Vediamo altro esempio.

$$EQ_{TM} = \{ \langle M_1, M_2 \rangle : M_1, M_2 \in TM$$
$$L(M_1) = L(M_2) \}$$

è indecidibile.

Per risolvere $E_{TM} = \{ \langle M \rangle : M \in TM, L(M) = \emptyset \}$ mostriamo che $E_{TM} \leq_m EQ_{TM}$. Devo costruire $f : \Sigma^* \to \Sigma^*$ t.c.

$$\langle M \rangle \in E_{TM} \text{ sse } f(\langle M \rangle) \in EQ_{TM}$$

Definiamo la TM F che computa f:

- Su input $\langle M \rangle$
- Costruisce $\langle M' \rangle$ t.c. su input x M' rifiuta sempre. ↳ (per ogni input)
- Output $\langle M, M' \rangle$.

$(\Rightarrow)$ Se $\langle M \rangle \in E_{TM}$, allora $L(M) = \emptyset$. Per costruzione, $L(M') = \emptyset$ e quindi $\langle M, M' \rangle \in EQ_{TM}$.

$(\Leftarrow)$ Se $\langle M, M' \rangle \in EQ_{TM}$, allora $L(M)$

$= L(M') = \emptyset$. Ovvero $\langle M \rangle \in E_{TM}$.

Vediamo come applicare le stesse tecniche alla Turing-riconoscibilità.

TEO Se $A \leq_m B$ e B è Turing-ric. allora A è Turing-ric.

Dim. Identica al caso di decidibilità

COR. Se $A \leq_m B$ e A non è Turing-ric. allora B non è Turing-ric.

Applicazione: posso dimostrare la non

Turing-ric. per risolvere ad altri linguaggi non Turing-ric. (e.g. $\overline{A_{TM}}$).

Siccome $\overline{A_{TM}}$ non è facile da maneggiare, possiamo ragionare sul complemento.

LEMMA Se $A \leq_m B$, allora $\overline{A} \leq_m \overline{B}$.

DIM. Basta considerare la stessa f mapping reduction che A e B.

Pertanto, se $\overline{A}$ non è Turing-ric. e $A \leq_m B$ allora $\overline{B}$ non è Turing-ric.

Esempio: EQ_{TM} non è Turing-ric. Pongo $\bar{A} = \overline{A_{TM}}$ ($A = A_{TM}$) e $\bar{B} = EQ_{TM}$ ($B = \overline{EQ_{TM}}$). Pertanto basta mostrare

$A_{TM} \le_m \overline{EQ_{TM}}$.

Definisco $f : \Sigma^* \to \Sigma^*$ computabile

t.c. $\langle M, w \rangle \in A_{TM}$ sse $f(\langle M, w \rangle) \in \overline{EQ_{TM}}$

TM F per calcolare f:

- Su input $\langle M, w \rangle$.

Made with Goodnotes

- Output $\langle M_1, M_2 \rangle$ t.c. M_1 rifiuta tutto, M_2 su input x esegue M su w e accetta x sse $M(w) = Acc.$

($\Rightarrow$) Se $\langle M, w \rangle \in A_{TM}$, allora $M(w) = Acc.$ Allora $L(M_2) = \Sigma^*$ mentre $L(M_1) = \emptyset$. Ovvero $L(M_1) \neq L(M_2)$ e quindi

$$\langle M_1, M_2 \rangle \in \overline{EQ_{TM}}.$$

($\Leftarrow$) Se $\langle M_1, M_2 \rangle \in \overline{EQ_{TM}}$ allora

$L(M_1) \neq L(M_2)$. Siccome M_1 rifiuta tutto, M_2 deve accettare almeno un x.

Ma questo è possibile solo se $M(w) = acc$.

Ovvero $\langle M, w \rangle \in A_{TM}$.

TEOREMI DI INCOMPLETEZZA DI GÖDEL.

Risultato classico della matematica, si può dimostrare usando solamente la teoria della calcolabilità.

Tutto nasce da una esigenza: formalizzare la così detta GOOD OLD REAL MATH (GORM).

Euclide nel 300 A.C. ha inventato il processo di formalizzazione della scrittura delle prove matematiche come sequenza di derivazioni logiche a partire da ASSIOMI:

1) Congiungendo 2 punti qualsiasi si ottiene un segmento.

2) Per un punto esterno a una retta passa una sola retta parallela.

...

