Combinatoria

Cos'è la *combinatoria*?

La combinatoria è l'arte di contare insiemi finiti.

Quali sono le figure fondamentali della combinatoria?

Il *principio moltiplicativo* permette di contare le scelte tra n1 oggetti di un tipo, n2 di un altro fino ad nt di un ultimo tipo. Per farlo è necessario moltiplicare il numero di oggetti di n1, n2 … nt.

Chiamiamo *disposizione semplice* di ordine k di n oggetti una sequenza ordinata di k oggetti distinti scelti tra gli n totali. Il numero delle disposizioni semplici è n!/(n-k)!.

Chiamiamo *disposizione con ripetizione* di ordine k di n oggetti una sequenza ordinata di k oggetti non necessariamente distinti scelti tra gli n totali. Il numero di disposizioni semplici è n^k.

Chiamiamo *permutazione semplice* una disposizione semplice in cui l'ordine è uguale al numero di elementi, quindi una sequenza ordinata degli n oggetti totali. Il numero di permutazioni semplici è n!

Chiamiamo anagrammi o permutazioni con ripetizioni delle permutazioni in cui alcuni elementi sono uguali. Il numero di disposizioni semplici è n! / n1!*n2!..*nt!, dove n1, n2, … , nt sono il numero degli elementi uguali di ogni elemento che si ripete.

Chiamiamo *combinazione semplice* di ordine k un raggruppamento di k elementi distinti scelti tra gli n totali. La differenza con le disposizioni è che qui, essendo un raggruppamento (un insieme), l'ordine non è importante. Il numero di combinazioni semplici si calcola applicando la regola del pastore, ossia si prende il numero di disposizioni semplici di ordine k degli n elementi e lo si divide per il numero di permutazioni degli n elementi. La *regola del pastore* dice che per contare le pecore in un gregge, conta le zampe e dividi per 4.

Il numero di combinazioni semplici prende il nome di *coefficiente binomiale*, ha una notazione a sé ed equivale a n!/k!*(n-k)!

La somma dei coefficienti binomiali da (n 0) a (n n) è uguale a 2^n.

Alcune proprietà dei coefficienti binomiali sono individuabili nel triangolo di Targaglia.

(n k) = (n n-k).

(n k) = (n-1 k-1) (con l'elemento a) + (n-1 k) (senza l'elemento a)

(n m) * (m k) = (n k) * (n-k m-k)

Per funzionare la regola del pastore sotto-intende tre condizioni:

- ogni pecora ha lo stesso numero di zampe;
- le zampe di una pecora non sono zampe di nessun'altra pecora;
- non esistono zampe che non sono di nessuna pecora.

Chiamiamo combinazione con ripetizione di ordine k di n elementi è un raggruppamento di k elementi non necessariamente distinti scelti tra gli n totali. Il numero di combinazioni con ripetizione è (n+k-1)! / (k-1)!

Come si conta il numero di sottoinsiemi?

Per contare il numero di sottoinsiemi possibili di un insieme (le possibili scelte di alcuni elementi tra un insieme) si imposta un bit per ogni elemento che assume valore 0 se non prendiamo l'elemento e valore 1 se lo prendiamo. In tutto le possibilità di scegliere un sottoinsieme sono 2^n, dove n è il numero di oggetti.

Cos'è la dimostrazione per doppio conteggio?

È una tecnica di dimostrazione che consiste nel contare in due modi diversi una stessa quantità deducendo l'identità tra i risultati ottenuti con i due conteggi.

Altre proprietà dei coefficienti binomiali.

Il nome di coefficiente binomiale è giustificato dalla stretta correlazione con i coefficienti della potenza di un binomio. (sommatoria)

I coefficienti binomiali possono essere utilizzati anche per trovare i modi di scrivere un numero come somma di n termini tenendo in considerazione l'ordine. Questo tipo di scrittura si chiama *scrittura additiva*. La scrittura additiva può essere usata per risolvere problemi sulla distribuzione x oggetti uguali tra n persone/oggetti (problema dei biscotti).

Funzioni e combinatoria

Cos'è il principio di inclusione-esclusione (PIE)?

Il *principio additivo* o *principio di inclusione-esclusione* dice che se gli oggetti di una collezione sono di due tipi distinti e mutualmente esclusivi, allora il loro numero è la somma degli oggetti del primo tipo e degli oggetti del secondo tipo. Altrimenti, il numero di oggetti totali è uguale al numero di oggetti del primo tipo più il numero di oggetti del secondo tipo meno gli oggetti che sono di entrambi i tipi, che sono stati contati più volte.

Il PIE può essere facilmente generalizzato a più termini.

Come si possono usare le figure della combinatoria nelle funzioni?

Le funzioni da A in B con #A = k e #B = n sono esattamente le disposizioni con ripetizione di ordine k su n elementi, n^k.

Le funzioni iniettive da A in B con #A = k e #B = n sono le disposizioni semplici di ordine k su n elementi.

Le funzioni biiettive da A in A con #A = k sono esattamente le permutazioni di k elementi.

Cos'è il *PHP*?

Il Pidgeon Hole Principle (PHP) dice che dati n+1 piccioni e n piccionaie, se vogliamo mettere i piccioni nelle piccionaie, almeno una piccionaia deve contenere più di un piccione.

Capitolo 1

Cos'è un *insieme*?

Il concetto di insieme può essere fatto corrispondere all'atto mentale mediante il quale associamo alcuni elementi in un tutto unico detto *insieme.* Non è richiesta una particolare omogeneità tra gli elementi di un insieme.

Come può essere rappresentato un insieme?

