

Calcolo e simboli: la scienza digitale

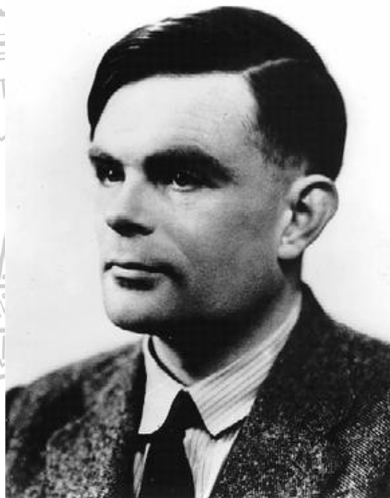
A.M. Turing a cent'anni dalla nascita

Simone Martini

Dipartimento di Informatica – Scienza e Ingegneria
Alma mater studiorum • Università di Bologna
and
EPI Focus • INRIA Sophia / Bologne

Accademia delle Scienze dell'Istituto di Bologna; 18 ott 2012
Accademia di Agricoltura Scienze e Lettere, Verona; 13 nov 2012

Chi è Alan M. Turing (1912–1954)?



nato: 23 giugno 1912

OBE, *Order of the British Empire*
FRS, *Fellow of the Royal Society*

Macchina del calcolo
Criptoanalisi
Gioco dell'imitazione
Morfogenesi

Chi è Alan M. Turing (1912–1954)?



nato: 23 giugno 1912

OBE, *Order of the British Empire*
FRS, *Fellow of the Royal Society*

Macchina del calcolo
Criptoanalisi
Gioco dell'imitazione
Morfogenesi

Chi è Alan M. Turing (1912–1954)?

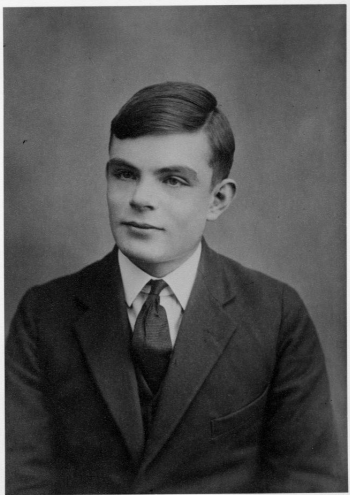


nato: 23 giugno 1912

OBE, *Order of the British Empire*
FRS, *Fellow of the Royal Society*

Macchina del calcolo
Criptoanalisi
Gioco dell'imitazione
Morfogenesi

Chi è Alan M. Turing (1912–1954)?



nato: 23 giugno 1912

OBE, *Order of the British Empire*
FRS, *Fellow of the Royal Society*

Macchina del calcolo
Criptoanalisi
Gioco dell'imitazione
Morfogenesi

Chi è Alan M. Turing (1912–1954)?



nato: 23 giugno 1912

OBE, *Order of the British Empire*
FRS, *Fellow of the Royal Society*

Macchina del calcolo
Criptoanalisi
Gioco dell'imitazione
Morfogenesi

Chi è Alan M. Turing (1912–1954)?



nato: 23 giugno 1912

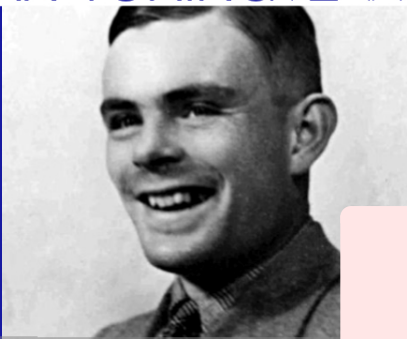
OBE, *Order of the British Empire*
FRS, *Fellow of the Royal Society*

Macchina del calcolo
Criptoanalisi
Gioco dell'imitazione
Morfogenesi

Chi è Alan M. Turing (1912–1954)?

