Logică Matematică și Computațională

Anul I, Semestrul I 2015/2016

Laurențiu Leuștean

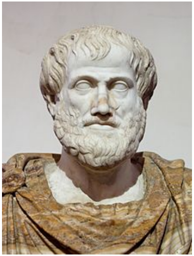
Pagina web: `http://imar.ro/~leustean/`

În prezentarea acestui curs sunt folosite parțial slideurile Ioanei Leuștean din Semestrul I 2014/2015.

Ce este logica?

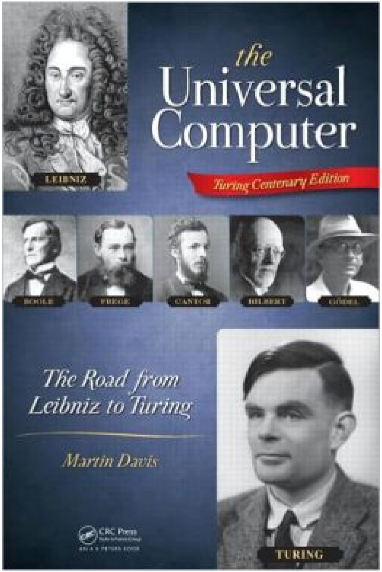
logiké tékhné= știința raționamentelor; logos = cuvânt, raționament

Aristotel (IV i.e.n.)



- http://plato.stanford.edu/entries/aristotle-logic/
- primul studiu formal al logicii
- a studiat silogismele, deducții formate din două premize și o concluzie.

	Barbara
Premiză	Toți 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."

Gottfried Wilhelm Leibniz (1646 -1716)

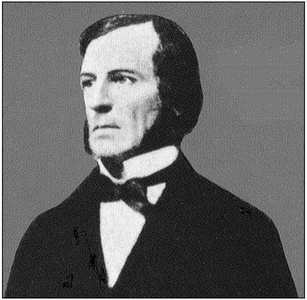
Visul lui Leibniz

- un limbaj matematic universal (lingua characteristica universalis) în care toată cunoașterea umană poate fi exprimată și reguli de calcul (calculus ratiocinator) pentru a deriva, cu ajutorul mașinilor, toate relațiile 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."

George Boole (1815-1864)

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



"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."

Gottlob Frege (1848-1925)

Begriffschrift (1847)

- A introdus sintaxa formală: obiecte, predicate, funcții; conectori propoziționali; cuantificatori.
- A inventat logica de ordinul întâi.
- van Heijenoort, From Frege to Godel, 1967: *"perhaps the most important single work ever written in logic."*

Exemplu:

- Toți oamenii sunt mortali.
- Pentru orice x, dacă x este om, atunci x este mortal.
- $\forall x(Man(x) \rightarrow Mortal(x))$.

Georg Cantor (1848-1925)

- A inventat teoria mulțimilor.
- A definit numere cardinale, ordinale.
- A dezvoltat o teorie matematică a infinitului.

Hilbert:

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

Georg Cantor (1848-1925)

- 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 mulțimilor, orice colecție definibilă este mulțime. Fie U mulțimea tuturor mulțimilor.

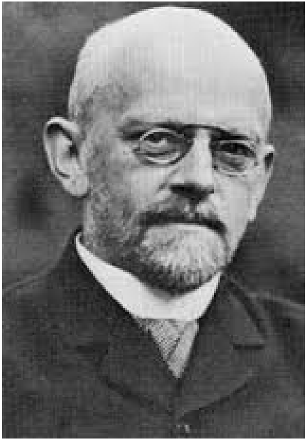
Paradoxul lui Russel (1902)

Fie $R = \{A \in U \mid A \notin A\}$. Atunci R este mulțime, deci $R \in U$. Obținem că $R \notin R \Leftrightarrow R \in R$.

