n \in \mathbb{N}_{>0}$ $\equiv_n \subseteq \mathbb{Z}\times\mathbb{Z}$: $(a,b)\in \equiv_n$ se $a-b=Kn$ $K\in\mathbb{Z}$. Dati $a=K_1 n + r_a$ e $b=K_2 n + r_b$.
Avremo che $a-b=(K_1-K_2)n+(r_a-r_b)$ quindi $a\equiv_n b \iff r_a=r_b$.
Dimostriamo che $\equiv_n$ è di equivalenza:
1) riflessiva: $n \mid a-a=0$ n è sempre divisore di 0
2) simmetrica: $n\mid a-b = n\mid b-a$
3) transitiva: $n\mid a-b$ e $n\mid b-c$, quindi $r_a=r_b$ e $r_b=r_c$ e quindi $r_a=r_c \Rightarrow n\mid a-c$

Si può pensare alle relazioni di equivalenza come una generalizzazione dell'eguaglianza.

Classe d'equivalenza

Sia $\rho \subseteq A\times A$ di equivalenza, dato un elemento $a\in A$ la classe d'equivalenza con rappresentante a rispetto ρ è:

$$[a]_\rho := \{ b\in A : (a,b)\in\rho \}$$

L'insieme delle classi d'equivalenza di ρ è chiamato insieme quoziente ed è indicato con $A/\rho := \{ [a]_\rho \ a\in A\}$

Una partizione è una collezione di insiemi A_i con $i\in I$ e $A_i\subseteq A$: $\bigcup_{i\in I} A_i = A$ e $\forall i,j\in I$ $i\neq j$ $A_i\cap A_j=\emptyset$. È facile capire che A/ρ forma una partizione di A. Viceversa, se A_i, $i\in I$ è una partizione di A, posso definire una relazione d'equivalenza σ tale che $A/\sigma = \{A_i \ i\in I\}$

Relazione d'ordine

Data una relazione $R\subseteq A\times A$, essa è d'ordine se è riflessiva, transitiva e antisimmetrica

Si può pensare alle relazioni d'ordine come una generalizzazione di $\leq$. Infatti si usa $\leq$ per indicare una relazione d'ordine.

Se $\forall a,b\in A$ $a\leq b$ o $b\leq a$ allora la relazione d'ordine è totale. Se invece $\exists a,b\in A$: $a\not\leq b$ e $b\not\leq a$ allora a e b si dicono non-confrontabili.

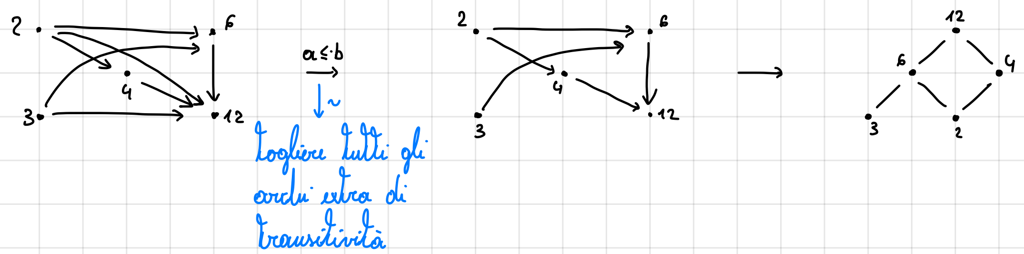
La coppia $(A,\leq)$ con $\leq$ relazione d'ordine si chiama POSET (Partially Ordered Set)

La chiusura d'ordine non sempre esiste perché in generale la chiusura antisimmetrica. Per tentare di chiudere una R antisimmetrica bisogna prima chiudere riflessivamente e transitivamente. Se quest'ultima chiusura è antisimmetrica, allora essa è la chiusura d'ordine di R.

