Relazioni e funzioni

Dati n insiemi A_n, una relazione R di arità n è un insieme nella forma

$$R \coloneqq \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i,\, i = 1, 2, \ldots, n\}.$$

Dunque, $R \subseteq A_a \times A_2 \times \ldots \times A_n$. Poiché sono insiemi, valgono le usuali operazioni ($\subset$, $\subseteq$, $=$, $\cap$, $\cup$). Proprietà:

Proprietà	$\cap$	$\cup$
Idempotenza	$R \cap R = R$	$R \cup R = R$
Commutatività	$R \cap S = S \cap R$	$R \cup S = S \cup R$
Associatività	$(R \cap S) \cap T = R \cap (S \cap T)$	$(R \cup S) \cup T = R \cup (S \cup T)$
Distributività	$R \cap (S \cup T) = (R \cap S) \cup (R \cap T)$	$R \cup (S \cap T) = (R \cup S) \cap (R \cup T)$

Il prodotto tra due relazioni $R \subseteq A_1 \times A_2$ e $S \subseteq A_2 \times A_3$ è definito come

$$R \cdot S \coloneqq \{(a_1, a_3) \mid \exists\, a_2 \in A_2 : (a_1, a_2) \in R \land (a_2, a_3) \in S\}.$$

Il prodotto tra relazioni è associativo, compatibile con l'inclusione ($R \subseteq T \subseteq A_1 \times A_2 \land S \subseteq V \subseteq A_2 \times A_3 \implies R \cdot S \subseteq T \cdot V$), ma non è commutativo.

Relazione inversa: $R^{-1} \coloneqq \{(a_2, a_1) \mid (a_1, a_2) \in R\}$. Proprietà:

- $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$,
- $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$,
- $R \cdot (S \cap T) = (R \cdot S) \cap (R \cdot T)$,
- $R \cdot (S \cup T) = (R \cdot S) \cup (R \cdot T)$,
- $(R \cdot S)^{-1} = S^{-1} \cdot R^{-1}$,
- $R \subseteq S \implies R^{-1} \subseteq S^{-1}$.

La potenza di una relazione binaria $R \subseteq A \times A$ è definita come

$$R^n \coloneqq \begin{cases} I_A & \text{se n} = 0 \\ R \cdot R^{n-1} & \text{se n} > 0 \end{cases} \qquad \text{dove } n \in \mathbb{N}.$$

La restrizione $B \subseteq A$ di una relazione $R \subseteq A \times A$ è definita come $R|_B \coloneqq R \cap (B \times B)$. Proprietà:

- $R|_\varnothing = \varnothing$,
- $R|_B \cup R|_C \subseteq R|_{B \cup C}$,
- $R|_B \cap R|_C = R|_{B \cap C}$.

Proprietà di una relazione binaria $R \subseteq A \times A$:

Serialità: $\forall\, a \in A, \exists\, a' \mid (a, a') \in R$;

Riflessività: $\forall\, a \in A, (a, a) \in R$,

Simmetria: $\forall\, (a, a') \in R, (a', a) \in R$,

Antisimmetria: $\forall\, a, a' \in A, (a, a') \in R \land (a', a) \in R \implies a = a'$,

Transitività: $\forall\, (a, a'), (a', a'') \in R, (a, a'') \in R$.

Dato un insieme di proprietà formali **P** ed una relazione binaria $R \subseteq A \times A$, si dice **P**-chiusura di R una relazione $S \subseteq A \times A$ tale che:

- $R \subseteq S$,
- S gode di tutte le proprietà in **P**,
- se $T \subseteq A \times A$ gode di tutte le proprietà in **P** e $R \subseteq T$ allora $S \subseteq T$.

Chiusure per $R \subseteq A \times A$:

Riflessiva: $R \cup I_A$;

Simmetrica: $R \cup R^{-1}$;

Transitiva: $\bigcup_{n>0} R^n$;

Riflessiva, simmetrica: $R \cup I_A \cup R^{-1}$;

Riflessiva, transitiva: $\bigcup_{n \geqslant 0} R^n$;

Equivalenza (riflessiva, simmetrica, transitiva): $\bigcup_{n>0} (R \cup I_A \cup R^{-1})^n$.

Data una relazione di equivalenza R, si dice classe di equivalenza $[a]_R \coloneqq \{x \in A \mid (a, x) \in R\}$.

