Università di Genova | DIMA DIPARTIMENTO DI MATEMATICA

La logica moderna

Giuseppe Rosolini

UNIVERSITÀ DI PARMA

Università di Genova | DIMA DIPARTIMENTO DI MATEMATICA

Parte I

La crisi dei fondamenti e la nascita della logica matematica

UNIVERSITÀ DI PARMA

David Hilbert e le basi della matematica

David Hilbert e le basi della matematica

- Le geometrie euclidea, iperbolica e ellittica sono riconducibili all'analisi
- L'analisi è riconducibile alla teoria degli insiemi e all'aritmetica
- La teoria degli insiemi è coerente
- L'aritmetica è coerente

La geometria euclidea

- Euclide
- Moritz Pasch
- Giuseppe Peano
- David Hilbert
- Alfred Tarski

Gli assiomi di Euclide

1. Per due punti distinti passa un segmento
2. Un segmento può essere prolungato indefinitamente
3. Dato un punto e un segmento esiste la circonferenza di centro il punto e raggio il segmento
4. Due angoli retti sono uguali
5. Se un segmento incontra due segmenti producendo due angoli la cui somma è inferiore a due retti, allora i prolungamenti dei due segmenti si intersecano da quella parte

Proposizione 1

Costruire un triangolo equilatero di base fissata.

Gli assiomi di Euclide

1. Per due punti distinti passa un segmento
2. Un segmento può essere prolungato indefinitamente
3. Dato un punto e un segmento esiste la circonferenza di centro il punto e raggio il segmento
4. Due angoli retti sono uguali
5. Se un segmento incontra due segmenti producendo due angoli la cui somma è inferiore a due retti, allora i prolungamenti dei due segmenti si intersecano da quella parte

Proposizione 1

Costruire un triangolo equilatero di base fissata.

Dimostrazione

Dato il segmento di base AB

Gli assiomi di Euclide

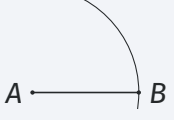
1. Per due punti distinti passa un segmento
2. Un segmento può essere prolungato indefinitamente
3. Dato un punto e un segmento esiste la circonferenza di centro il punto e raggio il segmento
4. Due angoli retti sono uguali
5. Se un segmento incontra due segmenti producendo due angoli la cui somma è inferiore a due retti, allora i prolungamenti dei due segmenti si intersecano da quella parte

Proposizione 1

Costruire un triangolo equilatero di base fissata.

Dimostrazione

Dato il segmento di base *AB*, per l'Assioma 3 tracciare la circonferenza di raggio *AB* con centro in *A*



Gli assiomi di Euclide

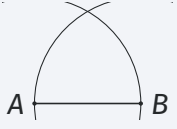
1. Per due punti distinti passa un segmento
2. Un segmento può essere prolungato indefinitamente
3. Dato un punto e un segmento esiste la circonferenza di centro il punto e raggio il segmento
4. Due angoli retti sono uguali
5. Se un segmento incontra due segmenti producendo due angoli la cui somma è inferiore a due retti, allora i prolungamenti dei due segmenti si intersecano da quella parte

Proposizione 1

Costruire un triangolo equilatero di base fissata.

Dimostrazione

Dato il segmento di base *AB*, per l'Assioma 3 tracciare la circonferenza di raggio *AB* con centro in *A* e quella con centro in *B*



Gli assiomi di Euclide

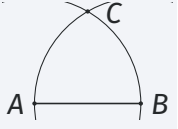
1. Per due punti distinti passa un segmento
2. Un segmento può essere prolungato indefinitamente
3. Dato un punto e un segmento esiste la circonferenza di centro il punto e raggio il segmento
4. Due angoli retti sono uguali
5. Se un segmento incontra due segmenti producendo due angoli la cui somma è inferiore a due retti, allora i prolungamenti dei due segmenti si intersecano da quella parte

Proposizione 1

Costruire un triangolo equilatero di base fissata.

Dimostrazione

Dato il segmento di base *AB*, per l'Assioma 3 tracciare la circonferenza di raggio *AB* con centro in *A* e quella con centro in *B*
Il terzo vertice del triangolo è l'intersezione *C* delle circonferenze



Gli assiomi di Euclide

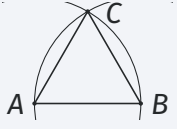
1. Per due punti distinti passa un segmento
2. Un segmento può essere prolungato indefinitamente
3. Dato un punto e un segmento esiste la circonferenza di centro il punto e raggio il segmento
4. Due angoli retti sono uguali
5. Se un segmento incontra due segmenti producendo due angoli la cui somma è inferiore a due retti, allora i prolungamenti dei due segmenti si intersecano da quella parte

Proposizione 1

Costruire un triangolo equilatero di base fissata.

Dimostrazione

Dato il segmento di base *AB*, per l'Assioma 3 tracciare la circonferenza di raggio *AB* con centro in *A* e quella con centro in *B*
Il terzo vertice del triangolo è l'intersezione *C* delle circonferenze



Gli assiomi di Euclide

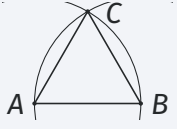
1. Per due punti distinti passa un segmento
2. Un segmento può essere prolungato indefinitamente
3. Dato un punto e un segmento esiste la circonferenza di centro il punto e raggio il segmento
4. Due angoli retti sono uguali
5. Se un segmento incontra due segmenti producendo due angoli la cui somma è inferiore a due retti, allora i prolungamenti dei due segmenti si intersecano da quella parte

Proposizione 1

Costruire un triangolo equilatero di base fissata.

Dimostrazione

Dato il segmento di base *AB*, per l'Assioma 3 tracciare la circonferenza di raggio *AB* con centro in *A* e quella con centro in *B*
Il terzo vertice del triangolo è l'intersezione *C* delle circonferenze



Gli assiomi di Euclide

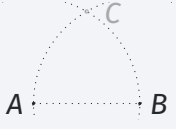
1. Per due punti distinti passa un segmento
2. Un segmento può essere prolungato indefinitamente
3. Dato un punto e un segmento esiste la circonferenza di centro il punto e raggio il segmento
4. Due angoli retti sono uguali
5. Se un segmento incontra due segmenti producendo due angoli la cui somma è inferiore a due retti, allora i prolungamenti dei due segmenti si intersecano da quella parte

Proposizione 1

Costruire un triangolo equilatero di base fissata.

Dimostrazione

Dato il segmento di base *AB*, per l'Assioma 3 tracciare la circonferenza di raggio *AB* con centro in *A* e quella con centro in *B*
Il terzo vertice del triangolo è l'intersezione *C* delle circonferenze



Un commento

Euclide

È molto difficile sovrastimare l'importanza della ricerca svolta da Euclide in relazione ai successivi sviluppi della scienza, in particolare della matematica

Gli assiomi di Hilbert

1. Dati due punti distinti esiste una e una sola retta che li contiene
2. Ogni retta ha almeno due punti distinti
3. Esistono tre punti non allineati
4. Se A è tra B e C, allora A è anche tra C e B
5. Se A è tra B e C, allora i tre punti stanno sulla stessa retta
6. Dati tre punti distinti e allineati, esattamente uno è tra gli altri due
7. Dati un triangolo e una retta che non passa per nessuno dei vertici, se la retta interseca un lato del triangolo allora ne interseca anche un altro
8. Dati un segmento $\overline{AB}$ e una semiretta uscente da C, esiste un punto D sulla semiretta tale che $\overline{CD} \equiv \overline{AB}$
9. Ogni segmento è congruente a se stesso
10. Due segmenti congruenti a un terzo sono congruenti tra loro
11. Dato un angolo $\angle sAt$ e un punto B, esistono semirette u e v uscenti da B uniche tali che $\angle sAt \equiv \angle uBv$
12. Ogni angolo è congruente a se stesso
13. Due angoli congruenti a un altro sono congruenti tra loro
14. Due triangoli che hanno congruenti due lati e l'angolo compreso hanno tutti gli altri elementi congruenti
15. Dati segmenti $\overline{AB}$ e $\overline{CD}$ esiste un numero naturale n e punti $A_1,\dots, A_n$ sulla semiretta uscente da A che contiene B tali che $\overline{CD} \equiv \overline{AA_1} \equiv \overline{A_iA_{i+1}}$, $i = 1, \dots, n-1$ e B è tra A e A_n
16. È impossibile estendere una retta con altri punti conservando la validità degli assiomi precedenti
17. Dato un punto A e una retta r che non contiene A, se le rette s e t passano per A e sono parallele a r, allora coincidono

Gli assiomi di Hilbert

1. Dati due punti distinti esiste una e una sola retta che li contiene
2. Ogni retta ha almeno due punti distinti
3. Esistono tre punti non allineati
4. Se A è tra B e C, allora A è anche tra C e B
5. Se A è tra B e C, allora i tre punti stanno sulla stessa retta
6. Dati tre punti distinti e allineati, esattamente uno è tra gli altri due
7. Dati un triangolo e una retta che non passa per nessuno dei vertici, se la retta interseca un lato del triangolo allora ne interseca anche un altro
8. Dati un segmento $\overline{AB}$ e una semiretta uscente da C, esiste un punto D sulla semiretta tale che $\overline{CD} \equiv \overline{AB}$
9. Ogni segmento è congruente a se stesso
10. Due segmenti congruenti a un terzo sono congruenti tra loro
11. Dato un angolo $\angle sAt$ e un punto B, esistono semirette u e v uscenti da B uniche tali che $\angle sAt \equiv \angle uBv$
12. Ogni angolo è congruente a se stesso
13. Due angoli congruenti a un altro sono congruenti tra loro
14. Due triangoli che hanno congruenti due lati e l'angolo compreso hanno tutti gli altri elementi congruenti
15. Dati segmenti $\overline{AB}$ e $\overline{CD}$ esiste un numero naturale n e punti $A_1, \ldots, A_n$ sulla semiretta uscente da A che contiene B tali che $\overline{CD} \equiv \overline{AA_1} \equiv \overline{A_iA_{i+1}}$, $i = 1, \ldots, n-1$ e B è tra A e A_n
16. È impossibile estendere una retta con altri punti conservando la validità degli assiomi precedenti
17. Dato un punto A e una retta r che non contiene A, se le rette s e t passano per A e sono parallele a r, allora coincidono

Gli assiomi di Hilbert

1. Dati due punti distinti esiste una e una sola retta che li contiene
2. Ogni retta ha almeno due punti distinti
3. Esistono tre punti non allineati
4. Se A è tra B e C, allora A è anche tra C e B
5. Se A è tra B e C, allora i tre punti stanno sulla stessa retta
6. Dati tre punti distinti e allineati, esattamente uno è tra gli altri due
7. Dati un triangolo e una retta che non passa per nessuno dei vertici, se la retta interseca un lato del triangolo allora ne interseca anche un altro
8. Dati un segmento $\overline{AB}$ e una semiretta uscente da C, esiste un punto D sulla semiretta tale che $\overline{CD} \equiv \overline{AB}$
9. Ogni segmento è congruente a se stesso
10. Due segmenti congruenti a un terzo sono congruenti tra loro
11. Dato un angolo $\angle sAt$ e un punto B, esistono semirette u e v uscenti da B uniche tali che $\angle sAt \equiv \angle uBv$
12. Ogni angolo è congruente a se stesso
13. Due angoli congruenti a un altro sono congruenti tra loro
14. Due triangoli che hanno congruenti due lati e l'angolo compreso hanno tutti gli altri elementi congruenti
15. Dati segmenti $\overline{AB}$ e $\overline{CD}$ esiste un numero naturale n e punti $A_1,\dots, A_n$ sulla semiretta uscente da A che contiene B tali che $\overline{CD} \equiv \overline{AA_1} \equiv \overline{A_iA_{i+1}}$, $i = 1, \dots, n-1$ e B è tra A e A_n
16. È impossibile estendere una retta con altri punti conservando la validità degli assiomi precedenti
17. Dato un punto A e una retta r che non contiene A, se le rette s e t passano per A e sono parallele a r, allora coincidono

