

Metodi matematici per l'informatica

Nicola Calvio

February 11, 2024

TEORIA

1 Introduzione

Appunti del corso di Metodi matematici per l'informatica, tenuto dal prof. Cenciarelli presso l'università Sapienza di Roma.

2 Insiemi

La teoria degli insiemi è una branca della matematica che studia le collezioni di oggetti, denominate insiemi, e le operazioni che possono essere effettuate su di essi.

2.1 Definizioni Base

Un **insieme** è una collezione di oggetti distinti, chiamati elementi dell'insieme. Gli insiemi vengono di solito denotati con lettere maiuscole, mentre gli elementi con lettere minuscole.

- Un insieme può essere definito elencando i suoi elementi tra parentesi graffe: $A = \{a, b, c\}$.
- La notazione $a \in A$ significa che a è un elemento dell'insieme A .
- La notazione $b \notin A$ significa che b non è un elemento dell'insieme A .

2.2 Operazioni sugli Insiemi

Le principali operazioni sugli insiemi includono l'unione, l'intersezione e la differenza di insiemi.

- **Unione:** L'unione di due insiemi A e B , denotata con $A \cup B$, è l'insieme degli elementi che appartengono ad A o a B (o ad entrambi).
- **Intersezione:** L'intersezione di due insiemi A e B , denotata con $A \cap B$, è l'insieme degli elementi che appartengono sia ad A che a B .
- **Differenza:** La differenza di due insiemi A e B , denotata con $A - B$ o $A \setminus B$, è l'insieme degli elementi che appartengono ad A e non a B .

2.3 Sottoinsiemi

Un insieme A si dice **sottoinsieme** di un insieme B , denotato con $A \subseteq B$, se ogni elemento di A è anche un elemento di B . Se A è un sottoinsieme di B ma A non è uguale a B , allora A si dice **sottoinsieme proprio** di B , denotato con $A \subset B$.

2.4 Insiemi Speciali

Alcuni insiemi hanno un'importanza particolare nella matematica:

- L'**insieme vuoto**, denotato con \emptyset , è l'insieme che non contiene elementi.
- Gli insiemi di numeri come gli **insiemi dei numeri naturali** \mathbb{N} , **interi** \mathbb{Z} , **razionali** \mathbb{Q} , **reali** \mathbb{R} , e **complessi** \mathbb{C} .

2.5 Proprietà degli Insiemi

Gli insiemi e le operazioni su di essi soddisfano diverse proprietà matematiche, come la commutatività, l'associatività, e le leggi distributive.

3 Coppie Ordinate

Una coppia ordinata è una collezione di due elementi in cui l'ordine degli elementi ha importanza. Le coppie ordinate sono comunemente utilizzate per definire concetti matematici come funzioni, relazioni e prodotti cartesiani.

3.1 Definizione

Una coppia ordinata (a, b) è composta da due elementi dove a è il primo elemento e b è il secondo elemento. L'ordine degli elementi è significativo, il che significa che $(a, b) \neq (b, a)$ a meno che $a = b$.

3.2 Notazione e Proprietà

La notazione per una coppia ordinata è la seguente:

- (a, b) indica una coppia ordinata dove a è il primo membro e b è il secondo membro.

Le proprietà principali delle coppie ordinate includono:

- **Unicità:** Due coppie ordinate (a, b) e (c, d) sono uguali se e solo se $a = c$ e $b = d$.
- **Ordine:** L'ordine degli elementi è cruciale. $(a, b) \neq (b, a)$ a meno che $a = b$.

3.3 Prodotto Cartesiano

Il prodotto cartesiano di due insiemi A e B , denotato con $A \times B$, è l'insieme di tutte le possibili coppie ordinate (a, b) dove $a \in A$ e $b \in B$.

3.3.1 Esempio

Dati gli insiemi $A = \{1, 2\}$ e $B = \{x, y\}$, il prodotto cartesiano $A \times B$ è:

$$A \times B = \{(1, x), (1, y), (2, x), (2, y)\}$$

3.4 Applicazioni delle Coppie Ordinate

Le coppie ordinate sono utilizzate in vari ambiti della matematica e delle sue applicazioni, inclusi:

- Definizione di funzioni come collezioni di coppie ordinate.
- Rappresentazione di punti nel piano cartesiano.
- Costruzione di relazioni tra elementi di due insiemi.

4 Relazioni

Le relazioni sono sottoinsiemi di prodotti cartesiani, ad esempio $R \subseteq A \times B$, dove A e B sono insiemi. Ci sono varie tipologie di relazioni (o arità), come relazioni binarie, ternarie, unarie, e nullarie.