Dato un insieme A ed un insieme non vuoto di indici I, si dice partizione di A una famiglia $\mathcal{B} \coloneqq \{B_i \mid i \in I\}$ tale che:

- $\forall\, i \in I, B_i \neq \varnothing$,
- $A = \bigcup_{i \in I} B_i$ (cioè $\mathcal{B}$ forma un ricoprimento di A),
- $B_i \cap B_j \neq \varnothing \implies B_i = B_j$.

Sia R una relazione di equivalenza su A, la partizione indotta da R su A si chiama insieme quoziente di A rispetto a R, dunque $A/R \coloneqq \{[a]_R \mid a \in A\}$.

Relazioni d'ordine

Una relazione R su A che goda delle proprietà riflessiva, antisimmetrica e transitiva si dice relazione d'ordine su A. Si indica con $(A, \leqslant)$. Se $\forall\, a, b \in A$, $(a, b) \in R$, ovvero tutti gli elementi sono confrontabili, la relazione d'ordine è totale. In caso contrario viene detta parziale. Se $\forall\, a \in A$, $(a, a) \notin R$, ovvero la relazione è antiriflessiva, la relazione si dice d'ordine stretto e si indica con $(A, <)$.

Minimali e massimali

Sia $(A, \leqslant)$ un insieme parzialmente ordinato e sia $m \in A$:

- se $\forall\, a \in A$, $m \leqslant a$, m si dice minimo di A;
- se $\forall\, a \in A$, $a \leqslant m \implies a = m$, m si dice minimale di A;
- se $\forall\, a \in A$, $a \leqslant m$, m si dice massimo di A;
- se $\forall\, a \in A$, $m \leqslant a \implies a = m$, m si dice massimale di A.

Dato un insieme parzialmente ordinato:

- se presenta un minimo/massimo, esso è unico;
- se l'insieme è finito e presenta un unico minimale/massimale, esso è il minimo/massimo.

Maggiornati e minoranti

Sia $(A, \leqslant)$ un insieme parzialmente ordinato, $B \subseteq A$ e $m \in A$:

- se $\forall\, b \in B$, $m \leqslant b$, m si dice minorante di B;
- il massimo rispetto a $\leqslant$ dei minoranti di B si dice estremo inferiore di B;
- se $\forall\, b \in B$, $b \leqslant m$, m si dice maggiornate di B;
- il minimo rispetto a $\leqslant$ dei maggiornati di B si dice estremo superiore di B.

Funzioni

Data una relazione $R \subseteq A \times B$, essa si dice:

- ovunque definita se è seriale rispetto all'insieme A;
- funzionale se per ogni $a \in A$ esiste al più un $b \in B$ con cui è in relazione.

Se una relazione è ovunque definita e funzionale prende il nome di funzione e si indica con $f : A \to B$. L'insieme A prende il nome di insieme delle immagini e B di insieme delle controimmagini.

Una funzione $f : A \to B$ è detta iniettiva se $\forall\, a_1, a_2 \in A$, $f(a_1) = f(a_2) \implies a_1 = a_2$. Si dice suriettiva una funzione tale che $f(A) = B$. Se una funzione è sia iniettiva che suriettiva si dice biiettiva o biunivoca.

Date due funzioni $f : A \to B$ e $g : B \to C$:

- se f e g sono iniettive, allora anche $f \cdot g$ lo è;
- se $f \cdot g$ è iniettiva, allora anche f lo è;
- se f e g sono suriettive, allora anche $f \cdot g$ lo è;
- se $f \cdot g$ è suriettiva, allora anche g lo è;
- se f e g sono biiettive, allora anche $f \cdot g$ lo è;
- se $f \cdot g$ è biiettiva, allora f è iniettiva e g è suriettiva.

Nota: $f \cdot g = g \circ f$.

Data una funzione $f : A \to B$, si dice funzione inversa la funzione $g : B \to A$ tale che $f \cdot g = I_A$ e $g \cdot f = I_B$. Nel caso sia ammessa solo un'identità, prende il nome di inversa destra o sinistra, rispettivamente.

Condizione necessaria e sufficiente affinché una funzione ammetta inversa destra è che sia iniettiva. Per quella sinistra, è necessario sia suriettiva. Nel caso sia biiettiva, ammette una ed una sola inversa.

Si dice nucleo o kernel di una funzione la relazione $\ker_f \subseteq A \times A$ tale che $\forall\, (a_1, a_2) \in \ker_f$, $f(a_1) = f(a_2)$.