Primo approccio formale risalgono al 1800 Tramite la logica di primo ordine e il calcolo deduttivo. Si possono esprimere enunciati del tipo: "Alice ha il papà + figo di tutti".

$$\forall x \; (\neg (x = a) \rightarrow IsCooler(Father(a), Father(x)))$$

connettivi : $\wedge$, $\vee$, $\neg$, $\rightarrow$

quantificatori : $\exists$, $\forall$, $=$

funzioni : $Father(\cdot)$

relazioni : $IsCooler(\cdot, \cdot)$.

Questo permette di rappresentare gli enunciati matematici e le prove come strumenti, che permettono di verificare se l'enunciato segue dagli assiomi.

Esempi: Assiomi di Tarski per la geometria piana. Aritmetica di Peano su $\mathbb{N}$. Gli assiomi di Zermelo-Fraenkel (ZFC).

<u>Peano</u>:

- Costanti: 0
- Funzioni: Successore(x), Plus(x, y), Times(x, y)

- Axioms:

*) $\forall x : \neg(\text{Successor}(x) = 0)$

*) $\forall x \forall y : (\text{Successor}(x) = \text{Successor}(y)) \rightarrow (x = y)$.

*) $\forall x : \text{Plus}(x, 0) = x$

*) $\forall x : \text{Times}(x, 0) = 0$.

...

Fatto: Alcuni sistemi assiomatici (Peano e ZFC) sono abbastanza espressivi da formalizzare enunciati tipo "$M(w)$ termina" dove $M \in TM$.

A questo punto siamo ambiziosi: vogliamo formalizzare la nostra branca preferita della matematica. Introduciamo sistema di prove Π tale che:

- Per ogni affermazione VERA o FALSA

esiste una sua rapp. come stringa $\langle x \rangle$.
di lunghezza finita.

- Per ogni dimostrazione esiste una rapp. $\langle \pi \rangle$ stringa di lunghezza finita.

- $\exists$ TM V t.c. $V(\langle x, \pi \rangle) = ACC$ sse π è una prova valida per x.

Diciamo: x DIMOSTRABILE se $\exists\, \pi$ t.c. $V(\langle x, \pi \rangle) = ACC$

π deve essere computabile: gli esigiamo sono riconoscibili. Più precisamente

$\{A : A$ è esistenza di $\pi\}$ è DECIDIBILE.

Dato V, posso definire dimostratore P:

TM $P(<x>)$:

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

2) Per ogni stringa w di length K

3) Se $V(<x, w>) = ACC$, ritorna w.

Posso anche considerare:

$L_{PROVABLE} = \{ \langle x \rangle : x$ è dimostrabile in $\Pi \}$

La seguente TM prova a decidere $L_{PROVABLE}$:

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

- Per $K = 1, 2, 3, \ldots$
- Per ogni w di lung. K
- Se $V(\langle x, w \rangle) = ACC$, ritorna ACC.

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

A seconda delle proprietà di Π, R potrebbe essere o meno un decisore.

DEF Sia Π sistema di prove. Diremo che:

- Π è CONSISTENTE, se $\forall x$ al più uno tra x e $\neg x$ è DIMOSTRABILE ($\forall x$, x DIMOSTRABILE $\Rightarrow$ $\neg x$ non è DIM.)
- Π è VALIDO se per ogni x, se x è DIM. allora x è VERA.

Made with Goodnotes

- Π è COMPLETO se $\forall$ x almeno uno tra x e $\neg x$ è dimostrabile.
($\forall x$, x DIM. $\vee$ $\neg x$ DIM.).

Se è INCOMPLETO, $\exists$ x detta affermazione indipendente.

Osservazioni:

- Se progetto Π, meglio che sia consistente. Altrimenti, ogni TH è dimostrabile.

THM. Bla Bla Bla.

DIM. Supponiamo non sia vero.

Assumo $\rightarrow x$.

Assumo $\rightarrow \neg x$

- Se Π è VALIDO è anche CONSISTENTE. Perché:

x DIM. $\Rightarrow$ x VERO.

Se $\neg x$ DIM. $\Rightarrow$ $\neg x$ VERO

$\Rightarrow$ x FALSO $\rightarrow$ $\Leftarrow$.

- Se Π è CONSISTENTE e COMPLETO, $\forall x$ solo uno tra x e $\neg x$ è dimostrabile.

- Se Π è VALIDO e COMPLETO, $\forall x$ solo uno tra x e $\neg x$ è DIM e quindi VERO.

$\Rightarrow$ Tutto e solo ciò che è VERO è DIMOSTRABILE.

Buone notizie: gli assiomi di TARSKI sono VALIDI e COMPLETI.