La rappresentazione degli elementi di un insieme può avvenire attraverso l'elencazione dei suoi elementi (*rappresentazione tabulare*) o la descrizione della proprietà che accomuna i suoi elementi (*rappresentazione caratteristica*). L'importante è che sia sempre decidibile se un elemento appartenga o no ad un insieme, quindi nel caso di rappresentazione caratteristica, questa deve usare proprietà oggettive.

A volte la rappresentazione tabulare risulta impraticabile nel caso si abbia a che fare con insiemi molto grandi o infiniti.

Caratteristiche di un insieme.

Gli insiemi vengono rappresentati per convenzione con lettere maiuscole, i suoi elementi invece vengono rappresentati con lettere minuscole. Negli insiemi, l'ordine non ha importanza.

L'insieme privo di elementi si dice *insieme vuoto*.

Due insiemi si dicono *uguali* se contengono gli stessi elementi (estensione), indipendentemente dalla loro rappresentazione caratteristica (intensione).

Cosa sono i sottoinsiemi?

L'insieme **A** si dice *sottoinsieme* di **B** se ad **A** non appartengono elementi differenti rispetto a quelli di **B**. Se ogni elemento di **A** è elemento di **B** allora si parla di sottoinsieme, e si dice che **A** è *incluso* in **B**.

Si definisce che **A** è sottoinsieme improprio di **B** se **A** è insieme vuoto o è **B**. Altrimenti si dice che **A** è sottoinsieme proprio di **B**.

Se **A** è sottoinsieme di **B** e **B** è contemporaneamente sottoinsieme di **A** si dice che i due insiemi sono uguali (*doppia inclusione*).

Quali operazioni possiamo compiere sugli insiemi?

L'*unione* di due insiemi consiste nel creare un insieme che contiene gli elementi che appartengono al primo insieme o gli elementi che appartengono al secondo insieme.

L'*intersezione* di due insiemi consiste nel creare un insieme che contiene gli elementi che appartengono contemporaneamente al primo e al secondo insieme.

La *differenza* di due insiemi consiste nel creare un insieme che contiene gli elementi che appartengono al primo insieme ma non appartengono al secondo insieme.

Il *complemento* di un insieme contenuto in un *insieme universo* è quell'insieme che contiene tutti gli elementi dell'insieme universo e che non appartengono all'insieme da complementare.

Cos'è *l'insieme universo*?

L'insieme universo non è l'insieme che contiene tutti gli insiemi (*antinomia*!), bensì è un insieme che contiene alcuni insiemi.

Cos'è *l'insieme potenza*?

L'insieme potenza è l'insieme di tutti i sottoinsiemi di un insieme e possiede 2^n elementi, dove n è il numero di elementi dell'insieme di cui si vuole calcolare l'insieme potenza.

Cos'è il prodotto cartesiano di due insiemi?

Per parlare del prodotto cartesiano di due insiemi dobbiamo andare oltre il concetto di insieme e introdurre il concetto di *coppia ordinata* (che comunque può essere ricavato dal concetto di insieme).

La differenza tra insieme e in generale una *n-pla (tupla)* è che nella *n-ple* si tiene conto dell'ordine.

Quando si fa il *prodotto cartesiano di due insiemi* pertanto si crea un insieme in cui gli elementi sono tutte quelle coppie ordinate che hanno come primo elemento un elemento del primo insieme e come secondo elemento un elemento del secondo insieme.

La *proiezione* di un sottoinsieme del prodotto cartesiano di due insiemi su uno dei due insiemi sono tutti quegli elementi che sono presenti nelle coppie ordinate del sottoinsieme nella rispettiva posizione dedicata all'insieme.

Capitolo 2

Cos'è una *relazione*?

Una *relazione* è il sottoinsieme di un prodotto cartesiano tra due insiemi. La relazione è esplicitata attraverso una qualche *proprietà o legge*. Quando si considera i due elementi presenti nelle coppie ordinate della relazione si dice semplicemente che il primo elemento è in relazione col secondo.

Si dice *relazione inversa* quella relazione ottenuta invertendo l'ordine delle coppie.

Quali sono le proprietà di una relazione tra un insieme e sé stesso?

Una relazione si dice *riflessiva* se ogni elemento è in relazione con sé stesso. Una relazione si dice *antiriflessiva* se ogni elemento non è in relazione con sé stesso.

Una relazione si dice *simmetrica* se, per ogni coppia di elementi in cui a è in relazione con b, b è in relazione con a. Una relazione si dice *antisimmetrica* se, quando a è in relazione con b e b è in relazione con a, allora a = b.

Una relazione si dice *transitiva* se quando a è in relazione con b e b è in relazione con c, allora a è in relazione con c. Data una relazione R non transitiva si può sempre costruire una "minima" relazione transitiva completando R e che equivale all'intersezione tra tutte le possibili relazioni transitive che contengono R. Questa relazione minima transitiva si chiama *chiusura transitiva di R.*

Quali sono i tipi notevoli di relazione?

Una relazione si dice di *equivalenza* se gode delle proprietà riflessiva, simmetrica e transitiva.

Si dice *classe di equivalenza* dell'elemento a appartenente al dominio della relazione di equivalenza il suo sottoinsieme contenente tutti gli elementi x tali che (a,x) appartiene alla relazione.

Siano a e b due elementi. Se le due classi di equivalenza sono distinte, allora sono *disgiunte* (non hanno alcun elemento in comune).

Si dice *insieme quoziente o partizione* dell'insieme di definizione di una relazione di equivalenza l'insieme di tutte le classi di equivalenza rispetto alla relazione stessa.

Una relazione si dice di *ordine* se gode delle proprietà riflessiva, antisimmetrica e transitiva.

Una relazione si dice di *ordine totale o largo* se ogni elemento dell'insieme di definizione è in relazione con ogni altro elemento del dominio o viceversa, altrimenti è detta di *ordine parziale o stretto*.