Diagramma di Hasse di un Poset

Sia $\leq \subseteq A \times A$ d'ordine. Diciamo che b copre a se $a \leq b$ e non esiste alcun $c \in A$ $c \neq a, b$: $a \leq c$ e $c \leq b$ (si indica $a \lessdot b$)
Si definisce diagramma di Hasse di $(A, \leq)$ un diagramma così costruito:
1) Nel grafo di adiacenza di $\leq$ considero solo gli archi $a \to b$ con $a \lessdot b$
2) Si orientano gli archi dall'alto verso il basso: $a \to b \implies$ b sopra a

ESEMPIO: $A = \{2, 3, 4, 6, 12\}$, $\leq \subseteq A \times A$ $a \leq b$ se $a | b$ (a divide b)



Minimo, minimale, massimo e massimale

Dato $(A, \leq)$ un Poset allora $a \in A$ è minimo se $\forall x \in A$ $a \leq x$ e massimo se $\forall x \in A$ $a \geq x$. Minimo e massimo sono unici.

Chiamiamo minimale un elemento $a \in A$ tale che se $x \leq a \Rightarrow x = a$. Analogamente il massimale è un $a \in A$: se $x \geq a \Rightarrow x = a$.
Se minimo o massimo esistono, essi saranno rispettivamente minimale o massimale e, in più, non esistono altri minimali o massimali che non sono minimi o massimi. Un minimale / massimale non per forza è un minimo / massimo

Se A è finito e in $(A, \leq)$ abbiamo un unico minimale (massimale) a, allora a è minimo (massimo). Se A è infinito, invece, la proposizione precedente non è valida.

Maggioranti, minoranti, estremo superiore e inferiore

Sia $(A, \leq)$ un Poset e $B \subseteq A$. Abbiamo che $m \in A$ si dice maggiorante se $\forall x \in B$ $x \leq m$ e minorante se $\forall x \in B$ $x \geq m$.
Chiamiamo, quindi, estremo superiore di $B \subseteq A$ il minimo dei maggioranti di B ed estremo inferiore il massimo dei minoranti.

Reticoli

Definiamo reticolo un Poset $(A, \leq)$ per cui $\exists \inf\{a, b\}$, $\exists \sup\{a, b\}$ $\forall a, b \in A$. I reticoli si possono assiomatizzare come strutture algebriche

FUNZIONI

Una funzione $f: A \to B$ è una relazione $f \subseteq A \times B$: $\forall a \in A$ $\exists! b \in B$: $(a, b) \in f$. Visto che l'elemento b associato ad a è unico e dipende da a (per definizione), invece di scrivere $(a, b) \in f$ si usa $b = f(a)$.

Data $f: A \to B$ con $b = f(a)$, chiamiamo:
- A dominio di f e B codominio
- $b \in B$ immagine di a.
- $a \in A$ controimmagine di b: $f^{-1}(b) = \{a \in A : f(a) = b\}$. !! $f^{-1}(E)$ può essere $\emptyset$, $f(C)$ non è mai vuoto

Composizione di funzioni

Data $f: A \to B$ e $g: B \to C$, allora il prodotto (o composizione) delle funzioni $f \cdot g$ è una funzione $f \cdot g : A \to C$.
La dicitura $f \cdot g$ è equivalente a $g \circ f(a) = g(f(a))$. Si dimostra che $I_A \cdot f = f$ e $f \cdot I_B = f$

Funzione inversa

La relazione inversa f^{-1} non sempre è una funzione. La prima condizione è che f sia iniettiva:

$$\left.\begin{array}{l} - \text{ se } f(a_1)=f(a_2) \Rightarrow a_1=a_2 \\ - \text{ se } a_1 \neq a_2 \Rightarrow f(a_1)\neq f(a_2) \\ - \ \forall b \in B \quad f^{-1}(b) \text{ contiene al più un elemento} \end{array}\right\} \text{Equivalenti}$$

Date $f: A \to B$ e $g: B \to C$, possiamo dire:

1) se f, g è iniettiva allora $f \cdot g$ è iniettiva
2) se $f \cdot g$ è iniettiva allora f è iniettiva.

