RELAZIONI

Prodotto di relazioni Date due relazioni $R \subseteq A_1 x A_2$e $S \subseteq A_2 x A_3$, il loro prodotto è $R \cdot S \subseteq A_1 x A_3$così definita: $R \cdot S = \{(a_1, a_3) | a_2 \in A_2 : (a_1, a_2) \in R \; e \; (a_2, a_3) \in S\}$.
Il codominio della prima relazione deve corrispondere con il domino della seconda (Le due relazioni sono componibili).
Matrice: prodotto riga per colonna delle matrici
Se $R \cdot S = S \cdot R$ le relazioni si dicono permutabili.
Relazione inversa data $R \subseteq A_1 x A_2$la sua inversa è data da $R^{-1} \subseteq A_2 x A_1$
Grafo: si invertono le frecce
Matrice: si traspone
Unione di relazioni somma con soglia delle matrici
Intersezione di relazioni matrice ha 1 dove in entrambe le matrici di cui si fa intersezione c'era 1
Proprietà seriale $\forall a \exists b((a, b) \in R)$
Grafo: da ogni vertice esce almeno un arco
Matrice: Su ogni riga almeno un 1
Proprietà riflessiva $\forall a((a, a) \in R)$
Grafo: su ogni vertice autoanello
Matrice: diagonale principale di tutti 1
Proprietà simmetrica $(a, b) \in R \iff (b, a) \in R$
Grafo: ogni arco ha doppia freccia
Matrice: è simmetrica
Proprietà antisimmetrica $\big((a, b) \in R \wedge (b, a) \in R\big) \Rightarrow a = b$
Grafo: unici archi con doppia freccia sono gli autoanelli
Matrice: ogni 1 della matrice, tranne che sulla diagonale, ha in posizione simmetrica uno 0 (gli 0 possono avere 0)
Proprietà transitiva $((a, b) \in R \wedge (b, c) \in R) \Rightarrow (a, c) \in R$
Grafo: ogni volta che $a \to b \to c$ c'è anche $a \to c$
Matrice: se 1 in (i, j)e in (j, k) allora anche in (i, k)
Equivale a verificare che $M^2 \leq M$ con M matrice.
Per aggiungere transitività con matrice si moltiplica la matrice per se stessa fino a che il prodotto si stabilizza e si fa unione di tutte le matrici ottenute
P-Chiusura di R Minima relazione che contiene R e ha tutte le proprietà di P. Per determinare una chiusura aggiungere alla relazione le proprietà della chiusura
Relazione di Equivalenza Relazione binaria su un insieme che sia riflessiva, simmetrica, transitiva
Equivalenza associata $E = xRy \wedge yRX = R \wedge R^{op}$
Con le matrici: $M_E = M_R \wedge {M_R}^t$
Determinare tutte relazioni di equivalenza contenenti una relazione R Determinare la chiusura di equivalenza e poi tutte le relazioni che la contengono e sono di equivalenza, per farlo considerare le combinazioni che si ottengono unendo classi di equivalenza all'interno della chiusura
Classe di equivalenza insieme degli elementi in relazione all'elemento rappresentante
L'insieme delle classi di equivalenza di R su A (Partizione indotta da R su A) è l'**insieme quoziente**. Si indica con A/R.
Descrivere il quozienteA/R con R di equivalenza
Grafo: insiemi che non hanno frecce che li collegano
Matrice: Blocchi di 1, quando la matrice è ordinata in modo da averne
Ognuno di essi è una classe di equivalenza $[a]_R = \{\dots\}$ con a come rappresentante
Congruenza modulo n $a \equiv b \pmod n$ se $a - b$ è un multiplo di n, cioè se $a - b = nk$
Classi di resto modulo n $[r]_t$ è la classe di resto r nella congruenza modulo t, cioè dei numeri $x = kt + r$, infatti $x - r = kt$
Dimostrare che una relazione sia d'equivalenza (ESEMPIO)
R è riflessiva e transitiva, dimostrare che *E* sia d'equivalenza. $xEy \coloneqq xRy \wedge yRx$
Riflessiva: xRx per ipotesi $xRx \wedge xRx \Rightarrow xEx$
Simmetrica: $xEy \Rightarrow xRy \wedge yRx \Rightarrow yRx \wedge yRx \Rightarrow yEx$ (perché $\wedge$ è commutativo)
Transitiva: $xEy \wedge yEz \Rightarrow (xRy \wedge yRx) \wedge (yRz \wedge zRy) \Rightarrow (xRy \wedge yRz) \wedge (zRy \wedge yRx) \Rightarrow xRz \wedge zRx \Rightarrow xEz$ (perché $\wedge$ commutativo e R transitiva)
Relazione d'ordine Relazione binaria su un insieme che sia riflessiva, antisimmetrica, transitiva; Indicata con $\leq$
Se non è riflessiva si ha una relazione d'ordine stretto
Determinare tutte relazioni d'ordine contenenti una relazione R Determinare la chiusura d'ordine aggiungendo riflessività e transitività e verificando antisimmetricità (se non c'è allora non esistono) e poi tutte le relazioni che la contengono e sono d'ordine, modificando la matrice in tutti i modi mantenendo antisimmetricità.

