Aniello Murano

Decidibilità delle teorie logiche

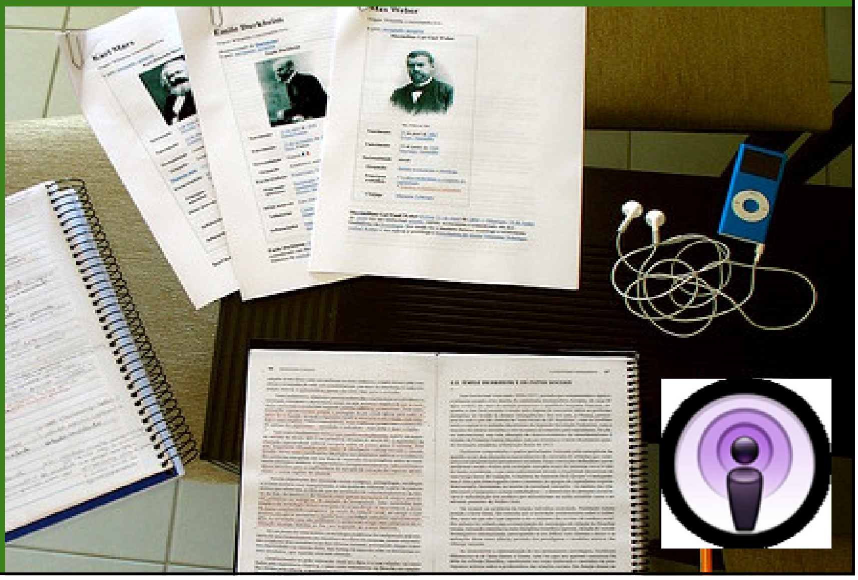
Lezione n.11
Parole chiave:
Teorie logiche

Corso di Laurea:
Informatica

Codice:

Email Docente:
murano@ na.infn.it

A.A. 2008-2009



Prefazione

- Nelle lezioni precedenti abbiamo trattato il concetto di decidibilià e indecidibilità nella teoria della computabilità.
- In questo contesto, possiamo dire che un insieme A è detto decidibile o ricorsivo se esiste un algoritmo che ricevuto in input un qualsiasi elemento, termina restituendo in output 0 o 1 a seconda che il valore appartenga o no all'insieme A.
- In questa lezione tratteremo la decidibilità e l'indecidibilità di teorie nella logica matematica.
- In particolare, concentreremo la nostra attenzione sul problema di determinare se affermazioni matematiche sono vere o false e investigheremo la decidibilità di questo problema.
- Si vedrà che la decidibilità dipende dal particolare dominio matematico in cui le affermazioni sono descritte.

Esempi di affermazioni matematiche

- Esempi di affermazioni matematiche sono i seguenti

$$\textbf{1. } \forall q\, \exists p\, \forall x,y\ \big[p>q \wedge (x,y>1 \rightarrow xy \neq p) \big],$$
$$\textbf{2. } \forall a,b,c,n\ \big[(a,b,c>0 \wedge n>2) \rightarrow a^n+b^n \neq c^n \big], \text{ and}$$
$$\textbf{3. } \forall q\, \exists p\, \forall x,y\ \big[p>q \wedge (x,y>1 \rightarrow (xy \neq p \wedge xy \neq p+2)) \big]$$

- La prima formula asserisce che esistono infiniti numeri primi. Questa affermazione è nota essere vera dal tempo di Euclide (più di 2300 anni fa).
- La seconda formula corrisponde all'ultimo teorema di Fermat che è stato dimostrato pochi anni fa ad opera di Andrew Wiles.
- La terza formula asserisce che esistono infinite coppie di numeri primi che differiscono di solo due unità. Questa è solo una congettura ed è tuttora non dimostrata ne confutata.
- **Nota:** Spiegheremo formalmente il loro significato nelle prossime diapositive…

