TEOREMI DI INCOMPLETEZZA

Dimostrati da Gödel, usando la logica.
Mostreremo come gli stessi risultati si ottengono in maniera semplice usando le TM.
Tutto parte dall'esigenza di poter verificare le dimostrazioni matematiche. Già nel 300 A.C. Euclide ha postulato alcuni assiomi per la geometria piana:

- Se congiungo 2 punti ottengo segmento
- ...

Non sembrano molto formali. Nell'800: se si può fare in modo rigoroso? Nasce la

la logica, ad es. la logica di primo ordine.
Ad es. "Alice ha il padre più figo del Mondo!"

$$\forall x \, [\neg (x = a) \Rightarrow \text{IsCooler}(\text{Father}(a), \text{Father}(x), x)]$$

Connettori: $\vee, \wedge, \neg, \rightarrow$
Variabili: x, y
Quantificatori: $\forall, \exists, \ldots$
Vocabolario: Funzioni (Father) relazioni (IsCooler).
Se ad es. S è vero e $S \rightarrow T$, T è vero.
Sistema di prove: Assiomi + FoL.
Esempi: gli assiomi di Tarski per la geometria
assiomi di Peano per aritmetica, assiomi di

Made with Goodnotes

Zermelo - Fraenkel (ZFC) per insiemi.

Assumiamo: sistema di prove Π. Proprietà:

-) Per ogni affermazione, vera o falsa, $\exists$ rappresentazione come stringa $\langle x \rangle$ di lunghezza finita.

-) Per ogni dimostrazione, esiste una rapp. come stringa $\langle w \rangle$ di lunghezza finita.

-) Esiste decisore TM V t.c. $V(\langle x, w \rangle) =$ ACC sse w è una prova per aff. x.

DEF x è DIMOSTRABILE, se $\exists\ w$ t.c. $V(\langle x, w \rangle) =$ ACC.

x è INDIPENDENTE se né x, né $\neg x$ sono

DIMOSTRABILI.

Proprietà utili per Π.

DEF Diciamo che Π è:

- CONSISTENTE se $\forall\, x$ al più una tra x e $\neg x$ è dimostrabile.

- VALIDO se $\forall\, x$, se x DIMOSTRABILE allora x è VERA.

- COMPLETO se $\forall\, x$, almeno uno tra x e $\neg x$ è dimostrabile.

(INCOMPLETO: $\exists\, x$ indipendente.)

Osservazioni: Se Π è valido, Π è consistente.

Se Π è completo e consistente, $\forall\, x$ solamente uno tra x e $\neg x$ è dimostrabile.

Se Π è valido e completo, come prima ed inoltre quello che è dim. è anche vero.

$\Rightarrow$ Tutto e solo ciò che è vero è dimostrabile!

Assiomi di Tarski sono validi e completi!

A partire dal 900 si è provato a fare lo stesso con ZFC. Fino a che Gödel ha spiegato che non è possibile. Piano:

- Mostriamo prima che se ZFC (Π) è VALIDO, allora non è COMPLETO.
- Infatti possiamo valutare la VALIDITÀ alla

CONSISTENZA. (1° THM INCOMPLETEZZA).

- Se ZFC è CONSISTENTE, allora l'affermazione x = "ZFC è CONSISTENTE" non è dimostrabile. (2° THM di INCOMPLETEZZA).

Per la dimostrazione, consideriamo la seguente TM.

<u>TM $P(\langle x \rangle)$</u> :

1) Per ogni $K = 1, 2, 3, \dots$

2) Per ogni w di lunghezza K

3) Se $V(\langle x, w \rangle) = ACC$, ritorna w.

$L_{PROVABLE} = \{ \langle x \rangle : x$ è DIMOSTRABILE $\}$.

TM $R(\langle x \rangle)$:

1) Per $K = 1, 2, 3, \dots$
2) Per ogni w t.c. $|w| = K$
3) Se $V(\langle x, w \rangle) = Acc$ allora Acc. Se $V(\langle \neg x, w \rangle) = REJ$, allora REJ.

Cosa possiamo dire su R?

- Se Π è VALIDO, quando R termina dà le risposte corrette. Ma non è detto che termini.
- Se Π è COMPLETO, allora R è un DECISORE.

Made with Goodnotes

- Se Π è VALIDO e COMPLETO allora R è decisore t.c. $\forall x$ se x è vera $R(\langle x \rangle) = ACC$ se x è falsa $R(\langle x \rangle) = REJ$.

La dimostrazione del 1° Teorema: Sia Π VALIDO e COMPLETO, allora consideriamo la seguente TM per decidere $HALT_{TM} = \{\langle M, w \rangle : M \in TM, M(w) \neq \infty\}$.

TM $D(\langle M, w \rangle)$

- Ritorna $R(\langle \text{"} M(w) \neq \infty \text{"} \rangle)$.

Chiaramente D decide $HALT_{TM}$ $\rightarrow \leftarrow$

THM ZFC non può essere VALIDO e COMPLETO.

Vabbè: Aggiungo x si è vero agli assiomi.
Ma il teorema è ancora vero, $\exists\, x'$ che è vero e non dimostrabile. Però se aggiungo tutti gli assiomi, gli assiomi non sono computabili.

Altro punto: Se x è vero ma non si può dimostrare, che vuol dire che è vero??

Gödel: Basta assumere T è CONSISTENTE.

THM. ZFC non può essere CONSISTENTE e COMPLETO.

DIM. La stessa cosa di prima: Sia ZFC consistente.

Usiamo un fatto: esistono affermazioni su cui possiamo essere convinti che sono vere.

LEMMA Se una TM ha una traccia di esecuzione per $t \geq 1$ passi, esiste una prova di questa affermazione in ZFC.

Dim. Basta controllare l'esecuzione di M. All'inizio M è nella configurazione iniziale. Al passo 1 sarà nella config. 1, etc. fino al passo t.

$\Rightarrow$ Se $M \in TM$ e $M(w) \neq \infty$, esiste in ZFC una prova dell'affermazione $X =$ "$M(w) \neq \infty$".

Considero la seguente TM.

TM $D(\langle M \rangle)$

- Per $K = 1, 2, 3, \dots$
- Per ogni w t.c. $|w| = K$
- Se w è una prova per "$M(\langle M \rangle)$ termina" vai nello stato "muovi sempre a Dx".
- Se w è una prova per "$M(\langle M \rangle) = \infty$", allora Termina.

Cosa dire su $D(\langle D \rangle)$? Siccome Π è CONSISTENTE, allora al più una di "$D(\langle D \rangle)$ Termina", "$D(\langle D \rangle)$ loop" è DIMOSTRABILE

- Suppongo "$D(\langle D \rangle)$ Loop" dimostrabile. Allora $D(\langle D \rangle)$ troverà la dimostrazione in di questa aff. e $D(\langle D \rangle)$ Termina.
Per il lemma esiste una prova per "$D(\langle D \rangle)$ Termina". $\rightarrow\leftarrow$

- Suppongo "$D(\langle D \rangle$ Termina" dimostrabile.
$D(\langle D \rangle)$ Trova la prova in e va in loop, poiché precisamente entra nello stesso "muovi sempre a destra".
Per il lemma c'è una prova per "$D(\langle D \rangle)$ loop". $\rightarrow\leftarrow$ $\blacksquare$