Logică matematică

Andrei Sipoș

Facultatea de Matematică și Informatică, DL Mate, Anul I

Semestrul II, 2021/2022

Aspecte organizatorice

Desfășurare

Informații actualizate despre curs, incluzând acest suport, se pot găsi la pagina:

https://cs.unibuc.ro/~asipos/lm/

Cursul și seminarele vor fi ținute conform procedurii de desfășurare a activității didactice în anul universitar 2021/2022.

Notare

Examenul va consta într-o lucrare scrisă ce va cuprinde probleme totalizând 12 puncte și va fi cu toate materialele pe masă (*open book exam*). Problemele vor fi asemănătoare cu cele din seminar (în particular, ele pot fi dintre enunțurile lăsate ca exercițiu la curs). În redactarea răspunsurilor puteți folosi orice rezultat din curs sau seminar care fie este **deja demonstrat**, fie este un exercițiu **ușor**.

Pentru promovarea examenului sunt necesare 5 puncte obținute în lucrarea scrisă.

La acest punctaj se poate adăuga maxim 1 punct dobândit în urma activității de la curs și seminar.

Introducere istorică

Logica tradițională

Logica antică a cunoscut în genere două abordări (studiate în liceu la disciplina Logică și argumentare): **logica silogistică** (introdusă de Aristotel) și **logica propozițiilor compuse** (introdusă de filosofii stoici).

Prima dintre ele a fost abordarea dominantă timp de 2000 de ani (până în secolul al XIX-lea), timp în care a fost oarecum îmbunătățită de logicieni musulmani (Avicenna, Averroes) și scolastici (Abelard, Occam, Buridan).

În ultimele secole ale acestei perioade (epoca Renașterii și epoca modernă timpurie), nu s-au mai înregistrat progrese semnificative.

Au existat în secolul al XIX-lea încercări de algebrizare (Boole, Venn).

Neajunsurile logicii tradiționale

Scopul acestor tehnici era realizarea unei argumentări corecte, însă multe enunțuri ce apăreau în argumentări nu se supuneau formelor studiate, de pildă enunțurile în care apăreau **generalități multiple**:

O pisică este temută de orice șoarece.

Ca urmare, logica avea o natură mai umanistă, în sensul că se limita la a preciza erori comune în argumentare, fără a avea pretenția de a caracteriza complet raționamentele corecte.

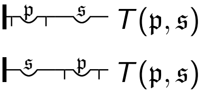
Logica lui Frege

În 1879, Gottlob Frege, în lucrarea sa *Begriffsschrift* (aprox. „notația conceptelor"), a introdus primul sistem logic în care se putea formaliza (și dezambiguiza) enunțul precedent:

$$\exists p \forall s T(p, s)$$

$$\forall s \exists p T(p, s)$$

Sistemul lui reprezintă ceea ce acum se numește **logica predicatelor** sau **logica de ordinul întâi**, însă notația lui Frege nu era cea contemporană de mai sus, ci arăta cam așa:



Alte abordări

Sistemul lui Frege nu a fost băgat în seamă până la Russell, însă ideea plutea în aer la acea vreme, un sistem similar fiind introdus de Charles Peirce începând cu anul 1882 (împreună cu studentul său, Oscar Mitchell). Sistemul său a fost mai apoi popularizat de Ernst Schröder și de Giuseppe Peano.

Peano a introdus și multe dintre simbolurile logicii actuale, de pildă semnul „$(\exists x)$" pentru „există x". (Noțiunea de „oricare x" era scrisă de el ca „(x)", notație întâlnită cam până la mijlocul secolului XX.)

Logică și matematică

Toate aceste abordări doreau cumva să obțină și o legătură a logicii cu matematica – Frege dorea să deducă afirmațiile matematice din cele logice (**logicism**), iar Peano a formulat binecunoscuta sa axiomatizare logică a aritmeticii.

Între timp, însă, matematica își trăia propria sa criză a fundamentelor.

În analiza matematică, nevoia de a formula și demonstra precis noi rezultate semnificative, precum teorema lui Fourier din 1807 ce spune că orice funcție continuă poate fi reprezentată ca o serie trigonometrică, a condus la definițiile moderne (cu ε și δ) ale limitei și continuității, datorate lui Augustin-Louis Cauchy, Bernard Bolzano și Karl Weierstrass.

Definirea riguroasă a conceptelor a permis descoperirea diverselor patologii, precum exemplul șocant al lui Weierstrass din 1872 de funcție reală continuă peste tot și derivabilă nicăieri.

În 1874, Georg Cantor, student al lui Weierstrass, analizând seriile trigonometrice, introduce primele noțiuni de **teoria mulțimilor**, incluzând faptul că (în limbaj actual) nu există o corespondență bijectivă între $\mathbb{N}$ și $\mathbb{R}$.

În următorii ani, Cantor publică mai multe rezultate de teoria mulțimilor, incluzând (în 1878) formularea **ipotezei continuumului** – orice submulțime infinită a lui $\mathbb{R}$ este în bijecție cu $\mathbb{N}$ sau cu $\mathbb{R}$ – pe care nu reușește, însă, să o demonstreze.

Metodele teoriei mulțimilor, fiind foarte puternice, au fost primite cu entuziasm de anumiți matematicieni, printre care și David Hilbert.

Hilbert

Hilbert îmbrățișase deja anumite metode matematice mai heterodoxe la acea vreme, rezolvând în 1888 o problemă pusă de Paul Gordan și demonstrând astfel că (în limbaj actual) orice ideal al unui inel de polinoame peste un corp într-un număr finit de nedeterminate este finit generat (**teorema bazei a lui Hilbert**), dar într-un mod complet neconstructiv, și nu computațional cum se rezolvaseră înainte anumite cazuri particulare.

Gordan: „*Das ist nicht Mathematik. Das ist Theologie.*"

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

Problemele lui Hilbert

În 1900, Hilbert lansează o listă de 23 de probleme, de care, în opinia sa, trebuia să se ocupe matematica secolului XX.

Prima problemă de pe listă era ipoteza continuumului a lui Cantor.

A doua problemă se referea la **consistența** fundamentelor matematicii, anume de a ne asigura că metodele folosite în demonstrațiile matematice (inclusiv cele controversate folosite de Hilbert și de către alții) nu produc contradicții.

Programul lui Hilbert

Aceste idei au condus la ceea ce a ajuns să fie numit **Programul lui Hilbert**, rezumat de obicei astfel:

1. Găsirea unui fundament adecvat pentru întreaga matematică.
2. Demonstrarea prin metode simple și necontroversate (așa-numitele **metode finitare**) că fundamentul găsit la primul punct nu produce contradicții.

Însă, contradicțiile începuseră deja să apară în sistemele existente la acea vreme.

Paradoxul lui Russell

În 1899, Ernst Zermelo descoperise o contradicție în teoria lui Cantor, pe care Bertrand Russell o redescoperă doi ani mai târziu. Ea poartă numele de **paradoxul lui Russell** și privește mulțimea $R = \{x \mid x \notin x\}$. Din definiția lui R, se deduce

$$R \in R \Leftrightarrow R \notin R,$$

absurd!

Russell observă că paradoxul se regăsește sub o anume formă și în sistemul lui Frege, și îi comunică faptul:

"There is just one point where I have encountered a difficulty."

Răspunsul lui Frege

Frege realizează eroarea și include o notă ca anexă a noii sale cărți: *"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."*

La vederea cărții lui Frege, Hilbert îi scrie:
"I believe Dr. Zermelo discovered it three or four years ago."

De asemenea, în același an 1903, Russell însuși publică paradoxul în cartea sa *The Principles of Mathematics*:
"Before taking leave of fundamental questions, it is necessary to examine more in detail the singular contradiction, already mentioned, with regard to predicates not predicable of themselves. [...] I may mention that I was led to it in the endeavour to reconcile Cantor's proof..."

Fiecare dintre cei doi descoperitori ai paradoxului a propus câte un mod prin care el putea fi evitat.

Bertrand Russell și Alfred North Whitehead au dezvoltat ceea ce astăzi se numește **teoria tipurilor** și au fundamentat matematica într-un asemenea sistem. Această muncă a fost publicată, începând cu 1910, în cartea lor *Principia Mathematica*. Notația adoptată de ei a fost în mare parte cea a lui Peano.

"An analysis of the paradoxes to be avoided shows that they all result from a kind of vicious circle. The vicious circles in question arise from supposing that a collection of objects may contain members which can only be defined by means of the collection as a whole. [...] The principle which enables us to avoid illegitimate totalities may be stated as follows: whatever involves all of a collection must not be one of the collection. [...] We shall call this the vicious-circle principle, because it enables us to avoid the vicious circles involved in the assumption of illegitimate totalities."

Zermelo a propus în schimb în 1908 o listă de axiome ce modelau (și deci restricționau) comportamentul mulțimilor lui Cantor. În următoarele decenii, Abraham Fraenkel, Thoralf Skolem și John von Neumann au extins această listă, ajungându-se la ceea ce se numește astăzi teoria axiomatică a mulțimilor **ZFC** (**Z**ermelo-**F**raenkel set theory with the axiom of **C**hoice).

ZFC a devenit în timp extrem de popular prin simplitatea lui și este în prezent sistemul îndeobște acceptat prin care este fundamentată matematica. Răspândirea lui a condus la ubicuitatea modelului

$$\text{matematică} = \text{logică} + \text{axiome},$$

renunțându-se așadar la proiectul logicist al lui Frege de a deduce matematica exclusiv din legi pur logice.

Vedem totuși că legile logice stăteau încă la temelie, și de aceea Hilbert și-a început realizarea programului său cu cele mai slabe asemenea legi, cele ale logicii propoziționale clasice. Prima problemă importantă tratată a fost cea a completitudinii axiomelor sale, anume dacă orice tautologie este demonstrabilă – în limbajul de astăzi, dacă pentru orice φ, avem

$$\models \varphi \quad \Rightarrow \quad \vdash \varphi.$$

Hilbert și asistentul său, Paul Bernays, în 1917-8, au demonstrat completitudinea unui set de axiome propoziționale gândit de ei.

În 1921, Emil Post a oferit și el o demonstrație a completitudinii logicii propoziționale, de data aceasta axiomele alese fiind cele din fragmentul corespunzător al *Principia Mathematica*.

Pasul următor era logica predicatelor, cea echivalentă cu sistemul lui Frege și cea în care toate axiomele matematice (cum ar fi ZFC) puteau fi exprimate.

Hilbert și un alt student al său, Wilhelm Ackermann, publică în 1928 cartea *Grundzüge der theoretischen Logik*, în care formulează logica predicatelor într-un mod care a rămas valabil până astăzi și în care ridică problema completitudinii.

În anul următor, **teorema de completitudine a logicii predicatelor** este demonstrată de Kurt Gödel, în teza sa de doctorat (exact în formularea Hilbert/Ackermann; demonstrația a fost încorporată în următoarele ediții ale cărții).

Aritmetica

Reamintim că prima parte a programului lui Hilbert cerea să se găsească un fundament adecvat pentru întreaga matematică.

În 1930, însă, tot Gödel dă prima lovitură programului, anunțând **prima sa teoremă de incompletitudine**: există propoziții aritmetice pe care sistemul din *Principia Mathematica* – iar, apoi, s-a observat că acesta poate fi înlocuit cu orice alt fundament plauzibil (din nou, cum ar fi ZFC) – nu le poate nici confirma, nici infirma.

Instrumentul principal al demonstrației a fost ceea ce se numește acum **Gödelizare**: codificarea formulelor și demonstrațiilor sub formă aritmetică.

Ierarhia sistemelor

Așadar, nu poate exista un singur sistem din care să se poată demonstra toate teoremele matematice, ci există o multitudine de sisteme „parțiale” cu puteri variate.

Sistemele concepute de oameni sunt grupate în general, după puterea lor de demonstrare, în trei categorii, anume, în ordine crescătoare:

- „aritmetică”;
- „analiză”;
- „teoria mulțimilor”.

Ele alcătuiesc **ierarhia Gödel**.

Consistența

Mai rămânea partea a doua a programului lui Hilbert, anume demonstrarea prin metode finitare a faptului că aceste sisteme sunt consistente (necontradictorii).

În 1931, Gödel publică demonstrația primei sale teoreme (care va reprezenta rezultatul central al tezei sale de abilitare, susținută în anul următor) împreună cu o **a doua teoremă**, ce spune că sistemele respective, **dacă** sunt consistente, **nu** își pot demonstra propria consistență (von Neumann reușise să deducă acest rezultat pornind doar de la primul anunț al lui Gödel).

Cum se aplică a doua teoremă

Acest rezultat zdrobește programul lui Hilbert! Să vedem cum.

Fie S un sistem consistent și notăm propoziția ce îi exprimă consistența prin $Con(S)$. Este posibil, uneori, să o demonstrăm într-un sistem T, mai puternic ca S și scriem $T \vdash Con(S)$. Însă, noi vrem să dobândim încredere în S. Or, acest lucru nu este posibil, având în vedere că ni s-ar cere ca, în prealabil, să avem încredere în sistemul mai puternic T.

De aceea, Hilbert dorea să arate consistența cu metode finitare, adică într-un sistem mai slab ca S, notat cu F. Dacă aceasta ar fi posibil, deci dacă am avea $F \vdash Con(S)$, atunci, cum $F \subseteq S$, am avea și $S \vdash Con(S)$. Însă, exact acest lucru este interzis de a doua teoremă a lui Gödel.

Entscheidungsproblem

O altă problemă ridicată în cartea Hilbert/Ackermann 1928 a fost așa-numita *Entscheidungsproblem* („problema de decizie") – care se referă la o potențială proprietate a logicii predicatelor mai puternică decât completitudinea – anume, dacă există o **procedură de decizie** pentru ea, un algoritm care să spună dacă un enunț este sau nu universal adevărat.

Pentru aceasta, trebuia spus mai întâi ce înseamnă un algoritm, o procedură de decizie sau, așa cum este numită acum, o funcție calculabilă.

Funcții primitiv-recursive

Ideea de la care s-a pornit a fost cea de recursivitate, metodă prin care multe funcții (de pildă șirul lui Fibonacci) erau deja uzual definite, și care are schema generală

$$f(0) := m, \quad f(n+1) := g\left(f_{|\{0,\ldots,n\}}\right)$$

Pornind de la această schemă, Skolem a introdus în 1923 clasa funcțiilor **primitiv-recursive**. Definiția precisă a fost dată de Gödel în cursul demonstrării teoremei de incompletitudine, funcțiile primitiv-recursive fiind un ingredient esențial al acelei demonstrații.

Funcții recursive

Gabriel Sudan (1927) și Wilhelm Ackermann (1928) au găsit, însă, exemple de funcții evident calculabile, dar care nu erau primitiv-recursive. (Exemplul oferit de obicei în cărțile actuale este o variantă a funcției lui Ackermann datorată lui Rózsa Péter, unul dintre părinții teoriei recursiei.)

Ca urmare, Gödel a definit în 1934 clasa funcțiilor **general-recursive**, ce includea și aceste exemple.

Modele de calcul

În 1936, Alonzo Church și Alan Turing introduc noi moduri de a defini funcțiile calculabile – modele de calcul – **calculul lambda**, respectiv **mașina Turing**. Fiecare dintre ei demonstrează că în modelul său nu poate fi decisă *Entscheidungsproblem*, folosindu-se în demonstrațiile lor de forme de Gödelizare. Problema pusă de Hilbert are așadar un răspuns negativ.

Doar mașinile Turing reușesc să îl convingă pe Gödel că reprezintă o definiție adecvată; Turing arată, însă, că ele sunt echivalente cu calculul lui Church (în plus, sunt echivalente și cu funcțiile general-recursive ale lui Gödel) și oferă argumente că ele cuprind întreaga sferă a ceea ce se poate calcula din punct de vedere informal (afirmație cunoscută acum ca **teza Church-Turing**).

Gentzen

Ultima contribuție majoră (despre care vom vorbi) a acestei perioade a logicii îi aparține lui Gerhard Gentzen.

Urmând contribuțiile sale esențiale la teoria demonstrațiilor (el fiind și cel care a introdus notația „$(\forall x)$" pentru „oricare x"), Gentzen a propus o soluție inovatoare pentru problema consistenței.

Consistența aritmeticii

Am văzut până acum că a demonstra consistența unui sistem consistent într-unul mai puternic era inutil, iar într-unul mai slab era imposibil.

Soluția lui Gentzen a fost de a o demonstra într-un sistem **incomparabil**, obținut prin adăugarea la metodele finitare principiul inducției finitare până la un ordinal **nefinitar**. El a obținut o asemenea demonstrație în 1936 pentru aritmetica de ordinul întâi, ordinalul respectiv fiind ε_0.

În anii următori, el a continuat să rafineze această demonstrație și să caute una valabilă și pentru sisteme mai puternice (de analiză), dar a murit prematur în 1945.

Logica în secolul XX

La sfârșitul celui de-al Doilea Război Mondial, toate noțiunile principale ale logicii sunt precis definite, iar limitările fundamentale sunt în mare cunoscute. Logica matematică își atinge deci maturitatea, fiind de atunci în mod convențional împărțită în patru ramuri principale:

- teoria mulțimilor
  - unde rezultatele lui Gödel (1940) și Cohen (1963) arată că ipoteza continuumului a lui Cantor este **independentă** de sistemul de axiome ZFC
- teoria recursiei (numită și teoria calculabilității)
- teoria modelelor
- teoria demonstrațiilor

împreună cu altele limitrofe: logica categorială, logicile neclasice, teoria algoritmică a informației etc.

ASL

Aceste patru ramuri sunt și cele recunoscute de forul internațional al logicii matematice, fondat în 1936, Association for Symbolic Logic (ASL).

Julia Knight (președinte ASL 2019-2021) și Ulrich Kohlenbach (președinte ASL 2016-2018)

Aplicații

Pe lângă studiul ei ca domeniu de sine stătător, logica are aplicații și în alte arii ale matematicii, dintre care amintim:

- teoria algebrică și geometrică a modelelor
    - aplicații în algebră și geometrie algebrică, cum ar fi teorema Ax-Grothendieck sau demonstrația dată de Ehud Hrushovski conjecturii Mordell-Lang pentru corpuri de funcții (de orice caracteristică)
- proof mining
    - subdomeniu introdus de Georg Kreisel și adus la maturitate de școala lui Ulrich Kohlenbach, el constă în aplicarea pentru demonstrații matematice concrete (de ex. din analiză neliniară, algebră comutativă) a tehnicilor teoriei demonstrațiilor

Planul cursului

În acest curs:

- vom studia teoria axiomatică a mulțimilor din punct de vedere naiv;
- vom descrie logica propozițională și logica predicatelor, împreună cu rezultatele lor principale și aplicațiile lor imediate;
- vom arăta cum se formalizează teoria mulțimilor în logica predicatelor, cum poate ea servi ca fundament al matematicii și cum poate fi productiv acest studiu logic al ei;
- vom arăta cum se poate aplica logica în alte ramuri ale matematicii.

Teoria mulțimilor

Motto

"We're doing set theory, so 'sets' are sets of sets."

– Donald A. Martin, *apud* Nik Weaver

Metoda axiomatică

Pentru ca raționamentele ei să fie suficient de riguroase, matematica face uz de ceea ce se numește **metoda axiomatică**. Până acum am întâlnit următoarele exemple ale aplicării metodei:

- structurile algebrice abstracte – grup, inel, corp;
- geometria euclidiană plană.

Ceea ce au aceste exemple în comun este că fiecare stabilește o listă de noțiuni primitive (în cazul grupului: element al lui și operația binară; în cazul planului: puncte, drepte, incidență) și o listă de axiome care descriu modul cum se comportă acele noțiuni primitive. Împreună, ele stabilesc cadrul teoriei matematice în discuție.

Deosebiri

Ceea ce diferă între exemplele date este că în vreme ce unele caută să descrie clase de asemenea obiecte (există mai multe grupuri, mai multe inele, cu proprietăți variate), celelalte caută să descrie cât mai fidel comportamentul unui anume obiect (cum este planul euclidian) și eventual să îl caracterizeze până la izomorfism (lucru care nu va fi mereu posibil).

Filosofii care studiază structuralismul matematic disting așadar după acest criteriu între teorii „algebrice" și „nealgebrice" (numite astfel deoarece primele apar deseori în algebră, chiar dacă nu în mod exclusiv).

Teoria mulțimilor va fi undeva la mijloc.

În dezvoltarea axiomatică a teoriei mulțimilor, noțiunile primitive vor fi cele de **mulțime** și de **relație de apartenență**, ultima având două argumente și fiind notată cu $\in$. Vom vedea că acestea sunt suficiente pentru a exprima propozițiile întregii matematici.

Universul de discurs va fi format așadar doar din mulțimi, iar despre ele vom putea face afirmații care se referă doar la relația $\in$. În plus, potrivit legilor logicii predicatelor (pe care le vom studia mai târziu în curs), se va presupune că egalitatea face parte din limbaj (cu proprietățile uzuale) și că universul conține cel puțin o mulțime.

Paradoxul lui Russell – discuție

Teoremă (Paradoxul lui Russell)

Nu există o mulțime R astfel încât pentru orice x,

$$x \in R \Leftrightarrow x \notin x.$$

Demonstrație

Presupunem că ar exista. Atunci, luând $x := R$, avem $R \in R \Leftrightarrow R \notin R$, o contradicție.

Observăm că:

- Acest rezultat este un fapt pur logic – nu avem nevoie de axiome ca să îl demonstrăm.
- Rezultatul ca atare nu este contradictoriu, el doar spune că o anume mulțime nu există. Ca urmare, dacă vrem să nu ajungem la o contradicție, trebuie ca axiomele pe care le vom introduce să nu ne permită să demonstrăm că acea mulțime există.

Axioma extensionalității

În continuare, vom descrie cele nouă axiome care alcătuiesc sistemul ZFC.

Axioma extensionalității

Pentru orice x, y, avem că dacă pentru orice z,

$$z \in x \Leftrightarrow z \in y,$$

atunci $x = y$.

Această axiomă este cea care ne permite ca în matematică să arătăm egalitatea de mulțimi „prin dublă incluziune". **Incluziunea** a două mulțimi x și y, notată cu $x \subseteq y$ (spunem și că x este **submulțime** a lui y), poate fi definită ca prescurtare a faptului că pentru orice z,

$$z \in x \Rightarrow z \in y.$$

De asemenea, notăm $x \subsetneq y$ pentru $x \subseteq y$ și $x \neq y$.

Unicitatea mulțimii vide

De asemenea, axioma ne permite să arătăm:

Teoremă

Există cel mult o mulțime vidă (fără elemente).

Demonstrație

Fie x, y mulțimi vide și fie z o mulțime oarecare. Atunci $z \notin x$ și $z \notin y$, deci echivalența

$$z \in x \Leftrightarrow z \in y$$

este adevărată. Aplicând Axioma extensionalității, rezultă $x = y$.

Nu știm, însă, că există **cel puțin** o mulțime vidă. Pentru aceasta, este nevoie să introducem încă o axiomă.

Axioma comprehensiunii

Axioma comprehensiunii (separării, specificării)

Pentru orice x și pentru orice „proprietate” P, există o mulțime y, astfel încât pentru orice z, avem

$$z \in y \Leftrightarrow z \in x \text{ și } P(z).$$

Observații:

- Am notat „z verifică P” cu $P(z)$.
- Echivalența de mai sus se va nota $y = \{z \in x \mid P(z)\}$.
- Noțiunea vagă de „proprietate” va fi lăsată nedefinită până la formularea riguroasă a ZFC în logica predicatelor; menționăm doar că este vorba doar de proprietăți ce au sens în limbajul ZFC, adică se referă doar la $\in$.
- Formularea axiomei arată un mod prin care este evitat paradoxul lui Russell, anume: nu ne permite să definim mulțimi arbitrare pornind de la anumite proprietăți, ci doar submulțimi.

Mulțimea tuturor mulțimilor

Paradoxul lui Russell poate fi aplicat acum ca să arătăm:

Teoremă

Nu există „mulțimea tuturor mulțimilor", adică o mulțime căreia să îi aparțină orice mulțime. Ca urmare, pentru orice x există y cu $y \notin x$.

Demonstrație

Presupunem că ar exista o asemenea mulțime și o notăm cu V. Atunci formăm $R := \{z \in V \mid z \notin z\}$. Dar atunci R este exact mulțimea despre care paradoxul lui Russell spune că nu există. Contradicție!

Observăm că mulțimea tuturor mulțimilor nu este un concept inerent contradictoriu, așa cum este cea din paradoxul lui Russell, ci este așa doar în lumina Axiomei comprehensiunii. Există teorii ale mulțimilor în care această mulțime există (cum ar fi **New Foundations**), și în care axioma corespunzătoare este, așadar, altfel formulată.

Existența mulțimii vide

În acest moment, putem arăta și:

Teoremă

Există o mulțime vidă.

Demonstrație

Fie x o mulțime (amintim că universul nostru de discurs conține măcar o mulțime). Formăm mulțimea

$$y := \{z \in x \mid z \neq z\}.$$

Dacă presupunem că ar exista $z \in y$, obținem $z \neq z$, contradicție. Ca urmare, y este vidă.

Acum știm că există și este unică o mulțime vidă și o notăm cu $\emptyset$.

De asemenea, putem defini **intersecția** și **diferența**, pentru orice x, y, prin $x \cap y := \{z \in x \mid z \in y\}$ și $x \setminus y := \{z \in x \mid z \notin y\}$.

Axioma perechii

Până în acest moment, nu am putut construi decât mulțimea vidă. De fapt, se poate observa că aceste două axiome permit ca singura mulțime să fie $\emptyset$, deoarece nu permit să „ieșim din cadru”. Pentru a construi mulțimi nevide, avem nevoie de:

Axioma perechii

Pentru orice x și y, există z astfel încât $x \in z$ și $y \in z$.

Observăm că z nu conține **doar** pe x și y, ci eventual și alte elemente (axiomele sunt exprimate în acest mod din motive care țin de minimalism), dar este ușor să obținem o mulțime (unică!) ce conține doar pe x și y aplicând Axioma comprehensiunii. Notăm acea mulțime cu $\{x, y\}$. În cazul în care $x = y$, vom nota mulțimea $\{x, x\}$ cu $\{x\}$. O mulțime de forma $\{x\}$ se va numi **singleton**.

Vom nota $1 := \{\emptyset\}$ și retrospectiv $0 := \emptyset$. Așadar $1 = \{0\}$. Notăm apoi $2 := \{0, 1\} = \{\emptyset, \{\emptyset\}\}$. 3 va putea fi definit doar mai târziu.

Perechi ordonate

Se observă că pentru orice x și y, $\{x, y\} = \{y, x\}$ (fapt exprimat colocvial prin „într-o mulțime nu contează ordinea elementelor”) și de aceea are sens să denumim această mulțime **perechea neordonată** a lui x și y.

În matematică, însă, se folosește deseori noțiunea de **pereche ordonată** a lui x și y, notată cu (x, y). Cum am spus, în universul nostru de discurs există doar mulțimi, deci trebuie și ca (x, y) să fie tot o mulțime. Ea trebuie să „codifice” ideea de pereche ordonată, adică pentru orice x, y să existe (x, y), iar aceasta să poată fi distinsă de (y, x), când $x \neq y$, sau în general de vreun (a, b) cu $a \neq x$ sau $b \neq y$. Nu va conta ce definiție alegem, atât timp cât va avea proprietățile dorite și o vom folosi în mod consecvent.

Proprietatea perechilor ordonate

Definiția cea mai frecvent folosită este cea dată de Kazimierz Kuratowski în 1921: $(x, y) := \{\{x\}, \{x, y\}\}$. Acum verificăm:

Proprietatea perechilor ordonate

Fie x, y, u, v cu $(x, y) = (u, v)$. Atunci $x = u$ și $y = v$.

Demonstrație

Avem $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$. Atunci $\{x\} \in \{\{u\}, \{u, v\}\}$. Distingem două cazuri.
Cazul I. Avem $\{x\} = \{u\}$. Deci $x = u$ și mai vrem $y = v$.
Subcazul I.1. Avem $x = y$. Atunci

$$(x, y) = \{\{x\}, \{x, x\}\} = \{\{x\}, \{x\}\} = \{\{x\}\}.$$

Cum $\{u, v\} \in (x, y)$, avem $\{u, v\} = \{x\}$, de unde scoatem $v = x$ și deci $y = v$.

Demonstrație (cont.)

Subcazul I.2. Avem $x \neq y$.
Atunci, cum $\{x, y\} \in \{\{u\}, \{u, v\}\}$, avem fie $\{x, y\} = \{u\}$ și deci $x = u$ și $y = u$, de unde avem $x = y$, o contradicție, fie $\{x, y\} = \{u, v\}$, deci $y = u$ sau $y = v$, dar cum $u = x$ și $x \neq y$, avem $y = v$, ceea ce trebuia demonstrat.

Cazul II. Avem $\{x\} = \{u, v\}$. Exercițiu!

Corolar

Fie x și y cu $x \neq y$. Atunci $(x, y) \neq (y, x)$.

Tupluri

Putem defini acum:

- **triplet** pentru x, y, z, ca fiind $(x, y, z) := ((x, y), z)$
- **cvadruplu** pentru x, y, z, t, ca fiind $(x, y, z, t) := (((x, y), z), t)$

și în general *n*-**tuplu** pentru orice $n \in \mathbb{N}$, dar doar în mod informal, pentru că nu avem (încă) la dispoziție numere naturale.

Când vom vrea să lucrăm cu liste de obiecte de lungime arbitrară (și ne vom putea atunci servi de $\mathbb{N}$), vom folosi o altă formalizare, lăsând-o pe cea de mai sus doar pentru listele de lungime fixă.

Axioma reuniunii

Dacă vrem să formăm mulțimi cu mai mult de două elemente, avem nevoie de următoarea axiomă.

Axioma reuniunii

Pentru orice F există x astfel încât pentru orice y, z cu $z \in y$ și $y \in F$ avem $z \in x$.

Ca mai înainte, putem folosi Axioma comprehensiunii pentru a obține, pentru orice F mulțimea care conține **exact** acei z cu proprietatea că există $y \in F$ cu $z \in y$. Vom nota această mulțime cu $\bigcup F$ și o numim **reuniunea** mulțimii F.

Atenție! Aceasta nu este reuniunea a două mulțimi cu care suntem obișnuiți, ci este, practic, „reuniunea tuturor mulțimilor din F". Reuniunea uzuală a două mulțimi, x și y, se obține ca:

$$x \cup y := \bigcup \{x, y\}.$$

Dacă F este o mulțime **nevidă**, definim **intersecția** mulțimii F ca fiind $\bigcap F := \{z \in \bigcup F \mid \text{pentru orice } x \text{ cu } x \in F, \text{ avem } z \in x\}$.

Definiție

Fie X o mulțime. Numim o mulțime $A \subseteq \mathcal{P}(X)$ **mulțime Moore** pe X dacă $X \in A$, iar pentru orice $B \subseteq A$ nevidă avem $\bigcap B \in A$.

Teoremă

Fie X o mulțime și A o mulțime Moore pe X. Atunci există și este unic $C \in A$, numit **minimul** lui A, astfel încât pentru orice $D \in A$, avem $C \subseteq D$.