ALAN TURING YEAR

2012



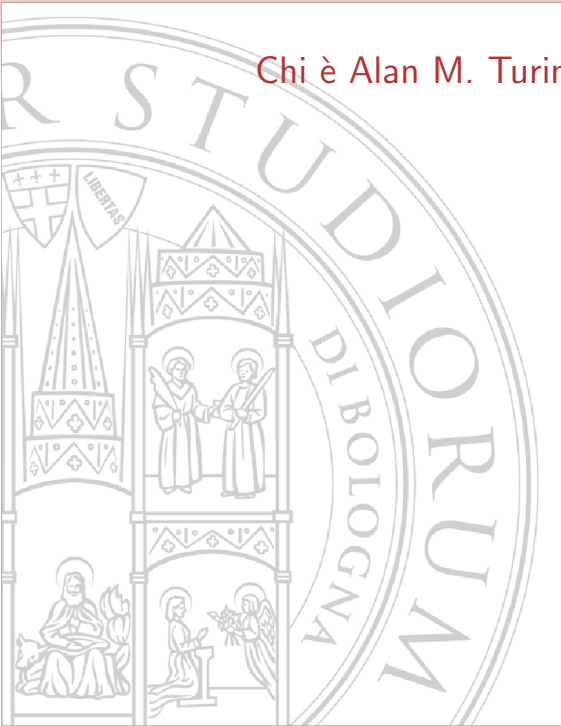
*Filo conduttore:
l'interfaccia del continuo*

nato: 23 giugno 1912

OBE, *Order of the British Empire*
FRS, *Fellow of the Royal Society*

Macchina del calcolo
Criptoanalisi
Gioco dell'imitazione
Morfogenesi

Chi è Alan M. Turing (1912–1954)?



Chi è Alan M. Turing (1912–1954)?

Creatore e fondatore della scienza (del) digitale.

Scienza (del) digitale ?

Numero ponderis et mensura Deus omnia condidit

Londini 11^{ma} Sept.
1722

D^{no} Pappatori plurimum colendo
Hanc Tessaram suam posuit.
Isaacus Newton

M. ACADEMIA
KÖNYVTÁRA

Scienza (del) digitale ?

- L'universo "è scritto in lingua matematica,"
Galileo Galilei, Saggiatore cap. 6.
- "e i caratteri son triangoli, cerchi ed altre figure geometriche"

Scienza (del) digitale ?

- L'universo "è scritto in lingua matematica,"
Galileo Galilei, Saggiatore cap. 6.
- "e i caratteri son triangoli, cerchi ed altre figure geometriche"

Matematico vs Numerico

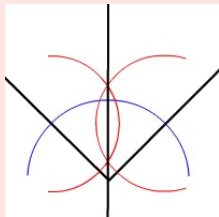
- Dire il reale in modo matematico
 - geometria
 - algebrizzazione della geometria
 - equazioni differenziali (del moto, del campo, ...)
- Dire il reale in modo numerico
 - Come è dato un numero reale?
 - Periodici, algebrici, trascendenti come π
- Cosa è una regola di calcolo? Cosa significa calcolare?
- Quasi incredibile:
 - la matematica non se lo chiede fino agli anni '30 del 900...

Ma qual è il problema?

Calcolo e matematica

- Fino al settecento non c'è grande differenza:
si cercano soluzioni mediante **costruzioni**
- Euclide: costruzione con riga e compasso:

Costruire la bisettrice di un angolo dato:



- Algebra: formula risolutiva dell'equazione di grado n

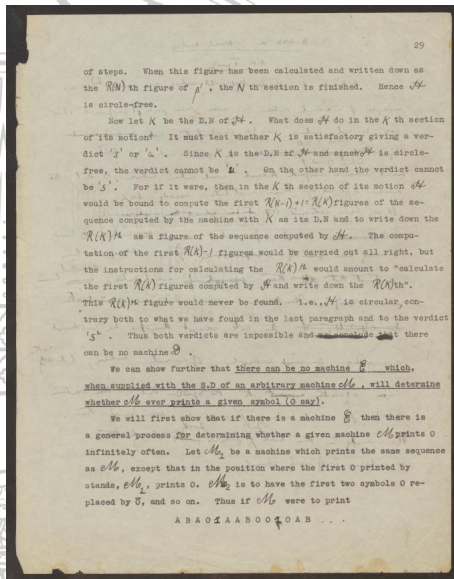
Calcolo e matematica: limitazioni

- Alcune costruzioni sono possibili
- Altre sono **dimostrabilmente** impossibili
- Con riga e compasso:
 - trisecazione di un angolo arbitrario (Wantzel, 1837)
 - duplicazione del cubo (Wantzel, 1837)
 - quadratura del cerchio (von Lindemann, 1882)
- Soluzione “per radicali”:
 - Formula risolutiva per equazioni di grado ≥ 5 (Ruffini, 1799)

Negatives are such difficult things to prove.

[A. Christie, Three blind mice.]

1936: Cosa significa calcolare?



