CURS 1

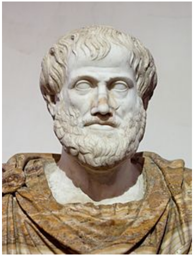
Logică Matematică şi Computaţională

FMI · Denisa Diaconescu · An universitar 2018/2019

O SCURTĂ ISTORIE

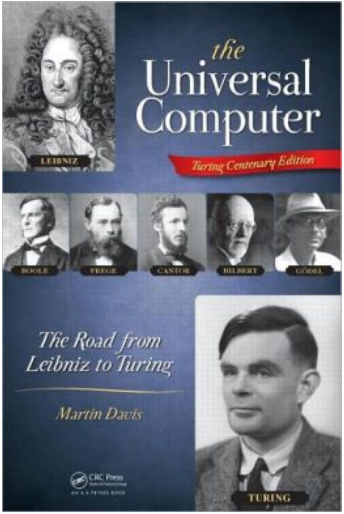
logiké tékhné = ştiinţa raţionamentelor; logos = cuvânt, raţionament

Aristotel (IV î.e.n.)



- `http://plato.stanford.edu/entries/aristotle-logic/`
- primul studiu formal al logicii
- a studiat silogismele (deducţii formate din două premize şi o concluzie).

	Barbara
Premiză	Toţi oamenii sunt muritori.
Premiză	Grecii sunt oameni.
Concluzie	Deci grecii sunt muritori.



"... a computing machine is really a logic machine. Its circuits embody the distilled insights of a remarkable collection of logicians, developed over century. Nowadays, as computer technology advances with such breathtaking rapidity, as we admire the truly accomplishments of the engineers, it is all too easy to overlook the logicians whose ideas made it all possible. This book tells their story."

– M. Davis

Visul lui Leibniz

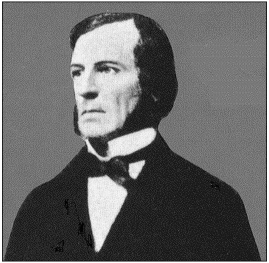
- un limbaj matematic universal (lingua characteristica universalis) în care toată cunoaşterea umană poate fi exprimată şi reguli de calcul (calculus ratiocinator) pentru a deriva, cu ajutorul maşinilor, toate relaţiile logice.

"If controversies were to arise, there would be no more need of disputation between two philosophers than between two accountants. For it would suffice to take their pencils in their hands, and say to each other: Calculemus - Let us calculate."

– G.W. Leibniz

GEORGE BOOLE (1815-1864)

- a iniţiat analiza raţionamentelor logice prin metode asemănătoare calculului algebric
- silogismele lui Aristotel sunt despre clase de obiecte, care pot fi studiate algebric.
- The Mathematical Analysis of Logic (1847), The Laws of Thought (1854)



"The design of the following treatise is to investigate the fundamental laws of the operations of the mind by which reasoning is performed; to give expressions to them in the symbolic language of calculus, and upon this foundation to establish the science of logic and constructs its methods."

– G. Boole

Begriffschrift (1879) (scriere conceptuală)

- a introdus sintaxa formală: obiecte, predicate, funcţii, conectori propoziţionali, cuantificatori.
- a inventat logica de ordinul întâi.

> *"perhaps the most important single work ever written in logic."*
>
> – van Heijenoort, From Frege to Godel, 1967

Exemplu:

- Toţi oamenii sunt muritori.
- Pentru orice x, dacă x este om, atunci x este muritor.
- $\forall x(Om(x) \to Muritor(x))$.

GEORG CANTOR (1845-1918)

- a inventat teoria mulţimilor.
- a definit numerele cardinale, ordinale.
- a dezvoltat o teorie matematică a infinitului.

"No one shall be able to expel us from the paradise that Cantor created for us."

– D. Hilbert

GEORG CANTOR (1845-1918)

Aristotel *"Infinitum Actu Non Datur"* (nu există infinit actual)

Leibniz *"I am so in favor of the actual infinite that instead of admitting that Nature abhors it, I hold that Nature makes frequent use of it everywhere."*

Gauss *"I protest above all the use of an infinite quantity as a completed one, which in mathematics is never allowed."*

Frege *"For the infinite will eventually refuse to be excluded from arithmetics . . . Thus we can foresee that this issue will provide for a momentous and decisive battle."*

Poincaré *"grave disease infecting mathematics".*

Kronecker (despre Cantor) *"scientific charlatan", "corrupter of youth"*

Wittgenstein *"utter nonsense"*

Mittag-Leffler (despre lucrările lui Cantor) *"about one hundred years too soon."*

Scrisoarea lui Bertrand Russell către Frege (16 iunie, 1902):

“I find myself in agreement with you in all essentials . . . I find in your work discussions, distinctions, and definitions that one seeks in vain in the work of other logicians . . . There is just one point where I have encountered a difficulty.”