L'iniettività non basta per rendere f^{-1} una funzione. Infatti può essere che la funzione f non copra tutto il codominio, rendendo la relazione inversa non funzione. Possiamo allora completare la relazione inversa con: $d = f^{-1} \cup \{(x, a_1) \quad x \in B / f(A)\}$ ($a_1 \in A$ scelto a caso). d soddisfa $f \cdot d = I_A$ ed è detta inversa destra. Si può dimostrare che f è iniettiva se e solo se f ammette inversa destra.

La seconda condizione affinché f^{-1} sia una funzione è che sia suriettiva:

$$\left.\begin{array}{ll} 1) & \forall b \in B \quad \exists a \in A : f(a)=b \\ 2) & \forall b \in B \quad |f^{-1}(b)| \geq 1 \\ 3) & f(A) = B \end{array}\right\} \text{Equivalenti}$$

Date $f: A \to B$ e $g: B \to C$ allora:

1) se f, g sono suriettive allora $f \cdot g$ è suriettiva
2) se $f \cdot g$ è suriettiva allora g è suriettiva

Analogamente all'iniettività, f è suriettiva se e solo se possiede l'inversa sinistra ossia $\exists s: B \to A: \quad s \cdot f = I_B$. La funzione s la definiamo come $s = \forall b \in B \quad s(b) = a$ con a scelto a caso in $f^{-1}(b)$.

Diciamo che f è biettiva se e solo se f possiede inversa destra e sinistra. Le due inverse coincidono e sono la funzione inversa di f $\; f^{-1} = s = d$

Funzione mappa

Data $\rho \subseteq A \times A$ d'equivalenza, posso costruire $\pi_\rho: A \to A/\rho$ con $\pi_\rho(a) = [a]_\rho \ \forall a \in A$ detta mappa canonica di ρ.

La mappa canonica di ρ è suriettiva poiché $\forall [b]_\rho \in A/\rho \quad \pi_\rho(b) = [b]_\rho$ e una inversa sinistra è: $s: A/\rho \to A$ con $s([a]_\rho) = a$

Nucleo di funzione

Data una funzione $f: A \to B$, definiamo il nucleo di f $\operatorname{Ker} f \subseteq A \times A$ come una relazione tale che $(a_1, a_2) \in \operatorname{Ker} f$ se $f(a_1) = f(a_2)$.
La relazione $\operatorname{Ker} f$ è di equivalenza.

Le classi di equivalenza di $\operatorname{Ker} f$ sono $[a]_{\operatorname{Ker} f} = f^{-1}(a)$

Teorema di fattorizzazione

Data $f: A \to B$, usando il nucleo di f è possibile costruire $\pi_{\operatorname{Ker} f}: A \to A/\operatorname{Ker} f$. Esiste un'unica funzione iniettiva $g: A/\operatorname{Ker} f \to B$ tale che $f = \pi_{\operatorname{Ker} f} \cdot g$. Inoltre se f è suriettiva, g è biunivoca.

CARDINALITÀ DI UN INSIEME

Due insiemi A e B hanno la stessa cardinalità (equipotenti, $|A| = |B|$) se esiste $g: A \to B$ biunivoca. Se $h: A \to B$ è iniettiva, allora $|A| \leq |B|$, nel caso in cui $\nexists g: A \to B$ biunivoca scriviamo $|A| < |B|$.

Se A è finito, allora può essere messo in relazione biunivoca con $\{1, \ldots, n\}$. Diciamo che A è numerabile se $|A| = |\mathbb{N}|$.