Dalle logiche ai linguaggi

- Al fine di automatizzare il processo di determinazione di verità delle affermazioni matematiche è utile considerare queste affermazioni come stringhe e definire un linguaggio formato da tutte le affermazioni vere.
- Il problema della determinazione di verità delle affermazioni si riduce a alla decidibilità di questo linguaggio

Definizione del linguaggio

- Per la definizione del linguaggio si consideri il seguente alfabeto:

$$\{\wedge, \vee, \neg, (,), \forall, x, \exists, R_1, \ldots, R_k\}$$

  - $\wedge$, $\vee$, e $\neg$, corrispondo alle operazioni booleane and,or e not;
  - *"(" e* ")" sono le parentesi;
  - *\forall ed \exists* sono i quantificatori universale ed esistenziale;
  - x denota variabili;
  - R_1 , … , R_k sono *relazioni.*
- *Una formula è una stringa sull'alfabeto dato*
- Una stringa della forma $R_i(x_i, \ldots, x_j)$ *è una formula atomica.* Il valore j è l'arità della relazione R_i.
- Una formula (ben formata), (in breve fbf)
  1. è una formula atomica,
  2. è una combinazione booleana di altre formule più piccole
  3. è una quantificazione su altre formule f del tipo \exist x_i [f] oppure \forall x_i [f]
- Nota:I quantificatori legano le variabili all'interno del loro "scope" (parentesi quadre). Se una variabile non è legata in una formula allora la variabile è chiamata **libera**. Le formule senza variabili libere sono chiamate **sentenze** o ***statements***.

Logica del primo ordine(1)

Formule ben Formate:

- $R_1(x1) \wedge R_2(x1, x2, x3)$
- \forall $x_1[R_1(x_1) \wedge R(x_1, x_2, x_3)]$
- \forall x_1\exists x_2 \exists $x_3[R_1(x_1) \wedge R_2(x_1, x_2, x_3)]$

Osservazione: solo l'ultima fbf è una sentenza.

- L'ultima si legge, per ogni x_1 esistono x_2 e x_3 tali che $R_1(x_1)$ e $R_2(x_1, x_2, x_3)$ sono veri

Logica del primo ordine(2)

Costruendo tale sistema possiamo ragionare su sentenze del tipo

1. \forall q, \exists x, y[p>q ∧ (x,y>1 → xy ≠ p)]. (infiniti numeri primi)

2. \forall a, b, c, n[(a,b,c>0 ∧ n>2) → a^n + b^n ≠ cn]. (ultimo teorema di Fermat)

3. \forall q \exists p \forall x, y[p>q ∧ (x,y>1 → (xy ≠ p ∧ xy ≠ p+2))].
   (congettura sui numeri primi gemelli)

Logica del primo ordine(3)

- Per avere senso, una logica ha bisogno che le venga assegnato un significato. Per fare questo, abbiamo bisogno di assegnare la sintassi a uno specifico costrutto matematico, chiamato modello.

- Un modello è composto da un **universo** e un insieme di **relazioni**, una per ogni simbolo di relazione nella logica.

- Esempio:
  - sia Σ = {∧, ∨, e ¬, (,), \forall, \exists, x,R_1(· , ·)}.
  - Un modello per questa logica è M_1 = (N,≤), con x → N and R1 →≤.
  - N è l'universo e la relazione ≤ є N × N è l'*interpretazione* per il simbolo di relazione binaria R_1.

Logica del primo ordine(4)