Frege, apendix la The Fundamental Laws of Arithmetic, Vol. 2:

“There is nothing worse that can happen to a scientist than to have the foundation collapse just as the work is finished. I have been placed in this position by a letter from Mr. Bertrand Russell.”

Conform teoriei naive a mulţimilor, orice colecţie definibilă este mulţime. Fie U mulţimea tuturor mulţimilor.

Paradoxul lui Russel (1902)

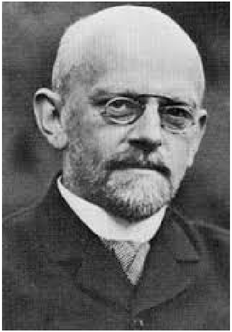
Fie $R = \{A \in U \mid A \notin A\}$. Atunci R este mulţime, deci $R \in U$.

Obţinem că $R \in R \iff R \notin R$.

Criza fundamentelor matematicii

- Paradoxul lui Russel $\Rightarrow$ Sistemul logic al lui Frege este inconsistent
- a declanşat criza fundamentelor matematicii (”foundations of mathematics”)
- s-a dezvoltat teoria axiomatică a mulţimilor: Zermelo-Fraenkel (ZF), ZFC: ZF+ Axioma alegerii (*Axiom of Choice*)

- unul dintre matematicienii de vârf ai generaţiei sale
- unul dintre fondatorii teoriei demonstraţiei şi logicii matematice
- lista sa de 23 probleme deschise (1902) a influenţat foarte mult matematica secolului XX



Programul lui Hilbert (1921)

Să se formalizeze matematica şi să se stabilească următoarele:

- Matematica este consistentă: un enunţ matematic şi negaţia sa nu pot fi demonstrate simultan.
- Matematica este completă: toate enunţurile matematice adevărate pot fi demonstrate.
- Matematica este decidabilă: există o regulă mecanică pentru a determina dacă un enunţ matematic dat este adevărat sau fals.

There is no such thing as an unsolvable problem.

We must know, we will know.

– D. Hilbert

Teoremele de incompletitudine ale lui Gödel (1931-33)

- incompletitudinea aritmeticii obişnuite (la 25 de ani).
- imposibilitatea de a demonstra consistenţa teoriei mulţimilor.
- au marcat eşecul programului lui Hilbert.

- este considerat cel mai mare logician al secolului XX.
- a introdus funcţiile calculabile.
- a demonstrat teorema de completitudine a logicii de ordinul întâi.
- a demonstrat că Axioma Alegerii şi Ipoteza Continuumului sunt consistente cu axiomele teoriei mulţimilor.

“Kurt Gödel’s achievement in modern logic is singular and monumental - indeed it is more than a monument, it is a landmark which will remain visible far in space and time .... The subject of logic has certainly completely changed its nature and possibilities with Gödel’s achievement.”

– J. von Neumann

Revista TIME (19 martie 1999)

Gödel a fost inclus în lista cu cei mai importanţi 20 oameni de ştiinţă şi gânditori ai secolului XX.

Entscheidungsproblem – Hilbert şi Ackermann (1928)

- Există un algoritm pentru a verifica dacă o anumită formulă din logica de ordinul întâi este adevărată?
- Cu alte cuvinte: Este logica de ordinul întâi decidabilă?

ALAN TURING(1912-1954)

- a demonstrat că logica de ordinul întâi este nedecidabilă (la 24 de ani) (rezultat obţinut independent de Church în 1935).
- a introdus maşina Turing (universală) pentru a formaliza noţiunea de algoritm.

- părintele informaticii şi inteligenţei artificiale
- maşina Turing universală este model al calculatoarelor actuale

Revista TIME (19 martie 1999)

Turing a fost inclus in lista cu cei mai importanţi 20 oameni de ştiinţă şi gânditori ai secolului XX.

"Virtually all computers today from 10 *million supercomputers to the tiny chips that power cell phones and Furbies, have one thing in common: they are all "von Neumann machines", variations on the basic computer architecture that John von Neumann, building on the work of Alan Turing, laid out in the 1940's."*

– Revista Time

Premiul Turing

- `http://amturing.acm.org/`
- decernat anual de către Association for Computing Machinery (ACM) pentru contribuţii în informatică
- este considerat un Premiu Nobel pentru Informatică

”Computing and Computing Science unavoidably emerge as an exercise in formal mathematics or, if you wish an acronym, as exercise in VLSAL (Very Large Scale Application of Logic).“

– E. W. Dijkstra

”Logic is the calculus of computation.”

