

**CHIARIMENTO SU SE/ALLORA**

Quando la proposizione "x è 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.

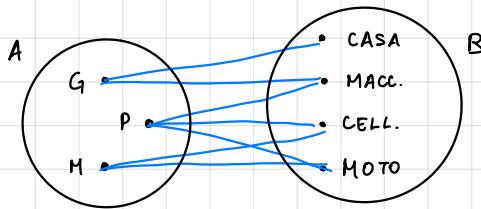
**Prodotto Cartesiano**

Si definisce prodotto cartesiano di  $A_1, \dots, A_n$  insiemni  $A_1 \times \dots \times A_n = \{(a_1, \dots, a_n) : a_1 \in A_1, \dots, a_n \in A_n\}$   
Nota bene:  $\{\alpha, b\}$  è una coppia non ordinata;  $(\alpha, b) := \{\alpha, \{b\}\}$  è una coppia ordinata (definizione obbligata 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 verrà  $R \subseteq A$ .

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  $T \subseteq R$
- $R \cap T = \{(a, b) \in A_1 \times A_2 : (a, b) \in R \wedge (a, b) \in T\}$
- $R \cup T = \{ \text{ " } \text{ " } : \text{ " } \vee \text{ " } \}$
- $(a, b) \in R = a R b$

Come rappresentiamo una relazione binaria?

1) A e B sono insiemni finiti ( $|A|, |B| < +\infty$ )

- grafo di adiacenza:

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

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

Come si costruisce la matrice di adiacenza in presenza di unioni ed intersezioni?

- intersezione: vengono presi gli 1 presenti in entrambe le matrici  $\Rightarrow (M_{R \cap T})_{ij} = (M_R)_{ij} \cdot (M_T)_{ij}$
- unione: vengono presi tutti gli 1  $\Rightarrow (M_{R \cup T})_{ij} = M_R \oplus M_T \rightarrow$  somma booleana

**Prodotto di relazioni**

Prendiamo due relazioni  $R \subseteq A_1 \times A_2$  e  $T \subseteq A_2 \times A_3$  definiamo allora il prodotto

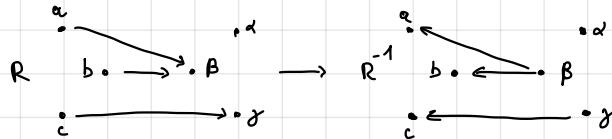
$$R \cdot T \subseteq A_1 \times A_3 = \{(a, c) \in A_1 \times A_3 : \exists b \in A_2 : (a, b) \in R \wedge (b, c) \in T\}$$

Supponiamo di conoscere  $M_R \in \text{Mat}(\{A_1\} \times \{A_2\}, \{0,1\})$  e  $M_T \in \text{Mat}(\{A_2\} \times \{A_3\}, \{0,1\})$ , 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  $i \in \mathcal{S}$  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.T.

Il prodotto di relazioni è associativo, ma non commutativo. Ese, 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'inclusione di  $R$ , quella di  $R^{-1}$  sarà  $M_{R^{-1}} = M_R^T$ . Inoltre, è facile 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 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).

Oltre alle relazioni nulle di questo tipo sono:

- La relazione vuota  $\emptyset$
- La relazione identità  $I_A$  (vuota:  $R^0 = I_A$ )
- La relazione universale  $w_A$

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

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 , , , :  $\forall a, b \in A \quad \exists (a, b) \in R \Rightarrow (b, a) \in R$  ( $M_R$  è simmetrica)
- , , , antisimmetrica , , , :  $\forall a, b \in A \quad \exists (a, b) \in R \text{ e } (b, a) \in R \Rightarrow a = b$
- , , , transitiva , , , :  $\forall a, b, c \in A \quad \exists (a, b) \in R \text{ e } (b, c) \in R \Rightarrow (a, c) \in R$  ( $R$  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 compongono unione, intersezione, prodotto e inversione rispetto alle proprietà precedenti?

	$\cap$	$\cup$	$\cdot$	$-1$
<b>SERIALE</b>	<b>x</b>	<b>✓</b>	<b>✓</b>	<b>x</b>
<b>RIFLESSIVA</b>	<b>✓</b>	<b>✓</b>	<b>✓</b>	<b>✓</b>
<b>SIMMETRICA</b>	<b>✓</b>	<b>✓</b>	<b>x</b>	<b>✓</b>
<b>ANTISIMMETR.</b>	<b>✓</b>	<b>x</b>	<b>x</b>	<b>✓</b>
<b>TRANSITIVA</b>	<b>✓</b>	<b>x</b>	<b>x</b>	<b>✓</b>

## 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  $T_2$  anche' 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 risulta  $P$ , 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'unione 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  $P = \{\text{Riflessiva, Transitiva, Simmetrica}\}$  esiste sempre la  $P$ -chiusura di  $R \subseteq A \times A$  e viene indicata  $\bar{R}^P$ . Di altre proprietà, in generale, non possono essere chiuse.

## Chiusura riflessiva

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

## Chiusura simmetrica

Per chiudere simmetricamente una relazione  $R$ , basta aggiungere tutte le frasi col contrario:  $\bar{R}^{SYM} = R \cup R^{-1}$  ( $M_R \oplus M_R^\top$ )

## 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
- $M_{\bar{R}^{TR}} = M_R \oplus M_R^\top \oplus M_R^2 \oplus \dots \oplus M_R^i$  dove  $i$  è il piccolo indice soddisfa  $M_R^{i+1} \subseteq M_R \oplus \dots \oplus M_R^i$

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

- 1)  $R \subseteq H$
- 2) È transitiva:  $(a,b), (b,c) \in H \Rightarrow (a,b) \in R^i \quad (b,c) \in R^{i+j} \Rightarrow (a,c) \in R^{i+j} \subseteq H$
- 3) Sia  $S$  una relazione  $R \subseteq S$  ed è transitiva. Allora da  $R \subseteq S \Rightarrow R^2 \subseteq SR$  e  $R \subseteq S \Rightarrow SR \subseteq S^2$  e quindi  $R^2 \subseteq S^2$ . Siccome  $S$  è transitiva ottieniamo 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  $H = \bigcup_{K \geq 0} R^K \subseteq S$ . Quindi  $H$  è la più piccola relazione transitiva che contiene  $R$ .

