Logica

1.75: Relazioni, Funzioni, ...

Claudio Sacerdoti Coen

<sacerdot@cs.unibo.it>

Universitá di Bologna

09,11/10/2017

Coppie ordinate

Coppie

Dati X, Y chiamiamo coppia ordinata di prima componente X e seconda componente Y, e la indichiamo con $\langle X, Y\rangle$ l'insieme $\{X, \{X, Y\}\}$

Teorema di caratterizzazione delle coppie

$$\langle X, Y\rangle = \langle X', Y'\rangle \iff X = X' \wedge Y = Y'$$

Dimostrazione: omessa

Corollario

$\langle X, Y\rangle \neq \langle Y, X\rangle$ a meno che $X = Y$

Prodotto cartesiano di insiemi

Teorema: esistenza del prodotto cartesiano di insiemi come insieme

$$\forall A, \forall B, \exists C, \forall Z, (Z \in C \iff \exists a, \exists b, (a \in A \wedge b \in B \wedge Z = \langle a, b \rangle))$$

L'insieme C viene chiamato prodotto cartesiano di A e B e indicato come $A \times B$.

Relazioni

Definizione di relazione

Una relazione fra A e B è un qualunque sottoinsieme di $A \times B$.

Elementi in relazione

Sia $\mathcal{R}$ una relazione. Scriviamo $a\mathcal{R}b$ sse $\langle a, b\rangle \in \mathcal{R}$.

Teorema: relazioni da/verso insiemi vuoti

se $\mathcal{R} \subseteq A \times \emptyset$ oppure $\mathcal{R} \subseteq \emptyset \times A$ allora $\mathcal{R} = \emptyset$ (la relazione vuota)

Dimostrazione: non posso formare coppie prendendo uno dei due elementi dall'insieme vuoto, perchè tale insieme è vuoto.

Funzioni

Definizione di funzione

Una funzione di dominio A e codominio B è una qualunque relazione $f \subseteq A \times B$ tale che

$$\forall x, \exists ! y, (X \in A \Rightarrow X\ f\ Y)$$

(per ogni elemento del dominio c'è un unico elemento del codominio in relazione con esso)

Notazione

Sia f una funzione. Scriviamo $y = f(x)$ per dire $x\ f\ y$, ovvero $\langle x, y \rangle \in f$.

Funzioni

Teorema: esistenza dello spazio di funzioni come insieme

$$\forall A, \forall B, \exists C, \forall f,$$
$$(f \in C \iff f \text{ è una funzione di dominio } A \text{ e codominio } B)$$

Indichiamo l'insieme C come B^A (spazio delle funzioni da A a B.

Funzioni da/verso insiemi vuoti

1. $B^\emptyset = \{\emptyset\}$
2. $\emptyset^A = \emptyset$ sse $A \neq \emptyset$

Dimostrazione: ogni funzione da A verso B è una relazione fra A e B. Se A o B sono vuoti, le uniche relazioni sono la relazione vuota (già dimostrato). La relazione vuota è una funzione solo se è il dominio a essere vuoto perchè altrimenti a un elemento del dominio dovrei associare uno e un solo elemento del codominio, ma questo non ne ha in quanto vuoto.

Quantificazione limitata come notazione

Quantificazione limitata

Nel seguito scriveremo

1. $\forall X \in A, P(X)$ (per ogni X in A vale $P(x)$) per indicare $\forall X, (X \in A \Rightarrow P(X))$
2. $\exists X \in A, P(X)$ (esiste un X in A tale che $P(x)$) per indicare $\exists X, (X \in A \wedge P(X))$
3. $\forall X, Y \in A, P(X, Y)$ per indicare $\forall X \in A, \forall Y \in A, P(X, Y)$
4. $\exists X, Y \in A, P(X, Y)$ per indicare $\exists X \in A, \exists Y \in A, P(X, Y)$

Relazioni di equivalenza

Proprietà riflessiva, simmetrica, transitiva

Sia $\mathcal{R} \subseteq A \times A$. La relazione $\mathcal{R}$ gode della proprietà