Demonstrație

Unicitatea rezultă imediat: dacă avem C_1, $C_2 \in A$ cu acea proprietate, atunci $C_1 \subseteq C_2$ și $C_2 \subseteq C_1$, deci $C_1 = C_2$. Pentru existență, cum $X \in A$, avem $A \neq \emptyset$, deci $\bigcap A \in A$. Luăm $C := \bigcap A$ și verificăm că are proprietatea căutată.

Mulțimi cu mai mult de două elemente

Dacă avem x, y și z, putem defini mulțimea ce conține exact aceste elemente prin

$$\{x, y, z\} := \bigcup\{\{x, y\}, \{z\}\} = \{x, y\} \cup \{z\}.$$

În acest mod, putem defini, pentru orice $n \in \mathbb{N}$, mulțimi cu n elemente date (din nou, acest „pentru orice $n \in \mathbb{N}$" este informal).

Definim, pentru orice x, $x^+ := x \cup \{x\}$, numind această mulțime **succesorul** lui x, și apoi $3 := 2^+$. Atunci 3 este egal cu

$$2^+ = 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\}$$

și are chiar trei elemente, în sensul că $0 \neq 1$, $0 \neq 2$ și $1 \neq 2$.

Mai mult, observăm că $0^+ = 1$ și $1^+ = 2$, ceea ce justifică denumirea de succesor.

Axioma mulțimii părților

Axioma mulțimii părților

Pentru orice x există y astfel încât pentru orice z cu $z \subseteq x$ avem $z \in y$.

Pentru orice x, notăm mulțimea ce conține **exact** acei z care verifică $z \subseteq x$ cu $\mathcal{P}(x)$ și o numim **mulțimea părților** lui x.

Propoziție

Fie x, y, X, Y cu $x \in X$ și $y \in Y$. Atunci $(x, y) \in \mathcal{P}(\mathcal{P}(X \cup Y))$.

Demonstrație

Trebuie să arătăm că pentru orice $z \in (x, y)$, avem $z \in \mathcal{P}(X \cup Y)$. Fie $z \in (x, y)$. Atunci trebuie să arătăm că pentru orice $t \in z$, $t \in X \cup Y$, adică $t \in X$ sau $t \in Y$. Fie $t \in z$. Cum $(x, y) = \{\{x\}, \{x, y\}\}$, avem $z = \{x\}$ sau $z = \{x, y\}$. Cum $t \in z$, avem $t = x$ sau $t = y$. Deci $t \in X$ sau $t \in Y$.

Ca urmare, pentru orice X și Y, mulțimea definită prin

$$X \times Y := \{w \in \mathcal{P}(\mathcal{P}(X \cup Y)) \mid \text{există } x \in X \text{ și } y \in Y \text{ cu } w = (x, y)\}$$

conține toate perechile ordonate de elemente din X cu elemente din Y. O numim **produsul cartezian** al lui X și Y.

Relații binare

Propoziție-Definiție

Fie R o mulțime. Următoarele afirmații sunt echivalente:

- există A și B astfel încât $R \subseteq A \times B$;
- elementele lui R sunt perechi ordonate, adică pentru orice $z \in R$ există x, y cu $z = (x, y)$.

În acest caz, R se numește **relație (binară)**, iar dacă A și B sunt ca mai sus, spunem că R este o relație **între** A și B. Dacă A este astfel încât R este între A și A, spunem că R este o relație **pe** A.

Demonstrație

Implicația „$\Rightarrow$" este evidentă. Pentru implicația „$\Leftarrow$", notăm mulțimea $\bigcup\bigcup R$ atât cu A, cât și cu B. Fie $z \in R$. Atunci există x, y cu $z = \{\{x\}, \{x, y\}\} \in R$. Așadar, $\{x\}$, $\{x, y\} \in \bigcup R$ și deci x, $y \in \bigcup\bigcup R$. Ca urmare, $(x, y) \in \bigcup\bigcup R \times \bigcup\bigcup R = A \times B$.

Observăm și că A și B **nu sunt unice** cu acea proprietate! De exemplu, $\emptyset$ este o relație pe $\emptyset$, dar și pe $\{\emptyset\}$.

Definiție

Dacă A este o mulțime, notăm cu Δ_A și denumim **relația diagonală** pe A acea relație pe A definită prin

$$\{p \in A \times A \mid \text{există } a \text{ cu } p = (a, a)\}.$$

Definiție

Fie A, B mulțimi și R o relație între A și B. Spunem că R este **grafic** între A și B dacă pentru orice $a \in A$ există și este unic $b \in B$ astfel încât $(a, b) \in R$.

Definiție

Fie A, B mulțimi. Spunem că f este **funcție între A și B** (și notăm aceasta cu $f : A \to B$) dacă există R un grafic între A și B astfel încât $f = (A, B, R)$. A se numește **domeniul** lui f, iar B **codomeniul** lui f. Pentru orice $a \in A$ vom nota cu $f(a)$ acel unic $b \in B$ cu $(a, b) \in R$.

Detalii de codificare

Un grafic și o funcție sunt mulțimi, dar ele nu sunt aceeași mulțime! Avem nevoie de includerea codomeniului în „codificarea” noțiunii de funcție pentru a putea mai târziu formaliza corect surjectivitatea.

Propoziție

Fie R o relație binară. Următoarele afirmații sunt echivalente:

- există A și B astfel încât R este grafic între A și B;
- pentru orice x, y, z cu (x, y), $(x, z) \in R$, avem $y = z$.

Propoziție

Fie R o relație binară și A, B, C, D astfel încât R este grafic atât între A și B, cât și între C și D. Atunci $A = C$.

Aceste două propoziții (care se vor demonstra la seminar) ne arată că domeniul unei funcții este complet determinat de grafic (și îl putem numi **domeniul graficului**), ca urmare el ar fi putut să nu fie inclus în modul de definiție. El este, totuși, inclus, prin tradiție.

Notații despre funcții

Pentru orice mulțime A, avem că (A, A, Δ_A) este funcție. O numim **funcția identică pe** A sau **funcția identitate pe** A și o notăm cu id_A.

În general, dacă A și B sunt mulțimi iar $E(x)$ este o „expresie" (în sensul informal al cuvântului, analog cu noțiunea de proprietate) în care apare x, astfel încât pentru orice $x \in A$, $E(x)$ indică (în mod demonstrabil) un unic element din B, atunci, când vom spune de acum încolo „fie $f : A \to B$ astfel încât pentru orice $x \in A$, $f(x) := E(x)$", vom înțelege prin aceasta că definim relația

$$R := \{p \in A \times B \mid \text{există } x \in A \text{ cu } p = (x, E(x))\}$$

și apoi definim f ca fiind egal cu tripletul (A, B, R).

Același lucru îl vom exprima și prin: „fie $f : A \to B$ definită prin $x \mapsto E(x)$".

Funcții și mulțimi

Observăm că dacă A, B sunt mulțimi, iar $f : A \to B$, atunci $f \in (\{A\} \times \{B\}) \times \mathcal{P}(A \times B)$, ca urmare putem defini mulțimea tuturor funcțiilor de la A la B, notată cu B^A, prin

$$\{f \in (\{A\} \times \{B\}) \times \mathcal{P}(A \times B) \mid f \text{ funcție}\}.$$

Definiție

Fie A, B și $f : A \to B$. Fie $X \subseteq A$ și $Y \subseteq B$. Atunci:

- notăm cu $f_*(X)$ și numim **imaginea directă** a lui X prin f mulțimea
$$\{y \in B \mid \text{există } x \in X \text{ cu } f(x) = y\};$$
- notăm cu $f^*(Y)$ și numim **imaginea inversă** a lui Y prin f mulțimea
$$\{x \in A \mid f(x) \in Y\};$$
- notăm cu $\mathrm{Im} f$ și numim **imaginea** lui f mulțimea $f_*(A)$.

Proprietăți ale funcțiilor

Mai definim **imaginea** unui grafic ca fiind imaginea unei funcții care îl are ca grafic. Știm din cele anterioare că există o asemenea funcție și putem arăta că imaginea nu depinde de funcția aleasă.

Definiție

Fie A, B și $f : A \to B$. Spunem că:

- f este **injectivă** sau **injecție** dacă pentru orice $x, y \in A$ cu $x \neq y$, avem $f(x) \neq f(y)$;
- f este **surjectivă** sau **surjecție** dacă $\mathrm{Im} f = B$, mai exact dacă pentru orice $y \in B$ există $x \in A$ cu $f(x) = y$;
- f este **bijectivă** sau **bijecție** dacă este injectivă și surjectivă.

Compunerea și restricția funcțiilor

Definiție

Fie A, B, C și $f : A \to B$, $g : B \to C$. Definim funcția $g \circ f : A \to C$ (citim „g compus cu f"; ea se notează uneori cu $f; g$, caz în care citim „f succedat de g"), pentru orice $x \in A$, prin

$$(g \circ f)(x) := g(f(x)).$$

Proprietăți elementare

Fie A, B, C, D și $f : A \to B$, $g : B \to C$, $h : C \to D$. Atunci:

- $(h \circ g) \circ f = h \circ (g \circ f)$;
- $f \circ \mathrm{id}_A = f$; $\mathrm{id}_B \circ f = f$.

Definiție

Fie A, B, $f : A \to B$ și $X \subseteq A$. Definim funcția $f_{|X} : X \to B$ (citim „f restricționat la X"), pentru orice $x \in X$, prin $f_{|X}(x) := f(x)$.

Funcții inversabile

Definiție

Fie A, B, $f : A \to B$. Dacă $g : B \to A$, $g \circ f = \mathrm{id}_A$ și $f \circ g = \mathrm{id}_B$, spunem că f este **inversabilă** iar g este **inversa** sa.

O inversă, dacă există, este unică. Mai exact, dacă avem A, B, $f : A \to B$, iar g_1, $g_2 : B \to A$ sunt inverse ale lui f, atunci $g_1 = g_2$, iar aceasta se poate demonstra doar folosind proprietățile elementare ale compunerii:

$$g_1 = g_1 \circ \mathrm{id}_B = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = \mathrm{id}_A \circ g_2 = g_2.$$

Următorul rezultat se demonstrează ușor:

Propoziție

O funcție este inversabilă dacă și numai dacă este bijectivă.

Fie A o mulțime. Se pune întrebarea: există $f : \emptyset \to A$? Dacă da, cum arată? Presupunem că ar exista o asemenea f. Atunci există R cu $f = (\emptyset, A, R)$ și $R \subseteq \emptyset \times A = \emptyset$, deci $R = \emptyset$ și $f = (\emptyset, A, \emptyset)$. Aceasta este într-adevăr o funcție. Ca urmare, există o unică funcție de la $\emptyset$ la A, anume $(\emptyset, A, \emptyset)$, pe care o numim **funcția vidă a lui** A. Așadar, avem că $A^{\emptyset} = A^0$ este un singleton. Spunem că $\emptyset$ este **mulțimea inițială**.

Dar invers? Există o funcție $g : A \to \emptyset$? Dacă A este nevidă, atunci există $a \in A$, și deci $g(a) \in \emptyset$, o contradicție, dat fiind că nu există $b \in \emptyset$. Ca urmare, funcția există doar când $A = \emptyset$, și atunci $g = (\emptyset, \emptyset, \emptyset)$ (caz particular al celui din paragraful precedent).

Fixăm X un singleton – de exemplu, putem lua $X := 1 = \{\emptyset\}$, dar alegerea precisă a lui X nu va conta.

Fie A o mulțime. Atunci există o unică funcție de la A la X, anume cea care duce orice element din A în unicul element al lui X. De aceea, spunem că orice singleton este **mulțime terminală** (noțiune **duală** celei de mulțime inițială).

Vrem acum, invers, să găsim toate funcțiile de la X la A. Pentru a găsi o asemenea funcție, trebuie doar să selectăm elementul din A în care va fi dus acel unic element al lui X. Așadar, funcțiile de la X la A sunt în corespondență biunivocă cu elementele lui A. Deseori, în acest curs, vom **identifica tacit** A^X cu A (indiferent care este precis singleton-ul X; de pildă, vom identifica A^1 cu A).

Familii

Fie I o mulțime. Numim **familie indexată după** I un grafic al cărui domeniu este I. Dacă F este o familie indexată după I, vom nota, pentru orice $i \in I$, acea unică mulțime x pentru care $(i, x) \in F$ cu F_i. De asemenea, vom mai scrie $(F_i)_{i \in I}$ în loc de F.

Definim **reuniunea** și **intersecția**, ca familie, a lui F – notate cu $\bigcup_{i \in I} F_i$, respectiv cu $\bigcap_{i \in I} F_i$ – ca fiind reuniunea, respectiv intersecția (ultima doar în cazul în care $I \neq \emptyset$) a imaginii ca grafic a lui F.

Mai definim **produsul cartezian** al lui F ca fiind mulțimea tuturor familiilor f indexate după I cu proprietatea că pentru orice $i \in I$, $f_i \in F_i$. Această mulțime există deoarece orice asemenea f este element al lui

$$\mathcal{P}\left(I \times \bigcup_{i \in I} F_i\right).$$

Tipuri de relații binare pe o mulțime

Definiție

Fie A o mulțime și R o relație pe A. Pentru orice x, $y \in A$, vom scrie xRy în loc de $(x, y) \in R$. Spunem că R este:

- **reflexivă** dacă pentru orice $x \in A$, xRx;
- **simetrică** dacă pentru orice x, $y \in A$ cu xRy, avem yRx;
- **tranzitivă** dacă pentru orice x, y, $z \in A$ cu xRy și yRz, avem xRz;
- **de echivalență** dacă este reflexivă, simetrică și tranzitivă;
- **totală** dacă pentru orice x, $y \in A$, avem xRy sau yRx;
- **antisimetrică** dacă pentru orice x, $y \in A$ cu xRy și yRx avem $x = y$;
- **de ordine parțială** (de obicei ele sunt notate cu $\leq$) dacă este reflexivă, antisimetrică și tranzitivă;
- **ireflexivă** dacă pentru orice $x \in A$, nu avem xRx;
- **asimetrică** dacă pentru orice x, $y \in A$ cu xRy, nu avem yRx.

Relații de ordine strictă

Propoziție-Definiție

Fie A o mulțime și R o relație tranzitivă pe A. Următoarele afirmații sunt echivalente:

- R este ireflexivă;
- R este asimetrică.

În acest caz, R se numește relație **de ordine strictă** (de obicei ele sunt notate cu $<$).

Demonstrație

Pentru implicația „$\Rightarrow$", fie x, $y \in A$ cu xRy. Dacă am avea yRx, din tranzitivitate am deduce xRx, contradicție. Invers, fie x și presupunem xRx. Atunci, din asimetrie, nu avem xRx, contradicție.

Legătura dintre cele două tipuri de relație de ordine

Propoziție

Fie A o mulțime.

- Dacă $\leq$ este o relație de ordine parțială pe A și dacă definim $< \subseteq A \times A$ ca fiind mulțimea tuturor perechilor (a, b) cu proprietatea că $a \leq b$ și $a \neq b$, atunci $<$ este o relație de ordine strictă pe A.
- Dacă $<$ este o relație de ordine strictă pe A și dacă definim $\leq \subseteq A \times A$ ca fiind mulțimea tuturor perechilor (a, b) cu proprietatea că $a < b$ sau $a = b$, atunci $\leq$ este o relație de ordine parțială pe A.

Se observă ușor și că cele două operații sunt inverse una celeilalte.

Demonstrație

Exercițiu de seminar.

Putem, deci, lucra interșanjabil cu cele două tipuri de relație, folosind semnele $<$ și $\leq$ după cum ne este convenabil.

Legătura cu alte cursuri

Firește, multe dintre aceste noțiuni au fost deja studiate într-o anume formă la cursurile de algebră sau analiză. Aici insistăm în special pe chestiunile care țin de axiomatizare și formalizare (de exemplu, fundamentarea existenței anumitor mulțimi, după cum am văzut) și pe noțiuni adiacente care ne vor servi mai târziu mai mult decât ar servi altor cursuri.

În ceea ce privește capitolul actual, vom considera cunoscute noțiunile de clasă de echivalență, mulțime-cât, element minim, maxim, minimal, maximal, minorant, majorant, infimum, supremum și proprietățile lor elementare. Reamintim și definiția:

Definiție

Fie A o mulțime și $\leq$ o relație de ordine parțială pe A. Spunem că $\leq$ este o relație de **bună ordine** dacă orice submulțime nevidă B a lui A are element minim.

Reamintim că am notat, pentru orice x, $x^+ := x \cup \{x\}$ și am definit „numerele" 0, 1, 2, 3 în felul următor:

$$
\begin{aligned}
0 &:= \emptyset && = \emptyset \\
1 &:= 0^+ = 0 \cup \{0\} = \{0\} && = \{\emptyset\} \\
2 &:= 1^+ = 1 \cup \{1\} = \{0, 1\} && = \{\emptyset, \{\emptyset\}\} \\
3 &:= 2^+ = 2 \cup \{2\} = \{0, 1, 2\} && = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}
\end{aligned}
$$

Intuitiv, lista ar putea continua, punând pentru orice n, $n+1$ ca fiind n^+, în felul acesta fiecare număr natural devenind mulțimea predecesorilor săi, dar nu putem zice riguros „pentru orice n" – am avea o referință circulară. O vom rezolva prin a defini mai întâi mulțimea numerelor naturale.

Mulțimi inductive

Observăm că mulțimea numerelor naturale, oricum ar fi ea definită, trebuie să conțină pe $\emptyset$, iar pentru orice x din ea, trebuie să conțină și pe x^+. Astfel formulăm:

Definiție

O mulțime A se numește **inductivă** dacă $\emptyset \in A$ și pentru orice $x \in A$, $x^+ \in A$.

O asemenea mulțime este clar (intuitiv vorbind, deoarece nu am introdus deocamdată conceptul) infinită. Axiomele de până acum permit ca toate mulțimile care există să fie finite. Ca urmare, avem nevoie de una nouă:

Axioma infinitului

Există o mulțime inductivă.

O proprietate imediată este aceea ce spune că dacă F este o mulțime nevidă ale cărei elemente sunt mulțimi inductive, atunci și $\bigcap F$ este inductivă. În particular, dacă x și y sunt inductive, $x \cap y$ este inductivă.

Mulțimi minimal inductive

Nu este suficient ca mulțimea pe care o dorim să conțină toate acele elemente, ci mai vrem și să nu conțină altele în plus.

Definiție

O mulțime inductivă A se numește **minimal inductivă** dacă pentru orice B inductivă cu $B \subseteq A$ avem $B = A$.

Propoziție

Fie A minimal inductivă. Atunci, pentru orice B inductivă avem $A \subseteq B$. În particular, există cel mult o mulțime minimal inductivă.

Demonstrație

Dacă B este ca în enunț, atunci $A \cap B$ este inductivă și $A \cap B \subseteq A$, deci $A \cap B = A$, i.e. $A \subseteq B$.

Mulțimea numerelor naturale

Propoziție

Există (și este deci unică) o mulțime minimal inductivă.

Demonstrație

Fie u o mulțime inductivă și notăm

$$F := \{x \in \mathcal{P}(u) \mid x \text{ inductivă}\}.$$

Cum $u \in F$, $F \neq \emptyset$, iar F conține numai mulțimi inductive. Așadar și $y := \bigcap F$ este inductivă. Vom arăta că y este minimal inductivă. Fie $z \subseteq y$ inductivă. Dat fiind că $u \in F$ și $y = \bigcap F$, avem $y \subseteq u$, și deci, cum $z \subseteq y$, $z \subseteq u$. Deci, din definiția lui F, $z \in F$, deci și $y \subseteq z$, ceea ce trebuia demonstrat.

Această unică mulțime minimal inductivă o vom numi **mulțimea numerelor naturale** și o vom nota cu $\mathbb{N}$.

Principiul inducției

Faptul că $\mathbb{N}$ este minimal inductivă se poate reformula în felul următor.

Principiul inducției

Fie $A \subseteq \mathbb{N}$ astfel încât $0 \in A$ și pentru orice $n \in A$, avem $n^+ \in A$.

Atunci $A = \mathbb{N}$.

Folosind acest principiu, vom putea construi relațiile și operațiile uzuale pe $\mathbb{N}$ și demonstra proprietățile lor cunoscute.

Având în vedere că gândim un număr ca fiind mulțimea predecesorilor săi (lucru pe care îl presupunem cunoscut acum și îl vom demonstra la seminar), vom defini, pentru orice n, $m \in \mathbb{N}$, $n < m$ exact atunci când $n \in m$.

Vom demonstra acum că pentru orice $n \in \mathbb{N}$, $0 \leq n$ – observând atât folosirea Principiului inducției, cât și faptul că putem vorbi de $\leq$ imediat ce l-am introdus pe $<$. Formăm

$$A := \{n \in \mathbb{N} \mid 0 \leq n\}.$$

Cum $0 = 0$, $0 \leq 0$, deci $0 \in A$. Fie $n \in A$. Atunci $0 \leq n$, adică $0 \in n$ sau $0 = n$. Așadar, $0 \in n \cup \{n\}$, ceea ce înseamnă că $0 < n^+$. Deci $0 \leq n^+$, i.e. $n^+ \in A$, ceea ce trebuia demonstrat.

Un alt rezultat imediat spune că pentru orice k, $n \in \mathbb{N}$, $k < n^+$ dacă și numai dacă $k \leq n$.

Principiul inducției complete

Acum putem demonstra următoarea variantă mai tare, deseori folosită în matematică, a Principiului inducției.

Principiul inducției complete

Fie $A \subseteq \mathbb{N}$ astfel încât pentru orice $n \in \mathbb{N}$ ce verifică faptul că pentru orice $k \in \mathbb{N}$ cu $k < n$ avem $k \in A$, avem $n \in A$.
Atunci $A = \mathbb{N}$.

Demonstrație

Fie $B := \{n \in \mathbb{N} \mid \text{pentru orice } k \in \mathbb{N} \text{ cu } k < n \text{ avem } k \in A\}$. Clar $B \subseteq A$, deci e suficient să arătăm $B = \mathbb{N}$, lucru pentru care folosim Principiul inducției.

Trivial, $0 \in B$. Dacă $n \in B$, atunci $n \in A$, deci pentru orice $k \leq n$, $k \in A$. Dar aceasta înseamnă că pentru orice $k < n^+$, $k \in A$, deci, din definiția lui B, $n^+ \in B$.

În continuare, vom demonstra proprietățile uzuale ale relației de ordine pe $\mathbb{N}$ cu ajutorul celor două principii de inducție.

Tranzitivitatea

Demonstrăm că $<$ este tranzitivă, adică că pentru orice k, m, $n \in \mathbb{N}$ cu $k < m$ și $m < n$, avem $k < n$.

Fie k, m cu $k < m$. Demonstrăm prin inducție după n că dacă $m < n$, atunci $k < n$.

Pentru $n = 0$, știm că nu putem avea $m < 0$ (ar însemna $m \in \emptyset$), deci concluzia este trivial adevărată.

Presupunem acum că dacă $m < n$, atunci $k < n$ și vrem să arătăm că dacă $m < n^+$, atunci $k < n^+$. Presupunem $m < n^+$, deci $m < n$ sau $m = n$. Dacă $m < n$, avem din ipoteza de inducție $k < n$, deci $k < n^+$, iar dacă $m = n$, avem că $k < n$ (și deci din nou că $k < n^+$) din faptul că $k < m$.

Ireflexivitatea

Demonstrăm acum că $<$ este ireflexivă, adică că pentru orice $n \in \mathbb{N}$, nu avem $n < n$.

Clar, nu avem $0 < 0$ (fiindcă $\emptyset \notin \emptyset$). Pentru pasul de inducție, trebuie să arătăm că pentru orice n, dacă $n^+ < n^+$, avem $n < n$.

Fie $n \in \mathbb{N}$. Dacă $n^+ < n^+$, atunci $n^+ < n$ – caz în care, cum $n < n^+$, ne folosim de tranzitivitate pentru a deduce $n < n$ – sau $n^+ = n$, caz în care $n < n$ rezultă imediat.

Am demonstrat, deci, că $<$ este relație de ordine strictă. În particular, a fost mai ușor să demonstrăm astfel decât dacă ar fi fost să demonstrăm direct că $\leq$ este relație de ordine parțială.

Injectivitatea operației de succesor

Lemă

Fie n, $m \in \mathbb{N}$ cu $n^+ = m^+$. Atunci $n = m$.

Demonstrație

Presupunem $n \neq m$. Avem

$$m \cup \{m\} = n \cup \{n\},$$

deci $m \in n \cup \{n\}$, iar cum $m \neq n$, avem $m \in n$, deci $m < n$, iar pe de altă parte avem $n \in m \cup \{m\}$, iar cum $n \neq m$, avem $n \in m$, deci $n < m$. Dar faptul că $m < n$ și $n < m$ contrazice asimetria lui $<$.

O proprietate

Demonstrăm acum următorul rezultat ajutător.

Lemă

Pentru orice n, $m \in \mathbb{N}$ cu $n < m$, avem $n^+ \leq m$.

Demonstrație

Fie n și demonstrăm prin inducție după m. Cazul $m = 0$ este trivial, cum nu este posibil ca $n < 0$.

Presupunem adevărat că dacă $n < m$, avem $n^+ \leq m$ și demonstrăm că dacă $n < m^+$, avem $n^+ \leq m^+$. Presupunem, deci $n < m^+$. Atunci $n < m$ sau $n = m$. Dacă $n < m$, din ipoteza de inducție avem $n^+ \leq m$, deci $n^+ \leq m^+$. Dacă $n = m$, atunci $n^+ = m^+$ și deci $n^+ \leq m^+$.

Folosind lema anterioară, putem arăta că $\leq$ este o relație de ordine totală pe $\mathbb{N}$, deci că pentru orice $m, n \in \mathbb{N}$, avem $m \leq n$ sau $n \leq m$. Fie m și demonstrăm prin inducție după n.

Știm că pentru orice $m \in \mathbb{N}$, $0 \leq m$, ceea ce ne asigură pasul de bază.

Presupunem adevărată ipoteza de inducție, deci că avem $m \leq n$ sau $n < m$. Dacă $m \leq n$, atunci $m < n^+$. Dacă $n < m$, din lemă avem că $n^+ \leq m$, iar demonstrația este încheiată.

Relația $\leq$ pe $\mathbb{N}$ este și exemplul *par excellence* de bună ordine, am putea spune chiar prototipul definiției.

Pentru a demonstra aceasta, fie $X \subseteq \mathbb{N}$ ce nu admite minim. Vrem să arătăm $X = \emptyset$, adică $\mathbb{N} \setminus X = \mathbb{N}$.

Din Principiul inducției complete, e suficient să arătăm că pentru orice n astfel încât pentru orice $k < n$ avem $k \notin X$, avem $n \notin X$. Presupunem că este fals, deci că există $n \in X$ astfel încât pentru orice $k < n$, $k \notin X$. Dar atunci, pentru orice $m \in X$, nu avem $m < n$, deci $n \leq m$. Ca urmare, n este minimul lui X, contradicție.

Fie A o mulțime. Numim **șir** A-valuat o familie care are imaginea inclusă în A și care are drept domeniu fie un număr natural n (caz în care îl numim **șir finit** de lungime n), fie pe $\mathbb{N}$ (caz în care îl numim **șir infinit**). Vom scrie șirurile finite și folosind notații precum

$$(a_i)_{i<n}.$$

Observăm că orice șir A-valuat aparține mulțimii $\mathcal{P}(\mathbb{N} \times A)$. Ca urmare, există mulțimea tuturor șirurilor A-valuate. Vom nota mulțimea tuturor șirurilor A-valuate *finite* cu $\mathrm{Seq}(A)$, iar pentru orice $n \in \mathbb{N}$, vom nota mulțimea tuturor șirurilor A-valuate de lungime n cu $\mathrm{Seq}_n(A)$.

Menționăm că aceste șiruri reprezintă formalizarea listelor de lungime arbitrară pe care am semnalizat-o anterior.

Definiții recursive

În matematică, se folosesc deseori (după cum am amintit și în Introducerea istorică) definiții recursive. Vom da de această dată ca exemplu definiția funcției factorial:

$$f(0) := 1, \qquad f(n+1) := (n+1) \cdot f(n).$$

Astfel de definiții enumeră condiții pe care o funcție trebuie să le satisfacă și lasă să se înțeleagă că există și este unică o asemenea funcție. Acest lucru nu este însă imediat și trebuie demonstrat.

Teorema recursiei

Fie A o mulțime, $a \in A$, $g : A \times \mathbb{N} \to A$. Atunci există și este unică o funcție $f : \mathbb{N} \to A$ astfel încât $f(0) = a$ și pentru orice $n \in \mathbb{N}$, $f(n^+) = g(f(n), n)$.

Fie X mulțimea tuturor acelor $R \in \mathcal{P}(\mathbb{N} \times A)$ cu proprietatea că $(0, a) \in R$ și pentru orice $n \in \mathbb{N}$, $z \in A$ cu $(n, z) \in R$ avem $(n^+, g(z, n)) \in R$. Atunci X este o mulțime Moore pe $\mathbb{N} \times A$ și putem lua pe S ca fiind minimul ei. Este suficient să arătăm că S este grafic, i.e. că pentru orice $n \in \mathbb{N}$ există și este unic $b \in A$ cu $(n, b) \in S$.

Existența rezultă imediat (exercițiu!). Pentru unicitate, considerăm B mulțimea acelor $n \in \mathbb{N}$ cu proprietatea că există și este unic $b \in A$ cu $(n, b) \in S$. Arătăm prin inducție că $B = \mathbb{N}$. Pentru 0, cum $(0, a) \in S$, presupunând prin absurd că ar exista $b \neq a$ cu $(0, b) \in S$, se arată (exercițiu!) că $S \setminus \{(0, b)\} \in X$, contrazicând faptul că S este minim. Presupunem acum că $n \in B$ și vrem $n^+ \in B$. Fie z cu $(n, z) \in S$, atunci avem $(n^+, g(z, n)) \in S$. La fel, presupunem că ar exista $b \neq g(z, n)$ cu $(n^+, b) \in S$, se arată (exercițiu!) că $S \setminus \{(n^+, b)\} \in X$, contrazicând faptul că S este minim.

Oarecum analog Principiului inducției complete, avem următoarea teoremă, care ne permite să definim funcții ce depind de valori ale lor dinaintea celei precedente pasului curent, de exemplu șirul lui Fibonacci dat ca exemplu în Introducere.

Teorema recursiei complete

Fie A o mulțime, $g : \mathrm{Seq}(A) \to A$. Atunci există și este unică o funcție $f : \mathbb{N} \to A$ astfel încât pentru orice $n \in \mathbb{N}$, $f(n) = g((f(i))_{i<n})$.

Schițăm doar demonstrația. Construim, folosind Teorema recursiei, $F : \mathbb{N} \to \mathrm{Seq}(A)$, prin $F(0) := \emptyset$ și pentru orice $n \in \mathbb{N}$, $F(n^+) := F(n) \cup \{(n, g(F(n)))\}$.

Atunci $f := (\mathbb{N}, A, \bigcup \mathrm{Im} F)$ este funcția căutată.

În aplicații pe care le vom vedea imediat, vom avea nevoie și de următoarea formă aparent mai puternică de recursie.