## Chiusura riflessiva + simmetrica

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

$$M_{\bar{R}^{REFL+SYM}} = M_R \oplus M_R^\top \oplus I$$

## Chiusura riflessiva + transitiva

$$\bar{R}^{REFL+TR} = \bigcup_{K \geq 0} R^K \cup I_A = \bigcup_{K \geq 0} R^K$$

## Chiusura simmetrica + transitiva

$$\bar{R}^{ST} = \bigcup_{K>0} (R \cup R^{-1})^K \quad !! \text{ Prima chiude simmetricamente poi transitivamente}$$

## Chiusura simmetrica + riflessiva + transitiva

$$\bar{R}^{EST} = \bigcup_{K>0} (R \cup R^{-1})^K \quad !! \text{ Prima chiude simmetricamente poi transitivamente}$$

## 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 salvare ogni connessione in ogni sottoun connesse.

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  $n \in \mathbb{N} > 0 \equiv_n \subseteq \mathbb{Z} \times \mathbb{Z}$ :  $(a, b) \in \equiv_n \Leftrightarrow a - b = kn \quad k \in \mathbb{Z}$ . 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  $a \equiv_n b \Leftrightarrow r_a = r_b$ .

Dimostriamo che  $\equiv_n$  è di equivalenza:

- 1) riflessiva:  $n | a - a = 0$   $n$  è sempre divisore di 0
- 2) simmetrica:  $n | a - b \Rightarrow n | b - a$
- 3) Transitiva:  $n | a - b$  e  $n | b - c$ , quindi  $r_a = r_b$  e  $r_b = r_c$  e quindi  $r_a = r_c \Rightarrow n | a - c$

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

## Classe d'equivalenza

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

$$[a]_P := \{b \in A : (a, b) \in P\}$$

L'insieme delle classi d'equivalenza di  $P$  è chiamato insieme quoziente ed è indicato con  $A_P := \{[a]_P : a \in A\}$

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  $\forall i, j \in I \quad i \neq j \Rightarrow A_i \cap A_j = \emptyset$ . È facile capire che  $A_P$  forma una partizione di  $A$ . Viceversa, se  $A_i, i \in I$  è una partizione di  $A$ , posso definire una relazione d'equivalenza  $\approx$  tale che  $\approx = \{A_i \times A_i : i \in I\}$

## Relazione d'ordine

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

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. La quest'ultima chiuderà è antisimmetrica, allora essa è la chiusura d'ordine di  $R$ .

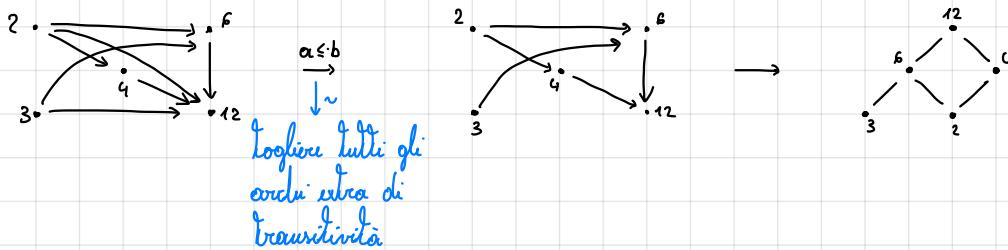
### Diagramma di Hasse di un Poset

Lia  $s \subseteq A \times A$  d'ordine. Diciamo che  $b$  copre  $a$  se  $a \leq b$  e non esiste alcun  $c \in A$   $c \neq a, b$ :  $a \leq c \leq b$  (si indica  $a \leq b$ )

Si definisce diagramma di Hasse di  $(A, \leq)$  un diagramma così costruito:

- 1) Nel grafo di adiacenza di  $\leq$  considero solo gli archi  $a \rightarrow b$  con  $a \leq b$
- 2) Li orientano gli archi dall'alto verso il basso:  $a \leq b \Rightarrow \downarrow^b_a$

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



### Minimo, mininale, massimo e maximale

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

Chiamiamo mininale un elemento  $a \in A$  tale che se  $x \leq a \Rightarrow x = a$ . Analogamente il maximale è un  $a \in A$ : se  $x \geq a \Rightarrow x = a$ . Se minimo o massimo esistono, essi saranno rispettivamente mininale o maximale e, in più, non esisterò altri mininali o maximali che non siano minimi o massimi. Un mininale/maximale non per forza è un minimo/massimo

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

### Maggioranti, minoranti, estremo superiore e inferiore

Lia  $(A, \leq)$  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.

### Reticolati

Definiamo reticolo un Poset  $(A, \leq)$  per cui  $\exists \text{Inf}\{\alpha, \beta\}$ ,  $\exists \text{Sup}\{\alpha, \beta\}$   $\forall \alpha, \beta \in A$ . I reticolati si possono caratterizzare come strutture algebriche.

### Funzioni

Una funzione  $f: A \rightarrow B$  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  $b = f(a)$ .

Dato  $f: A \rightarrow B$  con  $b = f(a)$ , diciamone:

- $A$  dominio di  $f$  e  $B$  codominio
- $b \in B$  immagine di  $a$ .
- $a \in A$  contrainmagine 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

Dato  $f: A \rightarrow B$  e  $g: B \rightarrow C$ , allora il prodotto (o composizione) delle funzioni  $f \cdot g$  è una funzione  $f \cdot g: A \rightarrow C$ . La chiusura  $f \cdot g$  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

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

- se  $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$ .
- se  $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$
- $\forall b \in B \quad f^{-1}(B)$  contiene al più un elemento

} Equivalenti

Dato  $f: A \rightarrow B$  e  $g: B \rightarrow C$ , poniamo che:

- 1) se  $f, g$  sono iniettive allora  $f \circ g$  è iniettiva
- 2) se  $f \circ g$  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. Poniamo allora complete la relazione inversa con:  $d = f^{-1} \cup \{(x, a_i) \mid x \in B \setminus f(A)\}$  ( $a_i \in A$  nullo a caso).  $d$  soddisfa  $d \circ d = I_A$  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:

- 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)  $f(A) = B$

} Equivalenti

Dato  $f: A \rightarrow B$  e  $g: B \rightarrow C$  allora:

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

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

Diciamo che  $f$  è biunivoca 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

Dato  $p \subseteq A \times A$  di equivalenza, posso costruire  $\pi_p: A \rightarrow A_p$  con  $\pi_p(a) = [a]_p$  l'insieme della mappa canonica di  $p$ .

La mappa canonica di  $p$  è suriettiva poiché  $\forall [b]_p \in A_p \quad \pi_p([b]_p) = [b]_p$  è una inversa sinistra e:  $s: A_p \rightarrow A$  con  $s([a]_p) = a$

### Nucleo di funzione

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

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

### Teorema di fattorizzazione

Dato  $f: A \rightarrow B$ , quando il nucleo di  $f$  è possibile costruire  $\pi_{\text{Ker } f}: A \rightarrow A_{\text{Ker } f}$ . Esiste un'unica funzione iniettiva  $g: A_{\text{Ker } f} \rightarrow B$  tale che  $f = \pi_{\text{Ker } f} \circ g$ . Inoltre se  $f$  è suriettiva,  $g$  è biunivoca.