Determinare matrice della relazione d'ordine associata $\bar{R}$

$$\begin{array}{ccc} X & \overset{R}{\rightarrow} & Y \\ P \downarrow & & \uparrow P^{op} \\ [\bar{X}] & \overset{\rightarrow}{\bar{R}} & [\bar{Y}] \end{array}$$

Allora $\bar{R} = P^{-1}RP$, dove P assegna a ogni elemento la sua classe di equivalenza; se avessimo ad esempio le classi: $|1| = \{1,2\}$ e $|3| = \{3\}$ la matrice di P sarebbe:

$P = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$ e P^{op} la sua trasposta

Relazione ben definita (o ben posta) $[x]R[y] \Leftrightarrow xRy$

se $x, x^I \in [x]$ e $y, y^I \in [y]$ allora $xRy \Leftrightarrow x^I R y^I$

La relazione non dipende dal rappresentante di classe scelto

Diagramma di Hasse grafo di una relazione d'ordine senza autoanelli e direzioni ma elementi ordinati a livelli dal basso verso l'alto secondo la relazione

Minimale $m \in A$: se $a \leq m$ allora $a = m$

NB: elementi da soli nel diagramma di hasse sono sia minimali che massimali

Minimo $m \in A$: $m \leq a \; \forall a \in A$

Un minimale è minimo se è l'unico minimale (il minimo deve essere unico)

Minorante m: $m \leq a \; \forall a \in A$ (m può $\notin A$)

Inf(B) massimo dei minoranti

Reticolo insieme parzialmente ordinato tale che per ogni coppia di elementi siano definiti inf e sup

Funzione relazione AxB tale che $\forall a \exists$uno (ovnq. definita) e un solo(funzionale) b t.c. $f(a)=b$

Grafo: uno e un solo arco da ogni vertice di A

Matrice: uno e un solo 1 su ogni riga

Funzioni contenute in una relazione sono date da tutte le matrici possibili eliminando gli 1 dalla matrice della relazione in modo da avere uno e un solo 1 su ogni riga

Il loro numero è dato dal prodotto tra il numero di volte che si ripetono gli 1 in ogni riga

Quante funzioni da A a B $|\{f: A \to B\}| = |B|^{|A|}$

Iniettività $\forall a_1, a_2$ se $f(a_1) = f(a_2)$ allora $a_1 = a_2$

Deve essere $|A| \leq |B|$

Grafo: uno e un solo arco da ogni elemento di A e al massimo un arco arriva a ogni elemento di B

Matrice: uno e un solo 1 su ogni riga e al più un 1 su ogni colonna

NB: ogni funzione da un insieme finito in sé stesso è iniettiva se e solo se è suriettiva

Suriettività $\forall b \in B \; \exists a: f(a) = b$

Grafo: uno e un solo arco da ogni elemento di A e almeno un arco arriva ad ogni elemento di B

Matrice: uno e un solo 1 su ogni riga e almeno un 1 su ogni colonna

Biunivocità iniettiva e suriettiva

Grafo: uno e un solo arco da ogni elemento di A e uno e un solo arco arriva a ogni elemento di B

Matrice: uno e un solo 1 su ogni riga e ogni colonn1

Proprietà $f \circ g$

f, g iniettive(suriettive)$\Rightarrow f \circ g$ iniettivo(suriettivo)

$f \circ g$ iniettivo $\Rightarrow f$ iniettiva

$f \circ g$ suriettivo $\Rightarrow g$ suriettiva

Relazione inversa $R^{-1} = R^t$

Inversa destra $h: B \to A$ t.c. $f \cdot h = I_A$

Una funzione ha inversa destra se è iniettiva

Inversa sinistra k: $B \to A$ t.c. $k \cdot f = I_B$

Una funzione ha inversa sinistra se è suriettiva

Inversa $g: B \to A$ t.c. $f \cdot g = I_A$ e $g \cdot f = I_B$

Una funzione ha inversa se è biunivoca

Possono esistere infinite inverse destre e sinistre ma esiste una sola inversa. Se una funzione ammette inversa allora tutte le sue inverse destre e sinistre coincidono con essa

Nucleo $(a_1, a_2) \in ker_f$ se e solo se $f(a_1) = f(a_2)$

Esiste sempre una funzione (proiezione canonica di a sul suo insieme quoziente A/R) suriettiva $\pi_R: A \to A/R$ t.c. $ker_\pi = R$

$a \in ker_f$ sse $f(a) = 0$

Cardinalità due insiemi hanno la stessa cardinalità (si scrive $|A| = |B|$) se esiste una corrispondenza biunivoca tra loro.

Un insieme è infinito se e solo se può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio.

Numerabile: ha cardinalità di $\mathbb{N}$ Continuo: ha cardinalità di $\mathbb{R}$

Ogni insieme ha cardinalità strettamente inferiore al suo insieme delle parti.