– A. R. Bradley, Z. Manna

“Computer science is the continuation of logic by other means.”

– G. Gottlob

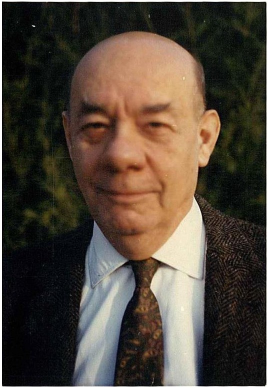
Aplicaţii ale logicii în informatică:

- limbaje de programare (semantică, programare logică, programare funcţională)
- software engineering (verificare, model checking)
- baze de date (algebre de relaţii, teoria modelelor finite)
- inteligenţă artificială
- criptografie şi securitate
- calculabilitate şi complexitate
- arhitectura calculatoarelor (circuite logice)
- ...

J. Y. Halpern, R. Harper, N. Immerman, P.G. Kolaitis, M.Y. Vardi, V. Vianu, *On the Unusual Effectiveness of Logic in Computer Science*, Bulletin of Symbolic Logic 7 (2001).

Grigore C. Moisil (1906-1973)

Computer Pioneer Award of IEEE Computer Society



"As a professor of the Bucharest University, he was the first to teach there mathematical logic. Articulating logic and automata, Moisil was well prepared to organize the Romanian development in the emergent field of Computer Science...we can say that 1957 is the date of birth of Romanian Computer Science, under the guidance of Professor Moisil and with the collaboration of engineers and mathematicians."

– S. Marcus

SISTEME LOGICE

Există diferite sisteme logice:

- logica propoziţională
- logica de ordinul întâi
- logica intuiţionistă
- logica modală
- logica temporală
- logica dinamică
- logica fuzzy
- ...

PRELIMINARII

Fie A, B, T mulţimi a.î. $A, B \subseteq T$.

$$
\begin{aligned}
A \cup B &= \{x \in T \mid x \in A \text{ sau } x \in B\} \\
A \cap B &= \{x \in T \mid x \in A \text{ şi } x \in B\} \\
A \setminus B &= \{x \in T \mid x \in A \text{ şi } x \notin B\} \\
C_T A &= T \setminus A = \{x \in T \mid x \notin A\}
\end{aligned}
$$

$C_T A$ se mai notează şi $\overline{A}$ când T este clar din context.

Notaţii.

- $\mathbb{N} = \{0, 1, 2, \ldots\}$ este mulţimea numerelor naturale
- $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$
- $\mathbb{Z}$ este mulţimea numerelor întregi
- $\mathbb{Q}$ este mulţimea numerelor raţionale.
- $\mathbb{R}$ este mulţimea numerelor reale

Mulţimea părţilor lui T este $\mathcal{P}(T) = \{A \mid A \subseteq T\}$.

Se mai notează şi 2^T.

Exemple.

- $\mathcal{P}(\emptyset) = \{\emptyset\}$,
- $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$,
- $\mathcal{P}(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$.

Dacă T are n elemente, atunci 2^T are 2^n elemente.

Notăm cu (a, b) perechea ordonată formată din a şi b (care sunt componentele lui (a, b)).

În teoria mulţimilor, (a, b) se defineşte ca fiind mulţimea $\{\{a\}, \{a, b\}\}$.

Observaţii.

- dacă $a \neq b$, atunci $(a, b) \neq (b, a)$
- $(a, b) \neq \{a, b\}$
- $(7, 7)$ este o pereche ordonată validă
- două perechi ordonate (a, b) şi (c, d) sunt egale ddacă $a = c$ şi $b = d$.

Definiţie.
Produsul cartezian a două mulţimi A şi B este definit astfel:

$$A \times B = \{(a, b) \mid a \in A \text{ şi } b \in B\}$$

Exerciţiu.

- $A \times (B \cup C) = (A \times B) \cup (A \times C)$
- $A \times (B \cap C) = (A \times B) \cap (A \times C)$

Definiţie.

O relaţie binară între A şi B este o submulţime a lui $A \times B$.

O relaţie binară pe A este o submulţime a lui $A \times A$.

Exemple.

- $< \subseteq \mathbb{N} \times \mathbb{N}$

$$<= \{(k, n) \mid \text{ există } m \in \mathbb{N} \text{ a.î. } m \neq 0 \text{ şi } m + k = n\}$$

- $| \subseteq \mathbb{N} \times \mathbb{N}$

$$| = \{(k, n) \mid \text{ există } m \in \mathbb{N} \text{ a.î. } mk = n\}$$

Definiţie.