### CARDINALITÀ DI UN INSIEME

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

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

Possiamo dire che:

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

### Teorema di Cantor

Prendiamo  $A$  infinito ( $|A| > |\mathbb{N}|$ ) 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  $A$ :  $|\mathbb{N}| < |A| < |\mathbb{R}|$  (Spazio del continuo).

### LOGICA PROPOZIZIONALE

Definiamo la sintassi:

- alfabeto: lettere enunciative
- connettivi:  $\neg$  (NOT),  $\wedge$  (AND),  $\vee$  (OR),  $\Rightarrow$  (se - allora),  $\Leftarrow$  (se - solo - se)
- simboli auxiliari:  $(, )$

Tra le stringhe formate con l'alfabeto sopra definiamo le formule ben formate:

- ogni lettera enunciativa è una formula ben formata
- se  $A$  e  $B$  sono formule ben formate, allora  $(A \Rightarrow B)$ ,  $(A \wedge B)$ ,  $(A \vee B)$ ,  $(A \Leftarrow B)$  e  $(\neg A)$  sono formule ben formate

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

SIMBOLO	ASSOCIAZIONE
PRIORITÀ MAGG: $\neg$	sx
$\wedge$	sx
$\vee$	sx
$\Rightarrow$	sx
PRIORITÀ MIN: $\Leftarrow$	sx

Ora dobbiamo definire la semantica. Definiamo l'interpretazione  $v : \{F : F \text{ ben formata}\} \rightarrow \{0, 1\}$  che soddisfa:

- $v(\neg A) = 1 - v(A)$
- $v(A \wedge B) = \min \{v(A), v(B)\}$
- $v(A \vee B) = \max \{v(A), v(B)\}$
- $v(A \Rightarrow B) = \max \{1 - v(A), v(B)\}$
- $v(A \Leftarrow B) = \min \{\max \{1 - v(A), v(B)\}, \min \{v(A), 1 - v(B)\}\}$

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

$v(A)$	$v(B)$	$v(A \wedge B)$	$v(A \vee B)$	$v(A \Rightarrow B)$	$v(A \Leftarrow B)$
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  $F$  ben formata è soddisfacibile se esiste un'interpretazione  $v$  tale che  $v(F) = 1$ , in questo caso  $v$  si chiama modello. Se  $\Gamma$  è un insieme di formule ben formate,  $\Gamma$  si dice soddisfacibile se esiste un modello  $v$  per tutte le formule di  $\Gamma$ .

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

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

Enunciamo il teorema di deduzione semantica:  $\Gamma \cup \{B\} \models A \iff \Gamma \models B \Rightarrow A$ . Enunciamo anche il legame tra insoddisfabilità e conseguenza semantica:  $\Gamma \not\models A \iff \Gamma \cup \{\neg A\}$  è insoddisfacibile

DIMOSTRAZIONE (2):  $\Rightarrow$  Sia  $v$  un'interpretazione, abbiamo due casi:

- $v$  è modello di  $\Gamma$ , quindi per ipotesi  $v(A)=1 \Rightarrow v(\neg A)=0 \Rightarrow$  non è modello di  $\Gamma \cup \{\neg A\}$
  - $v$  non è modello di  $\Gamma$ , quindi a maggior ragione non è modello di  $\Gamma \cup \{\neg A\}$
- $\Leftarrow$  Consideriamo  $v$  modello di  $\Gamma$ :
- $v$  è modello di  $A$ , quindi non è modello di  $\neg A$  e quindi  $\Gamma \models A$
  - $v$  non è modello di  $A$ , quindi è modello  $\neg A$  e  $\Gamma \cup \{\neg A\}$  è soddisfacibile, contrappositi.

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. Quel è allora la cardinalità di  $F_n/\equiv$  ( $F_n = \{A \text{ con } A_1, \dots, A_n \text{ libere immutabili}\}$ )? Sarà il numero di tavole di verità con  $n$  colonne. Poiché ogni tabella ha 2<sup>n</sup> righe ognuna con 2 valori, ci saranno 2<sup>n</sup> tavole.

Ricavare predicatori dalla Tabella di verità

Vedri ACSO:

- forma normale congiuntiva: secondo forma canonica
- forma normale disgiuntiva: prima forma canonica

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

## 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'infusura che permette di scrivere in modo algoritmico altre stringhe dato un certo insieme di stringhe.

Dato una teoria formale  $H$  chiamiamo dimostrazione una sequenza finita di stringhe che siano assioni o formule dedotte dalle precedenti tramite una regola d'infusura. Diciamo teorema della teoria una stringa  $t$  e scriviamo  $\vdash_H t$  se sia l'ultima formula di una dimostrazione.

Dato un insieme  $\Gamma$  di stringhe diciamo che una formula  $t$  è deducibile in  $H$  da  $\Gamma$  e scriviamo  $\Gamma \vdash_H t$  se esiste una sequenza finita di stringhe che siano o assioni o formule di  $\Gamma$  o formule dedotte dalle precedenti tramite le regole d'infusura la cui ultima formula sia  $t$ . Un teorema di  $H$  è, quindi, una formula deducibile da  $\Gamma$  vuoto.

## Teoria L o Sistema Hilbertiano

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

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

$$\left. \begin{array}{l} A_1: A \Rightarrow (B \Rightarrow A) \\ A_2: (A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C)) \\ A_3: (\neg A \Rightarrow \neg B) \Rightarrow ((\neg A \Rightarrow B) \Rightarrow A) \end{array} \right\} \text{gli assioni sono indipendenti e tautologici}$$

Questi assiomi, in realtà, sono schemi di assiomi poiché  $A, B, C$  non sono lettere prudicative.

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

**ESEMPIO** Proviamo una dimostrazione di  $\vdash A \Rightarrow A$ :

- 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'infusione troi  $D_3 \vdash D_2$   $D_4 = ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$
- 5) , , , ,  $D_1 \vdash D_4$   $D_5 = A \Rightarrow A$

### Teorema di correttezza e completezza

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

Quindi verificare che  $\Gamma \vdash A$  sembra inutile, ma grazie al teorema sopra mi basta solo verificare che  $\Gamma \models A$ .