*On Computable Numbers,
with an Application to the
Entscheidungsproblem,
Proc. Lond. Math. Soc. (2)
42 pp. 230-265 (1936)*

Ben prima delle macchine che calcolano...

- Primo calcolatore “universale” **elettromeccanico**:
Z3, 1941; Konrad Zuse, Germania.
- Primo calcolatore “universale” **elettronico**:
ENIAC, 1946; University of Pennsylvania's Moore School of Electrical Engineering

Imitiamo un contabile...
cioè un *computer*!

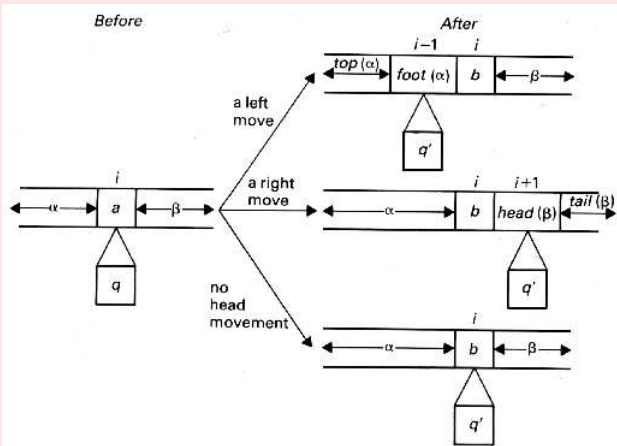
				1	1		
				2	7	3	+
				2	1	8	+
				0	1	1	=
				5	0	2	

Un commento un po' acido

Turing's "machines": These machines are humans who calculate.

*[L. Wittgenstein,
Remarks on the Philosophy of Psychology, Vol. 1,
Blackwell, Oxford, 1980.]*

La macchina di Turing



"The operation [...] is determined [...] by the state of mind of the computer and the observed symbols. In particular, they determine the state of mind of the computer after the operation is carried out."

La macchina che calcola

- Un oggetto astratto, completamente *immateriale*:
il massimo dell'analisi introspettiva di un processo umano meccanico genera un concetto matematico astratto
- Un oggetto **finito**:
alfabeto, stati, funzione di transizione
- Sono *possibili* computazioni infinite
- È una descrizione **alfabetica** del calcolo

(Mechanism and writing are from our point of view almost synonymous.)

Turing, A.M. Computing Machinery and Intelligence. Mind LIX, p. 456 (1950)

A physical symbol system has the necessary and sufficient means for general intelligent action.

Newell, A.; Simon, H. A. (1976), Computer Science as Empirical Inquiry, CACM 19 (3): 113-126,

La macchina che calcola

- Un oggetto astratto, completamente *immateriale*:
il massimo dell'analisi introspettiva di un processo umano meccanico genera un concetto matematico astratto
- Un oggetto **finito**:
alfabeto, stati, funzione di transizione
- Sono *possibili* computazioni infinite
- È una descrizione **alfabetica** del calcolo

(Mechanism and writing are from our point of view almost synonymous.)

Turing, A.M. Computing Machinery and Intelligence. Mind LIX, p. 456 (1950)

A physical symbol system has the necessary and sufficient means for general intelligent action.

Newell, A.; Simon, H. A. (1976), Computer Science as Empirical Inquiry, CACM 19 (3): 113-126,

La macchina che calcola

- Un oggetto astratto, completamente *immateriale*:
il massimo dell'analisi introspettiva di un processo umano meccanico genera un concetto matematico astratto
- Un oggetto **finito**:
alfabeto, stati, funzione di transizione
- Sono *possibili* computazioni infinite
- È una descrizione **alfabetica** del calcolo

(Mechanism and writing are from our point of view almost synonymous.)

Turing, A.M. Computing Machinery and Intelligence. Mind LIX, p. 456 (1950)

A physical symbol system has the necessary and sufficient means for general intelligent action.

Newell, A.; Simon, H. A. (1976), Computer Science as Empirical Inquiry, CACM 19 (3): 113–126,

La macchina universale

- Un'unica macchina, U , simula tutte le altre
- Il suo “programma cablato” è un programma di emulazione della macchina che è il suo dato
- U è un **calcolatore a programma memorizzato**
- L'intuizione di von Neumann

Limitazione della Macchina di Turing?