Teorema recursiei parametrizate

Fie A, P mulțimi, $a : P \to A$, $g : P \times A \times \mathbb{N} \to A$. Atunci există și este unică o funcție $f : P \times \mathbb{N} \to A$ astfel încât pentru orice $p \in P$, $f(p, 0) = a(p)$ și pentru orice $p \in P$ și $n \in \mathbb{N}$, $f(p, n^+) = g(p, f(p, n), n)$.

Pentru a o demonstra, definim $G : A^P \times \mathbb{N} \to A^P$, pentru orice $x \in A^P$, $n \in \mathbb{N}$, $p \in P$, prin $G(x, n)(p) := g(p, x(p), n)$ și apoi definim funcția $F : \mathbb{N} \to A^P$ recursiv, prin $F(0) := a$ și pentru orice $n \in \mathbb{N}$, $F(n^+) := G(F(n), n)$. Atunci putem defini f, pentru orice $p \in P$ și $n \in \mathbb{N}$, prin $f(p, n) := F(n)(p)$. Putem acum verifica:

$$\begin{aligned} f(p,0) &= F(0)(p) = a(p) \\ f(p,n^+) &= F(n^+)(p) = G(F(n),n)(p) = g(p, F(n)(p), n) \\ &= g(p, f(p,n), n). \end{aligned}$$

Adunarea

Dacă în Teorema recursiei parametrizate luăm $A := \mathbb{N}$, $P := \mathbb{N}$, $a := \mathrm{id}_{\mathbb{N}}$ și $g : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, definită, pentru orice a, b, $c \in \mathbb{N}$, prin $g(a, b, c) := b^+$, obținem că există o unică funcție $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ ce verifică:

- pentru orice $m \in \mathbb{N}$, $+(m, 0) = m$;
- pentru orice m, $n \in \mathbb{N}$, $+(m, n^+) = (+(m, n))^+$.

Vom numi funcția $+$ **adunarea numerelor naturale** și vom nota, pentru orice m, $n \in \mathbb{N}$, $m + n := +(m, n)$. De pildă, putem calcula:

$$1 + 1 = 1 + 0^+ = (1 + 0)^+ = 1^+ = 2.$$

$$1 + 2 = 1 + 1^+ = (1 + 1)^+ = 2^+ = 3.$$

În acest moment, putem demonstra că adunarea este comutativă, adică că pentru orice m, $n \in \mathbb{N}$, $m + n = n + m$.

Demonstrăm prin inducție dublă, după n iar apoi după m. Pentru $n = 0$ și $m = 0$, obținem $0 + 0 = 0 + 0$, adevărat, iar la pasul inductiv pentru m avem

$$m^+ + 0 = m^+ = (m + 0)^+ = (0 + m)^+ = 0 + m^+.$$

La pasul inductiv pentru n, avem pentru $m = 0$ că

$$0 + n^+ = (0 + n)^+ = (n + 0)^+ = n^+ = n^+ + 0,$$

iar la pasul inductiv pentru m avem

$$\begin{aligned} m^+ + n^+ &= (m^+ + n)^+ = (n + m^+)^+ = (n + m)^{++} = (m + n)^{++} \\ &= (m + n^+)^+ = (n^+ + m)^+ = n^+ + m^+. \end{aligned}$$

Comentarii

În acest mod, se pot demonstra și alte proprietăți ale adunării numerelor naturale și se pot introduce și celelalte operații uzuale pe $\mathbb{N}$ (înmulțirea, ridicarea la putere) împreună cu proprietățile lor.

Apoi, așa cum s-a studiat la cursurile de algebră și analiză, odată ce aceste fapte sunt complet justificate, se pot construi numerele întregi, raționale, reale. Noi vom presupune în continuare toate faptele aferente lor ca fiind cunoscute.

Mulțimi finite

Până acum, am vorbit informal de mulțimi „cu un element", „cu trei elemente", dar nu puteam face noțiunea să fie precisă.

Definiție

Fie A o mulțime. Dacă $n \in \mathbb{N}$, spunem că A **are** n **elemente** dacă există o bijecție de la n la A. Dacă există $n \in \mathbb{N}$ astfel încât A are n elemente, spunem că A este **finită**. Dacă A nu este finită, spunem că A este **infinită**.

Firește, mai trebuie demonstrat că acel n, dacă există, este unic determinat de A.

Mulțimi finite – proprietăți

Lemă

Un număr natural (și ca urmare, o mulțime finită) nu este în bijecție cu o parte strictă a sa.

Demonstrație

Fie n numărul și demonstrăm prin inducție după n. Pentru $n = 0$, rezultatul este trivial, dat fiind că nu există părți stricte ale lui $\emptyset$. Presupunem adevărat pentru n și demonstrăm pentru $n + 1$. Presupunem că ar exista X o parte strictă a lui $n + 1$ și o bijecție $f : (n + 1) \to X$. Distingem două cazuri. Dacă $n \notin X$, atunci funcția $g : n \to X \setminus \{f(n)\} \subsetneq n$, definită, pentru orice $m \in n$, prin $g(m) := f(m)$, este bine definită și bijectivă, contradicție. Dacă $n \in X$, demonstrația rămâne ca exercițiu.

Peste câteva cursuri, vom demonstra și reciproca acestei propoziții, anume că o mulțime infinită este în bijecție cu o parte strictă a sa, dar anumite cazuri particulare le vom putea arăta imediat.

Mulțimi finite – proprietăți

Corolar

- Dacă $n, m \in \mathbb{N}$ și $n \neq m$, nu există bijecție între n și m. Ca urmare, numărul de elemente al unei mulțimi finite este unic.
- Funcția $f : \mathbb{N} \to \mathbb{N} \setminus \{0\}$, definită, pentru orice n, prin $f(n) := n^+$ este bijectivă. Ca urmare, $\mathbb{N}$ este infinită.

Demonstrație

- Dacă $n \neq m$, știm că $n < m$ sau $m < n$. Presupunem fără a restrânge generalitatea (engl. *without loss of generality*, prescurtat de obicei w.l.o.g.) că $n < m$. Atunci pentru orice $p < n$, avem $p < m$ (din tranzitivitate), deci $n \subsetneq m$. Atunci concluzia rezultă din lema precedentă.
- Injectivitatea a fost demonstrată mai devreme, iar surjectivitatea rezultă dintr-un exercițiu din seminar.

Propoziție

- O submulțime a unei mulțimi finite este finită.
- Imaginea printr-o funcție a unei mulțimi finite este finită.
- Reuniunea a două mulțimi finite este finită.
- Reuniunea unei familii finite de mulțimi finite este finită.
- Mulțimea părților unei mulțimi finite este finită.

Demonstrație

Exercițiu (parțial la seminar).

Echipotență

Vedem, așadar, că mulțimile finite sunt „măsurate” cu ajutorul numerelor naturale și al bijecțiilor.

Cum măsurăm mulțimile infinite? Deocamdată, nu avem un analog al numerelor naturale, dar ne putem folosi încă de bijecții pentru a măsura mulțimile doar după ele însele.

Definiție

Două mulțimi A și B se numesc **echipotente** – și notăm $A \sim B$ – dacă există o bijecție de la A la B.

Echipotența ca „relație de echivalență”

Am putea fi tentați să spunem că echipotența este o relație binară, dar aceasta nu ar avea sens, dat fiind că ar fi trebuit să fie o relație pe „mulțimea tuturor mulțimilor”. Totuși, ea are proprietățile caracteristice unei relații de echivalență.

Propoziție

Fie A, B, C. Atunci:

- $A \sim A$;
- Dacă $A \sim B$, atunci $B \sim A$;
- Dacă $A \sim B$ și $B \sim C$, atunci $A \sim C$.

Demonstrație

Demonstrațiile sunt imediate. Considerăm $\mathrm{id}_A : A \to A$. Dacă avem $f : A \to B$ bijecție, atunci f^{-1} este tot bijecție. Dacă avem $f : A \to B$ și $g : B \to C$ bijecții, atunci și $g \circ f$ este bijecție.

Clase de echivalență?

Apare totuși întrebarea: chiar dacă $\sim$ nu este o relație de echivalență, putem considera clasele ei, adică, pentru orice A, să notăm $|A|$ mulțimea tuturor mulțimilor echipotente cu A? Ideea ar fi ca atunci să definim **cardinalul** unei mulțimi, după cum a făcut-o Cantor, ca fiind clasa ei de echipotență.

Clar (din cele arătate mai devreme), o mulțime este echipotentă cu $\emptyset$ dacă și numai dacă este $\emptyset$, deci $|\emptyset|$ ar fi $\{\emptyset\}$ – aici nu avem probleme.

Este imediat, însă, că o mulțime este echipotentă cu $\{\emptyset\}$ dacă și numai dacă este singleton. Or, am demonstrat la seminar că nu există mulțimea tuturor mulțimilor singleton. Ca urmare, nu putem vorbi de clase de echivalență pentru $\sim$.

Cardinali

Totuși, de obicei (de pildă, în liceu), se definește cardinalul unei mulțimi cu n elemente ca fiind n. Aceasta – precum și modul în care au fost definite aici numerele naturale – ne sugerează o altă abordare – anume de a fixa pentru fiecare „clasă” un reprezentant, iar acela să fie cardinalul oricărei mulțimi din „clasă”.

Vom face așadar următoarea presupunere: există un soi de mulțimi numite **cardinali** astfel încât oricărei mulțimi X i se asociază un cardinal, notat cu $|X|$, astfel încât $X \sim |X|$, pentru orice cardinal κ avem $|\kappa| = \kappa$, pentru orice n și orice X cu n elemente avem $|X| = n$ și pentru orice X și Y avem că $X \sim Y$ dacă și numai dacă $|X| = |Y|$. (Deci $|\emptyset|$ este $\emptyset$, iar nu $\{\emptyset\}$ ca mai devreme.)

Vom justifica presupunerea mai târziu. Deocamdată, însă, se va putea observa că orice formulăm și demonstrăm cu ajutorul acestei notații se poate face într-o egală măsură și fără a face uz de ea.

Pentru a compara mulțimi ce au eventual cardinal diferit, ne folosim de injecții pentru a defini o nouă pseudo-relație.

Definiție

Fie A, B. Spunem că A este **de cardinal mai mic sau egal ca** B – și notăm $A \preceq B$ – dacă există o injecție de la A la B.

Această definiție este compatibilă cu relația $\sim$, în felul următor (demonstrația este imediată):

Propoziție

Fie A, B, C. Atunci:

- Dacă $A \preceq B$ și $A \sim C$, atunci $C \preceq B$;
- Dacă $A \preceq B$ și $B \sim C$, atunci $A \preceq C$.

Putem defini deci fără probleme $|A| \leq |B|$ dacă $A \preceq B$. Observăm și că putem spune riguros ce înseamnă „a avea același cardinal ca" și „a avea cardinalul mai mic sau egal ca" fără a ști ce înseamnă cardinal.

Cardinalii sunt parțial ordonați

Vom vedea acum că $\leq$ are proprietățile unei relații de ordine parțială. Reflexivitatea și tranzitivitatea se demonstrează la fel ca pentru $\sim$:

Propoziție

Fie A, B, C. Atunci:

- $|A| \leq |A|$;
- Dacă $|A| \leq |B|$ și $|B| \leq |C|$, atunci $|A| \leq |C|$.

Antisimetria, însă, este un rezultat netrivial:

Teorema Cantor-Bernstein-Schröder

Dacă X și Y sunt astfel încât $X \preceq Y$ și $Y \preceq X$, atunci $X \sim Y$.

Pentru a-l demonstra, ne vom folosi de o lemă ce este practic un caz particular al său.

Lemă

Fie A, B, A_1 cu $A_1 \subseteq B \subseteq A$ și $A \sim A_1$. Atunci $A \sim B$.

Mai întâi, să vedem de ce lema ne demonstrează teorema. Dacă X și Y sunt ca în enunțul teoremei, iar $f : X \to Y$ și $g : Y \to X$ sunt injecții, atunci $f_*(X) \subseteq Y$ și deci

$$(g \circ f)_*(X) = g_*(f_*(X)) \subseteq g_*(Y) \subseteq X.$$

Cum $g \circ f$ este injectivă, avem $X \sim g_*(f_*(X))$. Aplicând lema, avem $X \sim g_*(Y)$. Cum g este injectivă, $g_*(Y) \sim Y$ și deci $X \sim Y$.

Demonstrăm acum lema. Fie $f : A \to A_1$ bijectivă. Definim recursiv $A_0 := A$ și pentru orice n, $A_{n+1} := f_*(A_n)$ și analog, $B_0 := B$ și pentru orice n, $B_{n+1} := f_*(B_n)$. Cum $A_1 \subseteq B_0 \subseteq A_0$, avem pentru orice n, $A_{n+1} \subseteq B_n \subseteq A_n$. Notăm, pentru orice n, $C_n := A_n \setminus B_n$ și apoi $C := \bigcup_{n \in \mathbb{N}} C_n$, $D := A \setminus C$.

Finalizare

Se arată apoi (exercițiu!) că pentru orice n, $f_*(C_n) = C_{n+1}$ și deci $f_*(C) = \bigcup_{n \in \mathbb{N} \setminus \{0\}} C_n$.

Definim acum $g : A \to B$, pentru orice $x \in A$, prin:

$$g(x) := \begin{cases} f(x), & \text{dacă } x \in C; \\ x, & \text{dacă } x \in D. \end{cases}$$

Se arată atunci (exercițiu!) că g este bine definită și bijectivă. Așadar, $A \sim B$.

Am terminat de demonstrat, deci, că $\leq$ are proprietățile unei relații de ordine parțială. Am putea crede că vom demonstra acum că $\leq$ este totală, adică pentru orice A, B, avem $|A| \leq |B|$ sau $|B| \leq |A|$. Aceasta este adevărat în ZFC, dar o vom putea arăta doar mai târziu.

Mulțimi numărabile

Definiție

O mulțime se numește **numărabilă** dacă este echipotentă cu $\mathbb{N}$.

Vom extinde presupunerea făcută punând pentru orice mulțime numărabilă A, $|A| = \mathbb{N}$ și îl vom nota în acest context pe $\mathbb{N}$ și cu $\aleph_0$ ($\aleph$, alef, este prima literă a alfabetului ebraic).

Propoziție

Dacă A este infinită, $|B| = \aleph_0$ și $A \subseteq B$, $|A| = \aleph_0$.

Demonstrație

Fie $g : \mathbb{N} \to B$ bijecție. Vom construi o bijecție $f : \mathbb{N} \to A$ prin Teorema recursiei complete, punând, pentru orice $k \in \mathbb{N}$,

$$m := \min\{n \in \mathbb{N} \mid g(n) \in A \setminus f_*(k)\}$$

(faptul că A este infinită ne garantează că mulțimea respectivă este nevidă și deci are minim) și apoi $f(k) := g(m)$.

Așadar, $\aleph_0$ este cel mai mic cardinal infinit.

Mulțimi cel mult numărabile

Propoziție-Definiție

Fie A o mulțime. Următoarele afirmații sunt echivalente:

- A este finită sau numărabilă;
- există B numărabilă (putem lua chiar $B := \mathbb{N}$) și $f : A \to B$ injectivă.

Atunci A se numește **cel mult numărabilă**.

Demonstrație

Dacă A este finită, există $n \in \mathbb{N}$ și $g : A \to n$ bijecție. Cum $n \subseteq \mathbb{N}$, putem prelungi pe g la $f : A \to \mathbb{N}$ injecție. Dacă A este numărabilă, atunci din start avem $f : A \to \mathbb{N}$ bijecție.

Pentru implicația inversă, dacă A nu este finită și $A \sim \mathrm{Im} f$, avem că $\mathrm{Im} f$ este infinită. Cum $\mathrm{Im} f \subseteq B$, avem că $\mathrm{Im} f$ numărabilă și deci că A este numărabilă.

Imaginea mulțimilor numărabile

Propoziție

Fie B o mulțime și $f : \mathbb{N} \to B$. Atunci $\mathrm{Im} f$ este cel mult numărabilă.

Demonstrație

Definim $g : \mathrm{Im} f \to \mathbb{N}$, pentru orice $b \in \mathrm{Im} f$, prin

$$g(b) := \min\{n \in \mathbb{N} \mid f(n) = b\}.$$

Atunci pentru orice $b \in \mathrm{Im} f$, avem $f(g(b)) = b$, deci g este injectivă. Prin urmare, $\mathrm{Im} f$ este cel mult numărabilă.

Corolar

Fie A, B cu A numărabilă și $f : A \to B$. Atunci $\mathrm{Im} f$ este cel mult numărabilă.

Reuniunea mulțimilor numărabile

Propoziție

Fie A, B numărabile. Atunci $A \cup B$ este numărabilă.

Demonstrație

Fie $f : \mathbb{N} \to A$ și $g : \mathbb{N} \to B$ bijecții. Definim $h : \mathbb{N} \to A \cup B$, pentru orice $n \in \mathbb{N}$, prin

$$h(n) := \begin{cases} f\left(\frac{n}{2}\right), & \text{dacă } n \text{ este par;} \\ g\left(\frac{n-1}{2}\right), & \text{dacă } n \text{ este impar.} \end{cases}$$

Avem că h este surjectivă, deci $A \cup B$ este cel mult numărabilă. Cum A este infinită, $A \cup B$ este infinită și deci numărabilă.

Corolar

Reununea unei familii finite nevide de mulțimi numărabile este numărabilă.

Produsul cartezian al mulțimilor numărabile

Propoziție

Mulțimea $\mathbb{N} \times \mathbb{N}$ este numărabilă.

Demonstrație

Definim $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, pentru orice $(n, k) \in \mathbb{N} \times \mathbb{N}$, prin

$$f(n, k) := 2^k(2n + 1) - 1.$$

Avem că f este bijecție.

Corolar

Fie A, B numărabile. Atunci $A \times B$ este numărabilă.

Corolar

Produsul cartezian al unei familii finite nevide de mulțimi numărabile este numărabil.

Familii numărabile

Propoziție

Fie $(A_n)_{n\in\mathbb{N}}$ și pentru orice n, o surjecție $f_n : \mathbb{N} \to A_n$. Atunci $\bigcup_{n\in\mathbb{N}} A_n$ este cel mult numărabilă.

Demonstrație

Definim $f : \mathbb{N} \times \mathbb{N} \to \bigcup_{n\in\mathbb{N}} A_n$, pentru orice $(n, k) \in \mathbb{N} \times \mathbb{N}$, prin $f(n, k) := f_n(k)$. Atunci f este surjecție.

Un număr numărabil de șiruri

Propoziție

Mulțimea $\mathrm{Seq}(\mathbb{N})$ este numărabilă.

Demonstrație

Avem că $\mathrm{Seq}(\mathbb{N}) = \bigcup_{n\in\mathbb{N}} \mathrm{Seq}_n(\mathbb{N})$. Vom defini, pentru orice $n \in \mathbb{N}$, în mod recursiv, o funcție surjectivă $f_n : \mathbb{N} \to \mathrm{Seq}_n(\mathbb{N})$ și apoi vom aplica propoziția precedentă pentru a arăta că $\mathrm{Seq}(\mathbb{N})$ este cel mult numărabilă. Cum $\mathbb{N} \sim \mathrm{Seq}_1(\mathbb{N}) \subseteq \mathrm{Seq}(\mathbb{N})$, avem că $\mathrm{Seq}(\mathbb{N})$ este infinită, deci numărabilă.

Punem $f_0 : \mathbb{N} \to \mathrm{Seq}_0(\mathbb{N}) = \{\emptyset\}$ funcția ce asociază fiecărui număr mulțimea vidă. Fixăm o bijecție $g : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ și apoi definim, pentru orice n, $f_{n+1} : \mathbb{N} \to \mathrm{Seq}_{n+1}(\mathbb{N})$, pentru orice $k \in \mathbb{N}$, punând $(a, b) := g(k)$ și $f_{n+1}(k) := f_n(a) \cup \{(n, b)\}$.

Corolar

Dacă A este numărabilă, atunci $\mathrm{Seq}(A)$ este numărabilă.

$\mathbb{Z}$ și $\mathbb{Q}$

Propoziție

Mulțimea $\mathbb{Z}$ este numărabilă.

Demonstrație

Scriem $\mathbb{Z} = \{0, 1, 2, 3, \ldots\} \cup \{-1, -2, -3, \ldots\}$.

Propoziție

Mulțimea $\mathbb{Q}$ este numărabilă.

Demonstrație

Definim $f : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Q}$, pentru orice (p, q), prin

$$f(p, q) := p/q.$$

Avem că f este surjecție, deci $\mathbb{Q}$ este cel mult numărabilă. Cum $\mathbb{Z}$ este infinită și $\mathbb{Z} \subseteq \mathbb{Q}$, $\mathbb{Q}$ este infinită și deci numărabilă.

Funcția caracteristică

Pentru orice X, A, cu $A \subseteq X$, definim funcția $\chi_{A,X} : X \to 2$, pentru orice $x \in X$, prin

$$\chi_{A,X}(x) := \begin{cases} 1, & \text{dacă } x \in A \\ 0, & \text{dacă } x \notin A. \end{cases}$$

și o numim **funcția caracteristică** sau **funcția indicator** a lui A în X (vom nota deseori doar cu χ_A atunci când X va fi clar din context).

Propoziție

Pentru orice X, $\mathcal{P}(X) \sim 2^X$.

Aceasta rezultă din existența bijecțiilor naturale $A \mapsto \chi_A$ și $f \mapsto f^*(\{1\})$ între cele două mulțimi.

Mulțimi nenumărabile

Propoziție

Pentru orice X, nu există o surjecție de la X la $\mathcal{P}(X)$, deci $|X| < |\mathcal{P}(X)|$.

Demonstrație

Presupunem că ar exista $f : X \to \mathcal{P}(X)$ surjecție. Notăm $A := \{x \in X \mid x \notin f(x)\} \in \mathcal{P}(X)$. Cum f este surjectivă, există $z \in X$ cu $f(z) = A$. Dar atunci

$$z \in A \Leftrightarrow z \notin f(z) \Leftrightarrow z \notin A,$$

o contradicție.

Ca urmare, $\mathbb{N} \not\sim \mathcal{P}(\mathbb{N})$, deci $\mathcal{P}(\mathbb{N})$ este infinită, nenumărabilă.

Vom arăta în continuare că $\mathcal{P}(\mathbb{N}) \sim \mathbb{R}$ folosind teorema Cantor-Bernstein. Ca urmare, vom construi injecții $\phi : \mathcal{P}(\mathbb{N}) \to \mathbb{R}$ și $\psi : \mathbb{R} \to \mathcal{P}(\mathbb{N})$.

Prima injecție

Punem, pentru orice $A \subseteq \mathbb{N}$,

$$\phi(A) = \lim_{n\to\infty} \sum_{i=0}^{n} \frac{2\chi_A(i)}{3^i}.$$

Trebuie mai întâi să arătăm că funcția ϕ e bine definită, deci că limita considerată mai sus există. Sumele au doar termeni nenegativi, de unde reiese că șirul este crescător. Mai mult, pentru orice n din $\mathbb{N}$, avem:

$$0 \leq \sum_{i=0}^{n} \frac{2\chi_A(i)}{3^i} \leq \sum_{i=0}^{n} \frac{2}{3^i} = 2\sum_{i=0}^{n} \frac{1}{3^i} = 2 \cdot \frac{1-\left(\frac{1}{3}\right)^n}{1-\frac{1}{3}} \leq 2 \cdot \frac{1}{\frac{2}{3}} = 3.$$

Așadar, șirul este mărginit. Fiind și monoton, obținem din teorema Weierstrass că este convergent, deci ϕ este bine definită.

Arătăm acum injectivitatea. Presupunem că $A \neq B$ și urmărim să demonstrăm că $\phi(A) \neq \phi(B)$. Deoarece A și B sunt diferite, există $j = \min\{i \in \mathbb{N} \mid \chi_A(i) \neq \chi_B(i)\}$. Presupunem w.l.o.g. că $\chi_A(j) = 0$ și $\chi_B(j) = 1$. Notăm

$$a := \sum_{i=0}^{j-1} \frac{2\chi_A(i)}{3^i} = \sum_{i=0}^{j-1} \frac{2\chi_B(i)}{3^i}.$$

Pentru orice $n \geq j+1$ avem:

$$\begin{aligned}
\sum_{i=0}^{n} \frac{2\chi_A(i)}{3^i} &= \sum_{i=0}^{j-1} \frac{2\chi_A(i)}{3^i} + \frac{2 \cdot 0}{3^j} + \sum_{i=j+1}^{n} \frac{2\chi_A(i)}{3^i} \\
&\leq a + 0 + \sum_{i=j+1}^{n} \frac{2}{3^i} = a + \frac{2}{3^{j+1}} \sum_{i=0}^{n-j-1} \frac{1}{3^i} \\
&= a + \frac{2}{3^{j+1}} \cdot \frac{1 - \left(\frac{1}{3}\right)^{n-j-1}}{1 - \frac{1}{3}} < a + \frac{2}{3^{j+1}} \cdot \frac{1}{\frac{2}{3}} = a + \frac{1}{3^j}.
\end{aligned}$$

De aici scoatem

$$\phi(A) = \lim_{n\to\infty} \sum_{i=0}^{n} \frac{2\chi_A(i)}{3^i} \leq \lim_{n\to\infty} \left(a + \frac{1}{3^j}\right) = a + \frac{1}{3^j}.$$

Pentru orice $n \geq j+1$:

$$\sum_{i=0}^{n} \frac{2\chi_B(i)}{3^i} = \sum_{i=0}^{j-1} \frac{2\chi_B(i)}{3^i} + \frac{2\cdot 1}{3^j} + \sum_{i=j+1}^{n} \frac{2\chi_B(i)}{3^i} \geq a + \frac{2}{3^j}.$$

Așadar,

$$\phi(B) = \lim_{n\to\infty} \sum_{i=0}^{n} \frac{2\chi_B(i)}{3^i} \geq \lim_{n\to\infty} \left(a + \frac{2}{3^j}\right) = a + \frac{2}{3^j} > a + \frac{1}{3^j} \geq \phi(A).$$

Deci, $\phi(A) < \phi(B)$, de unde $\phi(A) \neq \phi(B)$.

A doua injecție

Pentru a construi a doua injecție, ne folosim de o bijecție $j : \mathbb{N} \to \mathbb{Q}$. Punem acum, pentru orice $r \in \mathbb{R}$,

$$\psi(r) := \{n \in \mathbb{N} \mid j(n) \leq r\}.$$

Vrem să arătăm că ψ e injectivă.

Fie r_1 și r_2 două numere reale diferite și presupunem w.l.o.g. că $r_1 < r_2$. Din densitatea numerelor raționale, știm că există $q \in \mathbb{Q}$ astfel încât $r_1 < q < r_2$. Funcția j este surjectivă, deci există m un număr natural astfel încât $j(m) = q$. Deci $j(m) \leq r_2$ și $j(m) \not\leq r_1$, de unde avem $m \in \psi(r_2)$ și $m \notin \psi(r_1)$, demonstrând astfel că $\psi(r_1) \neq \psi(r_2)$.

Demonstrația este încheiată. Așadar, $\mathbb{R}$ este echipotentă cu $\mathcal{P}(\mathbb{N})$ și este și ea o mulțime infinită, nenumărabilă.

Adunarea cardinalilor

Pentru orice cardinali κ, λ, definim adunarea lor astfel: alegem A și B cu $|A| = \kappa$, $|B| = \lambda$ și $A \cap B = \emptyset$ și punem

$$\kappa + \lambda := |A \cup B|.$$

Această definiție are sens fiindcă:

- pentru orice A, B există A', B' cu $|A'| = |A|$, $|B'| = |B|$ și $A' \cap B' = \emptyset$ (iau, de pildă, $A' := \{0\} \times A$ și $B' := \{1\} \times B$);
- pentru orice A, B, A', B' cu $|A| = |A'|$, $|B| = |B'|$, $A \cap B = \emptyset$ și $A' \cap B' = \emptyset$, avem $|A \cup B| = |A' \cup B'|$.

Proprietățile adunării

Proprietăți imediate

Fie κ, κ', λ, μ cardinali. Atunci:

- $\kappa + \lambda = \lambda + \kappa$;
- $(\kappa + \lambda) + \mu = \kappa + (\lambda + \mu)$;
- $\kappa \leq \kappa + \lambda$;
- dacă $\kappa \leq \kappa'$ și $\lambda \leq \mu$, atunci $\kappa + \lambda \leq \kappa' + \mu$.

Înmulțirea cardinalilor

Pentru orice cardinali κ, λ, definim înmulțirea lor astfel: alegem A și B cu $|A| = \kappa$ și $|B| = \lambda$ și punem

$$\kappa \cdot \lambda := |A \times B|.$$

Această definiție are sens fiindcă pentru orice A, B, A', B' cu $|A| = |A'|$ și $|B| = |B'|$, avem $|A \times B| = |A' \times B'|$.

Proprietăți imediate

Fie κ, κ', λ, μ cardinali. Atunci:

- $\kappa \cdot \lambda = \lambda \cdot \kappa$;
- $(\kappa \cdot \lambda) \cdot \mu = \kappa \cdot (\lambda \cdot \mu)$;
- $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$;
- dacă $0 < \lambda$, atunci $\kappa \leq \kappa \cdot \lambda$;
- dacă $\kappa \leq \kappa'$ și $\lambda \leq \mu$, atunci $\kappa \cdot \lambda \leq \kappa' \cdot \mu$.

Înmulțirea cu doi

Propoziție

Pentru orice cardinal κ, $\kappa + \kappa = 2 \cdot \kappa$.

Demonstrație

Avem $|\{0\} \times \kappa| = |\{1\} \times \kappa| = \kappa$ și $(\{0\} \times \kappa) \cap (\{1\} \times \kappa) = \emptyset$, deci

$$\kappa + \kappa = |(\{0\} \times \kappa) \cup (\{1\} \times \kappa)|,$$

dar $(\{0\} \times \kappa) \cup (\{1\} \times \kappa) = 2 \times \kappa$, deci

$$|(\{0\} \times \kappa) \cup (\{1\} \times \kappa)| = |2 \times \kappa| = |2| \cdot |\kappa| = 2 \cdot \kappa.$$

Corolar

Pentru orice cardinal κ cu $2 \leq \kappa$, avem $\kappa + \kappa \leq \kappa \cdot \kappa$.

Exponențierea cardinalilor

Pentru orice cardinali κ, λ, definim exponențierea lor astfel: alegem A și B cu $|A| = \kappa$ și $|B| = \lambda$ și punem

$$\kappa^\lambda := |A^B|.$$

Această definiție are sens fiindcă pentru orice A, B, A', B' cu $|A| = |A'|$ și $|B| = |B'|$, avem $\left|A^B\right| = \left|A'^{B'}\right|$.

Proprietăți imediate

Fie κ, κ', λ, μ cardinali. Atunci:

- dacă $0 < \lambda$, atunci $\kappa \leq \kappa^\lambda$;
- dacă $1 < \kappa$, atunci $\lambda \leq \kappa^\lambda$;
- dacă $\kappa \leq \kappa'$ și $\lambda \leq \mu$, atunci $\kappa^\lambda \leq \kappa'^\mu$;
- $\kappa \cdot \kappa = \kappa^2$.