Una relazione di ordine parziale può essere rappresentata con i *diagrammi di Hasse*, in cui viene indicato l'orientamento della relazione dal basso verso l'alto e gli elementi vengono collegati da una freccia che indica la presenza di una relazione tra essi, e le frecce riflessive e transitive non vengono scritte perché si deducono.

Una relazione si dice di *preordine* se gode delle proprietà riflessiva e transitiva.

Dato un insieme **X** e una relazione d'ordine R, esistono sempre:

- un *massimo* x1, per ogni x, xRx1;
- un *minimo* x0, per ogni x, x0Rx
- un *massimo comune minorante*;
- un *minimo comune maggiorante*.

Cos'è una *immersione* tra ordini?

Sia R un ordine parziale su un insieme X e sia R* un ordine parziale su un insieme X*. Una funzione X->X* è una *immersione* tra due ordini se è iniettiva e se f(x) R* f(y) = x R y.

Sia X un insieme e R una relazione d'ordine. Esiste sempre una immersione in P(X) ordinata per inclusione.

Sotto-successioni monotone.

Sia n>=1. Data una successione di n^2+1 elementi distinti scelti su un insieme X su cui vale una relazione d'ordine totale, allora esiste sempre una sotto-successione strettamente crescente lunga n+1 oppure una sotto-successione strettamente decrescente lunga n+1.

Capitolo 3

Cos'è una *funzione*?

Le *funzioni* sono relazioni tra gli elementi di un insieme **D** e un insieme **C** tali che ad ogni elemento dell'insieme **D** corrisponda esattamente un elemento di **C**. Il primo insieme, **D**, si dice *dominio* e il secondo insieme, **C**, si dice *codominio*. Ad ogni elemento del dominio è associata un'unica *immagine* del codominio.

Data la funzione **D** -> **C**, l'insieme **Im (D)**, chiamato *insieme delle immagini* di **D**, è il sottoinsieme dell'insieme **C** costituito dalle immagini degli elementi di **D** nella funzione.

Quali sono i tipi di funzione?

Una funzione si dice *suriettiva* se ad ogni elemento del codominio è associato almeno un elemento del dominio.

Una funzione si dice *iniettiva* se ad ogni elemento del codominio è associato un unico elemento del dominio.

Una funzione si dice *biiettiva* se è sia suriettiva che iniettiva.

Cos'è e quali sono le proprietà della composizione di funzioni?

Date due funzioni f: **A**-> **B** e g: **B**-> **C**, si dice *funzione composta* la funzione g(f(x)) che ad ogni elemento di **A** fa corrispondere un elemento di g(f(x)). Se g ed f sono funzioni iniettive (suriettive/ biiettive) allora, se esiste, anche la loro composta è iniettiva (suriettiva/biiettiva).

Se g(f(x)) è una funzione iniettiva, allora f deve essere iniettiva e g può anche non esserlo.

Se g(f(x)) è una funzione suriettiva, allora g deve essere suriettiva e f può anche non esserlo.

Date due funzioni distinte g: X-> Y e h: X-> Y, f(g(x)) = f(h(x)), f non può essere iniettiva poiché le due funzioni sono distinte e dev'esserci almeno un elemento che ha una *contro-immagine* diversa.

Cos'è una funzione parziale?

Una *funzione parzia*le è una funzione definita su un sottoinsieme del loro dominio. Questo sottoinsieme viene chiamato *dominio (o insieme) di definizione*. Il dominio di una funzione composta pertanto potrebbe essere più piccolo dell'originale se alcuni degli elementi del codominio della prima funzione fanno parte del dominio della seconda funzione.

Quali sono i tipi notevoli di funzione?

Si dice *identità* su A una funzione che associa ad ogni elemento di A sé stesso.

Una funzione si dice *invertibile* quando anche la sua relazione inversa rispetta la definizione di funzione, ossia quando la funzione è biiettiva.

Capitolo 4

Quando due insiemi si dicono equipotenti?

Due insiemi si dicono *equipotenti* quando esiste una funzione biiettiva tra loro. La nozione di equivalenza esprime in maniera rigorosa quello che diciamo quando intuitivamente intendiamo dicendo che due insiemi hanno lo stesso numero di elementi, generalizzandola e rinunciando alle limitazioni che questa definizione presenta nei casi in cui si parla di equipotenza di insiemi infiniti.

Un insieme si dice *infinito* se è equipotente ad un suo sottoinsieme proprio. Un insieme si dice *finito* se non è equipotente ad alcun suo sottoinsieme proprio.

Che tipo di relazione è la relazione di equipotenza?

La relazione di equipotenza è una relazione di equivalenza. Considerando l'insieme quoziente di tale relazione di equipotenza su insieme finito, ogni classe di equivalenza conterrà tutti quegli insiemi che contengono lo stesso numero di elementi (n). Si dice che ogni insieme che appartiene alla classe di equivalenza in questione ha *potenza* (o *cardinalità*) n.

Si può anche introdurre una relazione d'ordine **#D** <= **#E** tra due insiemi dicendo che **D** è equipotente ad un sottoinsieme di **E**.

Cosa significa *potenza del numerabile*?

Si dice che un insieme ha la *potenza del numerabile* se esiste una biiezione tra quell'insieme e l'insieme dei numeri naturali. L'insieme dei numeri interi e quello dei numeri razionali hanno la potenza del numerabile, nonostante tra due naturali esistano infiniti razionali.

Cosa significa *potenza del continuo*?

Secondo *Cantor*, R non ha la potenza del numerabile. Si dice infatti che l'insieme dei numeri reali abbia la *potenza del continuo*.