- Dacă $R \subseteq A \times B$, atunci relaţia inversă $R^{-1} \subseteq B \times A$ este definită astfel:
$$R^{-1} = \{(b, a) \mid (a, b) \in R\}.$$

- Dacă $R \subseteq A \times B$ şi $Q \subseteq B \times C$, atunci compunerea lor $Q \circ R \subseteq A \times C$ este definită astfel:
$$Q \circ R = \{(a, c) \mid \text{ există } b \in B \text{ a.î. } (a, b) \in R \text{ şi } (b, c) \in Q\}.$$

- Diagonala lui A este $\Delta_A = \{(a, a) \mid a \in A\}$.

Exerciţiu.

- Compunerea relaţiilor este asociativă.
- Dacă $R \subseteq A \times B$ atunci $R \circ \Delta_A = R$ şi $\Delta_B \circ R = R$.

Definiţie.

O funcţie este un triplet (A, B, R), unde A şi B sunt mulţimi, iar $R \subseteq A \times B$ este o relaţie cu proprietatea că pentru orice $a \in A$ există un unic $b \in B$ cu $(a, b) \in R$.

Vom nota o funcţie (A, B, R) prin $f : A \to B$, simbolul f având semnificaţia: fiecărui element $x \in A$ îi corespunde un singur element $f(x) \in B$ a.î. $(x, f(x)) \in R$.

Spunem că $f : A \to B$ este definită pe A cu valori în B, A se numeşte domeniul de definiţie al funcţiei f şi B domeniul valorilor lui f.

Definiţie.
O funcţie parţială de la A la B este o funcţie $f : C \to B$, unde C este o submulţime a lui A.

Notaţie.

- B^A este mulţimea funcţiilor de la A la B.
- Fie $f : A \to B$ o funcţie, $X \subseteq A$ şi $Y \subseteq B$.
  - $f(A)$ este imaginea lui f.
  - $f(X) = \{f(x) \mid x \in X\}$ este imaginea directă a lui X prin f
  - $f^{-1}(Y) = \{x \in X \mid f(x) \in Y\}$ este imaginea inversă a lui Y prin f.

Definiţie.

Fie $f : A \to B$ o funcţie.

- f este injectivă dacă pentru orice $x_1, x_2 \in A$, $x_1 \neq x_2$ implică $f(x_1) \neq f(x_2)$ (sau, echivalent, $f(x_1) = f(x_2)$ implică $x_1 = x_2$).
- f este surjectivă dacă pentru orice $y \in B$ există $x \in A$ a.î. $f(x) = y$ (sau, echivalent, $f(A) = B$).
- f este bijectivă dacă f este injectivă şi surjectivă.

Definiţie.

Fie $f : A \to B$ şi $g : B \to C$ două funcţii. Compunerea lor $g \circ f$ este definită astfel:

$$g \circ f : A \to C, \quad (g \circ f)(x) = g(f(x)) \text{ pentru orice } x \in A.$$

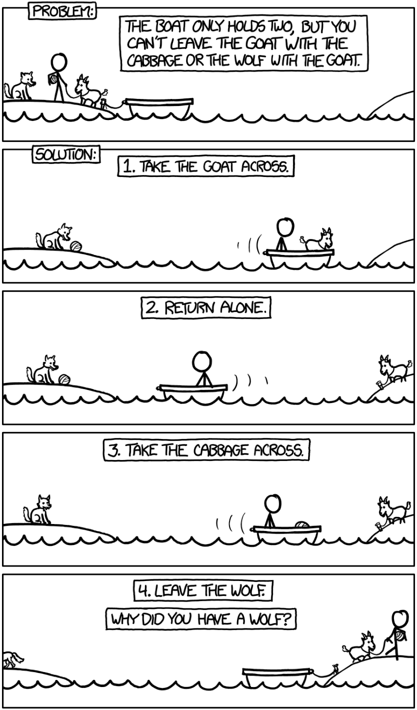
Funcţia identitate a lui A este funcţia $1_A : A \to A$, $1_A(x) = x$.

Definiţie.
O funcţie $f : A \to B$ este inversabilă dacă există $g : B \to A$ astfel încât $g \circ f = 1_A$ şi $f \circ g = 1_B$.

Exerciţiu.
O funcţie este bijectivă ddacă este inversabilă.

Definiţie.
Spunem că A este echipotentă cu B dacă există o bijecţie $f : A \to B$.
Notăm acest fapt prin $A \sim B$.

Exerciţiu.
A este echipotentă cu B ddacă B este echipotentă cu A.
De aceea, spunem de obicei că A şi B sunt echipotente.



Pe data viitoare!

Conţinutul tehnic al acestui curs se regăseşte în cursul de *Logică Matematică şi Computaţională* al prof. Laurenţiu Leuştean din anul universitar 2017/2018.

Comic-ul aparţine xkcd.