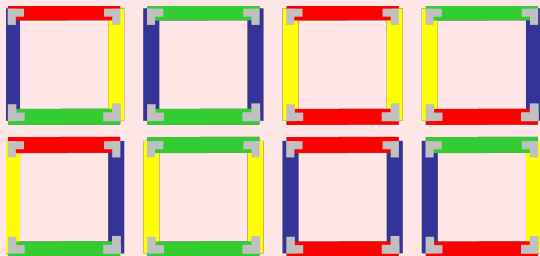
- Esistono costruzioni **non** calcolabili da nessuna macchina?
- Esistono numeri reali la cui espansione decimale **non** è prodotta da nessuna macchina
- Esistono problemi la cui soluzione non può essere calcolata: Problemi **indecidibili**.

Limitazione della Macchina di Turing?

- Esistono costruzioni **non** calcolabili da nessuna macchina?
- Esistono numeri reali la cui espansione decimale **non** è prodotta da nessuna macchina
- Esistono problemi la cui soluzione non può essere calcolata: Problemi **indecidibili**.

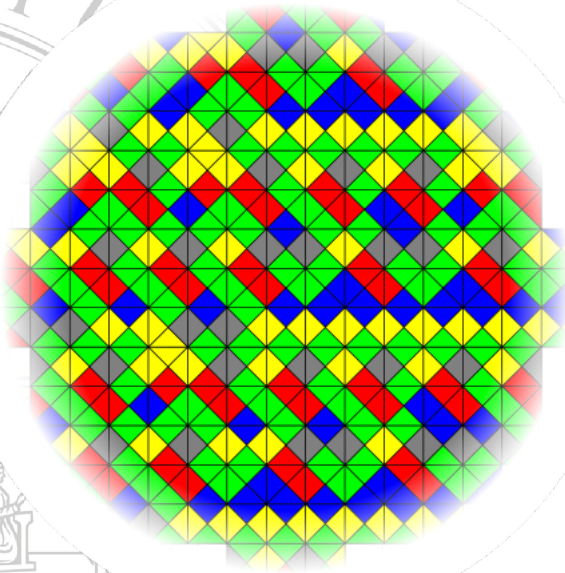
Un problema non decidibile

Piastrelle di Wang

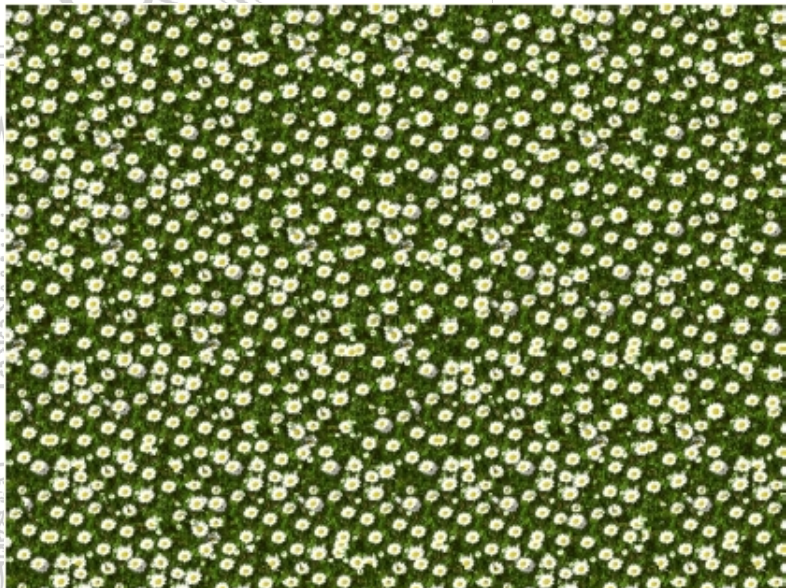


Dato un insieme di piastrelle,
decidere se possono piastrellare il piano

Piastrellature non periodiche



Un prato *non periodico* di margherite



Il concetto di calcolo e di calcolabile:

- Permette la descrizione della **realtà** (non solo del virtuale!)
- Permette di spiegarla
- Permette di **modificarla**

in modi nuovi e irriducibili alle altre scienze.

Ambient intelligence: sensing and actuation
Smart cities and homes

Il concetto di calcolo e di calcolabile:

- Permette la descrizione della **realtà** (non solo del virtuale!)
- Permette di spiegarla
- Permette di **modificarla**

in modi nuovi e irriducibili alle altre scienze.

Ambient intelligence: sensing and actuation
Smart cities and homes

Alfabeto o linguaggio?