4.1 Principi per Relazioni Binarie

Le seguenti sono proprietà comuni delle relazioni binarie su un insieme A :

4.2 Principi

- **Principio di simmetria:** se un certo x è in relazione con y allora y è in relazione con x una relazione si dice simmetrica quando per ogni $(a, b) \in R$ allora $(b, a) \in R$ oppure usando una notazione infissa possiamo scrivere se aRb allora bRa
- **Principio di riflessività:** una relazione binaria su un insieme A si dice riflessiva quando ogni elemento è in relazione con se stesso ossia per ogni $a \in A$ la coppia (a, a) è in relazione
- **Principio di transitività:** una relazione binaria su un insieme A si dice transitiva quando per ogni $a, b, c \in A$ se $(a, b) \in R$ e $(b, c) \in R$ allora $(a, c) \in R$
- **Principio di antisimmetria:** una relazione binaria su un insieme A si dice antisimmetrica quando per ogni $a, b \in A$ se $(a, b) \in R$ e $(b, a) \in R$ allora $a = b$
- **Principio di antitransitività:** una relazione binaria su un insieme A si dice antitransitiva quando per ogni $a, b, c \in A$ se aRb e bRc allora non deve essere aRc
- **Principio di antiriflessività:** una relazione binaria su un insieme A si dice antiriflessiva quando per ogni $a \in A$ non deve essere $(a, a) \in R$

4.3 Considerazioni Aggiuntive

- Le relazioni possono essere di varie arità, non solo binarie. Ad esempio, una relazione ternaria coinvolge triple di elementi.

5 Funzioni

Una funzione è un particolare tipo di relazione binaria che associa ogni elemento di un insieme A (detto dominio) con uno e un solo elemento di un insieme B (detto codominio).

5.1 Definizione Formale

Una funzione da un insieme A a un insieme B è una relazione $R \subseteq A \times B$ tale che per ogni elemento $a \in A$, esiste uno ed un solo elemento $b \in B$ tale che $(a, b) \in R$.

5.2 Tipi di Funzioni

- **Iniettività:** Una funzione $f : A \rightarrow B$ è iniettiva se, per ogni $a_1, a_2 \in A$, $f(a_1) = f(a_2)$ implica $a_1 = a_2$.
Se due elementi di A sono uguali devono avere lo stesso elemento in B come corrispondente
- **Suriettività:** Una funzione $f : A \rightarrow B$ è suriettiva se, per ogni $b \in B$, esiste almeno un $a \in A$ tale che $f(a) = b$.
Ogni elemento in B deve avere un collegamento in A
- **Biettività:** Una funzione $f : A \rightarrow B$ è biettiva (o biunivoca) se è sia iniettiva che suriettiva. Ciò significa che f stabilisce una corrispondenza uno-a-uno tra tutti gli elementi di A e B .

5.3 Funzione Inversa e Equipotenza

- **Funzione Inversa:** Se $f : A \rightarrow B$ è biettiva, esiste una funzione inversa $f^{-1} : B \rightarrow A$ tale che $f^{-1}(f(a)) = a$ per ogni $a \in A$ e $f(f^{-1}(b)) = b$ per ogni $b \in B$.
- **Equipotenza:** Due insiemi A e B sono equipotenti se esiste una funzione biettiva $f : A \rightarrow B$.

5.4 Composizione e Proprietà

- La composizione di due funzioni mantiene certe proprietà: la composizione di due funzioni iniettive è iniettiva; la composizione di due funzioni suriettive è suriettiva; la composizione di due funzioni biettive è biettiva.
- Invertendo l'ordine delle coppie di una funzione non iniettiva si ottiene una relazione che non è necessariamente una funzione, perché potrebbero esserci elementi in B associati a più elementi in A .
- Una funzione $f : A \rightarrow B$ è biettiva se e solo se invertendo l'ordine delle sue coppie si ottiene una funzione, la quale è l'inversa di f e si indica con $f^{-1} : B \rightarrow A$.

5.5 Considerazioni Aggiuntive

- **Dominio e Codominio:** È importante specificare il dominio e il codominio di una funzione, poiché questi insiemi influenzano le proprietà di iniettività, suriettività e biiettività.
- **Immagine e Controimmagine:** L'immagine di una funzione è l'insieme degli elementi di B che sono associati ad almeno un elemento di A . La controimmagine è l'insieme degli elementi di A che sono mappati su un dato elemento di B .
- **Funzioni Parziali:** Esistono anche funzioni parziali, dove alcuni elementi di A potrebbero non avere un'immagine in B .

6 Cardinalità

La **cardinalità** di un insieme si riferisce alla sua classe di **equipotenza**.

6.1 Definizione di Equipotenza

Due insiemi A e B si dicono **equipotenti** se esiste una biiezione tra A e B . In altre parole, A ha la stessa cardinalità di B se e solo se esiste una corrispondenza uno-a-uno e su tutto tra gli elementi di A e quelli di B .

6.2 Proprietà dell'Equipotenza

L'equipotenza è una relazione di equivalenza che presenta le seguenti proprietà:

- **Riflessiva:** Ogni insieme è equipotente a se stesso, poiché la funzione identità è una biiezione.
- **Simmetrica:** Se A è equipotente a B , allora B è equipotente a A .
- **Transitiva:** Se A è equipotente a B e B è equipotente a C , allora A è equipotente a C .

6.3 Notazione e Confronto di Cardinalità

La cardinalità di un insieme A viene indicata con $|A|$. La relazione di cardinalità tra due insiemi è definita come segue:

- $|A| \leq |B|$ se e solo se (sse) esiste una iniezione da A a B .
- $|A| = |B|$ se e solo se esiste una biiezione tra A e B .
- $|A| < |B|$ se $|A| \leq |B|$ ma $|A| \neq |B|$.