### Risoluzione

È basato sulla riflessione, ovvero  $\Delta$  è insoddisfacibile se e solo se  $\Delta \vdash \square$ . Definiamo ora qualche terminologia:

- 1) **Litterale:** una lettera univocale o la sua negazione
- 2) **Clausola:** insieme o disgiunzione di litterali. Chiamiamo clausola vuota  $\square = \{\}$

Per estrarre le clausole da  $\Delta$  dobbiamo:

- 1) portare  $\Delta$  in forma normale congiunta
  - 2) costruire un insieme di litterali delle  $n$  congiunzioni
- $$\left. \right\} \{A, \neg A\} = \{\}$$

Proviamo ora definire la risoluzione:

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

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

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

- 1)  $\Delta = \Gamma \cup \{\neg A\}$
  - 2) costruiamo  $\Delta^c$
  - 3)  $\text{Ris}(\Delta^c) = \Delta^c \cup \{R_{i,j} : R_{i,j} \text{ è una risolvente di } c_i, c_j \in \Delta^c\}$ . Sto eseguendo  $\text{Ris}^n(\Delta^c) = \text{Ris}(\text{Ris}^{n-1}(\Delta^c))$  e verifico che  $\square \in \text{Ris}^n(\Delta^c)$  per qualche  $n$
  - 4) Se  $\text{Ris}^m(\Delta^c) = \text{Ris}^{m-1}(\Delta^c)$  fermiamo. Se  $\square \in \text{Ris}^{m-1}(\Delta^c)$  allora  $\Gamma \models A$
- !! La m esiste sempre se  $\Delta^c$  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  $x$ , se  $x$  divide  $y$ , allora per ogni  $z$ ,  $x$  divide  $z \cdot y$ ". Ogni formula avrà un dominio in cui interpretare la formula.

Definiamo l'alfabeto:

- costanti:  $a, b, c, \dots$  al più numerabili
- variabili:  $x_1, x_2, \dots, x_n$  al più numerabili
- lettere funzionali:  $f_1^n, f_2^n, \dots, f_i^n$  al più numerabili dove  $n$  indica l'arità della lettera funzionale. Usiamo la notazione più semplice  $P(x, y, z)$  dove l'arità è implicita dal numero di variabili. Modellano funzioni con arità  $n$ .
- lettere predicative:  $A_1^n, A_2^n, \dots, A_i^n$  al più numerabili dove  $n$  indica l'arità. Quindi qua usiamo la notazione con arità implicita. Modellano relazioni di arità  $n$ .
- connettivi:  $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$
- quantificatori:  $\forall$  (universali),  $\exists$  (esistenziali). Quantificano le variabili
- simboli auxiliari:  $), ($

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  $(\neg A), (\exists A) \wedge (\forall A)$  sono ben formate; se  $A \wedge B$  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	ASSOCIAZIONE
$\neg$	$\neg, \exists, \forall$ 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 riscontrarla dentro il campo d'azione. Definiamo una formula chiusa una formula che non ha variabili libere. Se la formula dipende da variabili libere posso formarla chiudendola.

- 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  $\exists y$ .

### Semantica della logica predicativa

Definiamo interpretazione / struttura  $\langle D, I \rangle$  dove:

- $D$  è un insieme (dominio)
- $I = (I_1, I_2, I_3)$  con
  - $I_1: \text{Cost} = \{\text{costanti del linguaggio}\} \rightarrow D \quad a \in \text{Cost} \quad I_1(a) \in D$
  - $I_2: \text{corrisponde a ogni lettera funzionale } f^n \text{ di arità } n \text{ un'operazione o funzione } n\text{-aria: } I_2(f^n) = F(x_1, \dots, x_n) \text{ con}$

$$F: D \times \dots \times D \rightarrow D$$

- $I_3$ : associa ad ogni lettera predicativa  $n$ -aria  $A^n$  una relazione  $n$ -aria:  $I_3(A^n) = R \subseteq D \times \dots \times D$

Dato un linguaggio del primo ordine e sia  $\langle D, I \rangle$  una interpretazione, un conseguimento è una funzione:

$$S: \text{Var}(L) \xrightarrow{\text{Linguaggio}} D$$

Funzione delle variabili di L

Possiamo estendere  $S$  ad una funzione su tutti i termini di  $L$ :

$$S^*: \text{Term}(L) \rightarrow D$$

Funzione dei termini di L

In questo modo:

- $s^*(a) = I_1(a) \quad \forall a \in \text{Const}(L)$
- $s^*(x) = S(x) \quad \forall x \in \text{Var}(L)$
- se  $f^n$  è una lettera funzionale  $s^*(f^n(t_1, \dots, t_n)) = I_2(f^n)(s^*(t_1), \dots, s^*(t_n))$

Dia  $\mathcal{I} = \langle D, I \rangle$  una interpretazione e sia  $S: \text{Var}(L) \rightarrow D$  un assegnamento, diciamo che la formula  $\varphi \in L$  è soddisfatta da  $S$  e scriviamo  $\langle D, I \rangle, S \models \varphi$  se:

- $\varphi = A^n(t_1, \dots, t_n)$  è atomica se  $(s^*(t_1), \dots, s^*(t_n)) \in I_3(A^n)$  da  $A^n$  in  $\langle D, I \rangle$
- $\varphi = \neg \psi$  allora  $\langle D, I \rangle, S \models \varphi \Leftrightarrow \langle D, I \rangle, S \not\models \psi$
- $\varphi = \psi \wedge \theta$  ( $\varphi = \psi \vee \theta$ ) allora  $\langle D, I \rangle, S \models \varphi \Leftrightarrow \langle D, I \rangle, S \models \psi \wedge \theta$  ( $\varphi = \psi \Rightarrow \theta$ )  $\langle D, I \rangle, S \models \theta$
- $\varphi = \psi \Rightarrow \theta$  ( $\varphi = \psi \Leftarrow \theta$ ) allora  $\langle D, I \rangle, S \models \varphi \Leftrightarrow \langle D, I \rangle, S \models \psi$  implica che ( $\psi$  è solo se)  $\langle D, I \rangle, S \models \theta$
- $\varphi = \forall x \psi$  allora  $\langle D, I \rangle, S \models \varphi \Leftrightarrow \forall d \in D \langle D, I \rangle, S[d/x] \models \psi$  dove  $d/x$  indica l'assegnamento che è uguale ad  $S$  tranne in  $x$  in cui vale  $d$
- $\varphi = \exists x \psi$  allora  $\langle D, I \rangle, S \models \varphi \Leftrightarrow \exists d \in D: \langle D, I \rangle, S[d/x] \models \psi$

Dada un'interpretazione  $\langle D, I \rangle$  una formula si dice

- soddisfacibile se  $\exists S: \text{Var}(L) \rightarrow D: \langle D, I \rangle, S \models \varphi$
- vera se per ogni assegnamento  $S: \langle D, I \rangle, S \models \varphi$ . In questo caso scriviamo  $\langle D, I \rangle \models \varphi$
- falsa se per nessun assegnamento  $S: \langle D, I \rangle, S \not\models \varphi$
- logicamente valida se per ogni interpretazione  $\langle D, I \rangle \models \varphi$  ~tautologia, lo indichiamo con  $\vdash \varphi$
- logicamente contraddittoria se per ogni interpretazione  $\langle D, I \rangle \not\models \varphi$  ~contraddizione, lo indichiamo con  $\not\vdash \varphi$

Possiamo ora definire modello:

- la terna  $\langle D, I, S \rangle$  è un modello di  $\varphi$  se  $\langle D, I \rangle, S \models \varphi$
- $\langle D, I, S \rangle$  è un modello di un insieme di formule  $\Gamma$  se è un modello di tutte le formule di  $\Gamma$
- $\varphi$  è conseguenza semantica di  $\Gamma$  ( $\Gamma \models \varphi$ ) se ogni modello di  $\Gamma$  lo è anche di  $\varphi$
- $\Gamma$  è irsoddisfacibile se  $\Gamma$  non ha modelli

Possiamo enunciare l'equivalente dei teoremi di irsoddisfabilità e di chiusura semantica.