1. Riflessiva se $\forall X \in A, X\mathcal{R}X$
2. Simmetrica se $\forall X, Y \in A, (X\mathcal{R}Y \Rightarrow Y\mathcal{R}X)$
3. Transitiva se $\forall X, Y, Z \in A, (X\mathcal{R}Y \wedge Y\mathcal{R}Z \Rightarrow X\mathcal{R}Z)$

Esempi:

- $=$ gode di tutte e tre le proprietà
- $<$ sui numeri naturali è transitiva, ma non simmetrica e non riflessiva
- $\leq$ sui numeri naturali è transitiva e riflessiva, ma non simmetrica
- $\neq$ è simmetrica, ma non transitiva e riflessiva

Tipi di relazioni

Relazioni di ordinamento strette

Una relazione $\mathcal{R} \subseteq A \times A$ è di ordine stretto sse $\mathcal{R}$ è transitiva e non riflessiva.

Esempi:

- $=, \neq, \leq$ non sono relazioni di ordinamento strette
- $<$ è un ordinameno stretto dei numeri naturali
- *"essere antenato di"* è un ordinameno stretto sulle persone

Tipi di relazioni

Relazioni di ordinamento lasche

Una relazione $\mathcal{R} \subseteq A \times A$ è di ordine (lasco) sse

1. $\mathcal{R}$ è transitiva e riflessiva
2. $\mathcal{R}$ è antisimmetrica, ovvero
   $\forall X, Y \in A, (X\mathcal{R}Y \land Y\mathcal{R}X \Rightarrow X = Y)$

Esempi:

- $=, \leq, \subseteq$ sono relazioni di ordinamento
- $|$ (*"divide"*) è una relazione di ordinamento sui numeri naturali
- $<, \subsetneq, \neq$ non sono relazioni di ordinamento

Tipi di relazioni

Relazioni di equivalenza

Una relazione $\mathcal{R} \subseteq A \times A$ è di equivalenza sse $\mathcal{R}$ è riflessiva, simmetrica e transitiva.

Esempi:

- $=$ è una relazione di equivalenza
- *"avere lo stesso cognome"*, *"essere dello stesso modello"* sono relazioni di equivalenza
- $<, \leq, \neq$ non sono relazioni di equivalenza

Intuizione

Una relazione di equivalenza assomiglia all'uguaglianza e viene usata per confrontare oggetti a meno di dettagli non ritenuti rilevanti per quello che si deve fare.

Classi di equivalenza e insiemi quoziente

Classi di equivalenza

Sia $\equiv \subseteq A \times A$ una relazione di equivalenza su A. La classe di equivalenza di $x \in A$ rispetto a $\equiv$, è definita come segue:

$$[x]_{\equiv} \stackrel{\text{def}}{=\!=} \{y \in A \mid y \equiv x\}$$

Teorema

Sia $\equiv \subseteq A \times A$ una relazione di equivalenza. Per ogni $x, y \in A$, o $[x]_{\equiv} = [y]_{\equiv}$ (quando $x \equiv y$) oppure $[x]_{\equiv}$ e $[y]_{\equiv}$ sono insiemi disgiunti (= senza elementi in comune) (quando $x \not\equiv y$).

Dimostrazione: per la proprietà transitiva di $\equiv$, se $x \equiv y$ allora ogni $z \in [x]_{\equiv}$ è tale che $z \equiv x \equiv y$ e quindi $z \in [y]_{\equiv}$. Inoltre, per le proprietà simmetriche e transitive di $\equiv$, se $z \in [x]_{\equiv} \cup [y]_{\equiv}$ allora $x \equiv z \equiv y$ e perciò $[x]_{\equiv} = [y]_{\equiv}$. Quindi le due classi sono identiche o disgiunte.