Teoremă

Fie κ, λ, μ cardinali. Atunci:

- $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$;
- $(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$;
- $(\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$.

Demonstrație

Fie K, L, M cu $|K| = \kappa$, $|L| = \lambda$, $|M| = \mu$. Pentru primul punct, vom presupune $L \cap M = \emptyset$. Atunci formăm bijecția de la $K^L \times K^M$ la $K^{L \cup M}$ care duce orice pereche (f, g) în funcția h ce duce orice $x \in L \cup M$ în $f(x)$, dacă $x \in L$, respectiv în $g(x)$, dacă $x \in M$.

Pentru al doilea punct, formăm bijecția de la $K^{L \times M}$ la $(K^L)^M$ care duce orice f în funcția $m \mapsto (l \mapsto f(l, m))$. Pentru al treilea punct, formăm bijecția de la $K^M \times L^M$ la $(K \times L)^M$ care duce orice pereche (f, g) în funcția $m \mapsto (f(m), g(m))$.

Avem că pentru orice X, avem

$$|X| < |\mathcal{P}(X)| = \left|2^X\right| = |2|^{|X|} = 2^{|X|}.$$

Prin urmare, $\aleph_0 = |\mathbb{N}| < |\mathcal{P}(\mathbb{N})| = 2^{|\mathbb{N}|} = 2^{\aleph_0}$ și mai avem $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0}$. Fie n, m, $p \in \mathbb{N}$ cu $0 < m$ și $1 < p$. Avem următoarele inegalități:

$$2^{\aleph_0} \leq n + 2^{\aleph_0} \leq \aleph_0 + 2^{\aleph_0} \leq 2^{\aleph_0} + 2^{\aleph_0} = 2 \cdot 2^{\aleph_0} = 2^{\aleph_0 + 1} = 2^{\aleph_0}$$

$$2^{\aleph_0} \leq m \cdot 2^{\aleph_0} \leq \aleph_0 \cdot 2^{\aleph_0} \leq 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0}$$

$$2^{\aleph_0} \leq (2^{\aleph_0})^m \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0^2} = 2^{\aleph_0}$$

$$2^{\aleph_0} \leq p^{\aleph_0} \leq {\aleph_0}^{\aleph_0} \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0^2} = 2^{\aleph_0}$$

despre care se observă acum că sunt de fapt egalități, și deci orice cardinal ce apare în ele este egal cu $2^{\aleph_0}$.

Puterea continuumului

Acest cardinal $2^{\aleph_0}$ se notează cu $\mathfrak{c}$ și se numește **cardinalul continuumului** sau **puterea continuumului**.

Propoziție

- Pentru orice $n > 0$, $|\mathbb{R}^n| = \mathfrak{c}$.
- $|\mathbb{C}| = \mathfrak{c}$.
- $|\mathbb{N}^{\mathbb{N}}| = \mathfrak{c}$.
- $|\mathbb{R}^{\mathbb{N}}| = \mathfrak{c}$.

Diferența între continuum și numărabil

Teoremă

Fie A, B cu $A \subseteq B$, $|A| = \aleph_0$ și $|B| = \mathfrak{c}$. Atunci $|B \setminus A| = \mathfrak{c}$.

Demonstrație

Putem presupune $B = \mathbb{R}^2$ și e suficient să arătăm $\mathfrak{c} \leq |B \setminus A|$. Fie

$$P := \{x \in \mathbb{R} \mid \text{există } y \text{ cu } (x, y) \in A\}.$$

Definim funcția surjectivă $f : A \to P$, pentru orice $(x, y) \in A$, prin $f(x, y) := x$. Rezultă $|P| \leq \aleph_0$, deci există $z \in \mathbb{R} \setminus P$.

Definim funcția injectivă $g : \mathbb{R} \to B \setminus A$, pentru orice $y \in \mathbb{R}$, prin $g(y) := (z, y)$. Rezultă $\mathfrak{c} \leq |B \setminus A|$.

Corolar

$|\mathbb{R} \setminus \mathbb{Q}| = \mathfrak{c}$.

Ipoteza continuumului

Dat fiind că $\mathfrak{c}$ este un cardinal ubicuu în matematică, apare problema firească de a-i calibra mărimea. Cantor a formulat, fără însă a și demonstra, următorul enunț, pe care Hilbert l-a pus în fruntea listei sale de probleme pentru secolul XX:

Ipoteza continuumului

Nu există cardinal nenumărabil mai mic ca $\mathfrak{c}$.

Reamintim din Introducerea istorică că rezultatele lui Gödel (1940) și Cohen (1963) au arătat că acest enunț nu se poate nici infirma, respectiv nici confirma pornind de la axiomele ZFC (în ipoteza că acestea sunt consistente). Pentru această clarificare completă a chestiunii, Cohen a primit în 1966 medalia Fields.

Mulțimi mai mari decât $\mathfrak{c}$

Știm că $\mathfrak{c} < 2^{\mathfrak{c}}$ și avem că

$$2^{\mathfrak{c}} = 2^{2^{\aleph_0}} \leq \aleph_0^{2^{\aleph_0}} \leq \left(2^{\aleph_0}\right)^{2^{\aleph_0}} = 2^{\aleph_0 \cdot 2^{\aleph_0}} = 2^{2^{\aleph_0}} = 2^{\mathfrak{c}}.$$

Ca urmare, $|\mathbb{N}^{\mathbb{R}}| = \aleph_0^{2^{\aleph_0}} = 2^{\mathfrak{c}}$ și $|\mathbb{R}^{\mathbb{R}}| = \left(2^{\aleph_0}\right)^{2^{\aleph_0}} = 2^{\mathfrak{c}}$.

Numere infinite

Pentru a da înțeles acestor cardinali, va trebui, firește, să prelungim noțiunea de număr finit (natural) astfel încât să cuprindă și valori „infinite". Am văzut că cel mai mic cardinal infinit este $\mathbb{N}$, care a fost notat în acel context cu $\aleph_0$. În contextul care urmează, îl vom nota cu ω. Așadar,

$$\omega = \{0, 1, 2, \ldots\}.$$

Putem prelungi „numerele" dincolo de ω folosindu-ne de operația de succesor:

$$\omega^+ = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\}$$
$$\omega^{++} = \omega^+ \cup \{\omega^+\} = \{0, 1, 2, \ldots, \omega, \omega^+\}$$

iar mai apoi am vrea să ajungem și la ceva precum:

$$\omega + \omega := \{0, 1, 2, \ldots, \omega, \omega^+, \omega^{++}, \ldots\}$$

Ca la numerele naturale, va trebui să definim cumva unitar această clasă de obiecte (pe care le vom numi **ordinali**). Observăm că toate mulțimile de mai sus au o structură canonică de bună ordine, deci are sens să studiem întâi această noțiune mai în profunzime.

Mulțimi ordonate

Vom numi o relație de ordine strictă $<$ ca fiind de bună ordine dacă relația de ordine parțială asociată $\leq$ este în acel fel (distingând după context și notație la care ne referim). De asemenea, vom spune că o pereche (A, R) (notată deseori tot cu A) este o mulțime (parțial, strict, bine) ordonată dacă R este o relație de felul respectiv pe A.

Propoziție

Fie $(W, <)$ o mulțime bine ordonată și $S \subsetneq W$ astfel încât pentru orice $x \in W$, $y \in S$ cu $x < y$ avem $x \in S$. Atunci există $a \in W$ astfel încât $S = \{x \in W \mid x < a\} =: W[a]$.

Demonstrație

Fie $X := W \setminus S \neq \emptyset$. Fie a minimul lui X și arătăm că este cel cerut. Dacă $x \in S$ și $x \not< a$, atunci $a \leq x$ și deci $a \in S$, contradicție. Dacă $x < a$ și $x \notin S$, atunci $x \in X$, contradicție cu minimalitatea lui a.

Tot despre mulțimi bine ordonate

Propoziție

Fie $(W, <)$ o mulțime bine ordonată și $f : W \to W$ astfel încât pentru orice x_1, $x_2 \in W$ cu $x_1 < x_2$ avem $f(x_1) < f(x_2)$. Atunci pentru orice $x \in W$, $x \leq f(x)$.

Demonstrație

Presupunem că există x cu $x \not\leq f(x)$ și aleg a minim cu această proprietate. Așadar, $f(a) < a$ și rezultă $f(f(a)) < f(a)$, de unde rezultă că și $f(a)$ are proprietatea respectivă, contrazicând minimalitatea lui a.

Dacă (W_1, R) și (W_2, S) sunt mulțimi ordonate, un **izomorfism** între ele este o bijecție $f : W_1 \to W_2$ astfel încât pentru orice x_1, $x_2 \in W_1$, avem $x_1 R x_2$ dacă și numai dacă $f(x_1) S f(x_2)$ (deseori, vom nota pe R și pe S cu același simbol), caz în care spunem că cele două mulțimi ordonate sunt **izomorfe**.

Proprietăți legate de izomorfism

Propoziție

Fie $(W, <)$ și $(W', <)$ mulțimi bine ordonate.

- Fie $a \in W$. Atunci W nu e izomorfă cu $W[a]$.
- Fie $f : W \to W$ izomorfism (automorfism). Atunci $f = \mathrm{id}_W$.
- Există cel mult un izomorfism de la W la W'.

Demonstrație

- Presupunem că există $f : W \to W[a]$ izomorfism. Atunci $f(a) \in W[a]$, deci $f(a) < a$, contradicție cu propoziția anterioară.
- Fie $x \in W$. Aplicând propoziția anterioară pentru f și f^{-1}, rezultă că $x \leq f(x)$ și $x \leq f^{-1}(x)$. Din ultima avem $f(x) \leq x$, deci $x = f(x)$.
- Presupunem că am avea $f, g : W \to W'$ izomorfisme. Atunci $g^{-1} \circ f$ este automorfism al lui W, deci $g^{-1} \circ f = \mathrm{id}_W$, adică $f = g$.

Proprietatea fundamentală

Teoremă

Fie $(W_1, <)$ și $(W_2, <)$ mulțimi bine ordonate. Atunci se întâmplă exact unul din următoarele lucruri:

- W_1 și W_2 sunt izomorfe.
- Există $a \in W_2$ astfel încât W_1 este izomorf cu $W_2[a]$.
- Există $a \in W_1$ astfel încât W_2 este izomorf cu $W_1[a]$.

În plus, conform propoziției anterioare (din care rezultă și că posibilitățile sunt mutual exclusive), izomorfismul este unic.

Demonstrație

Notăm $R := \{(x, y) \in W_1 \times W_2 \mid W_1[x] \text{ este izomorf cu } W_2[y]\}$. Clar, din propoziția anterioară rezultă că R este grafic. Fie D domeniul său și E imaginea sa. Atunci $f := (D, E, R)$ va fi o surjecție. Faptul că este injectivă va rezulta analog faptului că R este grafic. Arătăm acum că f este izomorfismul cerut și că domeniul și codomeniul ei sunt cele posibile din enunț.

Proprietatea fundamentală

Demonstrație (cont.)

Fie x, $y \in D$, vrem $x < y \Leftrightarrow f(x) < f(y)$. Din simetria definiției lui R, e suficient să arătăm „$\Rightarrow$". Presupunem $x < y$. Știm că există un izomorfism între $W_1[x]$ și $W_2[f(x)]$, precum și între $W_1[y]$ și $W_2[f(y)]$, iar pe ultimul îl notăm cu h. Cum $x < y$, h induce un izomorfism între $W_1[x]$ și $W_2[h(x)]$. Deci $W_2[f(x)]$ și $W_2[h(x)]$ sunt izomorfe, prin urmare $f(x) = h(x) < f(y)$.

Din simetria enunțului, rămâne de arătat că dacă $D \neq W_1$, atunci există a cu $D = W_1[a]$ și $E = W_2$. Pentru primul punct, e suficient să arătăm (din prima propoziție) că pentru orice $x \in W_1$ și $y \in D$ cu $x < y$ avem $x \in D$. Ca mai înainte, avem un izomorfism h între $W_1[y]$ și $W_2[f(y)]$, care induce un izomorfism între $W_1[x]$ și $W_2[h(x)]$. Deci $(x, h(x)) \in R$ și deci $x \in D$.

Demonstrație (cont.)

Pentru al doilea punct, presupunem $E \neq W_2$ și, cu același raționament, avem că există $b \in W_2$ cu $E = W_2[b]$. Deci f este un izomorfism între $W_1[a]$ și $W_2[b]$, ca urmare $(a, b) \in R$, deci $a \in D$. Dar $D = W_1[a]$, deci $a < a$, contradicție!

Acum putem trece la definirea ordinalilor.

Mulțimi tranzitive și ordinali

Definiție

O mulțime T se numește **tranzitivă** dacă pentru orice $x \in T$, $x \subseteq T$ (altfel spus, pentru orice $x \in T$ și $y \in x$ avem $y \in T$, de unde denumirea de tranzitivă).

Pentru orice mulțime A, notăm $\in_A := \{(x, y) \in A \times A \mid x \in y\}$ (sau chiar cu $\in$ când va fi clar din context).

Definiție

O mulțime α se numește **ordinal** dacă α este tranzitivă și $(\alpha, \in_\alpha)$ este mulțime bine ordonată.

Ca exemple, orice număr natural este ordinal, și chiar $\mathbb{N}$ este.

Vom nota, așa cum am spus și mai devreme, cu ω pe $\mathbb{N}$ atunci când îl privim drept ordinal – așa cum l-am notat cu $\aleph_0$ atunci când îl priveam drept cardinal. Vom vedea mai târziu de ce folosim mai multe notații pentru același obiect.

Proprietățile ordinalilor

Următoarele proprietăți se vor demonstra la seminar:

Propoziție

- Dacă α este ordinal, atunci α^+ este ordinal.
- Dacă α este ordinal, atunci $\alpha \notin \alpha$.
- Dacă α este ordinal și $\beta \in \alpha$, β este ordinal.
- Dacă α și β sunt ordinali și $\alpha \subsetneq \beta$, atunci $\alpha \in \beta$.

Numim un ordinal de forma β^+ **ordinal succesor** (de exemplu ω^+). Un ordinal care nu este 0 sau succesor se numește **ordinal limită**. Ca la numere naturale, pentru orice ordinali α și β vom nota $\alpha < \beta$ pentru $\alpha \in \beta$ și, tot ca acolo, avem, pentru orice ordinali α și β, $\alpha \leq \beta$ dacă și numai dacă $\alpha \in \beta^+$. Mai avem și că orice ordinal este mulțimea celor mai mici decât el.

Relația de ordine pe ordinali

Următoarea propoziție ne spune că $<$ are proprietățile unei relații de ordine strictă pe ordinali astfel încât $\leq$ este totală.

Propoziție

Fie α, β, γ ordinali.

- Dacă $\alpha < \beta$ și $\beta < \gamma$, atunci $\alpha < \gamma$.
- Nu avem că $\alpha < \alpha$.
- Avem că $\alpha < \beta$ sau $\alpha = \beta$ sau $\beta < \alpha$.

Demonstrație

Primul punct rezultă din faptul că γ este tranzitivă, iar al doilea din propoziția anterioară. Pentru al treilea, ne folosim de faptul că $\alpha \cap \beta$ este ordinal (exercițiu!). Presupunem $\alpha \cap \beta \subsetneq \alpha$ și $\alpha \cap \beta \subsetneq \beta$. Atunci, din propoziția anterioară $\alpha \cap \beta \in \alpha$ și $\alpha \cap \beta \in \beta$, deci $\alpha \cap \beta \in \alpha \cap \beta$, contradicție cu propoziția anterioară. Deci $\alpha \cap \beta = \alpha$ sau $\alpha \cap \beta = \beta$, de unde $\alpha \subseteq \beta$ sau $\beta \subseteq \alpha$, așadar, $\alpha \in \beta$ sau $\alpha = \beta$ sau $\beta \in \alpha$.

Ordinalii în ansamblu

Teorema bunei ordonări

Fie P o proprietate și α un ordinal astfel încât $P(\alpha)$. Atunci există β astfel încât $P(\beta)$ și orice γ cu $P(\gamma)$ avem $\beta \leq \gamma$. În particular, orice mulțime nevidă ale cărei elemente sunt ordinali admite minim relativ la $<$. De aici rezultă că orice mulțime de ordinali este bine-ordonată de $<$.

Demonstrație

Fie $Y := \{\delta \in \alpha \mid P(\delta)\}$. Distingem două cazuri:
Cazul I. $Y = \emptyset$. Iau $\beta := \alpha$. Fie γ cu $P(\gamma)$. Presupunem $\alpha \not\leq \gamma$. Atunci $\gamma < \alpha$, deci $\gamma \in Y$, contradicție.
Cazul II. $Y \neq \emptyset$. Din faptul că α este bine ordonată, există minimul lui Y, notat cu β. Fie γ cu $P(\gamma)$. Atunci, ori $\gamma < \alpha$, deci $\gamma \in Y$ și deci $\beta \leq \gamma$, ori $\alpha \leq \gamma$, și cum $\beta < \alpha$, avem $\beta \leq \gamma$.

Supremum

Propoziție

Fie X o mulțime ale cărei elemente sunt ordinali. Notăm $\sup X := \bigcup X$. Atunci:

- $\sup X$ este ordinal; pentru orice $\alpha \in X$, $\alpha \leq \sup X$; pentru orice ordinal γ astfel încât pentru orice $\alpha \in X$ avem $\alpha \leq \gamma$, avem $\sup X \leq \gamma$;
- $(\sup X)^+ \notin X$, deci există $\alpha \notin X$.

Demonstrație

Primul punct este lăsat ca exercițiu. Pentru al doilea, presupunem $(\sup X)^+ \in X$. Atunci $(\sup X)^+ \subseteq \bigcup X$, deci $(\sup X)^+ \leq \sup X$. Avem așadar $(\sup X)^+ \in (\sup X)^+$, contradicție.

În particular, acest ultim punct ne arată că nu există mulțimea tuturor ordinalilor. Ca urmare, $<$ și $\leq$ nu denotă relații, ci doar pseudo-relații – echivalența demonstrată la seminar între $<$ și $\leq$ se păstrează, însă.

Alte fapte despre ordinali

Propoziție

Ordinalul ω este limită.

Demonstrație

Clar $\omega \neq 0$. Rămâne de arătat că nu este succesor. Presupunem că există α cu $\omega = \alpha^+ = \alpha \cup \{\alpha\}$. Atunci $\alpha \in \omega$, deci, din definiția lui ω (care este $\mathbb{N}$), avem $\alpha^+ \in \omega$, adică $\omega \in \omega$, contradicție.

Se mai observă și că orice ordinal finit este număr natural (exercițiu!).

Fie α, β ordinali. Observăm că dacă $\alpha \in \beta$, atunci $\alpha = \beta[\alpha]$. Așadar, dacă $\alpha \neq \beta$, atunci $(\alpha, \in_\alpha)$ și $(\beta, \in_\beta)$ nu sunt izomorfe ca mulțimi bine ordonate.

În continuare, vom demonstra că ordinalii formează un (pseudo!) sistem complet de reprezentanți pentru (pseudo!) relația de izomorfism între mulțimile bine ordonate.

Teoremă

Fie $(W, <)$ o mulțime bine ordonată. Atunci există un ordinal α astfel încât $(W, <)$ este izomorfă cu $(\alpha, \in_\alpha)$.

Demonstrație

Notăm $T := \{a \in W \mid \text{există un ordinal izomorf cu } W[a]\}$. Vom presupune (și vom justifica mai târziu) că avem o mulțime α ce conține exact acei ordinali izomorfi cu un $W[a]$. Se arată că α este ordinal (exercițiu!) și că pentru orice $a \in T$ și $b \in W$ cu $b < a$ avem $b \in T$ (exercițiu!). Rezultă că $T = W$ sau există $c \in W$ cu $T = W[c]$.

Definim $f : T \to \alpha$, punând pentru orice $a \in T$, $f(a)$ (unic determinat!) astfel încât $f(a)$ este izomorf cu $W[a]$. Atunci f este izomorfism (exercițiu!). Dacă există $c \in W$ cu $T = W[c]$, avem că $c \in T$ și deci $c < c$, contradicție. Așadar $T = W$ și f este izomorfismul căutat.

Justificarea lui α

Rămâne întrebarea: de ce există mulțimea α? Observăm că ea ar putea fi scrisă intuitiv ca

$$\alpha = \{\beta(a) \mid a \in T\}.$$

Abstractizând, ajungem la forma

$$\{F(x) \mid x \in A\},$$

întâlnită uneori în matematică, dar necuprinsă în tiparul Axiomei comprehensiunii.

Dacă F ar fi o funcție, atunci acea mulțime ar fi pur și simplu imaginea ei, dar în exemple ca al nostru, avem de-a face cu „operații" despre care nu știm (și posibil nici nu este adevărat) că pot fi reprezentate prin funcții.

Ca urmare, dacă avem P o proprietate (ca și la Axioma comprehensiunii, sensul exact al cuvântului va putea fi deslușit abia când se va introduce logica de ordinul I) ce are două argumente și pentru orice x există și este unic y cu $P(x, y)$, putem spune că ea denotă o operație F și vom nota acel y cu $F(x)$. În acest moment, putem enunța o nouă axiomă.

Axioma înlocuirii

Pentru orice operație F și orice mulțime A există o mulțime B astfel încât pentru orice $x \in A$, $F(x) \in B$.

Din nou, ca și la alte axiome (a perechii, a reuniunii, a mulțimii părților), putem forma cu ajutorul Axiomei comprehensiunii mulțimea ce conține **exact** acei $F(x)$ cu $x \in A$, pe care o notăm, cum am sugerat mai devreme, cu $\{F(x) \mid x \in A\}$.

Existența lui α

Ca urmare, dacă definesc operația G, pentru orice mulțime a, prin

$$G(a) := \begin{cases} \text{acel ordinal } \beta \text{ izomorf cu } W[a], & \text{dacă } a \in T; \\ \emptyset, & \text{altfel.} \end{cases}$$

atunci vom avea

$$\alpha = \{G(a) \mid a \in T\}.$$

Inducție pe ordinali

Ca și la numere naturale, putem formula un principiu al inducției pentru ordinali.

Principiul inducției pentru ordinali

Fie P o proprietate și presupunem că pentru orice ordinal α avem că dacă pentru orice $\beta < \alpha$, $P(\beta)$, atunci $P(\alpha)$. Atunci pentru orice ordinal α avem $P(\alpha)$.

Demonstrație

Fie proprietatea Q, definită, pentru orice x, prin $Q(x)$ dacă și numai dacă nu avem $P(x)$. Presupunem că există γ astfel încât nu avem $P(\gamma)$, deci avem $Q(\gamma)$. Din Teorema bunei ordonări, există β cu $Q(\beta)$ – deci nu avem $P(\beta)$ – și pentru orice γ cu $Q(\gamma)$, avem $\beta \leq \gamma$. Altfel spus, pentru orice $\gamma < \beta$, nu avem $Q(\gamma)$, deci avem $P(\gamma)$. Aplicând ipoteza teoremei, rezultă $P(\beta)$. Contradicție!

Forma a doua a inducției

Exploatând împărțirea ordinalilor în zero, succesor și limită, putem da următoarea variantă a principiului inducției.

Principiul inducției pentru ordinali, forma a doua

Fie P o proprietate și presupunem că:

- $P(0)$;
- pentru orice α ordinal cu $P(\alpha)$, avem $P(\alpha^+)$;
- pentru orice α ordinal limită astfel încât pentru orice $\beta < \alpha$, $P(\beta)$, avem $P(\alpha)$.

Atunci pentru orice ordinal α avem $P(\alpha)$.

Observăm că această a doua formă corespunde inducției obișnuite pe numerele naturale, în vreme ce prima corespundea mai degrabă principiului inducției complete.

Recursie pe ordinali

Tot analog numerelor naturale, putem formula o teoremă a recursiei pentru ordinali.

Teorema recursiei pentru ordinali

Fie G o operație. Atunci pentru orice ordinal α există și este unic y astfel încât există o funcție t ce are domeniul α^+ astfel încât pentru orice $\beta \leq \alpha$, $t(\beta) = G(t_{|\beta})$ și $y = t(\alpha)$.

Practic, pentru orice operație G, am definit o operație F astfel încât pentru orice ordinal α, $F(\alpha) = G(F_{|\alpha})$.

Demonstrația teoremei (care depășește cadrul cursului) se face extinzând oarecum ideile demonstrației teoremei recursiei pentru numere naturale. De asemenea, există o formă parametrică a ei pe care o vom folosi în scurt timp pentru a defini, ca și în cazul numerelor, operații pe ordinali.

Forma a doua a recursiei

Și teorema recursiei are o a doua formă ce permite definirea recursivă a operațiilor după tipul ordinalului curent.

Teorema recursiei pentru ordinali, forma a doua

Fie G_1, G_2, G_3 operații. Atunci pentru orice ordinal α există și este unic y astfel încât există o funcție t ce are domeniul α^+ astfel încât pentru orice $\beta \leq \alpha$:

- dacă $\beta = 0$, $t(\beta) = G_1(0)$,
- dacă există δ cu $\beta = \delta^+$, $t(\beta) = G_2(t(\delta))$,
- dacă β este limită, $t(\beta) = G_3(t_{|\beta})$,

iar $y = t(\alpha)$.

Aici, pentru orice operații G_1, G_2, G_3, am definit o operație F astfel încât (intuitiv vorbind):

- $F(0) = G_1(0)$;
- pentru orice ordinal α, $F(\alpha^+) = G_2(F(\alpha))$;
- pentru orice ordinal limită α, $F(\alpha) = G_3(F_{|\alpha})$.

Adunarea ordinalilor

Acum că avem la dispoziție recursia (menționăm în treacăt că și forma a doua admite o variantă parametrizată), putem defini adunarea ordinalilor, adică pentru orice ordinali α și β, punem:

- $\alpha + 0 := \alpha$;
- $\alpha + \beta^+ := (\alpha + \beta)^+$;
- dacă β este ordinal limită, $\alpha + \beta := \sup\{\alpha + \gamma \mid \gamma < \beta\}$.

Avertisment

Din ce am văzut până acum, atât 1 cât și $\mathbb{N}$ sunt și ordinali, și cardinali (anticipând puțin lucrurile, vom vedea peste nu mult timp că orice cardinal este ordinal). Dacă îi adunăm în ipostaza de cardinali, obținem

$$\mathbb{N} + 1 = |\mathbb{N} \cup \{\mathbb{N}\}| = |\mathbb{N}| = \mathbb{N},$$

iar dacă îi adunăm în ipostaza de ordinali, obținem

$$\mathbb{N} + 1 = \mathbb{N} + 0^+ = (\mathbb{N} + 0)^+ = \mathbb{N}^+ = \mathbb{N} \cup \{\mathbb{N}\},$$

deci cele două adunări nu coincid. Aceasta justifică cele două notații pentru $\mathbb{N}$, anume $\aleph_0$ și ω. Mai mult, dacă efectuăm următoarea adunare de ordinali:

$$1 + \mathbb{N} = \sup\{1 + n \mid n \in \mathbb{N}\} = \sup\{n^+ \mid n \in \mathbb{N}\} = \mathbb{N},$$

(faptul că pentru orice $n \in \mathbb{N}$, $1 + n = n^+$ se arată prin inducție), observăm că adunarea ordinalilor nici nu este comutativă. Subliniem că nu vom insista prea mult pe operațiile acestea pe ordinali, ele fiind prezentate mai mult cu titlu informativ.

Înmulțirea și exponențierea ordinalilor

Putem defini mai apoi, tot recursiv, înmulțirea și exponențierea ordinalilor, folosindu-ne de următoarele formule:

- $\alpha \cdot 0 := 0$;
- $\alpha \cdot \beta^+ := (\alpha \cdot \beta) + \alpha$;
- dacă β este ordinal limită, $\alpha \cdot \beta := \sup\{\alpha \cdot \gamma \mid \gamma < \beta\}$;
- $\alpha^0 := 1$;
- $\alpha^{\beta^+} := \alpha^\beta \cdot \alpha$;
- dacă β este ordinal limită, $\alpha^\beta := \sup\{\alpha^\gamma \mid \gamma < \beta\}$.

Mai departe, dacă punem $\omega_1 := \omega$ și pentru orice $n \in \mathbb{N}$, $\omega_{n^+} := \omega^{\omega_n}$, putem defini

$$\varepsilon_0 := \sup\{\omega_n \mid n \geq 1\} = \sup\left\{\omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \ldots\right\}.$$

Acest ε_0 este cel care a fost pomenit în Introducerea istorică în conjuncție cu demonstrația de consistență a lui Gentzen.

Ordinali inițiali

Am spus că orice cardinal va fi ordinal. Prin urmare, definim cardinalii ca fiind o clasă anume de ordinali.

Definiție

Un ordinal se numește **inițial** dacă nu este echipotent cu un ordinal mai mic ca el.

Ca exemple, putem da orice număr natural, dar și pe ω. Ordinalul ω^+ nu este inițial, dat fiind că este echipotent cu ω. În general, pentru orice ordinal infinit α, avem $\omega \subseteq \alpha$ și deci putem defini bijecția $f : \alpha^+ \to \alpha$, pentru orice $\beta \in \alpha^+$, prin

$$f(\beta) := \begin{cases} \beta^+, & \text{dacă } \beta \text{ este finit,} \\ \beta, & \text{dacă } \omega \leq \beta < \alpha, \\ 0, & \text{dacă } \beta = \alpha. \end{cases}$$

și ca urmare α^+ nu este inițial. Mai menționăm faptul imediat că doi ordinali inițiali diferiți nu pot fi echipotenți.

Mulțimi bine-ordonabile

Definiție

O mulțime se numește bine-ordonabilă dacă există o relație de bună ordine pe ea.

Teoremă

Pentru orice mulțime bine-ordonabilă există și este unic un ordinal inițial echipotent cu ea.

Demonstrație

Unicitatea este imediată. Pentru existență, fie X mulțimea și fie $<$ o relație de bună ordine pe ea. Am arătat că există un ordinal α astfel încât $(X, <)$ este izomorfă cu $(\alpha, \in_\alpha)$. În particular, X este echipotentă cu α. Ca urmare, există un cel mai mic ordinal echipotent cu X, iar acesta trebuie neapărat să fie inițial.

Mai mult, remarcăm că orice mulțime echipotentă cu un ordinal trebuie să fie bine-ordonabilă.

Cardinali

Pentru mulțimile bine-ordonabile, le putem defini, deci, cardinalul ca fiind acel ordinal inițial corespunzător. Vom vedea mai târziu că toate mulțimile sunt bine-ordonabile, deci această definiție este suficientă: cardinalii sunt, prin urmare, exact ordinalii inițiali. Deocamdată, însă, să observăm că, în această ipoteză, presupunerile pe care le-am făcut rezultă imediat din definiție. Le reamintim aici:

- pentru orice $n \in \mathbb{N}$ și orice X, avem că dacă $X \sim n$, $|X| = n$;
- pentru orice X, dacă $X \sim \mathbb{N}$, $|X| = \mathbb{N}$;
- pentru orice X, $X \sim |X|$;
- pentru orice cardinal κ, $|\kappa| = \kappa$;
- pentru orice X și Y, avem $X \sim Y$ dacă și numai dacă $|X| = |Y|$.