- $\Gamma \models \varphi \Leftrightarrow \Gamma \cup \{\neg \varphi\}$  è irsoddisfacibile
- $\Gamma \cup \{\varphi\} \models \varphi \Leftrightarrow \Gamma \models (\varphi \Rightarrow \varphi)$

Diciamo due formule semanticamente equivalenti se  $\varphi \models \psi \wedge \psi \models \varphi$

### Forma normale posse

Una formula binaria  $A$  si dice in forma normale posse se tutti i quantificatori sono all'inizio di  $A$ :

$$A : Q_1 x_1 Q_2 x_2 \dots Q_n x_n B(x_1, \dots, x_n), \quad Q_i \in \{\forall, \exists\}$$

$B$  è detta matrice di  $A$ . Una f.b.f può essere sempre trasformata in una equivalente in f.n.p. Vi è, inoltre, un algoritmo che trasforma  $A$  in f.n.p. L'idea dell'algoritmo è di usare le seguenti equivalenze semantiche per portare fuori tutti i quantificatori:

- $\forall x A \equiv \exists x \forall A$
- $\forall \exists x A \equiv \forall x \exists A$
- con  $A(x)$  sostituiamo che  $x$  è libero in  $A$ , se  $y$  è una variabile che è terminale libero per  $x$ . Se  $B$  è una formula in cui non ci sono occorrenze libere di  $y$ :  $\text{di } B \text{ contiene occorrenze libere di } x, \forall x \text{ è inutile.}$
- $\forall x A(x) \wedge B \equiv \forall y (A[y/x] \wedge B)$
- $\exists x A(x) \wedge B \equiv \exists y (A[y/x] \wedge B)$
- $\forall x A(x) \vee B \equiv \forall y (A[y/x] \vee B)$
- $\exists x A(x) \vee B \equiv \exists y (A[y/x] \vee B)$
- $\forall x A(x) \Rightarrow B \equiv \exists y (A[y/x] \Rightarrow B)$
- $\exists x A(x) \Rightarrow B \equiv \forall y (A[y/x] \Rightarrow B)$
- $B \Rightarrow \forall x A \equiv \forall y (B \Rightarrow A[y/x])$
- $B \Rightarrow \exists x A \equiv \exists y (B \Rightarrow A[y/x])$

**ESEMPIO**

$$\begin{aligned} \exists x A(x, x) \wedge B(y, y) &\equiv \exists t (A(t, t) \wedge B(y, y)) \\ &\equiv \exists x (A(x, x) \wedge B(y, y)) \\ \exists x A(x, x) \wedge B(x, x) &\equiv \exists t (A(t, t) \wedge B(x, x)) \end{aligned}$$

La f.n.p. in generale non è unica in quanto dipende dall'ordine di applicazione delle equivalenze.

### Forma di Skolem

Sei  $A$  una f.b.f in f.n.p.  $A = Q_1 x_{m_1} \dots Q_n x_{m_n} B(x_1, \dots, x_m, x_{m_1}, \dots, x_{m_n})$ ,  $Q_i \in \{\exists, \forall\}$ . La forma di Skolem elimina i quantificatori esistenziali con il seguente algoritmo:

1) chiudi universalmente  $A$ :  $\forall x_1 \dots \forall x_m Q_1 x_{m_1} \dots Q_n x_{m_n} B(\dots)$

2) finisci non ci sono più quantificatori esistenziali.

a) sia  $x_3$  la prima variabile quantificata  $\exists x_3$ , costruisci:  $\forall x_1 \dots \forall x_{3-1} Q_{3+1} x_{3+1} \dots Q_{n+m} \hat{B}(x_1, \dots, x_{m+n})$  dove  $\hat{B}$  è ottenuta da  $B$  sostituendo a  $x_3$  una nuova lettera funzionale di valle  $\beta^{-1}(x_1, \dots, x_{3-1})$  dipendente dalle variabili  $x_1, \dots, x_{3-1}$  quantificate prima del  $\exists x_3$ .

Poiché il numero di quantificatori è finito, l'algoritmo termina sempre restituendo  $F_{Sk}$ . La forma di Skolem non è in generale equivalente alla forma di partenza. Un modello di  $F_{Sk}$  è anche modello di  $F$ , ma non viceversa. Un modello di  $F$  può essere esteso a modello di  $F_{Sk}$ . Quindi  $F$  è soddisfacibile, cioè  $\vdash_D, I \models F \Leftrightarrow \vdash_D, I \models F_{Sk}$ . Il teorema di Skolem afferma che se  $F$  è insoddisfacibile se e solo se  $F_{Sk}$  è insoddisfacibile.

### Forma a clausole

Dada una f.b.f in forma di Skolem si dice in forma a clausole se è del tipo:

$$\forall x_1 \dots \forall x_n ((L_1 \vee L_2 \vee \dots) \wedge (L_1 \vee L_{m_1} \vee \dots) \dots)$$

Con  $L_i$  literali, cioè formule atomiche o negazioni di formule atomiche.

Usando le usuali equivalenze semantiche della logica proposizionale, se  $F_{Sk}$  è in forma di Skolem, lavorando solo sulla matrice

di  $\mathcal{F}_{SK}$  posso portarla in una equivalente  $\mathcal{F}'_{SK}$  a clausole.

### Teoremi deduttivi predicativi / Sistemi formali del 1° ordine rifutativi

Ci sono due principali sistemi: sistema tableau (teoria K) e sistema per rifutazione (rifutazione).

La rifutazione vorrebbe se un insieme di formule  $A$  è insoddisfacibile. Enunciamo, allora, il teorema di correttezza e completezza per rifutazione:  $A$  è insoddisfacibile se e solo se  $\Delta_{SK}^c \vdash_{\square} \{\}$  dove  $\Delta_{SK}^c$  sono le clausole ottenute da  $\Delta_{SK}$ . Data  $\mathcal{F}_{SK}$  in forma a clausole,  $\mathcal{F}'_{SK}$  si ricava come già visto.