- **Alfabeto:**
il calcolo è manipolazione combinatoria di simboli
- **Linguaggio:**
la descrizione del calcolo a livelli e con modi diversi

Davvero il linguaggio conta?

- Altre definizioni della calcolabilità

Turing: \mathcal{T}

Kleene: \mathcal{R}

Gödel: equazioni ricorsive

Church: λ -calcolo

Post: sistemi di riscrittura

Kolmogorov

...

e tutti i linguaggi di programmazione!

- Sono tutti equivalenti

*La classe delle funzioni calcolabili
è indipendente dal linguaggio in cui è definita*

Davvero il linguaggio conta?

- Altre definizioni della calcolabilità

Turing: \mathcal{T}

Kleene: \mathcal{R}

Gödel: equazioni ricorsive

Church: λ -calcolo

Post: sistemi di riscrittura

Kolmogorov

...

e tutti i linguaggi di programmazione!

- Sono tutti **equivalenti**

*La classe delle funzioni calcolabili
è indipendente dal linguaggio in cui è definita*

Un paradosso?

- La **nozione di calcolabile** è invariante per cambio di linguaggio mentre
- **Un** calcolo è (estremamente) sensibile al linguaggio in cui è espresso
 - ◇ Una MdT sporca un numero potenzialmente *infinito* di celle (con simboli da alfabeto finito)
 - ◇ Una RAM sporca un numero *finito* di registri (con interi potenzialmente infiniti)
 - ◇ Un λ -termine definisce solo funzioni sequenziali (sui λ -termini)

Un paradosso?

- La **nozione di calcolabile** è invariante per cambio di linguaggio mentre
- **Un** calcolo è (estremamente) sensibile al linguaggio in cui è espresso
 - ◇ Una MdT sporca un numero potenzialmente *infinito* di celle (con simboli da alfabeto finito)
 - ◇ Una RAM sporca un numero *finito* di registri (con interi potenzialmente infiniti)
 - ◇ Un λ -termine definisce solo funzioni sequenziali (sui λ -termini)

Equivalenze

- Equivalenza attraverso codifica (“gödelizzazione”)
- Distrugge la struttura:
 - del problema
 - della sua soluzione
- Anche in traduzioni “composizionali”: compilazione

Irriducibilità

- Livelli di descrizione: gerarchie (“stack”)
- Fenomeni emergenti
- Riduzione di un livello ad un altro
possibile in principio (ovvietà!)
sbagliata metodologicamente
non esistono traduzioni **fedeli**,
neppure all'interno della stessa lingua

Una lingua riempie una cella nell'alveare delle percezioni e delle interpretazioni possibili. Articola una gerarchia di valori, di significati e di supposizioni che non corrisponde esattamente a quella di nessun'altra lingua.

[G. Steiner, Errata, cap. 7, 1997]

Irriducibilità

- Livelli di descrizione: gerarchie (“stack”)
- Fenomeni emergenti
- Riduzione di un livello ad un altro
possibile in principio (ovvietà!)
sbagliata metodologicamente
non esistono traduzioni **fedeli**,
neppure all’interno della stessa lingua

Una lingua riempie una cella nell’alveare delle percezioni e delle interpretazioni possibili. Articola una gerarchia di valori, di significati e di supposizioni che non corrisponde esattamente a quella di nessun altra lingua.

[G. Steiner, Errata, cap. 7, 1997]

Proposed Electronic Calculator

Note dattiloscritte, senza data; circa dicembre 1945.

Turing Archive, AMT/B/1

1. La pila delle attivazioni

When we wish to start on a subsidiary operation we need only make a note of where we left off the major operation and then apply the first instruction of the subsidiary. When the subsidiary is over we look up the note and continue with the major operation. Each subsidiary operation can end with instructions for this recovery of the

note. How is the burying and disinterring of the note to be done? There are of course many ways. One is to keep a list of these notes in one or more standard size delay lines (1024), with the most recent last. The position of the most recent of these will be kept in a fixed TS, and this reference will be modified every time a subsidiary is started or finished. The burying and disinterring processes are fairly elaborate, but there is fortunately no need to repeat the instructions involved. Each time, the burying being done through a standard instruction table BURY, and the disinterring by the table UNBURY.

Proposed Electronic Calculator

Note dattiloscritte, senza data; circa dicembre 1945.