6.4 Teoremi Fondamentali

- **Teorema:** Se $|A| \leq |B|$ e $|B| \leq |A|$, allora $|A| = |B|$. Questo è noto come il **teorema di Cantor-Bernstein-Schroeder**, che afferma che se esistono funzioni iniettive da A a B e da B a A , allora esiste una biiezione tra A e B .

6.5 Teorema di Cantor

Georg Cantor ha dimostrato che non esiste una biiezione tra un insieme e il suo insieme delle parti. In altre parole:

- **Teorema:** $|A| < |P(A)|$ per ogni insieme A , dove $P(A)$ indica l'insieme delle parti di A .

7 Algebra di Boole

7.1 Definizione

L'algebra di Boole è definita su un gruppo con delle operazioni e dei valori, queste strutture e operazioni verificano alcune proprietà, l'algebra.

7.2 operazioni

Le operazioni dell'algebra di Boole sono:

- **meet** che si indica con il simbolo \wedge e ha valenza dell'AND logico
- **join** che si indica con il simbolo \vee e ha valenza dell'OR logico
- **complemento** che si indica con il simbolo \bar{a} e ha valenza del NOT logico (\neg)

7.3 proprietà dell'algebra di Boole

- **Associativa**
 $A \vee (B \vee C) = (A \vee B) \vee C$
 $A \wedge (B \wedge C) = (A \wedge B) \wedge C$
- **Commutativa**
 $A \vee B = B \vee A$ $A \wedge B = B \wedge A$
- **Assorbimento**
 $A \vee (A \wedge B) = A$ $A \wedge (A \vee B) = A$
- **Idempotenza**
 $A \vee A = A$ $A \wedge A = A$
- **Distributiva**
 $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$
 $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$
- **Identità**
 $A \vee \perp = A$ $A \vee \top = A$
- **Complemento**
 $A \vee \bar{A} = \top$ $A \wedge \bar{A} = \perp$
- **De Morgan**
 $\overline{A \vee B} = \bar{A} \wedge \bar{B}$ $\overline{A \wedge B} = \bar{A} \vee \bar{B}$

7.4 Considerazioni Aggiuntive

- Le operazioni booleane sono definite su un insieme di due elementi, tipicamente rappresentati come 0, 1, \perp , \top , o false, true.

8 Assiomi di Hilbert per la Logica Proposizionale

Gli assiomi di Hilbert sono formule di base in un sistema logico che, insieme alle regole di inferenza, permettono la deduzione di teoremi.

8.1 Assiomi

- $A \rightarrow (B \rightarrow A)$
- $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$
- $(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$

8.2 Regola di Inferenza

La **modus ponens** è l'unica regola di inferenza nel sistema di Hilbert, che afferma: se abbiamo A e $A \rightarrow B$, allora possiamo dedurre B .

8.2.1 Esempio

Se abbiamo una formula che afferma "se piove allora porto l'ombrello" e un'affermazione che dice "piove", allora possiamo dedurre "porto l'ombrello".

8.3 Teorema di Deduzione

8.3.1 Sequente

Un sequente è un'espressione in cui abbiamo un simbolo di deduzione \vdash e un insieme di formule. Per esempio, $A, B, C \vdash D$ significa che da A, B, C possiamo dedurre D .

8.3.2 Derivazione

Una derivazione è una sequenza di formule dove ogni formula è un'istanza di un assioma o è ottenuta tramite la regola di inferenza (modus ponens), usando come premesse due formule che la precedono.

8.4 Formula della Transitività dell'Implicazione

La transitività dell'implicazione è espressa dalla formula:

$$(A \rightarrow B) \wedge (B \rightarrow C) \rightarrow (A \rightarrow C)$$

9 Logica Proposizionale

La logica proposizionale è un ramo della logica matematica che studia i modi in cui le proposizioni possono essere combinate e le relazioni tra di esse.

9.1 Linguaggio della Logica Proposizionale

Il **linguaggio** della logica proposizionale è composto da:

- **Simboli proposizionali atomici**: Sono le lettere che rappresentano proposizioni semplici e indivisibili, come p , q , r , ecc.
- **Operatori logici**: Sono utilizzati per costruire formule più complesse a partire da quelle semplici. Gli operatori includono:
 - **Implicazione** (\rightarrow): Indica una relazione di conseguenza logica.
 - **Negazione** (\neg): Esprime il contrario di una proposizione.
 - **Disgiunzione** (\vee): Corrisponde all'operatore logico "or".
 - **Coniunzione** (\wedge): Corrisponde all'operatore logico "and".
 - **Doppia implicazione** (\leftrightarrow): Indica una relazione di equivalenza logica, anche detta "se e solo se" (sse).

9.2 Deduzione e deduzione semantica

La **deduzione** si indica con il simbolo \vdash e rappresenta la relazione tra una formula e un insieme di formule, indicando che la formula è deducibile dall'insieme di formule. La **deduzione semantica** si indica con il simbolo \models e rappresenta la relazione tra una formula e un insieme di formule, indicando che la formula è vera in tutti i modelli dell'insieme di formule.