Come funziona la risoluzione tra clausole? Date  $c_1 = \{ \dots, \neg B(x, t(a), y) \}$  e  $c_2 = \{ \dots, B(c, y, b) \}$ , vorrei eliminare  $B(\ )$  e  $\neg B(\ )$ , ma esse non sono la stessa cosa, come faccio? Cerco di renderli uguali usando delle sostituzioni:  $c'_x, t(a)'_y$  e  $b'_y$  ma non si può fare poiché stanno sostituendo alla stessa variabile termini diversi. Rinominiamo le variabili:  $c_1 = \{ \dots, \neg B(x, t(a), y) \}$ ,  $c_2 = \{ \dots, B(c, w, b) \}$ ; se consideriamo le sostituzioni  $\sigma = \{ c'_x, t(a)'_w, b'_y \}$ , allora riusciamo a rendere i due littorali sintatticamente equivalenti.

Definiamo sostituzione o la scrittura  $\sigma = \{ t'_x, \dots, t'_{x_n} \}$  dove  $x_1, \dots, x_n$  sono variabili distinte e  $t_1, \dots, t_n$  sono termini.

Definiamo unificatore una sostituzione  $\sigma$  che, dato un insieme di espressioni  $E_1, \dots, E_k$  del primo ordine, si ha  $E_1 \cdot \sigma = E_2 \cdot \sigma = \dots = E_k \cdot \sigma$ .

Date due sostituzioni  $\sigma = \{ t'_x, \dots, t'_{x_n} \}$  e  $\theta = \{ u'_x, \dots, u'_{x_n} \}$ ,  $\sigma \cdot \theta$  è la sostituzione ottenuta da  $\{ t'_{x_1}, \dots, \frac{t_n \theta}{x_n}, \frac{u_n}{x_1}, \dots, u'_n \}$  cancellando:

- tutte le sostituzioni  $u'_j/x_j$  con  $y_j = x_j$  (per qualche  $j \in i$ )
- $t'_{x_K}/x_K$  tale che  $t_K \cdot \theta_K = x_K$  ( $\frac{\sigma \cdot \theta}{x_K} = \frac{x_K}{x_K}$ )

Definiamo unificatore più generale di  $E_1, \dots, E_k$  espressioni del primo ordine è un'unificatore  $\sigma$  tale che per ogni altro unificatore  $\theta$  di  $E_1, \dots, E_k$  abbiamo che  $\theta = \sigma \cdot \rho$  dove  $\rho$  è un'altra sostituzione. ossia  $\sigma$  unifica con meno vincoli di  $\theta$ . Esiste un algoritmo che prende in input ha delle espressioni  $E_1, \dots, E_k$  e vi costruisce (se esiste) una U.P.G. Esso è sostanzialmente un parser da sx a dx che quando trova un carattere diverso cerca con delle sostituzioni di renderlo uguale.

Possiamo ora definire la risolvente tra due clausole. Siano  $c_1, c_2$  due clausole e supponiamo che  $c_1$  e  $c_2$  abbiano variabili distinte; individuiamo  $c_1 = \{ \dots, L_1, \dots, L_i, \dots \}$  e  $c_2 = \{ \dots, \neg L_i, \dots, \neg L_{i+1} \}$  e supponiamo che esista l'unificatore più generale  $\sigma$  di  $L_1, \dots, L_i, \neg L_i, \dots, \neg L_{i+1}$ ; una risolvente tra  $c_1$  e  $c_2$  è la clausola  $R = (c_1 \cdot \sigma \setminus L) \cup (c_2 \cdot \sigma \setminus \neg L)$ .

Sia  $\Delta_c$  un insieme di clausole, una derivazione di  $c$  da  $\Delta_c$  ( $\Delta_c \vdash_c c$ ) è una sequenza  $c_1, \dots, c_n = c$  tale che  $\Delta_c \vdash_c c_1, \Delta_c \cup \{c_1\} \vdash_c c_2 \dots \Delta_c \cup \{c_1, \dots, c_{i-1}\} \vdash_c c_i$  dove  $c_i \in \Delta_c \cup \{c_1, \dots, c_{i-1}\}$  oppure  $c_i$  è una risolvente tra due clausole di  $\Delta_c \cup \{c_1, \dots, c_{i-1}\}$ .

Enunciamo, allora, il teorema di correttezza e completezza:

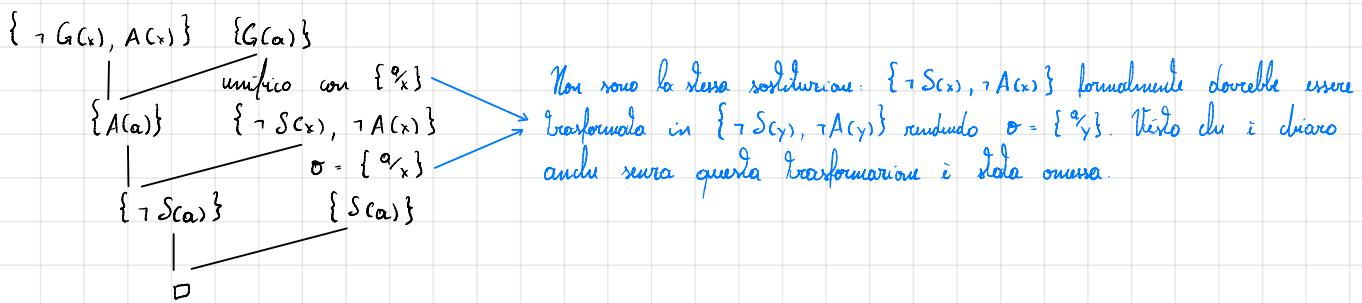
TEOREMA  $A$  è insoddisfacibile se e solo se  $\Delta_{SK}^c \vdash_{\square} A$  e  $\Gamma \models A$  se e solo se  $(\Gamma \cup \neg A)^c_{SK} \vdash_{\square} \{\}$ . Nota bene: la rifutazione è un problema indecidibile, contrariamente al caso della logica proposizionale.

**ESERCIZIO** Provare che da  $\Gamma = \{ \text{"Tutti i giocatori di basket sono alti", "Qualunque giocatore di pallacanestro è studente universitario"} \}$  si deduce  $A$ : "Qualche studente universitario è alto".

