Insieme delle parti di A:

insieme i cui elementi sono TUTTI i sottoinsiemi di A

Funzione:

f: AxB | f(x)=y, f={<x,y> | per ogni x in A esiste unica y in B | f(x)=y}

f={<1,2>, <2,3>, <3,3>} : {1,2,3}→{1,2,3} | f(1)=2, f(2)=3, f(3)=3

Insieme immagine:

Im(f)={y in Y | esiste x in X : f(x)=y}

Composizione di funzioni:

f: X→Y, g: X→Z → g(f(x)):X→Z

Funzione invertibile:

f: X→Y, g: X→Z → g(f(x))=x e f(g(y))=y

f e` invertibile ↔ e` biiettiva

Cardinalita `:

A e B hanno la stessa cardinalita` se esiste una funzione biettiva da A in B.

Un insieme e` *numerabile se ha la stessa cardinalita `di N: se esiste f: A→N. Se A e B sono numerabili, AxB e `numerabile.*

Principio di induzione:

Sia P(n) una proposizione. Verifico

- P(a) true;
- P(n) true → P(n+1) true;

Relazione binaria:

Sia R un sottoinsieme di AxB → R e` detta relazione (binaria) tra A e B.

Relazione di equivalenza:

relazione riessiva, simmetrica e transitiva.

Relazione d'ordine:

relazione riessiva, antisimmetrica e transitiva.

Partizione:

P(x) e` una famiglia di sottoinsiemi di X non vuoti, mutuamente disgiunti, la cui unione e` TUTTO X

Classe di equivalenza:

sottoinsieme di X tale che [x]={y in X | xRy}

e.g.:

X={1,2,3,4}, R di equivalenza

R={<1,1>, <1,2>, <1,3>, <2,1>, <2,2>, <2,3>, <3,1>, <3,2>, <3,3>, <4,4>}

classi di equivalenza: [1]=[2]=[3]={1,2,3}, [4]={4}

[x]=[y] ↔ xRy

Minimali e massimali:

Sia X={2, 3, 4, 5, 6, 7, 8, 9, 10}:

elementi minimali: 2, 3, 5, 7

elementi massimali: 6, 7, 8, 9, 10 ← 4 non c'e`: divide 8, ed e` divisibile per 2

Numero primo:

Un numero si dice primo se e` divisibile solo per se stesso e per 1

Teorema fondamentale dell'aritmetica:

Per ogni intero n>1 esistono numeri primi pi (unici a meno dell'ordine) tali che *n=p1*p2*...*pt*

I numeri primi sono infiniti:

Se I numeri primi fossero in numero finito p1, p2, …, pn, allora il numero *N=p1p2….pn+1* sarebbe un intero privo di divisori primi, contro il *Teorema fondamentale dell'Aritmetica*.

Divisione con resto:

Esistono unici due interi, *quoziente* q e *resto* r, tali che *a=qb+r*, r<b

Massimo comun divisore:

Massimo numero che divide entrambi a e b in Z.

mcd(a,b)=ax+by (e.g. mcd(7007,1991) = 11 = 52*7007 – 183*1991)

Algebre di Boole

Operazione binaria:

BxB → B (e.g. RxR → R, (x,y) → x+y)

Operazione unaria:

B → B

Algebra di Boole:

insieme B dotato di 2 operazioni binarie ∧ (AND, *) e ∨ (OR, +), e di un'operazione unaria ¬ (NOT), tale che valgono le seguenti proprieta`:

- comutativita`
- distributivita`
- elementi neutri
- complemento

Morfismi di algebre di Boole:

Siano B e C algebre di Boole. Una funzione f: B → C e` detta *morfismo* se, per ogni x, y in B:

- $f(x) \vee f(y)=f(x \vee y)$
- $f(x) \wedge f(y)=f(x \wedge y)$
- $\neg f(x)=f(\neg x)$

Forma normale disgiuntiva:

somma unica di prodotti *completa* (prodotti in cui ci sono tutte le *indeterminate*).

Se p e` un prodotto ed f una *somma di prodotti*, p e` un *implicante primo* se implica f, ma ogni prodotto ottenuto da p cancellando una variabile non implica f. Ogni somma di prodotti e` equivalente alla somma di tutti I suoi implicanti primi.

Calcolo proposizionale

Logica proposizionale:

linguaggio formale con una semplice *struttura sintattica* basata su *proposizioni elementari* e su *connettivi logici* di tipo vero-funzionale che restituiscono il valore di verita` di una proposizione in base al valore di verita` delle proposizioni connesse.

Semantica:

definisce il *significato dei simboli* e di qualsiasi proposizione che rispetti le regole sintattiche del linguaggio.

Modello:

interpretazione di un insieme di proposizioni (associazione tra le proposizioni elementari) che permette di generare un insieme infinito di proposizioni con significato definito.

Struttura delle frasi (sintassi):

e` fondata su:

- un *alfabeto* di simboli
- un insieme di sequenze di simboli (*linguaggio*) definito tramite una *grammatica generativa*

Alfabeto:

costituito da:

- un insieme numerabile di *simboli*: p, q, r, ...
- simboli dei *connettivi logici*: ¬ , ∧, ∨, → (implicazione), ↔ (doppia impl.)
- *parentesi*: hanno lo scopo di evitare ambiguita`

Formule ben formate (wff in inglese):

espressioni "*sintatticamente corrette*", definite mediante la seguente *definizione ricorsiva*:

- un simbolo di proposizione e` una wff
- se A e` una wff, lo e` anche ¬A
- se A e B sono wff, lo sono anche (A∧B), (A∨B), (A→B), (A↔B)
- niente altro e` una wff

Funzione di valutazione:

funzione che va dall'insieme L delle wff nell'insieme {**T**,**F**} (true, false):

*v: L → {**T**,**F**}* tale che per ogni coppia di wff x e y valgono le seguenti condizioni:

- v(¬x)=**T** if v(x)=**F**; v(¬x)=**F** if v(x)=**T**
- v(x∧y)=**T** iff v(x)=**T** AND v(y)=**T**
- v(x∨y)=**T** iff v(x)=**T** OR v(y)=**T**
- v(x→y)=**T** iff v(x)=**F** OR v(y)=**T**
- v(x↔y)=**T** iff v(x)=v(y)

Tavola di verita `

P	***Q***	¬***Q***	***P*∧*Q***	***P*∨*Q***	***P*↔*Q***	***P*→*Q***
F	F	T	F	F	T	T
F	T	F	F	T	F	T
T	F	T	F	T	F	F
T	T	F	T	T	T	T

Soddisfacibilita`, tautologie e contraddizioni:

Una formula ben formata A si dice:

- *soddisfacibile*: se esiste una *valutazione* v tale che v(A)=**T**
- *contraddizione*: se non e` soddisfacibile ($p \wedge \neg p$)
- *tautologia*: se per ogni valutazione v si ha v(A)=**T** ($p \vee \neg p$)

Problema decidibile:

si puo` risolvere considerando *tutte le possibili combinazioni di valutazioni* sui simboli proposizionali e *calcolando il corrispondente valore di verita` della formula composta* sfruttando le proprieta` della funzione di valutazione.

Teorema di compattezza:

Un insieme di wff S e` soddisfacibile de e solo se ogni suo sottoinsieme finito e` soddisfacibile.

Definizioni:

Una formula ben formata A e`:

- *soddisfacibile*: se esiste una *interpretazione* I di A in cui A e` vera (in questo caso I si dice modello di A)
- *falsificabile*: se esiste una interpretazione I tale che A e` falsa (I e` contromodello di A)
- *valida*: se A e` vera *in ogni* interpretazione