Logica

UniVR - Dipartimento di Informatica

Fabio Irimie

1° Semestre 2023/2024

Indice

1 Ripasso di matematica

1.1 Relazioni

Prendendo in considerazione 2 insiemi A, B e una relazione $f \subseteq A \times B$ si definisce **dominio** l'insieme A e **codominio** l'insieme B. Il prodotto cartesiano è definito nel seguente modo:

$$A \times B = \{(a, b)|a \in A, b \in B\}$$

Ciò significa che si prende in considerazione una coppia ordinata di elementi formata da un elemento di A e uno di B. La relazione f è una funzione sse (se e solo se) $\forall a \in A \; \exists$ unico $b \in B$ si dice che: $(a, b) \in f$, oppure $f(a) = b$.

1.2 Sottoinsieme delle parti

Dato un insieme A si definisce **sottoinsieme delle parti** (scritto $\mathcal{P}(A)$ o 2^A) l'insieme di tutti i sottoinsiemi di A, cioè $2^A = x|x \subseteq A$.

Un esempio è il seguente:

$$A = \{3, 5\}$$

$$2^A = \{\emptyset, \{3\}, \{5\}, \{3, 5\}\}$$

$\emptyset$ è l'insieme vuoto, cioè l'insieme che non contiene nessun elemento.

2 Introduzione

La logica ha lo scopo di formalizzare il ragionamento matematico che è caratterizzato dal concetto di dimostrazione senza ambiguità

3 Sintassi della logica proposizionale

La logica proposizionale è formata da simboli formali ben definiti e sono divisi in:

3.1 Connettivi

- $\vee$ Congiunzione, And logico
- $\wedge$ Disgiunzione, Or logico
- $\neg$ Negazione, Not logico (non connette niente, è solo una costante logica che equivale a 0 nella logica booleana)
- $\perp$ Falso, Bottom, Assurdo
- $\rightarrow$ Implicazione, If-then

3.2 Ausiliari

- () Le parentesi non fanno parte della proposizione, ma servono solo a costruire il linguaggio

3.3 Simboli proposizionali

- $p_n, q_n, \psi_n, \ldots$ Le lettere minuscole indicizzate vengono usate per indicare una proposizione (sono infiniti simboli numerabili)

3.4 Altri simboli

- $|$ Tale che

- $\leftrightarrow$ Se e solo se

> ***Definizioni utili 3.1***
>
> 1. ***Stringa:*** *Una sequenza finita di simboli o caratteri*
>
> 2. ***Infinito numerabile:*** *Un insieme è infinito numerabile se è il più piccolo infinito possibile, cioè se è in corrispondenza biunivoca con l'insieme* $\mathbb{N}$

4 Principio di induzione

Il principio di induzione è un principio logico che permette di dimostrare che una proprietà è vera per tutti gli elementi di un insieme infinito numerabile.

Una prima definizione induttiva fatta in modo non formale, ma con frasi in italiano è la seguente:

L'insieme di proposizioni $PROP$ è così definito *induttivamente*:

1. $\perp \to PROP$

2. se p è un simbolo proposizionale allora $p \in PROP$

3. **(Caso induttivo)** se $\alpha, \beta \in PROP$ allora $(\alpha \wedge \beta) \in PROP, (\alpha \vee \beta) \in PROP, (\alpha \to \beta) \in PROP, (\neg\alpha) \in PROP$

4. nient'altro appartiene a $PROP$

In questo modo è stato creato l'insieme $PROP$ che contiene tutte le proposizioni che possono essere create usando gli unici simboli che abbiamo definito $(\wedge, \vee, \to, \neg)$.

Esempi di proposizioni corrette e scorrette:

- $(p_7 \to p_0) \in PROP$

- $p_7 \to p_0 \notin PROP$ (mancano le parentesi)
- $((\bot \vee p_{32}) \wedge (\neg p_2)) \in PROP$
- $((\to \wedge \notin PROP$
- $\neg\neg\bot \notin PROP$

4.1 Definizione induttiva formale dell'insieme $PROP$

Adesso l'insieme $PROP$ viene definito in modo formale usando i simboli proposizionali.