Possiamo dire che:

1) $|\mathbb{Z}| = |\mathbb{N}|$
2) $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$
3) $|\mathbb{Q}| = |\mathbb{N}|$
4) Σ alfabeto finito, $|\Sigma^*| = |\mathbb{N}|$
5) Una famiglia di insiemi A_i $i \in I$ con $|I| \leq |\mathbb{N}|$ e $|A_i| \leq |\mathbb{N}| \Rightarrow |\bigcup_{i \in I} A_i| \leq |\mathbb{N}|$
6) $|\mathbb{R}| > |\mathbb{N}|$ → argomento di Cantor: diagonalizzazione.

Teorema di Cantor

Prendiamo A infinito ($|A| \geq |\mathbb{N}|$) allora l'insieme delle parti di A $2^A = P(A) = \{B : B \subseteq A\}$ ha cardinalità $|P(A)| > |A|$

L'infinito più piccolo di tutti ($|\mathbb{N}|$) viene detto $\aleph_0$. Quello successivo è $|\mathbb{R}| = \aleph_1$. Quelli superiori si costruiscono usando il teorema sopra. Non è ancora stato dimostrato se esiste A: $|\mathbb{N}| < |A| < |\mathbb{R}|$ (Ipotesi del continuo).

LOGICA PROPOSIZIONALE

Definiamo la sintassi:
- alfabeto: lettere enunciative
- connettivi: $\sim$ (NOT), $\wedge$ (AND), $\vee$ (OR), $\Rightarrow$ (se-allora), $\Leftrightarrow$ (se-solo-se)
- simboli ausiliari: (,)

Tra le stringhe formate con l'alfabeto sopra definiamo le formule ben formate:
- ogni lettera enunciativa è una formula ben formata
- se $\mathcal{A}$ e $\mathcal{B}$ sono formule ben formate, allora $(\mathcal{A} \Rightarrow \mathcal{B})$, $(\mathcal{A} \wedge \mathcal{B})$, $(\mathcal{A} \vee \mathcal{B})$, $(\mathcal{A} \Leftrightarrow \mathcal{B})$ e $(\sim \mathcal{A})$ sono formule ben formate

C'è una priorità tra i connettivi per ridurre il numero di parentesi:

	SIMBOLO	ASSOCIATIVITÀ
PRIORITÀ MAGG:	$\sim$	SX
	$\wedge$	SX
	$\vee$	SX
	$\Rightarrow$	SX
PRIORITÀ MIN:	$\Leftrightarrow$	SX

Dobbiamo ora definire la semantica. Definiamo l'interpretazione $v: \{\mathcal{F} : \mathcal{F} \text{ ben formata}\} \to \{0,1\}$ che soddisfa:
- $v(\sim \mathcal{A}) = 1 - v(\mathcal{A})$
- $v(\mathcal{A} \wedge \mathcal{B}) = \min\{v(\mathcal{A}), v(\mathcal{B})\}$
- $v(\mathcal{A} \vee \mathcal{B}) = \max\{v(\mathcal{A}), v(\mathcal{B})\}$
- $v(\mathcal{A} \Rightarrow \mathcal{B}) = \max\{1 - v(\mathcal{A}), v(\mathcal{B})\}$
- $v(\mathcal{A} \Leftrightarrow \mathcal{B}) = \min\{\max\{1 - v(\mathcal{A}), v(\mathcal{B})\}, \min\{v(\mathcal{A}), 1 - v(\mathcal{B})\}\}$

Le tavole di verità sono la rappresentazione delle varie interpretazioni v:

$v(\mathcal{A})$	$v(\mathcal{B})$	$v(\mathcal{A} \wedge \mathcal{B})$	$v(\mathcal{A} \vee \mathcal{B})$	$v(\mathcal{A} \Rightarrow \mathcal{B})$	$v(\mathcal{A} \Leftrightarrow \mathcal{B})$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Diciamo che $\mathcal{F}$ ben formata è soddisfacibile se esiste un'interpretazione v tale che $v(\mathcal{F}) = 1$, in questo caso v si chiama modello. Se Γ è un insieme di formule ben formate, Γ si dice soddisfacibile se esiste un modello per tutte le formule di Γ.