Turing Archive, AMT/B/1

2. Gerarchia di linguaggi

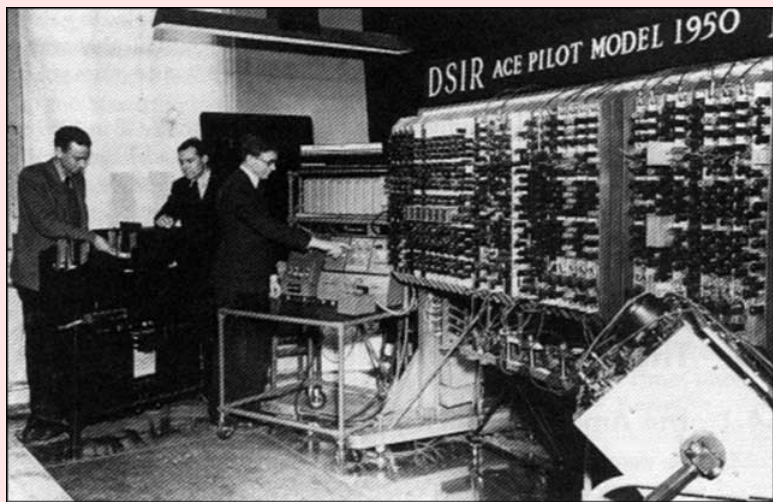
Each instruction will appear in a number of different forms, probably three or four.

Machine form. - When the instruction is expressed in full so as to be understood by the machine it will occupy one minor cycle. This we call machine form.

Permanent form. - The same instruction will appear in different machine forms in different jobs, on account of the renumbering technique as described in pp.13,14. Each of these machine form instructions arises from the permanent form of the instruction. These permanent forms are on Hollerith cards and are kept in a sort of library.

Popular form. - Besides the cards we need some form of the table which can be easily read, i.e. is in the form of print on paper rather than punching. This will be the popular form of the table. It will be much more abbreviated than the machine form or the permanent form, at any rate as regards the descriptions of the CAO. The names of the instructions used will probably be the same as those in the permanent form.

Pilot Automatic Computing Engine



Ancora Turing, 2

Lecture on Automatic Computing Engine

London Mathematical Soc., 20 Feb 1947.

Note dattiloscritte, in Turing Archive, AMT/C/32

Linguaggi di alto livello

trouble is bound to result. Actually one could communicate with these machines in any language provided it was an exact language, i.e. in principle one should be able to communicate in any symbolic logic, provided that the machine were given instruction tables which would enable it to interpret that logical system. This should mean that there will be much more practical scope for logical systems than there has been in the past. As regards mathematical

Ancora Turing, 2

Lecture on Automatic Computing Engine

London Mathematical Soc., 20 Feb 1947.

Note dattiloscritte, in Turing Archive, AMT/C/32

Linguaggi di alto livello

Actually one could communicate with these machines in any language provided it was an exact language, i.e. **in principle one should be able to communicate in any symbolic logic**, provided that the machine were given instruction tables which would allow it to interpret that logical system. This would mean that **there will be much more practical scope for logical systems** than there has been in the past. **Some attempts will probably be made to get the machine to do actual manipulations of mathematical formulae.** To do so will require the development of a special logical system for the purpose. This system should resemble normal mathematical procedure closely, but at the same time should be as unambiguous as possible.

Informatica: tre *personæ*

- Un insieme di **applicazioni**
- Una **tecnologia** che rende possibili quelle applicazioni
- Una **scienza** che fonda quella tecnologia

L'informatica:

- Studia i procedimenti **effettivi** di elaborazione dell'**informazione**.
- Contribuisce alle scienze con concetti propri, quali:
 - effettività
 - complessità computazionale
 - gerarchia di astrazione
 - informazione
- Condivide con altre scienze:
 - interazione
 - comunicazione
 - problem solving**

Ma soprattutto...

- Mette a disposizione **strumenti linguistici**
- Affinché ciò sia possibile e semplice
- Cioè evocativo, sintetico, economico
- Nella pluralità feconda dei linguaggi

Ipsa forma est substantia

L'essenza dell'informatica risiede nell'immateriale dell'espressione linguistica del calcolo e dell'interazione.

Il modo di esprimere un concetto (un algoritmo, la struttura di un protocollo, un'architettura software) è altrettanto importante del concetto espresso.

Questa forma è influenzata in modo cruciale dal linguaggio che scegliamo per esprimerla.

In altre scienze...



In altre scienze...

Matematica: troppo facile!