Gli assiomi di Hilbert

1. Dati due punti distinti esiste una e una sola retta che li contiene
2. Ogni retta ha almeno due punti distinti
3. Esistono tre punti non allineati
4. Se A è tra B e C, allora A è anche tra C e B
5. Se A è tra B e C, allora i tre punti stanno sulla stessa retta
6. Dati tre punti distinti e allineati, esattamente uno è tra gli altri due
7. Dati un triangolo e una retta che non passa per nessuno dei vertici, se la retta interseca un lato del triangolo allora ne interseca anche un altro
8. Dati un segmento $\overline{AB}$ e una semiretta uscente da C, esiste un punto D sulla semiretta tale che $\overline{CD} \equiv \overline{AB}$
9. Ogni segmento è congruente a se stesso
10. Due segmenti congruenti a un terzo sono congruenti tra loro
11. Dato un angolo $\angle sAt$ e un punto B, esistono semirette u e v uscenti da B uniche tali che $\angle sAt \equiv \angle uBv$
12. Ogni angolo è congruente a se stesso
13. Due angoli congruenti a un altro sono congruenti tra loro
14. Due triangoli che hanno congruenti due lati e l'angolo compreso hanno tutti gli altri elementi congruenti
15. Dati segmenti $\overline{AB}$ e $\overline{CD}$ esiste un numero naturale n e punti $A_1, \ldots, A_n$ sulla semiretta uscente da A che contiene B tali che $\overline{CD} \equiv \overline{AA_1} \equiv \overline{A_iA_{i+1}}$, $i = 1, \ldots, n-1$ e B è tra A e A_n
16. È impossibile estendere una retta con altri punti conservando la validità degli assiomi precedenti
17. Dato un punto A e una retta r che non contiene A, se le rette s e t passano per A e sono parallele a r, allora coincidono

Gli assiomi di Hilbert

1. Dati due punti distinti esiste una e una sola retta che li contiene
2. Ogni retta ha almeno due punti distinti
3. Esistono tre punti non allineati
4. Se A è tra B e C, allora A è anche tra C e B
5. Se A è tra B e C, allora i tre punti stanno sulla stessa retta
6. Dati tre punti distinti e allineati, esattamente uno è tra gli altri due
7. Dati un triangolo e una retta che non passa per nessuno dei vertici, se la retta interseca un lato del triangolo allora ne interseca anche un altro
8. Dati un segmento $\overline{AB}$ e una semiretta uscente da C, esiste un punto D sulla semiretta tale che $\overline{CD} \equiv \overline{AB}$
9. Ogni segmento è congruente a se stesso
10. Due segmenti congruenti a un terzo sono congruenti tra loro
11. Dato un angolo $\angle sAt$ e un punto B, esistono semirette u e v uscenti da B uniche tali che $\angle sAt \equiv \angle uBv$
12. Ogni angolo è congruente a se stesso
13. Due angoli congruenti a un altro sono congruenti tra loro
14. Due triangoli che hanno congruenti due lati e l'angolo compreso hanno tutti gli altri elementi congruenti
15. Dati segmenti $\overline{AB}$ e $\overline{CD}$ esiste un numero naturale n e punti $A_1,\dots, A_n$ sulla semiretta uscente da A che contiene B tali che $\overline{CD} \equiv \overline{AA_1} \equiv \overline{A_iA_{i+1}}$, $i = 1, \dots, n-1$ e B è tra A e A_n
16. È impossibile estendere una retta con altri punti conservando la validità degli assiomi precedenti
17. Dato un punto A e una retta r che non contiene A, se le rette s e t passano per A e sono parallele a r, allora coincidono

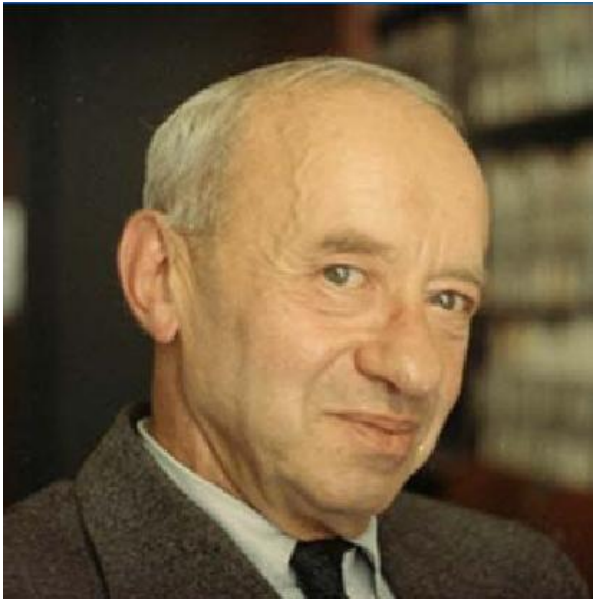
Gli assiomi di Hilbert

1. Dati due punti distinti esiste una e una sola retta che li contiene
2. Ogni retta ha almeno due punti distinti
3. Esistono tre punti non allineati
4. Se A è tra B e C, allora A è anche tra C e B
5. Se A è tra B e C, allora i tre punti stanno sulla stessa retta
6. Dati tre punti distinti e allineati, esattamente uno è tra gli altri due
7. Dati un triangolo e una retta che non passa per nessuno dei vertici, se la retta interseca un lato del triangolo allora ne interseca anche un altro
8. Dati un segmento $\overline{AB}$ e una semiretta uscente da C, esiste un punto D sulla semiretta tale che $\overline{CD} \equiv \overline{AB}$
9. Ogni segmento è congruente a se stesso
10. Due segmenti congruenti a un terzo sono congruenti tra loro
11. Dato un angolo $\angle sAt$ e un punto B, esistono semirette u e v uscenti da B uniche tali che $\angle sAt \equiv \angle uBv$
12. Ogni angolo è congruente a se stesso
13. Due angoli congruenti a un altro sono congruenti tra loro
14. Due triangoli che hanno congruenti due lati e l'angolo compreso hanno tutti gli altri elementi congruenti
15. Dati segmenti $\overline{AB}$ e $\overline{CD}$ esiste un numero naturale n e punti $A_1,\dots, A_n$ sulla semiretta uscente da A che contiene B tali che $\overline{CD} \equiv \overline{AA_1} \equiv \overline{A_iA_{i+1}}$, $i = 1, \dots, n-1$ e B è tra A e A_n
16. È impossibile estendere una retta con altri punti conservando la validità degli assiomi precedenti
17. Dato un punto A e una retta r che non contiene A, se le rette s e t passano per A e sono parallele a r, allora coincidono

Gli assiomi di Hilbert

1. Dati due punti distinti esiste una e una sola retta che li contiene
2. Ogni retta ha almeno due punti distinti
3. Esistono tre punti non allineati
4. Se A è tra B e C, allora A è anche tra C e B
5. Se A è tra B e C, allora i tre punti stanno sulla stessa retta
6. Dati tre punti distinti e allineati, esattamente uno è tra gli altri due
7. Dati tre punti non allineati A, B e C e una retta che non contiene nessuno di essi, se la retta interseca $\overline{AB}$ allora la retta interseca $\overline{BC}$ oppure $\overline{AC}$
8. Dati un segmento $\overline{AB}$ e una semiretta uscente da C, esiste un punto D sulla semiretta tale che $\overline{CD} \equiv \overline{AB}$
9. Ogni segmento è congruente a se stesso
10. Due segmenti congruenti a un terzo sono congruenti tra loro
11. Dato un angolo $\angle sAt$ e un punto B, esistono semirette u e v uscenti da B uniche tali che $\angle sAt \equiv \angle uBv$
12. Ogni angolo è congruente a se stesso
13. Due angoli congruenti a un altro sono congruenti tra loro
14. Due triangoli che hanno congruenti due lati e l'angolo compreso hanno tutti gli altri elementi congruenti
15. Dati segmenti $\overline{AB}$ e $\overline{CD}$ esiste un numero naturale n e punti $A_1,\dots, A_n$ sulla semiretta uscente da A che contiene B tali che $\overline{CD} \equiv \overline{AA_1} \equiv \overline{A_iA_{i+1}}$, $i = 1, \dots, n-1$ e B è tra A e A_n
16. È impossibile estendere una retta con altri punti conservando la validità degli assiomi precedenti
17. Dato un punto A e una retta r che non contiene A, se le rette s e t passano per A e sono parallele a r, allora coincidono

Gli assiomi di Tarski



Gli assiomi di Tarski

- Tre punti sono *allineati* se uno sta sul segmento determinato dagli altri due

1. Il segmento $\overline{ab}$ è congruente al segmento $\overline{ba}$
2. Un segmento congruente al segmento $\overline{cc}$ è sempre della forma $\overline{aa}$
3. Due segmenti congruenti a un terzo sono congruenti tra loro
4. Fissato un punto su ciascuno di due lati di un triangolo, i segmenti che li congiungono ai vertici opposti si intersecano
5. Date proprietà P e Q che determinano classi contigue su una retta, esiste almeno un elemento che le separa
6. Esistono tre punti non allineati
7. Il luogo dei punti equidistanti da due punti fissati è una retta
8. Tre punti non allineati stanno su una circonferenza
9. Due triangoli che hanno due lati e l'angolo compreso congruenti hanno anche il terzo lato congruenti
10. Da un punto a si può tracciare un segmento fissato in direzione e verso fissati

Gli assiomi di Tarski

- $\mathrm{A}(a,b,c) \overset{\mathrm{df}}{\Leftrightarrow} [\mathrm{T}(a,b,c) \vee \mathrm{T}(b,c,a) \vee \mathrm{T}(c,a,b)]$

1. $\forall_a \forall_b \mathrm{C}(a,b,b,a)$
2. $\forall_a \forall_b \forall_c [\mathrm{C}(a,b,c,c) \Rightarrow a = b]$
3. $\forall_a \forall_b \forall_c \forall_d \forall_e \forall_f [(\mathrm{C}(a,b,c,d) \wedge \mathrm{C}(a,b,e,f)) \Rightarrow \mathrm{C}(c,d,e,f)]$
4. $\forall_a \forall_b \forall_c \forall_d \forall_e \left[(\mathrm{T}(d,a,c) \wedge \mathrm{T}(e,b,c)) \Rightarrow \exists_f (\mathrm{T}(f,d,b) \wedge \mathrm{T}(f,e,a))\right]$
5. $\forall_{x_1} \cdots \forall_{x_n} \left[\exists_c \forall_a \forall_b \left[(P(\vec{x},a) \wedge Q(\vec{x},b)) \Rightarrow \mathrm{T}(c,a,b)\right] \Rightarrow \exists_d \forall_a \forall_b \left[(P(\vec{x},a) \wedge Q(\vec{x},b)) \Rightarrow \mathrm{T}(a,d,b)\right]\right]$
6. $\exists_a \exists_b \exists_c \neg \mathrm{A}(a,b,c)$
7. $\forall_a \forall_b \forall_c \forall_d \forall_e [(a \neq b \wedge \mathrm{C}(a,c,b,c) \wedge \mathrm{C}(a,d,b,d) \wedge \mathrm{C}(a,e,b,e)) \Rightarrow \mathrm{A}(c,d,e)]$
8. $\forall_a \forall_b \forall_c \left[\neg \mathrm{A}(a,b,c) \Rightarrow \exists_d (\mathrm{C}(a,d,b,d) \wedge \mathrm{C}(a,d,c,d))\right]$
9. $\forall_a \forall_b \forall_c \forall_d \forall_{a_1} \forall_{b_1} \forall_{c_1} \forall_{d_1}$
   $[[(a \neq b \wedge \mathrm{T}(a,b,c) \wedge \mathrm{T}(a_1,b_1,c_1) \wedge \mathrm{C}(a,b,a_1,b_1) \wedge \mathrm{C}(b,c,b_1,c_1) \wedge \mathrm{C}(a,d,a_1,d_1) \wedge \mathrm{C}(b,d,b_1,d_1))] \Rightarrow \mathrm{C}(c,d,c_1,d_1)]$
10. $\forall_a \forall_b \forall_c \forall_d \exists_e [\mathrm{T}(d,a,e) \wedge \mathrm{C}(a,e,b,c)]$

