Fondamenti Logico Matematici dell'Informatica

UniShare

Davide Cozzi
@dlcgold

Indice

Capitolo 1

Introduzione

Questi appunti sono presi a lezione. Per quanto sia stata fatta una revisione è altamente probabile (praticamente certo) che possano contenere errori, sia di stampa che di vero e proprio contenuto. Per eventuali proposte di correzione effettuare una pull request. Link: `https://github.com/dlcgold/Appunti`.

Capitolo 2

Il Paradigma Dimostrazioni = Algoritmi

Prendiamo come *linguaggio di specifica* un **linguaggio del prim'ordine con identità**.

Si ricorda che, in *logica matematica*:

Definizione 1. *Definiamo* ***linguaggio del primo ordine*** *come un linguaggio formale che serve per gestire meccanicamente enunciati e ragionamenti che coinvolgono i connettivi logici, le relazioni e i quantificatori* $\forall$ *e* $\exists$*.*
Si ha che "del primo ordine" ndica che c'è un insieme di riferimento e i quantificatori possano riguardare solo gli elementi di tale insieme e non i sottoinsiemi (posso dire "per tutti gli elementi" ma non "per tutti i sottoinsiemi"). Tale linguaggio è caratterizzato da:

- *un* ***alfabeto di simboli*** *per variabili, costanti, predicati, funzioni, connettivi, quantificatori o punteggiatura*
- *un* ***insieme di termini*** *per denotare gli elementi dell'insieme in analisi*
- *un* ***insieme di formule ben formate (FBF)*** *ovvero un insieme di stringhe composte di simboli dell'alfabeto che vengono considerate sintatticamente corrette*

Definizione 2. *Definiamo* ***sistema assiomatico*** *come un insieme di assiomi che possono essere usati per dimostrare teoremi. Una teoria matematica consiste quindi in una assiomatica e tutti i teoremi che ne derivano.*

Definizione 3. *Definiamo un sistema formale come una formalizzazione rigorosa e completa della nozione di sistema assiomatico costituito da:*

- *un alfabeto*
- *una grammatica che specifica quali sequenze finite dei simboli dell'alfabeto corrispondono ad una FBF. La grammatica deve essere ricorsiva, nel senso che deve esistere un algoritmo per decidere se una sequenza di simboli è o meno una formula ben formata*
- *un sottoinsieme delle FBF che sono gli assiomi. L'insieme degli assiomi è ricorsivo*
- *le regole di inferenze che associano formule ben formate ad n-uple di formule ben formate*

Definizione 4. *Definiamo gli* ***assiomi di Peano*** *come un gruppo di assiomi ideati al fine di definire assiomaticamente l'insieme dei numeri naturali:*

- *esiste un numero naturale: 0 (alternativamente 1 se si vuole escludere 0):*
$$0/1 \in \mathbb{N}$$
- *ogni naturale ha un naturale come successore. Ho quindi una funzione "successore" tale che:*
$$S : \mathbb{N} \to \mathbb{N}$$
- *numeri diversi hanno successori diversi, ovvero:*
$$x \neq y \implies S(x) \neq S(y)$$
- *0 (o alternativamente 1) non è il successore di alcun naturale, ovvero:*
$$S(x) \neq 0, \forall x \in \mathbb{N}$$
- *ogni sottoinsieme di numeri naturali che contenga lo zero e il successore di ogni proprio elemento coincide con l'intero insieme dei numeri naturali. Ovvero dato $U \subseteq \mathbb{N}$ tale che:*
  - $0 \in U$
  - $x \in U \implies S(x) \in U$

allora:

$$U = \mathbb{N}$$

Tale assioma è detto ***assioma dell'induzione*** *o* ***principio di induzione***

Definizione 5. *In una teoria del primo ordine si chiama* ***chiusura universale*** *di una formula ben formata $A(x_1, \ldots, x_n)$, con $x_1, \ldots, x_n$ variabili libere, la formula:*

$$\forall x_1 \forall x_2 \forall x_n \; A(x_1, \ldots, x_n)$$

ottenuta premettendo un quantificatore universale su ogni variabile libera.