Observăm și că pentru orice ordinal α, $|\alpha| \leq \alpha$.

Ordonarea cardinalilor

Mai mult, avem că (pseudo!) relația de ordine definită pe cardinali atunci când nu le cunoșteam natura coincide cu cea indusă de cea pe ordinali. O consecință va fi faptul promis că ordonarea cardinalilor este totală.

Mai exact, dacă κ și λ sunt cardinali astfel încât $\kappa \leq \lambda$ drept ordinali, atunci $\kappa \subseteq \lambda$ și deci $\kappa \leq \lambda$ drept cardinali.

Presupunem acum că avem $\kappa \leq \lambda$ drept cardinali și $\kappa \not\leq \lambda$ drept ordinali. Atunci $\lambda < \kappa$, și deci $\lambda \leq \kappa$ drept ordinali, iar din paragraful anterior avem $\lambda \leq \kappa$ drept cardinali, deci $\lambda = \kappa$, contradicție cu $\kappa \neq \lambda$.

Am văzut că ordinalii finiți, și deci și cardinalii finiți, sunt exact numerele naturale. În continuare vom vedea cum arată cardinalii infiniți.

Ordinali Hartogs

Propoziție-Definiție

Pentru orice mulțime A există un ordinal α cu proprietatea că nu este echipotent cu nicio submulțime a lui A. Prin urmare, există un ordinal minim cu această proprietate, ce este evident inițial. Îl numim **ordinalul Hartogs** al lui A și îl notăm cu $h(A)$. Așadar, $h(A)$ este cel mai mic ordinal α cu proprietatea că nu există injecție de la el la A.

Demonstrație

Clar, pentru orice $B \subseteq A$ și orice relație de bună ordine R pe B, avem $R \subseteq B \times B \subseteq A \times A$ și $B = \bigcup\bigcup R$. Notăm cu C mulțimea tuturor acelor $R \in \mathcal{P}(A \times A)$ cu proprietatea că există $B \subseteq A$ astfel încât R este relație de bună ordine pe B. Atunci pentru orice $R \in C$ există și este unic un ordinal α astfel încât el este izomorf ca mulțime bine ordonată cu $(\bigcup\bigcup R, R)$.

Ordinali Hartogs

Demonstrație (cont.)

Folosind Axioma înlocuirii, formăm H ca fiind mulțimea tuturor acelor ordinali, iar dintr-o propoziție anterioară, avem că există $\alpha \notin H$. Demonstrăm acum că α este cel căutat. Presupunem că el ar fi echipotent cu o submulțime a lui A, deci că există $B \subseteq A$ și $f : B \to \alpha$ o bijecție. Atunci pot construi o relație de bună ordine pe B punând pentru orice x, $y \in B$, $x < y$ dacă și numai dacă $f(x) \in f(y)$. Rezultă că $(B, <)$ este izomorf cu $(\alpha, \in_\alpha)$ și deci $\alpha \in H$, contradicție cu modul cum a fost ales α.

Acel indice 0 din $\aleph_0$ sugerează că el este parte dintr-un șir mai lung. Vom defini acum acel șir, în mod recursiv, punând pentru orice ordinal α,

$$\aleph_{\alpha^+} := h(\aleph_\alpha)$$

și pentru orice ordinal limită α,

$$\aleph_\alpha := \sup\{\aleph_\beta \mid \beta < \alpha\}.$$

Conform definiției ordinalului Hartogs, avem că pentru orice ordinal α, $|\aleph_\alpha| < |\aleph_{\alpha^+}|$. Așadar, pentru orice ordinali α, β cu $\alpha < \beta$, avem $|\aleph_\alpha| < |\aleph_\beta|$.

Orice alef este cardinal infinit

Propoziție

- Pentru orice ordinal α, $\aleph_\alpha$ este ordinal inițial infinit.
- Pentru orice ordinal α, $\alpha \leq \aleph_\alpha$.

Demonstrație

- Vom demonstra prin inducție după α. Singurul caz netrivial este atunci când α este ordinal limită. Presupunem că $\aleph_\alpha$ nu e inițial, deci există $\gamma < \aleph_\alpha$ cu $|\aleph_\alpha| = |\gamma|$. Din definiția supremumului, există $\beta < \alpha$ cu $\gamma < \aleph_\beta$, deci $|\aleph_\alpha| = |\gamma| \leq |\aleph_\beta|$, contradicție cu $|\aleph_\beta| < |\aleph_\alpha|$.
- Exercițiu.

Așadar, pentru orice ordinal α, avem $|\aleph_\alpha| = \aleph_\alpha$.

Orice cardinal infinit este alef

Propoziție

Pentru orice ordinal γ și orice $\beta < \aleph_\gamma$ ordinal inițial infinit, există $\alpha < \gamma$ cu $\beta = \aleph_\alpha$.

Demonstrație

Demonstrăm prin inducție după γ. Pentru $\gamma = 0$, enunțul este trivial (dar aici folosim faptul că β este infinit!).

Presupunem acum că există δ cu $\gamma = \delta^+$. Atunci $\beta < \aleph_\gamma = \aleph_{\delta^+} = h(\aleph_\delta)$, deci $|\beta| \leq |\aleph_\delta|$, i.e. $\beta \leq \aleph_\delta$. Dacă $\beta < \aleph_\delta$, din ipoteza de inducție există $\alpha < \delta < \gamma$ cu $\beta = \aleph_\alpha$. Dacă $\beta = \aleph_\delta$, atunci luăm $\alpha := \delta$.

Presupunem acum că γ este limită. Avem $\beta < \aleph_\gamma = \sup\{\aleph_\delta \mid \delta < \gamma\}$, deci există $\delta < \gamma$ cu $\beta < \aleph_\delta$, deci din ipoteza de inducție există $\alpha < \delta < \gamma$ cu $\beta = \aleph_\alpha$.

Orice cardinal infinit este alef

Corolar

Pentru orice ordinal inițial infinit β, există un ordinal α cu $\beta = \aleph_\alpha$.

Demonstrație

Notăm $\gamma := \beta^+$. Atunci $\beta \leq \aleph_\beta < \aleph_{\beta^+} = \aleph_\gamma$ și pot aplica deci propoziția anterioară.

Dat fiind că orice cardinal este ori finit, ori infinit, am demonstrat așadar că orice cardinal este ori un număr natural, ori un alef.

Așadar, mai este nevoie să demonstrăm doar că orice mulțime este bine-ordonabilă. Pentru aceasta, vom avea nevoie de o nouă axiomă.

Propoziție

Următoarele enunțuri sunt echivalente:

- Pentru orice S cu $\emptyset \notin S$ există $(g_y)_{y \in S}$ astfel încât pentru orice $y \in S$, $g_y \in y$.
- Pentru orice I și orice familie de mulțimi **nevide** indexată după I, $(F_i)_{i \in I}$, avem că $\prod_{i \in I} F_i \neq \emptyset$, i.e. există $(f_i)_{i \in I}$ astfel încât pentru orice $i \in I$, $f_i \in F_i$.
- Pentru orice I și orice familie de mulțimi **nevide**, **disjuncte două câte două**, indexată după I, $(D_i)_{i \in I}$, avem că $\prod_{i \in I} D_i \neq \emptyset$, i.e. există $(d_i)_{i \in I}$ astfel încât pentru orice $i \in I$, $d_i \in D_i$.

Oricare dintre cele trei enunțuri de mai sus este cunoscut ca **Axioma alegerii**. În continuare, le vom demonstra echivalența.

Arătăm întâi echivalența dintre prima și a doua formă.

Pentru a demonstra că primul enunț îl implică pe al doilea, notăm $S := \{F_i \mid i \in I\}$ și obținem că există $(g_y)_{y \in S}$ astfel încât pentru orice $y \in S$, $g_y \in y$. Pentru orice $i \in I$, cum $F_i \in S$, notăm $f_i := g_{F_i}$. Atunci familia $(f_i)_{i \in I}$ este cea căutată, deoarece pentru orice $i \in I$, avem $f_i = g_{F_i} \in F_i$.

Invers, acum! Presupunem că avem S și notăm $F := \{(i, i) \mid i \in S\}$. Atunci F este o familie indexată după S și pentru orice $i \in S$, $F_i = i$. Ca urmare, există $(f_y)_{y \in S}$ astfel încât pentru orice $y \in S$, $f_y \in F_y = y$ și am terminat.

Mulțimi disjuncte

Rămâne de demonstrat că al treilea enunț îl implică pe al doilea.

Pentru orice $i \in I$ punem $D_i := \{i\} \times F_i$. Atunci familia $(D_i)_{i \in I}$ satisface condițiile din al treilea enunț, deci există $(d_i)_{i \in I}$ astfel încât pentru orice $i \in I$, $d_i \in D_i$.

Avem că pentru orice $i \in I$ există și este unic $a \in F_i$ cu $d_i = (i, a)$ – unicitatea este imediată, iar existența rezultă din faptul că pentru orice $i \in I$, $d_i \in D_i = \{i\} \times F_i$.

Punem, pentru orice $i \in I$, f_i să fie acel $a \in F_i$ cu $d_i = (i, a)$. Atunci familia $(f_i)_{i \in I}$ este cea căutată.

Lema lui Zorn

Axioma alegerii ne permite să demonstrăm un rezultat util în matematică, anume Lema lui Zorn.

Definiție

Fie $(A, \leq)$ o mulțime ordonată și $B \subseteq A$. B se numește **lanț** al lui A dacă pentru orice $x, y \in B$, avem $x \leq y$ sau $y \leq x$.

Definiție

Fie $(A, \leq)$ o mulțime ordonată. Ea se numește **inductiv ordonată** dacă orice lanț al său admite majorant, i.e. pentru orice $B \subseteq A$ care este lanț, există $z \in A$ astfel încât pentru orice $x \in B$, $x \leq z$. (Observăm că dacă aplicăm condiția pentru $B := \emptyset$, obținem $A \neq \emptyset$.)

Lema lui Zorn

Orice mulțime inductiv ordonată admite un element maximal.

Presupunem prin absurd că există o mulțime inductiv ordonată $(A, \leq)$ fără element maximal. Facem observația că pentru orice lanț $B \subseteq A$ există $z \in A$ astfel încât pentru orice $y \in B$ avem $y \leq z$, iar, cum z nu e maximal, există x cu $z < x$, deci, pentru orice $y \in B$, avem $y < x$.

Aplicăm Axioma alegerii pentru mulțimea $I := \mathcal{P}(A) \setminus \{\emptyset\}$ și obținem o familie $(g_i)_{i \in I}$ astfel încât pentru orice $i \in I$, $g_i \in i$. Fie $b \notin A$ și vom defini o operație pe ordinali F prin recursie. Fie α un ordinal. Presupunem că am definit, pentru orice $\gamma < \alpha$, $F(\gamma)$ și definim $F(\alpha)$.

În cazul în care, pentru orice $\gamma < \alpha$, $F(\gamma) \in A$ și există $x \in A$ astfel încât pentru orice $\gamma < \alpha$, $F(\gamma) < x$, punem

$$F(\alpha) := g_{\{x \in A \mid \text{pentru orice } \gamma < \alpha,\ F(\gamma) < x\}},$$

altfel punem $F(\alpha) := b$.

Demonstrația lemei lui Zorn

Demonstrăm acum prin inducție că, pentru orice ordinal α, $F(\alpha) \in A$ și pentru orice $\beta < \alpha$, $F(\beta) < F(\alpha)$. Presupunem enunțul adevărat pentru orice $\gamma < \alpha$ și demonstrăm pentru α. Fie

$$L := \{F(\gamma) \mid \gamma < \alpha\} \subseteq A.$$

Atunci, pentru orice β, δ cu $\beta < \delta < \alpha$, din ipoteza de inducție avem că $F(\beta)$, $F(\delta) \in A$ și $F(\beta) < F(\delta)$. Deci L este lanț și așadar există x astfel încât pentru orice $\gamma < \alpha$, $F(\gamma) < x$. Atunci, din definiția lui F, $F(\alpha)$ este un asemenea x și am încheiat.

Wikipedia: *"This sequence is **really long**."*

Definim acum $f : h(A) \to A$, pentru orice $\alpha \in h(A)$, prin $f(\alpha) := F(\alpha)$. Atunci f este injectivă și deci $|h(A)| \leq |A|$, ceea ce contrazice definiția ordinalului Hartogs.

Teorema lui Zermelo

În acest moment, putem arăta enunțul dorit.

Teorema bunei ordonări (Zermelo)

Orice mulțime este bine-ordonabilă.

Demonstrația teoremei lui Zermelo

Fie X o mulțime. Observăm că pentru orice $A \subseteq X$ și orice $R \subseteq A \times A$, avem $(A, R) \in \mathcal{P}(X) \times \mathcal{P}(X \times X)$, deci pot defini

$$W := \{(A, R) \mid A \subseteq X \text{ și } R \text{ este o relație de bună ordine pe } A\}.$$

Pe W definesc următoarea relație de ordine: pentru orice (A, R), $(B, S) \in W$, avem $(A, R) \leq (B, S)$ dacă $A \subseteq B$ și $R = S \cap (A \times A)$.

Fie $L \subseteq W$ un lanț. Notăm

$$M := \{A \subseteq X \mid \text{există } R \text{ cu } (A, R) \in L\}$$

și

$$N := \{R \subseteq X \times X \mid \text{există } A \text{ cu } (A, R) \in L\}.$$

Atunci $(\bigcup M, \bigcup N) \in W$ și este majorant pentru L (exercițiu!). Deci $(W, \leq)$ este inductiv ordonată și, deci, aplicând Lema lui Zorn, admite un element maximal pe care îl notăm cu (A, R).

Vrem să arătăm că $A = X$ și atunci R va fi relația de bună ordine cerută.

Dacă $A \neq X$, există $a \in X \setminus A$. Atunci avem că

$$(A \cup \{a\}, R \cup \{(y, a) \mid y \in A\} \cup \{(a, a)\}) \in W$$

(exercițiu!), ceea ce contrazice maximalitatea lui (A, R). Demonstrația este deci încheiată.

Acest mod de aplicare a Lemei lui Zorn este tipic.

Mai mult, dacă admitem Teorema lui Zermelo, putem demonstra Axioma alegerii în felul următor. Fie S cu $\emptyset \notin S$. Fie $\leq$ o relație de bună ordine pe $\bigcup S$. Știm că pentru orice $y \in S$, avem $y \subseteq \bigcup S$. Definim atunci $(g_y)_{y \in S}$, punând, pentru orice $y \in S$, $g_y := \min(y) \in y$.

Prin urmare, am arătat că Axioma alegerii, Lema lui Zorn și Teorema bunei ordonări sunt enunțuri echivalente.

Jerry Bona: *"The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?"*

Inverse la dreapta

La seminar se va demonstra că și următorul enunț este echivalent cu Axioma alegerii.

Propoziție

Fie X, Y mulțimi și $g : Y \to X$ surjectivă. Atunci există $f : X \to Y$ cu $g \circ f = \mathrm{id}_X$.

Funcția f se numește **inversa la dreapta** a lui g și se observă (exercițiu!) că este injectivă, deci $|X| \leq |Y|$.

Există și următorul enunț mai slab.

Principiul Partiției

Fie X, Y mulțimi și $g : Y \to X$ surjectivă. Atunci există $f : X \to Y$ injectivă.

Problemă deschisă (Levy, 1963): Este acest enunț echivalent cu Axioma alegerii sau este **strict** mai slab?

Înapoi la cardinali

Prin urmare, Axioma alegerii ne permite să folosim fără probleme definiția cardinalilor ca ordinali inițiali. În particular, ordonarea cardinalilor este totală, iar pentru orice mulțime infinită A există un ordinal α cu $|A| = \aleph_\alpha$.

Propoziție

Orice mulțime infinită admite o submulțime numărabilă.

Demonstrație

Fie A o mulțime infinită și α astfel încât există o bijecție $g : \aleph_\alpha \to A$. Cum $\aleph_0 \leq \aleph_\alpha$, există o injecție $f : \aleph_0 \to \aleph_\alpha$. Fie B imaginea lui $g \circ f$. Atunci B este submulțimea căutată.

Faptul demonstrat că $\aleph_0 < 2^{\aleph_0}$ se poate reformula acum ca $\aleph_1 \leq 2^{\aleph_0}$. De asemenea, ipoteza continuumului se poate reformula ca

$$2^{\aleph_0} = \aleph_1.$$

Cardinalul reuniunii

Propoziție

Fie I o mulțime și λ un cardinal. Fie $(A_i)_{i\in I}$ astfel încât, pentru orice $i \in I$, $|A_i| \leq \lambda$. Atunci

$$\left|\bigcup_{i\in I} A_i\right| \leq |I| \cdot \lambda.$$

Demonstrație

Pentru orice $i \in I$, există $g : A_i \to \lambda$ injectivă și deci mulțimea $S_i := \{g : A_i \to \lambda \mid g \text{ injectivă}\}$ este nevidă. Aplicăm Axioma alegerii pentru $(S_i)_{i\in I}$ și obținem o familie $(s_i)_{i\in I}$ astfel încât pentru orice $i \in I$, s_i este o injecție de la A_i la λ. (Acesta este un mod tipic de aplicare a Axiomei alegerii pentru a face un număr potențial infinit de alegeri.)

Demonstrație (cont.)

Fie $\leq$ o relație de bună ordine pe I. Definim o funcție $f : \bigcup_{i\in I} A_i \to I$, pentru orice $a \in \bigcup_{i\in I} A_i$, astfel: știm că $\{i \in I \mid a \in A_i\} \neq \emptyset$ și atunci punem

$$f(a) := \min(\{i \in I \mid a \in A_i\}).$$

Definim apoi $h : \bigcup_{i\in I} A_i \to I \times \lambda$, pentru orice $a \in \bigcup_{i\in I} A_i$, prin

$$h(a) := (f(a), s_{f(a)}(a)).$$

Atunci h este injectivă (exercițiu!) și deci

$$\left|\bigcup_{i\in I} A_i\right| \leq |I \times \lambda| = |I| \cdot |\lambda| = |I| \cdot \lambda.$$

Cardinalul reuniunii cel mult numărabile

Corolar

O reuniune cel mult numărabilă de mulțimi cel mult numărabile este cel mult numărabilă.

Demonstrație

Din propoziția anterioară, cardinalul reuniunii trebuie să fie cel mult $\aleph_0 \cdot \aleph_0 = |\mathbb{N} \times \mathbb{N}| = \aleph_0$.

Corolar

O reuniune numărabilă de mulțimi numărabile este numărabilă.

Demonstrație

Reuniunea conține o mulțime numărabilă și este deci infinită.

Are sens, deci, să studiem mai mult cum arată produsele de cardinali.

Propoziție

Pentru orice cardinal infinit κ, avem $\kappa \cdot \kappa = \kappa$.

Demonstrație

Presupunem contrariul, și deci există un κ **minim** cu $\kappa \cdot \kappa \neq \kappa$. Cum $\kappa = \kappa \cdot 1 \leq \kappa \cdot \kappa$, avem $\kappa < \kappa \cdot \kappa$. Pe mulțimea $\kappa \times \kappa$ definim relația R astfel: pentru orice α, β, γ, $\delta \in \kappa$, avem

$$\begin{aligned}(\alpha, \beta) R (\gamma, \delta) :\Leftrightarrow\ & \max(\alpha, \beta) < \max(\gamma, \delta) \\ & \text{SAU } \max(\alpha, \beta) = \max(\gamma, \delta) \text{ și } \alpha < \gamma \\ & \text{SAU } \max(\alpha, \beta) = \max(\gamma, \delta) \text{ și } \alpha = \gamma \text{ și } \beta < \delta.\end{aligned}$$

Avem că R este o relație de bună ordine strictă (exercițiu!). Deci există α astfel încât $(\kappa \times \kappa, R)$ este izomorfă cu $(\alpha, \in_\alpha)$ și fie f un izomorfism.

Demonstrație (cont.)

Atunci

$$\kappa < \kappa \cdot \kappa = |\kappa \times \kappa| = |\alpha| \leq \alpha,$$

deci $\kappa \in \alpha$ și prin urmare există β, $\gamma \in \kappa$ cu $f(\beta, \gamma) = \kappa$. Avem că mulțimea tuturor acelor (δ, ε) cu $(\delta, \varepsilon) R (\beta, \gamma)$ este de cardinal κ.

Avem că $\max(\beta, \gamma) < \kappa$ și deci $\varphi := \max(\beta, \gamma)^+ \leq \kappa$. Însă κ este inițial, deci nu e succesor, prin urmare $\varphi < \kappa$. Cum pentru orice δ, ε cu $(\delta, \varepsilon) R (\beta, \gamma)$, avem $\max(\delta, \varepsilon) \leq \max(\beta, \gamma) < \varphi$ și deci δ, $\varepsilon < \varphi$, avem

$$\kappa \leq |\varphi \times \varphi| = |\varphi| \cdot |\varphi|.$$

Dar cum avem $|\varphi| \leq \varphi < \kappa$, atunci, dacă $|\varphi|$ este finit, avem că $|\varphi| \cdot |\varphi|$ este tot finit, iar dacă $|\varphi|$ este infinit, avem, din minimalitatea lui κ, că $|\varphi| \cdot |\varphi| = |\varphi|$. În ambele cazuri, avem $|\varphi| \cdot |\varphi| < \kappa$. Contradicție!

Corolar

Fie κ un cardinal infinit și $n \in \mathbb{N}$, $n \neq 0$. Atunci $\kappa^n = \kappa$.

Corolar

Fie λ, μ cardinali cu $\lambda \leq \mu$ și μ infinit. Atunci $\lambda + \mu = \mu$.

Demonstrație

Avem $\mu \leq \lambda + \mu \leq \mu + \mu = 2 \cdot \mu \leq \mu \cdot \mu = \mu$.

Corolar

Fie λ, μ cardinali cu $1 \leq \lambda \leq \mu$ și μ infinit. Atunci $\lambda \cdot \mu = \mu$.

Demonstrație

Avem $\mu = 1 \cdot \mu \leq \lambda \cdot \mu \leq \mu \cdot \mu = \mu$.

Propoziție

Fie X infinită. Atunci există $Y \subsetneq X$ cu $X \sim Y$.

Demonstrație

Avem că $X \sim |X| \sim |X|^+$. Fie $g : |X|^+ \to X$ o bijecție. Luăm Y să fie imaginea lui $|X|$ prin g.

Așadar, o mulțime este infinită dacă și numai dacă este în bijecție cu o parte strictă a sa.

Părți finite

Pentru orice $n \in \mathbb{N}$ și X, definim $\mathcal{P}_n(X) := \{A \in \mathcal{P}(X) \mid |A| = n\}$.

Propoziție

Pentru orice $n \in \mathbb{N} \setminus \{0\}$ și orice X infinită, avem $|\mathcal{P}_n(X)| = |X|$.

Demonstrație

Pentru a găsi o injecție de la X la $\mathcal{P}_n(X)$, fixăm întâi $a_0, \ldots, a_n \in X$, diferite două câte două. Apoi, orice $x \in \{a_i \mid i \leq n\}$ va fi dus în $\{a_i \mid i \leq n\} \setminus \{x\}$, iar orice x din afara acelei mulțimi va fi dus în $\{a_i \mid i < n-1\} \cup \{x\}$.

În sens invers, bine-ordonăm X și atunci fiecărui element $\{x_i \mid i < n\}$ al lui $\mathcal{P}_n(X)$, considerând w.l.o.g. $x_0 < \ldots < x_{n-1}$ îi asociem elementul $(x_0, \ldots, x_{n-1}) \in X^n$. Așadar, $|\mathcal{P}_n(X)| \leq |X^n| = |X|$.

Părți finite

Pentru orice X, definim $\mathcal{P}_{\text{fin}}(X) := \{A \in \mathcal{P}(X) \mid A \text{ finită}\}$.

Propoziție

Pentru orice X infinită, avem $|\mathcal{P}_{\text{fin}}(X)| = |X|$.

Demonstrație

Cum

$$\mathcal{P}_{\text{fin}}(X) = \bigcup_{n \in \mathbb{N}} \mathcal{P}_n(X),$$

avem

$$|\mathcal{P}_{\text{fin}}(X)| \leq |\mathbb{N}| \cdot |X| = |X|$$

și, pe de altă parte,

$$|X| = |\mathcal{P}_1(X)| \leq |\mathcal{P}_{\text{fin}}(X)|.$$

Cardinalul spațiilor vectoriale

Considerăm cunoscute de la Algebră liniară noțiunile de spațiu vectorial și bază. Cu titlu informativ, menționăm că faptul că orice spațiu vectorial admite o bază este echivalent cu Axioma alegerii.

Propoziție

Fie k un corp, V un k-spațiu vectorial și B o bază pentru V cu $B \neq \emptyset$ (i.e. $V \neq \{0_V\}$). Atunci $\max(|B|, |k|) \leq |V|$.

Demonstrație

Cum $B \neq \emptyset$, fie $v \in B$. Considerăm $f : k \to V$, definită, pentru orice $\alpha \in k$, prin $f(\alpha) := \alpha \cdot v$. Atunci f este injectivă și, deci, $|k| \leq |V|$. Cum $B \subseteq V$, avem $|B| \leq |V|$, de unde obținem concluzia dorită.

Cardinalul spațiilor vectoriale

Propoziție

Fie k un corp infinit, V un k-spațiu vectorial și B o bază pentru V cu $B \neq \emptyset$ și B finită. Atunci $|V| = |k|$.

Demonstrație

Avem că V este izomorf cu $k^{|B|}$, deci $|V| = |k|^{|B|} = |k|$.

Teoremă

Fie k un corp infinit, V un k-spațiu vectorial și B o bază pentru V cu B infinită. Atunci $|V| = \max(|B|, |k|)$.

Demonstrație

Avem

$$V = \bigcup_{D \in \mathcal{P}_{\text{fin}}(B)} \langle D \rangle,$$

deci $|V| \leq |\mathcal{P}_{\text{fin}}(B)| \cdot |k| = |B| \cdot |k| = \max(|B|, |k|)$.

Mulțimea funcțiilor de la $\mathbb{N}$ la $\mathbb{Q}$, notată cu $\mathbb{Q}^{\mathbb{N}}$, are o structură naturală de $\mathbb{Q}$-spațiu vectorial.

Propoziție

Fie B o bază pentru $\mathbb{Q}^{\mathbb{N}}$. Atunci $|B| = \mathfrak{c}$.

Demonstrație

Avem că $\left|\mathbb{Q}^{\mathbb{N}}\right| = |\mathbb{Q}|^{|\mathbb{N}|} = \aleph_0^{\aleph_0} = 2^{\aleph_0} = \mathfrak{c}$.

Clar, $\mathbb{Q}^{\mathbb{N}} \neq \{0_{\mathbb{Q}^{\mathbb{N}}}\}$, deci $B \neq \emptyset$. Presupunem că B este finită. Atunci $\left|\mathbb{Q}^{\mathbb{N}}\right| = |\mathbb{Q}| = \aleph_0$, contradicție.

Rezultă că B este infinită, de unde scoatem $\left|\mathbb{Q}^{\mathbb{N}}\right| = \max(|B|, |\mathbb{Q}|) = \max(|B|, \aleph_0) = |B|$, deci $|B| = \mathfrak{c}$.

Axioma regularităţii

Ultima axiomă a sistemului ZFC este Axioma regularităţii.

Axioma regularităţii

Pentru orice mulţime nevidă a, există $b \in a$ cu $a \cap b = \emptyset$.

Pentru a oferi o intuiţie asupra axiomei, vom prezenta anumite consecinţe imediate.

Propoziţie

Nu există x cu $x \in x$.

Demonstraţie

Presupunem că există x cu $x \in x$. Fie $a := \{x\}$, deci $x \in a \cap x$. Din Axioma regularităţii, avem că există $b \in a$ cu $a \cap b = \emptyset$. Dar, cum $a = \{x\}$, avem $b = x$, deci $a \cap x = \emptyset$. Contradicţie!

Cicli de lungime 2 sau 3

Raționamentul se poate extinde ușor la cicli de lungime scurtă.

Propoziție

Nu există x, y cu $x \in y \in x$.

Demonstrație

Presupunem că există x, y cu $x \in y \in x$. Fie $a := \{x, y\}$, deci $x \in a \cap y$ și $y \in a \cap x$. Din Axioma regularității, avem $a \cap x = \emptyset$ sau $a \cap y = \emptyset$, contradicție.

Propoziție

Nu există x, y, z cu $x \in y \in z \in x$.

Demonstrație

Presupunem că există x, y, z cu $x \in y \in z \in x$. Fie $a := \{x, y, z\}$, deci $x \in a \cap y$, $y \in a \cap z$ și $z \in a \cap x$. Din Axioma regularității, avem $a \cap x = \emptyset$, $a \cap y = \emptyset$ sau $a \cap z = \emptyset$, contradicție.

Putem arăta acum că nu există cicli de lungime arbitrară.

Propoziție

Nu există $n \in \mathbb{N}$ și $(x_i)_{i<n^+}$ astfel încât $x_0 \in x_n$, iar pentru orice $i < n$ să avem $x_{i^+} \in x_i$.

Demonstrație

Presupunem că am avea $n \in \mathbb{N}$ și $(x_i)_{i<n^+}$ astfel încât $x_0 \in x_n$, iar pentru orice $i < n$ avem $x_{i^+} \in x_i$. Notăm

$$a := \{x_i \mid i < n^+\}.$$

Atunci, din Axioma regularității, există $i < n^+$, deci $i \leq n$, cu $a \cap x_i = \emptyset$. Dacă $i < n$, avem $x_{i^+} \in a \cap x_i$, contradicție. Dacă $i = n$, avem $x_0 \in a \cap x_n = a \cap x_i$, contradicție.

Mai mult, putem arăta că nu există nici șiruri descendente infinit de lungi.

Propoziție (Principiul șirului)

Nu există $(x_i)_{i\in\mathbb{N}}$ astfel încât pentru orice $i \in \mathbb{N}$ să avem $x_{i^+} \in x_i$.

Demonstrație

Presupunem că am avea $(x_i)_{i\in\mathbb{N}}$ astfel încât pentru orice $i \in \mathbb{N}$ avem $x_{i^+} \in x_i$. Notăm

$$a := \{x_i \mid i \in \mathbb{N}\}.$$

Atunci, din Axioma regularității, există $i \in \mathbb{N}$ cu $a \cap x_i = \emptyset$. Dar atunci $x_{i^+} \in a \cap x_i$, contradicție.

Acest principiu are o formă mai intuitivă ca Axioma regularității, dar este echivalent cu ea, după cum vom vedea imediat.

Înapoi la Axioma regularității

Propoziție

Principiul șirului implică Axioma regularității.

Demonstrație

Fie a o mulțime nevidă și presupunem că pentru orice $b \in a$, $a \cap b \neq \emptyset$. Notăm $I := \mathcal{P}(a) \setminus \{\emptyset\}$. Atunci, aplicând Axioma alegerii, există $(g_i)_{i \in I}$ astfel încât, pentru orice $i \in I$, $g_i \in i$. Definim $h : \mathbb{N} \to a$ punând $h(0) := g_a$, iar pentru orice $n \in \mathbb{N}$, $h(n^+) := g_{a \cap h(n)}$. Așadar, am construit un șir $h(0) \ni h(1) \ni h(2) \ni \ldots$, contradicție!