Classi di equivalenza e insiemi quoziente

Insieme quoziente

Sia $\equiv \subseteq A \times A$ una relazione di equivalenza. L'insieme quoziente di A rispetto a $\equiv$ è definito come segue:

$$A_{/\equiv} \stackrel{\text{def}}{=\!=} \{[x]_{\equiv} \mid x \in A\}$$

Nota: che tale insieme esista è conseguenza dell'assioma di rimpiazzamento

Esempi:

- *"avere la stessa età"* è una relazione di equivalenza (chiamiamola $\equiv$)
  1. $[\textit{Claudio Sacerdoti Coen}]_{\equiv}$ sono tutti i 41-enni; esso rappresenta l'età 41
  2. $\textit{Persone}_{/\equiv}$ ha un elemento per età; tale elemento è l'insieme di tutte le persone identificate per età

Intuizione

Gli insiemi quozienti sono uno strumento potentissimo per creare nuovi concetti costruendoli a partire da concetti pre-esistenti e poi semplificandone via i dettagli dovuti alla rappresentazione.

Esempio: i numeri interi $\mathbb{Z}$

Vogliamo costruire i numeri interi a partire dai naturali.
Gli interi completano i naturali permettendo di fare sottrazioni fra naturali arbitrari ($2 - 4 =?$).

- $Z = \mathbb{N} \times \mathbb{N}$
  intuizione: $\langle 2, 4\rangle \in Z$ rappresenta $2 - 4$
- $\equiv \subseteq Z \times Z : \langle u_1, l_1\rangle \equiv \langle u_2, l_2\rangle \stackrel{\text{def}}{=\!=} u_1 + l_2 = u_2 + l_1$
  $\langle 2, 4\rangle \equiv \langle 3, 5\rangle$ perchè rappresentano la stessa sottrazione: infatti $2 - 4 = 3 - 5$ sse $2 + 5 = 4 + 3$
- $\mathbb{Z} \stackrel{\text{def}}{=\!=} Z_{/\equiv}$
- $\mathbb{Z} = \{\ldots, [\langle 0, 2\rangle]_{/\equiv}, [\langle 0, 1\rangle]_{/\equiv}, [\langle 0, 0\rangle]_{/\equiv}, [\langle 1, 0\rangle]_{/\equiv}, [\langle 2, 0\rangle]_{/\equiv}, \ldots\}$
- Zucchero sintattico: indichiamo $[\langle 0, i\rangle]_{/\equiv}$ con $-i$, $[\langle 0, 0\rangle]_{/\equiv}$ con 0 e $[\langle i, 0\rangle]_{/\equiv}$ con $+i$.
- $\mathbb{Z} = \{\ldots, -2, -1, 0, +1, +2, \ldots\}$

Iniettività, suriettività, biettività

$f \in B^A$ è

1. iniettiva quando $\forall x, y \in A, (f(x) = f(y) \Rightarrow x = y)$
2. suriettiva quando $\forall y \in B, \exists x \in A, f(x) = y$
3. biettiva quando è sia iniettiva che suriettiva

Esempi:

- $+1$ è biettiva sui numeri interi, iniettiva ma non suriettiva sui naturali
- $|\cdot|$ (il valore assoluto) è non suriettiva e non iniettiva sugli interi

Intuizione: proprietà delle funzioni e cardinalità degli insiemi

Sia $f \in B^A$. Intuitivamente

1. Se f è iniettiva allora B ha almeno tanti elementi quanti ne ha A.
2. Se f è suriettiva allora A ha almeno tanti elementi quanti ne ha B.
3. Se f è biettiva allora A e B hanno lo stesso “numero” di elementi.

L'intuizione è buona, ma non in termine di numeri:

1. Quanti elementi ha (in numero) un insieme infinito?
2. Ci sono insiemi infinit più infiniti di altri?

Cardinalità di un insieme

Avere la stessa cardinalità

Due insiemi A, B hanno la stessa cardinalità sse esiste una biiezione fra A e B.

Avere la stessa cardinalità è una “relazione di equivalenza”, ma sulla classe di tutti gli insiemi.

Numeri cardinali

Sia U la classe di tutti gli insiemi. Un numero cardinale è un elemento di $U_{/_{/ equiv}}$ dove $\equiv$ significa avere la stessa cardinalità.