STRUTTURE ALGEBRICHE

Elemento neutro u t.c. per ogni $a \in A : u * a = a$(sx) e $a * u = a$(dx)
Zero z t.c. per ogni $a \in A : z * a = z$ (sx) e a$* z = z$ (dx)
Inverso se esiste l'elemento neutro u allora è $\bar{a} \in A$ t.c. $\bar{a} * a = u$
Struttura algebrica coppia $< A, \mathcal{O} >$ dove A è un insieme non vuoto, detto *sostegno,* e $\mathcal{O}$ è un insieme non vuoto di operazioni su A. La cardinalità di A si chiama ordine della struttura.
Strutture simili hanno lo stesso numero di operazioni con la stessa arità
Semigruppo $\langle A,* \rangle$ dove $*$ è una operazione binaria associativa
Monoide $\langle A,*,u \rangle$ dove $*$ è una operazione binaria associativa e u è l'elemento neutro.
L'elemento neutro di un monoide è unico.
Gruppo dato il monoide $\langle A,*,u \rangle$, è un gruppo se ogni elemento di A ammette inverso
In un gruppo ogni elemento ha un unico inverso
Per ogni a esiste u t.c. $u * a = a$ ed esiste b t.c. $a * b = u$
Per ogni $a, b \in A$ le equazioni $a * x = b$ e $x * a = b$ ammettono ciascuna una e una sola soluzione in A.
Leggi di cancellazione per ogni $a, b, c \in A$ se $a * b = a * c$ allora $b = c$ e se $a * b = c * b$ allora $a = c$
Gruppo abeliano Gruppo in cui l'operazione è commutativa
Anello $\langle A,*,\circ,u \rangle$ in cui $\langle A,*,u \rangle$ è un gruppo abeliano, detto *gruppo additivo* dell'anello, e $\langle A,\circ \rangle$ è un semigruppo, detto *semigruppo moltiplicativo* dell'anello, e valgono le proprietà distributive di $\circ$ rispetto a $*$, cioè:
$a * (b \circ c) = (a * b) \circ (a * c)$ e $(b \circ c) * a = (b * a) \circ (c * a)$
Anello con unità il semigruppo moltiplicativo è un monoide.
Anello commutativo il semigruppo moltiplicativo è commutativo.
Privo di divisori dello zero non esistono $a, b \in A$ diversi da 0 t.c. $a \circ b = 0$
Un anello è privo di divisori dello zero se e solo se nel semigruppo $\langle A \setminus \{0\},\circ \rangle$ valgono le leggi di cancellazione.
Corpo Anello in cui gli elementi *diversi dallo zero* formano un gruppo rispetto al prodotto (esiste neutro e ognuno ha inverso)
Campo Corpo in cui il prodotto gode della proprietà commutativa, cioè in un campo: $\langle A, + \rangle$ è un gruppo abeliano, $\langle A \setminus \{0\},\cdot \rangle$ è un gruppo abeliano, valgono le proprietà distributive del prodotto rispetto alla somma. NB: Ogni corpo finito è un campo
Reticolo $\langle A,\wedge,\vee \rangle$ dove $\wedge$ e $\vee$ sono operazioni associative e commutative sull'insieme non vuoto A, per le quali valgono le leggi di assorbimento: $a \vee (a \wedge b) = a$ e $a \wedge (a \vee b) = a$
Sottostruttura data una struttura algebrica, una sua sottostruttura è un suo sottoinsieme non vuoto che è una struttura dello stesso tipo rispetto a tutte le sue operazioni.
Sottosemigruppo Dato il semigruppo $(A,\cdot)$, un sottoinsieme $H \subseteq A$ è un sottosemigruppo se e solo se per ogni $a, b \in H$ si ha $a \cdot b \in H$
Sottomonoide Dato il monoide $(A,\cdot,1)$, un sottoinsieme $H \subseteq A$ è un sottomonoide se e solo se per ogni $a, b \in H$ si ha $a \cdot b \in H$ e $1 \in H$
Sottogruppo *primo criterio del sottogruppo*: Dato il gruppo $(A,\cdot, \ ^{-1}, 1)$, un sottoinsieme $H \subseteq A$ è un sottogruppo se e solo se per ogni $a, b \in H$ si ha $a \cdot b \in H$ e $a^{-1} \in H$
secondo criterio del sottogruppo: Dato il gruppo $(A,\cdot, \ ^{-1}, 1)$, un sottoinsieme $H \subseteq A$ è un sottogruppo se e solo se per ogni $a, b \in H$ si ha $a \cdot b^{-1} \in H$
terzo criterio del sottogruppo: Se A è un insieme finito, un sottoinsieme $H \subseteq A$ è un sottogruppo se e solo se per ogni $a, b \in H$ si ha $a \cdot b \in H$
L'insieme formato dal solo elemento neutro $\{1\}$ e l'intero gruppo A sono *sottogruppi banali*.
Sottogruppo generato Sia $(A,\cdot)$ o $(A,+)$ un gruppo e sia $a \in A$. L'insieme $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$ o $\langle a \rangle = \{na | n \in \mathbb{Z}\}$ è un sottogruppo di A detto *sottogruppo generato* da a.
Se esiste $a \in A$ t.c. $\langle a \rangle = A$, allora $(A,\cdot)$ è un gruppo ciclico e l'elemento a è un generatore di A.
Sottogruppo normale sottogruppo H per cui ogni $h \in H$ e per ogni $a \in A$ si ha $h^a = a^{-1} \cdot h \cdot a \in H$, si scrive $H \trianglelefteq A$
L'insieme $a \cdot H \cdot a^{-1} = \{a \cdot h \cdot a^{-1} | h \in H\}$ di dice *coniugato*.
Un sottogruppo di un gruppo abeliano è sempre normale.
Sottoanello *primo criterio del sottoanello*: Dato l'anello $(A,+,\cdot,-,0)$, un sottoinsieme $H \subseteq A$ è un sottoanello se e solo se per ogni $a, b \in H$ si ha $a + b \in H$ e $-a \in H$ e $a \cdot b \in H$
Secondo criterio del sottoanello: Dato l'anello $(A,+,\cdot,-,0)$, un sottoinsieme $H \subseteq A$ non vuoto è un sottoanello se e solo se per ogni $a, b \in H$ si ha $a - b \in H$ e $a \cdot b \in H$
Sottoanello ideale un sottoanello I di $(A,+,\cdot)$ si dice ideale se per ogni $i \in I$ e per ogni $a \in A$ si ha $i \cdot a \in I$ e $a \cdot i \in I$, si scrive $I \trianglelefteq A$
Dato l'anello $(A,+,\cdot,-,0)$, un sottoinsieme I di A è un ideale se e solo se per ogni $i, j \in I$ si ha $i - j \in I$ e per ogni $a \in A$ si ha $ia \in I$ e $ai \in I$

- Stabilire I non sia vuoto, basta fornire un elemento
- Mostrare che l'inverso appartiene ad I
- Mostrare chiusura rispetto a somma
- Mostrare $i \cdot a \in I$
- Mostrare $a \cdot i \in I$