La retta euclidea è un modello dell'analisi reale

Teorema

Fissati due punti O e U di una retta nella geometria di Hilbert, la funzione

$$\{X \mid X \text{ è sulla retta } OU\} \xrightarrow{\ p\ } \mathbb{R}$$

$$X \longmapsto \begin{cases} \dfrac{\overline{OX}}{\overline{OU}} & \text{se } X \text{ tra } O \text{ e } U \text{ oppure } U \text{ tra } O \text{ e } X \\ -\dfrac{\overline{OX}}{\overline{OU}} & \text{se } O \text{ tra } X \text{ e } U \end{cases}$$

che, di un punto arbitrario X della retta, calcola il rapporto $p(X)$ tra la lunghezza di OX e la lunghezza di OU e attribuisce segno negativo esattamente nel caso che X e U siano da parti opposte di O, produce una biezione verso $\mathbb{R}$
In particolare

$$\text{se } p(X_1) \le p(X) \le p(X_2), \text{ allora } X \text{ è tra } X_1 \text{ e } X_2$$

La geometria euclidea è riconducibile all'analisi reale

Teorema

L'insieme $\mathbb{R}^2$ *con le relazioni*

$$[\![\mathrm{T}]\!] \stackrel{df}{=} \left\{ (\langle x_1,y_1\rangle,\langle x_2,y_2\rangle,\langle x_3,y_3\rangle) \,\middle|\, (x_2\neq x_1\neq x_3 \vee y_2\neq y_1\neq y_3)\wedge\exists_k \left(0<k<1\wedge(x_1-x_2)=k(x_3-x_2)\wedge(y_1-y_2)(y_3-y_2)\right) \right\}$$

$$[\![\mathrm{C}_s]\!] \stackrel{df}{=} \left\{ (\langle x_1,y_1\rangle,\langle x_2,y_2\rangle,\langle x_3,y_3\rangle,\langle x_4,y_4\rangle) \,\middle|\, \frac{\sqrt{(x_2-x_1)^2+(y_2-y_1)^2}}{\sqrt{(x_4-x_3)^2+(y_4-y_3)^2}}=1 \right\}$$

$$[\![\mathrm{C}_a]\!] \stackrel{df}{=} \left\{ (\langle x_0,y_0\rangle,\langle x_1,y_1\rangle,\langle x_2,y_2\rangle,\langle v_0,w_0\rangle,\langle v_1,w_1\rangle,\langle v_2,w_2\rangle) \,\middle|\, \begin{array}{l} \dfrac{(x_1-x_0)(x_2-x_0)+(y_1-y_0)(y_2-y_0)}{\sqrt{(x_1-x_0)^2+(x_2-x_0)^2}\sqrt{(y_1-y_0)^2+(y_2-y_0)^2}} = \\ = \dfrac{(v_1-v_0)(v_2-v_0)+(w_1-w_0)(w_2-w_0)}{\sqrt{(v_1-v_0)^2+(v_2-v_0)^2}\sqrt{(w_1-w_0)^2+(w_2-w_0)^2}} \end{array} \right\}$$

verifica tutti gli assiomi di Hilbert

L'analisi reale è riconducibile alla teoria degli insiemi

Teorema

- $\mathbb{R} \xrightarrow{\sim} \left\{(a_n)_n : \mathbb{N} \longrightarrow \mathbb{Q} \;\middle|\; \forall_k \exists_n \forall_{m_1} \forall_{m_2} \left[(n < m_1 \wedge n < m_2) \Rightarrow |a_{m_1} - a_{m_2}| < \frac{1}{k}\right]\right\} \Big/ \simeq$

  $$\text{dove} \quad (a_n)_n \simeq (b_n)_n \quad \text{se} \quad \forall_k \exists_n \forall_m \left[(n < m) \Rightarrow |a_m - b_m| < \frac{1}{k}\right]$$

- $\mathbb{Q} \xrightarrow{\sim} (\mathbb{Z} \times \mathbb{N}_*)/_{\cong} \qquad \text{dove} \quad (z_1, z_2) \cong (w_1, w_2) \quad \text{se} \quad z_1 w_2 = w_1 z_2$

- $\mathbb{Z} \xrightarrow{\sim} (\mathbb{N} \times \mathbb{N})/_{\approx} \qquad \text{dove} \quad (n_1, n_2) \approx (m_1, m_2) \quad \text{se} \quad n_1 + m_2 = m_1 + n_2$

- $\mathbb{N} \xrightarrow{\sim} \left\{x \;\middle|\; \forall_y \left[\left(\varnothing \in y \wedge \forall_z \left(z \in y \Rightarrow z \cup \{z\} \in y\right)\right) \Rightarrow x \in y\right]\right\}$

Aspetti costruttivi

Aspetti costruttivi

- Per A un insieme numerabile, la collezione $\mathbf{P}(A)$ dei suoi sottoinsiemi è fuori dalla comprensione; i suoi elementi non possono essere introdotti cumulativamente
- L'insieme $\mathbb{N}$ deve essere compreso come costruzione esplicita; non c'è alcun controllo sugli elementi pensandolo come il più piccolo insieme induttivo
- Anche se le costruzioni di $\mathbb{Z}$ e $\mathbb{Q}$ possono essere rese più esplicite senza utilizzare relazioni di equivalenza $\cong$ e $\approx$ rimane la necessità di identificare successioni di Cauchy $(a_n)_n \colon \mathbb{N} \longrightarrow \mathbb{Q}$
- Anche la costruzione di Dedekind di $\mathbb{R}$ impone di fare riferimento a una collezione potenza $\mathbf{P}(\mathbb{Q})$

Le parole di una dimostrazione formale

Le parole di una dimostrazione formale

Definizione

Una *conseguenza formale* è

$$x_{j_1}, x_{j_2}, \dots, x_{j_m}; \alpha_1, \alpha_2, \dots, \alpha_n \vdash \beta$$

dove

1. $(x_{j_1}, x_{j_2}, \dots, x_{j_m})$ è una lista di variabili a due a due distinte
2. $\alpha_1, \alpha_2, \dots, \alpha_n, \beta$ sono formule ben formate nelle variabili indicate

Regole formali strutturali

$$\frac{}{\vec{x};\Gamma,\varphi \vdash \varphi}\ \text{Ipotesi} \qquad \frac{\vec{x};\Gamma,\varphi,\psi,\Delta \vdash \vartheta}{\vec{x};\Gamma,\psi,\varphi,\Delta \vdash \vartheta}\ \text{Scambio} \qquad \frac{\vec{x};\Gamma \vdash \vartheta}{\vec{x};\Gamma,\varphi \vdash \vartheta}\ \text{Indebolimento}$$

$$\frac{\vec{x};\Gamma \vdash \varphi \quad \vec{x};\Gamma,\varphi \vdash \psi}{\vec{x};\Gamma \vdash \psi}\ \text{Taglio}$$

Regole formali per i connettivi

$$\frac{\vec{x}; \Gamma \vdash \varphi \wedge \psi}{\vec{x}; \Gamma \vdash \varphi} \wedge\text{-El1} \qquad \frac{\vec{x}; \Gamma \vdash \varphi \wedge \psi}{\vec{x}; \Gamma \vdash \psi} \wedge\text{-El2} \qquad \frac{\vec{x}; \Gamma \vdash \varphi \quad \vec{x}; \Gamma \vdash \psi}{\vec{x}; \Gamma \vdash \varphi \wedge \psi} \wedge\text{-In}$$

$$\frac{\vec{x}; \Gamma \vdash \varphi}{\vec{x}; \Gamma \vdash \varphi \vee \psi} \vee\text{-In1} \qquad \frac{\vec{x}; \Gamma \vdash \psi}{\vec{x}; \Gamma \vdash \varphi \vee \psi} \vee\text{-In2} \qquad \frac{\vec{x}; \Gamma, \varphi \vdash \vartheta \quad \vec{x}; \Gamma, \psi \vdash \vartheta}{\vec{x}; \Gamma, \varphi \vee \psi \vdash \vartheta} \vee\text{-El}$$

$$\frac{\vec{x}; \Gamma \vdash \varphi \qquad \vec{x}; \Gamma \vdash \varphi \Rightarrow \psi}{\vec{x}; \Gamma \vdash \psi} \Rightarrow\text{-El} \qquad \frac{\vec{x}; \Gamma, \varphi \vdash \psi}{\vec{x}; \Gamma \vdash \varphi \Rightarrow \psi} \Rightarrow\text{-In}$$

$$\frac{}{\vec{x}; \Gamma \vdash \top} \top\text{-In} \qquad \frac{}{\vec{x}; \Gamma, \bot \vdash \vartheta} \bot\text{-El} \qquad \frac{}{\vec{x}; \Gamma, \varphi, \neg\varphi \vdash \bot} \neg\text{-El} \qquad \frac{\vec{x}; \Gamma, \varphi \vdash \bot}{\vec{x}; \Gamma \vdash \neg\varphi} \neg\text{-In}$$

$$\frac{\vec{x}; \Gamma, \neg\varphi \vdash \bot}{\vec{x}; \Gamma \vdash \varphi} \text{ per assurdo}$$

Regole formali per gli operatori

$$\frac{}{\vec{x}; \Gamma, t = s, \varphi[t/x] \vdash \varphi[s/x]} \text{ = -El} \qquad \frac{}{\vec{x}; \Gamma \vdash t = t} \text{ = -In}$$

$$\frac{\vec{x}; \Gamma \vdash \forall_{x_j:T} \varphi}{\vec{x}; \Gamma \vdash \varphi[t/x_j]} \forall\text{-El} \qquad \frac{\vec{x}, x_j : T; \Gamma \vdash \varphi}{\vec{x}; \Gamma \vdash \forall_{x_j:T} \varphi} \forall\text{-In}$$

$$\frac{\vec{x}; \Gamma \vdash \varphi[t/x_j]}{\vec{x}; \Gamma \vdash \exists_{x_j:T} \varphi} \exists\text{-In} \qquad \frac{\vec{x}, x_j : T; \Gamma, \varphi \vdash \vartheta}{\vec{x}; \Gamma, \exists_{x_j:T} \varphi \vdash \vartheta} \exists\text{-El}$$

Le dimostrazioni formali e i teoremi

Definizione

Una *dimostrazione formale* è un albero finito in cui

- i nodi sono esempi di regole formali
- gli archi sono premessa di un nodo e conclusione di un altro
- le foglie sono regole iniziali