Esempio

- $3 \overset{\text{def}}{=\!=} [\{1,2,3\}] = \{\{1,2,3\},\{5,2,8\},\{\emptyset,3,\langle 1,2\rangle\},\ldots\}$
- $0 \overset{\text{def}}{=\!=} [\emptyset] = \{\emptyset\}$
- $\aleph_0 \overset{\text{def}}{=\!=} [\mathbb{N}] = \{\mathbb{N},\{n \in \mathbb{N} \mid n \text{ è pari}\},\mathbb{Q},\ldots\}$

Cardinalità di un insieme

Teorema: esistenza dei numeri cardinali come insiemi

Con un certo sforzo è possibile costruire i numeri cardinali senza usare le classi di equivalenza su classi, ma lavorando solo su insiemi. Ogni numero cardinale viene ottenuto come insieme.

Notazione dei numeri cardinali

Usiamo come notazione per i numeri cardinali relativi a insiemi finiti (vedi dopo) i numeri naturali 0,1,2, $\ldots$ (le classi degli insiemi con 0, 1, 2, $\ldots$ elementi).

Si usano altri simboli speciali per i cardinali degli insiemi infiniti (vedi dopo).

Cardinalità di un insieme

Cardinalità di un insieme

Per ogni insieme A si definisce cardinalità di A, indicata con $|A|$ il numero cardinale $[A]_{/\equiv}$.

Esempio:

$$|\{1,2,3\}| = [\{1,2,3\}]_{/\equiv}$$
$$= \{\{1,2,3\},\{5,2,8\},\{\emptyset,3,\langle 1,2\rangle\},\ldots\} = 3$$

Insiemi finiti

Un insieme si dice finito quando non è infinito.

Osservazione

Intuitivamente sappiamo che un insieme con 3 elementi è finito.

Immaginate un albergo con 3 stanze singole tutte occupate. Arriva un nuovo cliente. Può l'albergatore con una qualche manovra accomodare tutti i clienti nell'hotel rispettando il fatto che una singola può essere occupata da un solo cliente?

L'albergo di Hilbert

Intuitivamente sappiamo che l'insieme dei numeri naturali è infinito.

Immaginate un albergo con una stanza singola per ogni numero naturale, tutte occupate. Arriva un nuovo cliente. Può l'albergatore con una qualche manovra accomodare tutti i clienti nell'hotel rispettando il fatto che una singola può essere occupata da un solo cliente?

L'albergo di Hilbert

Intuitivamente sappiamo che l'insieme dei numeri naturali è infinito.

Immaginate un albergo con una stanza singola per ogni numero naturale, tutte occupate. Arriva un nuovo cliente. Può l'albergatore con una qualche manovra accomodare tutti i clienti nell'hotel rispettando il fatto che una singola può essere occupata da un solo cliente?

Soluzione: per ogni n si chiede al cliente nella stanza n di trasferirsi nella stanza $n + 1$; ora la stanza 0 è libera per il nuovo arrivato.

Insiemi infiniti

Un insieme A si dice infinito quando è in biiezione con un suo sottoinsieme proprio B (i.e. $B \subsetneq A$ e $|B| = |A|$).

L'ordinamento dei numeri cardinali

$\leq$ su numeri cardinali

Siano x, y due numeri cardinali. $x \leq y$ se dati due insiemi A e B tali che $|A| = x$ e $|B| = y$ esiste una iniziezione fra A e B. In particolare, $|C| \leq |D|$ sse esiste una iniezione fra C e D.

$<$ su numeri cardinali

Siano x, y due numeri cardinali. $x < y$ se $x \leq y$ e $x \neq y$. In particolare $|A| < |B|$ sse esiste una iniezione di A in B e non esiste nessuna biiezione fra A e B.