Dobbiamo risolvere  $\Gamma \models A$ . Definiamo  $G(x) = "x \text{ è giocatore di basket}"$ ,  $A(x) = "x \text{ è alto}"$  e  $S(x) = "x \text{ è studente}"$  le nostre lettere predicative. Avremo  $\Gamma = \{ \forall x (G(x) \Rightarrow A(x)), \exists x (G(x) \wedge S(x)) \}$  e  $\neg A = \neg (\exists x (S(x) \wedge A(x))) = \forall x (\neg S(x) \vee \neg A(x))$ . Prepariamo le nostre formule:

- $\forall x (G(x) \Rightarrow A(x)) \equiv \forall x (\neg G(x) \vee A(x))$
- $\exists x (G(x) \wedge S(x)) \xrightarrow{SK} G(a) \wedge S(a)$
- $\forall x (\neg S(x) \vee \neg A(x))$  è OK

Abbiamo  $(\Gamma_{SA} \cup \neg A_{SA})^c = \{\{\neg G(x), A(x)\}, \{G(a)\}, \{\neg S(a)\}, \{\neg \neg S(x), \neg A(x)\}\}$ . Dovremo:



Possiamo quindi affermare che  $\Gamma \models t$ .

### Sistemi deduttivi predicativi / sistemi formali del I° ordine non rifutativi

Diamo ora un accenno di sistema formale non rifutativo: la teoria K

- **SINTASSI**: sole f.b.f
- **ASSIOMI**: gli assi della teoria + più
  - \*  $(\forall x A(x)) \Rightarrow A(t/x)$  dove t è un termine libero per x
  - \*  $\forall x (A \Rightarrow B) \Rightarrow (A \Rightarrow \forall x B)$  purché non ci siano occorrenze libere di x in t.
- **REGOLE D'INFERENZA**
  - \* Modus ponens:  $A, A \Rightarrow B \vdash_K B$
  - \* Generalizzazione:  $A \vdash_K \forall x A$
- **TEOREMA DI CORRETEZZA E COMPLETITÀ**:  $\Gamma \models t \Leftrightarrow \Gamma \vdash_K t$

Ricorda la teoria K in sé non è decidibile, aggiungiamo degli altri assiomi ( $\Gamma \neq \emptyset$ ). Quelle teorie K sono delle "con assiomi propri":

- **TEORIA CON IDENTITÀ**: Data  $E(x,y)$  la terna predicativa che indica l'uguaglianza, definiamo  
 $\Gamma = \{\forall x E(x,x); \forall x \forall y (E(x,y) \Rightarrow (A(x)x) \Rightarrow A(x)y))$  con  $A(x)x)$  una qualsiasi formula con occorrenza libera di x suddivisa arbitrariamente in due blocchi e  $A(x)y)$  indica che il secondo blocco di x è dato sostituito con y
- **TEORIA CON IDENTITÀ DEI NUMERI NATURALI** (Assiomi di Peano): Enumeriamoli informalmente:
  - \* 0 è naturale
  - \* se x è naturale, allora esiste un numero naturale x' dello successivo di x
  - \*  $0 \neq x' \quad \forall x \in \mathbb{N}$
  - \*  $x' = y' \Rightarrow x = y$
  - \* Il principio d'induzione

Il primo teorema di incompletezza di Gödel afferma che se s è una teoria del I° ordine che contiene l'aritmetica e che sia corrente (non produce né  $\varphi$  né  $\neg\varphi$ ), allora esiste una f.b.f  $\Psi$  tale che né  $\Psi$  né  $\neg\Psi$  sono dimostrabili, inoltre  $\Psi$  è un'affermazione che è vera sulla teoria dei numeri naturali.

### STRUTTURE ALGEBRICHE

Difiniamo ora legge di composizione interna n-aria (operazione n-aria) è una funzione  $w: A \times \dots \times A \rightarrow A$ . Ci noi interveranno i casi  $n = \overset{\text{regole un elemento}}{0, 1, 2}$ . Possiamo, quindi, una struttura algebrica come una coppia  $(A, \omega)$  dove  $\omega$  è un insieme di operazioni su A.

### Demigruppo

La struttura algebrica più studiata è il semigruppo:  $(A, \cdot)$  con · binaria che gode della proprietà associativa. Se nel semigruppo vale anche la proprietà commutativa, allora esso si dice semigruppo commutativo. La proprietà associativa ci permette di definire le potenze di un elemento.

Se vogliamo vedere la teoria dei semigruppi come teoria K con identità ci basta considerare  $P(x,y) = x \cdot y$  e il seguente assioma:  $\forall x \forall y \forall z (E(P(x, P(y, z)), P(P(x, y), z)))$

### Monoidi

Definiamo  $(M, *, e)$  monoidi se:

- $(M, *)$  è un semigruppo

- $e$  è un'identità (o elemento neutro) sinistra o destra  $\forall a \in M$

Se in  $M$   $s$  è identità sinistra e  $d$  è identità destra allora  $s=d$ . In particolare questo dimostra che in un monoido ha identità essa è unica.

In un monoide possiamo definire anche la potenza nulla con  $a^0 = e$ .

Come teoria del primo ordine con identità, per descrivere la teoria dei monoidi sopra, oltre all'assioma di associazività dovrai aggiungere

$$\exists x \forall y (E(P(y, x), y) \wedge E(P(x, y), y)) \quad \text{oppure} \quad \forall y (E(P(y, e), y) \wedge E(P(e, y), y))$$

### Gruppi

Definiamo  $(G, *, e, {}^{-1})$  dove

- $(G, *, e)$  è un monoido

- per ogni  $g \in G$  ha un inverso, ossia  $\forall g \in G \exists h \in G : g * h = h * g = e$

Dall'associazività si può ricavare l'unicità dell'inverso di un elemento ponendoci di dire che  ${}^{-1}$  è unaria e scrivere  $g^{-1} = h$

Proprietà dei gruppi:

- $(g^{-1})^{-1} = g$

- $(g * h)^{-1} = h^{-1} * g^{-1}$

- in un gruppo  $a * x = b$  ha come unica soluzione  $x = a^{-1} * b$

$(\mathbb{Z}_n, \odot)$  non è un gruppo  $[0]_n \forall [a]_n [a]_n \odot [0]_n = [0]_n = [1]_n$ . Considerando  $\mathbb{Z}/\{[0]_n\}$  invece  $\odot$  non è più chiuso. Se  $n$  è primo, però, allora  $(\mathbb{Z}/\{[0]_n\}, \odot)$  è un gruppo. Un caso particolare è:  $\mathbb{Z}_n = \{[x]_n \in \mathbb{Z}_n \setminus \{[0]_n\} : \text{H.C.D}(x, n) = 1\}$  è un gruppo. Come calcoliamo l'inverso di  $[x]_n$ ? Usiamo l'algoritmo di Euclide.