Sottocampo *Primo criterio del sottocampo*: Dato il campo $(A, +, \cdot, -, \ ^{-1}, 0, 1)$, un sottoinsieme $H \subseteq A$ è un sottocampo se e solo se per ogni $a, b \in H$ si ha $a + b \in H$ e $-a \in H$ e $a \cdot b \in H$, $1 \in H$ e, se $a \neq 0$, $a^{-1} \in H$
Secondo criterio del sottocampo: Dato il campo $(A, +, \cdot, -, \ ^{-1}, 0, 1)$, un sottoinsieme $H \subseteq A$ è un sottocampo se e solo se $1 \in H$ e per ogni $a, b \in H$ si ha $a - b \in H$ e, se $b \neq 0$, $a \cdot b^{-1} \in H$
Teorema di Lagrange Sia $(A, \cdot)$ un gruppo di ordine n, allora ogni suo sottogruppo ha ordine che divide n
Teorema Sia $(A, \cdot)$ un gruppo abeliano di ordine n, allora per ogni divisore d di n esiste un sottogruppo di ordine d
Relazione compatibile una relazione su A è compatibile con una operazione $*$ se per ogni $a_1, a_2, b_1, b_2 \in A$ tali che $(a_1, a_2) \in R$ e $(b_1, b_2) \in R$ allora $a_1 * b_1 = a_2 * b_2$
Relazione di congruenza Relazione compatibile con tutte le operazioni dello spazio algebrico.
Intersezione di congruenze è una congruenza.
La relazione universale è una congruenza.
La minima congruenza contenente una relazione R è la congruenza generata da R su A.
Operazione indotta funzione $\overline{op}$: $\left(\frac{A}{R}\right)^n \to \frac{A}{R}$ dove R è una congruenza e n è l'arità dell'operazione op. Definita da $\overline{op}([a_1]_R, \dots) = [op(a_1, \dots)]_R$
Struttura quoziente di A su una congruenza R è la struttura $\left(\frac{A}{R}, \bar{o}\right)$ avente come sostegno l'insieme quoziente di A rispetto a R e come insieme di operazioni l'insieme di $\overline{op}$ indotte dalle operazioni originali.
Omomorfismo $f\big(op(a_1, \dots)\big) = \pi(op)(f(a_1), \dots)$ è una funzione tra due strutture algebriche simili che conserva le operazioni.
Omomorfismo tra gruppi f è un omomorfismo tra due gruppi $(A, +)$ e $(\hat{A}, \hat{+})$ se e solo se per ogni $a, b \in A$ si ha $f(a + b) = f(a) \hat{+} f(b)$
Omomorfismo tra anelli f è un omomorfismo tra due anelli $(A, +, \cdot)$ e $(\hat{A}, \hat{+}, \hat{\cdot})$ se e solo se per ogni $a, b \in A$ si ha $f(a + b) = f(a) \hat{+} f(b)$ e $f(a \cdot b) = f(a) \hat{\cdot} f(b)$
Monomorfismo omomorfismo iniettivo
Epimorfismo omomorfismo suriettivo
Isomorfismo omomorfismo biunivoco
Endomorfismo omomorfismo tra due strutture uguali
Automorfismo endomorfismo biiettivo
La composizione di mono/epi/isomorfismi è dello stesso tipo.
Siano $(A, \mathcal{O})$ e $(A', \mathcal{O}')$ due strutture simili e sia f un omomorfismo tra loro, la relazione $ker_f = \{(x, y) \in A \times A | f(x) = f(y)\}$ è una congruenza su $(A, \mathcal{O})$.
Proiezione canonica $\pi_R: A \to A/R$ definita da $\pi_R(a) = [a]_R$ è un epimorfismo tra $(A, \mathcal{O})$ e $(A/R, \bar{\mathcal{O}})$ e $ker_f = R$
Teorema di fattorizzazione degli omomorfismi Siano $(A, \mathcal{O})$ e $(A', \mathcal{O}')$ due strutture simili e sia f un omomorfismo tra loro. Sia $(A/ker_f, \bar{\mathcal{O}})$ la struttura quoziente di $(A, \mathcal{O})$ rispetto alla congruenza ker_f e sia π_R la proiezione canonica tra $(A, \mathcal{O})$ e $(A/ker_f, \bar{\mathcal{O}})$. Allora esiste unico un monomorfismo g tra $(A_1/ker_f, \bar{\mathcal{O}})$ e $(A', \mathcal{O}')$ tale che $f = \pi_R \cdot g$. Inoltre se f è un epimorfismo allora g è un isomorfismo.
Equazioni di aritmetica modulare
Del tipo $[a]x + [b] = [c]$ in $\mathbb{Z}_k$ o $\mathbb{Z}/k$
Calcolare $MCD(a, k)$
- Se $MCD(a, k) = 1$ (a è primo con k) allora l'equazione ha una e una sola soluzione: ogni $[a]$ ha inverso $[a]^{-1} = k$ quandi risulta $x = [a]^{-1}[c - b]$
- Altrimenti l'equazione può ammettere più soluzioni oppure nessuna: ogni $[a]$ è un divisore dello zero, quindi possiamo dedurre, al massimo, la sola esistenza delle soluzioni. $\exists d$: $[a][d] = [0]$

COSE UTILI:
Matrice singolare: ha determinante nullo
Matrice inversa: $A^{-1} = A^*/\det A$ dove A^* è la matrice aggiunta ottenuta come segue: Si trova la matrice formata dai complementi algebrici di A (Ogni elemento si sostituisce con il numero ottenuto così: si elimina la sua riga e la sua colonna dalla matrice, si calcola il determinante poi e si moltiplica per $(-1)^{n+k}$ con n e k rispettivamente il numero di riga e colonna) e si scrive la trasposta di quella appena trovata
Funzione identica del tipo $f(x) = x$
Elemento neutro spazio matrici con prodotto è la matrice identità

LOGICA PROPOSIZIONALE

Interpretazioni

$v(\neg A) = 1 - v(A)$

$v(A \wedge B) = 1$ sse $A = 1$ *e* $B = 1$

$v(A \vee B) = 1$ sse almeno uno tra A e B vale 1

$v(A \Rightarrow B) = \max(\neg A, B)$ … è 0 solo se $A = 1$ e $B = 0$

$v(A \Leftrightarrow B) = 1$ sse $v(A) = v(B)$… è 1 se A e B hanno stesso valore

NB: una formula con n lettere enunciative ha 2^npossibili valutazioni

Modello una valutazione v di una formula è un suo modello se vale 1

Formula soddisfacibile Una formula è soddisfacibile se esiste almeno un suo modello, cioè se almeno una sua valutazione vale 1, altrimenti è detta insoddisfacibile (o contraddizione)

Tautologia (f.b.f. valida) Formula per cui ogni valutazione è un modello, si scrive $\vDash \varphi$

Se si considera un **insieme Γ di f.b.f.** un modello è una valutazione che sia modello per ogni f.b.f. $\in \Gamma$, mentre Γ si dice soddisfacibile se esiste almeno un suo modello

Determinare se un insieme di formule è soddisfacilbile

A) Scrivere tavola di verità per tutte le formule, se c'è un modello che le soddisfa tutte allora l'insieme è soddisfacibile.

