1 Proprietà relazioni

1.1 seriale

$\forall a \in A\ \exists b \in A (a,b) \in R$
Grafo: ogni vetice ha una freccia uscente
Matrice: ogni riga ha almeno un "1"

1.2 riflessiva

$\forall a \in A\ (a,a) \in R$
Grafo: ogni vetice ha un cappio
Matrice: sulla diagonale ho tutti "1"

1.3 simmetrica

$\forall a,b \in A\ (a,b) \in R \Rightarrow (b,a) \in R$
Grafo: Ogni freccia in una direzione ne ha una della direzione opposta
Matrice: $Mr = Mr^T$

1.4 antisimmetrica

$\forall a,b \in A\ se\ (a,b) \in R\ e\ (b,a) \in R \Rightarrow a = b$
Grafo: Non ci devono essere doppie freccie
Matrice: eccetto la diagonale, se in pos (i,j) c'è un 1, allora in posizione (j,i) ci deve essere 0

1.5 transitiva

$\forall a,b,c \in A\ (a,b) \in Re\ (b,c) \in R \Rightarrow (a,c) \in R$
Grafo: se a è collegato a b e b è collegato a c anche a deve essere collegato a c
Matrice: $Mr^2 \subseteq Mr$

Osservazioni

- seriale $\not\Rightarrow$ riflessiva
- antisimmetrica $\not\Rightarrow$ non simmetrica
- transitiva + simmetrica $\not\Rightarrow$ riflessiva
- riflessiva $\Rightarrow$ seriale
- transitiva + simmetrica + seriale $\Rightarrow$ riflessiva

1.6 Relazioni di equivalenza

Una relazione si dice di equivalenza se è riflessiva, transitiva, simmetrica (tutti i possibili collegamenti in ogni componente connessa nel grafo)

1.7 Relazioni d'ordine

Una relazione si dice d'ordine se è riflessiva, transitiva, antisimmetrica (per esistere una ch d'ordine la relazione deve essere antisimmetrica, se facendo la chiusura riflessiva e transitiva rimane antisimmetrica ora è una ch d'ordine)

1.8 elementi estremali

- Massimo: $se\ \forall\ x \in A\ a \leq x$
- Minimo: $se\ \forall\ x \in A\ a \geq x$
- Minimale: $\forall\ x \in A\ se\ x \leq a \Rightarrow x = a$
- Massimale: $\forall\ x \in A\ se\ x \geq a \Rightarrow x = a$

Oss: Un minimo è minimale, un massimo è massimale (minimali e massimali esistono in relazioni d'ordine)

1.9 Maggiorante/minorante, sup/inf

Un elemento m si dice

- Maggiorante di B se $\forall b \in B\ b \leq m$
- Minorante di B se $\forall b \in B\ b \geq m$
- Estremo sup di B se è il minimo dei maggioranti (se esiste)
- Estremo inf di B se è il massimo dei minoranti (se esiste)

1.10 funzioni in relazioni

Proprietà della funzionalità :
Grafo: un elemento punta solo ad un altro (possono esserci varie funzioni da una relazione, ma la relazione deve essere per forza seriale) Matrice: per avere una funz devo avere un 1 per riga

Funzione iniettiva (ha inversa destra):
Matrice: in ogni colonna c'è al più un 1 **Funzione suriettiva (ha inversa sinistra):**
Matrice: in ogni colonna c'è almeno un 1

2 Logica proposizionale

2.1 sintassi

- Lettere enunciative: $A_1, A_2, ..., A_n$
- Connettivi: $\neg, \wedge, \vee, \implies, \iff$
- Simboli ausiliari: ( ) ;

2.2 formula ben formata

1. Ogni lettera enunciativa è una f.b.f.
2. Se A, B sono sono f.b.f. allora $(A \implies B), (A \iff B), (A \wedge B), (A \vee B), (\neg A)$ sono f.b.f.
3. Nient'altro è una f.b.f.