Criza fundamentelor matematicii

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

David Hilbert (1862-1943)



- unul dintre matematicienii de vârf ai generației sale
- unul dintre fondatorii teoriei demonstrației și logicii matematice
- lista sa de 23 probleme deschise (1902) a influențat foarte mult matematica secolului XX

Programul lui Hilbert (1921)

Să se formalizeze matematica și să se stabilească următoarele:

- Matematica este consistentă: un enunț matematic și negația sa nu pot fi demonstrate simultan.
- Matematica este completă: toate enunțurile matematice adevărate pot fi demonstrate.
- Matematica este decidabilă: există o regulă mecanică pentru a determina dacă un enunț matematic dat este adevărat sau fals

Programul lui Hilbert

Hilbert a fost convins că aceste obiective pot fi atinse:

"Every mathematical problem must necessarily be susceptible to an exact statement either in the form of an actual answer to the question asked, or by the proof of the impossibility of its solution".

"Once a logical formalism is established one can expect that a systematic, so-to-say computational, treatment of logic formulas is possible, which would somewhat correspond to the theory of equations in algebra."

Kurt Gödel (1906-1978)

Teoremele de incompletitudine ale lui Gödel (1931-33)

- Incompletitudinea aritmeticii obișnuite.
- Imposibilitatea de a demonstra consistența teoriei mulțimilor.
- Au marcat eșecul programului lui Hilbert.

- Este considerat cel mai mare logician al secolului XX.
- A introdus funcțiile calculabile.
- A demonstrat teorema de completitudine a logicii de ordinul I.
- A demonstrat că Axioma Alegerii și Ipoteza Continuumului sunt consistente cu axiomele teoriei mulțimilor.

Kurt Gödel (1906-1978)

John von Neumann:

"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."

Revista TIME (19 martie 1999)

Gödel a fost inclus in lista cu cei mai importanți 20 oameni de știință și gânditori ai secolului XX.

Problema de decizie (Entscheidungsproblem)

- Hilbert și 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)

Turing, *On computable numbers, with an application to the Entscheidungsproblem*, Proc. London Math. Soc. 42 (1936).

- a demonstrat că logica de ordinul întâi este nedecidabilă (rezultat obținut independent de Church (1936)).
- a introdus mașina Turing (universală) pentru a formaliza noțiunea de algoritm.

- părintele informaticii și inteligenței artificiale
- mașina Turing universală este model al calculatoarelor actuale

Revista TIME (19 martie 1999)

Turing a fost inclus in lista cu cei mai importanți 20 oameni de știință și 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.*

Premiul Turing

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

E. W. Dijkstra, The next fifty years (EWD1243a). E.W. Dijkstra Archive. Center for American History, University of Texas at Austin:

"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)."

Aaron R. Bradley, Zohar Manna, The Calculus of Computation Decision Procedures with Applications to Verification, Springer, 2007:

"Logic is the calculus of computation."

Georg Gottlob, Logic and Artificial Intelligence, VSL 2014:

"Computer science is the continuation of logic by other means."

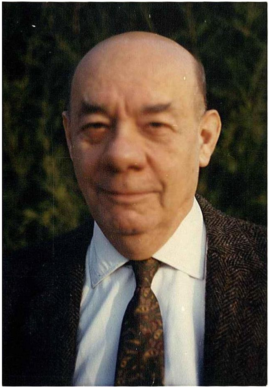
Aplicatii ale logicii în informatică:

- calculabilitate și complexitate
- arhitectura calculatoarelor (circuite logice)
- software engineering (verificare, model checking)
- limbaje de programare (semantică, programare logică, programare funcțională)
- baze de date (algebre de relații, teoria modelelor finite)
- inteligență artificială
- criptografie și securitate

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



S. Marcus, *Grigore C. Moisil: A life becoming a myth*, 2006.

"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."

PRELIMINARII

Operații cu mulțimi

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

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

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

Notații: $\mathbb{N} = \{0, 1, 2, \ldots\}$ este mulțimea numerelor naturale; $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$; $\mathbb{Z}$ este mulțimea numerelor întregi; $\mathbb{R}$ este mulțimea numerelor reale; $\mathbb{Q}$ este mulțimea numerelor raționale.

Mulțimea părților lui T este $\mathcal{P}(T) = \{A \mid A \subseteq T\}$. Se mai notează și 2^T.