Attraverso una costruzione geometrica (una proiezione), possiamo dimostrare che l'insieme dei numeri reali è equipotente all'intervallo aperto (0,1) in R. Anche l'insieme delle parti di N è equipotente ad R.

Un insieme equipotente a R si dice avere la *potenza del continuo*.

Cosa dice l'*ipotesi del continuo*?

Indichiamo con *Aleph null* (o *aleph con zero*) la potenza del numerabile e con 2 elevato ad Aleph null la potenza del continuo. Questi numeri sono detti *numeri transfiniti*. Esistono infiniti numeri transfiniti.

L'ipotesi che ogni sottoinsieme di R che non ha la potenza del continuo abbia la potenza del numerabile è detta *ipotesi del continuo*, ed equivale a negare che non esistano transfiniti intermedi tra la potenza del numerabile e quella del continuo. *Cohen* dimostrò che l'ipotesi del continuo appartiene ad una serie di questioni *indecidibili*, cioè impossibili da negare o dimostrare.

Cosa dice il *Teorema di Cantor*?

Il *Teorema di Cantor* dice che non esiste una funzione biiettiva tra A e il suo insieme potenza, quindi non possono essere in equipotenza. Questo perché gli elementi dell'insieme potenza di A sono superiori di numero a quelli di A, rendendo impossibile la presenza di una suriezione.

Se ne deduce quindi che la cardinalità dell'insieme A è sempre minore della cardinalità dell'insieme potenza di A, qualunque sia A.

Il *Teorema di Cantor-Bernstein* dice che se esiste una iniezione tra A e B ed esiste una iniezione tra B ed A, allora esiste anche una biiezione tra A e B.

Cos'è un'antinomia?

Si dice antinomia, da anti (contro) e nomos (legge), una contraddizione, ad esempio una proposizione che risulta essere vera e falsa contemporaneamente. Si distingue dal *paradosso* perché, a differenza di esso, un'antinomia non può essere dimostrata.

Una delle più celebri antinomie è l'*antinomia del mentitore*, detta di Epimenide.

Prima della pubblicazione della seconda parte della grande opera logica *Aritmetica di Frege*, Russell rilevò una contraddizione nel capolavoro del logico tedesco che venne chiamata *antinomia di Russell* o *antinomia degli insiemi normali*.

Veniva definito *insieme normale* un insieme che non conteneva sé stesso come elemento.

Consideriamo *l'insieme N avente per gli elementi tutti e soltanto gli insiemi normali*: N contiene sé stesso? Se sì, allora N non è un insieme normale e quindi non è vero che contiene soltanto insiemi normali (perché contiene sé stesso); se no, allora N è un insieme normale e quindi dovrebbe contenere sé stesso.

Capitolo 5

Come è cambiato nel tempo il metodo di definire i numeri naturali?

Già dall'antichità si parlava di *serie dei numeri naturali*. Nell'antichità classica però, non si pose il problema di definire in maniera rigorosa i numeri naturali, poiché essi avevano uno *status metafisico* che li rendeva più reali degli oggetti fisici.

Nel Medioevo si volle abbandonare questa visione si cercò di dare una prima definizione della serie naturale vedendo i numeri come termini di un linguaggio. *Campano Da Novara* fu il primo che definì la serie naturale dei numeri quella per la quale il calcolo dei numeri avviene aggiungendo *un'unità*.

Aggiunse poi che:

- di ogni numero si possono prendere quante copie o multipli si vuole;
- la serie dei numeri continua all'infinito;
- non si può diminuire un numero all'infinito (forma primitiva del *buon ordinamento*).

In questa definizione manca però il concetto secondo il quale la serie dei numeri naturali parte sempre dallo stesso numero, concetto molto importante ma che contemporaneamente rappresenta un livello di rigore impensabile per l'epoca.

Le *teorie di Boole e Cantor* e le ricerche logico-matematiche di *Frege* alla fine del XIX secolo rendono più rigoroso l'intero mondo matematico. Nell'*Aritmetica di Frege* si trova la definizione fondamentale di numero, dove fa corrispondere il numero "*zero*" ad una condizione *impossibile*, a qualcosa che è diverso da sé stesso. Poi introduce ricorsivamente tutti gli altri numeri, ciascuno basato sul precedente.

Giuseppe Peano poi introduce una sua prima definizione di serie naturale in *Sul concetto di numero*, basata su tre concetti primitivi, *l'unità*, il *numero* e il *successivo*, e sei postulati. L'unità verrà sostituita dallo *zero* nella sua ultima definizione in *Aritmetica* del suo *Formulario di Matematica*.

I tre concetti primitivi sono:

- lo zero;
- il numero;
- il successivo.

I sei assiomi sono:

0) I numeri formano una classe (un insieme);
1) Lo zero è un numero;
2) Se a è un numero, anche il suo successivo è un numero;
3) Se **S** è una classe contenete lo zero, e per ogni a di **S**, il suo successivo appartiene ad **S**, allora ogni numero naturale è in **S** (*principio di induzione*);
4) Se a e b sono due numeri e i loro successivi sono uguali, allora a e b sono uguali;
5) Se a è un numero, allora il suo successivo non è zero.

La relazione *successivo* è dunque una funzione.

Peano usò questo principio anche per definire le operazioni sui numeri naturali.

Cos'è il *principio di induzione*?

Il *principio di induzione* è un principio che ci permette di dimostrare alcune proprietà per successioni infinite di numeri.

Esistono due tipi di proprietà: quelle che sono molto simili dimostrate tra un numero e l'altro e quelle che cambiamo completamente (vedere quelle dei numeri primi). Il principio di induzione si occupa di dimostrare proprio le prime.

