Sistemi Formali (07-03-2025)

Se devo dimostrare matematicamente che un programma "rispetti la specifica", mi serve utilizzare un "Sistema Formale"

Chi mi garantisce la correttezza del processo? La logica è intesa come studio del *"Ragionamento Corretto"*
Parafrasando, è possibile effettuare e dimostrare "Ragionamenti Corretti" matematicamente, ma in quanto informatici deve essere anche possibile farlo utilizzando l'informatica

Quindi cos'è un sistema formale?

> Una descrizione del modo di ragionamento corretto, rappresentazione precisa di come si ragiona in un determinato ambito

Vedi Logica Proposizionale, Strutture Discrete

- Logica di Hoare (Separation Logic) # Non lo affronteremo

Esistono ovviamente diversi sistemi formali, quindi esiste una caratteristica comune a tutti: La sequenza di affermazioni e il termine della sequenza, quindi, sequenza finita ed ordinata di affermazioni/asserzioni/giudizi/forme ben formate

Affermazioni

Cosa sono le affermazioni? In italiano sono semplicemente le frasi, ed è importante sapere come sono formati alla base definendo quindi l'insieme di caratteri dell'alfabeto.

Utilizzeremo un sistema formale semplice chiamato CL per cui definiremo questo alfabeto

$$S = \{ \mathrm{k}, \mathrm{s}, (,), = \}$$

Ci occuperemo dei sistemi formali dal punto di vista *Sintattico*, "prescindendo dal senso (semantica) della frase analizzata"

In CL, un'affermazione è una stringa formata dai caratteri dell'insieme S

Dobbiamo definire un Linguaggio W

$$W \subseteq S^*$$

dove W è l'insieme di formule ben formate (fbf)

Insieme Decidibile

> Un insieme è decidibile quando esiste un algoritmo in tempo finito che risponde alla domanda "Questo elemento appartiene a questo insieme?" per capire se una data stringa fa parte dell'insieme formale o è una stringa a casaccio

Si deve definire un insieme Ax (Assiomi)

$$Ax \subseteq W$$

sottoinsieme di tutti i giudizi

Assiomi

> Affermazioni inserite nel discorso senza necessità di "Giustificazioni"(Sintatticamente)
> Affermazione Sempre Vera (Semanticamente, credo.)

Es. "Pippo Pippo Gioca veramente bene"
Questa frase viene usata come assioma del sistema formale perché l'interlocutore lo da per ovvio e totalmente veramente, quindi Pippo Pippo ... E' un assioma del proprio sistema formale, se qualcuno ragiona con un altro sistema formale può trovare falso un tuo assioma

Dimostrazione di un Sistema Formale

Riprendendo la definizione di SF

> Sequenza finita di affermazioni

ed estendiamola dicendo che

> ..ogni affermazione della sequenza è giustificata

Ovviamente se l'affermazione non appartiene all'insieme degli Assiomi per esempio un assioma del sistema cl sarà: ks = ks

Come si giustifica un'affermazione?

> Le giustificazioni sono **Regole di inferenza** ovvero dei metodi che permettono di giustificare un giudizio inserito precedentemente nella sequenza

$$\frac{\alpha \implies \beta \quad \alpha}{\beta}$$

Beta è chiamata Conclusione, Alpha Implica Beta e Alpha sono premesse

Deduzioni:

> Sequenze di affermazioni che sono elementi di Ax oppure basate su delle regole di inferenza le cui premesse sono state affermate in precedenza

In un SF Una regola di inferenza è rappresentabile come operazione ternaria tra tutti i sottoinsiemi delle affermazioni per cui

$$MP = \{(\alpha \implies \beta, \alpha, \beta) | \alpha, \beta \in W\}$$

Ipotesi

> Un ragionamento che contiene affermazioni che non sono ne assiomi ne conclusioni

Quindi si usa per la sequenza l'insieme delle Ipotesi del proprio SF.
I ragionamenti possono essere con o senza ipotesi, nel caso in cui si usa l'insieme delle ipotesi il suo utilizzo deve essere dichiarato

$$M \vdash_D \alpha$$

A PARTIRE DA M POSSO DERIVARE ALFA

^^
^

(Una sequenza che termina con alfa dove le affermazioni sono assiomi o date da una regola d'inferenza le cui componenti sono ipotesi)

Esempi di Insiemi formali

Usiamo CL
Riprendiamo S
definiamo W

$$W = \{P = Q | P, Q \in t\}$$

dove t è l'insieme dei termini così definito
Quindi sono tutte le stringhe in cui troviamo un operatore binario (=) tra due componenti appartenenti a t

Fantoccio, Cos'è una definizione?