Definiamo tautologia una formula ben formata che per ogni interpretazione ha $v(F)=1$. La indichiamo con $\models F$

Definiamo una formula ben formata A conseguenza semantica di un insieme di formule Γ se ogni modello v di Γ è anche modello di A. Indichiamo ciò con $\Gamma \models A$. Se $\emptyset \models A$, allora A è una tautologia (tutte le interpretazioni sono modelli di $\emptyset$) e abbreviamo in $\models A$

Enunciamo il teorema di deduzione semantica: $\Gamma \cup \{B\} \models A \iff \Gamma \models B \Rightarrow A$. Enunciamo anche il legame tra insoddisfacibilità e conseguenza semantica: $\Gamma \models A \iff \Gamma \cup \{\sim A\}$ è insoddisfacibile

DIMOSTRAZIONE (2): $\Rightarrow$) Sia v un'interpretazione, abbiamo due casi:
- v è modello di Γ, quindi per ipotesi $v(A)=1 \Rightarrow v(\sim A)=0 \Rightarrow$ non è modello di $\Gamma \cup \{\sim A\}$
- v non è modello di Γ, quindi a maggior ragione non è modello di $\Gamma \cup \{\sim A\}$

$\Leftarrow$) Consideriamo v modello di Γ:
- v è modello di A, quindi non è modello di $\sim A$ e quindi $\Gamma \models A$
- v non è modello di A, quindi è modello $\sim A$ e $\Gamma \cup \{\sim A\}$ è soddisfacibile, contraipotesi.

Diciamo che A e B sono semanticamente equivalenti ($A \equiv B$) se $A \models B$ e $B \models A$. Abbiamo che $\equiv$ è di equivalenza. Qual è allora la cardinalità di $F_n/\equiv$ ($F_n = \{A$ con $A_1, \dots, A_n$ lettere enunciative$\}$)? Sarà il numero di tavole di verità con n colonne. Poiché ogni tabella ha 2^n righe ognuna con 2 valori, ci saranno 2^{2^n} tavole.

Ricavare predicati dalla tabella di verità

Vedi ACSO:
- forma normale congiuntiva: seconda forma canonica
- forma normale disgiuntiva: prima forma canonica

Chiamiamo formule complete le formule $\{\sim, \vee\}$, $\{\sim, \wedge\}$ e $\{\sim, \Rightarrow\}$.

TEORIA FORMALE

Una teoria formale è definita solo quando sono fissati: un alfabeto, un insieme di simboli privilegiati, un insieme privilegiato di stringhe, un insieme di regole d'inferenza che permette di scrivere in modo algoritmico altre stringhe dato un certo insieme di stringhe.

Data una teoria formale H chiamiamo dimostrazione una sequenza finita di stringhe che siano assiomi o formule dedotte dalle precedenti tramite una regola d'inferenza. Diciamo teorema della teoria una stringa A e scriviamo $\vdash_H A$ che sia l'ultima formula di una dimostrazione.

Dato un insieme Γ di stringhe diciamo che una formula A è deducibile in H da Γ e scriviamo $\Gamma \vdash_H A$ se esiste una sequenza finita di stringhe che siano o assiomi o formule di Γ o formule dedotte dalle precedenti tramite le regole d'inferenza la cui ultima formula sia A. Un teorema di H è, quindi, una formula deducibile da Γ vuoto.

Teoria L o Sistema Hilbertiano

È una teoria che permette di ottenere tutte e solo le tautologie come teoremi e permette di dedurre da un insieme Γ di formule tutte e sole le conseguenze semantiche di Γ.

La sintassi è formata da formule ben formate usando solo $\sim$ e $\Rightarrow$. Sono definiti anche i seguenti assiomi:

$$\left.\begin{array}{ll} A_1: & A \Rightarrow (B \Rightarrow A) \\ A_2: & (A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C)) \\ A_3: & (\sim A \Rightarrow \sim B) \Rightarrow ((\sim A \Rightarrow B) \Rightarrow A) \end{array}\right\}$$ gli assiomi sono indipendenti e tautologici

Questi assiomi, in verità, sono schemi di assiomi poichè A, B, C non sono lettere predicative.