Logica proposizionale

Alfabeto ε:

- lettere enunciative, indicate con lettere latine maiuscole;
- connettivi logici, composti da $\neg$, $\wedge$, $\vee$, $\implies$, $\iff$, in questo ordine di precedenza, a partire dal più importante;
- parentesi tonde.

Gli operatori associano a sinistra.
Si dice formula ben formata un formula $\varphi ::= A \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \implies \varphi \mid \varphi \iff \varphi$.
L'insieme $S(\varphi)$ delle sottoformule di φ è definito come:

- se $\varphi = A$, $S(\varphi) = \{\varphi\}$;
- se $\varphi = \neg\psi$, $S(\varphi) = \{\varphi\} \cup S(\psi)$;
- se $\varphi = \psi \circ \vartheta$, $S(\varphi) = \varphi \cup S(\psi) \cup S(\vartheta)$.

Si dice interpretazione la funzione $i : \varepsilon \to \{0, 1\}$ che agisce sulle singole lettere. Estendendo il concetto alle f.b.f. prende il nome di valutazione ed è definita come:

- $v(A) = i(A)$;
- $v(\neg\varphi) = 1 - v(\varphi)$;
- $v(\varphi \wedge \psi) = \min\{v(\varphi), v(\psi)\}$;
- $v(\varphi \vee \psi) = \max\{v(\varphi), v(\psi)\}$;
- $v(\varphi \implies \psi) = \max\{1 - v(\varphi), v(\psi)\}$;
- $v(\varphi \iff \psi) = 1 - |v(\varphi) - v(\psi)|$.

Se φ è una f.b.f. diciamo che una valutazione v è un suo modello se $v(\varphi) = 1$. Dunque:

- se esiste almeno un modello per φ, questa è detta soddisfacibile;
- se ogni valutazione è modello per φ, questa è detta tautologia e si indica con $\models \varphi$;
- se nessuna valutazione è modello per φ, questa è detta contraddizione od insoddisfacibile.

Sia Γ un insieme di f.b.f., allora:

- un modello per Γ è modello $\forall\varphi \in \Gamma$;
- se Γ ammette un modello è detta soddisfacibile;
- se Γ non ammette modelli è detta insoddisfacibile.

Se ogni modello di Γ è modello di φ questa è detta conseguenza semantica di Γ e si scrive $\Gamma \models \varphi$. In caso contrario si scrive $\Gamma \not\models \varphi$.
Date $\varphi, \psi \in \Gamma$, $\Gamma \cup \psi \models \varphi$ sse $\Gamma \models \psi \implies \varphi$. Dunque, $\psi \models \varphi$ sse $\models \psi \implies \varphi$ e $\Gamma \models \varphi$ sse $\Gamma \cup \{\neg\varphi\}$ è insoddisfacibile.
Due f.b.f con modelli equivalenti si dicono semanticamente equivalenti.
Leggi (ad eccezione delle defizioni di implicazione doppia e singola, è sempre possibile sostituire $\wedge$ e $\vee$):

Formula	Nome
$A \equiv \neg\neg A$	Doppia negazione
$A \wedge B \equiv B \wedge A$	Commutatività
$A \wedge A \equiv A$	Idempotenza
$(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$	Associatività
$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$	Distributività
$A \wedge (A \vee B) \equiv A$	Assorbimento
$\neg(A \wedge B) \equiv \neg A \vee \neg B$	De Morgan
$A \implies B \equiv \neg B \implies \neg A$	Contrapposizione
$A \implies B \equiv \neg A \vee B$	Implicazione
$A \iff B \equiv (A \implies B) \wedge (B \implies A)$	Doppia implicazione
$(\neg A \wedge A) \vee B \equiv B$	Non contraddizione

Teoria $\mathcal{L}$

Tutte le f.b.f. contengono unicamente i connettivi $\neg$ e $\implies$.

Assiomi:

1. $A \implies (B \implies A)$;
2. $(A \implies (B \implies C)) \implies ((A \implies B) \implies (A \implies C))$;
3. $(\neg A \implies \neg B) \implies ((\neg A \implies B) \implies A)$.

Modus ponens: da A e $A \implies B$ deduco B.

Teorema di correttezza e completezza: siano φ, $\psi \in \Gamma$ due f.b.f., allora

Correttezza se $\Gamma \vdash_{\mathcal{L}} \varphi$, allora $\Gamma \models \varphi$;

Completezza se $\Gamma \models \varphi$, allora $\Gamma \vdash_{\mathcal{L}} \varphi$.