9.3 Semantica

La **semantica** si occupa del significato delle formule della logica, attribuendogli un valore di verità: vero (\top) o falso (\perp).

9.3.1 Tabelle di Verità

Le tabelle di verità sono uno strumento fondamentale nella logica proposizionale, in quanto permettono di analizzare le formule per determinare il loro valore di verità in base ai valori delle proposizioni atomiche da cui sono composte.

9.4 Modello della Logica Proposizionale

Un **modello** in logica proposizionale è un'attribuzione specifica di valori di verità ai simboli proposizionali atomici. Ad esempio, in un dato modello, le proposizioni A , B , e C possono essere tutte vere, tutte false, o avere una combinazione di valori di verità.

10 Come Usare i Tableau Proposizionali

I tableau proposizionali sono un potente strumento utilizzato nella logica per determinare la soddisfacibilità di formule proposizionali. Questo metodo si basa sull'espansione di un albero di decisione seguendo regole specifiche per gli operatori logici.

10.1 Principi Base

Il procedimento inizia con la formula che si vuole analizzare. L'obiettivo è decomporre la formula in componenti più semplici fino a raggiungere proposizioni atomiche, seguendo un insieme di regole di decomposizione che variano in base agli operatori logici presenti.

10.2 Regole di Decomposizione

Le regole di decomposizione per i vari operatori logici sono le seguenti:

- **Negazione** (\neg): La negazione di una proposizione atomica o di una formula complessa viene decomposta invertendo il suo valore di verità.
- **Coniunzione** (\wedge): Una formula del tipo $A \wedge B$ viene decomposta in due rami, uno per A e uno per B , che devono entrambi essere veri.
- **Disgiunzione** (\vee): Una formula del tipo $A \vee B$ genera due sottorami separati, uno con A vero e l'altro con B vero, indicando che almeno uno dei due deve essere vero.
- **Implicazione** (\rightarrow): Un'implicazione $A \rightarrow B$ viene trattata come $\neg A \vee B$, generando due sottorami: uno con A falso e l'altro con B vero.
- **Doppia implicazione** (\leftrightarrow): Una doppia implicazione $A \leftrightarrow B$ viene decomposta in due parti: $A \rightarrow B$ e $B \rightarrow A$.

10.3 Chiusura del Tableau

Un ramo del tableau si dice *chiuso* se contiene una contraddizione, ovvero la stessa proposizione atomica appare sia in forma affermativa che negativa. Se tutti i rami del tableau sono chiusi, la formula iniziale è insoddisfacibile. Se almeno un ramo rimane aperto (senza contraddizioni), la formula è soddisfacibile, e le assegnazioni di verità lungo il ramo aperto forniscono un modello che soddisfa la formula.

10.4 Esempio di Applicazione

Consideriamo la formula $(P \rightarrow Q) \wedge (\neg Q \vee R)$. Per analizzarla con un tableau proposizionale, si inizia scrivendo la formula sulla cima del tableau e poi si procede a decomporla seguendo le regole sopra descritte, espandendo l'albero fino a raggiungere proposizioni atomiche o contraddizioni.

10.5 Conclusioni

I tableau proposizionali sono uno strumento essenziale per la verifica della soddisfacibilità delle formule logiche. Grazie alla loro struttura sistematica, permettono di esplorare tutte le possibili assegnazioni di valori di verità per determinare la veridicità di una formula.

11 Esercizi

questi esercizi sono tratti dal web seminar:

- 5 luglio 2021
- 29 luglio 2021
- 11 settembre 2021
- 20 dicembre 2021
- 11 gennaio 2022
- 2 febbraio 2022
- 2 aprile 2022
- 13 giugno 2022
- 3 novembre 2023
- 24 novembre 2023
- 8 dicembre 2023
- 29 ottobre 2022
- 17 novembre 2022
- 6 dicembre 2022

11.1 Insiemi

Domanda: La differenza tra due insiemi A e B

Risposta: È definita come le X che non appartengono ad A ma appartengono a B .

Domanda: Come definisci l'intersezione tra due insiemi A e B ?

Risposta: L'intersezione è le $X \in A : X \in B$ (principio di comprensione)

Domanda: Come definisci l'unione?

Risposta: L'insieme di elementi che appartengono ad A più quelli che appartengono a B . Per dimostrarlo serve un assioma della teoria degli insiemi che dato un insieme A e un insieme B esiste un insieme C tale che $A \subseteq C \wedge C, B \subseteq C$

Domanda: Dimostra l'uguaglianza $A - (B \cup C) = (A - B) \cap (A - C)$

Risposta:

Domanda: Cos'è la chiusura di un insieme rispetto ad una proprietà, esempio insieme delle coppie $(n, n + 1)$ ossia funzione successore vista come insieme di Coppie, voglio la chiusura simmetrica

Risposta: La chiusura simmetrica della funzione successore è costituita da tutte quelle coppie (x, y) tali che y è il successore di x oppure x è il successore di y

Domanda: Fammi la chiusura transitiva della funzione successore

Risposta: La chiusura transitiva della funzione successore è l'insieme delle coppie (x, y) in cui $x \preceq y$

Domanda: Qual è il più piccolo sovrainsieme della funzione successore che ha la proprietà di essere una funzione transitiva?