Definiamo la regola d'inferenza: se $A,\ A \Rightarrow B \vdash_L B$. Se da un insieme Γ e dagli assiomi A_x con la regola d'inferenza ottengo una sequenza $D_1, \dots, D_n$ di formule tali che $\Gamma \cup A_x \vdash_L D_1, \dots, \Gamma \cup \{D_1\} \cup A_x \vdash_L D_2, \dots$ $\Gamma \cup \{D_1, \dots, D_{n-1}\} \cup A_x \vdash D_n$ allora diciamo che D_n è un teorema della teoria che ha per premesse Γ e che $D_0, \dots, D_n$ è una dimostrazione D_n e scriviamo $\Gamma \vdash_L D_n$

ESEMPIO Troviamo una dimostrazione di $\vdash_L A \Rightarrow A$:

1) con A_1 con $B = A$ scrivo la formula $D_1 = A \Rightarrow (A \Rightarrow A)$
2) " A_2 con $B = A \Rightarrow A$ " " " $D_2 = A \Rightarrow ((A \Rightarrow A) \Rightarrow A)$
3) " A_3 con $B = A$, $C = A$ " " " $D_3 = (A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$
4) Regola d'inferenza tra D_3 e D_2 $D_4 = ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$
5 " " " D_1 e D_4 $D_5 = A \Rightarrow A$

Teorema di correttezza e completezza

La teoria L è corretta se $\Gamma \vdash_L A \Rightarrow \Gamma \models A$. La teoria L è completa se $\Gamma \models A \Rightarrow \Gamma \vdash_L A$. Quindi $\Gamma \models A \Leftrightarrow \Gamma \vdash_L A$

Quindi verificare che $\Gamma \vdash_L A$ sembra indecidibile, ma grazie al teorema sopra mi basta solo verificare che $\Gamma \models A$

Risoluzione

È basato sulla refutazione, ossia Λ è insoddisfacibile se e solo se $\Lambda \vdash_R \square$. Definiamo innanzitutto una terminologia:

1) Letterale: una lettera enunciativa o la sua negata
2) Clausola: insieme o disgiunzione di letterali. Chiamiamo clausola vuota $\square = \{\}$

Per estrarre le clausole da A dobbiamo:

1) portare A in forma normale congiunta
2) costruire n insiemi di letterali dalle n congiunzioni

$\{A, \sim A\} = \{\}$

Possiamo ora definire la risoluzione:

1) Insieme numerabile di letterali
2) Le clausole su letterali e $\square$ sono stringhe privilegiate
3) Regola d'inferenza: diciamo che la clausola R è risolvente di $c_1 = \{\dots, A, \dots\}$ e $c_2 = \{\dots, \sim A, \dots\}$ con $c_1, c_2 \vdash R = c_1 \setminus \{A\} \cup c_2 \setminus \{\sim A\}$
   !! Non vanno rimossi più letterali contemporaneamente !!

Sia Λ^c l'insieme di clausole, una derivazione per risoluzione della clausola C dalle clausole Λ^c, $\Lambda^c \vdash_R C$ è una sequenza $A_1, \dots, A_m$ di clausole tale che $A_m = C \wedge \Lambda^c \vdash_R A_1,\ \Lambda^c \cup \{A_1\} \vdash A_2, \dots, \Lambda^c \cup \{A_1, \dots, A_{m-1}\} \vdash_R A_m = C$ e ciascun A_i è risolvente di due clausole in $\Lambda^c \cup \{A_1, \dots, A_{i-1}\}$.