INPUT:  $a, b \in \mathbb{Z}$

OUTPUT:  $d = \text{M.C.D}(a, b)$  e  $\alpha, \beta$ :  $d = \alpha \cdot a + \beta \cdot b$

ALGORITMO:

$$\begin{aligned} 1) \quad a &= q_0 \cdot b + r_0 & r_0 \\ 2) \quad b &= q_1 \cdot r_0 + r_1 & \downarrow \\ 3) \quad r_0 &= q_2 \cdot r_1 + r_2 & \vdots \\ &\vdots & \vdots \\ s+2) \quad r_{s-2} &= q_s \cdot r_{s-1} + r_s & r_s = 0 \end{aligned}$$

$$r_{s-1} = d = \text{M.C.D}(a, b)$$

Sostituendo all'interno la iterazione ottengo  $\alpha$  e  $\beta$

Sappiamo che  $\text{H.C.D}(x, n) = 1$ , allora mi basta risolvere  $[1]_n = [\alpha x + \beta n]_n$  trovando che  $[x]_n^{-1} = [\alpha]_n$

La Teoria dei gruppi come Teoria del primo ordine ha in più questo assioma:

$$\exists_x (\underbrace{\forall_y (E(P(x,y),y) \wedge E(P(y,x),y))}_{\text{monoido}} \wedge \underbrace{\forall_y \exists_z (E(P(y,z),x) \wedge E(P(z,y),x))}_{\text{inverso}})$$

Se invece avessimo avuto una costante e avremmo avuto:

- assioma associatività
- assioma dell'identità:  $\forall_y (E(P(e,y),y) \wedge E(P(y,e),y))$
- $\forall_y \exists_z (E(P(y,z),e) \wedge E(P(z,y),e))$

TEOREMA Sono equivalenti:

- 1)  $(G, *)$  gruppo
- 2) esiste identità dx:  $\exists e \forall g \in G g * e = g$   
esiste inverso dx:  $\forall g \in G \exists h \in G g * h = e$
- 3) esiste comutatività sx:  $\exists d \forall g \in G d * g = g$   
esiste inverso sx:  $\forall g \in G \exists t \in G t * g = d$
- 4) le equazioni  $a * x = b$  e  $y * a = b$  hanno un'unica soluzione

Con il teorema sopra possiamo semplificare la Teoria dei gruppi:

$$\exists_x (\forall g E(P(g,x),g) \wedge \forall g \exists h E(P(g,h),x))$$

### Anello

L'anello è una struttura algebrica  $(A, +, \cdot)$  dove:

- $(A, +)$  è un gruppo commutativo con elemento neutro 0
- $(A, \cdot)$  è un semigruppo
- valgono le proprietà distributive:
  - $\forall a, b, c \in A a \cdot (b+c) = ab + ac$
  - $\forall a, b, c \in A (b+c) \cdot a = ba + ca$

Per descrivere gli assiomi di anello come Teoria del primo ordine con identità ci sono:

- assiomi di gruppo per la somma e la commutatività
- assiomi di semigruppo per il prodotto e la distributività

$$\forall a, b, c \in A (P(a, S(b, c)), S(P(a, b), P(a, c))) \quad (\text{a } \propto; \text{ a dx è analogo})$$

Se  $(A, +)$  è un monoido, allora l'anello ha unità e si indica con 1; se  $(A, \cdot)$  è commutativo allora l'anello si dice commutativo.

L'elemento neutro di  $(A, +)$  si indica con 0 e si chiama "zero" poiché è lo zero per  $(A, \cdot)$ . Diciamo che un elemento  $z \in S$ ,  $(S, \cdot)$  è uno zero di  $S$  se  $\forall s \in S s \cdot z = z \cdot s = 0$ . Se lo zero esiste, esso è unico.

PROPOSIZIONE In un anello  $(A, +, \cdot)$  l'unità 0 di  $(A, +)$  è lo zero del semigruppo  $(A, \cdot)$ . Inoltre:

$$\forall a, b \quad a(-b) = (-a)b = - (ab)$$

DIMOSTRAZIONE -  $a \cdot 0 = 0$   $\forall a \in A : a \cdot b = a \cdot (b+0) = a \cdot b + a \cdot 0 \rightarrow -(ab) + (ab) = ab + a \cdot 0 - ab$   
 -  $a \cdot (-b) = -(ab) : 0 = a \cdot 0 = a(b + (-b)) = ab + a \cdot (-b) \rightarrow -(ab) = -(ab) + ab + a(-b)$  ■

Definiamo, in un anello  $(A, +, \cdot)$ , divisori dello zero se  $a, b \neq 0$  e  $ab = 0$ . Collegato a ciò, in un anello valgono le leggi di cancellazione:

$$\begin{aligned} ab = ac &\Rightarrow b = c \quad \forall a \neq 0, \forall b, c \in A \\ ba = ca &\Rightarrow b = c \end{aligned}$$

Un anello  $(A, +, \cdot)$  è privo di divisori dello zero se e solo se valgono le leggi di cancellazione.

Chiamiamo campo uno speciale tipo di anello in cui  $(A \setminus \{0\}, \cdot)$  è anche un gruppo. Se  $(A \setminus \{0\}, \cdot)$  è commutativo, viene chiamato campo.

### Sottostruzione di una struttura algebrica

Della  $(A, \circ)$  struttura algebrica,  $H \subseteq A$  si dice sottostruzione di  $(A, \circ)$  se  $(H, \circ)$  è ancora una struttura algebrica dello stesso tipo. In poche parole tutte le operazioni  $\circ$  si restringono ad  $H$ .

- $(H, \cdot)$  è un sottosemigruppo di un semigruppo  $(S, \cdot)$  se e solo se  $\forall a, b \in H \quad a \cdot b \in H$
- $(H, \cdot, e)$  è un sottomonoidale di  $(M, \cdot, e)$  se e solo se  $(H, \cdot)$  è un semigruppo di  $(M, \cdot)$  e  $e \in H$
- $(H, \cdot, e, -1)$  è un sottogruppo di  $(G, \cdot, e, -1)$  se e solo se
  - $\forall a, b \in H \quad a \cdot b \in H \quad \left. \begin{array}{l} a \cdot b^{-1} \in H \\ a^{-1} \in H \end{array} \right\} \rightarrow$  condurrete in  $\forall a, b \in H \quad a \cdot b^{-1} \in H$
  - $\forall a \in H \quad a^{-1} \in H$
- $(H, +, \cdot)$  è un sottocampo di  $(A, +, \cdot)$  se e solo se:
  - $(H, +)$  è un sottogruppo di  $(A, +) \rightarrow \forall a, b \in H \quad a + (-b) \in H$
  - $(H, \cdot)$  è un sottosemigruppo di  $(A, \cdot) \rightarrow \forall a, b \in H \quad a \cdot b \in H$