La conseguenza alla radice della dimostrazione formale è un *teorema formale*

Esempio di dimostrazione formale

$$\dfrac{\dfrac{}{x;(\varphi \wedge \psi) \Rightarrow \vartheta, \varphi, \psi \vdash \varphi}\,\text{Ipotesi} \quad \dfrac{}{x;(\varphi \wedge \psi) \Rightarrow \vartheta, \varphi, \psi \vdash \psi}\,\text{Ipotesi}}{x;(\varphi \wedge \psi) \Rightarrow \vartheta, \varphi, \psi \vdash \varphi \wedge \psi}\,\wedge\text{-In} \qquad \dfrac{\dfrac{}{\vec{x};(\varphi \wedge \psi) \Rightarrow \vartheta, \varphi, \psi, \varphi \wedge \psi \vdash \varphi \wedge \psi}\,\text{Ipotesi} \quad \dfrac{}{\vec{x};(\varphi \wedge \psi) \Rightarrow \vartheta, \varphi, \psi, \varphi \wedge \psi \vdash (\varphi \wedge \psi) \Rightarrow \vartheta}\,\text{Ipotesi}}{x;(\varphi \wedge \psi) \Rightarrow \vartheta, \varphi, \psi, \varphi \wedge \psi \vdash \vartheta}\,\Rightarrow\text{-El}$$

$$\dfrac{x;(\varphi \wedge \psi) \Rightarrow \vartheta, \varphi, \psi \vdash \varphi \wedge \psi \qquad x;(\varphi \wedge \psi) \Rightarrow \vartheta, \varphi, \psi, \varphi \wedge \psi \vdash \vartheta}{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{x;(\varphi \wedge \psi) \Rightarrow \vartheta, \varphi, \psi \vdash \vartheta}{x;(\varphi \wedge \psi) \Rightarrow \vartheta, \varphi \vdash \psi \Rightarrow \vartheta}\,\Rightarrow\text{-In}}{x;(\varphi \wedge \psi) \Rightarrow \vartheta \vdash \varphi \Rightarrow (\psi \Rightarrow \vartheta)}\,\Rightarrow\text{-In}}{x;\vdash [(\varphi \wedge \psi) \Rightarrow \vartheta] \Rightarrow [\varphi \Rightarrow (\psi \Rightarrow \vartheta)]}\,\Rightarrow\text{-In}}{\vdash \forall_x\,[[(\varphi \wedge \psi) \Rightarrow \vartheta] \Rightarrow [\varphi \Rightarrow (\psi \Rightarrow \vartheta)]]}\,\forall\text{-In}}\,\text{Taglio}$$

Struttura delle regole

$$\frac{\vec{x};\Gamma \vdash \varphi \wedge \psi}{\vec{x};\Gamma \vdash \varphi}\ \wedge\text{-El1} \qquad \frac{\vec{x};\Gamma \vdash \varphi \wedge \psi}{\vec{x};\Gamma \vdash \psi}\ \wedge\text{-El2} \qquad \frac{\vec{x};\Gamma \vdash \varphi \quad \vec{x};\Gamma \vdash \psi}{\vec{x};\Gamma \vdash \varphi \wedge \psi}\ \wedge\text{-In}$$

$$\frac{\vec{x};\Gamma \vdash \varphi}{\vec{x};\Gamma \vdash \varphi \vee \psi}\ \vee\text{-In1} \qquad \frac{\vec{x};\Gamma \vdash \psi}{\vec{x};\Gamma \vdash \varphi \vee \psi}\ \vee\text{-In2} \qquad \frac{\vec{x};\Gamma \vdash \forall_{x_j:T}\varphi}{\vec{x};\Gamma \vdash \varphi[t/x_j]}\ \forall\text{-El} \qquad \frac{\vec{x};\Gamma \vdash \varphi[t/x_j]}{\vec{x};\Gamma \vdash \exists_{x_j:T}\varphi}\ \exists\text{-In}$$

$$\frac{\vec{x};\Gamma \vdash \varphi \qquad \vec{x};\Gamma \vdash \varphi \Rightarrow \psi}{\vec{x};\Gamma \vdash \psi}\ \Rightarrow\text{-El} \qquad \frac{\vec{x};\Gamma \vdash \bot}{\vec{x};\Gamma \vdash \vartheta}\ \bot\text{-El}^{+} \qquad \frac{\vec{x};\Gamma \vdash \varphi \qquad \vec{x};\Gamma \vdash \neg\varphi}{\vec{x};\Gamma \vdash \bot}\ \neg\text{-El}^{+}$$

$$\frac{\vec{x};\Gamma \vdash t = s \qquad \vec{x};\Gamma \vdash \varphi[t/x]}{\vec{x};\Gamma \vdash \varphi[s/x]}\ =\text{-El}^{+} \qquad \frac{}{\vec{x};\Gamma \vdash t = t}\ =\text{-In} \qquad \frac{}{\vec{x};\Gamma \vdash \top}\ \top\text{-In}$$

Struttura delle regole

$$\frac{\vec{x};\Gamma,\varphi\vee\psi,\varphi\vdash\vartheta \quad \vec{x};\Gamma,\varphi\vee\psi,\psi\vdash\vartheta}{\vec{x};\Gamma,\varphi\vee\psi\vdash\vartheta}\ \vee\text{-El}^{+} \qquad \frac{\vec{x};\Gamma,\varphi\vdash\psi}{\vec{x};\Gamma\vdash\varphi\Rightarrow\psi}\ \Rightarrow\text{-In} \qquad \frac{\vec{x};\Gamma,\varphi\vdash\bot}{\vec{x};\Gamma\vdash\neg\varphi}\ \neg\text{-In}$$

$$\frac{\vec{x};\Gamma,\neg\varphi\vdash\bot}{\vec{x};\Gamma\vdash\varphi}\ \text{per assurdo} \qquad \frac{\vec{x},x_j\colon T;\Gamma\vdash\varphi}{\vec{x};\Gamma\vdash\forall_{x_j:T}\varphi}\ \forall\text{-In} \qquad \frac{\vec{x},x_j\colon T;\Gamma,\exists_{x_j:T}\varphi,\varphi\vdash\vartheta}{\vec{x};\Gamma,\exists_{x_j:T}\varphi\vdash\vartheta}\ \exists\text{-El}^{+}$$

Struttura delle regole

$$\frac{}{\vec{x}; \Gamma, \varphi \vdash \varphi}\ \text{Ipotesi}$$

$$\frac{\vec{x}; \Gamma \vdash \vartheta}{\vec{x}; \Gamma, \varphi \vdash \vartheta}\ \text{Indeb.}$$

$$\frac{\vec{x}; \Gamma \vdash \varphi \quad \vec{x}; \Gamma, \varphi \vdash \psi}{\vec{x}; \Gamma \vdash \psi}\ \text{Taglio}$$

$$\frac{\vec{x}; \Gamma, \varphi, \psi, \Delta \vdash \vartheta}{\vec{x}; \Gamma, \psi, \varphi, \Delta \vdash \vartheta}\ \text{Scambio}$$

Esempio di dimostrazione formale

1:	$x : T$	presupposto
2:	$(\varphi \wedge \psi) \Rightarrow \vartheta$	presupposto
3:	φ	presupposto
4:	ψ	presupposto
5:	$\varphi \wedge \psi$	$\wedge$-In 3,4
6:	ϑ	$\Rightarrow$ -El 2,5
7:	$\psi \Rightarrow \vartheta$	$\Rightarrow$ -In 4-6
8:	$\varphi \Rightarrow (\psi \Rightarrow \vartheta)$	$\Rightarrow$ -In 3-7
9:	$[(\varphi \wedge \psi) \Rightarrow \vartheta] \Rightarrow [\varphi \Rightarrow (\psi \Rightarrow \vartheta)]$	$\Rightarrow$ -In 2-8
10:	$\forall_x [[(\varphi \wedge \psi) \Rightarrow \vartheta] \Rightarrow [\varphi \Rightarrow (\psi \Rightarrow \vartheta)]]$	$\forall$-In 1-9

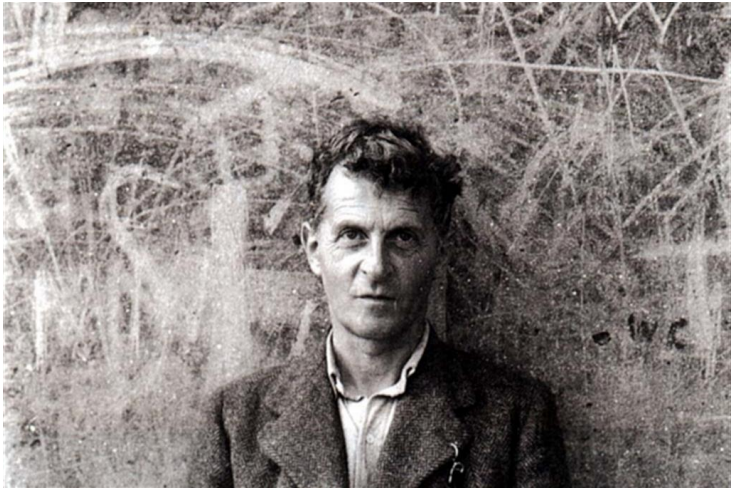
Per sperimentare si può usare JΨΡ∃ `http://www.japeforall.org.uk/japeforallindex.html` con il file `cdni.jt`.

Le dimostrazioni sono disponibili nella cartella.

Esempio di dimostrazione formale

«Il significato di una parola è il suo uso nel linguaggio»

Ludwig Wittgenstein, *Philosophische Untersuchungen* 43



La teoria dell'aritmetica

La teoria dell'aritmetica

1. La funzione "successore" è iniettiva
2. La funzione "successore" non è suriettiva
3. La funzione "somma con un numero" ha definizione per induzione
4. La funzione "prodotto con un numero" ha definizione per induzione
5. Per dimostrare una proprietà con parametri, basta dimostrare
   - la proprietà per zero, e
   - che, dalla proprietà per un numero, segue la proprietà per il successore di quel numero

La teoria dell'aritmetica

1. $\forall_x \forall_y [\mathrm{s}(x) = \mathrm{s}(y) \Rightarrow x = y]$
2. $\forall_x \neg\, \mathrm{s}(x) = 0$
3. $\forall_x \left[0 + x = x \wedge \forall_y\, x + \mathrm{s}(y) = \mathrm{s}(x + y)\right]$
4. $\forall_x \left[0 \times x = 0 \wedge \forall_y\, x \times \mathrm{s}(y) = (x \times y) + x\right]$
5. $\forall_{x_1} \cdots \forall_{x_n} \left[\left[\varphi(\vec{x}, 0) \wedge \forall_y\, (\varphi(\vec{x}, y) \Rightarrow \varphi(\vec{x}, \mathrm{s}(y)))\right] \Rightarrow \forall_x \varphi(\vec{x}, x)\right]$

I risultati negativi

Problema n. 2

Determinare con metodi finitistici se la teoria dell'aritmetica di Peano è coerente

I risultati negativi

I risultati negativi

Problema n. 2

Determinare con metodi finitistici se la teoria dell'aritmetica di Peano è coerente

Teorema (Gödel, Primo Teorema di Incompletezza)

In qualunque teoria $\mathcal{T}$ che sia effettivamente assiomatizzabile e estenda l'aritmetica di Peano, esistono enunciati φ tali che

$$\mathcal{T} \nvdash \varphi \qquad e \qquad \mathcal{T} \nvdash \neg\varphi$$

Teorema (Gödel, Secondo Teorema di Incompletezza)

Qualunque teoria $\mathcal{T}$ che sia effettivamente assiomatizzabile e estenda l'aritmetica di Peano può esprimere la propria coerenza.
Ma un tale enunciato γ è indecidibile, cioè

$$\mathcal{T} \nvdash \gamma \qquad e \qquad \mathcal{T} \nvdash \neg\gamma$$

Quanto è negativo?

Problema n. 2

Determinare con metodi finitistici se la teoria dell'aritmetica di Peano è coerente

Quanto è negativo?

Problema n. 2

Determinare con metodi finitistici se la teoria dell'aritmetica di Peano è coerente

Teorema (Gentzen, Teorema di eliminazione del taglio)

La teoria dell'aritmetica con il principio di induzione ristretto a formule senza parametri e con dimostrazioni a struttura transfinita ricorsiva è coerente

Quanto è negativo?