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

Produsul cartezian

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

Observații: $(a, b) \neq (b, a)$; $(a, b) \neq \{a, b\}$; $(7, 7)$ este o pereche ordonată validă; două perechi ordonate (a, b) și (c, d) sunt egale ddacă $a = c$ și $b = d$. În teoria mulțimilor, (a, b) se definește ca fiind mulțimea $\{\{a\}, \{a, b\}\}$.

Definiție

Produsul cartezian a două mulțimi A și B este definit astfel:

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

Exercițiu.

$$\begin{aligned} A \times (B \cup C) &= (A \times B) \cup (A \times C) \\ A \times (B \cap C) &= (A \times B) \cap (A \times C) \end{aligned}$$

Definiție

O relație binară între A și B este o submulțime a produsului cartezian $A \times B$.
O relație binară pe A este o submulțime a lui A^2.

Exemple

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

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

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

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

Fie A, B, C mulțimi.

- Dacă $R \subseteq A \times B$, atunci relația inversă $R^{-1} \subseteq B \times A$ este definită astfel:

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}.$$

- Dacă $R \subseteq A \times B$ și $Q \subseteq B \times C$, atunci compunerea lor $R \circ Q \subseteq A \times C$ este definită astfel:

$$R \circ Q = \{(a, c) \mid \text{ există } b \in B \text{ a.î. } (a, b) \in R \text{ și } (b, c) \in Q\}.$$

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

Exercițiu

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

Definiție

O funcție este un triplet (A, B, R), unde A și B sunt mulțimi, iar $R \subseteq A \times B$ este o relație cu proprietatea că pentru orice $a \in A$ există un unic $b \in B$ cu $(a, b) \in R$.

Vom nota o funcție (A, B, R) prin $f : A \to B$, simbolul f având următoarea semnificație: fiecărui element $x \in A$ î 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 numește domeniul de definiție al funcției f și B se numește domeniul valorilor lui f.

Notație: B^A este mulțimea funcțiilor de la A la B.

Definiție

O funcție parțială de la A la B este o funcție $f : C \to B$, unde C este o submulțime a lui A.

Funcții

Notații: Fie $f : A \to B$ o funcție, $X \subseteq A$ și $Y \subseteq B$.

- $f(X) = \{f(x) \mid x \in X\}$ este imaginea directă a lui X prin f; $f(A)$ este imaginea lui f.
- $f^{-1}(Y) = \{x \in X \mid f(x) \in Y\}$ este imaginea inversă a lui Y prin f.

Definiție

Fie $f : A \to B$ o funcție

- 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 și surjectivă.

Funcții

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

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

Funcția identică a lui A: $1_A : A \to A$, $1_A(x) = x$.

Definiție

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

Exercițiu. O funcție este bijectivă ddacă este inversabilă.

Definiție

Spunem că A este echipotentă cu B dacă există o bijecție $f : A \to B$. Notație: $A \sim B$.

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

Funcția caracteristică

Definiție

Fie A, T mulțimi a.î. $A \subseteq T$. Funcția caracteristică a lui A în raport cu T este definită astfel:

$$\chi_A : T \to \{0,1\}, \quad \chi_A(x) = \begin{cases} 1, & \text{dacă } x \in A \\ 0, & \text{dacă } x \notin A \end{cases}$$

Proprietăți

Dacă A, $B \subseteq T$ și $x \in T$ atunci

$$\begin{aligned} \chi_{A\cap B}(x) &= \min\{\chi_A(x), \chi_B(x)\} = \chi_A(x) \cdot \chi_B(x) \\ \chi_{A\cup B}(x) &= \max\{\chi_A(x), \chi_B(x)\} = \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x) \\ \chi_{\overline{A}}(x) &= 1 - \chi_A(x). \end{aligned}$$

Observație

Funcția caracteristică se poate folosi pentru a arăta că două mulțimi sunt egale: $A = B$ ddacă $\chi_A = \chi_B$.

Familii

Fie I o mulțime nevidă.

Fie A o mulțime. O familie de elemente din A indexată de I este o funcție $f : I \to A$. Notăm cu $(a_i)_{i\in I}$ familia $f : I \to A$, $f(i) = a_i$ pentru orice $i \in I$. Vom scrie și $(a_i)_i$ sau (a_i) atunci când I este dedusă din context.