Il *principio di induzione* afferma che se una proprietà vale per il primo numero, e, se vale per un numero vale anche per il successivo, allora vale per tutti i numeri naturali. Il principio di induzione è basato sull'assioma tre di Peano.

La permanenza dello schema permette di ridurre gli infiniti passaggi a due, ossia:

- Si dimostra la proprietà per il passo base;
- Si dimostra la proprietà per il passo induttivo.

Il principio di induzione può essere usato, oltre che per dare dimostrazioni, anche per dare definizioni.

Il *principio del buon ordinamento* o *principio del minimo numero*, equivalente al principio di induzione, è il principio secondo il quale ogni insieme non vuoto di interi non-negativi possiede un elemento minimo.

I passaggi per utilizzare il principio del minimo numero sono:

1) Negare la tesi;
2) Definire l'insieme dei controesempi;
3) Verificare che il minimo non può essere il minimo della tesi e quindi che non appartiene all'insieme dei controesempi;
4) Verificare che neanche il numero precedente appartiene all'insieme dei controesempi.

Cosa sono il principio di *induzione forte* e il principio di *induzione strutturale*?

Il principio di *induzione completa* o *induzione forte* dice che se una proprietà è dimostrata per il minimo e per tutti i valori minori di un certo numero, allora è dimostrata anche per quel numero e per i successivi.

Solitamente si utilizza quando c'è una chiamata ricorsiva a valori precedenti che non sono distanti necessariamente un'unità.

Il principio di *induzione strutturale* invece è una generalizzazione del principio di induzione normale, che viene applicato però a delle strutture (come insiemi, grafi, alberi, linguaggi) che sono scomponibili in oggetti più semplici. Questo principio può fornire definizioni o dimostrazioni solitamente lavorando non sulle strutture stesse ma su indici associati a certe proprietà delle strutture.

Il principio di induzione strutturale funziona come quello normale ma aggiunge la clausola che "nessun altro elemento appartiene alla struttura".

Quali sono alcune proprietà dei numeri naturali?

Un'importante proprietà dei numeri naturali è la divisibilità.

Il *teorema del resto euclideo* dice che il dividendo = divisore * quoziente + resto. Si dice che il divisore divide il dividendo o che il dividendo è divisibile per il divisore.

Per il principio di induzione, prima o poi il processo di ottenere divisori termina, pertanto ogni numero ha un numero finito di divisori.

Due numeri si dicono *congruenti modulo* m se divisi per m danno lo stesso resto. La congruenza modulo m è una relazione di equivalenza. Le equivalenze tra le classi di equivalenza della relazione di congruenza vengono chiamate *congruenze*.

Quali sono le principali nozioni legate ai numeri primi?

Un naturale a si dice *divisibile* per un naturale b se esiste un naturale c tale che a = b * c. Si dice allora che b è un divisore di a.

Il naturale p si dice *primo* se è maggiore di 1 ed è divisibile solo per 1 e per se stesso. Un naturale maggiore di 1 non primo si dice *composto*.

Il *crivello di Eratostene* dice che, per trovare tutti i numeri primi minori di un certo numero n >= 2 bisogna guardare il primo numero, vedere se è primo e sé si eliminare tutti i suoi multipli, e continuare così per tutti gli altri numeri fino a sqrt(n)

Ogni numero naturale maggiore di 1 è un prodotto di numeri primi.

La scomposizione in fattori primi di un numero naturale è unica, a meno di permutazioni di fattori.

I numeri primi sono sempre più di ogni assegnata quantità di primi.

Il *Piccolo Teorema di Fermat* dice che se p è un numero primo, allora ap – a deve essere multiplo di p, qualunque sia a (condizione necessaria ma non sufficiente).

Il *teorema di Wilson* che utilizza le congruenze e la *formula di Willans* che espande quella di Wilson sono alcune condizioni necessarie e sufficienti per calcolare numeri primi.

Alcuni problemi aperti sui numeri primi sono la *congettura di Goldbach* (tutti i numeri pari maggiori di 2 sono somme di due numeri primi non necessariamente distinti) e la *congettura dei primi gemelli* (che dice che esistono infinite coppie di primi detti gemelli, ossia tali che dato p esiste anche p+2).

Esiste una forte *asimmetria tra addizione e moltiplicazione*, poiché mentre nella somma esiste un unico elemento atomico (1), nella moltiplicazione ne esistono infiniti (i primi).

Capitolo 6

Quali sono le proprietà delle operazioni insiemistiche?

Le proprietà delle operazioni insiemistiche sono:

- *Commutatività* dell'unione e dell'intersezione;
- *Associatività* dell'unione e dell'intersezione;
- *Distributività* dell'unione e dell'intersezione;
- *Elementi neutri* dell'unione e dell'intersezione;

- *Elementi annullatori* dell'unione e dell'intersezione;
- *Idempotenza* dell'unione e dell'intersezione.

Cos'è l'algebra di Boole?

L'*algebra di Boole* è un'algebra sviluppata da Boole per risolvere problemi di logica. Più precisamente, l'algebra di Boole è una sestupla composta da (B, intersezione, unione, complemento, insieme vuoto, insieme universo).

Per ogni insieme X, se esiste un'algebra di Boole in X, esiste anche in P(X).

Nell'algebra di Boole sono valide le leggi di *De Morgan*.

Per ogni elemento dell'algebra di Boole esiste un unico complemento.

Una delle più importanti applicazioni della teoria delle algebre di Boole è quella dei circuiti (elettrici o meno, *Claude Shannon*). La caratteristica di questi circuiti dev'essere la presenza di soli due valori, aperto o chiuso.

I connettivi logici possono essere usati anche nei circuiti sotto forma di circuiti elementari detti "porte logiche" (*composizione in serie o parallelo*).

Capitolo 7

Parli della formalizzazione matematica.