Există suficiente mulțimi

Următoarea propoziție ne arată că avem, într-un anume sens, suficiente mulțimi de orice cardinal.

Propoziție

Fie A o mulțime și κ un cardinal. Atunci există B cu $|B| = \kappa$ astfel încât $A \cap B = \emptyset$.

Demonstrație

Fie $B := \{A\} \times \kappa$. Clar, $|B| = \kappa$. Presupunem că ar exista $x \in A \cap B$. Atunci avem $x \in A$, iar, cum $x \in B$, există $\alpha \in \kappa$ astfel încât $x = (A, \alpha)$, deci $x = \{\{A\}, \{A, \alpha\}\}$. Așadar,

$$A \in \{A\} \in \{\{A\}, \{A, \alpha\}\} = x \in A,$$

deci avem un ciclu de lungime 3. Contradicție!

Ierarhia cumulativă von Neumann

Axioma regularității ne permite să descriem, oarecum, modul cum sunt „formate" mulțimile. Definim recursiv un șir de mulțimi indexat de ordinali ce se numește **ierarhia von Neumann**: $V_0 := \emptyset$, pentru orice ordinal β, punem $V_{\beta^+} := \mathcal{P}(V_\beta)$, iar pentru orice ordinal limită α, punem

$$V_\alpha := \bigcup\{V_\gamma \mid \gamma < \alpha\} = \bigcup_{\gamma<\alpha} V_\gamma.$$

Fie x o mulțime astfel încât există α cu $x \in V_\alpha$ și alegem α **minim** cu această proprietate. Atunci $\alpha \neq 0$ (fiindcă $V_0 = \emptyset$) și α nu poate fi limită, fiindcă atunci ar exista $\gamma < \alpha$ cu $x \in V_\gamma$, contrazicând minimalitatea lui α. Rezultă că există β cu $\alpha = \beta^+$, iar pe acest β îl numim **rangul** lui x. Îl notăm cu $\mathrm{rg}(x)$. Mai spunem, deci, pentru orice x, că x **are rang** dacă există α cu $x \in V_\alpha$.

Rangul și apartenența

Propoziție

Fie α un ordinal, $x \in V_\alpha$, $y \in x$. Atunci există $\delta < \alpha$ astfel încât $y \in V_\delta$.

Demonstrație

Demonstrăm prin inducție după α. Dacă $\alpha = 0$, $V_\alpha = \emptyset$ și nu avem ce demonstra. Dacă α este limită, atunci există $\gamma < \alpha$ cu $x \in V_\gamma$ și aplic ipoteza de inducție pentru γ. Rămâne cazul când există β cu $\alpha = \beta^+$. Atunci $x \in V_{\beta^+} = \mathcal{P}(V_\beta)$, deci $x \subseteq V_\beta$. Cum $y \in x$, avem $y \in V_\beta$, deci putem lua $\delta := \beta$.

Așadar, dacă x și y sunt astfel încât $y \in x$ și x are rang, atunci y are rang și $\mathrm{rg}(y) < \mathrm{rg}(x)$.

Incluziunea mulțimilor din ierarhie

Următoarea propoziție arată faptul că ierarhia mulțimilor este **cumulativă**.

Propoziție

Fie α un ordinal. Atunci:

- Dacă $\gamma < \alpha$, atunci $V_\gamma \subseteq V_\alpha$.
- Avem că V_α este tranzitivă.

Demonstrație

- Din nou, demonstrăm prin inducție după α, iar cazul succesor este cel netrivial. Fie β cu $\alpha = \beta^+$. Fie $x \in V_\gamma$. Atunci, ori $\gamma < \beta$, iar din ipoteza de inducție avem $x \in V_\beta$, ori $\gamma = \beta$, deci $x \in V_\beta$. Fie $y \in x$. Atunci există $\delta < \beta$ cu $y \in V_\delta$, iar, din nou din ipoteza de inducție, avem $y \in V_\beta$. Am demonstrat că $x \subseteq V_\beta$, deci $x \in \mathcal{P}(V_\beta) = V_{\beta^+} = V_\alpha$.
- Fie $x \in V_\alpha$ și $y \in x$. Atunci există $\delta < \alpha$ cu $y \in V_\delta$, și avem $V_\delta \subseteq V_\alpha$, deci $y \in V_\alpha$.

Dacă toate elementele au rang

Propoziție

Fie x o mulțime ale cărei elemente au toate rang. Atunci x are rang.

Demonstrație

Fie $H := \{\mathrm{rg}(y) \mid y \in x\}$ și $\alpha := \sup H$. Fie $y \in x$. Atunci, pentru orice $y \in x$, $y \in V_{(\mathrm{rg}(y))^+}$. Avem $\mathrm{rg}(y) \leq \alpha$, deci $\mathrm{rg}(y)^+ \leq \alpha^+$ și $V_{(\mathrm{rg}(y))^+} \subseteq V_{\alpha^+}$. Rezultă că $y \in V_{\alpha^+}$. Am demonstrat că $x \subseteq V_{\alpha^+}$, deci $x \in \mathcal{P}(V_{\alpha^+}) = V_{\alpha^{++}}$.

Pentru orice mulțime X, definim $T_0(X) := X$ și apoi, recursiv, pentru orice $n \in \mathbb{N}$, $T_{n^+}(X) := \bigcup T_n(X)$. Punem:

$$T(X) := \bigcup_{n \in \mathbb{N}} T_n(X).$$

Mulțimea $T(X)$ se numește **închiderea tranzitivă** a lui X. Este o mulțime tranzitivă ce include pe X, iar pentru orice mulțime tranzitivă Y cu $X \subseteq Y$, avem $T(X) \subseteq Y$.

Pentru a demonstra că este tranzitivă (lucru de care vom avea nevoie în scurt timp), fie $b \in T(X)$ și $a \in b$. Atunci există n cu $b \in T_n(X)$, și deci $a \in \bigcup T_n(X) = T_{n^+}(X) \subseteq T(X)$. Cealaltă afirmație rămâne ca exercițiu.

Principiul rangului

Propoziție (Principiul rangului)

Orice mulțime are rang.

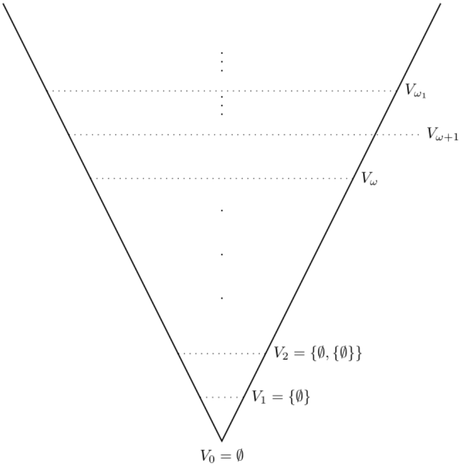
Demonstrație

Presupunem că există o mulțime X fără rang. Fie $A := T(\{X\})$. Atunci A este tranzitivă și $X \in A$. Aplicăm Axioma alegerii ca să obținem o familie $(g_Y)_{Y \in \mathcal{P}(A) \setminus \{\emptyset\}}$ astfel încât pentru orice $Y \subseteq A$ nevidă, $g_Y \in Y$. Fie $b \notin A$. Definim, recursiv, o funcție $h : \mathbb{N} \to A \cup \{b\}$ prin $h(0) := X$, iar pentru orice $n \in \mathbb{N}$, dacă $h(n) \in A$ și $h(n)$ nu are rang, atunci există $z \in h(n)$ fără rang, iar, cum A este tranzitivă, $h(n) \subseteq A$, deci putem pune

$$h(n^+) := g_{\{z \in h(n) \mid z \text{ nu are rang}\}} \in h(n),$$

iar în caz contrar, punem $h(n^+) := b$. Se arată prin inducție că pentru orice n, $h(n) \in A$ și $h(n)$ nu are rang. Ca urmare, am construit un șir $h(0) \ni h(1) \ni h(2) \ni \ldots$, contradicție!

Așadar, acceptând Axioma regularității, toate mulțimile sunt cuprinse în ierarhia von Neumann:



Notația V vine atât de la numele lui von Neumann, cât și de la forma de V a ierarhiei.

Înapoi la Principiul șirului

Putem folosi și Principiul rangului pentru a demonstra Principiul șirului, în felul următor. Fie $(x_n)_{n\in\mathbb{N}}$ un șir cu

$$x_0 \ni x_1 \ni x_2 \ni \dots$$

Atunci avem

$$\mathrm{rg}(x_0) > \mathrm{rg}(x_1) > \mathrm{rg}(x_2) > \dots$$

Mulțimea nevidă de ordinali $\{\mathrm{rg}(x_i) \mid i \in \mathbb{N}\}$, deci, nu are minim, contradicție!

Am arătat, deci, că Axioma regularității, Principiul șirului și Principiul rangului sunt enunțuri echivalente. Mare atenție, însă – în demonstrarea echivalenței am folosit Axioma alegerii!

Mulțimi închise la intersecții finite

Pentru tot restul capitolului, fixăm I o mulțime **nevidă**.

Următoarea propoziție rezultă imediat prin inducție.

Propoziție-Definiție

Fie $G \subseteq \mathcal{P}(I)$. Următoarele afirmații sunt echivalente:

- pentru orice $S_1, S_2 \in G$, $S_1 \cap S_2 \in G$;
- pentru orice $A \subseteq G$ finită nevidă, $\bigcap A \in G$.

În acest caz, spunem că G este **închisă la intersecții finite**.

Filtre

Definiție

Se numește **filtru** pe I o submulțime F a lui $\mathcal{P}(I)$ cu următoarele proprietăți:

- $\emptyset \notin F$, $I \in F$;
- F este închisă la intersecții finite;
- pentru orice $S_1, S_2 \subseteq I$ cu $S_1 \in F$ și $S_1 \subseteq S_2$, avem $S_2 \in F$.

De exemplu, $\{I\}$ este filtru pe I (aici folosim faptul că I este nevidă). Observăm și că dacă F este un filtru, pentru niciun $S \subseteq I$ nu pot avea simultan $S \in F$ și $I \setminus S \in F$, deoarece atunci am avea $\emptyset = S \cap (I \setminus S) \in F$, contradicție.

Proprietatea intersecțiilor finite

Definiție

Fie $G \subseteq \mathcal{P}(I)$.

- Spunem că G are **proprietatea** (slabă a) **intersecțiilor finite** dacă pentru orice $A \subseteq G$ finită nevidă, $\bigcap A \neq \emptyset$.
- Spunem că G are **proprietatea tare a intersecțiilor finite** dacă $\emptyset \notin G$, iar G este închisă la intersecții finite.

Clar, proprietatea tare a intersecțiilor finite o implică pe cea slabă. Orice filtru posedă proprietatea tare a intersecțiilor finite.

Filtrul generat

Propoziție-Definiție

Fie $G \subseteq \mathcal{P}(I)$ ce are proprietatea intersecțiilor finite. Dacă $G \neq \emptyset$, atunci mulțimea

$$\{S \in \mathcal{P}(I) \mid \text{există } A \subseteq G \text{ finită nevidă cu } \bigcap A \subseteq S\}$$

este filtru ce include pe G și îl numim **filtrul generat** de G. Dacă $G = \emptyset$, spunem că filtrul generat de G este $\{I\}$.

Demonstrație

Notăm cu F acea mulțime. Dacă am avea $\emptyset \in F$, ar exista $A \subseteq G$ finită nevidă cu $\bigcap A \subseteq \emptyset$, deci $\bigcap A = \emptyset$, ceea ce contrazice faptul că G are proprietatea intersecțiilor finite. Cum $G \neq \emptyset$, există $X \in G$, iar $\bigcap\{X\} = X \subseteq I$, deci $I \in F$. Vedem și că, pentru orice $X \in G$, avem $\bigcap\{X\} = X \subseteq S$, deci $X \in F$.

Demonstrație (cont.)

Fie S_1, $S_2 \in F$. Avem că există A, $B \subseteq G$ finite nevide cu $\bigcap A \subseteq S_1$ și $\bigcap B \subseteq S_2$. Atunci

$$\bigcap(A \cup B) = \left(\bigcap A\right) \cap \left(\bigcap B\right) \subseteq S_1 \cap S_2,$$

iar cum $A \cup B \subseteq G$ este finită și nevidă, avem $S_1 \cap S_2 \in F$.

Fie S_1, $S_2 \subseteq I$ cu $S_1 \in F$ și $S_1 \subseteq S_2$. Avem că există $A \subseteq G$ finită nevidă cu $\bigcap A \subseteq S_1$, deci $\bigcap A \subseteq S_2$ și $S_2 \in F$.

De asemenea, pentru orice $G \subseteq \mathcal{P}(I)$ și orice filtru ce include pe G, avem că acel filtru include filtrul generat de G (exercițiu!).

Dacă avem $T \subseteq I$ nevidă, atunci $\{T\}$ are proprietatea (chiar tare a) intersecțiilor finite. Notez filtrul generat de $\{T\}$ cu $[T)$, i.e.

$$[T) := \{S \subseteq I \mid T \subseteq S\}.$$

Un asemenea filtru se numește **filtru principal**.

Corolar

Fie $G \subseteq \mathcal{P}(I)$. Următoarele afirmații sunt echivalente:

- G are proprietatea intersecțiilor finite.
- Există un filtru pe I ce include pe G.

Demonstrație

Dacă G are proprietatea a intersecțiilor finite, atunci filtrul generat de G este un filtru pe I ce include pe G. Invers, dacă există un filtru F ce include pe G, atunci pentru orice $A \subseteq G$ finită nevidă, $A \subseteq F$ și deci $\bigcap A \in F$ și $\bigcap A \neq \emptyset$.

Ultrafiltre

Propoziție-Definiție

Fie U un filtru pe I. Următoarele afirmații sunt echivalente:

- pentru orice filtru F cu $U \subseteq F$, avem $U = F$ (adică U este filtru **maximal**);
- pentru orice S_1, $S_2 \subseteq I$ cu $S_1 \cup S_2 \in U$, avem $S_1 \in U$ sau $S_2 \in U$;
- pentru orice $S \subseteq I$, avem (exact una dintre) $S \in U$ sau $I \setminus S \in U$.

În acest caz, U se numește **ultrafiltru**.

Demonstrație

Începem prin a arăta echivalența ultimelor două proprietăți. Dacă avem $S \subseteq I$, atunci $S \cup (I \setminus S) = I \in U$ și deci $S \in U$ sau $I \setminus S \in U$. Invers, dacă avem S_1, $S_2 \subseteq I$ cu $S_1 \cup S_2 \in U$, presupunem $S_1 \notin U$ și atunci $I \setminus S_1 \in U$, deci $(S_1 \cup S_2) \cap (I \setminus S_1) \in U$. Dar $(S_1 \cup S_2) \cap (I \setminus S_1) \subseteq S_2$, deci $S_2 \in U$.

Demonstrație (cont.)

Arătăm acum echivalența dintre prima și a treia proprietate. Presupunem că există F cu $U \subsetneq F$. Fie $S \in F \setminus U$. Cum $S \notin U$, avem $I \setminus S \in U$, deci $I \setminus S \in F$, contradicție cu $S \in F$.

În sfârșit, presupunând că U este maximal, fie $S \subseteq I$ cu $S \notin U$. Vrem $I \setminus S \in U$. Dacă $S = \emptyset$, atunci $I \setminus S = I \in U$. Presupunem $S \neq \emptyset$. Fie $G := U \cup \{S\}$. Dacă ar exista un filtru F cu $G \subseteq F$, atunci $U \subsetneq F$, contradicție cu maximalitatea lui U. Deci G nu are proprietatea intersecțiilor finite, i.e. există $A \subseteq G$ finită nevidă cu $\bigcap A = \emptyset$. Cum U este filtru, $A \not\subseteq U$, deci $S \in A$. Dacă $A = \{S\}$, atunci $\bigcap A = S \neq \emptyset$, contradicție. Deci există $B \subseteq U$ finită nevidă cu $A = B \cup \{S\}$. Avem $\bigcap B \in U$ și $\emptyset = \bigcap A = (\bigcap B) \cap S$. Așadar, $\bigcap B \subseteq I \setminus S$ și cum $\bigcap B \in U$, avem $I \setminus S \in U$.

Teorema de existență a ultrafiltrului

Teoremă

Fie F un filtru. Atunci există un ultrafiltru U cu $F \subseteq U$.

Demonstrație

Notăm

$$\mathcal{F} := \{H \subseteq \mathcal{P}(I) \mid H \text{ este filtru și } F \subseteq H\}.$$

Atunci $(\mathcal{F}, \subseteq)$ este mulțime parțial ordonată (exercițiu!) și $F \in \mathcal{F}$. Arătăm că $(\mathcal{F}, \subseteq)$ este inductiv ordonată. Fie $L \subseteq \mathcal{F}$ un lanț. Dacă $L = \emptyset$, atunci F majorează pe L. Dacă $L \neq \emptyset$, atunci $\bigcup L$ este un filtru din $\mathcal{F}$ ce majorează pe L (exercițiu!). Așadar, din Lema lui Zorn, există un element maximal U în $\mathcal{F}$. Mai trebuie arătat că U este maximal ca filtru. Dacă avem un filtru J cu $U \subseteq J$, atunci, cum $F \subseteq U$, avem $F \subseteq J$ și deci $J \in \mathcal{F}$ și avem $U = J$ din maximalitatea lui U în $\mathcal{F}$.

Corolar

Fie $G \subseteq \mathcal{P}(I)$. Următoarele afirmații sunt echivalente:

- G are proprietatea intersecțiilor finite.
- Există un filtru pe I ce include pe G.
- Există un ultrafiltru pe I ce include pe G.

Ultrafiltre principale

Fie $x \in I$. Atunci se poate vedea că $[\{x\}) = \{S \subseteq I \mid x \in S\}$ este ultrafiltru: anume, dacă am avea un filtru F cu $[\{x\}) \subsetneq F$, atunci am avea $S \in F$ cu $x \notin S$, și atunci $\emptyset = \{x\} \cap S \in F$, contradicție!

Putem arăta și că orice ultrafiltru principal este de această formă. Fie T nevidă astfel încât $U := [T)$ este ultrafiltru. Fie $x \in T$ și presupunem $T \neq \{x\}$. Avem și că $T \neq T \setminus \{x\}$, iar $\{x\} \cup (T \setminus \{x\}) = T \in U$. Deci $\{x\} \in U$ sau $T \setminus \{x\} \in U$, adică $T \subseteq \{x\}$ sau $T \subseteq T \setminus \{x\}$. Niciuna dintre aceste posibilități nu este adevărată, deci am ajuns la o contradicție.

Mai mult, putem arăta și că un ultrafiltru este principal dacă și numai dacă el conține o mulțime finită. Un sens este arătat de raționamentul anterior, așadar rămâne să îl arătăm pe celălalt, i.e. pentru orice ultrafiltru U ce conține o mulțime finită (nevidă) S, avem că U este principal.

Demonstrăm prin inducție după cardinalul nenul al lui S.

Dacă el este 1, există x cu $S = \{x\}$, deci $[\{x\}) \subseteq U$. Dar $[\{x\})$ este ultrafiltru, deci maximal, așadar $U = [\{x\})$.

Fie n cu $1 \leq n$ astfel încât S are cardinalul n^+. Atunci există $x \in S$ și T de cardinal n astfel încât $\{x\} \cup T = S \in U$. Atunci $\{x\} \in U$ sau $T \in U$ și putem aplica ipoteza de inducție.

În particular, pe o mulțime finită, orice ultrafiltru este principal.

Ultrafiltre neprincipale

Dacă I este infinită, atunci mulțimea

$$\{T \subseteq I \mid I \setminus T \text{ este finită}\}$$

este filtru pe I (exercițiu!), numit **filtrul Fréchet** pe I.

Dacă U este un ultrafiltru neprincipal pe I, atunci el include filtrul Fréchet. Dacă nu ar fi așa, atunci ar exista $T \subseteq I$ cu $I \setminus T$ finită și $T \notin U$. Dar atunci $I \setminus T \in U$ și deci U conține o mulțime finită și este principal, contradicție.

Invers, dacă U include filtrul Fréchet, presupunând că U este principal, avem că există $S \in U$ finită. Notând $T := I \setminus S$, avem $I \setminus T = S$ și deci T este în filtrul Fréchet, deci și în U. Dar atunci $\emptyset = T \cap S \in U$, contradicție.

Am demonstrat că, pe o mulțime infinită, un ultrafiltru este neprincipal dacă și numai dacă el include filtrul Fréchet. Ca urmare, pe orice mulțime infinită există un ultrafiltru neprincipal.

Logica propozițională

În acest moment putem începe studiul sistemelor logice. Dintre ele, logicii de ordinul I i se poate observa de pe acum relevanța, deoarece cu ajutorul ei se vor putea formaliza riguros axiomele teoriei mulțimilor ZFC ce au fost studiate în capitolul precedent.

În definirea și în studiul acestor sisteme, vom folosi, însă, aparatul teoriei mulțimilor. Apare astfel o problemă de genul „ce a fost înainte, oul sau găina?” care va trebui clarificată la un moment dat.

Înainte de a studia ideile și conceptele logicii de ordinul I, le vom studia pe cele ale logicii propoziționale, care deseori sunt imagini în miniatură ale primelor și pot ajuta la formarea unei intuiții.

Motto

"An exposition of what logicians call the propositional calculus can annoy and mystify mathematicians. It looks like a lot of fuss [...], it puts much emphasis on the alphabet and it gives detailed consideration to 'variables' (which do not in any sense vary). Despite (or because of?) all the pedantic machinery, it is hard to see what genuine content the subject has. Insofar as it talks about implications between propositions, everything it says looks obvious. Does it really have any mathematical value?"

– Paul Halmos, *I Want to Be a Mathematician: An Automathography* (1985)

Tabele de adevăr – recapitulare

În liceu, la disciplina Logică și argumentare (și nu numai acolo), s-au studiat tabele de adevăr. Acestea serveau la soluționarea unor cerințe precum: să se arate că formula $p \to ((q \to r) \to p)$ este tautologie.

p	q	r	$q \to r$	$(q \to r) \to p$	$p \to ((q \to r) \to p)$
1	1	1	1	1	1
1	1	0	0	1	1
1	0	1	1	1	1
1	0	0	1	1	1
0	1	1	1	0	1
0	1	0	0	1	1
0	0	1	1	0	1
0	0	0	1	0	1

Vom arăta acum un prim mod de a formula și rezolva riguros o asemenea cerință.

Operații pe 2

Reamintim: $2 = \{0, 1\}$. Vom defini operațiile $\neg : 2 \to 2$, $\rightarrow$, $\wedge$, $\vee$, $\leftrightarrow$: $2^2 \to 2$ în mod exhaustiv, prin următoarele tabele:

p	$\neg p$
0	1
1	0

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Tabelul de adevăr riguros

Prin urmare, enunțul anterior se poate reformula ca: să se arate că pentru orice p, q, $r \in 2$, avem $p \to ((q \to r) \to p) = 1$.

p	q	r	$q \to r$	$(q \to r) \to p$	$p \to ((q \to r) \to p)$
1	1	1	1	1	1
1	1	0	0	1	1
1	0	1	1	1	1
1	0	0	1	1	1
0	1	1	1	0	1
0	1	0	0	1	1
0	0	1	1	0	1
0	0	0	1	0	1

Proprietăți imediate

Propoziție

Fie p, $q \in 2$. Atunci:

- $\neg p = 1 \Leftrightarrow p = 0$, $\neg p = 0 \Leftrightarrow p = 1$, $\neg\neg p = p$;
- $p \rightarrow q = 1 \Leftrightarrow p \leq q$;
- $p \rightarrow q = \neg p \vee q$, $p \vee q = \neg p \rightarrow q$;
- $p \wedge q = \neg(p \rightarrow \neg q)$;
- $\neg(p \wedge q) = (\neg p) \vee (\neg q)$, $\neg(p \vee q) = (\neg p) \wedge (\neg q)$ (de Morgan);
- $p \leftrightarrow q = (p \rightarrow q) \wedge (q \rightarrow p)$.

În particular, toate operațiile definite anterior se pot exprima în funcție de $\neg$ și $\rightarrow$. În continuare, vom dezvolta formalismul logicii propoziționale, al cărui prim câștig va fi faptul că vom putea formula și demonstra chiar mai mult decât atât, anume că orice operație la care ne-am fi putut gândi se poate exprima în funcție de $\neg$ și $\rightarrow$.

Simboluri

Ideea este de a defini formulele logice ca obiecte matematice în sine, anume ca șiruri finite de simboluri. Vom **fixa** două obiecte $\neg$ și $\rightarrow$ astfel încât $\neg \neq \rightarrow$ (ele pot fi orice, de pildă numerele 7 și 31), precum și o mulțime **nevidă** Q – ale cărei elemente vor reprezenta **variabilele** sau **simbolurile propoziționale** – cu proprietatea că $\neg, \rightarrow \notin Q$. Mulțimea simbolurilor care vor apărea în formule va fi, deci, $S(Q) := Q \cup \{\neg, \rightarrow\}$.

Atunci când știm $\kappa := |Q|$, vom fixa tacit o bijecție $f : \kappa \rightarrow Q$, iar pentru orice $\alpha \in \kappa$, vom nota $f(\alpha)$ cu v_α. Dacă Q este finită, cum este nevidă, există $n \in \mathbb{N}$ astfel încât

$$Q = \{v_i \mid i \leq n\} = \{v_0, \ldots, v_n\},$$

iar dacă Q este numărabilă,

$$Q = \{v_i \mid i \in \mathbb{N}\} = \{v_0, v_1, v_2, \ldots\}.$$

Formule

Formulele vor fi, deci, elemente ale lui $\mathrm{Seq}(S(Q))$, iar proprietățile pe care o mulțime $A \subseteq \mathrm{Seq}(S(Q))$ trebuie să le verifice pentru ca ea să fie mulțime de formule vor fi:

- $\mathrm{Seq}_1(Q) \subseteq A$ (adică variabilele „sunt" formule);
- dacă $\varphi \in A$, atunci $\neg\varphi \in A$;
- dacă φ, $\psi \in A$, atunci $\rightarrow \varphi\psi \in A$.

Submulțimile lui $\mathrm{Seq}(S(Q))$ ce verifică aceste proprietăți formează o mulțime Moore. Așadar, putem lua minimul ei pe care îl notăm cu $E(Q)$ (în particular, $E(Q)$ este nevidă, fiindcă va include $\mathrm{Seq}_1(Q) \neq \emptyset$). Numim elementele acestei mulțimi **formule** sau **enunțuri** peste Q (atenție, doar la Logica propozițională aceste două concepte vor coincide).

Observăm că am folosit forma **prefixată** a formulelor pentru a le defini – am scris $\rightarrow \varphi\psi$ în loc de $\varphi \rightarrow \psi$ – deoarece ne va fi mai comod la unele demonstrații. În scurt timp, vom oferi un mod prin care vom putea folosi în discursul nostru forma obișnuită, i.e. **infixată**.

În general, dacă Σ este o mulțime oarecare, o putem gândi ca pe un alfabet, iar atunci $\mathrm{Seq}(\Sigma)$ va fi mulțimea **cuvintelor** cu „litere" din Σ. De pildă, dacă a, $b \in \Sigma$, atunci vom scrie $ab \in \mathrm{Seq}(\Sigma)$, unde prin ab înțelegem șirul $\{(0, a), (1, b)\}$. **Lungimea** unui cuvânt este pur și simplu domeniul său (în exemplul anterior, acela este 2). O submulțime a lui $\mathrm{Seq}(\Sigma)$ se va numi **limbaj formal** peste Σ – de pildă, $E(Q)$ este limbaj formal peste $S(Q)$.

Avem că $\emptyset \in \mathrm{Seq}(\Sigma)$ – în acest context se numește **cuvântul vid** și se notează în general cu λ.

Cuvintele care au lungimea 1, adică elementele lui $\mathrm{Seq}_1(\Sigma)$, vor fi identificate tacit cu literele, adică elementele lui Σ. În aceeași idee, în situații precum cea de pe slide-ul anterior unde am scris $\mathrm{Seq}_1(Q)$ vom putea scrie Q.

Principiul inducției pe formule

Următoarea teoremă reprezintă o formă de inducție **structurală** pe mulțimea formulelor.

Principiul inducției pe formule

Fie $B \subseteq E(Q)$ astfel încât:

- $Q \subseteq B$;
- dacă $\varphi \in B$, atunci $\neg\varphi \in B$;
- dacă $\varphi, \psi \in B$, atunci $\rightarrow \varphi\psi \in B$.

Atunci $B = E(Q)$.

Enunțul rezultă imediat din faptul că B este una din mulțimile ce participă la intersecția prin care a fost definit $E(Q)$.

Citirea formulelor

Proprietatea de citire

Fie $\chi \in E(Q)$. Atunci se întâmplă exact una dintre următoarele alternative:

- $\chi \in Q$;
- există $\varphi \in E(Q)$ cu $\chi = \neg\varphi$;
- există $\varphi, \psi \in E(Q)$ cu $\chi = \rightarrow \varphi\psi$.

Demonstrație

Notăm cu B mulțimea formulelor ce se pot scrie sub acele forme. Atunci, clar, B verifică condițiile Principiului de inducție și deci $B = E(Q)$. Faptul că se întâmplă cel mult una dintre alternative rezultă din condițiile $\neg \neq \rightarrow$ și $\neg, \rightarrow \notin Q$.

Corolar

Orice formulă are lungimea cel puțin 1 (i.e. $\lambda \notin E(Q)$).

Despre segmente inițiale

Lemă

Fie $\chi \in E(Q)$. Atunci nu există $\alpha \in E(Q)$ care să fie segment inițial strict al lui χ.

Demonstrație

Demonstrăm prin inducție, dar nu structurală, ci inducție completă pe numere după lungimea lui χ. Presupunem că există α ca în enunț. Din proprietatea de citire, distingem trei cazuri. Dacă $\chi \in Q$, atunci $\alpha = \lambda$, ceea ce nu se poate. Dacă există φ cu $\chi = \neg\varphi$, atunci există φ' cu $\alpha = \neg\varphi'$ și deci φ' este segment inițial strict al lui φ, contradicție cu ipoteza de inducție (φ are lungime strict mai mică ca χ). Dacă există φ, ψ cu $\chi = \to \varphi\psi$, atunci există φ', ψ' cu $\alpha = \to \varphi'\psi'$. Dacă φ și φ' ar avea lungimi diferite, atunci unul ar fi segment inițial strict al celuilalt, contradicție cu ipoteza de inducție. Așadar, $\varphi = \varphi'$ și deci ψ și ψ' au lungimi diferite, de unde rezultă din nou o contradicție cu ipoteza de inducție.

Citirea unică a formulelor

Proprietatea de citire unică

Fie φ, ψ, φ', $\psi' \in E(Q)$. Atunci:

- dacă $\neg\varphi = \neg\varphi'$, atunci $\varphi = \varphi'$;
- dacă $\to \varphi\psi = \to \varphi'\psi'$, atunci $\varphi = \varphi'$ și $\psi = \psi'$.