Definizione 4.1
L'insieme $PROP$ è il più piccolo insieme X di stringhe tale che:

1. $\bot \in X$
2. $p \in X$ *(Perchè è un simbolo proposizionale)*
3. *se* $\alpha, \beta \in X$ *allora* $(\alpha \to \beta) \in X, (\alpha \vee \beta) \in X, (\alpha \wedge \beta) \in X, (\neg\alpha) \in X$

$p, \alpha, \beta, \ldots$ *sono elementi proposizionali generici*

$AT =$ simboli proposizionali $+ \bot$ è l'insieme di tutte le proposizioni atomiche, cioè quelle che non contengono connettivi, sono quindi la più piccola parte non ulteriormente scomponibile

5 Proprietà su un insieme

Definito P un insieme di proprietà assunte da un insieme A si ha che:

- $P \subseteq A$
- $a \in A$ dove a è un elemento generico dell'insieme A

Si dice che a gode della proprietà P se $a \in P$.

Altri modi per dire che a gode della proprietà P sono:

- $P(a)$
- $P[a]$ (per non creare confusione con le parentesi tonde che sono usate come simboli ausiliari per costruire il linguaggio)

$P \subseteq PROP \qquad \forall\alpha \in PROP \,.\, P(\alpha)$
(il punto mette in evidenza ciè che viene dopo di esso e può anche essere omesso)

Esempio 5.1
Esempio di una proprietà sull'insieme $\mathbb{N}$*:*

$P = \{n | n \in \mathbb{N}$ *ed è pari* $\}$ *essendo* n *un numero generico indica la proprietà di essere pari.*

$P[5]\ \times$
$P[4]\ \surd$

5.1 Principio di induzione sui numeri naturali $\mathbb{N}$

$P \subseteq \mathbb{N}$

1. **Caso base**: se $P[0]$ e
2. **Passo induttivo**: se $\forall n \in \mathbb{N}(P[n] \Rightarrow P[n+1])$ allora $\forall n \in \mathbb{N}\ .\ P[n]$

Se si dimostra la proprietà per n e per il successivo $(n+1)$, allora si dimostra che la proprietà è vera per tutti i numeri naturali. Si sfrutta il fatto che esiste un minimo a cui prima o poi si arriva.

Esercizio 5.1
Dimostra per induzione che:

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

6 Teorema del principio di induzione su $PROP$

Definizione 6.1
$P \subseteq PROP$

1. *Se* $P[\alpha], \alpha \in AT$ *e*
2. *Se* $P[\alpha] \Rightarrow P[(\neg\alpha)]$ *e*
3. *se* $P[\alpha]$ *e* $P[\beta] \Rightarrow P[(\alpha \wedge \beta)], P[(\alpha \vee \beta)P[(\alpha \rightarrow \beta)]$
   allora $\forall\psi \in PROP\ .\ P[\psi]$

Con questo teorema si possono dimostrare intere proposizioni complesse dimostrando i pezzi più piccoli (***sottoformule***) come mostrato nella figura 1.

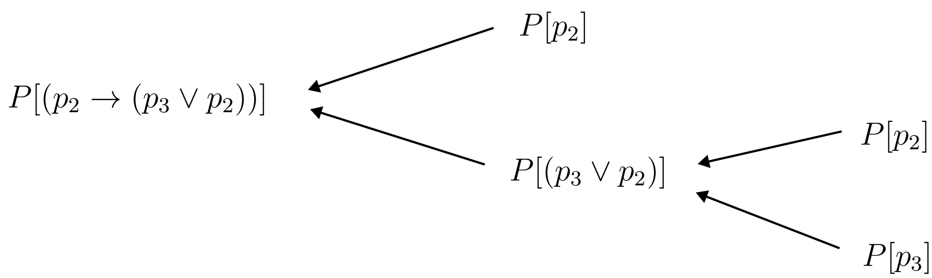

Figura 1: Dimostrazione di una formula complessa

Esercizio 6.1
Dimostra che ogni $\psi \in PROP$ *ha un numero pari di parentesi usando il principio di induzione per dimostrare proprietà sintattiche sulla struttura delle formule.*