Dal XIX secolo in poi assistiamo ad un grande sviluppo dell'aspetto della formalizzazione di diversi linguaggi, tra cui quelli della teoria degli insiemi, dei numeri e delle algebre di Boole.

Qui ritroviamo i due oggetti principali di formalizzazione: il *calcolo* ed il *linguaggio*.

In maniera più rigorosa diciamo che noi stiamo costruendo una *sintassi* (cioè un insieme di regole per la manipolazione dei termini) alla quale deve corrispondere una *semantica* (cioè quello che intendiamo quando interpretiamo la sintassi).

È importante che se uno schema sintattico viene accettato allora tutte le sue interpretazioni dovranno essere vere (*correttezza*), e viceversa che se una certa interpretazione è vera allora il sistema sintattico dovrà essere in grado di rappresentarla (*completezza*).

Mentre la prima è fondamentale, la seconda è meno importante.

Ci troviamo di fronte a due tipi di calcolo diversi: quello degli *enunciati-connettivi* e quello dei *predicati-quantificatori*.

Capitolo 8

Quali sono le caratteristiche fondamentali della logica?

La logica viene utilizzata per parlare di cose che hanno solo due possibili valori di verità: vero o falso. Le dimostrazioni logiche riguardano fatti più o meno evidenti o plausibili, ma riguardano comunque fatti veri: con l'attribuzione di un valore bivalente alla verità si vuole intendere che l'espressione in questione è oggettiva e può essere stabilita senza dubbio.

Si sono provate diverse interpretazioni per poter dare un significato al concetto di verità.

Oggi, per dare una definizione al concetto di verità usiamo un linguaggio detto formalizzato, ossia caratterizzato da precise regole sintattiche.

Come si definisce un linguaggio proposizionale?

Un *linguaggio proposizionale* è un insieme L di simboli contenente:

- i simboli detti connettivi logici;
- le parentesi tonde chiuse o aperte;
- una quantità finita o infinita numerabile di simboli dette variabili proposizionali, VAR di L.

Sia L un linguaggio proposizionale. L'insieme delle proposizioni ben formate in L è il minimo insieme X di stringhe che contiene:

- tutte le variabili proposizionali in L;
- se A è in X, allora anche not A è in X;
- se A e B sono in X, allora anche A (connettivo logico) B sono in X.

Questo insieme di proposizioni viene chiamato *PROP* di L, ed è il minimo insieme di proposizioni poiché facendo l'intersezione di tutti i possibili *insiemi chiusi* (che soddisfano le tre condizioni elencate in precedenza) otteniamo l'insieme chiuso più piccolo.

Una proposizione B si *dice sotto-formula* di una proposizione A se è verificato che:

- A è identica a B;
- A è not C e B è sotto-formula di C;
- A è C (connettivo logico) D e B è sotto-formula di C o D.

Il principio di induzione strutturale può essere usato per definire delle proprietà su un linguaggio proposizionale. Un linguaggio proposizionale soddisfa la proprietà P se:

- P vale per tutte le variabili proposizionali;
- se P vale per A allora P vale anche per not A;
- se P vale per A e B allora vale anche per A (connettivo logico) B.

Questo avviene perché l'insieme che si ottiene da queste proprietà è un insieme chiuso, pertanto PROP di L è sottoinsieme di questo.

Un linguaggio proposizionale può essere definito anche ricorsivamente in base alla sua "altezza".

Cos'è una *proposizione*?

Una *proposizione* o *enunciato* è un'affermazione che assume uno ed un solo *valore di verità*, o vero o falso. Enunciati costituiti da una sola affermazione sono detti *enunciati atomici*.

Nella logica degli enunciati si prescinde dalla "*struttura interna*" delle affermazioni. Nonostante si esamini la struttura degli enunciati, gli enunciati atomici non sono gli unici ad essere presi in considerazione. Chiamiamo infatti *enunciati complessi* quegli enunciati che sono costituti da più enunciati collegati da alcuni *connettivi*.

Cosa sono i *connettivi*?

I *connettivi* formalizzano alcune parole e sono indicati da opportuni simboli (and, or, not, implicazione *materiale* e doppia implicazione). Talvolta, "not" viene indicato come operatore e non come connettivo.

Grazie ai connettivi è possibile definire induttivamente l'insieme degli enunciati partendo da un alfabeto costituito da lettere minuscole (enunciati atomici) e utilizzando poi su di essi i connettivi, parentesi e virgole.

Cos'è una *interpretazione*?

Chiameremo *interpretazione* o *assegnamento* di un enunciato composto una funzione v che assegna uno dei due valori di verità ai singoli enunciati atomici e che ne deriva il valore di verità all'enunciato

composto sulla base dei valori definiti nelle funzioni di verità dei vari connettivi, o più brevemente delle *tavole di verità* dei connettivi utilizzati.

v: VAR -> {0,1}

v': PROP -> {0,1}

Due enunciati si dicono *logicamente equivalenti* se per ogni assegnamento assumono lo stesso valore di verità.

Una relazione di equivalenza logia è una relazione di equivalenza che gode delle seguenti proprietà:

- A equivale logicamente a sé stesso (riflessività);
- Se B equivale logicamente a A e C equivale logicamente a B, allora C equivale logicamente ad A (transitività);
- Se A equivale a B allora B equivale ad A;
- Se A equivale a B allora per ogni assegnamento A implica B e B implica A.

Sia F un insieme di proposizioni e A una proposizione. Si dice che A è *conseguenza logica* di F se ogni assegnamento che mette a vero tutti gli elementi F soddisfa anche A. Si dice anche che F *implica logicamente* A. Se F è insieme vuoto allora diciamo che A è soddisfatta da tutti gli assegnamenti, perché è vero a vuoto.