[ESEMPIO] $\{x \wedge (\neg y \Rightarrow x), x \Rightarrow (\neg y \Rightarrow \neg x)\}$

x	y	¬	¬y⇒	x∧(¬y⇒	¬x	¬y⇒	x⇒(¬y⇒
0	0	1	0	0	1	1	1
0	1	0	1	0	1	1	1
1	0	1	1	1	0	0	0
1	1	0	1	1	0	1	1

Esiste un input, che è [1,1], che è modello di entrambe le formule, quindi l'insieme è soddisfacibile

B) Scrivere l'albero semantico e verificare si trovi una formula vera

Conseguenza semantica φ è conseguenza semantica di Γ se ogni modello di Γ è modello di φ, si scrive $\Gamma \vDash \varphi$

Teorema di deduzione semantica $\Gamma \cup \{B\} \vDash A$ sse $\Gamma \vDash (B \Rightarrow A)$

Corollario 1 (f. debole) $B \vDash A$ sse $\vDash (B \Rightarrow A)$ [B⇒A *è una tautologia*]

Corollario 2 $\Gamma \vDash A$ sse $\Gamma \cup \{\sim A\}$ è insoddisfacibile

Stabilire se affermazione è corretta [ESEMPIO]

$(A \Leftrightarrow B) \vDash (A \Rightarrow B)$

A) Con definizione $(A \Rightarrow B)$ è conseguenza semantica di $(A \Leftrightarrow B)$ se ogni modello di $(A \Leftrightarrow B)$ è modello di $(A \Rightarrow B)$, verificarlo

A	B	$(A \Leftrightarrow B)$
0	0	**1** ←
0	1	0
1	0	0
1	1	**1** ←

A	B	$(A \Rightarrow B)$
0	0	1
0	1	1
1	0	0
1	1	1

Modelli di $(A \Leftrightarrow B)$: [0,0] [1,1]

Tutti sono anche modelli di $(A \Rightarrow B)$, dunque affermazione corretta

B) Con Th di ded. Semantica $(A \Leftrightarrow B) \vDash (A \Rightarrow B)$ sse $\vDash (A \Leftrightarrow B) \Rightarrow (A \Rightarrow B)$

A	B	A⇔B	A⇒B	(A⇔B)⇒(A⇒B)
1	1	1	1	**1**
1	0	0	0	**1**
0	1	0	1	**1**
0	0	1	1	**1**

Essendo l'ultima colonna di tutti 1, dunque affermazione corretta

C) Si può anche usare il secondo corollario del Th. di ded. sem.

Soddisfare $\boldsymbol{A \nvDash B}$ A deve avere un modello in corrispondenza del quale B sia falsa

Teorema di compattezza Γ soddisfacibile sse lo è ogni suo sottoinsieme

Equivalenza semantica $A \equiv B$ se tutti i modelli di A sono modelli di B e viceversa

Corollario 1 $A \equiv B$ sse $\vDash (A \Leftrightarrow B)$ [A⇔B *è una tautologia*]

Le formule non semanticamente equivalenti con n lettere enunciative sono $2\text{^}(2^n)$

Dimostrare equivalenza scrivere tavole di verità, se sono uguali allora formule sono equivalenti

Costruzione di una formula data la sua tavola di verità

Forma normale disgiuntiva si considerano le righe in cui la formula vale 1, per ognuna si scrive l'AND delle sue lettere enunciative o della loro negazione, a seconda di se valgono rispettivamente 1 o 0 su quella riga. Si fa l'OR dei termini così ottenuti

Forma normale congiuntiva si considerano le righe in cui la formula vale 0, per ognuna si scrive l'OR delle sue lettere enunciative o della loro negazione, a seconda di se valgono rispettivamente 0 o 1 su quella riga. Si fa l'AND dei termini così ottenuti

In alternativa, considerando le stesse righe in cui la formula vale 0, per ognuna si procede come nella forma disgiuntiva, e infine si piazza un NOT di fronte all'intera espressione. (con de morgan si torna a forma congiuntiva)

SEMPLIFICAZIONI[ESEMPIO]

$(\sim y \wedge \sim z) \vee (\sim y \wedge z) \equiv \sim y \wedge (\sim z \vee z) \equiv \sim y$

$(\sim x \vee y) \wedge (x \vee y) \equiv (\sim x \wedge x) \vee y \equiv y$

Insiemi adeguati di connettivi $\{\sim,\wedge\},\{\sim,\vee\},\{\sim,\Rightarrow\}$

Ogni f.b.f. si può riscrivere utilizzando solo questi insiemi

Equivalenze fondamentali

$\wedge$ e $\vee$ sono commutative e associative:

$A \vee (B \vee C) \equiv A \vee B \vee C \equiv B \vee A \vee C$

$\begin{cases} A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C) \\ A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C) \end{cases}$ distributività

$\begin{cases} A \wedge (A \vee B) \equiv A \\ A \vee (A \wedge B) \equiv A \end{cases}$ leggi di assorbimento

$\begin{cases} \sim (A \wedge B) \equiv \sim A \vee \sim B \\ \sim (A \vee B) \equiv \sim A \wedge \sim B \end{cases}$ leggi di De Morgan

$A \Rightarrow B \equiv \sim B \Rightarrow \sim A$ legge di contrapposizione

$A \Rightarrow B \equiv \sim A \vee B$ def. implicazione

$A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$ def. doppia implicazione

$(\sim A \wedge A) \vee B \equiv B$ legge di non contraddizione

$(\sim A \vee A) \wedge B \equiv B$ legge del terzo escluso

Teorema φ di $\mathcal{H}$ formula ottenuta da una dimostrazione a partire dagli assiomi e dalle regole di inferenza di $\mathcal{H}$, si scrive $\vdash_{\mathcal{H}} \varphi$