Problema n. 2

Determinare con metodi finitistici se la teoria dell'aritmetica di Peano è coerente

Teorema (Gentzen, Teorema di eliminazione del taglio)

La teoria dell'aritmetica con il principio di induzione ristretto a formule senza parametri e con dimostrazioni a struttura transfinita ricorsiva è coerente

Teorema (Tarski–Givant)

La teoria $\mathcal{G}$ della geometria di Tarski è decidibile, cioè per ogni enunciato α

$$\mathcal{G} \vdash \gamma \qquad \textit{oppure} \qquad \mathcal{G} \vdash \neg\gamma$$

I risultati negativi, II

Problema n. 10

Dato un polinomio a coefficienti interi $p(a_1, \dots, a_k, x_1, \dots, x_n)$ in $a_1, \dots, a_k, x_1, \dots, x_n$, produrre un procedimento che determini, mediante un numero finito di operazioni, per quali parametri $a_1, \dots, a_k$ l'equazione $p(a_1, \dots, a_k, x_1, \dots, x_n) = 0$, nelle variabili $x_1, \dots, x_n$, ha o non ha soluzioni intere

I risultati negativi, II

I risultati negativi, II

Problema n. 10

Dato un polinomio a coefficienti interi $p(a_1, \dots, a_k, x_1, \dots, x_n)$ in $a_1, \dots, a_k, x_1, \dots, x_n$, produrre un procedimento che determini, mediante un numero finito di operazioni, per quali parametri $a_1, \dots, a_k$ l'equazione $p(a_1, \dots, a_k, x_1, \dots, x_n) = 0$, nelle variabili $x_1, \dots, x_n$, ha o non ha soluzioni intere

Teorema (Bowman–Matijasevič–Robinson)

Gli insiemi diofantei

$$\left\{ \langle a_1, \dots, a_k \rangle \in \mathbb{N}^k \;\middle|\; \exists_{x_1} \cdots \exists_{x_n} \; p(a_1, \dots, a_k, x_1, \dots, x_n) = 0 \right\}$$

sono gli insiemi effettivamente calcolabili

Corollario

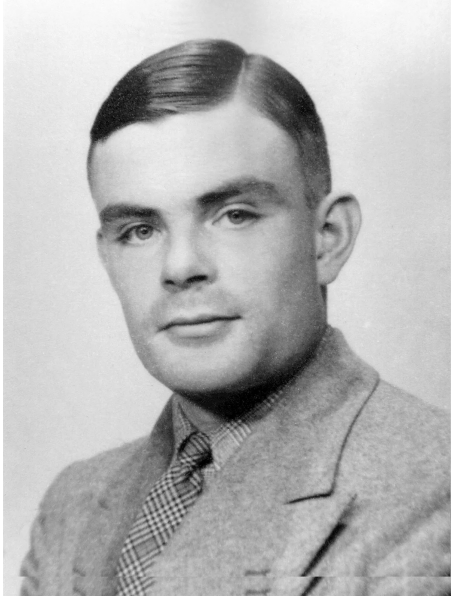
Non esiste un procedimento che risolva il problema n. 10

Das Entscheidungsproblem

Il problema della decisione

Determinare un procedimento che determini, mediante un numero finito di operazioni, se un problema matematico ha soluzione oppure no

Das Entscheidungsproblem



Das Entscheidungsproblem

Il problema della decisione

Determinare un procedimento che determini, mediante un numero finito di operazioni, se un problema matematico ha soluzione oppure no

Teorema (Turing, Teorema della Macchina Universale)

Esiste una macchina che esegue tutte le altre macchine

Corollario

Non esiste una macchina che risolva il problema della decisione

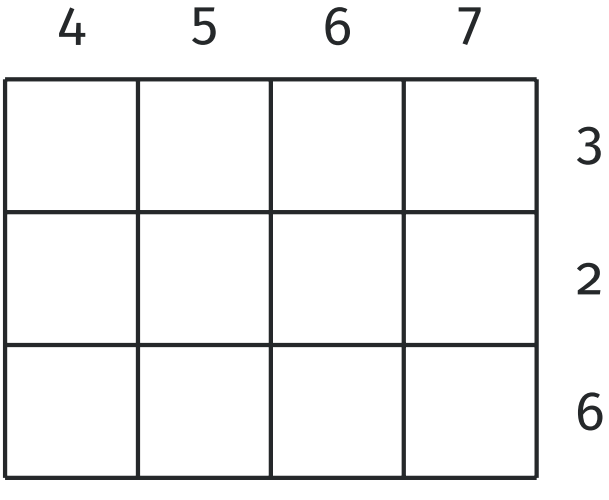
Università di Genova | DIMA DIPARTIMENTO DI MATEMATICA