Nel goo' tentativo di fare lo stesso per tutta la matematica: Gödel e Turing dimostrano che è impossibile.

Torniamo alla TM R definita sopra.

- Se Π è VALIDO, quando R termina fornisce la risposta corretta. Ma non è detto che termini.
- Se Π è COMPLETO, allora R è un DECISORE. Infatti se $R(\langle x \rangle) = \infty$ allora né x, né $\neg x$ sono dimostrabili.
- Se Π è VALIDO e COMPLETO allora R è un DECISORE tale che: $\forall x$

se x è vera $R(<x>) = ACC$ e se

x è FALSA $R(<x>) = REJ$.

Supponiamo che Π sia VALIDO e COMPLETO. Costruisco TM per decidere:

$$HALT_{TM} = \{ <M, w> : M \in TM \; M(w) \neq \infty \}.$$

<u>TM $D_{HALT}(<M, w>)$</u>:

- Riforma $R(<$ "$M(w) \neq \infty$" $>)$

Unica assunzione: Π deve poter esprimere "$M(w) \neq \infty$". Se Π è sia VALIDO che COMPLETO D_{HALT} decide $HALT_{TM}$ $\rightarrow$ ↯.

THM ZFC (Peano) non può essere VALIDO e COMPLETO.

Conseguenza: Se ZFC è VALIDO, allora $\exists\ x$ che pur essendo vera non può essere dimostrata.

Tentativo: Siccome x è VERA la

aggiungo agli assiomi. Ma il sistema che ottengo soddisfa ancora le assunzioni del TdI di incompletezza e quindi $\exists\, x$ che non è dimostrabile seppur sia vero. E così via .... Ma poi il sistema di assiomi non è COMPUTABILE.

Confusione: Come può essere x vera se non è dimostrabile? Ma il concetto di verità non è influenzato dalla logica di $\mathbb{T}$. Tuttavia, possiamo fare di meglio

THM ZFC non può essere CONSISTENTE e COMPLETO.

DIM. Il punto di partenza è che ci sono affermazioni così semplici che sono certamente VERE. Es.: ci sono 25 numeri primi < 100.

LEMMA Se una TM ha traccia di esecuzione per $t \geq 1$ passi, allora c'è una prova di questo in ZFC.

Basta controllare: M è nella config. iniziale, ..., dopo t passi M è nella configurazione t. È banale.

Conseguenza: Se $M \in TM$ e $M(w) \neq \infty$, c'è una prova di "$M(w)$ termina" in ZFC.

Consideriamo la seg. TM D:

TM $D(\langle M \rangle)$:

- Per $K = 1, 2, 3, \dots$

- Per ogni stringa w lunga K
- Se w è dimostrazione per "$M(\langle M \rangle) \neq \infty$" entra nello stato "muovi sempre a Dx".
- Se w è dimostrazione per affermazione "$M(\langle M \rangle) = \infty$" allora Termina.

Che succede se guardo $D(\langle D \rangle)$?

Assumiamo ZFC consistente: al più uno tra "$D(\langle D \rangle)$ Termina" oppure

"D(<D>) loop" è dimostrabile.
In realtà però:

- Supponiamo "D(<D>) va in loop" sia dimostrabile. In questo caso D(<D>) trova la dimostrazione e termina. Pertanto per il lemma esiste una prova per "D(<D>) Termina". Questo contraddice consistenza.

- Supponiamo "D(<D>) Termina"

sia dimostrabile. Ma allora $D(\langle D \rangle)$ trova la prova ed entra nello stato "muovi sempre a Dx". Per il lemma esiste prova in ZFC per "$D(\langle D \rangle)$ loop". Questo contraddice consistenza.

Pertanto ZFC è INCOMPLETO $\blacksquare$

Bonus: Ma che fa $D(\langle D \rangle)$? Termina o loop? Andrà in loop. Se codifico questo in ZFC la dimostrazione per

"$D(\langle D \rangle)$ loop". In realtà non abbiamo dimostrato questo, ma:
"Se ZFC consistente, allora $D(\langle D \rangle)$ va in loop".
Ovvero, un'affermazione del tipo "$A \to B$".
Se ZFC assumiamo sia consistente abbiamo visto B non è dimostrabile in ZFC. Unica possibilità: Non possiamo dimostrare in ZFC "ZFC è

CONSISTENTE".

THM. Sia ZFC consistente. Allora ZFC è INCOMPLETO e l'affermazione "ZFC è CONSISTENTE" non è dimostrabile.