Risposta: Minore stretto perchè è il sovrainsieme più grande

Domanda: Cos'è la chiusura transitiva e simmetrica della funzione successore (dobbiamo trovare la più piccola relazione simmetrica e transitiva che contiene come sottoinsieme la funzione successore)

Risposta: Sono tutte le coppie (x, y) tale che $x < y$ per simmetria anche tutte le coppie $y < x$ quindi è l'unione

della relazione $< e >$

11.2 Relazioni

Domanda: Perché si parla sempre di relazione riflessiva, anti-riflessiva, simmetrica e antisimmetrica però di transitiva non si parla mai di una relazione anti-transitiva?

Risposta: La relazione anti-transitiva è una relazione che non soddisfa la proprietà di transitività. In altre parole, una relazione R è anti-transitiva se esistono a, b, c tali che aRb e bRc , ma non aRc . Un esempio è la relazione del successore. Tuttavia, questa proprietà non è così comune o rilevante come le altre proprietà delle relazioni, quindi non è spesso menzionata in modo specifico.

Domanda: Fammi esempi di funzione riflessiva, simmetrica, anti-transitiva.

Risposta: Un esempio di funzione riflessiva è la funzione identità, $f(x) = x$. Un esempio di funzione simmetrica è $f(x) = -x$. Un esempio di funzione anti-transitiva è $f(x) = x + 1$.

Domanda: È possibile avere una relazione riflessiva e antitransitiva? Se sì quale.

Risposta: Sì, solo l'insieme vuoto.

Domanda: È possibile avere una relazione transitiva e antiriflessiva? Se sì quale.

Risposta: Sì, l'insieme vuoto.

Domanda: Qual'è la differenza tra relazione vuota su $N \times N$ e la relazione vuota su insieme vuoto?

Risposta: La relazione vuota su $N \times N$ è un sottoinsieme di $N \times N$ che non contiene alcuna coppia ordinata. La relazione vuota sull'insieme vuoto è un sottoinsieme dell'insieme vuoto, che non contiene alcun elemento.

Domanda: Relazioni simmetriche e antisimmetriche in contemporanea.

Risposta:

Domanda: Quali sono le proprietà delle relazioni che vengono preservate da intersezione e unione **Risposta:**

Domanda: Se faccio intersezione di due relazioni riflessive quello che ottengo è ancora una relazione riflessiva?

Risposta: Sì, l'intersezione di due relazioni riflessive è ancora una relazione riflessiva. Lo dimostriamo prendendo due insiemi R_1 e R_2 riflessivi, la loro intersezione è riflessiva perché prendo gli elementi che sono sia nel primo che nel secondo insieme, essendo questi elementi riflessivi anche l'intersezione sarà riflessiva

Domanda: L'intersezione preserva la simmetria?

Risposta: Sì

Domanda: L'unione preserva la transitività?

Risposta: No, se unisco due relazioni transitive non ottengo una relazione transitiva

Domanda: Se ho due funzioni iniettive e le compongo la funzione composta è innettiva?

Risposta:

Domanda: Se ho due funzioni suriettive e le compongo la funzione composta è suriettiva?

Risposta:

Domanda: Se f e g sono funzioni dove non so nulla ma so che la loro composta è iniettiva, posso concludere che sia f che g sono due funzioni iniettive?

Risposta:

Domanda: Dammi una relazione transitiva e una non transitiva sugli insiemi dei booleani.

Risposta:

11.3 Funzioni

Domanda: Una funzione è un particolare tipo di relazione, una funzione è invertibile se e solo se vista e considerata come relazione è una relazione simmetrica.

Risposta: Quindi è una relazione binaria su un insieme dato che va da A in A . Per dimostrare che una funzione è invertibile deve essere biunivoca ossia suriettiva e iniettiva.

Domanda: supponiamo di avere una funzione da A in A . $f : f = f \circ f$ (idempotenza) dammi esempi dove questo avviene (no identità)

Risposta:

Domanda: trovare delle condizioni necessarie e sufficienti affinché questo avvenga, quali sono le proprietà che deve avere questa funzione $f \times f = f \circ f$

Risposta:

Domanda: Cos'è una funzione da A in B ?

Risposta: E' una relazione tale che per $\forall a \in A \exists b \in B : aRb$

Domanda: Quando una funzione da A in B si dice iniettiva?

Risposta: f è iniettiva $\forall a, b \in A$ se $f(a) = f(b) \Rightarrow a = b$

Domanda: Se ho due funzioni iniettive e faccio la composizione di queste funzioni, quello che ottengo è una funzione iniettiva?

Risposta: Sì, la composizione di due funzioni iniettive è iniettiva.

Domanda: Se ho una composizione iniettiva allora g e f sono iniettive?

Risposta: No, f e g potrebbero correggere la non iniettività di una delle due funzioni

Domanda: Se ho due funzioni suriettive e le compongo la funzione composta è suriettiva?

Risposta: Sì, la composizione di due funzioni suriettive è suriettiva.

Domanda: La composizione di f e g è suriettiva ma implica che f e g lo siano?