Parte II

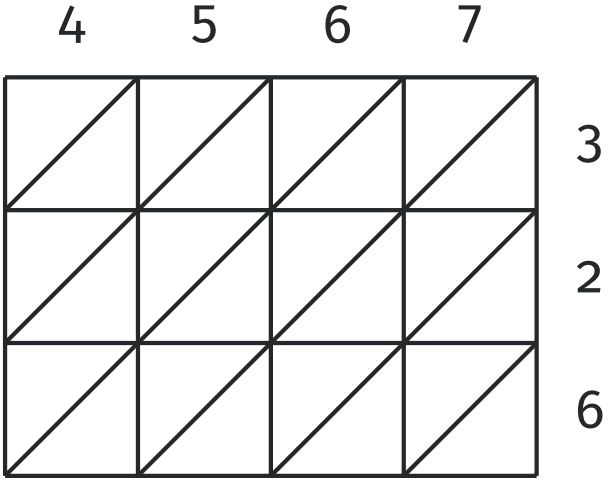
Le funzioni calcolabili

UNIVERSITÀ DI PARMA

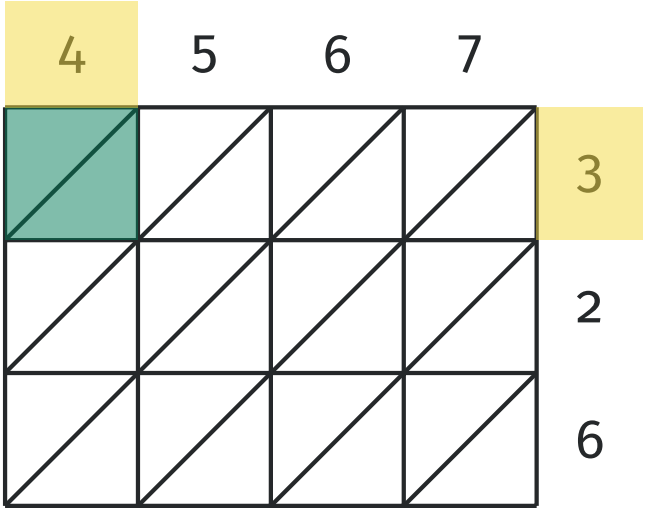
Un algoritmo



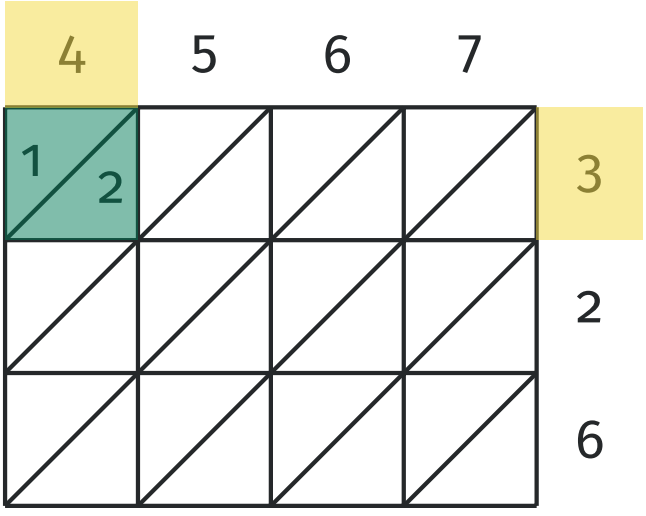
Un algoritmo



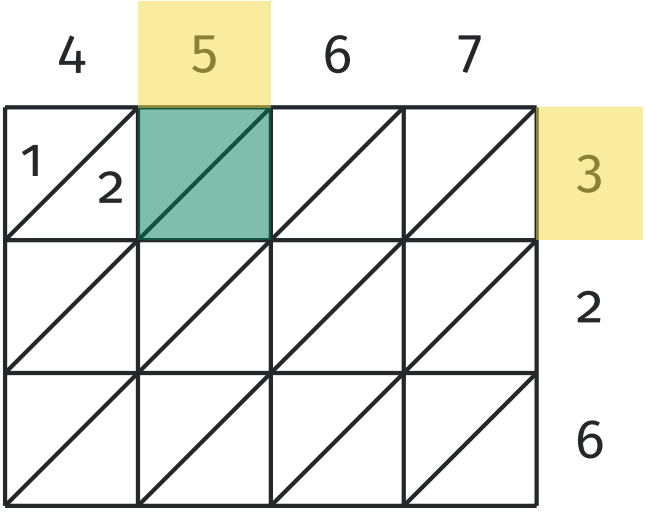
Un algoritmo



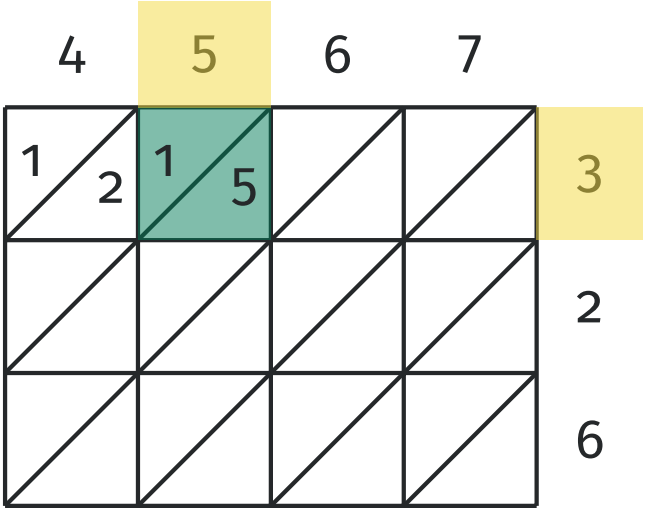
Un algoritmo



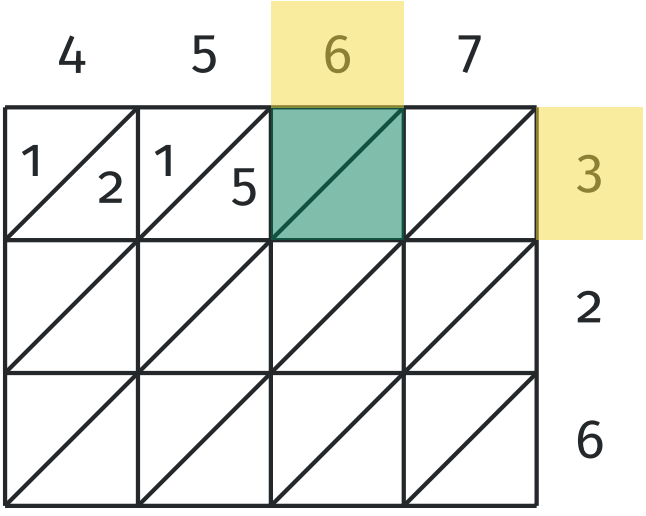
Un algoritmo



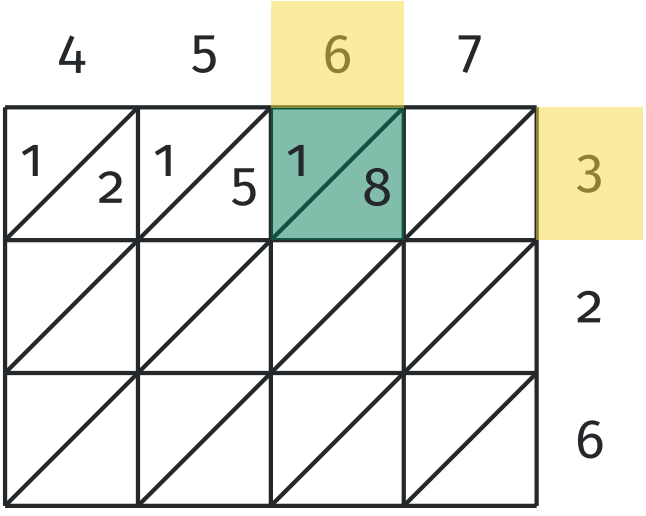
Un algoritmo



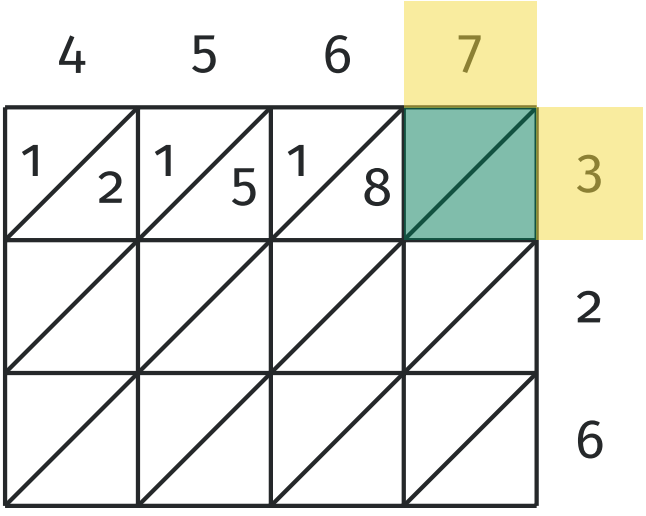
Un algoritmo



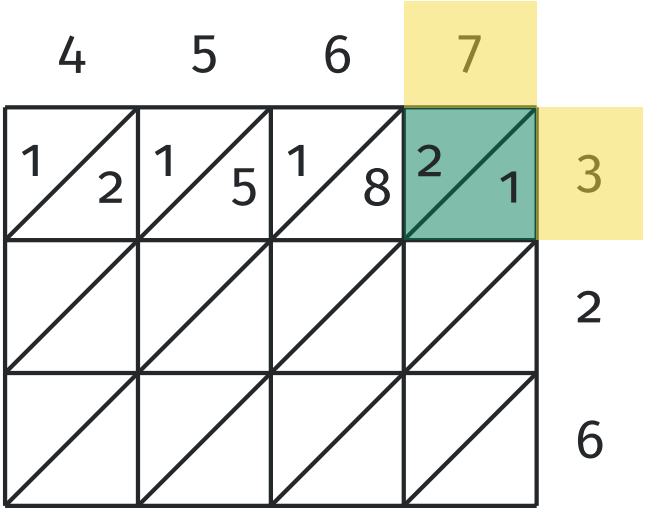
Un algoritmo



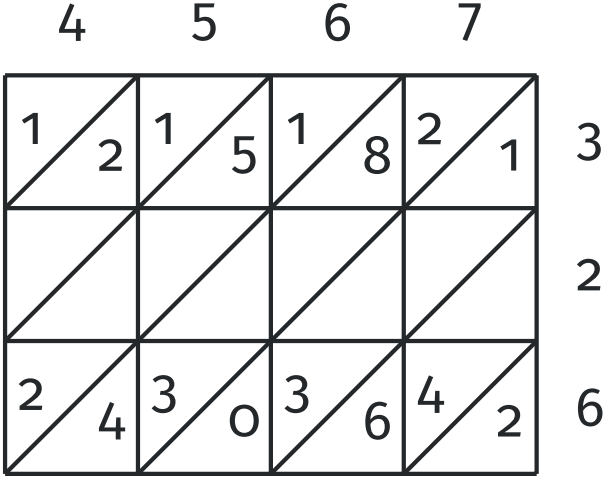
Un algoritmo



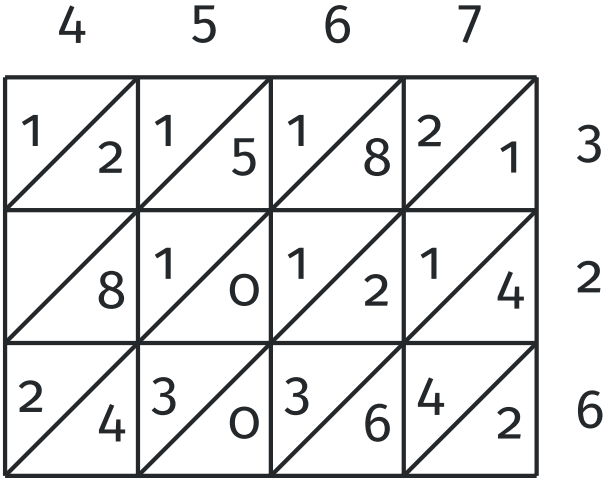
Un algoritmo



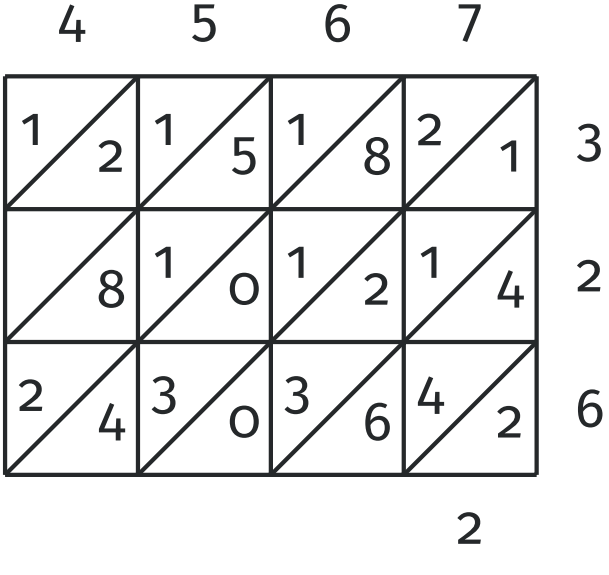
Un algoritmo



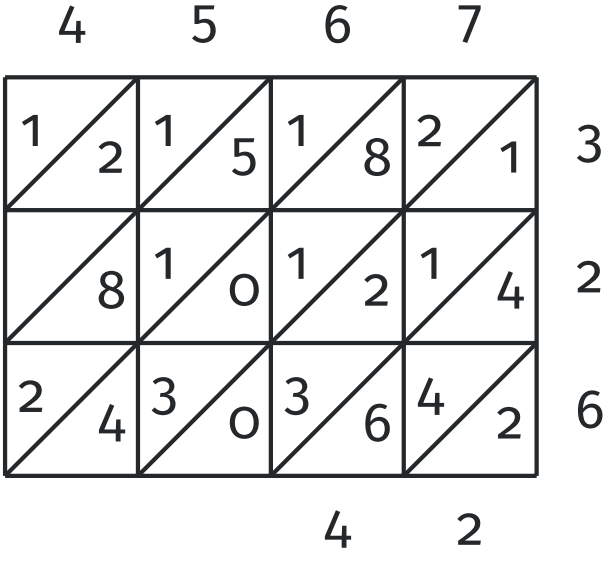
Un algoritmo



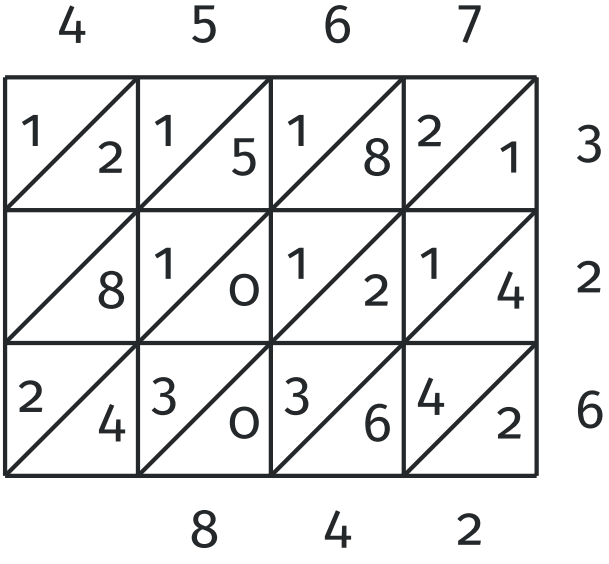
Un algoritmo



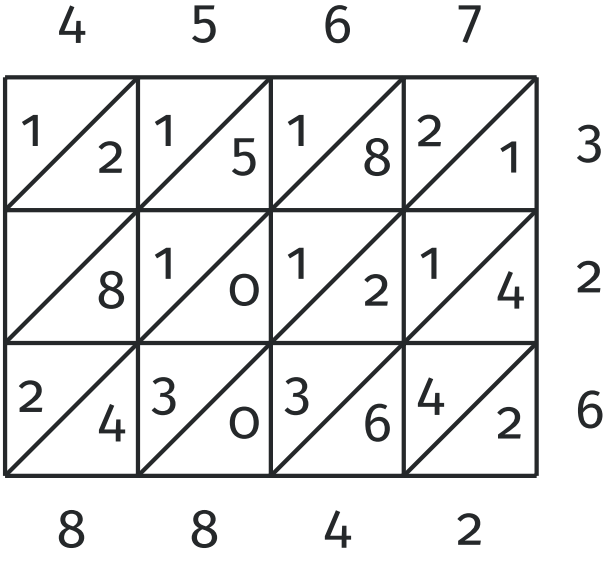
Un algoritmo



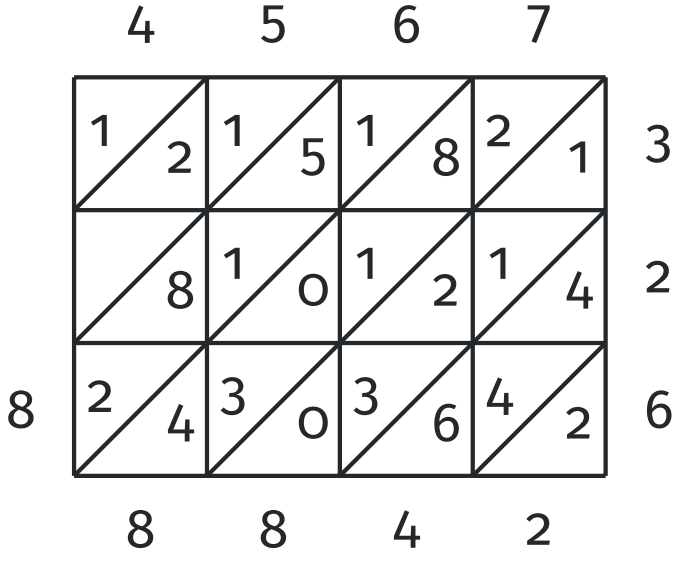
Un algoritmo



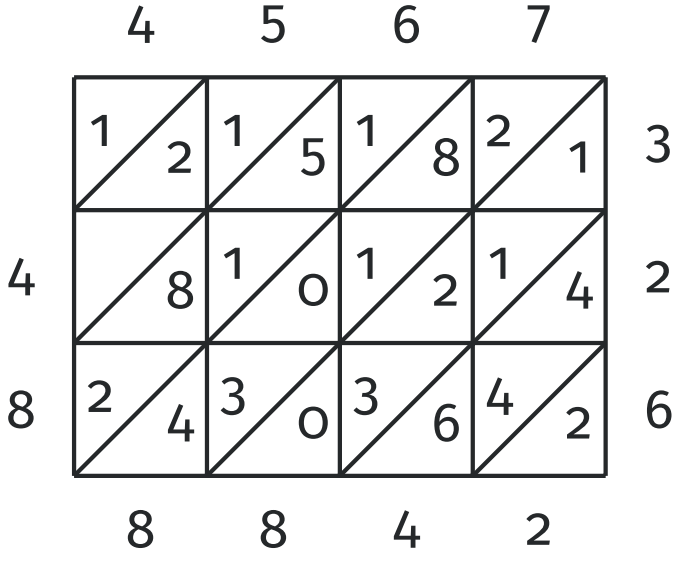
Un algoritmo



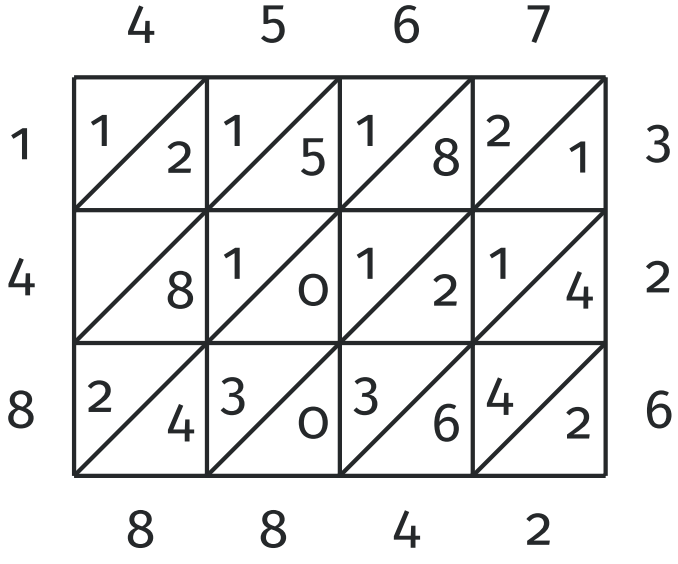
Un algoritmo



Un algoritmo



Un algoritmo



On computable numbers (A. Turing, 1936)

On computable numbers (A. Turing, 1936)

Possiamo paragonare un uomo nell'atto di calcolare un numero reale a una macchina che è in grado di considerare soltanto un numero finito di condizioni $q_1, q_2, \ldots, q_R$ che chiameremo *configurazioni-macchina*.
La macchina è provvista di un *nastro* (l'analogo della carta), che scorre attraverso di essa ed è diviso in sezioni (chiamate *riquadri*) ciascuna in grado di riportare un *simbolo*. In ogni istante c'è esattamente un riquadro, che riporta diciamo il simbolo S, che è *all'interno della macchina*. Possiamo chiamare questo il *riquadro in lettura*. Il simbolo nel riquadro in lettura può venir chiamato il *simbolo in lettura*. Il simbolo in lettura è l'unico di cui la macchina sia, per così dire, *a diretta conoscenza*.
Ad ogni istante, il comportamento della macchina è determinato dalla configurazione-macchina q_n e dal simbolo in lettura S. Questa coppia q_n, S sarà chiamata "configurazione": la configurazione determina il comportamento della macchina.
In configurazioni in cui il riquadro in lettura è non scritto (cioè non riporta nessun simbolo) la macchina può scrivere un simbolo nel riquadro in lettura, in altre configurazioni può cancellare il simbolo in lettura o scriverne un altro. La macchina può anche cambiare il riquadro in lettura, ma soltanto spostandolo di un posto a destra o a sinistra. In aggiunta a queste operazioni, la configurazione-macchina può essere cambiata.

Esempi di numeri calcolabili

$0.010101010101010\ldots = 0.\overline{01}$

configurazione		comportamento		
c.-m.	lettura	scrittura	movimento	c.-m.
q_1	–	0	R	q_2
q_2	–	·	R	q_3
q_3	–	0	R	q_4
q_4	–	1	R	q_3

$0.0101101111011110\ldots 0\underbrace{11\ldots1}_{n}0\underbrace{11\ldots1}_{n+1}0\ldots$

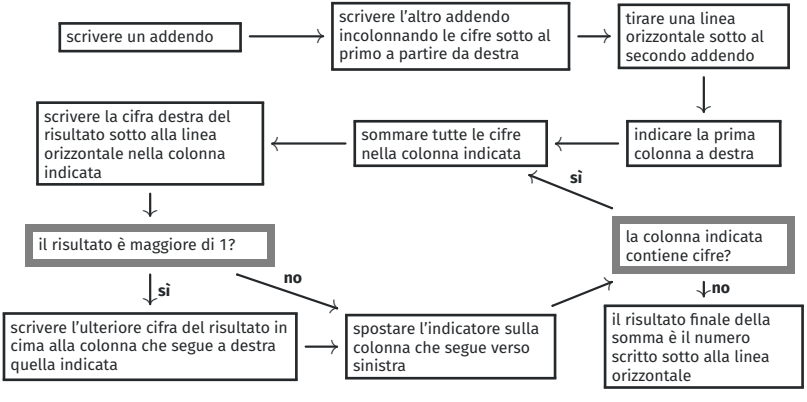
La prima definizione matematica di algoritmo

$M = (L, Q)$ è una *macchina di Turing con input e output numerici* se

- L è un insieme finito e il segno bianco $\_$ sta in L
- Q è un insieme di quintuple, contenuto in
  $\{q_n \mid n \in \mathbb{N}\} \times (\{0, 1, \langle, \rangle, ,\} \cup L) \times (\{0, 1, \langle, \rangle, ,\} \cup L) \times \{\mathrm{L}, \mathrm{R}\} \times \{q_n \mid n \in \mathbb{N}\}$
  ed è tale che non ci sono due quintuple con le stesse prime due componenti
  cioè $Q: \{q_n \mid n \in \mathbb{N}\} \times (\{0, 1, \langle, \rangle, ,\} \cup L) \rightharpoonup (\{0, 1, \langle, \rangle, ,\} \cup L) \times \{\mathrm{L}, \mathrm{R}\} \times \{q_n \mid n \in \mathbb{N}\}$

Un algoritmo

Un algoritmo per la somma di due numeri interi positivi in notazione binaria



Altri esempi di algoritmi

Algoritmo di Euclide per il massimo comun divisore tra due numeri

Formula risolutiva delle equazioni di secondo grado

Regola di Ruffini per la divisione di un polinomio con un polinomio di primo grado

Algoritmo per la divisione di due numeri interi positivi

Algoritmo per la moltiplicazione di due numeri interi positivi

Algoritmo per la scrittura in notazione binaria di un numero razionale

Funzioni calcolabili

$f\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$ una funzione parziale