- Data una logica e un modello, possiamo verificare se una particolare sentenza è vera nel modello.
- Esempio 1:
  - Data la logica Σ = {∧, ∨, e ¬, (,), \forall, \exists, x,R_1(·, ·)}, col modello M_1 = (N,≤).
  - Possiamo chiederci se la sentenza \forall x \exists y[R_1(x, y) ∨ R_1(y, x)] è vera.
  - Chiaramente la sentenza è vera, visto che per ogni assegnamento x → a e y → b per a, b є N, abbiamo che a ≤ b or b ≤ a.
- Esempio 2:
  - Data la logica Σ = {∧, ∨, e ¬, (,), \forall, \exists, x,R_1(·, ·)}, col modello M_2 = (N,<)
  - Possiamo dire che la sentenza \forall x \forall y[R_1(x, y) ∨ R_1(y, x)] non è vera. Questo perché per l'assegnamento x → a e y → a con a є N abbiamo a < a or a < a, che è chiaramente falso.
- Esempio 3:
  - Data la logica Σ = {∧, ∨, e ¬, (,), \forall, \exists, x,R_1(· , · , ·)}, col modello M_3 = (R,+) e R_1 relazione ternaria
  - possiamo dire che la sentenza \forall y \exists x[R_1(x, x, y)] è vera. Infatti per ogni assegnamento x → a e y → b con a, b є R abbiamo che +(a, a, b), o nella classica notazione matematica b = a + a, è vera. Falso se il dominio è N

Una teoria decidibile

- Sia M un modello. Diremo che la collezione di tutte le sentenze vere sotto quel modello è la *teoria* del modello e scriveremo Th(M).
- **Teorema: la teoria Th(N,+) è decidibile.**
- Cosa significa che una teoria è decidibile? Significa che noi possiamo decidere se una particolare sentenza appartiene alla teoria o no. Quindi possiamo trattare la teoria Th(N,+) come un linguaggio e possiamo costruire un decisore per questo linguaggio.
- Consideriamo la sentenza \forall x \exists y[y = x + x]. Questa sentenza è vera ed è anche un elemento della teoria Th(N,+).
- Consideriamo ora \exists x \forall y[y = x + x]. Questa sentenza è falsa è quindi non è un membro della teoria.
- E' possibile mostrare la decidibilità della teoria Th(N,+) costruendo un automa finito che decide il linguaggio.

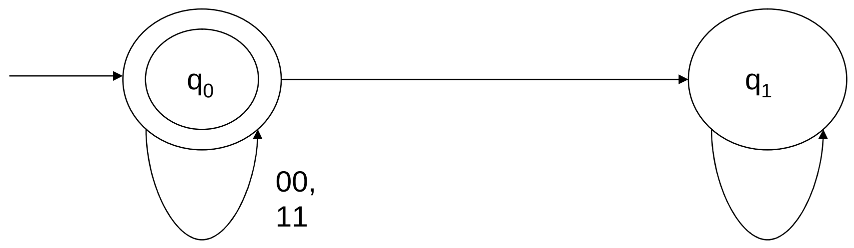
Premessa alla prova: operazioni con automi(1)

Sia Σ = { 00, 01, 10, 11} dove la coppia di nuperi ij rappresenta un elemento di una matrice trasposta 2 x 1 di binari.

Si noti che ogni parola costruita su Σ rappresenta due numeri binari. Per esempio 00 11 10 10 rappresenta i numeri 0111 e 0100

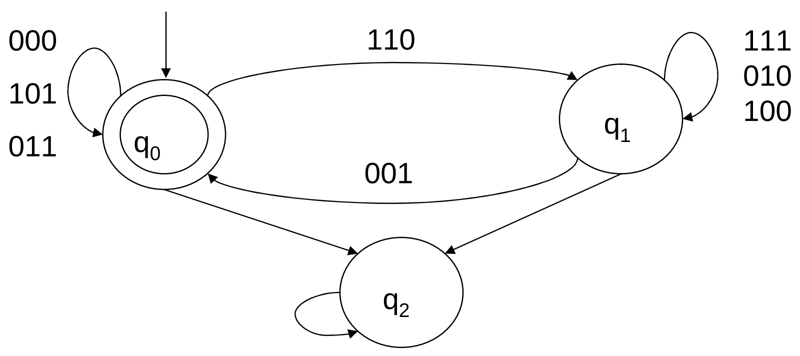
Sia A = { w є Σ* | la prima riga sia uguale alla seconda}.