Risposta: No, però g deve essere suriettiva altrimenti la composizione non lo sarebbe.

Domanda: Se f e g sono funzioni dove non so nulla ma so che la loro composta è iniettiva, posso concludere che sia f che g sono due funzioni iniettive? (riflessione della proprietà)

Risposta:

11.4 Cardinalità

Domanda: le relazioni SAS (sono le relazioni simmetriche e antisimmetriche contemporaneamente) e TAT (le relazioni transitive e antitransitive). Son di più le relazioni SAS o TAT?

Risposta: Per confrontare la cardinalità delle relazioni che sono simultaneamente simmetriche e antisimmetriche (SAS) con quelle che sono sia transitive che antitransitive (TAT), consideriamo il concetto di infinità e le proprietà delle relazioni tra insiemi di numeri.

Prima di tutto, ricordiamo che un insieme di numeri primi è infinito e numerabile, mentre l'insieme delle parti di un insieme infinito numerabile, come l'insieme dei numeri primi P , è un'infinità non numerabile. Questo è un risultato diretto del teorema di Cantor, che afferma che l'insieme delle parti di qualsiasi insieme A ha una cardinalità maggiore dell'insieme A stesso.

Per dimostrare che le relazioni TAT hanno una cardinalità almeno pari all'insieme delle parti dei numeri primi, consideriamo una costruzione specifica. Prendiamo un qualsiasi sottoinsieme di numeri primi, ad esempio $\{7, 11, 13\}$, e costruiamo una relazione che includa coppie del tipo $(p, p+1)$, dove p è un numero primo e $p+1$ è il suo successore immediato. Per il nostro esempio, otteniamo le coppie $(7, 8)$, $(11, 12)$, $(13, 14)$. Questa costruzione garantisce che la relazione sia antitransitiva, poiché non esistono tre elementi a, b, c tali che se (a, b) e (b, c) appartengono alla relazione, allora (a, c) dovrebbe appartenere alla relazione, il che è impossibile per la nostra costruzione.

Ogni sottoinsieme di numeri primi può essere associato univocamente a una relazione TAT mediante questa costruzione. Questo stabilisce una funzione iniettiva dall'insieme delle parti dei numeri primi all'insieme delle relazioni TAT, dimostrando che la cardinalità dell'insieme delle relazioni TAT è maggiore o uguale alla cardinalità dell'insieme delle parti dei numeri primi, che è non numerabile.

In conclusione, poiché l'insieme delle parti dei numeri primi è non numerabile e ogni sottoinsieme di numeri primi può essere associato univocamente a una relazione TAT, segue che l'insieme delle relazioni TAT è anch'esso non numerabile e, per costruzione, la sua cardinalità è almeno pari a quella dell'insieme delle parti dei numeri primi. Questo ragionamento non si applica direttamente alle relazioni SAS, la cui cardinalità dipende da considerazioni diverse, ma suggerisce che le relazioni TAT rappresentano un insieme vasto e complesso di relazioni.

Domanda: Sono di più i numeri naturali o le liste finite di numeri naturali?

Risposta: La cardinalità di N si indica con ω , 2^ω è riferita alla cardinalità del continuo. Qui parliamo di insiemi di sequenza di n. L'equipotenza ossia che 2 cose hanno la stessa cardinalità avviene quando c'è una funzione biettiva. **Bernstein Schroder** dice che se esistono due funzioni iniettive una in un senso e una in un altro allora esiste una funzione biettiva. Abbiamo quindi dimostrato che la cardinalità di n, parti finite di n hanno la stessa cardinalità.

Domanda: Sono più i numeri naturali o i sottoinsiemi finiti dei naturali? **Risposta:**

Domanda: Tirar fuori la cardinalità 49 dall'insieme 7 usando le funzioni

Risposta: Se ho un insieme A e un insieme B la cardinalità delle funzioni da A a B è B^A . Voglio sapere le funzioni iniettive (tutto il dominio è mappato nel codominio), quindi ci sono tante funzioni iniettive quante le permutazioni di 7 ossia 7!. L'insieme delle parti di 7 è 2^7 ed è l'insieme di tutte le funzioni da 7 in bool, gli elementi di 7×7 è 49 (tanti quanti da bool a giorni della settimana).

Domanda: l'insieme dei numeri naturali è equipotente alle coppie di numeri naturali?

Risposta:

Domanda: Capire se N e N^* (stella di clini) sono equipotenti.

Risposta:

Domanda: Secondo te ci sono più elementi nell'insieme $bool \times nat$ ossia il prodotto cartesiano tra (true,false) e i naturali o le funzioni che vanno dai booleani ai naturali? **Risposta:** $bool \times nat$ è infinito, è l'insieme di tutte le coppie di cui il primo elemento è booleano e il secondo naturale, le funzioni da bool a nat sono anche esse infinite. In conclusione vediamo come possiamo mappare allo stesso modo i valori $bool \times nat$ e i valori $bool \rightarrow nat$ quindi essi sono equipotenti.