Esempi

- $2 = |\{1, 2\}| < |\{a, b, c\}| = 3$ come testimoniato dall'iniezione $1 \mapsto a,\ 2 \mapsto b$ e dall'assenza di biezioni
- $2 = |\{1, 2\}| < |\mathbb{N}| = \aleph_0$ come testimoniato dall'iniezione funzione $1 \mapsto 1,\ 2 \mapsto 2$ e dall'assenza di biezioni
- $|\mathbb{P}| = |\{n \in \mathbb{N} \mid n \text{ è pari}\}| \leq |\mathbb{N}|$ come testimoniato dalla funzione identità che è una iniezione
- $|\mathbb{P}| \not< |\mathbb{N}|$ in quanto $|\mathbb{P}| = |\mathbb{N}|$ come testimoniato dalla biezione $f(x) = 2 * x$, $f \in \mathbb{N}^{\mathbb{P}}$

Insiemi finiti e insiemi infiniti

Osservazione

Le intuizioni che ci derivano dalla nostra interazione quotidiana con oggetti finiti sono spesso fuorvianti quando applicate all'infinito.

Teorema: per ogni insiemi finito A e per ogni suo sottoinsieme B (i.e. $B \subseteq A$), $B \subsetneq A$ sse $|B| < |A|$.

Definizione di insieme infinito: per ogni insieme infinito A c'è un suo sottoinsieme proprio B (i.e. $B \subsetneq A$) tale che $|B| = |A|$.

Quindi la nozione intuitiva di taglia indotta dall'essere un sottoinsieme proprio è fuorviante quando applicata fuori da un contesto infinito ed è meglio quindi non considerarla anche nel finito.

Metodo di diagonalizzazione Cantor

Teorema di Cantor

L'idea alla base del teorema è ancora lo sfruttamento del paradosso del mentitore:

Enunciato: sia $|T|$ un insieme non vuoto. Allora $|T| < |2^T|$.
Dimostrazione per assurdo:
Per assurdo, supponiamo $|T| = |2^T|$, ovvero che esista una biiezione g fra T e 2^T (l'insieme delle parti di T).
Sia $A \stackrel{\text{def}}{=} \{x \in T \mid x \notin g(x)\}$.
Poichè $A \in 2^T$ e g è una biiezione, deve essercy un $y \in T$ tale che $g(y) = A$, il che è assurdo poichè $y \in g(y) = A \iff y \notin g(y)$ per definizione di A.
Quindi T e T^T non possono essere in biiezione e poichè $f(x) = \{x\} \in 2^T$ è una iniezione di T in 2^T concludiamo che $|T| < |T^T|$.

Funzioni caratteristiche

Sia $\mathbb{B}$ un qualuque insieme con due elementi, chiamati booleani, e indicati con 0 e 1, sia A un insieme e sia $C \subseteq A$.

La funzione caratteristica di C (come sottoinsieme di A) è la funzione $\chi_C \in \mathbb{B}^A$ tale che $\chi_C(x) = 1 \iff x \in C$.

La funzione che associa a ogni $C \in 2^A$ la funzione $\chi_C \in \mathbb{B}^A$ è una biiezione. Pertanto $|2^A| = |\mathbb{B}^A|$.

Corollario al teorema di Cantor

Enunciato: Per ogni insieme T con almeno due elementi, $|T| < |T^T|$.
Dimostrazione: poichè T ha almeno due elementi, vi è un $\mathbb{B} \subseteq T$ tale che $|\mathbb{B}| = 2$.
Quindi $|T| < |2^T| = |\mathbb{B}^T| \leq |T^T|$ per il teorema di Cantor e poichè le funzioni di codominio $|T|$ saranno non meno delle funzioni di codominio $\mathbb{B} \subseteq T$.

Osservazione

Il teorema di Cantor ci dice che esistono insiemi infiniti di cardinalità crescente:

$$\aleph_0 = |\mathbb{N}| < |2^{\mathbb{N}}| < |2^{2^{\mathbb{N}}}| < \dots$$

Insiemi numerabili

Un insieme A si dice numerabile se $|A| = \aleph_0$, ovvero se posso stabilire una biiezione fra i numeri naturali e gli elementi di A, ovvero se posso enumerare uno dopo l'altro tutti gli elementi di A.