Esempio: 00 11 00 11 11 11 є A and ¬(11 00 10 00 11 01 00 є A)



Premessa alla prova: operazioni con automi(2)

- Sia Σ = {000, 001, 010, 011, 100, 101, 110, 111}.
- Si consideri il seguente linguaggio:
  B = { w є Σ* | la somma delle prime due righe è uguale alla terza}
  Per esempio, 001 110 011 є B, mentre ¬ (001 110 010 001 є B)



Prova di decidibilità di Th(N,+)

- Sia $\varphi = Q_1 x_1 \ldots Q_n x_n(\psi)$ una sentenza di Th(N,+), dove
  - ciascun Q_i è un quantificatore esistenziale ($\exists$) o universale ($\forall$)
  - ψ non ha quantificatori.
- Sia inoltre $\varphi_i = Q_i x_i \ldots Q_n x_n (\psi)$. In particolare siano $\varphi_0 = \varphi$ e $\varphi_n = \psi$.
- Sia Σ_i l'alfabeto di tutte le parole binarie di lunghezza ì.
- Si costruisca A_n su Σ_n che accetti tutte le parole che rendano vera $\varphi_n = \psi$.
  - Si noti che ψ non ha quantificatori e solo operazioni di somma.
- Si costruisca A_i a partire da A_{i+1}, nel seguente modo:
- Si assuma che Q_i sia esistenziale. Allora costruire A_i in modo da fare una scelta non deterministica sull'i+1-esimo elemento di Σ.
- Se Q_i è universale, allora a fronte della equivalenza $\forall x_{i+1}\ \varphi_{i+i} = \neg\exists x_{i+1}\ \neg\varphi_{i+i}$ si costruisce prima il complemento di A_{i+1} poi si applica il procedimento precedente per Q_i esistenziale e poi si complementa l'automa ottenuto
- L'automa A_0 accetta qualche input se e solo se $\varphi_0 = \varphi$ è vera.
- Dunque, l'ultimo passo dell'algoritmo è testare il vuoto A_0.

Una teoria non decidibile

- Il seguente teorema ha delle conseguenze filosofiche molto profonde.
- Esso mostra che la matematica non può essere "meccanizzata".
- Mostra inoltre che alcuni problemi nella teoria dei numeri non sono algoritmici, cosa che provocò una grande sorpresa nei matematici all'inizio del 1900.
- Allora infatti si credeva che tutti i problemi matematici potessero essere risolti algoritmicamente e che bisognasse solo trovare l'algoritmo per risolvere un dato problema.
- **Teorema: la teoria Th(N,+,×) è indecidibile.**
- Questo significa che non esiste un algoritmo che si ferma su tutte le sentenze φ sull'alfabeto appropriato. Quello che più sorprende è la semplicità della struttura di questa logica indecidibile.
- Questo vuol dire che ci sono delle fondamentali limitazioni algoritmiche nella matematica.
- La dimostrazione si ottiene tramite una riduzione del problema A_{TM} alla teoria Th(N,+,×).

Teorema di incompletezza(1)

- **Teorema: la collezione di sentenze provabili in Th(N,+,×) è Turing-riconoscibile.**
- **Dimostrazione:**
  - il seguente algoritmo P accetta il suo input φ se e solo se φ è dimostrabile.
  - L'algoritmo P prova tutte le possibili stringhe come candidate per una prova π di φ usando un "proof checker"(verificatore della prova).
  - Se viene trovata una stringa che è una prova, allora l'algoritmo accetta.

Teorema di incompletezza(2)

- **Teorema (di incompletezza di Kurt Gödels): alcune sentenze vere in Th(N,+,×) non sono dimostrabili**.
- Con qualche semplificazione, questo teorema afferma che

  "In ogni formalizzazione coerente della matematica che sia sufficientemente potente da poter assiomatizzare la teoria elementare dei numeri naturali — vale a dire, sufficientemente potente da definire la struttura dei numeri naturali dotati delle operazioni di somma e prodotto — è possibile costruire una proposizione sintatticamente corretta che non può essere né dimostrata né confutata all'interno dello stesso sistema."

This document was created with Win2PDF available at http://www.win2pdf.com.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.
This page will not be added after purchasing Win2PDF.