Deducibilità φ è deducibile in $\mathcal{H}$ dall'insieme di f.b.f. Γ se esiste una sequenza di formule derivanti da $\mathcal{H}$ e Γ che termina con φ, si scrive $\Gamma \vdash_{\mathcal{H}} \varphi$

Modus ponens da A e $A \Rightarrow B$ si riscrive B

Teorema di correttezza e di completezza (forte) $\Gamma \vDash A$ sse $\Gamma \vdash_L A$

Stabilire se $\Gamma \vdash_L A$ per Th di correttezza: $\Gamma \vdash_L A$ sse $\Gamma \vDash A$, stabilire se l'affermazione $\Gamma \vDash A$ è corretta, se si allora è vero che $\Gamma \vdash_L A$

Teorema di deduzione sintattica $\vdash_L \psi \Rightarrow \varphi$ sse $\psi \vdash_L \varphi$

Clausola: disgiunzione finita di letterali, esempio: $(\sim A \vee B)$

In forma a clausole formula scritta come congiunzione $\wedge$ di clausole

Insieme delle clausole [ESEMPIO]: $(A \Rightarrow B) \wedge (C \Rightarrow (A \wedge B))$ si scrive in forma normale congiuntiva: $\varphi \equiv (\sim A \vee B) \wedge \big(\sim C \vee (A \wedge B)\big) \equiv (\sim A \vee B) \wedge (\sim C \vee A) \wedge (\sim C \vee B)$

Quindi l'insieme delle clausole è $\varphi^C \equiv \big\{\{\sim A, B\},\{\sim C, A\},\{\sim C, B\}\big\}$

Forma a clausole è $\{\bar{A}B, \bar{C}A, \bar{C}B\}$

Regola di risoluzione

$\dfrac{A \cup B \quad C \cup \bar{B}}{A \cup C}$ se C è deducibile da Γ^C si scrive $\Gamma^C \vdash_R C$

Teorema di correttezza e completezza per refutazione

Un insieme di clausole Γ è insoddisfacibile(inconsistente) se e solo se $\Gamma \vdash_R \emptyset$ dove $\emptyset$ rappresenta l'insieme vuoto di letterali

NB: da questo teorema e dal Corollario 2 del teorema di deduzione semantica si ricava che una formula φ è semanticamente deducibile da un insieme di f.b.f. Γ sse $\Gamma^C \cup (\neg\varphi)^C \vdash_R \emptyset$

Stabilire se un insieme Γ di f.b.f. è soddisfacibile(consistente) o no

Trovare forma a clausole, risolvere, se si trova $\emptyset$ allora Γ è insoddisfacibile, se non si riesce a trovare verificare soddisfacibilità di Γ con albero oppure trovando il risolvente completo e verificando che non contenga $\emptyset$

[ESEMPIO]Γ: $\{x \Rightarrow y \vee z, y \Rightarrow \sim x, \sim z \Rightarrow x\}$

$x \Rightarrow y \vee z \equiv \neg x \vee (y \vee z) \equiv \{\bar{x}yz\}$

$y \Rightarrow \neg x \equiv \neg y \vee \neg x \equiv \{\bar{x}\bar{y}\}$

$\neg z \Rightarrow x \equiv z \vee x \equiv \{xz\}$

$\Gamma^C = \{\bar{x}yz, \bar{x}\bar{y}, xz\}$ non si riesce a risolvere per trovare $\emptyset$, allora trovare risolvente completo:

Ris_0: $\bar{x}yz, \bar{x}\bar{y}, xz$

Ris_1: $\bar{x}z, yz, \bar{y}z$

Ris_2: z

I risolventi si calcolano combinando elementi di tutti i livelli superiori a coppie contenenti al più un letterale opposto

Nel risolvente completo (unione di tutti i livelli) non compare mai $\emptyset$, quindi Γ è consistente

Stabilire se una f.b.f. φ è cons. semantica di insieme di f.b.f. Γ

($\Gamma \vDash \varphi$ o $\Gamma \vdash \varphi$ per Th di corr. e comp.)

Trovare l'insieme delle clausole Γ^C di Γ e $(\neg\varphi)^C$di $(\neg\varphi)$, scrivere l'insieme $\Delta = \Gamma^C \cup (\neg\varphi)^C$ di tutte queste clausole. Risolvere a partire da Δ per stabilirne consistenza. Se si riesce a trovare ∅, Δ è inconsistente e vale $\Gamma \vDash \varphi$, se Δ è consistente non vale la cons. sem.

[ESEMPIO]: stabilire la correttezza di: $x \Rightarrow (y \wedge z) \vDash (x \Rightarrow y) \wedge (x \Rightarrow z)$

Sono Γ: $x \Rightarrow (y \wedge z)$ e $(\neg\varphi)$: $\neg((x \Rightarrow y) \wedge (x \Rightarrow z))$

Γ:x⇒(y∧z)≡¬x∨(y∧z)≡(¬x∨y)∧(¬x∨z)

$(\neg\varphi)$: ¬((x⇒y)∧(x⇒z))≡¬(x⇒y)∨¬(x⇒z)≡¬(¬x∨y)∨¬(¬x∨z)

≡(x∧¬y)∨(x∧¬z)≡x∧(x∨¬z)∧(¬y∨x)∧(¬y∨¬z)

Quindi $\Gamma^C = \{\bar{x}y, \bar{x}z\}$ e $(\neg\varphi)^C = \{x, x\bar{z}, x\bar{y}, \bar{y}\bar{z}\}$

Per cui $\Delta = \{\bar{x}y, \bar{x}z, x, x\bar{z}, x\bar{y}, \bar{y}\bar{z}\}$

Si può risolvere nel seguente modo:

$$\dfrac{\dfrac{\dfrac{\bar{x}y \quad x}{y} \quad \bar{y}\bar{z}}{\bar{z}} \quad \dfrac{\bar{x}z \quad x}{z}}{\emptyset}$$