$M = (L, Q)$: macchina di Turing *calcola* $f\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$ se

- partendo con la k-pla $\langle a_1, \dots, a_k \rangle$ scritta su nastro
  nella c.-m. q_1 in lettura sul carattere più a sinistra della k-pla
  M si ferma se e solo se $\langle n_1, \dots, n_k \rangle$ è nel dominio di f

- quando M si ferma
  in ogni riquadro alla destra del riquadro in lettura c'è il segno $\_$
  e a sinistra dal riquadro in lettura è scritto il valore $f(a_1, \dots, a_k)$

Diremo che $f\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$ è *Turing-calcolabile*

Über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter Systeme (K. Gödel, 1931)

Über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter Systeme (K. Gödel, 1931)

Lo sviluppo della matematica verso una maggiore precisione ha portato, com'è ben noto, alla formalizzazione di gran parte di essa; in questa si dimostrano teoremi di ogni tipo usando soltanto poche regole meccaniche. I sistemi formali più comprensivi al momento sono il sistema dei *Principia Mathematica* e il sistema di assiomi per la teoria degli insiemi di Zermelo–Fraenkel (sviluppato ulteriormente da J. von Neumann). [Le considerazioni che seguono si applicano anche ai sistemi formali (per quel che è disponibile al momento) prodotti di recente da Hilbert e i suoi collaboratori.]
Questi due sistemi sono così comprensivi che in essi sono formalizzati tutti i metodi di dimostrazione utilizzati oggi in matematica (formalizzati nel senso che sono ridotti a alcuni assiomi e regole deduttive). Si potrebbe dunque congetturare che tali assiomi e regole deduttive sono sufficienti per decidere *qualsiasi* questione matematica, esprimibile in tali sistemi. Si mostrerà nel seguito che questo non è il caso, che al contrario ci sono problemi relativamente semplici di aritmetica che non possono essere decisi sulla base degli assiomi. Questa situazione non è dovuta per nulla alla natura speciale dei due sistemi considerati, ma vale per un'ampia classe di sistemi formali[...]

Le funzioni calcolate in modo esplicito

Sono le funzioni $f\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$ che si possono ottenere a partire da

- zero: $a \mapsto 0\colon \mathbb{N}^1 \longrightarrow \mathbb{N}$
- succ: $a \mapsto a + 1\colon \mathbb{N}^1 \longrightarrow \mathbb{N}$
- $\mathrm{pr}_i^k\colon \langle a_1, \dots, a_k \rangle \mapsto a_i\colon \mathbb{N}^k \longrightarrow \mathbb{N}$, $1 \leq i \leq k$

mediante

composizione vettoriale $\quad \langle a_1, \dots, a_k \rangle \mapsto g(f_1(a_1, \dots, a_k), \dots, f_\ell(a_1, \dots, a_k))\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$

induzione
$$h(a_1, \dots, a_k, 0) = f(a_1, \dots, a_k)$$
$$h(a_1, \dots, a_k, b+1) = g(a_1, \dots, a_k, b, h(a_1, \dots, a_k, b))$$

minimizzazione $\quad \langle a_1, \dots, a_k \rangle \mapsto \min \left\{ b \in \mathbb{N} \;\middle|\; \begin{array}{l} f(a_1, \dots, a_k, b) = 0 \wedge \\ \wedge\, \forall_{c<b}\, f(a_1, \dots, a_k, c) > 0 \end{array} \right\}$

Le funzioni calcolate in modo esplicito

Sono le funzioni $f\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$ che si possono ottenere a partire da

- zero: $a \mapsto 0\colon \mathbb{N}^1 \longrightarrow \mathbb{N}$
- succ: $a \mapsto a + 1\colon \mathbb{N}^1 \longrightarrow \mathbb{N}$
- $\mathrm{pr}_i^k\colon \langle a_1, \dots, a_k \rangle \mapsto a_i\colon \mathbb{N}^k \longrightarrow \mathbb{N}$, $1 \le i \le k$

mediante

composizione vettoriale $\quad \langle a_1, \dots, a_k \rangle \mapsto g(f_1(a_1, \dots, a_k), \dots, f_\ell(a_1, \dots, a_k))\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$

induzione
$$h(a_1, \dots, a_k, 0) = f(a_1, \dots, a_k)$$
$$h(a_1, \dots, a_k, b+1) = g(a_1, \dots, a_k, b, h(a_1, \dots, a_k, b))$$

minimizzazione $\quad \langle a_1, \dots, a_k \rangle \mapsto \min \left\{ b \in \mathbb{N} \;\middle|\; \begin{array}{l} f(a_1, \dots, a_k, b) = 0 \wedge \\ \wedge\, \forall_{c<b}\, f(a_1, \dots, a_k, c) > 0 \end{array} \right\}$

$$\mathrm{somma}\colon \langle a_1, a_2 \rangle \mapsto a_1 + a_2\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$$

$\mathrm{somma}(a_1, 0) = a_1 + 0$ $\qquad$ $f(a_1) = \mathrm{pr}_1^1(a_1)$

$\mathrm{somma}(a_1, b+1) = \mathrm{somma}(a_1, b) + 1$ $\qquad$ $g(a_1, a_2, a_3) = \mathrm{succ}(\mathrm{pr}_3^3(a_1, a_2, a_3))$