DISCOURS PRÉLIMINAIRE.

Chimica:

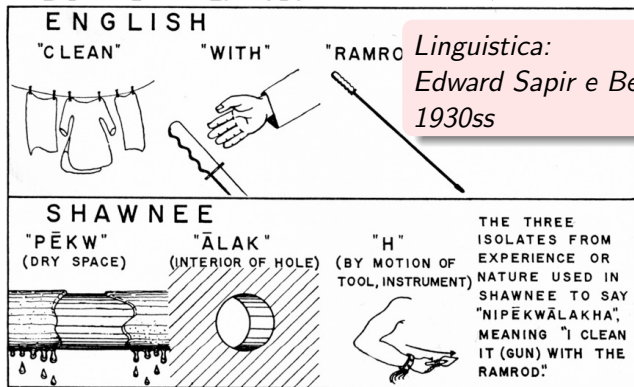
Antoine-Laurent de Lavoisier,

Traité élémentaire de chimie, 1789

Je n'avais pour objet, lorsque j'ai entrepris cet ouvrage, que de donner plus de développement au Mémoire que j'ai lu à la séance publique de l'Académie des sciences du mois d'avril 1787, sur la nécessité de réformer et de perfectionner la nomenclature de la chimie.

C'est en m'occupant de ce travail que j'ai mieux senti que je ne l'avais encore fait jusqu'alors l'évidence des principes qui ont été posés par l'abbé de Condillac dans sa Logique et dans quelques autres de ses ouvrages. Il y établit que *nous ne pensons qu'avec le secours des mots; que les langues sont de véritables méthodes analytiques; que l'algèbre la plus simple, la plus exacte et la mieux adaptée à son objet de toutes les manières de s'énoncer, est à la fois une langue et une méthode analytique; enfin, que l'art de raisonner se réduit à une langue bien faite.* Et en effet, tandis que je croyais ne m'occuper que de nomenclature, tandis que je n'avais pour objet que de perfectionner le langage de la chimie, mon ouvrage s'est transformé

In altre scienze...



Linguistica:
Edward Sapir e Benjamin Whorf
1930ss

Figure 9. Languages dissect nature differently. The different isolates of meaning (thoughts) used by English and Shawnee in reporting the same experience, that of cleaning a gun by running the ramrod through it. The pronouns 'I' and 'it' are not shown by symbols, as they have the same meaning in each language. In Shawnee ni- equals 'I'; -a equals 'it.'

Linguaggi cosiddetti *di programmazione*

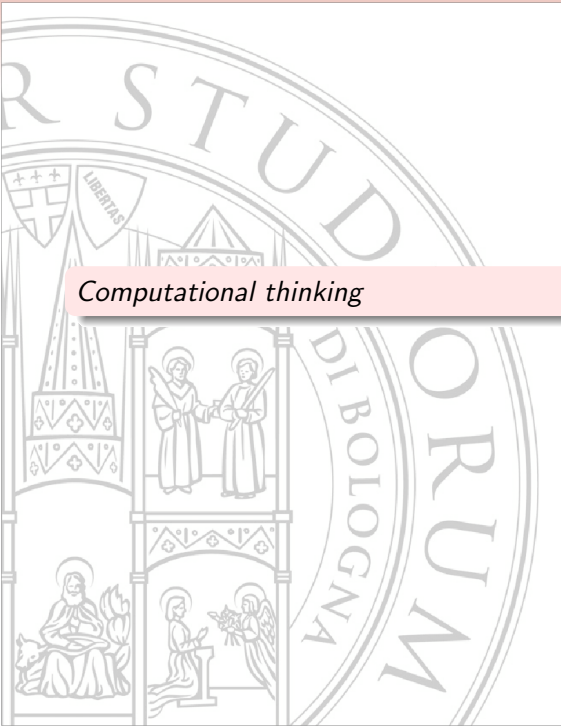
- Prescrizione del calcolo: marginale
- Astrazione: centrale
 - del problema
 - della soluzione
 - delle interazioni interne
 - delle interazioni con l'esterno

Astrazione e linguaggi

- Ricchi modelli dei dati
- Ricchi modelli procedurali
- Ricchi modelli di interazione
- Ricchi modelli di concorrenza e sincronizzazione

Articolazione del reale

- Un oggetto (*artefatto*) software è **un** modo per rendere intelligibile la realtà
- Categorie nuove ed irriducibili a quelle di altre scienze
 - Effettività
 - Complessità (computazionale), *feasibility*
 - Interazione (tra agenti)
 - ...