Dacă fiecărei $i \in I$ îi este asociată o mulțime A_i, obținem o familie (indexată) de mulțimi $(A_i)_{i\in I}$.

Fie $(A_i)_{i\in I}$ o familie de submulțimi ale unei mulțimi T. Reuniunea și intersecția familiei $(A_i)_{i\in I}$ sunt definite astfel:

$$\begin{aligned} \bigcup_{i\in I} A_i &= \{x \in T \mid \text{ există } i \in I \text{ a.î. } x \in A_i\} \\ \bigcap_{i\in I} A_i &= \{x \in T \mid \text{ pentru orice } i \in I, x \in A_i\} \end{aligned}$$

Produsul cartezian al unei familii

Fie I o mulțime nevidă, și $(A_i)_{i\in I}$ familie de mulțimi indexată de I.

Produsul cartezian al familiei $(A_i)_{i\in I}$ se definește astfel:

$$\begin{aligned}\prod_{i\in I} A_i &= \left\{ f : I \to \bigcup_{i\in I} A_i \mid f(i) \in A_i \text{ pentru orice } i \in I \right\}\\ &= \{(x_i)_{i\in I} \mid x_i \in A_i \text{ pentru orice } i \in I\}.\end{aligned}$$

Pentru orice $j \in I$, aplicația $\pi_j : \prod_{i\in I} A_i \to A_j, \quad \pi_j((x_i)_{i\in I}) = x_j$ se numește proiecție canonică a lui $\prod_{i\in I} A_i$. π_j este surjectivă.

Exercițiu. Fie I, J mulțimi nevide. Atunci

$$\bigcup_{i\in I} A_i \times \bigcup_{j\in J} B_j = \bigcup_{(i,j)\in I\times J} A_i \times B_j \text{ și } \bigcap_{i\in I} A_i \times \bigcap_{j\in J} B_j = \bigcap_{(i,j)\in I\times J} A_i \times B_j.$$

$I = \{1, \ldots, n\}$

Fie n număr natural, $n \geq 1$, $I = \{1, \ldots, n\}$ și A_1, ..., $A_n \subseteq T$.

- $(x_i)_{i \in I} = (x_1, \ldots, x_n)$, un n-tuplu (ordonat)
- $\bigcup_{i \in I} A_i = \bigcup_{i=1}^{n} A_i$ și $\bigcap_{i \in I} A_i = \bigcap_{i=1}^{n} A_i$
- $\prod_{i \in I} A_i = \prod_{i=1}^{n} A_i = A_1 \times \cdots \times A_n$ și $A^n = \underbrace{A \times \cdots \times A}_{n}$

Definiție

O relație n-ară între A_1, ..., A_n este o submulțime a produsului cartezian $\prod_{i=1}^{n} A_i$.
O relație n-ară pe A este o submulțime a lui A^n. Dacă R este relație n-ară, spunem că n este aritatea lui R.

Principiul bunei ordonări

Orice submulțime nevidă a lui $\mathbb{N}$ are un cel mai mic element.

Principiul inducției

Fie $S \subseteq \mathbb{N}$ astfel încât:

(i) $0 \in S$ și

(ii) pentru orice $n \in \mathbb{N}$, dacă $n \in S$, atunci $n + 1 \in S$.

Atunci $S = \mathbb{N}$.

Dem.: Fie $S \subseteq \mathbb{N}$ a.î. (i) și (ii) sunt adevărate. Presupunem că $S \neq \mathbb{N}$, deci $\mathbb{N} \setminus S \neq \emptyset$. Fie n_0 cel mai mic element din $\mathbb{N} \setminus S$. Din (i) rezultă că $n_0 \neq 0$. Deoarece $1, \ldots, n_0 - 1 \in S$, din (ii) rezultă că $n_0 \in S$. Am obținut o contradicție. Prin urmare, $S = \mathbb{N}$. $\square$

Observație

Principiul bunei ordonări și principiul inducției sunt echivalente.