Demonstrație

Primul punct este evident. Pentru al doilea, dacă φ și φ' ar avea lungimi diferite, atunci unul ar fi segment inițial strict al celuilalt, contradicție. Rezultă că φ și φ' au aceeași lungime. Dar de aici rezultă imediat concluzia dorită.

Operații pe $E(Q)$

Pentru a putea folosi, după cum am anunțat, o notație infixată, definim pe $E(Q)$ operațiile $\neg : E(Q) \to E(Q)$ și $\to: E(Q)^2 \to E(Q)$, pentru orice φ, $\psi \in E(Q)$, prin

$$\neg\varphi := \neg\varphi, \quad \varphi \to \psi := \to \varphi\psi.$$

Atenție: $\neg$ și $\to$ reprezintă obiecte complet diferite în stânga și în dreapta respectivelor ecuații – anume, în stânga este vorba de operația pe care o definim acum, iar în dreapta este vorba de simbolul fixat mai devreme. Ele sunt însă utilizate în contexte destul de asemănătoare cât să folosim același semn grafic.

De asemenea, putem defini operațiile derivate $\wedge$, $\vee$ și $\leftrightarrow: E(Q)^2 \to E(Q)$ luând inspirație de la legile pe care le respectă $\wedge$, $\vee$, respectiv $\leftrightarrow$, i.e., pentru orice φ, $\psi \in E(Q)$, prin

$$\varphi \wedge \psi := \neg(\varphi \to \neg\psi), \quad \varphi \vee \psi := (\neg\varphi) \to \psi,$$

$$\varphi \leftrightarrow \psi := (\varphi \to \psi) \wedge (\psi \to \varphi).$$

Principiul recursiei pe formule

Principiul recursiei pe formule

Fie A o mulțime și $G_0 : Q \to A$, $G_\neg : A \to A$, $G_\to : A^2 \to A$. Atunci există și este unică $F : E(Q) \to A$ astfel încât:

- pentru orice $v \in Q$, $F(v) = G_0(v)$;
- pentru orice $\varphi \in E(Q)$, $F(\neg\varphi) = G_\neg(F(\varphi))$;
- pentru orice φ, $\psi \in E(Q)$, $F(\varphi \to \psi) = G_\to(F(\varphi), F(\psi))$.

Demonstrație

Unicitatea rezultă imediat prin inducție structurală (exercițiu!). Pentru existență, vom construi $S \subseteq E(Q) \times A$ astfel încât să verifice:

- pentru orice $v \in Q$, $(v, G_0(v)) \in S$;
- pentru orice $\varphi \in E(Q)$ și $a \in A$ cu $(\varphi, a) \in S$, avem $(\neg\varphi, G_\neg(a)) \in S$;
- pentru orice φ, $\psi \in E(Q)$ și a, $b \in A$ cu $(\varphi, a) \in S$ și $(\psi, b) \in S$, avem $(\varphi \to \psi, G_\to(a, b)) \in S$,

și să fie cea mai mică cu aceste proprietăți – ca mai înainte, o construim luând intersecția, la care participă $E(Q) \times A$, a tuturor submulțimilor ce verifică proprietățile.

Rămâne de arătat că S este grafic între $E(Q)$ și A – atunci, clar, $F := (E(Q), A, S)$ va fi funcția căutată.

Principiul recursiei pe formule

Demonstrație (cont.)

Trebuie să arătăm că pentru orice $\varphi \in E(Q)$ există și este unic $a \in A$ cu $(\varphi, a) \in S$. Existența rezultă prin inducție structurală (exercițiu!), astfel că vom demonstra în continuare unicitatea.

Fie B mulțimea acelor $\varphi \in E(Q)$ cu proprietatea că există și este unic $a \in A$ cu $(\varphi, a) \in S$. Presupunem prin absurd că $B \neq E(Q)$. Atunci, din contrapusa principiului de inducție pe formule, avem că fie $Q \not\subseteq B$, fie există $\varphi_0 \in B$ cu $\neg\varphi_0 \notin B$, fie există φ_0, $\psi_0 \in B$ cu $\varphi_0 \to \psi_0 \notin B$. Ultimul caz este cel mai complex și de aceea îl vom demonstra doar pe acela, primele două rămânând ca exercițiu.

Presupunem, deci, că avem φ_0, $\psi_0 \in B$ cu $\varphi_0 \to \psi_0 \notin B$. Cum φ_0, $\psi_0 \in B$, există și sunt unice a_0, b_0 cu $(\varphi_0, a_0) \in S$ și $(\psi_0, b_0) \in S$, deci avem $(\varphi_0 \to \psi_0, G_\to(a_0, b_0)) \in S$. Cum $\varphi_0 \to \psi_0 \notin B$, există $q \neq G_\to(a_0, b_0)$ cu $(\varphi_0 \to \psi_0, q) \in S$.

Principiul recursiei pe formule

Demonstrație (cont.)

Iau $T := S \setminus \{(\varphi_0 \to \psi_0, q)\}$. Vom arăta că T verifică cele trei proprietăți, ceea ce va contrazice faptul că S este cea mai mică asemenea mulțime.

Fie $v \in Q$. Atunci $(v, G_0(v)) \in S$, iar cum $(v, G_0(v)) \neq (\varphi_0 \to \psi_0, q)$, avem $(v, G_0(v)) \in T$. Cea de-a doua proprietate se arată analog.

Pentru a treia, fie φ, $\psi \in E(Q)$ și a, $b \in A$ cu $(\varphi, a) \in T$ și $(\psi, b) \in T$. Vrem $(\varphi \to \psi, G_\to(a, b)) \in T$.

Cum $(\varphi, a) \in S$ și $(\psi, b) \in S$, avem $(\varphi \to \psi, G_\to(a, b)) \in S$. Dacă $(\varphi \to \psi, G_\to(a, b)) \notin T$, înseamnă că $(\varphi \to \psi, G_\to(a, b)) = (\varphi_0 \to \psi_0, q)$, deci $\varphi \to \psi = \varphi_0 \to \psi_0$ și $G_\to(a, b) = q$.

Demonstrație (cont.)

Cum $\varphi \to \psi = \varphi_0 \to \psi_0$, din Proprietatea de citire unică avem $\varphi = \varphi_0$ și $\psi = \psi_0$. Cum $\varphi = \varphi_0$, $(\varphi_0, a) = (\varphi, a) \in S$. Dar cum $(\varphi_0, a_0) \in S$ și $\varphi_0 \in B$, avem $a = a_0$. Analog, $b = b_0$. Deci $q = G_\to(a, b) = G_\to(a_0, b_0)$, contradicție cu presupunerea inițială $q \neq G_\to(a_0, b_0)$.

Demonstrația este acum încheiată.

Mulțimea variabilelor

Corolar

Există și este unică $Var : E(Q) \to \mathcal{P}(Q)$ astfel încât:

- pentru orice $v \in Q$, $Var(v) = \{v\}$;
- pentru orice $\varphi \in E(Q)$, $Var(\neg\varphi) = Var(\varphi)$;
- pentru orice $\varphi, \psi \in E(Q)$, $Var(\varphi \to \psi) = Var(\varphi) \cup Var(\psi)$.

De exemplu, $Var(\neg v_0 \to v_1) = Var(\neg v_0) \cup Var(v_1) = Var(v_0) \cup Var(v_1) = \{v_0\} \cup \{v_1\} = \{v_0, v_1\}$.

Următorul enunț se arată prin inducție structurală.

Corolar

Pentru orice $\varphi \in E(Q)$, $Var(\varphi)$ este finită.

Observăm și că pentru orice $\varphi \in E(Q)$, $\varphi \in E(Var(\varphi))$.

Evaluarea formulelor

Corolar

Fie $e : Q \to 2$. Atunci există și este unică $e^+ : E(Q) \to 2$ astfel încât:

- pentru orice $v \in Q$, $e^+(v) = e(v)$;
- pentru orice $\varphi \in E(Q)$, $e^+(\neg\varphi) = \neg e^+(\varphi)$;
- pentru orice $\varphi, \psi \in E(Q)$, $e^+(\varphi \to \psi) = e^+(\varphi) \to e^+(\psi)$.

Corolar

Fie $e : Q \to 2$ și $\varphi, \psi \in E(Q)$. Atunci:

- $e^+(\varphi \wedge \psi) = e^+(\varphi) \wedge e^+(\psi)$;
- $e^+(\varphi \vee \psi) = e^+(\varphi) \vee e^+(\psi)$;
- $e^+(\varphi \leftrightarrow \psi) = e^+(\varphi) \leftrightarrow e^+(\psi)$.

Semnul $\models$

Vom introduce acum semnul $\models$, care va avea un număr foarte mare de semnificații pe parcursul cursului.

Definiție

- Fie $e : Q \to 2$ și $\varphi \in E(Q)$. Spunem că e **satisface** φ sau că e este **model** pentru φ și notăm $e \models \varphi$ dacă $e^+(\varphi) = 1$. Mulțimea modelelor unei formule φ se notează cu $Mod(\varphi)$.
- Fie $\varphi \in E(Q)$. Spunem că φ este **tautologie** și scriem $\models \varphi$ dacă pentru orice e, $e \models \varphi$, i.e. dacă $Mod(\varphi) = 2^Q$.
- Spunem că $\varphi \in E(Q)$ este **satisfiabilă** dacă există e cu $e \models \varphi$, i.e. dacă $Mod(\varphi) \neq \emptyset$.
- Spunem că o formulă φ este **nesatisfiabilă** dacă φ nu este satisfiabilă, i.e. dacă $Mod(\varphi) = \emptyset$.
- Fie φ, $\psi \in E(Q)$. Spunem că din φ **se deduce semantic** ψ și scriem $\varphi \models \psi$ dacă pentru orice e cu $e \models \varphi$ avem $e \models \psi$, i.e. dacă $Mod(\varphi) \subseteq Mod(\psi)$.

Tautologii și formule nesatisfiabile

Propoziție

Fie $\varphi \in E(Q)$. Atunci:

- φ este tautologie dacă și numai dacă $\neg\varphi$ este nesatisfiabilă;
- φ este nesatisfiabilă dacă și numai dacă $\neg\varphi$ este tautologie.

Implicația formală vs. implicația materială

Propoziție

Fie φ, $\psi \in E(Q)$. Atunci $\varphi \models \psi$ dacă și numai dacă $\models \varphi \to \psi$.

Demonstrație

Avem:

$$
\begin{aligned}
\varphi \models \psi &\Leftrightarrow \text{pentru orice } e : Q \to 2 \text{ cu } e \models \varphi,\ e \models \psi \\
&\Leftrightarrow \text{pentru orice } e : Q \to 2 \text{ cu } e^{+}(\varphi) = 1,\ e^{+}(\psi) = 1 \\
&\Leftrightarrow \text{pentru orice } e : Q \to 2,\ e^{+}(\varphi) \leq e^{+}(\psi) \\
&\Leftrightarrow \text{pentru orice } e : Q \to 2,\ e^{+}(\varphi) \boldsymbol{\to} e^{+}(\psi) = 1 \\
&\Leftrightarrow \text{pentru orice } e : Q \to 2,\ e^{+}(\varphi \to \psi) = 1 \\
&\Leftrightarrow \text{pentru orice } e : Q \to 2,\ e \models \varphi \to \psi \\
&\Leftrightarrow\ \models \varphi \to \psi.
\end{aligned}
$$

Mulțimi diferite de variabile

Până acum, am lucrat cu o mulțime fixă de variabile Q. Este interesant de văzut ce se întâmplă atunci când considerăm aceeași formulă ca făcând parte din mulțimile enunțurilor peste două mulțimi de variabile diferite.

Propoziție

Fie $Q' \subseteq Q$, deci $E(Q') \subseteq E(Q)$. Fie $f \in 2^Q$ și $e := f_{|Q'}$. Atunci, pentru orice $\chi \in E(Q')$, $e^+(\chi) = f^+(\chi)$.

Demonstrație

Demonstrăm prin inducție structurală după φ. Dacă $\varphi \in Q'$, atunci $e^+(\chi) = e(\chi) = f(\chi) = f^+(\chi)$. Dacă există $\varphi \in E(Q')$ cu $\chi = \neg\varphi$, din ipoteza de inducție avem $e^+(\varphi) = f^+(\varphi)$. Atunci

$$e^+(\chi) = e^+(\neg\varphi) = \neg e^+(\varphi) = \neg f^+(\varphi) = f^+(\neg\varphi) = f^+(\chi).$$

Cazul implicației rămâne ca exercițiu.

Evaluări ce coincid pe variabilele formulei

Corolar

Fie e_1, $e_2 \in 2^Q$ și $\varphi \in E(Q)$. Presupunem că pentru orice $v \in Var(\varphi)$, $e_1(v) = e_2(v)$. Atunci $e_1^+(\varphi) = e_2^+(\varphi)$.

Demonstrație

Notăm $Q' := Var(\varphi)$. Atunci $\varphi \in E(Q') \subseteq E(Q)$. Notăm $e := e_{1|Q'} = e_{2|Q'}$. Atunci, folosind propoziția anterioară,

$$e_1^+(\varphi) = e^+(\varphi) = e_2^+(\varphi).$$

Definiție

Fie I o mulțime. O **funcție booleană** peste I este o funcție de la 2^I la 2.

Avem că $\neg$ este o funcție booleană peste 1, iar $\rightarrow$, $\wedge$, $\vee$, $\leftrightarrow$ sunt funcții boolene peste 2. Orice $\varphi \in E(Q)$ determină o funcție booleană $F_\varphi : 2^Q \to 2$, definită, pentru orice $e \in 2^Q$, prin $F_\varphi(e) := e^+(\varphi)$. Obținem așadar o funcție

$$\Psi : E(Q) \to 2^{2^Q}$$

definită, pentru orice $\varphi \in E(Q)$, prin $\Psi(\varphi) := F_\varphi$.

Vom arăta că dacă Q este **finită**, atunci Ψ este surjectivă, i.e. orice funcție booleană provine dintr-o formulă. Aceasta ne va arăta lucrul pe care ni l-am propus mai devreme, i.e. faptul că $\neg$ și $\to$ sunt suficienți.

Q infinită

Mai întâi, însă, să vedem că acest enunț este fals atunci când Q este infinită, i.e. atunci există $G \in 2^{2^Q}$ astfel încât pentru orice φ, $G \neq F_\varphi$. Definim G, pentru orice $e \in 2^Q$, prin:

$$G(e) = 1 :\Leftrightarrow \{v \in Q \mid e(v) = 1\} \text{ este infinită.}$$

Presupunem că există φ cu $G = F_\varphi$. Definim $e_0 : Q \to 2$, pentru orice $v \in Q$, prin

$$e_0(v) := \begin{cases} 1, & \text{dacă } v \in Var(\varphi), \\ 0, & \text{dacă } v \notin Var(\varphi). \end{cases}$$

Definim $e_1 : Q \to 2$ ca fiind funcția constantă 1. Cum $Var(\varphi)$ este finită, avem $G(e_0) = 0$ și, cum Q este infinită, $G(e_1) = 1$, deci $0 = F_\varphi(e_0) = e_0^+(\varphi)$ și $1 = F_\varphi(e_1) = e_1^+(\varphi)$. Însă, pentru orice $v \in Var(\varphi)$, $e_0(v) = e_1(v) = 1$, deci $e_0^+(\varphi) = e_1^+(\varphi)$, contradicție.

Q finită

Acum arătăm că dacă Q este finită, pentru orice $G \in 2^{2^Q}$ există φ cu $G = F_\varphi$. Demonstrăm prin inducție după cardinalul lui Q. Cum Q este nevidă, primul pas va fi acela când putem scrie $Q = \{v_0\}$.

În acest caz $2^Q = \{e_0, e_1\}$, unde $e_0(v_0) = 0$ și $e_1(v_0) = 1$. Așadar 2^{2^Q} va avea patru elemente și anume:

	G_0	G_1	G_2	G_3
e_0	0	0	1	1
e_1	0	1	0	1

Se observă acum (exercițiu!) că $G_0 = F_{\neg(v_0 \to v_0)}$, $G_1 = F_{v_0}$, $G_2 = F_{\neg v_0}$, $G_3 = F_{v_0 \to v_0}$.

Presupunem, acum, că există $n \neq 0$ cu $Q = \{v_0, \ldots, v_n\}$. Notăm $Q' := \{v_i \mid i < n\}$, iar pentru orice $e \in 2^{Q'}$, definim e^0, $e^1 \in 2^Q$ ce prelungesc pe e, cu $e^0(v_n) = 0$ și $e^1(v_n) = 1$.

Fie $G : 2^Q \to 2$. Definim G_0, $G_1 : 2^{Q'} \to 2$, pentru orice $e \in 2^{Q'}$, prin $G_0(e) := G(e^0)$ și $G_1(e) := G(e^1)$. Din ipoteza de inducție, există φ_0, $\varphi_1 \in E(Q')$ cu $G_0 = F_{\varphi_0}$ și $G_1 = F_{\varphi_1}$. Notăm $\varphi := (\neg v_n \to \varphi_0) \wedge (v_n \to \varphi_1)$. Vom arăta că $F_\varphi = G$.

Fie $f \in 2^Q$ și presupunem w.l.o.g. că $f(v_n) = 0$. Notăm $e := f_{|Q'}$ și deci $f = e^0$, iar $e^+(\varphi_0) = f^+(\varphi_0)$. Atunci am terminat, deoarece avem, pe de o parte,

$$F_\varphi(f) = f^+(\varphi) = (1 \to f^+(\varphi_0)) \wedge (0 \to f^+(\varphi_1)) = f^+(\varphi_0),$$

iar, pe de alta,

$$G(f) = G(e^0) = G_0(e) = F_{\varphi_0}(e) = e^+(\varphi_0) = f^+(\varphi_0).$$

Echivalența semantică

Pentru orice φ, $\psi \in E(Q)$, spunem că φ și ψ sunt **echivalente semantic** – și notăm $\varphi \sim \psi$ sau $\varphi \mathrel{\text{⫤}\!\!\models} \psi$ – dacă pentru orice $e \in 2^Q$ avem $e^+(\varphi) = e^+(\psi)$ sau, altfel spus, dacă $F_\varphi = F_\psi$, sau, încă, dacă $Mod(\varphi) = Mod(\psi)$.

Avem că $\sim$ este o relație de echivalență (exercițiu!), iar astfel putem defini o funcție $\widetilde{\Psi} : E(Q)/\sim \to 2^{2^Q}$, punând, pentru orice $\varphi \in E(Q)$,

$$\widetilde{\Psi}(\widehat{\varphi}) := \Psi(\varphi) = F_\varphi,$$

care este injectivă.

Dat fiind că atunci când Q este finită, $\widetilde{\Psi}$ este și surjectivă, obținem următorul rezultat.

Corolar

Dacă Q este finită, $|E(Q)/\sim| = 2^{2^{|Q|}}$.

Cardinalul lui $E(Q)$

Dacă Q este cel mult numărabilă, se arată ușor (exercițiu!) că $E(Q)$ este numărabilă. Următoarele propoziții ne oferă un răspuns pentru cazul când Q este o mulțime infinită oarecare.

Propoziție

Fie A o mulțime infinită. Atunci $|\mathrm{Seq}(A)| = |A|$.

Demonstrație

Avem $|\mathrm{Seq}(A)| = |\bigcup_{n\in\mathbb{N}} A^n| \leq |\mathbb{N}| \cdot |A| = |A|$.

Propoziție

Dacă Q este infinită, $|E(Q)| = |Q|$.

Demonstrație

Avem $Q \subseteq E(Q) \subseteq \mathrm{Seq}(S(Q))$ și deci
$|Q| \leq |E(Q)| \leq |\mathrm{Seq}(S(Q))| = |S(Q)| = |Q|$.

Două notații

Pentru orice $v \in Q$ și $e : Q \to 2$, vom defini

$$v^e := \begin{cases} v, & \text{dacă } e(v) = 1, \\ \neg v, & \text{dacă } e(v) = 0, \end{cases}$$

și, clar, $e^+(v^e) = 1$. În plus, pentru orice $W \subseteq Q$ și $e : Q \to 2$, notăm $W^e := \{v^e \mid v \in W\}$.

De asemenea, fixăm o variabilă v (de exemplu, dacă are deja sens v_0, punem $v := v_0$) și notăm $\bot := \neg(v \to v)$. Atunci, clar, pentru orice $e : Q \to 2$, avem $e \not\models \bot$, i.e. $\bot$ este nesatisfiabilă.

Mulțimi de formule

Vom introduce acum alte semnificații ale lui $\models$.

Fie $\Gamma \subseteq E(Q)$. Pentru orice $e : Q \to 2$, spunem că e **satisface** Γ sau că e este **model** pentru Γ, și scriem $e \models \Gamma$, dacă pentru orice $\varphi \in \Gamma$, $e \models \varphi$. Mulțimea modelelor lui Γ se notează cu $Mod(\Gamma)$.

Spunem că Γ este **satisfiabilă** dacă există e cu $e \models \Gamma$, i.e. dacă $Mod(\Gamma) \neq \emptyset$, și că este **nesatisfiabilă** dacă nu este satisfiabilă, i.e. dacă $Mod(\Gamma) = \emptyset$.

Observăm că, pentru orice $e : Q \to 2$ și $\varphi \in E(Q)$, $e \models \{\varphi\}$ dacă și numai dacă $e \models \varphi$.

O mulțime se numește **finit satisfiabilă** dacă orice submulțime finită a sa este satisfiabilă.

Leme

Lemă

Fie $\Gamma \subseteq E(Q)$, $\Delta \subseteq \Gamma$ și $e \in Mod(\Gamma)$. Atunci $e \in Mod(\Delta)$.

Demonstrație

Fie $\varphi \in \Delta$. Atunci $\varphi \in \Gamma$ și deci $e \models \varphi$.

Corolar

Fie $\Gamma \subseteq E(Q)$ și $\Delta \subseteq \Gamma$ nesatisfiabilă. Atunci Γ este nesatisfiabilă.

Lemă

Fie $\Gamma \subseteq E(Q)$ și $e : Q \to 2$. Atunci $e \models \Gamma$ dacă și numai dacă pentru orice $\Delta \subseteq \Gamma$ finită, $e \models \Delta$.

Demonstrație

Implicația „$\Rightarrow$" este dată de prima lemă. Pentru „$\Leftarrow$", fie $\varphi \in \Gamma$. Atunci $\{\varphi\} \subseteq \Gamma$ finită, deci $e \models \{\varphi\}$, i.e. $e \models \varphi$.

Deducție semantică din mulțimi

Fie $\Gamma \subseteq E(Q)$ și $\varphi \in E(Q)$. Spunem că din Γ **se deduce semantic** φ și scriem $\Gamma \models \varphi$ dacă pentru orice e cu $e \models \Gamma$ avem $e \models \varphi$, i.e. dacă $Mod(\Gamma) \subseteq Mod(\varphi)$.

Se observă că, pentru orice $\varphi \in E(Q)$, avem $\emptyset \models \varphi$ dacă și numai dacă $\models \varphi$, iar pentru orice $\varphi, \psi \in E(Q)$, $\{\varphi\} \models \psi$ dacă și numai dacă $\varphi \models \psi$.

Lemă

Fie $\Gamma \subseteq E(Q)$, $\Delta \subseteq \Gamma$ și $\varphi \in E(Q)$ cu $\Delta \models \varphi$. Atunci $\Gamma \models \varphi$.

Demonstrație

Fie e cu $e \models \Gamma$. Cum $\Delta \subseteq \Gamma$, $e \models \Delta$, deci $e \models \varphi$.

Lemă

Fie $\Gamma \subseteq E(Q)$. Atunci Γ este nesatisfiabilă dacă și numai dacă $\Gamma \models \bot$.

Demonstrație

Pentru „$\Rightarrow$", fie e cu $e \models \Gamma$. Dar aceasta este imposibil, în particular $e \models \bot$. Pentru „$\Leftarrow$", presupunem că Γ este satisfiabilă și fie e un model al său. Atunci $e \models \bot$, contradicție!

Lemă

Fie $\Gamma \subseteq E(Q)$ și $\varphi \in E(Q)$. Atunci $\Gamma \models \varphi$ dacă și numai dacă $\Gamma \cup \{\neg\varphi\}$ este nesatisfiabilă.

Demonstrație

Pentru „$\Rightarrow$", fie $e \models \Gamma \cup \{\neg\varphi\}$. Atunci $e \models \Gamma$ și deci $e \models \varphi$, contradicție cu $e \models \neg\varphi$. Pentru „$\Leftarrow$", fie $e \models \Gamma$. Dacă $e \not\models \varphi$, atunci $e \models \neg\varphi$ și deci $e \models \Gamma \cup \{\neg\varphi\}$, contradicție!

Teorema deducției semantice

Propoziție

Fie $\Gamma \subseteq E(Q)$ și $\varphi, \psi \in E(Q)$. Atunci $\Gamma \cup \{\varphi\} \models \psi$ dacă și numai dacă $\Gamma \models \varphi \to \psi$.

Demonstrație

$$
\begin{aligned}
\Gamma \cup \{\varphi\} \models \psi &\Leftrightarrow \text{pentru orice } e \models \Gamma \cup \{\varphi\},\ e \models \psi \\
&\Leftrightarrow \text{pentru orice } e \text{ cu } e \models \Gamma \text{ și } e \models \varphi,\ e \models \psi \\
&\Leftrightarrow \text{pentru orice } e \models \Gamma,\ e \models \varphi \text{ implică } e \models \psi \\
&\Leftrightarrow \text{pentru orice } e \models \Gamma,\ e^+(\varphi) = 1 \text{ implică } e^+(\psi) = 1 \\
&\Leftrightarrow \text{pentru orice } e \models \Gamma,\ e^+(\varphi) \leq e^+(\psi) \\
&\Leftrightarrow \text{pentru orice } e \models \Gamma,\ e^+(\varphi) \boldsymbol{\to} e^+(\psi) = 1 \\
&\Leftrightarrow \text{pentru orice } e \models \Gamma,\ e^+(\varphi \to \psi) = 1 \\
&\Leftrightarrow \text{pentru orice } e \models \Gamma,\ e \models \varphi \to \psi \\
&\Leftrightarrow \Gamma \models \varphi \to \psi.
\end{aligned}
$$

Teorema de compacitate

Următorul rezultat este central în ceea ce privește deducția semantică din mulțimi de formule.

Teorema de compacitate – versiunea 1 (TK1)

Fie $\Gamma \subseteq E(Q)$ și $\varphi \in E(Q)$. Atunci $\Gamma \vDash \varphi$ dacă și numai dacă există $\Delta \subseteq \Gamma$ finită cu $\Delta \vDash \varphi$.

Rezultatul este exprimat uneori și sub următoarea formă.

Teorema de compacitate – versiunea 2 (TK2)

O mulțime de formule este satisfiabilă dacă și numai dacă este finit satisfiabilă.

Implicațiile triviale

Vom începe prin a arăta că fiecare dintre versiuni are o implicație care este imediată.

Teoremă (TK1$\Leftarrow$)

Fie $\Gamma \subseteq E(Q)$ și $\varphi \in E(Q)$. Presupunem că există $\Delta \subseteq \Gamma$ finită cu $\Delta \models \varphi$. Atunci $\Gamma \models \varphi$.

Demonstrație

Este un caz particular al unei leme precedente (unde nu aveam ipoteza de finitudine).

Teoremă (TK2$\Rightarrow$)

Fie $\Gamma \subseteq E(Q)$ satisfiabilă. Atunci Γ este finit satisfiabilă.

Demonstrație

Fie $\Delta \subseteq \Gamma$ finită. Cum Γ este satisfiabilă, există $e \models \Gamma$. Dar atunci $e \models \Delta$, deci Δ este satisfiabilă.

Echivalența dintre implicațiile netriviale

Următorul pas constă în a arăta că cele două implicații netriviale sunt echivalente între ele.

Teoremă – (TK1$\Rightarrow$) $\Rightarrow$ (TK2$\Leftarrow$)

Presupunem că pentru orice $\Gamma \subseteq E(Q)$ și $\varphi \in E(Q)$ cu $\Gamma \models \varphi$, există $\Delta \subseteq \Gamma$ finită cu $\Delta \models \varphi$. Atunci orice mulțime finit satisfiabilă este satisfiabilă.

Demonstrație

Fie Γ finit satisfiabilă. Presupunem că Γ este nesatisfiabilă. Atunci $\Gamma \models \bot$ și, deci, există $\Delta \subseteq \Gamma$ finită cu $\Delta \models \bot$. Dar atunci Δ este nesatisfiabilă, ceea ce contrazice faptul că Γ este finit satisfiabilă.

Echivalența dintre implicațiile netriviale

Teoremă – (TK2$\Leftarrow$) $\Rightarrow$ (TK1$\Rightarrow$)

Presupunem că orice mulțime finit satisfiabilă este satisfiabilă. Atunci, pentru orice $\Gamma \subseteq E(Q)$ și $\varphi \in E(Q)$ cu $\Gamma \models \varphi$, există $\Delta \subseteq \Gamma$ finită cu $\Delta \models \varphi$.

Demonstrație

Fie $\Gamma \subseteq E(Q)$ și $\varphi \in E(Q)$ cu $\Gamma \models \varphi$. Atunci $\Gamma \cup \{\neg\varphi\}$ este nesatisfiabilă și, deci, există $\Sigma \subseteq \Gamma \cup \{\neg\varphi\}$ finită nesatisfiabilă. Luăm $\Delta := \Sigma \cap \Gamma$. Clar, Δ este o submulțime finită a lui Γ. Rămâne de arătat că $\Delta \models \varphi$. Cum $\Sigma \subseteq \Gamma \cup \{\neg\varphi\}$, avem:

$$\begin{aligned}\Sigma &= \Sigma \cap (\Gamma \cup \{\neg\varphi\}) = (\Sigma \cap \Gamma) \cup (\Sigma \cap \{\neg\varphi\}) \\ &= \Delta \cup (\Sigma \cap \{\neg\varphi\}) \subseteq \Delta \cup \{\neg\varphi\}.\end{aligned}$$

Cum Σ este nesatisfiabilă, rezultă că și $\Delta \cup \{\neg\varphi\}$ este nesatisfiabilă, deci $\Delta \models \varphi$.

Ultraproduse

Ne mai rămâne de demonstrat oricare dintre acele implicații netriviale despre care am arătat că sunt echivalente. Instrumentul principal în acea demonstrație va fi conceptul de **ultraprodus**.

Fie I o mulțime nevidă și $e = (e_i)_{i \in I}$ o familie de evaluări (elemente ale lui 2^Q). Fie U un ultrafiltru pe I. Numim **ultraprodusul** lui e relativ la U funcția $e^U : Q \to 2$, definită, pentru orice $x \in Q$, prin

$$e^U(x) = 1 :\Leftrightarrow \{i \in I \mid e_i(x) = 1\} \in U.$$

Teorema fundamentală a ultraproduselor (Łoś)

Fie I o mulțime nevidă, $e = (e_i)_{i \in I}$ o familie de evaluări și U un ultrafiltru pe I. Atunci, pentru orice $\chi \in E(Q)$,

$$e^U \models \chi \Leftrightarrow \{i \in I \mid e_i \models \chi\} \in U.$$

Demonstrație

Demonstrăm prin inducție structurală după χ. Cazul $\chi \in Q$ este evident. Presupunem acum că există φ cu $\chi = \neg\varphi$. Atunci

$$\begin{aligned}
e^U \models \neg\varphi \Leftrightarrow e^U \not\models \varphi & \\
\Leftrightarrow \{i \in I \mid e_i \models \varphi\} \notin U & \qquad \text{(din ipoteza de inducție)} \\
\Leftrightarrow I \setminus \{i \in I \mid e_i \models \varphi\} \in U & \qquad (U \text{ fiind ultrafiltru}) \\
\Leftrightarrow \{i \in I \mid e_i \not\models \varphi\} \in U & \\
\Leftrightarrow \{i \in I \mid e_i \models \neg\varphi\} \in U. &
\end{aligned}$$

Teorema fundamentală a ultraproduselor

Demonstrație (cont.)