Essendo $\Gamma \cup (\sim \varphi)$ inconsistente, vale $\Gamma \vDash \varphi$

Provare che $\vdash_L \psi \Rightarrow \varphi$

Per th. ded. sint. $\vdash_L \psi \Rightarrow \varphi$ sse $\psi \vdash_L \varphi$

Stabilire se è vero che $\psi \vdash_L \varphi$

LOGICA DEL PRIMO ORDINE

Traduci in linguaggio del primo ordine

[ESEMPIO]: $\langle 0,1,+,\times,\leq\rangle$ con identità

Ogni due numeri Naturali diversi da 0 hanno un unico massimo comun divisore:

x diverso da zero: $x \neq 0 \coloneqq \sim(x = 0)$

z è divisore di x: $z/x \coloneqq \exists w(x = w \times z)$

z è div. com. di x e y: $z/x \wedge z/y$

z è massimo c.d. di x e y: z è c.d. di x e y e se w è c.d. di x e y allora w è un div. di z $G(x,y,z) \coloneqq z/x \wedge z/y \wedge \forall w(w/x \wedge w/y \Rightarrow z/w)$

Frase completa:∀xy(x≠0∧y≠0⇒∃z(G(x,y,z)∧∀w(G(x,y,z)⇒w=z))

[ESEMPIO]: $\langle \mathbb{R}, 0,1,-,+,\times,\leq\rangle$ con identità

Il quadrato di un positivo è positivo, di un negativo è positivo. Essendo il quadrato di 0 non negativo, nessun negativo è un quadrato.

x^2:=x×x x≠y:=∼(x=y) x>y:=(y≤x∧x≠y) x<y:=(x≤y∧x≠y)

Quadrato di pos è pos: $\forall x(x > 0 \Rightarrow x^2 > 0)$

Quadrato di neg è pos: $\forall x(x < 0 \Rightarrow x^2 > 0)$

Se 0 non neg, no neg è un quadrato: $\sim(0<0)\Rightarrow\sim\exists x((x<0)\wedge\exists y(x=y^2))$

Argomentazione: $\forall x(x>0\Rightarrow x^2>0)$, $\forall x(x<0\Rightarrow x^2>0) \vDash \sim(0<0)\Rightarrow\sim\exists x((x<0)\wedge\exists y(x=y^2))$

Campo d'azione di ∀ o ∃ in $\forall x(\psi)$ è ψ

Occorrenza vincolata si trova nel campo d'azione di un quantificatore di cui è argomento o è l'argomento stesso [ESEMPIO]: $\forall x(A(x))$

Occorrenza libera non vincolata [ESEMPIO]: x in $A(x)$ o $\forall y(A(x))$

Insieme variabili libere: $FV(\psi)$

Se $FV(\psi) = \{\emptyset\}$ la f.b.f. ψ si dice chiusa, altrimenti aperta

Chiusura universale e esistenziale dato $FV(\psi) = \{x_1, x_2, \dots, x_n\}$, la chiusura universale di una f.b.f. ψ è $\forall x_1 \forall x_2 \dots \forall x_n \psi$, quella esistenziale è $\exists x_1 \exists x_2 \dots \exists x_n \psi$

Termine libero per una variabile x *t* tale che nessuna occorrenza libera di x cade nel campo d'azione di un quantificatore che abbia come argomento una variabile che compare in *t*

[ESEMPIO]:

$\exists y(f(x,y))$ f(x,y) non è libero per x perché x è libera e cade nel campo di azione di un quantificatore che ha per argomento y che è una variabile di f(x,y)

$\exists y(f(x,z))$ f(x,z) è libero rispetto a z

Interpretazione Sia φ una f.b.f. e siano $\langle D, I\rangle$ una struttura interpretativa e s un assegnamento. $(\langle D, I\rangle, s)$ è una intepretazione.
Se s soddisfa φ in $\langle D, I\rangle$ allora l'interpretazione $(\langle D, I\rangle, s)$ è un **modello**
Si scrive: $(\langle D, I\rangle, s) \vDash \varphi$
Se si ha insieme Γ di f.b.f. un modello lo è se modello per tutte le f.b.f.

f.b.f. soddisfacibilità

In una struttura interpretativa:
Soddisfacibile: esiste un assegnamento che la soddisfa, altrimenti è insoddisfacibile o falsa
Vera: ogni assegnamento la soddisfa
Falsa: nessun assegnamento la soddisfa
NB: in una struttura una *formula chiusa* non può essere al contempo soddisfacibile ma non vera, quindi è solo vera o falsa
Su una segnatura: (quindi non si ha interpretazione)
Soddisfacibile: esiste almeno un modello, cioè esiste una interpretazione con un assegnamento che sia un modello, altrimenti è insoddisfacibile o contraddittoria
Valida: ogni interpretazione è un modello
Contraddittoria: nessuna interpretazione è un modello
φ è valida sse $\neg\varphi$ è insoddisfacibile
NB: Chiusura universale di φ vera(valida) sse φ è vera(valida)
Chiusura esistenziale di φ è vera(valida) sse φ è soddisfacibile

Determinare soddisfacibilità verità o insoddisfacibilità

[ESEMPIO]: $\varphi \coloneqq x \neq 0 \Rightarrow \exists y(xy = 1)$ in $\mathbb{N}$
$\varphi(0) \coloneqq 0 \neq 0 \Rightarrow \exists y(0y = 1) \quad False \Rightarrow False$ vera in $\mathbb{N}$
$\varphi(1) \coloneqq 1 \neq 0 \Rightarrow \exists y(1y = 1) \quad True \Rightarrow True$ vera in $\mathbb{N}$
$\varphi(2) \coloneqq 2 \neq 0 \Rightarrow \exists y(2y = 1) \quad True \Rightarrow False$ falsa in $\mathbb{N}$
φ è soddisfacibile ma non vera

Esempio di tautologia f.b.f. logicamente valida ottenuta da una tautologia di logica preposizionale
Forma normale prenessa $Q_1x_1Q_2x_2 \dots Q_nx_n\psi$ dove $Q_i = \{\forall, \exists\}$ e ψ è una f.b.f. che non contiene quantificatori.
Si ottiene con equivalenze semantiche:

1. $\sim\forall x\psi \equiv \exists x{\sim}\psi$
2. $\sim\exists x\psi \equiv \forall x{\sim}\psi$
3. $\forall x\psi \wedge \theta \equiv \forall y(\psi[y/x] \wedge \theta)$
4. $\exists x\psi \wedge \theta \equiv \exists y(\psi[y/x] \wedge \theta)$
5. $\forall x\psi \vee \theta \equiv \forall y(\psi[y/x] \vee \theta)$
6. $\exists x\psi \vee \theta \equiv \exists y(\psi[y/x] \vee \theta)$
7. $\forall x\psi \Rightarrow \theta \equiv \exists y(\psi[y/x] \Rightarrow \theta)$
8. $\exists x\psi \Rightarrow \theta \equiv \forall y(\psi[y/x] \Rightarrow \theta)$
9. $\theta \Rightarrow \forall x\psi \equiv \forall y(\theta \Rightarrow \psi[y/x])$
10. $\theta \Rightarrow \exists x\psi \equiv \exists y(\theta \Rightarrow \psi[y/x])$

Si opera la sostituzione $[y/x]$ se e solo se $x \in FV(\theta)$, e si sostituisce con una variabile $y \notin FV(\theta)$ che è libera per x in ψ

Forma di Skolem in forma normale prenessa e non contiene quantificatori esistenziali

1. Portare in forma prenessa
2. Osservare primo quantificatore
   - Se è $\exists x$ allora si elimina e si sostituisce ogni occorrenza di x che è diventata libera con una nuova costante
   - Se si incontrerebbe esistenziale $\exists x$ dopo altri $\forall x_1\forall x_2 \dots \forall x_n$, allora si elimina $\exists x$ e si sostituisce ogni occorrenza di x che è diventata libera con un nuovo termine $t(x_1, x_2, \dots, x_n)$
3. Tornare al punto 2 fino a che non si ha una forma di Skolem

NB: se $\exists x$ non ha nessuna x nel su campo d'azione, può essere eliminata senza ulteriori operazioni

Teorema di Skolem una f.b.f. ψ è insoddisfacibile sse una forma di Skolem della sua chiusura universale è insoddisfacibile

Teorema di correttezza e completezza sia φ una formula del linguaggi del primo ordine contenente solo gli operatori $\neg$, $\Rightarrow$, $\forall$, allora: se $\vdash \varphi$ allora φ è vera per ogni modello ed è logicamente valida; se φ è logicamente valida allora $\vdash \varphi$

Teorema di deduzione sintattica siano φ e ψ delle formule del primo ordine contenti solo gli operatori $\neg$, $\Rightarrow$, $\forall$, e sia Γ un insieme di formule, allora se ψ è chiusa: $\Gamma \cup \{\psi\} \vdash \varphi$ sse $\Gamma \vdash \psi \Rightarrow \varphi$

Sostituzione Insieme di regole del tipo t/x dove x è una variabile e t è un termine diverso con cui sostituirla.
Il prodotto di sostituzioni corrisponde alla loro applicazione successiva. Un unificatore è una sostituzione che dato un insieme di stringhe a cui è applicata lo trasforma in un insieme di stringhe tutte uguali.
[ESEMPIO] Si vuole unificare $\{A(x,z), A(f(z),a), A(y,g(x))\}$, si nota che il primo argomento delle A è diverso, allora si utilizza la sostituzione $\sigma=[f(z)/x, f(z)/y]$ ottenendo $\{A(f(z),z), A(f(z),a), A(f(z),g(x))\}$. Ora si nota che il secondo argomento delle A contiene sia una costante a che una lettera funzionale $g(x)$ non si può procedere con una ulteriore sostituzione, quindi l'insieme non è unificabile.
[ESEMPIO] $\{A(x,z), A(f(z),a)\}$ è unificabile: infatti applicando prima $\sigma=[f(z)/x]$ e poi $\sigma=[a/z]$ si ottiene $\{A(f(a),a), A(f(a),a)\}$

Stabilire se una f.b.f. φ è cons. semantica di insieme di f.b.f. Γ

$\Gamma \vDash \varphi$ sse $\Gamma \vDash \psi$, dove ψ è la chiusura universale di φ, sse $\Gamma \cup \{\neg\psi\}$ è insoddisfacibile. Si portano in forma di Skolem Γ e ψ; si portano in forma di clausola le loro matrici e si ottiene l'insieme delle clausole. Si applica il metodo di risoluzione: se si riesce a ottenere la clausola vuota allora $\Gamma \cup \{\neg\psi\}$ è insoddisfacibile e $\Gamma \vDash \varphi$.
[ESEMPIO] $\Gamma \coloneqq \{\forall x(A(x) \Rightarrow B(g(x))), \forall x A(f(x)) \Rightarrow \neg B(x))\}$ e $\varphi \coloneqq B(x) \Rightarrow B(g(f(x)))$; vogliamo stabilire se $\Gamma \vDash \varphi$. Si fa la chiusura universale di φ ottenendo $\psi \coloneqq \forall x(B(x) \Rightarrow B(g(f(x))))$. Si skolemizza le formule di $\Gamma \cup \{\neg\psi\}$ e si pongono in forma a clausoe ottenendo l'insieme di clausole:
$S = \{\{\neg A(x), B(g(x))\}, \{A(f(x)), \neg B(x)\}, \{B(a)\}, \{\neg B(g(f(a)))\}\}$
Si separano le variabili ottenendo l'insieme:
$S = \{\{\neg A(x), B(g(x))\}, \{A(f(y)), \neg B(y)\}, \{B(a)\}, \{\neg B(g(f(a)))\}\}$
Si applica la risoluzione

$$\dfrac{\dfrac{\dfrac{\{\neg A(x), B(g(x))\} \quad \{\neg B(g(f(a)))\}}{\neg A(f(a))}\ [f(a)/x] \qquad \{A(f(y)), \neg B(y)\}}{\{\neg B(a)\}}\ [a/y] \qquad \{B(a)\}}{\emptyset}$$