Fondamenti di Teoria delle Basi di Dati

Riccardo Torlone

Parte 3:Tecniche di dimostrazione

Dimostrazioni formali e informali

- Dimostrazione (formale): procedimento per cui, in un certo contesto, un enunciato (la tesi) viene derivato in maniera formale a partire da alcune ipotesi e da un insieme di nozioni accettate per evidenza (gli assiomi) mediante un insieme di regole formali (derivazioni logiche) che permettono di generare un enunciato a partire da altri enunciati

$$P_1 \wedge \ldots \wedge P_n \wedge A_1 \wedge \ldots \wedge A_m \rightarrow Q$$

- In pratica si usano dimostrazioni informali: descrizioni discorsive dei passi principali della dimostrazione nelle quali si omettono i dettagli

Esempio

- **Theorem** *Let x and y be two integers. If x is even and y is even then xy is also even.*
- **Proof.** Let x and y be two even integers. We can take n and m such that $x = 2n$ and $y = 2m$. Then, $xy = 2(2nm)$. Since $2nm$ is an integer, xy is an even number. □

Anche l'enunciato è informale

- Let x and y be two integers. [Il contesto]
- Assume x and y are even. [Le ipotesi: $P_1 \wedge \ldots \wedge P_n$]
- Then, xy is even. [La tesi : Q]

Dettagli omessi nella dimostrazione

1. Let x and y be two even integers.
   - Implicit universal quantification
2. We can take n and m such that x = 2n and y = 2m.
   - Implicit use of the axiom: x is even if and only if there exists n such that x = 2n
   - Implicit universal quantification for x and y
   - Implicit existential quantification for n and m
3. Then, xy = 2(2nm)
   - Implicit use of rules of arithmetic and of logical implication
4. Since 2nm is an integer, xy is an even number :
   - Implicit universal quantification of the definition of an even number
   - Implicit use of logical implication

Regole

- The goal of a proof is to be read by humans (in particular yourself) in order to convince those humans
- A reader will be convinced by the proof if he/she can check that he could translate each step of the proof into one or several steps of a formal proof
- A reader will be convinced by the proof if he/she can check that all the steps are valid

Tecniche di dimostrazione

- Disproof by counter example
  - Conjecture. If n is a positive integer, then $n! < n^3$
- Direct proof
- (1) Assume P (2) Deduce Q
  - Example. If x and y are even, then xy is even.
- Exhaustive proof
- All cases have been exhausted (and so are you ...).
  - Example. Propositional logic formula (the truth table is finite)

Tecniche di dimostrazione

- Proof by contradiction
- (1) Assume ¬ Q (the consequent is false) (2) Deduce a contradiction
  - This technique relies on the fact that :
  - (1) if P → False, then P is false
  - (2) Q ∧ ¬ Q is always false
- Proof by contraposition
- (1) Assume ¬ Q (the consequent is false) (2) Prove ¬ P (the antecedent is also false)
  - Example. Prove that if n^2 is odd, then n is odd: prove instead that if n is even, then n^2 is even
  - This technique relies on the fact that P → Q is equivalent to ¬ Q → ¬ P

Tecniche di dimostrazione

- Proof by induction
  - Based on the first principle of mathematical induction
  - Let P(k) be an inductive hypothesis. If :
    - (a) P(1) is true (base case)
    - (b) For any $k > 1$, $P(k - 1)$ true implies P(k) true (induction step)
  - Then : P(k) is true for all $k \geq 1$
- Example: Let $S(k)=S(k-1)+2^{k-1}$ $(S(1) = 1)$, then $S(k) = 2^k - 1$.
- Proof
  - Base case : $S(1) = 1 = 2^1 - 1$. So, P(1) is true.
  - Induction step : Assume that, for $k > 1$, $S(k-1) = 2^{k-1} - 1$
    Then, $S(k) = S(k-1) + 2^{k-1} = 2^{k-1} - 1 + 2^{k-1} = 2^k - 1$.
  - So, P(k) is also true.
- Others
  - proof by reduction

Tecniche di dimostrazione non valide

- Proof by example
  - The author gives only the case n = 2 and suggests that it contains most of the ideas of the general proof.
- Proof by intimidation
  - "Trivial"
- Proof by vigorous handwaving
  - Works well in a classroom or seminar setting.
- Proof by cumbersome notation
  - Best done with access to at least four alphabets and special symbols.
- Proof by exhaustion
  - An issue or two of a journal devoted to your proof is useful.

Tecniche di dimostrazione non valide

- Proof by omission
  - "The reader may easily supply the details.“, "The other 253 cases are analogous."
- Proof by obfuscation
  - A long plotless sequence of true and/or meaningless syntactically related statements.
- Proof by eminent authority
  - "I saw Karp in the elevator and he said it was probably NP-complete."
- Proof by personal communication
  - "Eight-dimensional colored cycle stripping is NP-complete [Karp, personal communication]."
- Proof by reduction to the wrong problem
  - "To see that infinite-dimensional colored cycle stripping is decidable, we reduce it to the halting problem."

Tecniche di dimostrazione non valide

- Proof by reference to inaccessible literature
  - The author cites a simple corollary of a theorem to be found in a privately circulated memoir of the Slovenian Philological Society, 1883.
- Proof by importance
  - A large body of useful consequences all follow from the proposition in question
- Proof by accumulated evidence
  - Long and diligent search has not revealed a counterexample.
- Proof by cosmology
  - The negation of the proposition is unimaginable or meaningless. Popular for proofs of the existence of God.
- Proof by mutual reference
  - In reference A, Theorem 5 is said to follow from Theorem 3 in reference B, which is shown from Corollary 6.2 in reference C, which is an easy consequence of Theorem 5 in reference A.

Tecniche di dimostrazione non valide

- Proof by picture
  - A more convincing form of proof by example. Combines well with proof by omission.
- Proof by vehement assertion
  - It is useful to have some kind of authority in relation to the audience.
- Proof by ghost reference
  - Nothing even remotely resembling the cited theorem appears in the reference given.
- Proof by forward reference
  - Reference is usually to a forthcoming paper of the author, which is often not as forthcoming as at first.
- Proof by exercise
  - The reader is left to do the proof as an exercise. Most commonly found in textbooks.