The background of the slide features a large, faint watermark of the seal of the University of Bologna. The seal is circular and contains the text "R STUD" at the top and "DI BOLOGNA" and "ORUM" at the bottom. In the center, there is a shield with a cross and three stars, and below it, a building with a tower. At the bottom of the seal, there are two scenes: one showing a seated figure with a dog, and another showing a kneeling figure and a standing figure.

Computational thinking

Intermezzo lampo L'ultimo Turing

*Was sich überhaupt sagen lässt, lässt sich klar sagen;
und wovon man nicht reden kann, darüber muss man schweigen*

[L. Wittgenstein, Tractatus, prefazione; 1921.]

- All'interfaccia tra il continuo e il digitale...
- Alfabeto e linguaggio non esauriscono la realtà
- Vi sono descrizioni continue irriducibili alla digitalizzazione
- La morfogenesi: reazione e diffusione

Intermezzo lampo L'ultimo Turing

*Quanto può dirsi, si può dir chiaro;
e su ciò, di cui non si può parlare, si deve tacere.*

[L. Wittgenstein, Tractatus, prefazione; 1921.]

- All'interfaccia tra il continuo e il digitale. . .
- Alfabeto e linguaggio non esauriscono la realtà
- Vi sono descrizioni continue irriducibili alla digitalizzazione
- La morfogenesi: reazione e diffusione

Intermezzo lampo L'ultimo Turing

*Quanto può dirsi, si può dir chiaro;
e su ciò, di cui non si può parlare, si deve tacere.*

[L. Wittgenstein, Tractatus, prefazione; 1921.]

- All'interfaccia tra il continuo e il digitale. . .
- Alfabeto e linguaggio non esauriscono la realtà
- Vi sono descrizioni continue irriducibili alla digitalizzazione
- La morfogenesi: reazione e diffusione

Hybris?

L'universo "è scritto in lingua matematica,"

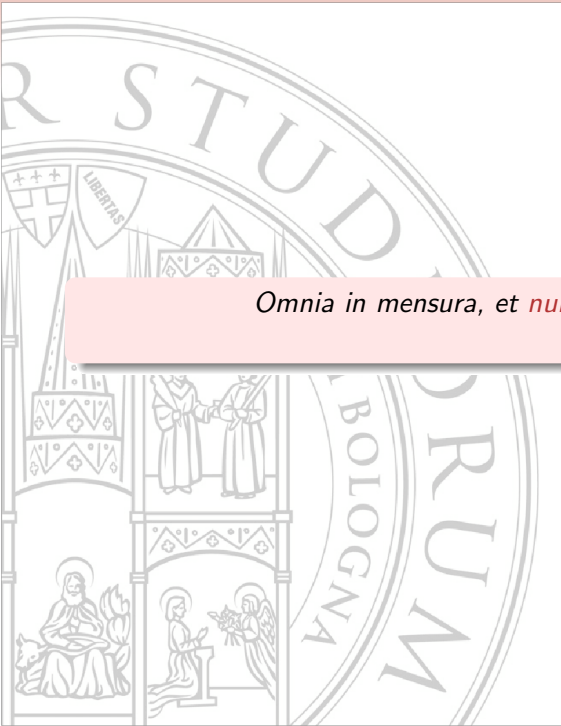
- "e i caratteri son triangoli, cerchi ed altre figure geometriche"
- e i caratteri son numeri, procedimenti effettivi ed astrazioni.
- Le descrizioni coesistono e si complementano tra loro
- Pluralità feconda dei linguaggi e delle descrizioni

Hybris?

L'universo "è scritto in lingua matematica,"

- "e i caratteri son triangoli, cerchi ed altre figure geometriche"
- e i caratteri son numeri, procedimenti effettivi ed astrazioni.

- Le descrizioni coesistono e si complementano tra loro
- Pluralità feconda dei linguaggi e delle descrizioni

The background of the slide features a large, faint watermark of the seal of the University of Bologna. The seal is circular and contains the text 'UNIVERSITAS STUDII BOLOGNENSIS' around the perimeter. In the center, there is a shield with a cross and three stars, and the word 'LIBERTAS' written on a banner. Below the shield, there are two figures in robes, one standing and one kneeling, and a seated figure with a halo and a lamb.

*Omnia in mensura, et **numero** et pondere disposuisti*
Sapienza 11,20.