Le funzioni calcolate in modo esplicito

Sono le funzioni $f\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$ che si possono ottenere a partire da

- zero: $a \mapsto 0\colon \mathbb{N}^1 \longrightarrow \mathbb{N}$
- succ: $a \mapsto a + 1\colon \mathbb{N}^1 \longrightarrow \mathbb{N}$
- $\mathrm{pr}_i^k\colon \langle a_1, \dots, a_k \rangle \mapsto a_i\colon \mathbb{N}^k \longrightarrow \mathbb{N}$, $1 \leq i \leq k$

mediante

composizione vettoriale $\quad \langle a_1, \dots, a_k \rangle \mapsto g(f_1(a_1, \dots, a_k), \dots, f_\ell(a_1, \dots, a_k))\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$

induzione
$$h(a_1, \dots, a_k, 0) = f(a_1, \dots, a_k)$$
$$h(a_1, \dots, a_k, b+1) = g(a_1, \dots, a_k, b, h(a_1, \dots, a_k, b))$$

minimizzazione $\quad \langle a_1, \dots, a_k \rangle \mapsto \min \left\{ b \in \mathbb{N} \;\middle|\; \begin{array}{l} f(a_1, \dots, a_k, b) = 0 \wedge \\ \wedge\, \forall_{c<b}\, f(a_1, \dots, a_k, c) > 0 \end{array} \right\}$

$$\mathrm{prod}\colon \langle a_1, a_2 \rangle \mapsto a_1 + a_2\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$$

$\mathrm{prod}(a_1, 0) = 0 \qquad f(a_1) = \mathrm{zero}(a_1)$

$\mathrm{prod}(a_1, b+1) = \mathrm{prod}(a_1, b) + a_1 \qquad g(a_1, a_2, a_3) = \mathrm{somma}(\mathrm{pr}_3^3(a_1, a_2, a_3), \mathrm{pr}_1^3(a_1, a_2, a_3))$

Altre funzioni ricorsive

- $\exp\colon \langle a, b\rangle \mapsto b^a\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$
- $\mathrm{ftr}\colon a \mapsto a!\colon \mathbb{N}^1 \longrightarrow \mathbb{N}$
- $\min\colon \langle a, b\rangle \mapsto \min(a, b)\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$
- $\max\colon \langle a, b\rangle \mapsto \max(a, b)\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$
- $\mathrm{rst}\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$ per $a = q \cdot b + \mathrm{rst}(a, b)$ e $0 \leq \mathrm{rst}(a, b) < b$ quando $b > 0$
- $\mathrm{quot}\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$ dove $\mathrm{quot}(a, b)$ è il minimo q tale che $a = q \cdot b + \mathrm{rst}(a, b)$

Teorema

Data $f\colon \mathbb{N}^{k+1} \rightharpoonup \mathbb{N}$ ricorsiva, sono ricorsive anche le seguenti:

- $\langle a_1, \ldots, a_k, b\rangle \mapsto \sum_{c<b} f(a_1, \ldots, a_k, c)\colon \mathbb{N}^{k+1} \rightharpoonup \mathbb{N}$
- $\langle a_1, \ldots, a_k, b\rangle \mapsto \prod_{c<b} f(a_1, \ldots, a_k, c)\colon \mathbb{N}^{k+1} \rightharpoonup \mathbb{N}$
- $\langle a_1, \ldots, a_k, b\rangle \mapsto \min_{c<b} f(a_1, \ldots, a_k, c)\colon \mathbb{N}^{k+1} \rightharpoonup \mathbb{N}$
- $\langle a_1, \ldots, a_k, b\rangle \mapsto \max_{c<b} f(a_1, \ldots, a_k, c)\colon \mathbb{N}^{k+1} \rightharpoonup \mathbb{N}$
- $\langle a_1, \ldots, b\rangle \mapsto \begin{cases} \min_{c<b} f(a_1, \ldots, c) = 0 \\ b \quad \textit{se il min non esiste} \end{cases} \colon \mathbb{N}^{k+1} \rightharpoonup \mathbb{N}$

Le funzioni ricorsive sono Turing-calcolabili

Teorema

Se $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$ *è una funzione ricorsiva*
allora f *è Turing-calcolabile*

Le funzioni ricorsive sono Turing-calcolabili

Teorema

Se $f\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$ *è una funzione ricorsiva*
allora f *è Turing-calcolabile*

Dimostrazione

zero: $a \mapsto 0\colon \mathbb{N}^1 \longrightarrow \mathbb{N}$

c.-m.	lettura	scrittura	movimento	c.-m.
q_1	0	▬	R	q_1
q_1	1	▬	R	q_1
q_1	▬	0	R	q_2
q_2	▬	▬	L	q_2

Le funzioni ricorsive sono Turing-calcolabili

Teorema

Se $f\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$ *è una funzione ricorsiva*
allora f *è Turing-calcolabile*

Dimostrazione

succ: $a \mapsto a + 1\colon \mathbb{N}^1 \rightharpoonup \mathbb{N}$

c.-m.	lettura	scrittura	movimento	c.-m.
q_1	0	0	R	q_1
q_1	1	1	R	q_1
q_1	▬	▬	L	q_2
q_2	0	1	L	q_5
q_2	1	0	L	q_3
q_3	1	0	L	q_3
q_3	0	1	L	q_4
q_3	▬	1	L	q_4
q_4	0	0	L	q_4
q_4	1	1	L	q_4
q_4	▬	▬	R	q_5

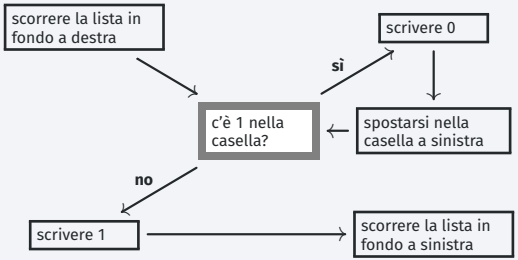
Le funzioni ricorsive sono Turing-calcolabili

Teorema

Se $f\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$ *è una funzione ricorsiva*
allora f *è Turing-calcolabile*

Dimostrazione

succ: $a \mapsto a + 1\colon \mathbb{N}^1 \rightharpoonup \mathbb{N}$



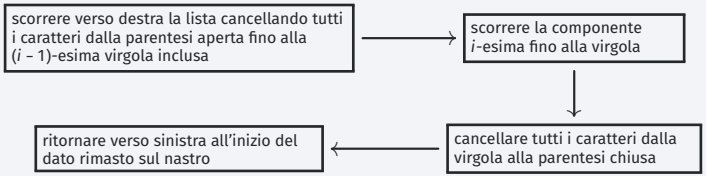
Le funzioni ricorsive sono Turing-calcolabili

Teorema

Se $f: \mathbb{N}^k \rightharpoonup \mathbb{N}$ *è una funzione ricorsiva allora* f *è Turing-calcolabile*

Dimostrazione

$\mathrm{pr}_i^k: \langle a_1, \ldots, a_k \rangle \mapsto a_i: \mathbb{N}^k \longrightarrow \mathbb{N}$, $1 \leq i \leq k$



Le funzioni ricorsive sono Turing-calcolabili

Teorema

Se $f\colon \mathbb{N}^k \longrightarrow \mathbb{N}$ *è una funzione ricorsiva*
allora f *è Turing-calcolabile*

Dimostrazione

composizione vettoriale $\langle a_1, \dots, a_k \rangle \mapsto g(f_1(a_1, \dots, a_k), \dots, f_\ell(a_1, \dots, a_k))\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$

induzione
$$h(a_1, \dots, a_k, 0) = f(a_1, \dots, a_k)$$
$$h(a_1, \dots, a_k, b+1) = g(a_1, \dots, a_k, b, h(a_1, \dots, a_k, b))$$

minimizzazione $\langle a_1, \dots, a_k \rangle \mapsto \min\left\{ b \in \mathbb{N} \;\middle|\; \begin{array}{l} \forall_{c<b}\, f(a_1, \dots, a_k, c) > 0 \wedge \\ \quad \wedge\, f(a_1, \dots, a_k, b) = 0 \end{array} \right\}$

Le funzioni ricorsive sono Turing-calcolabili

Teorema

Se $f\colon \mathbb{N}^k \longrightarrow \mathbb{N}$ *è una funzione ricorsiva allora* f *è Turing-calcolabile*

Dimostrazione

composizione vettoriale $\langle a_1, \dots, a_k \rangle \mapsto g(f(a_1, \dots, a_k))\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$

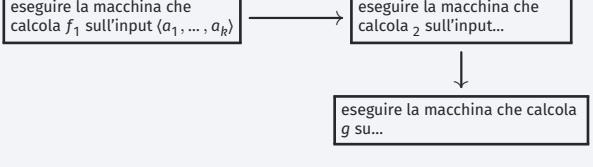
Le funzioni ricorsive sono Turing-calcolabili

Teorema

Se $f\colon \mathbb{N}^k \longrightarrow \mathbb{N}$ *è una funzione ricorsiva*
allora f *è Turing-calcolabile*

Dimostrazione

composizione vettoriale $\langle a_1, \dots, a_k \rangle \mapsto g(f_1(a_1, \dots, a_k), f_2(a_1, \dots, a_k))\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$



Le funzioni ricorsive sono Turing-calcolabili

Teorema

Se $f\colon \mathbb{N}^k \longrightarrow \mathbb{N}$ *è una funzione ricorsiva*
allora f *è Turing-calcolabile*

Dimostrazione

composizione vettoriale $\langle a_1, \dots, a_k \rangle \mapsto g(f_1(a_1, \dots, a_k), \dots, f_\ell(a_1, \dots, a_k))\colon \mathbb{N}^k \rightharpoonup \mathbb{N}$

induzione
$$h(a_1, \dots, a_k, 0) = f(a_1, \dots, a_k)$$
$$h(a_1, \dots, a_k, b+1) = g(a_1, \dots, a_k, b, h(a_1, \dots, a_k, b))$$

minimizzazione $\langle a_1, \dots, a_k \rangle \mapsto \min\left\{ b \in \mathbb{N} \;\middle|\; \begin{array}{l} \forall_{c<b}\, f(a_1, \dots, a_k, c) > 0 \wedge \\ \quad \wedge\, f(a_1, \dots, a_k, b) = 0 \end{array} \right\}$

Il Lemma della memoria mobile

Lemma

Siano

- $M = (L, Q)$ *una macchina di Turing con input e output numerici*
- $f_M : \mathbb{N}^k \rightharpoonup \mathbb{N}$ *la funzione calcolata da* M
- $A = \{/, \backslash\}$

Esiste una macchina $M' = (L, Q')$ *che calcola la funzione parziale*

$$f_{M'} : (\{0, 1, (,), \text{,}, /, \backslash\})^* \rightharpoonup (\{0, 1, (,), \text{,}, /, \backslash\})^*$$

determinata da

$$f_{M'}(p_1 / w \backslash p_2) \asymp p_1 / f_M(w) \backslash p_2$$

per ogni $p_1, p_2 \in (\{0, 1, (,), \text{,}, /, \backslash\})^*$ *e ogni* $w \in \mathbb{N}^k$

Funzioni calcolabili e la Tesi di Church-Turing

Teorema

Se $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$ *è Turing-calcolabile, allora* f *è ricorsiva*

Funzioni calcolabili e la Tesi di Church-Turing

Teorema

Se $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$ *è Turing-calcolabile, allora* f *è ricorsiva*

Tesi di Church-Turing

Una funzione calcolabile in modo esplicito può essere calcolata mediante una macchina di Turing

Università
di Genova