$P[\psi] \equiv \psi$ *ha un numero pari di parentesi*

1. ***Caso base*** $\psi \in AT$ *quindi* ψ *ha 0 parentesi e quindi è pari:* $P[\psi]$ $\surd$
2. ***Ipotesi induttiva*** $\alpha, \beta \in PROP$, $P[\alpha], P[\beta]$? $P[(\alpha \to \beta)]$ *(per* α *vale e per* β *vale, si sono aggiunte due parentesi, quindi la formula è ancora pari)*
3. ***Passo induttivo*** $P[\alpha], P[\beta] \Rightarrow P[(\alpha \to \beta)], P[(\alpha \vee \beta)], P[(\alpha \wedge \beta)]$ *allora* $\forall \psi \in PROP \ . \ P[\psi]$

7 Definizione ricorsiva di funzioni su PROP

Definizione 7.1
Riprendendo l'esercizio 6.1 si definisce la funzione π *che associa ad ogni formula proposizionale (equivalente di un input nell'informatica) un numero naturale (equivalente di un output nell'informatica). La funzione* π *quindi dopo aver dato in input un argomento (qualsiasi formula proposizionale atomica o complessa) restituisce in output il numero di parentesi che contiene la formula in input.*

$$\pi : PROP \to \mathbb{N}$$

1. ***Caso base*** $\pi[\alpha] = 0$ *se* $\alpha \in AT$
2. ***Ipotesi induttiva*** $\pi[(\neg\alpha)] = \pi[\alpha] + 2$ *In questo passaggio viene chiamata la funzione* π *dentro la funzione* π *stessa, quindi è una defini-*

zione ricorsiva. In questo caso si aggiungono 2 parentesi al numero di parentesi di α $\pi[\alpha]$

3. ***Passo induttivo*** $\pi[(\alpha \to \beta)] = \pi[(\alpha \vee \beta)] = \pi[(\alpha \wedge \beta)] = \pi[\alpha] + \pi[\beta] + 2$ *dove* $\pi[\alpha]$ *e* $\pi[\beta]$ *sono il numero di parentesi di* α *e* β *e si aggiungono 2 parentesi per il connettivo.*

Di seguito ci sono 2 esempi in cui viene messa in pratica la funzione π definita sopra in modo da capire meglio come funziona.

Esempio 7.1

$$\pi[(p_2 \to p_1)] \overset{caso\ 3}{=} \pi[p_2] + \pi[p_1] + 2 \overset{caso\ 1}{=} 0 + 0 + 2 = 2$$

Esempio 7.2

$$\pi[(p_1 \vee (p_2 \vee p_1))] = (\pi[p_2] + \pi[p_1] + 2) + \pi[p_1] + 2 = (0 + 0 + 2) + 0 + 2 = 4$$

Tutte le funzioni definite ricorsivamente sono funzioni, e non tutte le funzioni possono essere definite ricorsivamente.

7.1 Definizione più precisa dell'esercizio 6.1

Ogni $\alpha \in PROP$ ha un numero pari di parentesi: $\forall \alpha \in PROP\ P[\alpha] \overset{sse}{\Leftrightarrow} \pi[\alpha]$ è pari

1. $P[\alpha]$ $\alpha \in AT$

   se $\alpha \in AT$ $\pi[\alpha] \overset{def}{=} 0$ quindi $\surd$

2. Suppongo che valga $P[\alpha],\ P[(\neg\alpha)]$?

   $P[\alpha] \Leftrightarrow \pi[\alpha] pari$ è pari perchè lo abbiamo supposto prima (consideriamo 0 come pari)

   $\pi[(\neg\alpha)] = \pi[\alpha] + 2$ è pari quindi $P[(\neg\alpha)]$ $\surd$

   Si può definire un simbolo nuovo che non vuole dire niente nel linguaggio proposizionale e gli si assegnano i connettivi possibili per non doverli più scrivere ogni volta. Per questo esercizio prendiamo in considerazione

   $$\circ \in \{\to, \vee, \wedge\}$$

3. $(\alpha \circ \beta)$

   suppongo $P[\alpha], P[\beta]$

   allora $\pi[\alpha]$ e $\pi[\beta]$ sono pari

   quindi $\pi[(\alpha \circ \beta)] = \pi[\alpha] + \pi[\beta] + 2$ (è pari)

Ho dimostrato per induzione che $\forall \psi \in PROP\ P[\psi]$ $\square$
($\square$ è un simbolo che indica la fine della dimostrazione.)