Definizione 6. *Definiamo, in logica matematica,* ***aritmetica di Peano (PA)*** *come una teoria del primo ordine che ha come assiomi propri una versione degli* ***assiomi di Peano*** *espressi nel linguaggio del primo ordine. Si ha quindi che il linguaggio di PA è il linguaggio dell'aritmetica del primo ordine con i seguenti simboli:*

- *vari simboli per le variabili: x, y, z, x_1 etc...*
- *costanti individuali: 0 etc...*
- *simboli per funzioni unarie: S*
- *simboli per funzioni binarie $+$, $\times$ ($+(x, y)$ si indica anche con $x + y$ e analogamente si fa per $\times$)*
- *simboli per relazioni unarie: $=$*
- *simboli per connettivi logici, quantificatori e parentesi*

Gli assiomi di PA sono costituiti da:

- *gli assiomi logici*
- *gli assiomi per l'uguaglianza*
- *i seguenti assiomi propri (che "traducono" nella logica di Peano gli assiomi di Peano):*
  - $\forall x \neg(S(x) = 0)$
  - $\forall x \forall y (S(x) = S(y) \implies x = y)$
  - $\forall x (x + 0 = x)$

- $\forall x \forall y(x + S(y) = S(x + y))$
- $\forall x(x \times 0 = 0)$
- $\forall x \forall y(x \times S(y) = (x \times y) + x)$

Agli assiomi propri si aggiunge anche il seguente assioma proprio:

$$(\phi(0, x_1, \ldots, x_n) \wedge (\forall x(\phi(x, x_1, \ldots, x_n) \implies \phi(S(x), x_1, \ldots, x_n)) \implies \forall x \phi(x, x_1, \ldots, x_n)$$

per ogni FBF $\phi(x, x_1, \ldots, x_n)$ di cui $x, x_1, \ldots, x_n$ sono variabili libere. Questo è uno schema di assiomi detto ***schema di induzione*** *e si ha un assioma per ogni FBF ϕ*

Definizione 7. *Definiamo, in logica classica, il* ***principio del terzo escluso*** *che stabilisce che una proposizione e la sua negazione hanno valore opposto, non avendo una "terza opzione". In logica classica è una* ***tautologia****.*

Definizione 8. *Un termine è un* ***termine chiuso*** *sse non contiene delle variabili individuali.*

Definizione 9. *Una* ***formula chiusa*** *è una formula costruita nel linguaggio dei predicati in cui o non compaiono variabili o tutte le variabili presenti sono vincolate a un quantificatore e sono dunque variabili legate.*

Esempio 1. *Vediamo qualche esempio:*

$$\forall x, y \in \mathbb{N},\ \exists z \in \mathbb{N}\ t.c.\ mcd(x, y, z)$$

ovvero z è l'mcd di x e y.
Un altro esempio:

$$\forall x \in \mathbb{N},\ \exists y \in \mathbb{N}\ t.c.\ fatt(x, y)$$

ovvero y è il fattoriale di z.

Formule come quelle dell'esempio possono essere lette come **specifiche del problema di trovare un algoritmo totalmente corretto** che calcoli il risultato di tale problema per ogni input valido. Questa lettura non è implicita nella logica classica, dove non è richiesto di stabilire come viene prodotto il risultato. Si ha quindi a che fare con una lettura di un problema algoritmico di interesse per un informatico.
Le **dimostrazioni** di questa tipologia di formule, nell'ambito dell'**aritmetica di Peano (*PA*)**, sono quindi interpretabili come gli algoritmi che calcolano le funzioni specificate.
Come *vantaggi* di questa "atteggiamento" si ha che:

- l'attenzione si concentra su costruire la dimostrazione, sui passi dimostrativi, e non sulla stesura del codice
- i passi elementari della dimostrazione sono automatici
- la correttezza della dimostrazione è verificabile in modo automatico
- l'estrazione/sintesi dell'algoritmo dalla dimostrazione è diretta. Una volta che si ha la dimostrazione corretta si può estrarre direttamente l'algoritmo. Tale algoritmo è totalmente corretto rispetto alla specifica