Priorità connettivi: $\neg, \wedge, \vee, \implies, \iff$
Significato connettivi

- $(A \implies B)$ Sempre vero se A=0, Se A=1 vero solo se anche B=1
- $(A \iff B)$ Vero se A=B
- $(A \implies B) = \neg A \vee B$
- $(A \iff B) = (A \implies B) \wedge (B \implies A)$

2.3 equivalenze

- $A \implies B = \neg B \implies \neg A$
- $(\neg A \wedge A) \vee B = B$
- $A \wedge (A \vee B) = A$
- $A \vee (A \wedge B) = A$
- $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$
- $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$

- Una f.b.f. A si dice soddisfacibile se esiste almeno una interpretazione che è modello di A
- Una f.b.f. A per cui ogni interpretazione è un modello si dice tautologia
- Una f.b.f. che non ammette modelli si dice insoddisfacibile
- Una f.b.f. B che ha gli stessi modelli di A si dice conseguenza semantica di A

2.4 risoluzione logica proposizionale

- Letterali: Una lettera enunciativa (A) o la sua negata $(\neg A)$
- Clausola: Insieme di letterali (disgiunzione di letterali) $(\{\neg A, B, C\}, \{B, C, D\})$

1. Portare in forma normale congiuntiva es: $(A \vee B \vee \neg C) \wedge (B \vee D \vee \neg A)$ (or tra lettere e and tra gruppi)
2. Convertire a letterali e clausole es: $\{A, B, \neg C\}, \{B, D, \neg A\}$ (ogni parentesi diventa una clausola con i propri letterali dentro)
3. L'obiettivo è raggiungere la clausola vuota, abbinado una clausola con un'altra ed eliminando IL letterale che in una è normale e nell'altra è negato

3 Logica del primo ordine

3.1 sintassi

- Lettere predicative: $D(x,y) = 0/1$ falso o vero (es uguaglianza)
- Lettere funzionali: $P(x,y) = x \cdot y$ risultato della funzione (es moltiplicazione)
- variabili/ costanti (es x,y/a,b)
- connettivi soliti
- quantificatori: $\exists, \forall$

Per chiudere una formula del primo ordine si quantifica ogni variabile libera con il $\forall$
Forma normale prenessa
Sposto tutti i quantificatori in testa (dopo aver chiuso la formula)

Forma di skolem
- la formula non deve più contenere $\exists$
- sostituisco le variabili precedute da $\exists$ con tante lettere funzionali quanti $\forall$ ci sono prima del $\exists$ che devo togliere (le variabili che uso sono quelle dei $\forall$ precedenti al $\exists$ che ho tolto)

3.2 equivalenze

- $\neg \forall x A(x) = \exists x \neg A(x)$
- $\neg \exists x A(x) = \forall x \neg A(x)$
- $\forall A(x) \wedge B = \forall y (A(y) \wedge B(y))$
- (vale anche per $\exists$ e anche per $\vee$) (estraendo un quantificatore da $\vee$ o $\wedge$ non lo cambio) (si rinomina la variabile per sicurezza)
- $\forall x A(x) \implies B = \exists y (A(y) \implies B)$
- $\forall x B \implies A(X) = \forall y (B \implies A(y))$
- estraendo un quantificatore da un $\implies$ si cambia se lo si estrae dal primo termine, non si cambia se lo si estrae dal secondo termine

3.3 Forma a clausole

$\forall x_1, ..., \forall x_n ((L_1 \vee L_2 \vee L_3) \wedge (...) \wedge ...)$

4 algebra

4.1 strutture algebriche

- semigruppi $\rightarrow$ proprietà associativa
- monoidi $\rightarrow$ semigruppi + elemento neutro unico
- gruppo $\rightarrow$ monoide + inverso
- gruppo abelliano $\rightarrow$ gruppo + commutatività
- anello (A,+,$\cdot$) dove A(+) gruppo abelliano e A($\cdot$) semigruppo e vale la proprietà distributiva $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$
- corpo $\rightarrow$ anello + gli elementi != 0 sono invertibili + elemento neutro
- campo $\rightarrow$ corpo + commut rispetto a $\cdot$