Una relazione di *conseguenza logica* gode delle seguenti proprietà:

- A è conseguenza logica di sé stesso (riflessività);
- Se B è conseguenza logica di A e C è conseguenza logica di B, allora C è conseguenza logica di A (transitività);
- Se B è conseguenza logica di A allora per ogni assegnamento A implica B.

Un enunciato si dice *soddisfacibile* se esiste *(concetto esistenziale)* almeno un assegnamento per il quale l'enunciato assume valore di verità vero. Altrimenti si dice che l'enunciato è *insoddisfacibile*.

Un enunciato che assume valore di verità vero per ogni assegnamento *(concetto universale)* si dice *valido* o *tautologia.*

Le tautologie della logica degli enunciati sono verità nel linguaggio oggetto ma spesso vengono anche assunte come principi del metalinguaggio, come il principio del terzo escluso ("un'affermazione o la sua negazione devono essere per forza vere"), il principio di non contraddizione ("un'affermazione e la sua negazione non possono essere contemporaneamente vere").

Dato un insieme di proposizioni A1, A2… An, A, dire che A è conseguenza logica di A1, A2... An equivale a dire che l'implicazione tra l'AND delle proposizioni A1,A2...An e A è TAUT e che l'AND tra le proposizioni A1, A2…An in AND con la negazione di A è UNSAT.

Il metodo delle tavole di verità è computazionalmente *inefficiente*, questo perché ad ogni variabile sono associati due possibili valori di verità e questo porta ad un aumento esponenziale delle operazioni. Non si conoscono algoritmi efficienti (polinomiali) per verificare che una certa proposizione A sia TAUT o per risolvere problemi logici complessi (trovarlo significa risolvere il problema *P = NP* del Clay Mathematical Institute, problema del millennio). Sono però nati dei metodi un po' più veloci per verificare se una certa proposizione è TAUT oppure no.

Cosa dicono i teoremi di sostituzione?

- se A è una tautologia, se sostituisco in A una variabile proposizionale con una formula qualunque ottengo ancora una TAUT;
- se A e B sono equivalenti, e sostituisco in A e B una stessa variabile proposizionale con una stessa formula qualunque, ottengo ancora una TAUT;

- se sostituisco in una stessa formula A una variabile proposizionale con due formule equivalenti, ottengo due formule equivalenti.

Cosa dice il principio di dualità?

Il *principio di dualità* dice che se sostituiamo agli 0 gli 1 e viceversa e gli AND con gli OR e viceversa, allora si ottiene un enunciato duale altrettanto corretto. Questo prevede anche la sostituzione di TAUT con UNSAT e UNSAT con TAUT. Il principio di dualità è corretto perché gli assiomi dell'algebra di Boole sono duali.

Che tipo di proposizioni possono essere formalizzate in logica proposizionale?

- argomenti matematici che non riguardano quantificatori;
- semplici argomenti verbali;
- principi combinatori su domini finiti.

Cos'è una *forma normale*?

Chiamiamo *letterale* ogni variabile proposizionale e ogni sua negazione. A è in *Forma Normale Congiuntiva* (CNF) se A è una congiunzione di disgiunzioni di letterali. A è in *Forma Normale Disgiuntiva* (DNF) se A è una disgiunzione di congiunzioni di letterali.

Per ogni proposizione A esistono una CNF e una DNF logicamente equivalenti.

Una CNF è una *tautologia* se e solo se tutti i suoi congiunti sono tautologie.

Una DNF è una *insoddisfacibile* se e solo se tutti i suo0i disgiunto sono insoddisfacibili.

Algoritmo per passare da CNF a DNF e viceversa.

1) si eliminano i connettivi implicazione e doppia implicazione;
2) si spingono le negazioni all'interno (anche usando De Morgan);
3) si sostituisce And con * e OR con + o viceversa;
4) si sviluppa usando la legge di distributività;
5) si risostituisce.

Trovare se una formula è SAT o UNSAT

Cosa dice *l'algoritmo di Davis e Putnam* per il calcolo della soddisfacibilità?

L'*algoritmo di Davis e Putnam* si mette nella posizione più difficile per risolvere il problema F appartiene a SAT, poiché partendo da una CNF dobbiamo decidere se essa è SAT o UNSAT.

Nella CNF, ogni disgiunzione di letterali è detta *clausola*. Rappresentiamo ogni clausola come l'insieme dei suoi letterali, e la formula come insieme di ogni clausola.

Indichiamo la clausola vuota come UNSAT e la formula vuota come SAT. Se una formula contiene una clausola vuota allora è UNSAT. Come prerequisito, le formule in questo metodo non possono contenere clausole tautologiche (vanno eleminate).

Definiamo una clausola *l-positiva* se contiene occorrenze positive di l. Definiamo una clausola *l-negativa* se contiene occorrenze negative di l. Definiamo una clausola *l-neutra* se non contiene l (positive o negative).

POS-l di una formula è l'insieme delle clausole l-neutre più quelle l-positive. NEG-l di una formula è l'insieme delle clausole l-neutre più quelle l-negative.

Il *teorema dello splitting* dice che, sia F in CNF e l un letterale, allora F è SAT se e solo se POS di l è SAT o NEG di l è SAT.

La *PURE LITERAL RULE* dice che, se F non contiene occorrenze negative del letterale l, allora per definizione ho che NEG di l di F ha solo clausole l-neutre, quindi basta dimostrare che NEG di sia SAT.

La *UNIT RULE* dice che, se F contiene clausole che contengono solo un letterale l, dato che {l} – {l} è clausola vuota, allora POS di l non può essere SAT. Dunque basta controllare che NEG di l sia SAT.