11.5 Sistema di Hilbert

Domanda: Dimostrami che $A \vdash A$

Risposta: Significa che A è deducibile da A , $A \rightarrow ((A \rightarrow A) \rightarrow A)$ istanza del primo assioma, prendendo il secondo assioma $(A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow (A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)$ applichiamo il modus ponens alle 2 ne deduciamo $(A \rightarrow (A \rightarrow A)) \rightarrow A \rightarrow A$ ora dobbiamo dimostrarla.

Dal primo assioma prendiamo un'altra istanza $A \rightarrow (A \rightarrow A)$ ora applichiamo modus ponens e arriviamo ad $A \rightarrow A$ quindi per il teorema di deduzione sappiamo che da A si deriva A .

Domanda: Cos'è un sequente?

Risposta: La formula che sta a destra del simbolo di deduzione è derivabile da ciò che sta a sinistra, vuol dire che esiste una dimostrazione di ciò che sta a destra usando quello che sta a sinistra.

Una dimostrazione è una sequenza di formule in cui ciascuna formula nella sequenza è un'istanza di assioma, premesse o ottenute da modus ponens. **Domanda:** Questo sequente è corretto? $B, B \rightarrow A, A \rightarrow C \vdash C$

Risposta:

Domanda: cos'è una dimostrazione?

Risposta: è una serie di passaggi logici, si parte da degli assiomi (che non richiedono dimostrazione)

11.6 Algebra di boole

Domanda: Esiste un'algebra di boole che ha 4 elementi?

Risposta: Sì, è l'insieme che contiene insieme vuoto, true, false, (true, false).

Domanda: Esiste un'algebra di boole con 3 elementi?

Risposta:

11.7 Logica

Domanda: Dimostrare che $A \vee B \rightarrow B \vee A$ **Risposta:** Si può fare con le tavole di verità, con Hilbert o con i Tableau. Risolvendo con gli assiomi di Hilbert possiamo modificare la formula usando solo \neg e \rightarrow . In questo caso $A \vee B$ diventa $\bar{A} \rightarrow B$.

Quindi traducendo abbiamo $\bar{A} \rightarrow B \rightarrow \bar{B} \rightarrow A$. Possiamo anche dimostrare con Tableau, prendo la formula e la nego poi applico Tableau e dimostro che costruisco un albero chiuso, questo significa che la formula negata non è soddisfacibile

Domanda: Supponiamo di prendere la formula $\vdash (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$

Risposta: Per dimostrare l'assioma possiamo usare il teorema di deduzione e il modus ponens

- $A \rightarrow (B \rightarrow C) \vdash (A \rightarrow B) \rightarrow (A \rightarrow C)$
- poi applichiamo di nuovo il teorema di deduzione
- $A \rightarrow (B \rightarrow C), A \rightarrow B \vdash A \rightarrow C$
- $(A \rightarrow B), A, A \rightarrow (B \rightarrow C) \vdash C$

Domanda: Che cos'è una dimostrazione

Risposta: Una sequenza di formule che contiene o deduzioni o istanze di assiomi o premesse, l'ultima della quale è C nel caso sopra.

Domanda: $a \vee b = a \iff a \wedge b = b$ ti torna? **Risposta:** Se una cosa è vera nel mondo degli insiemi sicuramente è vera nell'algebra di boole, per il **Teorema di Stone** che dice che le algebre fatte in modo tale che i suoi elementi sono insiemi, che l'unione corrisponde al join ecc sono totalmente generali. Quindi se decidiamo di dimostrarlo negli insiemi sarà dimostrato anche per qualunque algebra di boole. Prendiamo quindi due insiemi a e b prendo l'unione di a e b se è uguale ad a significa che la parte di b non intersecata con a è vuota, quindi b è un sottoinsieme di a . oppure usiamo l'algebra di boole per dimostrare.

- iniziamo con la prima direzione $a \vee b = a \Rightarrow a \wedge b = b$
- si inizia dalla conclusione sapendo che per fare la dimostrazione posso usare l'ipotesi
- il modo tipico di dimostrare è creare una catena di uguaglianze
- $a \vee b$ sostituisco con l'ipotesi a
- $(a \vee b) \wedge b$
- possiamo applicare la proprietà di assorbimento
- quindi $(a \vee b) \wedge b = b$ quindi $a \wedge b = b$ abbiamo dimostrato
- ora dimostriamo l'altra direzione $a \vee b = a \Leftarrow a \wedge b = b$
- $a \vee b = a \vee (a \wedge b) = a$ per proprietà assorbimento quindi dimostrato

Domanda: $a \wedge \bar{b} = \perp \iff a \vee b = b$ **Risposta:**

- $a \vee b = b$ significa che $a \subseteq b$ quindi $a \leq b$
- nel mondo degli insiemi il bottom corrisponde all'insieme vuoto mentre il top è l'intero universo
- insiemisticamente $a \subseteq b$

Ora proviamo a dimostrarlo con l'algebra di boole senza usare gli insiemi

- $a \wedge \bar{b} = \perp \iff a \vee b = b$
- scegliamo una delle due direzioni
- scegliamo quindi $a \vee b = b$ come ipotesi e dimostriamo $a \wedge \bar{b} = \perp$
- quindi usiamo De Morgan
- $\perp = \perp \wedge \bar{b} = (a \wedge \bar{a}) \wedge \bar{b} = a \wedge (\bar{a} \wedge \bar{b}) = a \wedge \overline{(a \vee b)} = (a \vee \bar{b})$
- perchè ricordiamo $\perp \wedge a = \perp$ e $\top \vee a = \top$

Domanda: quanti modelli ci sono se ho solo 3 simboli proposizionali?