> Un modo non ambiguo per identificare un oggetto matematico

Definiamo t in modo induttivo per costruire tutti gli elementi appartenenti a t

$$k \in t, s \in t$$

$$se\ P, Q \in T\ allora\ (PQ) \in t$$

$$\text{nient'altro è un termine}$$

DEFINIAMO UN INSIEME CHE HA K S ED UNA PAPARELLA
L'insieme è valido anche se appartiene una paperella perché la condizione dice che devono appartenere gli elementi di t

t invece è l'insieme più piccolo che soddisfa le 3 condizioni precedenti quindi l'insieme paperella non è t

Definiamo Ax utilizzando schemi di assiomi

$$\forall P, Q, R \in T:$$

$$((kP)Q) = P \qquad (Axk)$$

$$P = P$$

$$(((sP)Q)R) = ((PR)(QR)) \qquad (Axs)$$

Regole di inferenza

$$R = \{R_1, R_2, R_3, R_4\}$$

non le copierò

Esempio di deduzione in CL

Dimostriamo che

$$\vdash_{cl} (((sk)k)k) = k$$

$$1.(((sk)k)k) = ((kk)(kk))$$

$$2.((kk)(kk)) = k$$

$$3.(((sk)k)k) = k$$

Questa cosa è possibile secondo lo schema di assiomi per i primi due passaggi e poi per la seconda regola di inferenza che non ho scritto

Proposizioni

> Proprietà che valgono per ogni sistema formale

$$M \vdash_D \alpha_1 \dots M \vdash_D \alpha_n e \{\alpha_1 \dots \alpha_n\} \vdash_d \beta, allora \quad M \vdash_D \beta$$

In una sequenza con conclusione B che contiene delle ipotesi,possiamo sostituire le ipotesi con ciò da cui derivano, ovvero le sequenze che hanno come conclusione l'ipotesi che sostituiamo
le ipotesi sostituite, mettiamo siano alfa 1 e 3, e le sue derivazioni quindi affermano B
circa.

Dico che la mia conclusione alpha su D potrebbe usare un ipotesi M
GUARDARE PROPOSIZIONE 2.3 pag10
logica.dvi

Data Una Regola R in un sistema formale D è derivabile quando

$$\frac{\alpha_1 \dots \alpha_n}{\beta} R$$

Se prendo un sistema formale D e gli aggiungo la regola R

$$se \ \Gamma \vdash_{D \cup \{R\}} \gamma \rightarrow \Gamma \vdash_D \gamma$$

In pratica è una regola inutile che serve solo ad arrivare alla stessa conclusione con un altro ragionamento, possibilmente lo semplifica

Allora vale la seguente proprietà

$$\Gamma \vdash_{D \cup \{R\}} \gamma \iff \Gamma \vdash_D \gamma$$

Consistenza

- proprietà che dovrebbero avere tutti i SF

> Un SF D si dice Consistente/Coerente quando l'insieme dei teoremi di D per alfa appartenente alle formule ben formate non appartiene alle formule ben formate

$$\{\vdash_D \alpha | \alpha \in W\} \neq W$$

perché sennò il sistema potrebbe concludere qualsiasi cosa
un sistema ha senso solo se c'è qualcosa che non puoi dimostrare

$$\vdash_D \alpha \ \leftarrow Teorema\ (notare\ mancanza\ di\ M\ che\ rappresenta\ l'ipotesi)$$

Conseguenze

Avendo un insieme di fbf Gamma in D chiamiamo l'insieme delle conseguenze tutte le formule ben formate derivate da Gamma

$$CON_d(\Gamma) = \{\Gamma \vdash_d \alpha | \alpha \in W\}$$

$$CON_d(\phi) \neq W condizione\ di\ consistenza$$

Un insieme di fbf è consistente in D quando è diverso da W

Esempio di inconsistenza: Sistema PA
PA dice che se prendi un insieme Gamma che sia l'insieme di fbf

Teoria

Una teoria è un insieme Gamma di fbf per cui se viene usato come ipotesi per D si riesce a trovare tutto ciò che appartiene già a Gamma
quindi un insieme chiuso per derivazione. Posso usare Gamma solo per trovare fbf già presenti in Gamma

$$CON_D(\Gamma) = \Gamma$$

Teoria Pura
Prendendo un insieme di teoremi

$$CON_D(\phi)$$

è teoria pura perché non usiamo ipotesi
Una teoria è l'insieme delle sue conseguenze (?)

$$Con_D(Con_D(\phi)) = Con_D(\phi)$$

Può capitare che

$$\Gamma \neq \Gamma' \ ma\ Con_D(\Gamma) = Con_d(\Gamma')$$

Regola Ammissibile

Una regola è ammissibile quando $\vdash_{D+R} \alpha \implies \vdash_D \alpha$

La proprietà di derivabilità è più forte dell'ammissibilità

Se una regola è derivabile è ammissibile

$$R \text{ è derivabile per } R \frac{\alpha_1 \dots \alpha_n}{\beta}$$

è ammissibile quando se ho un teorema in D+R è un teorema anche in D

$$\vdash_{D+R} \alpha \implies \vdash_D \alpha$$

Presa qualunque regola ammissibile non è detto sia derivabile

Semantica di un sistema formale

Dire che un ragionamento per fbf è valido o non valido
il concetto di validità coincide con quello di tautologia

Che caratteristiche deve avere la semantica di un SF?
Le due caratteristiche principali sono

- Correttezza

  > Quando i teoremi che ottengo nell'SF sono tutti Validi
  > Se ho un ragionamento che usa dell ipotesi e conclude con una certa fbf il sistema formale è corretto rispetto alla sua semantica
  > Se le ipotesi sono validi che portano a un teorema valido è corretto

- Completezza

  > Tutto ciò che è valido si può ottenere come conclusione di un ragionamento
  > Non c'è una relazione tra un sistema completo e corretto

Non è completo se c'è una fbf valida ma non dimostrabile

ved es 115