Teorema di deduzione sintattica: siano φ, $\psi \in \Gamma$ due f.b.f., allora $\Gamma \cup \psi \vdash_{\mathcal{L}} \varphi$ sse $\Gamma \vdash_{\mathcal{L}} \psi \implies \varphi$.

Calcolo per risoluzione

Si basa su f.b.f. in forma normale congiuntiva. Ogni disgiunzione finita di letterali è detta clausola, dunque una formula è una congiunzione di clausole.

Regola di risoluzione: date le clausole C_1 e C_2 ed un letterale A, la regola di risoluzione si scrive come

$$\frac{C_1 \cup \{A\} \quad C_2 \cup \{\neg A\}}{C_1 \cup C_2}.$$

Teorema di correttezza e completezza per refutazione:

Correttezza se $\Gamma^C \vdash_{\mathcal{R}} \square$, allora Γ è insoddisfacibile;

Completezza se Γ è insoddisfacibile, allora $\Gamma^C \vdash_{\mathcal{R}} \square$.

L'insieme delle clausole deducibili è definito come $\mathrm{Ris}\left(\Gamma^C\right) = \Gamma^C \cup \{C_{i,j} \mid C_{i,j} \text{ è la risolvente di } C_i \text{ e } C_j\}$.

Algoritmo di risoluzione:

1. $\Gamma \models \varphi$ sse $\Gamma \cup \{\neg \varphi\}$ è insoddisfacibile;
2. Γ è insoddisfacibile sse $\Gamma^C \cup (\neg \varphi)^C \vdash_{\mathcal{R}} \square$;
3. sia $\Delta = \Gamma^C \cup (\neg \varphi)^C$, ripetere
   (a) $\Delta' = \Delta$;
   (b) $\Delta = \mathrm{Ris}(\Delta)$;

   finché $\square \notin \Delta$ o $\Delta \neq \Delta'$;
4. se $\square \in \Delta$ allora $\Gamma \models \varphi$, altrimenti $\Gamma \not\models \varphi$.

Logica del primo ordine

Alfabeto:

- costanti, indicate con le prime lettere latine minuscole;
- variabili, indicate con le ultime lettere latine minuscole;
- lettere funzionali, indicate con le lettere latine intermedie minuscole;
- lettere predicative, indicate con le prime lettere latine maiuscole;
- connettivi logici, equivalenti a quelli proposizionali;
- quantificatori universale ed esistenziale;
- parentesi tonde.

Si dice segnatura un qualunque insieme S di costanti, lettere funzionali e predicative. Si dice termine su S una sequenza di costanti, variabili, lettere funzionali e parentesi, dove:

- ogni costante o variabile è un termine;

- ogni lettera funzionale con i relativi parametri è un termine.

Una formula atomica è una formula composta da una lettera predicativa, avente termini come parametri. Definizione di f.b.f.: $\varphi ::= A \mid \neg\varphi \mid \forall x\,\varphi \mid \exists x\,\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \implies \varphi \mid \varphi \iff \varphi$. Per l'insieme delle sottoformule, valgono le stesse regole della logica proposizionale, dove $\varphi = Q\,x\,\psi$ diventa $S(\varphi) = \{\varphi\} \cup S(\psi)$. Una variabile si dice legata se è quantificata, si dice libera altrimenti. Se in una formula non esistono variabili libere, questa viene detta chiusa; in caso contrario è detta aperta. Una formula chiusa è detta chiusura universale od esistenziale se presenta in testa solo quantificatori del rispettivo tipo. Si dice termine libero per una variabile un termine tale che detta variabile non sia libera quando un'altra variabile del termine è legata.

Strutture interpretative

Data una segnatura S, si dice struttura interpretativa la coppia $\langle D; I\rangle$ dove

- D è un insieme non vuoto detto dominio;
- I è una funzione di interpretazione, formata da tre funzioni I_1, I_2 e I_3, dove
  - I_1 associa alle costanti in S valori in D;
  - I_2 associa alle lettere funzionali in S operazioni in D;
  - I_3 associa alle lettere predicative in S relazioni in D.

Si dice assegnamento la funzione $s : VAR \to D$. Questa può essere estesa ai termini, diventando $s^* : TER(S) \to D$.

Una f.b.f. si dice soddisfacibile (in una struttura) se ammette un modello, logicamente valida (vera, in una struttura) se ogni interpretazione è modello e logicamente contraddittoria/insoddisfacibile (falsa, in una struttura) se non ammette modelli.

