Automi e Linguaggi Formali

Introduzione alle dimostrazioni formali

06 Ottobre 2014

Università degli Studi di Padova

A.A. 2014-2015
Enrico Mezzetti
emezzett@math.unipd.it

Dimostrazioni formali

- Dimostrare scientificamente la correttezza di un programma
  - Importante tanto quanto l'implementazione
  - *Testing* non sempre esaustivo (spazio degli input)
  - Difficile testare una ricorsione o iterazione complessa
- Correttezza di un programma $\leftrightarrow$ ipotesi deduttive/induttive
  - Deduzione sulle sequenze di operazioni del programma
  - Induzione su strutture ricorsive e iterative
- Teoria degli automi si presta a dimostrazioni di entrambi i tipi
  - Utilizzeremo diversi meccanismi e tecniche:

Quantificatori sulle variabili

- **Quantificatore universale**
  - *Per ogni x* ($\forall x$): enunciato vale per tutti i valori della var
- **Quantificatore esistenziale**
  - *Esiste x* ($\exists x$): enunciato vale per almeno un valore della var
- Fondamentale l'ordine con cui si adoperano
- Esempio: definizione (inusuale) di insieme infinito
  - ✓ *Un insieme S e' infinito iff* $\forall$ *intero n,* $\exists$ *almeno un sottoinsieme* $T \subset S$ *con n elementi* $[\forall - \exists]$
  - ✗ *Un insieme S e' infinito iff* $\exists T \subset S$ *tale che* $\forall n$ *intero T ha n elementi* $[\exists - \forall]$

Dimostrazioni deduttive

Processo deduttiva

Sequenza di enunciati la cui verita' porta da un enunciato iniziale (*ipotesi*) ad un enunciato finale (*conclusione*).

- Forma del teorema: "se H allora C"

  hypotesis $\uparrow$ $\qquad$ $\uparrow$ *conlcusion*
- Esempio: se $x \geq 4$, allora $2^x \geq x^2$
  - x parametro *quantificato universalmente*
- **Sequenza deduttiva** $\rightarrow$ ad un enunciato ne *consegue* un altro
  - Modus ponens regola logica per avanzare nella sequenza deduttiva $H \rightarrow \mathrm{C}, H \therefore \mathrm{C}$

Dimostrazioni deduttive - 2

- Esempio:

  "Se $f(x)$ e' pari allora $f(x)$ non e' inettiva"

- Passi deduttivi:
  1. Esplicitare le premesse
     $f(x) : A \to B$ e' *pari* se $\forall x \in A, f(x) = f(-x)$
     $f(x) : A \to B$ *iniettiva* se $\forall x, y \in A, x \neq y \Rightarrow f(x) \neq f(y)$
  2. Se $f(x)$ e' pari $\Rightarrow$ f(x)=f(-x) $\forall$ x
  3. Se $f(x) = f(-x) \Rightarrow \exists a, b, a \neq b$ s.t. $f(a) = f(b)$
  4. Se $\exists a, b, a \neq b$ s.t. $f(a) = f(b) \Rightarrow f(x)$ non iniettiva ■

Dimostrazioni deduttive - 3

- Formulazioni equivalenti
  - "H implica C" ($\rightarrow$)
  - "H solo se C" (`if`)
  - "C se H" (inverso)
  - "quando H segue C" ($\vdash$)
  - "se $\neg$C allora $\neg$H" (contronominale)
  - "H $\wedge \neg$C $\rightarrow$ *false*" (assurdo)
- Formulazioni alternative
  - "se $H_1 \wedge H_2$ allora C"
  - "H se e solo se C" (`iff` - due direzioni di prova)
- Confutazione
  - Trovare un controesempio (es. per "H $\wedge \neg$C")
  - Non vale il ragionamento opposto (*proof by example*)

Dimostrazioni per induzione

Processo induttivo

Dimostrazioni di un enunciato iniziale che si articola a partire da un caso iniziale (*base*) che viene esteso al caso generale applicando una formulazione ricorsiva (*passo induttivo*).

- Utili quando ci sono cose definite ricorsivamente
- **Induzione sugli interi**
  - Dobbiamo dimostrare un enunciato $S(n)$ su un intero n

Base: Dimostriamo $S(i)$ per un intero particolare (0 o 1 di solito)
Passo induttivo: Per $n \geq i$, dimostriamo che $S(n) \Rightarrow S(n+1)$
Conclusione: $S(n)$ e' vero per ogni $n \geq i$

Esempio induzione su interi

- Formula per il calcolo della soma dei primi n interi
- **Theorem**: $S_n = 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$
  - Dimostrazione:

Base (n=1) Enunciato e' vero $\frac{n(n+1)}{2} = 1$
Passo induttivo Assumiamo che l'enunciato sia vero per $n = k$, cioe' $1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}$
Dobbiamo dimostrare che lo stesso vale per $n = k + 1$

$$\begin{aligned} 1 + 2 + 3 + \ldots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= (k+1)(\tfrac{k}{2} + 1) \\ &= (k+1)\tfrac{k+2}{2} \\ &= (k+1)\tfrac{(k+1)+1}{2} \end{aligned}$$ ■

Induzione strutturale

- **Induzione strutturale**
  - Molte strutture possono essere definite ricorsivamente
  - Es: definizione ricorsiva di albero

caso base: Un singolo nodo *root* e' un albero (ne e' anche la radice)
ricorsione: Se $T_1, T_2, \ldots, T_k$ sono alberi, allora collegando *root* alle radici degli alberi $T_1, T_2, \ldots, T_k$ otteniamo un nuovo albero

  - Dobbiamo dimostrare un enunciato $S(X)$ sulle strutture X

Base: Dimostriamo $S(X)$ per la struttura di base X
Passo induttivo: Per definizione ricorsiva della struttura ogni elemento non di base X e' formato da altri elementi $Y_1, Y_2, \ldots, Y_k$. Presumiamo veri gli enunciati $S(Y_1), S(Y_2), \ldots, S(Y_k)$ e dimostriamo $S(X)$.
Conclusione: $S(X)$ e' vero per ogni X

Esempio induzione strutturale

- **Espressioni ricorsive**

caso base Qualsiasi numero o variabile e' un'espressione
ricorsione Se E e F sono espressioni $\Rightarrow$ lo sono anche $E + F$, $E \times F$, e (E)

- **Teorema**: *Ogni espressione ha un numero uguale di parentesi aperte e chiuse.*
  - Dimostrazione:

Passo base : zero parentesi $\Rightarrow$ enunciato vero
Passo induttivo Tre modi per costruire un'espressione induttivamente:

- Casi $E + F$ e $E \times F$: se enunciato vale per E e F $\Rightarrow$ vale anche se applichiamo gli operatori $+$ e $\times$
- Caso (E): se enunciato vale per E, con n parentesi aperte ed altrettante chiuse $\Rightarrow$ (E) ne ha esattamente $n + 1$ ■