4.2 sottostrutture

- $(H, \cdot)$ sottosemigruppo di $(S, \cdot)$ sse $\forall a, b \in H$ il risultato della moltiplicazione è ancora interno a H
- $(H, \cdot, e)$ sottomonoide di $(M, \cdot, e)$ (con e elemento neutro unico) sse è un sottosemigruppo e $e \in H$
- $(H, \cdot, e, ^{-1})$ sottogruppo di $(G, \cdot, e, ^{-1})$ sse: H è chiuso rispetto alla moltiplicazione e all'inverso
- $(H, +, \cdot)$ sottoanello di $(A, +, \cdot)$ se $(H, +)$ sottogruppo di $(A, +)$ e $(H, \cdot)$ sottosemigruppo di $(A, \cdot)$
- $(H, +, \cdot)$ sottocampo/ sottocorpo di $(A, +, \cdot)$ se è un sottoanello e $(H \backslash \{0\}, \cdot)$ è sottogruppo di $(A \backslash \{0\}, \cdot)$

4.3 congruenza

Data una struttura algebrica (A, Ω) una relazione $\rho \subseteq AxA$ si dice compatibile per $* \in \Omega$ se:
$\forall a_1, b_2, b_1, b_2$
$a_1 \rho b_1 e\ a_2 \rho b_2 \implies a_1 * a_2 \rho b_1 * b_2$
se ρ è compatibile con tutte le operazioni di Ω di chiama congruenza

4.4 struttura quoziente

Con (A, Ω) struttura algebrica e ρ congruenza allora per ogni operazione * possiamo definire una operazione binaria interna A/ρ definita da:
$*_\rho : A/\rho X A/\rho \implies A/\rho$
$[a]_\rho *_\rho [b]_\rho := [a * b]_\rho$

4.5 omorfismi

Date due strutture algebriche $A_1, \Omega_1, A_2, \Omega_2$ una funzione $F : A_1 \rightarrow A_2$ preserva tutte le operazioni tra Ω_1, Ω_2 si chiama omomorfismo:

- f è iniettiva $\rightarrow$ monomorfismo
- f è suriettiva $\rightarrow$ epimorfismo
- f è biunivoca $\rightarrow$ isomorfismo

criterio per gruppi
Dati $(G, *), (H, \cdot)$ gruppi e $f : G \rightarrow H$ omomorfismo $\iff \forall g_1, g_2$
$f(g_1 * g_2) = f(g_1) * f(g_2)$

criterio per anelli
Dati $(A, +, \cdot)$, $(B, \oplus, \odot)$ anelli e $\gamma : A \rightarrow B$ omomorfismo $\iff$
- $\forall a, b \in A$ - $\gamma(a + b) = \gamma(a) \oplus \gamma(b)$
- $\forall a, b \in A$ - $\gamma(a \cdot b) = \gamma(a) \odot \gamma(b)$

5 SPASS

5.1 struttura di un programma spass

list_of_symbols.
functions[(n_funz,arità),...,(cost,0)].
predicates[(n_predicato,arità),...].
end_of_list.

list_of_formulae(axioms).
formula(...). end_of_list.

list_of_formulae(conjectures).
congettura_da_verificare(...). end_of_list.

5.2 sintassi

- $\wedge$ = and(), $\vee$ = or(), $\neg$ = not()
- $\implies$ = implies(), $\iff$ = equiv()
- $\forall$ = forall([x],...)
- $\exists$ = exists([x],...)

spass lavora solo su formule chiuse

funzioni: ad esempio moltiplicazione (le costanti sono funzioni di arità 0)
predicati: ad esempio uccide, è presente, è incantato, commercia