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 SPASS

4.1 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.
```

4.2 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

5 Algebra

5.1 Strutture algebriche

- Le strutture algebriche sono una coppia (A,Ω) Dove $\Omega = \omega_1, ..., \omega_K$ è un insieme di operazioni interne all'insieme A

tipi di strutture algebriche

- **semigruppo** (A,·) Dove · è un'operazione binaria che soddisfa la proprietà associativa (se l'operazione è commutativa il semigruppo si dice semigruppo commutativo)
- **Monoide** (M,*,e) Dove (M,*) è un semigruppo e e∈M è un elemento neutro (unico) all'operazione *
- **Gruppo** (G,*,e,$^{-1}$) Dove (G,*,e) è un monoide ed esiste l'inverso $\forall g \in G\ \exists h \in G$ tale che g*h=h*g=e (h è l'inverso destro e sinistro di g)
- **Anello** (A,+,·) Dove (A,+) è un gruppo commutativo con elementro neutro 0, e (A,·) è un semigruppo
- **Corpo e campo** Un corpo è un anello (A,+,·,1) con identità tale che (A\{0},·) è un gruppo, se questo gruppo è commutativo si parla di campo

Zero di un sermigruppo (S,·) (elemento assorbente)
è un elemento $z \in S$ tale che $\forall s \in S$
$s \cdot z = z \cdot s = z$
Divisori dello zero
In un anello (A,+,·) due elementi a,b a≠0,b≠0 si dicono divisori dello zero se a·b=0
In un anello privo di divisori dello zero valgono le leggi di cancellazione a sinistra e destra
Osservazione
Se il semigruppo moltiplicativo (A\{0},·) è un gruppo $\implies$ l'anello non ha divisori dello zero

Quaternioni:corpo che non è un campo
Definiti da: $H = \{a \cdot i + b \cdot j + c \cdot k + d\ \ a, b, c, d \in \Re\}$

5.2 Sottostrutture

Data (A,Ω) struttura algebrica e H⊆A, (H,Ω) è una sottostruttura algebrica se tutte le operazioni di omega "si restringono" ad H:
$* \in \Omega\ \ \forall h_1, h_2 \in H\ \ h_1 * h_2 \in H$
Quindi tutte le operazioni Ω sono chiuse in H

1. (H,·) è sottosemigruppo di un semigruppo (S,·) (H⊆ S) $\iff \forall a, b \in H\ \ a \cdot b \in H$
$\cdot : H \times H \to H$
2. (H,·,e) è sottomonoide del monoide (M,·,e) $\iff$ è un sottosemigruppo $\wedge\ e \in H$
3. (H,·,e, $^{-1}$) è un sottogruppo del gruppo (G,·,e, $^{-1}$) $\iff$
$\forall a, b \in H\ \ a \cdot b \in H$
$\forall a \in H\ \ a^{-1} \in H$

   Criterio per gruppi:
   (H,·) è sottogruppo $\iff$
   $\forall a, b \in H\ \ a \cdot b^{-1} \in H$
4. (H,+,·) è un sottoanello di (A,+,·) $\iff$:
(H,+) è un sottogruppo di (A,+)
(H,·) è un sottosemigruppo di (A,·)
5. (H,+,·) sottocampo/sottocorpo di (A,+,·) se è un sottoanello e (H \{0},·) è un sottogruppo di (A \{0},·)

Strategia: uso i criteri delle sottostrutture tramite strutture note

Strutture note:

- Campi:$(\mathbb{Z}/5, +, \cdot), (\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$
- Anelli: $(\mathbb{R}[x], +, \cdot)$ (polinomi in x), $(\mathbb{M}_{nn}(\mathbb{R}), +, \cdot)$ (matrici quadrate), $(\mathbb{Z}/5, +, \cdot)$ (classi di equivalenza per numeri non primi (anelli con divisori deello zero))
- Gruppi: $(GL_n(\mathbb{R}), +)$ (matrici con determinante $\neq 0$)
- Monoidi: $(\mathbb{N}, +, 0)$

5.3 Congruenza/strutture quoziente/omomorfismi

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

Data (A,Ω) struttura e $\rho \subseteq A \times A$ congruenza allora per ogni operazione *∈ Ω possiamo definire una nuova operazione interna A\ρ
$*_\rho : A \setminus \rho \times A \setminus \rho \to A \setminus \rho$
Definita da $[a]_\rho *_\rho [b]_\rho := [a * b]_\rho$
Nuova struttura algebrica: $(A \setminus \rho, \Omega_\rho)$ dove $\Omega_\rho = \{*_\rho\ \ * \in \Omega\}$

Omomorfismo
Un omomorfismo è una funzione f che preserva tutte le operazioni Ω_1 e Ω_2 tra le strutture (A_1, Ω_1) e (A_2, Ω_2)
Tipi di omomorfismo in base a f:

- f iniettiva → monomorfismo
- f suriettiva → epimorfismo
- f biunivoca → isomorfismo

Criterio per gruppi
Dati (G,*) e (H,·) gruppi $f : G \to H$ è un omomorfismo $\iff \forall g_1, g_2\ \ \ f(g_1, g_2) = f(g_1) \cdot f(g_2)$
Criterio per anelli
Dati (A,+,·) e (B,⊕,⊙) anelli $\phi : A \to B$ è un omomorfismo se:
$\forall a, b \in A\ \ \ \varphi(a + b) = \varphi(a) \oplus \varphi(b)$
$\forall a, b \in A\ \ \ \varphi(a \cdot b) = \varphi(a) \odot \varphi(b)$

5.4 Sottogruppi normali(gruppi)/ ideali(anelli)

Un sottogruppo H di un gruppo (G,*) si dice normale se:
$\forall g \in G, \forall h \in H\ \ \ \ g^{-1} * h * g \in H\ \ \ (\iff \forall g \in G\ \ g^{-1} * h * g \subseteq H)$
Osservazione: se G è commutativo $\implies$ tutti i sottogruppi sono normali $g^{-1} * h * g = g^{-1} * g * h = h * e_G = h \in H\ \ \forall h \in h\ \ \forall g \in G$
Proposizione: se ρ è una congruenza del gruppo (G,*) allora $[e_G]_\rho$ è un sottogruppo normale

Un **ideale** I di un anello (A,+,·) è un sottoanello di A che soddisfa l'assorbimento $\forall a \in A$:
Destra: I·A = $\{x \cdot a : x \in I\}$ ⊆ I
Sinistra: I·A = $\{a \cdot x : x \in I\}$ ⊆ I