Possiamo, quindi, enunciare il teorema di correttezza e completezza: Λ è insoddisfacibile se e solo se $\Lambda^c \vdash \square$.
L'algoritmo di verifica di $\Gamma \models A$ è, quindi, facile da implementare:

1) $\Lambda = \Gamma \cup \{\sim A\}$
2) costruisco Λ^c
3) $Ris(\Lambda^c) = \Lambda^c \cup \{R_{ij} : R_{ij}$ è una risolvente di $c_i, c_j \in \Lambda^c\}$. Itero eseguendo $Ris^n(\Lambda^c) = Ris(Ris^{n-1}(\Lambda^c))$ e verifico che $\square \in Ris^n(\Lambda^c)$ per qualche n
4) Se $Ris^m(\Lambda^c) = Ris^{m-1}(\Lambda^c)$ termino. Se $\square \in Ris^{m-1}(\Lambda^c)$ allora $\Gamma \models A$
   !! Tale m esiste sempre se Λ^c è finito poiché tutte le possibili clausole sono 2^i dove i è il numero di simboli !!

Molto più espressiva della logica proposizionale. Permette di esprimere frasi del tipo: "per ogni intero x, se x divide y, allora per ogni z, x divide z·y". Ogni formula avrà un dominio in cui interpreterò la formula.

Definiamo l'alfabeto:
- costanti: a, b, c, ... al più numerabili
- variabili: $x_1, x_2, \dots, x_n$ al più numerabili
- lettere funzionali: $f_1^{n_1}, f_2^{n_2}, \dots, f_i^{n_i}$ al più numerabili dove n_i indica l'arità della lettera funzionale. Useremo la notazione più semplice $P(x,y,z)$ dove l'arità è implicita dal numero di variabili. Modellano funzioni con arità n_i.
- lettere predicative: $A_1^{n_1}, A_2^{n_2}, \dots, A_i^{n_i}$ al più numerabili dove n_i indica l'arità. Anche qua useremo la notazione con arità implicita. Modellano relazioni di arità n_i
- connettivi: $\sim, \wedge, \vee, \Rightarrow, \Leftrightarrow$
- quantificatori: $\forall$ (universale), $\exists$ (esistenziale). Quantificano le variabili
- simboli ausiliari:), (

Definiamo termine:
- ogni variabile
- ogni costante
- induttivamente se $t_1, \dots, t_m$, se f_i^m è una lettera funzionale di arità m, allora $f_i^m(t_1 \dots t_m)$

Definiamo formula atomica (analogo delle lettere enunciative), essendo A^n una lettera predicativa di arità n e $t_1, \dots, t_n$ termini, $A^n(t_1, \dots, t_n)$. Le formule atomiche, quindi, possiedono un valore di verità.

Possiamo ora definire le formule ben formate: ogni formula atomica è ben formata; se A è ben formata, allora $(\sim A)$, $(\exists A)$ e $(\forall A)$ sono ben formate; se A e B sono ben formate allora $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$, $(A \Leftrightarrow B)$ sono ben formate e nient'altro lo è.

Definiamo la priorità:

	SIMBOLO	ASSOCIATIVITÀ
+	$\sim, \exists, \forall$	ordine di scrittura
	$\wedge$	SX
	$\vee$	SX
	$\Rightarrow$	SX
-	$\Leftrightarrow$	SX

Definiamo il campo d'azione di un quantificatore la sottoformula a cui quel quantificatore si riferisce. Se una variabile cade nel campo d'azione di un quantificatore, essa si dice vincolata, altrimenti libera. Se una variabile è vincolata, posso rinominarla dentro il campo d'azione. Definiamo una formula chiusa una formula che non ha variabili libere. Se la formula dipende da variabili libere posso farne la chiusura:
- universale: $\forall x_1 \dots \forall x_n\ F(x_1, \dots, x_n)$
- esistenziale: $\exists x_1 \dots \exists x_n\ F(x_1, \dots, x_n)$

Un termine $t(\dots y \dots)$ si dice libero per una variabile x libera nella formula se nessuna occorrenza libera di x cade nel campo d'azione di un quantificatore $\exists y$.