Il *metodo della risoluzione* dice che, date due clausole che contengono una un letterale positivo e l'altro un letterale negativo, la sua derivazione è l'unione tra le due clausole senza meno i due letterali.

L'algoritmo per SAT consiste nell'applicare la PURE LITERAL RULE, la UNIT RULE e poi il metodo di risoluzione a ripetizione.

Il metodo di risoluzione è *corretto* (perché possiamo ricavare effettivamente se una formula è UNSAT applicandolo) e *completo* (perché se abbiamo una formula UNSAT allora possiamo scoprirlo con il metodo di risoluzione).

Capitolo 9

Cos'è la logica dei predicati e qual è la differenza con la logica proposizionale?

La *logica dei predicati* si presenta come un'estensione della logica proposizionale: infatti essa presenta tutte le caratteristiche della logica proposizionale, però introduce un'analisi della struttura interna delle proposizioni, in cui si distinguono *gli individui dai concetti astratti* che essi rappresentano (*proprietà*).

La logica dei predicati infatti propone una formalizzazione che è in grado di lavorare più efficacemente con insiemi molto grandi ed è in grado di lavorare anche con insiemi infiniti, oppure insiemi dinamici, ossia che cambiano nel tempo: è ovvio che quando abbiamo a che fare con un insieme che si modifica nel tempo (come la popolazione terrestre), non vogliamo ogni volta che la popolazione cambia sistemare le nostre dimostrazioni. È proprio qui che entra in gioco l'astrazione dei concetti tipica della logica dei predicati.

La logica predicativa ci permette di introdurre il concetto di *quantificatore*, che ci permette di distinguere il soggetto singolo da una certa quantità di soggetti che soddisfano una determinata caratteristica.
All'interno delle *formule atomiche* del nostro linguaggio si vanno ad analizzare anche gli individui dei quali si predica qualcosa ed i predicati stessi. Gli individui prendono il nome di *termini* del linguaggio, e sono *variabili*, *costanti* e *funzioni* (ad uno o più posti). I predicati prendono invece il nome di *formule*.

Come è composto l'alfabeto della logica proposizionale?

L'alfabeto della logica proposizionale è composto da:

- simboli per variabili, indicati con lettere minuscole ed eventualmente indici;
- simboli per costamti, indicati con lettere minuscole ed eventualmente indici;
- simboli funzionali a uno o più posti denotati sempre da lettere minuscole ed eventualmente indici;
- simboli predicativi (simboli di relazioni) a uno o più posti denotati da lettere maiuscole ed eventualmente indici;
- i connettivi logici not, and, or, implicazione, doppia implicazione;
- i quantificatori "per ogni" ed "esiste;
- parentesi e virgole.

Assumiamo un insieme numerabile di variabili.

I *termini* di un linguaggio per la logica dei predicati sono definiti induttivamente:

- variabili e costanti sono termini;
- se t1,..,tn sono termini ed f ha n posti, f(t1,..tn) è un termie;

Le *formule* di un linguaggio per la logica dei predicati sono definite induttivamente:

- se P ha n posti e t1,..,tn sono termini, allora P(t1,..,tn) è una formula (atomica);
- se A è una formula, allora anche la sua negazione è una formula.
- se A e B sono formule, allora anche A (connettivo) B sono formule;
- se A è una formula, allora anche per ogni x A ed esiste x A sono formule.

Cosa sono i *quantificatori*?

I quantificatori sono un metodo che usiamo per riferirci ad una quantità notevole di individui che soddisfano una determinata proprietà.

Esistono due tipi di quantificatori: il quantificatore esistenziale, che garantisca l'esistenza di almeno un elemento della classe considerata che verifichi una proprietà data; il quantificatore universale, che garantisce che tutti gli elementi della classe considerata verifichino una proprietà data.

Come calcolare la veridicità di un predicato?

Per calcolare se un predicato assume valore di verità vero o falso dobbiamo prima dare un'interpretazione agli elementi che lo compongono (variabili, funzioni, relazioni), al suo ambiente. Questa interpretazione prende il nome di *struttura*.

Soltanto una volta che si decide la struttura si può calcolare la veridicità di un predicato. Data una formula F, una struttura è fatta da:

- un dominio non vuoto D;
- una relazione n-aria su D;
- una funzione n-aria su D;
- un elemento fissato in D per ogni simbolo di costante in F.

Data una struttura S, si dice che la formula è *soddisfacibile nella struttura* se esiste un assegnamento alle variabili libere che la mette a vero.

Data una struttura S, si dice che la formula è *vera nella struttura* se è soddisfatta per ogni assegnazione alle variabili libere.

Esistono casi di predicati che sono sempre veri in ogni struttura, e questo dovuto semplicemente alla loro struttura sintattica e alla semantica del linguaggio. Questi predicati prendono il nome di predicati *validi* e si dice la formula è *verità logica*.

Quali sono i tipi di variabili nei predicati?

L'ambito di un quantificatore è tutto ciò che è influenzato dal quantificatore stesso. Le variabili che si trovano subito dopo i quantificatori si dicono *vincolate o quantificate* nel quantificatore. Una variabile che non è vincolata o quantificata si dice libera.

Una stessa variabile può essere contemporaneamente libera e vincolata nella stessa formula in base all'ambito a cui ci si riferisce.

Una formula predicativa si dice *chiusa* se non ha variabili libere, *aperta* altrimenti.

Un *enunciato* è una formula senza variabili libere.

Un termine è liberamente sostituibile ad un altro termine se sostituendo in tutte le occorrenze di quel termine un altro termine qualsiasi allora nessuna variabile che prima non era quantificata risulti quantificata e viceversa.

Più in generale, un termine è liberamente sostituibile da una formula se il suo valore di verità non cambia dopo la sostituzione.