Esempi:

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{N} \times \mathbb{N}$ sono enumerabili
- $2^{\mathbb{N}}, 2^{2^{\mathbb{N}}}$ non sono enumerabili

Osservazione

Un computer può rappresentare in memoria, come sequenza di bit, tutti gli elementi di un insieme sse questo insieme è enumerabile.

Spoiler

Procediamo ora a dimotrare che i numeri reali (e quindi anche i complessi, i quaternioni, i vettori, etc.) non sono enumerabili.

I numeri reali

Costruirete l'insieme $\mathbb{R}$ dei numeri reali nel corso di Analisi Matematica.

- Un numero reale può essere rappresentato da una sequenza infinit di cifre, di cui un numero finito prima della virgola (chiamata parte intera)
  Esempio: $\pi = 3.14159265\ldots$
- Un numero reale può essere rappresentato in più di un modo
  Esempio: $1 = 3 * 1/3 = 3 * 0.333\ldots = 0.999\ldots$
- In base 10 si ottiene una rappresentazione univoca escludendo le rappresentazioni che terminano con un 9 periodico
  Esempio: escludiamo $0.999\ldots$ e teniamo solo 1

Cardinalità dei numeri reali

$|\mathbb{N}| < |\mathbb{R}|$

Dimostrazione usando il teorema di Cantor.
$[0,1] \subseteq \mathbb{R}$ e quindi $|[0,1]| \leq |\mathbb{R}|$.
Rappresentato in base 2, un numero in $[0,1]$ ha come parte intera 0 e come parte decimale (dopo la virgola) una sequenza infinita di 0 o 1.
In altre parole, ogni $x \in \mathbb{B}^{\mathbb{N}}$ rappresenta un numero reale (in maniera non univoca per via delle sequenze con 1 periodici, similmente a quello che accade in base 10).
Pertanto il numero di rappresentazioni è $|\mathbb{B}^{\mathbb{N}}| > |\mathbb{N}|$. Il numero cardinale di rappresentazioni duplicate è $|\mathbb{N}|$ (perchè?) che è $< |\mathbb{B}^{\mathbb{N}}|$ e con un ragionamento qui omesso si dimostra che quindi quello delle non duplicate rimane $|\mathbb{B}^{\mathbb{N}}|$.
Concludendo $|\mathbb{N}| < |\mathbb{B}^{\mathbb{N}}| = |[0,1]| \leq |\mathbb{R}|$.

Osservazioni

Il teorema precedente ci dice che i numeri reali (e i complessi, i vettori, etc.) non sono enumerabili.

Pertanto un computer non può rappresentare tutti i numeri reali, ma solo un piccolissimo sottoinsieme enumerabile.

L'aritmetica dei calcolatori è pertanto profondamente diversa da quella vista nel corso di analisi.

Nel corso di Analisi Numerica studierete alcuni modi di rappresentare alcuni numeri reali sul computer e come effettuare computazioni approssimate con essi.

Le funzioni matematiche non sono computabili

Osservazione

Tutte le funzioni che posso scrivere in un linguaggio di programmazione sono enumerabili.

(scrivo prima tutti i programmi con un carattere, poi quelli con due, . . .)

le funzioni matematiche $\mathbb{N}^{\mathbb{N}}$ sono non enumerabili, così come molti insiemi, e quindi non programmabili/rappresentabili in un computer

Dalle funzioni ai programmi

Soluzione (1/2)

Nel resto del corso eviteremo (quasi sempre) il ricorso a insiemi generici e funzioni matematiche. Al loro posto introdurremo un linguaggio di programmazione con tipi di dati da usare al posto degli insiemi e funzioni ricorsive (= programmi) per definire procedure di calcolo su di essi.

Soluzione (2/2)

Descriveremo i linguaggi artificiali che useremo per evitare i paradossi logici e scrivere formule, dimostrazioni, etc. come tipi di dati.

Esempio: una formula sarà un tipo di dato e quindi rappresentabile in memoria; scriveremo programmi che manipolano formule.