Risposta: $2 \times 2 \times 2$ ossia $2^3 = 8$

Domanda: supponiamo che i simboli proposizionali siano 3: A, B, C quanti modelli ci sono dove la formula $A \rightarrow B$ è vera?

Risposta: ci sono 6 modelli

1. $A = \top, B = \top, C = \top$ $\therefore B$ è vera
2. $A = \top, B = \top, C = \perp$ $\therefore B$ è vera
3. $A = \top, B = \perp, C = \top$ $\therefore B$ è falsa
4. $A = \top, B = \perp, C = \perp$ $\therefore B$ è falsa
5. $A = \perp, B = \top, C = \top$ $\therefore B$ è vera
6. $A = \perp, B = \top, C = \perp$ $\therefore B$ è vera
7. $A = \perp, B = \perp, C = \top$ $\therefore B$ è vera
8. $A = \perp, B = \perp, C = \perp$ $\therefore B$ è vera

Domanda: e se la mia formula fosse $A \rightarrow (B \rightarrow A)$ (sempre considerando che i simboli proposizionali sono A, B, C)

Risposta: ci sono 8 modelli **Domanda:** voglio dedurre la seguente formula $A \wedge B \rightarrow B$ usando Hilbert

Risposta: Negli assiomi di Hilbert noi abbiamo solo il \neg e \rightarrow sembrerebbe che non abbiamo \vee e \wedge ecc ma in realtà possiamo derivarli

- $A \vee B = \overline{A} \rightarrow B$
- $A \wedge B = \overline{\overline{A} \rightarrow \overline{B}}$

quindi possiamo derivare la formula $A \wedge B \rightarrow B$

- $\overline{\overline{A} \rightarrow \overline{B}} \rightarrow B$
- $\overline{B} \rightarrow (A \rightarrow \overline{B})$ è una particolare istanza del primo assioma di Hilbert
- $(A \rightarrow \overline{B}) \rightarrow \overline{\overline{\overline{A} \rightarrow \overline{B}}}$ sto assumendo che $A \rightarrow \overline{A}$
- applico la transitività $\overline{B} \rightarrow \overline{\overline{\overline{A} \rightarrow \overline{B}}}$
- terzo assioma di Hilbert $(\overline{A} \rightarrow \overline{B}) \rightarrow (B \rightarrow A)$

posso usare alcune cose come lo scambio di premesse $\frac{A \rightarrow (B \rightarrow C)}{B \rightarrow (A \rightarrow C)}$,

la transitività $(A \rightarrow B) \rightarrow (B \rightarrow C) \rightarrow (A \rightarrow C)$ e lo pseudo scoto **Domanda:** Cos'è correttezza e completezza?

Risposta: La correttezza è la proprietà di un sistema logico che garantisce che tutte le formule dimostrabili siano vere. La completezza è la proprietà di un sistema logico che garantisce che tutte le formule vere siano dimostrabili.

Domanda: Il seguente enunciato $(A \rightarrow \neg A) \rightarrow false$ è vero quando

Risposta:

- quando A è vero?
- quando A è false?
- $A \wedge \neg A$ è vero
- non è mai vero
- è sempre vero

La risposta corretta è che l'enunciato $(A \rightarrow \neg A) \rightarrow false$ è vera quando A è vero, perchè l'implicazione $A \rightarrow \neg A$ in questo caso sarebbe false, rendendo vero l'enunciato dato secondo le regole dell'implicazione.

Domanda: $(A \wedge B) \rightarrow [C \rightarrow (A \wedge C)]$ dimostralolo

Risposta: traduco in formule logicamente equivalenti con not e implica $A \vee B \equiv \neg A \rightarrow B$ e $A \wedge B \equiv \neg(A \rightarrow \neg B)$. Dimostriamo quindi creando due lemmi $A \wedge B \rightarrow A$ e $A \rightarrow [C \rightarrow (A \wedge C)]$. Se riusciamo a dimostrare questi due lemmi per la proprietà transitiva $(A \wedge B) \rightarrow [C \rightarrow (A \wedge C)]$. Dimostriamo quindi $A \wedge B \rightarrow A$ e la riscriviamo come $\neg(A \rightarrow \neg B) \rightarrow A$.

$$\frac{\frac{\neg A \rightarrow (A \rightarrow \neg B)}{\neg(A \rightarrow \neg B) \rightarrow A}}{A \wedge B \rightarrow A} \quad (1)$$

Abbiamo quindi inverito l'implica negando le due proposizioni. Adesso applichiamo la deduzione.

$\neg A \vdash A \rightarrow \neg B$, giro di nuovo negando: $\neg A \vdash B \rightarrow \neg A$. riappliciamo teorema di deduzione. $\vdash \neg A \rightarrow (B \rightarrow \neg A)$ che non ho bisogno di dimostrare poiché primo assioma di Hilbert.