Una formula chiusa può essere solo o vera o falsa, mai soddisfacibile ma non vera. La chiusura universale di una f.b.f. è vera sse la formula è vera nella struttura interpretativa. La chiusura esistenziale è vera sse la formula è soddisfacibile.

Forma di normale prenessa e di Skolem

Una formula si dice in forma normale prenessa se presenta tutti i quantificatori in testa alla formula. Regole di normalizzazione:

1. $\neg\forall x\,\psi \equiv \exists x\,\neg\psi$;
2. $\forall x\,\psi \wedge \vartheta \equiv \forall y\,(\psi[y/x] \wedge \vartheta)$;
3. $\forall x\,\psi \implies \vartheta \equiv \exists y\,(\psi[y/x] \implies \vartheta)$;
4. $\vartheta \implies \forall x\,\psi \equiv \forall y\,(\vartheta \implies \psi[y/x])$.

È sempre possibile invertire $\forall/\exists$ e $\wedge/\vee$ in queste regole.

Una formula si dice in forma di Skolem se è prenessa e presenta solo quantificatori universali. Skolemizzazione:

1. si porta la formula in forma prenessa;
2. si elimina ogni esistenziale in testa, sostituendo le varibili con delle costanti;
3. si elimina ogni esistenziale successivo agli universali, sostituendo le varibili con lettere funzionali di arità pari al numero di universali che precedono, con le relative variabili come parametri.

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

Data una formula in forma di Skolem, è possibile risolverla mediante metodi equivalenti a quelli della logica proposizionale, applicando opportune sostituzioni di variabili.

Teoria $\mathcal{K}$

Equivalente alla teoria $\mathcal{L}$, con l'aggiunta di $\forall$.

Assiomi aggiuntivi:

1. $\forall x\,A \implies A\,[t/x]$;
2. $\forall x\,(A \implies B) \implies (A \implies \forall x\,B)$.

Oltre al modus ponens, esiste la generalizzazione: A diventa $\forall x\,A$.

Strutture algebriche

Semigruppo Una struttura algebrica nella forma $(A, +)$, dove $+$ è un'operazione associativa sull'insieme A;

Semigruppo commutativo Un semigruppo con l'aggiunta della proprietà commutativa;

Monoide Un semigruppo con l'aggiunta di un'elemento neutro (scrittura: $(A, +, u)$);

Gruppo Un monoide che presenta l'inverso per ogni elemento dell'insieme;

Gruppo abeliano Un gruppo che presenta la proprietà commutativa;

Anello Una struttura nella forma $(A, +, *, u)$, dove

- $(A, +, u)$ forma un gruppo abeliano;
- $(A, *)$ forma un semigruppo;
- $*$ è distributiva rispetto a $+$;

Anello con unità Un anello con un monoide al posto del semigruppo;

Anello commutativo Un anello dove il semigruppo è commutativo;

Corpo Un anello dove $(A\backslash\{u\}, *)$ forma un gruppo;

Campo Un corpo dove $(A\backslash\{u\}, *)$ forma un gruppo abeliano.

Note:

- in un gruppo, l'inverso di un elemento è sempre unico;
- in un gruppo, vale la legge di cancellazione, ovvero $a + b = b + c \equiv b = c$;
- in un anello, $a * u = u * a = u$;
- in un anello, $a * b = a * c \equiv b = c$ dove $a \neq u$.

Sottostrutture e morfismi

Criteri sottostrutture:

- per i sottogruppi, controllare se $a - b$ appartiene;
- per i sottoanelli, controllare se $a - b$ e $a * b$ appartengono.

Per controllare se è presente un omomorfismo, dati $(A, +, u)$, $(\hat{A}, \hat{+}, \hat{u})$ e $f : A \to \hat{A}$, controllare se $f(a+b) = f(a)\hat{+}f(b)$ e $f(u) = \hat{u}$.

SPASS

Esempio:

```
list_of_symbols.
    functions[(f, 0), (g, 1)].
    predicates[(A, 0), (B, 1)].
end_of_list.

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

list_of_formulae(conjectures).
    formula(...).
end_of_list.
```

Funzioni standard:

`lnot(fbf)` not logico;

`and(fbf, fbf [, fbf...])` and logico;

`or(fbf, fbf [, fbf...])` or logico;

`implies(fbf, fbf)` implicazione;

`equiv(fbf, fbf)` doppia implicazione;

`equal(fbf, fbf)` uguaglianza;

`forall([var [, var...]], fbf)` per ogni;

`exists([var [, var...]], fbf)` esiste;.