La difficoltà si trasferisce dall'ambito convenzionale della programmazione e codifica dell'algoritmo in se alla costruzione dimostrazione e dei passi dimostrativi.
Si hanno quindi anche degli *svantaggi*, abbastanza problematici:

- l'algoritmo ottenuto non è ottimale rispetto al problema. Rispetto a questo bisognerebbe capire come incorporare "più semantica" del problema da risolvere nella dimostrazione stessa
- il formalismo e il linguaggio delle dimostrazioni sono "lontani" da quelli usati usualmente nella pratica informatica

Non tutte le dimostrazioni sono direttamente interpretabili come algoritmi. Per vedere questa cosa prendiamo un esempio famoso di formula da dimostrare in analisi.

Esempio 2 (esempio di Troelstra)**.** *Esistono due numeri irrazionali n e m tali che n^m è razionale. In termini di formula del primo ordine si ha quindi:*

$$\exists n, m \in \{\mathbb{R}/\mathbb{Q}\} \ t.c. \ n^m \in \mathbb{Q}$$

Cerchiamo di capire se:

$$\sqrt{2}^{\sqrt{2}} \in \mathbb{Q} \ o \ \sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$$

Vediamo quindi i due casi (sono solo due per il principio del terzo escluso):

1. *assumo $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$ e pongo $n = m = \sqrt{2}$ avendo trovato due numeri irrazionali n e m tali per cui $n^m \in \mathbb{Q}$*

2. assumo $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$ *e pongo* $n = \sqrt{2}^{\sqrt{2}}$ *e* $m = \sqrt{2}$*. Ne segue che:*

$$n^m = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^2 = 2 \in \mathbb{Q}$$

e quindi ho due numeri irrazionali n *e* m *tali per cui* $n^m \in \mathbb{Q}$

Non possiamo essere soddisfatti di questa dimostrazione. Non veniamo a conoscenza, tramite la dimostrazione, che $\sqrt{2}^{\sqrt{2}}$ *sia o meno razionale. Non possiamo capirlo in quanto assumo il terzo escluso e quindi non so quale dei due casi sia valido, non abbiamo un "esiste" costruttivo (*$\exists n, m \in \{\mathbb{R}/\mathbb{Q}\}$*) in quanto non sappiamo se* $\sqrt{2}^{\sqrt{2}}$ *è razionale o meno. Nonostante ciò al dimostrazione sta perfettamente "in piedi" ma non esibisce* n *e* m *in quanto non determina se* $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$*.*

Quanto successo nell'esempio di Troelstra non può succedere in un **sistema costruttivo**.

Definizione 10. *Definiamo* ***sistema costruttivo*** *un sistema dove si hanno come requisiti minimali:*

- $S \vdash A \vee B \implies S \vdash A$ *oppure* $S \vdash B$ *quindi se nel sistema dimostro* $A \vee B$ *allora nel sistema dimostro* A *o dimostro* B*, con* A *e* B *formule chiuse. Questa è la* ***disjunction property (DP)***
- $S \vdash \exists x A(x) \implies S \vdash A(t)$ *quindi se ho dimostrato un esistenziale allora deve esistere un termine chiuso* t *per cui dimostro* $A(t)$ *nel sistema. Questa è la* ***explicitly definibility property (EDP)****, detta anche* ***existence/witness property***

La logica classica quindi **non è un sistema costruttivo** perché in logica classica riesco sempre a dimostrare $A \vee \neg A$ mentre nell'esempio di Troelstra si nota come non si possa dimostrare né A né $\neg A$. Quindi da una dimostrazione classica di $A \vee \neg A$ io non tiro fuori una dimostrazione classica di A oppure una dimostrazione classica di $\neg A$ quindi non vale la DP. Inoltre non vale nemmeno la EDP, ho dimostrato l'esistenza di n e m (che sono termini chiusi) ma non ho trovato se vale la proprietà che siano irrazionali. La logica classica quindi non è una logica costruttiva.