8 Dimostrazione ricorsiva di rango e sottoformula

Il rango di una formula è il numero di connettivi che contiene.

Definizione 8.1
Considerato r il rango di una proposizione
$r : PROP \to \mathbb{N}$

1. $r[\psi] = 0$ *se* $\psi \in AT$
2. $r[(\neg\psi)] = 1 + r[\psi]$
3. $r[(\psi \circ \gamma)] = 1 + max(r[\psi], r[\gamma]) \qquad \circ \in \{\vee, \wedge, \to\}$

La sottoformula è una formula che è contenuta in un'altra formula più grande.

Definizione 8.2
Considerata sub la sottoformula di una proposizione
$sub : PROP \to 2^{PROP}$

1. $sub[\alpha]\ \alpha = ((p_2 \vee p_1) \vee p_0)$
2. $sub[\alpha] = \{\alpha, p_2, p_0, (p_2 \vee p_1)\}$

8.1 Applicazione della definizione di sottoformula

1. $sub[\psi] = \{\psi\}$ se $\psi \in AT$
2. $sub[(\neg\psi)] = \{(\neg\psi)\} \cup sub[\psi]$
3. $sub[(\psi \to \gamma)] = \{(\psi \circ \gamma)\} \cup sub[\psi] \cup sub[\gamma]$

Teorema 1 *Vogliamo dimostrare per induzione su* β *:*
Se $\alpha \in sub[\beta]$ *e* $\alpha \neq \beta$ *(dove* α *è una sottoformula propria, cioè vengono considerate tutte le sottoformule di* β *tranne* β *stessa) allora* $r[\alpha] < r[\beta]$

1. ***Caso base*** $\beta \in AT$
   β *non ha sottoformule proprie, quindi* α *non può essere una sottoformula propria di* β*. Essendo falsa la premessa la tesi è vera.*
2. *Se* $\beta = (\neg\beta_1)$ *: se* $\alpha \in sub[\beta]$ *e* $\alpha \neq \beta$ *allora* $\alpha \in sub[\beta_1]$ *e si dimostra* $r[\alpha] \leq r[\beta_1]$ ***(ipotesi induttiva)***

(a) $\alpha \in sub[\beta_1]$ *e* $\alpha \neq \beta_1$ *per ipotesi induttiva* $r[\alpha] < r[\beta_1]$

(b) $\alpha = \beta_1$ $r[\alpha] = r[\beta_1]$
$r[\alpha] \leq r[\beta_1]$

Quindi

$$r[(\neg \overset{\beta}{\beta_1})] \overset{def\ r}{=} 1 + r[\beta_1] \geq 1 + r[\alpha] > r[\alpha]$$

Quindi

$$r[\alpha] < r[\beta]$$

3. ***Caso induttivo***
$\beta = (\beta_1 \to \beta_2)$ *se* α *è sottoformula di* β *e* $\alpha \neq \beta$ *allora* $\alpha \in sub[\beta_1]$ *o* $\alpha \in sub[\beta_2]$

(a) *se* $\alpha \in sub[\beta_1]$ *(ipotesi induttiva)*

   i. *Se* $\alpha \neq \beta_1 \Rightarrow r[\alpha] \overset{ii\ su\ \beta_1}{\leq} r[\beta_1]$

   ii. *Se* $\alpha = \beta_1 \Rightarrow r[\alpha] = r[\beta_1]$

   Da 3(a)i e 3(a)ii si ricava $r[\alpha] \leq r[\beta_1]$

(b) *se* $\alpha \in sub[\beta_2]$

   i. *Se* $\alpha \neq \beta_2 \Rightarrow r[\alpha] \overset{ii\ su\ \beta_2}{\leq} r[\beta_2]$

   ii. *Se* $\alpha = \beta_2 \Rightarrow r[\alpha] = r[\beta_2]$

   Da 3(b)i e 3(b)ii si ricava $r[\alpha] \leq r[\beta_2]$

$$r[(\beta_1 \overset{\beta}{\to} \beta_2)] = 1 + max\{r\overset{\geq\alpha}{[\beta_1]}, r\overset{\geq\alpha}{[\beta_2]}\} \geq 1 + max\{r[\alpha], r[\alpha]\} \geq 1 + r[\alpha] > r[\alpha]$$