Presupunem acum că există φ, ψ cu $\chi = \varphi \to \psi$. Notăm $A_\varphi := \{i \in I \mid e_i \models \varphi\}$ și $A_\psi := \{i \in I \mid e_i \models \psi\}$. Atunci

$$\begin{aligned}
e^U \models \varphi \to \psi &\Leftrightarrow e^U \not\models \varphi \text{ sau } e^U \models \psi \\
&\Leftrightarrow A_\varphi \notin U \text{ sau } A_\psi \in U \\
&\qquad \text{(din ipoteza de inducție)} \\
&\Leftrightarrow I \setminus A_\varphi \in U \text{ sau } A_\psi \in U \\
&\qquad (U \text{ fiind ultrafiltru}) \\
&\Leftrightarrow (I \setminus A_\varphi) \cup A_\psi \in U \\
&\qquad (U \text{ fiind ultrafiltru}) \\
&\Leftrightarrow \{i \in I \mid e_i \not\models \varphi \text{ sau } e_i \models \psi\} \in U \\
&\Leftrightarrow \{i \in I \mid e_i \models \varphi \to \psi\} \in U.
\end{aligned}$$

Teorema fundamentală a ultraproduselor – versiunea 2

Fie I o mulțime nevidă, $e = (e_i)_{i \in I}$ o familie de evaluări și U un ultrafiltru pe I. Atunci, pentru orice $\Delta \subseteq E(Q)$ finită,

$$e^U \models \Delta \Leftrightarrow \{i \in I \mid e_i \models \Delta\} \in U.$$

Demonstrație

Demonstrăm prin inducție după cardinalul lui Δ. Dacă $\Delta = \emptyset$, atunci $e^U \models \Delta$ și avem $\{i \in I \mid e_i \models \Delta\} = I \in U$ (U fiind filtru).

Demonstrație (cont.)

Presupunem acum că există $n \in \mathbb{N}$ astfel încât $|\Delta| = n^+$ și luăm $\Gamma \subseteq E(Q)$ și $\varphi \in E(Q)$ cu $|\Gamma| = n$ și $\Delta = \Gamma \cup \{\varphi\}$. Atunci avem

$$
\begin{aligned}
e^U \models \Delta &\Leftrightarrow e^U \models \Gamma \text{ și } e^U \models \varphi \\
&\Leftrightarrow \{i \in I \mid e_i \models \Gamma\} \in U \text{ și } e^U \models \varphi \\
&\qquad \text{(din ipoteza de inducție)} \\
&\Leftrightarrow \{i \in I \mid e_i \models \Gamma\} \in U \text{ și } \{i \in I \mid e_i \models \varphi\} \in U \\
&\qquad \text{(din teorema fundamentală)} \\
&\Leftrightarrow \{i \in I \mid e_i \models \Gamma\} \cap \{i \in I \mid e_i \models \varphi\} \in U \\
&\qquad (U \text{ fiind filtru}) \\
&\Leftrightarrow \{i \in I \mid e_i \models \Gamma \text{ și } e_i \models \varphi\} \in U \\
&\Leftrightarrow \{i \in I \mid e_i \models \Delta\} \in U.
\end{aligned}
$$

Demonstrația teoremei de compactitate

Putem, acum, în sfârșit, demonstra teorema de compactitate.

Teoremă (TK2$\Leftarrow$)

Fie $\Gamma \subseteq E(Q)$ finit satisfiabilă. Atunci Γ este satisfiabilă.

Demonstrație

Fie $I := \mathcal{P}_{\text{fin}}(\Gamma) = \{\Delta \in \mathcal{P}(\Gamma) \mid \Delta \text{ finită}\}$. Cum $\emptyset \in I$, $I \neq \emptyset$. Pentru orice $\Delta \in I$, avem $Mod(\Delta) = \{e \in 2^Q \mid e \models \Delta\} \neq \emptyset$. Aplicăm Axioma alegerii pe familia $(Mod(\Delta))_{\Delta \in I}$ pentru a obține o familie de evaluări $(e_\Delta)_{\Delta \in I}$ astfel încât, pentru orice $\Delta \in I$, $e_\Delta \in Mod(\Delta)$, i.e. $e_\Delta \models \Delta$.

Fie U un ultrafiltru pe I. Atunci $e^U \models \Gamma$ dacă și numai dacă pentru orice $\Sigma \in I$, $e^U \models \Sigma$ dacă și numai dacă pentru orice $\Sigma \in I$, $\{\Delta \in I \mid e_\Delta \models \Sigma\} \in U$. Notăm, pentru orice $\Sigma \in I$, $S_\Sigma := \{\Delta \in I \mid e_\Delta \models \Sigma\}$. Pentru a arăta că Γ este satisfiabilă, este suficient, deci, să găsim un ultrafiltru U ce include $\{S_\Sigma \mid \Sigma \in I\}$, i.e. să arătăm că $\{S_\Sigma \mid \Sigma \in I\}$ are proprietatea intersecțiilor finite.

Demonstrația teoremei de compactitate

Demonstrație (cont.)

Vom arăta chiar mai mult, anume că $\{S_\Sigma \mid \Sigma \in I\}$ are proprietatea **tare** a intersecțiilor finite, i.e. că:

- pentru orice $\Sigma \in I$, $S_\Sigma \neq \emptyset$;
- pentru orice $\Sigma_1, \Sigma_2 \in I$, există $\Sigma \in I$ cu $S_{\Sigma_1} \cap S_{\Sigma_2} = S_\Sigma$.

Prima proprietate este imediată, dat fiind că, pentru orice $\Sigma \in I$, $e_\Sigma \models \Sigma$, deci $\Sigma \in S_\Sigma$. Pentru a doua, fie $\Sigma_1, \Sigma_2 \in I$. Atunci $\Sigma_1 \cup \Sigma_2 \in I$ și avem

$$\begin{aligned} S_{\Sigma_1} \cap S_{\Sigma_2} &= \{\Delta \in I \mid e_\Delta \models \Sigma_1 \text{ și } e_\Delta \models \Sigma_2\} \\ &= \{\Delta \in I \mid e_\Delta \models \Sigma_1 \cup \Sigma_2\} = S_{\Sigma_1 \cup \Sigma_2}, \end{aligned}$$

deci putem lua $\Sigma := \Sigma_1 \cup \Sigma_2$. Demonstrația este, deci, încheiată.

A se observa că în această demonstrație, spre deosebire de cele care au precedat-o, s-a folosit Axioma alegerii (de două ori: o dată explicit și o dată via Teorema de existență a ultrafiltrului).

O aplicație a teoremei de compactitate

Vom arăta acum un mod de a aplica această teoremă în afara logicii.

Numim **graf** (neorientat) o pereche (A, R) astfel încât R este o relație ireflexivă și simetrică pe A. Un graf (A, R) se numește **finit** dacă A este finită. Dacă (A, R) și (B, S) sunt grafuri, spunem că (B, S) este **subgraf** al lui (A, R) dacă $B \subseteq A$ și $S \subseteq R$. Dacă $k \in \mathbb{N}$, o k-**colorare** pe un graf (A, R) este o funcție $f : A \to k$ astfel încât pentru orice $x, y \in A$ cu xRy, avem $f(x) \neq f(y)$ – dacă există o asemenea funcție, spunem că (A, R) este k-**colorabil**.

Vom demonstra următorul rezultat.

Teoremă

Fie $k \in \mathbb{N}$. Atunci un graf este k-colorabil dacă și numai dacă orice subgraf finit al său este k-colorabil.

Implicația „$\Rightarrow$" este imediată: fie (A, R) un graf și fie (B, S) un subgraf finit al său. Atunci, dacă f este o k-colorare a lui (A, R), avem că $f_{|B}$ este o k-colorare a lui (B, S).

Demonstrăm implicația „$\Leftarrow$". Fie (A, R) un graf. Luăm Q astfel încât $Q \cap \{\neg, \rightarrow\} = \emptyset$ și $|Q| = |A \times k|$ (un asemenea Q există din propoziția demonstrată cu ajutorul Axiomei regularității). Fixăm o bijecție $q : A \times k \rightarrow Q$ și notăm, pentru orice $a \in A$ și $i \in k$, $q(a, i)$ cu $v_{a,i}$. Fie mulțimile:

$$\Gamma_1 := \{v_{a,0} \vee \ldots \vee v_{a,k-1} \mid a \in A\}$$
$$\Gamma_2 := \{v_{a,i} \rightarrow \neg v_{a,j} \mid a \in A, i, j \in k, i < j\}$$
$$\Gamma_3 := \{\neg(v_{a,i} \wedge v_{b,i}) \mid a, b \in A, aRb, i < k\}$$

și $\Gamma := \Gamma_1 \cup \Gamma_2 \cup \Gamma_3$.

Vom arăta că Γ este finit satisfiabilă. Atunci, din Teorema de compacitate, Γ este satisfiabilă și deci există $e \models \Gamma$. Se poate atunci defini o k-colorare $f : A \to k$, punând, pentru orice $a \in A$ și $i \in k$,

$$f(a) = i :\Leftrightarrow e(v_{a,i}) = 1.$$

Pentru a demonstra că Γ este finit satisfiabilă, fie $\Delta \subseteq \Gamma$ finită. Atunci

$$B := \{a \in A \mid \text{există } i < k, \varphi \in \Delta \text{ cu } v_{a,i} \in Var(\varphi)\}$$

este finită. Notăm $S := R \cap (B \times B)$. Atunci (B, S) este un subgraf finit al lui (A, R) și deci admite o k-colorare $g : B \to k$. Definim $e : Q \to 2$, punând, pentru orice $a \in B$ și $i \in k$,

$$e(v_{a,i}) = 1 :\Leftrightarrow g(a) = i,$$

iar pentru $a \notin B$ și $i \in k$, punem $e(v_{a,i}) := 1$. Atunci $e \models \Delta$.

Fie $\Gamma \subseteq E(Q)$. Definim mulțimea **consecințelor sintactice** ale lui Γ ca fiind cea mai mică submulțime A a lui $E(Q)$ ce verifică următoarele proprietăți (definiția are sens, v. „mulțimi Moore''):

- $\Gamma \subseteq A$;
- pentru orice φ, ψ, $\chi \in E(Q)$, avem:
  - (A1) $\varphi \to (\psi \to \varphi) \in A$;
  - (A2) $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi)) \in A$;
  - (A3) $(\neg\psi \to \neg\varphi) \to (\varphi \to \psi) \in A$;
- (MP) pentru orice φ, $\psi \in E(Q)$ cu $\varphi \in A$ și $\varphi \to \psi \in A$, avem $\psi \in A$.

Această mulțime tocmai definită se notează cu $Thm(\Gamma)$. Pentru orice $\varphi \in E(Q)$, spunem că din Γ **se deduce sintactic** φ și scriem $\Gamma \vdash \varphi$ dacă $\varphi \in Thm(\Gamma)$.

Prescurtările (A1)-(A3), (MP) semnifică *Axioma 1-3*, respectiv *Modus (Ponendo-)Ponens*.

Teoreme formale

Definim mulțimea **teoremelor formale** ca fiind cea mai mică submulțime A a lui $E(Q)$ ce verifică următoarele proprietăți (din nou, definiția are sens):

- pentru orice φ, ψ, $\chi \in E(Q)$, avem:
  - (A1) $\varphi \to (\psi \to \varphi) \in A$;
  - (A2) $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi)) \in A$;
  - (A3) $(\neg\psi \to \neg\varphi) \to (\varphi \to \psi) \in A$;
- (MP) pentru orice φ, $\psi \in E(Q)$ cu $\varphi \in A$ și $\varphi \to \psi \in A$, avem $\psi \in A$.

Această mulțime tocmai definită se notează cu Thm. Observăm că $Thm = Thm(\emptyset)$. Pentru orice $\varphi \in E(Q)$, notăm faptul că φ este teoremă formală (i.e. că $\varphi \in Thm = Thm(\emptyset)$, deci $\emptyset \vdash \varphi$) prin $\vdash \varphi$.

Acest mod de a defini deducția sintactică se numește îndeobște **sistem deductiv Hilbert**.

Inducție pe deducția sintactică

Precum în cazurile anterioare, modul de definire a mulțimii consecințelor sintactice conduce imediat la un principiu de inducție.

Principiul inducției pe deducția sintactică

Fie Γ, $B \subseteq E(Q)$ astfel încât:

- $\Gamma \subseteq B$;
- pentru orice φ, ψ, $\chi \in E(Q)$, avem:
  - $\varphi \to (\psi \to \varphi) \in B$;
  - $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi)) \in B$;
  - $(\neg\psi \to \neg\varphi) \to (\varphi \to \psi) \in B$;
- pentru orice φ, $\psi \in E(Q)$ cu $\varphi \in B$ și $\varphi \to \psi \in B$, avem $\psi \in B$.

Atunci $Thm(\Gamma) \subseteq B$.

Nu avem, însă, nimic analog proprietății de citire unică, ca urmare nu vom avea niciun principiu de recursie corespunzător.

Consecințe

Corolar

Fie $\Gamma, \Delta \subseteq E(Q)$ cu $\Gamma \subseteq \Delta$. Atunci $Thm(\Gamma) \subseteq Thm(\Delta)$, i.e. pentru orice $\varphi \in E(Q)$ cu $\Gamma \vdash \varphi$, avem $\Delta \vdash \varphi$.

Demonstrație

Se observă că $Thm(\Delta)$ satisface condițiile impuse pentru mulțimea B din enunțul Principiului inducției pe deducția sintactică.

Corolar

Fie $\Gamma \subseteq E(Q)$. Atunci $Thm \subseteq Thm(\Gamma)$, i.e. pentru orice $\varphi \in E(Q)$ cu $\vdash \varphi$, avem $\Gamma \vdash \varphi$.

$\vdash \varphi \to \varphi$

Propoziție

Pentru orice $\varphi \in E(Q)$, avem $\vdash \varphi \to \varphi$.

Demonstrație

(1) $\vdash (\varphi \to ((\varphi \to \varphi) \to \varphi)) \to ((\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi))$
(A2) (cu $\varphi \mapsto \varphi$, $\psi \mapsto \varphi \to \varphi$, $\chi \mapsto \varphi$)

(2) $\vdash \varphi \to ((\varphi \to \varphi) \to \varphi)$
(A1) (cu $\varphi \mapsto \varphi$, $\psi \mapsto \varphi \to \varphi$)

(3) $\vdash (\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)$
(MP): (1), (2)

(4) $\vdash \varphi \to (\varphi \to \varphi)$
(A1) (cu $\varphi \mapsto \varphi$, $\psi \mapsto \varphi$)

(5) $\vdash \varphi \to \varphi$
(MP): (3), (4)

Teorema deducției (sintactice)

Teorema deducției (sintactice)

Fie $\Gamma \subseteq E(Q)$ și $\varphi, \psi \in E(Q)$. Atunci $\Gamma \vdash \varphi \to \psi$ dacă și numai dacă $\Gamma \cup \{\varphi\} \vdash \psi$.

Demonstrație

Demonstrăm întâi „$\Rightarrow$”. Presupunem că $\Gamma \vdash \varphi \to \psi$. Atunci avem $\Gamma \cup \{\varphi\} \vdash \varphi \to \psi$. Cum $\varphi \in \Gamma \cup \{\varphi\}$, avem $\Gamma \cup \{\varphi\} \vdash \varphi$, deci obținem, aplicând (MP), că $\Gamma \cup \{\varphi\} \vdash \psi$.

Pentru „$\Leftarrow$”, fie $\Sigma := \{\psi \in E(Q) \mid \Gamma \vdash \varphi \to \psi\}$. Trebuie să demonstrăm că $Thm(\Gamma \cup \{\varphi\}) \subseteq \Sigma$. O vom face prin inducție pe deducția sintactică.

Teorema deducției (sintactice)

Demonstrație (cont.)

Fie $\psi \in \Gamma \cup \{\varphi\}$. Distingem două subcazuri. Dacă $\psi \in \Gamma$, atunci $\Gamma \vdash \psi$. Din (A1), avem $\Gamma \vdash \psi \rightarrow (\varphi \rightarrow \psi)$, iar aplicând (MP) obținem $\Gamma \vdash \varphi \rightarrow \psi$, deci $\psi \in \Sigma$. Dacă $\psi = \varphi$, atunci, din propoziția anterioară, avem $\vdash \varphi \rightarrow \varphi$, deci $\Gamma \vdash \varphi \rightarrow \psi$, deci, din nou, $\psi \in \Sigma$.

Cazurile corespunzătoare axiomelor se tratează exact ca subcazul „$\psi \in \Gamma$" de mai sus.

Rămâne cazul când avem $\psi \in \Sigma$ și $\psi \rightarrow \chi \in \Sigma$, deci avem $\Gamma \vdash \varphi \rightarrow \psi$, respectiv $\Gamma \vdash \varphi \rightarrow (\psi \rightarrow \chi)$, și vrem $\chi \in \Sigma$. Din (A2), avem

$$\Gamma \vdash (\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi)),$$

iar aplicând (MP) de două ori, obținem $\Gamma \vdash \varphi \rightarrow \chi$, i.e. $\chi \in \Sigma$.

Consecințe

Propoziție

Pentru orice φ, ψ, $\chi \in E(Q)$,

$$\vdash (\varphi \to \psi) \to ((\psi \to \chi) \to (\varphi \to \chi)).$$

Demonstrație

$$\begin{array}{lll}
(1) & \{\varphi \to \psi, \psi \to \chi, \varphi\} & \vdash \varphi \\
(2) & \{\varphi \to \psi, \psi \to \chi, \varphi\} & \vdash \varphi \to \psi \\
(3) & \{\varphi \to \psi, \psi \to \chi, \varphi\} & \vdash \psi \to \chi \\
(4) & \{\varphi \to \psi, \psi \to \chi, \varphi\} & \vdash \psi \qquad \text{(MP): (1), (2)} \\
(5) & \{\varphi \to \psi, \psi \to \chi, \varphi\} & \vdash \chi \qquad \text{(MP): (3), (4).}
\end{array}$$

Aplicând apoi Teorema deducției de trei ori, obținem:

$$\begin{array}{lll}
(6) & \{\varphi \to \psi, \psi \to \chi\} & \vdash \varphi \to \chi \\
(7) & \{\varphi \to \psi\} & \vdash (\psi \to \chi) \to (\varphi \to \chi) \\
(8) & & \vdash (\varphi \to \psi) \to ((\psi \to \chi) \to (\varphi \to \chi)).
\end{array}$$

Consecințe

Propoziție

Pentru orice $\Gamma \subseteq E(Q)$ și φ, ψ, $\chi \in E(Q)$ cu $\Gamma \vdash \varphi \to \psi$ și $\Gamma \vdash \psi \to \chi$, avem $\Gamma \vdash \varphi \to \chi$.

Demonstrație

Avem:

(1)	$\Gamma \vdash \varphi \to \psi$	Ipoteză
(2)	$\Gamma \vdash (\varphi \to \psi) \to ((\psi \to \chi) \to (\varphi \to \chi))$	Prop. precedentă
(3)	$\Gamma \vdash (\psi \to \chi) \to (\varphi \to \chi)$	(MP): (1), (2)
(4)	$\Gamma \vdash \psi \to \chi$	Ipoteză
(5)	$\Gamma \vdash \varphi \to \chi$	(MP): (3), (4).

Propoziție

Pentru orice $\Gamma \subseteq E(Q)$ și $\varphi \in E(Q)$ cu $\Gamma \cup \{\neg\varphi\} \vdash \bot$, avem $\Gamma \vdash \varphi$.

Demonstrație

Fie v acea variabilă în funcție de care s-a definit $\bot$ ca fiind $\neg(v \to v)$. Avem $\Gamma \cup \{\neg\varphi\} \vdash \neg(v \to v)$, deci:

(1)	$\Gamma \vdash \neg\varphi \to \neg(v \to v)$	T. deducției
(2)	$\Gamma \vdash (\neg\varphi \to \neg(v \to v)) \to ((v \to v) \to \varphi)$	(A3)
(3)	$\Gamma \vdash (v \to v) \to \varphi$	(MP): (1), (2)
(4)	$\Gamma \vdash v \to v$	Prop. ant.
(5)	$\Gamma \vdash \varphi$	(MP): (3), (4).

Rezultatele din următoarea propoziție se vor demonstra la seminar.

Propoziție

Fie $\varphi, \psi \in E(Q)$. Atunci avem:

- $\vdash \neg\psi \to (\psi \to \varphi)$;
- $\vdash \varphi \to \neg\neg\varphi$;
- $\vdash (\neg\varphi \to \varphi) \to \varphi$;
- $\vdash \psi \to (\neg\varphi \to \neg(\psi \to \varphi))$;
- $\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$.

Consecințe

Propoziție

Pentru orice $\Gamma \subseteq E(Q)$ și $\varphi, \psi \in E(Q)$ cu $\Gamma \cup \{\psi\} \vdash \varphi$ și $\Gamma \cup \{\neg\psi\} \vdash \varphi$, avem $\Gamma \vdash \varphi$.

Demonstrație

(1)	$\Gamma \cup \{\psi\}$	$\vdash \varphi$	Ipoteză
(2)	Γ	$\vdash \psi \to \varphi$	Teorema deducției
(3)	$\Gamma \cup \{\neg\psi\}$	$\vdash \varphi$	Ipoteză
(4)	Γ	$\vdash \neg\psi \to \varphi$	Teorema deducției
(5)	Γ	$\vdash (\psi \to \varphi) \to (\neg\varphi \to \neg\psi)$	Prop. precedentă
(6)	Γ	$\vdash \neg\varphi \to \neg\psi$	(MP): (2), (5)
(7)	Γ	$\vdash \neg\varphi \to \varphi$	P. ant.: (4), (6)
(8)	Γ	$\vdash (\neg\varphi \to \varphi) \to \varphi$	Prop. precedentă
(9)	Γ	$\vdash \varphi$	(MP): (7), (8).

Teorema de corectitudine

Apare acum problema firească de a determina legătura dintre semnele $\vdash$ și $\models$, dintre deducția sintactică și deducția semantică. Un prim răspuns este dat de următorul rezultat.

Teorema de corectitudine

Pentru orice $\Gamma \subseteq E(Q)$ și $\varphi \in E(Q)$ cu $\Gamma \vdash \varphi$, avem $\Gamma \models \varphi$.

Demonstrație

Fie $\Sigma := \{\varphi \in E(Q) \mid \Gamma \models \varphi\}$. Vom demonstra că $Thm(\Gamma) \subseteq \Sigma$ prin inducție pe deducția sintactică.

Dacă $\psi \in \Gamma$, atunci clar pentru orice e cu $e \models \Gamma$, avem că $e \models \psi$, deci $\Gamma \models \psi$, i.e. $\psi \in \Sigma$.

Cazurile corespunzătoare axiomelor rămân ca exercițiu.

Teorema de corectitudine

Demonstrație (cont.)

Rămâne cazul când avem $\psi \in \Sigma$ și $\psi \to \chi \in \Sigma$, deci avem $\Gamma \models \psi$, respectiv $\Gamma \models \psi \to \chi$, și vrem $\chi \in \Sigma$, i.e. $\Gamma \models \chi$. Fie e cu $e \models \Gamma$. Atunci $e \models \psi$, deci $e^+(\psi) = 1$, și $e \models \psi \to \chi$, deci

$$1 = e^+(\psi \to \chi) = e^+(\psi) \rightarrow e^+(\chi) = 1 \rightarrow e^+(\chi).$$

Rezultă că $e^+(\chi) = 1$, i.e. $e \models \chi$, ceea ce trebuia demonstrat.

Corolar

Pentru orice $\varphi \in E(Q)$ cu $\vdash \varphi$, avem $\models \varphi$.

Mulțimi consistente

Spunem că $\Gamma \subseteq E(Q)$ este **consistentă** dacă $\Gamma \nvdash \bot$, și **inconsistentă** dacă $\Gamma \vdash \bot$.

Observăm că $\{\bot\} \vdash \bot$, deci $\{\bot\}$ este inconsistentă și că $\bot \in E(Q)$, deci $E(Q) \vdash \bot$ și, prin urmare, $E(Q)$ este inconsistentă.

Presupunem că am avea $\vdash \bot$. Atunci Teorema de corectitudine ne spune că $\models \bot$. Luând $e \in 2^Q$ oarecare, obținem $e \models \bot$, contradicție. Așadar, $\emptyset \nvdash \bot$ și deci $\emptyset$ este consistentă.

Teorema de corectitudine – versiunea 2

Orice mulțime satisfiabilă este consistentă.

Demonstrație

Fie $\Gamma \subseteq E(Q)$ satisfiabilă. Atunci $\Gamma \not\models \bot$, deci $\Gamma \nvdash \bot$, i.e. Γ este consistentă.

O propoziție ajutătoare

Rezultatul care urmează arată o primă legătură în sens opus, de la $\models$ la $\vdash$.

Propoziție

Fie $e : Q \to 2$ și $\varphi \in E(Q)$. Atunci:

- dacă $e^+(\varphi) = 1$, atunci $Var(\varphi)^e \vdash \varphi$;
- dacă $e^+(\varphi) = 0$, atunci $Var(\varphi)^e \vdash \neg\varphi$.

Demonstrație

Demonstrăm prin inducție pe formule.

Fie $v \in Q$ și demonstrăm pentru $\varphi := v$. Atunci $Var(\varphi)^e = \{v^e\}$ și $e^+(v) = e(v)$. Dacă $e(v) = 1$, atunci $v^e = v$, deci $\{v^e\} \vdash v$. Dacă $e(v) = 0$, atunci $v^e = \neg v$, deci $\{v^e\} \vdash \neg v$.

O propoziție ajutătoare

Demonstrație (cont.)

Fie acum ψ o formulă pentru care este adevărată concluzia. Vom demonstra că este adevărată și pentru $\varphi := \neg\psi$. Avem $Var(\varphi) = Var(\psi)$, deci $Var(\varphi)^e = Var(\psi)^e$.

Dacă $e^+(\varphi) = 1$, atunci $e^+(\psi) = 0$, deci, conform ipotezei de inducție pentru ψ, $Var(\psi)^e \vdash \neg\psi$, adică $Var(\varphi)^e \vdash \varphi$.

Dacă $e^+(\varphi) = 0$, atunci $e^+(\psi) = 1$, deci, conform ipotezei de inducție pentru ψ, $Var(\psi)^e \vdash \psi$, adică $Var(\varphi)^e \vdash \psi$. Dintr-o propoziție anterioară, avem $\vdash \psi \to \neg\neg\psi$, deci putem aplica (MP) pentru a obține $Var(\varphi)^e \vdash \neg\neg\psi$, i.e. $Var(\varphi)^e \vdash \neg\varphi$.

O propoziție ajutătoare

Demonstrație (cont.)

Fie acum ψ, χ formule pentru care este adevărată concluzia. Vom demonstra că este adevărată și pentru $\varphi := \psi \to \chi$. Avem $Var(\varphi) = Var(\psi) \cup Var(\chi)$, deci $Var(\psi)^e \subseteq Var(\varphi)^e$ și $Var(\chi)^e \subseteq Var(\varphi)^e$.

Dacă $e^+(\psi \to \chi) = 0$, atunci $e^+(\psi) = 1$ și $e^+(\chi) = 0$. Din ipoteza de inducție pentru ψ și $Var(\psi)^e \subseteq Var(\varphi)^e$, avem $Var(\varphi)^e \vdash \psi$. Similar, avem $Var(\varphi)^e \vdash \neg\chi$. Dar dintr-o propoziție anterioară, avem $\vdash \psi \to (\neg\chi \to \neg(\psi \to \chi))$. Aplicând (MP) de două ori, obținem $Var(\varphi)^e \vdash \neg(\psi \to \chi)$, i.e. $Var(\varphi)^e \vdash \neg\varphi$, ceea ce trebuia demonstrat.

O propoziție ajutătoare

Demonstrație (cont.)

Dacă $e^+(\psi \to \chi) = 1$, atunci $e^+(\psi) = 0$ sau $e^+(\chi) = 1$.

În primul caz, obținem, din ipoteza de inducție pentru ψ, $Var(\psi)^e \vdash \neg\psi$. Dintr-o propoziție anterioară, avem $\vdash \neg\psi \to (\psi \to \chi)$, deci, aplicând (MP), avem $Var(\psi)^e \vdash \psi \to \chi$, deci $Var(\varphi)^e \vdash \psi \to \chi$.

În al doilea caz, obținem, din ipoteza de inducție pentru χ, $Var(\chi)^e \vdash \chi$. Din (A1), avem $\vdash \chi \to (\psi \to \chi)$, deci, aplicând (MP), avem $Var(\chi)^e \vdash \psi \to \chi$, deci $Var(\varphi)^e \vdash \psi \to \chi$.

Teorema de completitudine

Teorema de completitudine (slabă)

Pentru orice $\varphi \in E(Q)$ cu $\models \varphi$, avem $\vdash \varphi$.

Demonstrație

Fie φ o tautologie și $Var(\varphi) = \{x_1, \ldots, x_n\}$. Vom demonstra prin inducție după k proprietatea:

$$(*) \qquad \text{pentru orice } k \leq n, \text{ pentru orice } e : Q \to 2, \\ \{x_1^e, \ldots, x_{n-k}^e\} \vdash \varphi.$$

Pentru $k = n$, (*) ne va da $\vdash \varphi$.

Pentru $k = 0$, fie $e : Q \to 2$. Deoarece φ este tautologie, $e^+(\varphi) = 1$. Din propoziția anterioară, avem

$$Var(\varphi)^e = \{x_1^e, \ldots, x_n^e\} \vdash \varphi,$$

ceea ce trebuia demonstrat.

Demonstrație (cont.)

Presupunem acum că (*) este adevărată pentru un $k < n$ și fie $e : Q \to 2$. Trebuie să arătăm că $\{x_1^e, \ldots, x_{n-k-1}^e\} \vdash \varphi$. Considerăm evaluarea $f : Q \to 2$, definită pentru orice $v \neq x_{n-k}$, prin $f(v) := e(v)$, iar $f(x_{n-k}) := \neg e(x_{n-k})$. Rezultă că, pentru orice $i \in \{1, \ldots, n-k-1\}$, $x_i^f = x_i^e$ și

$$x_{n-k}^f = \begin{cases} \neg x_{n-k}, & \text{dacă } x_{n-k}^e = x_{n-k}, \\ x_{n-k}, & \text{dacă } x_{n-k}^e = \neg x_{n-k}. \end{cases}$$

Din (*) pentru e și f, obținem $\{x_1^e, \ldots, x_{n-k-1}^e, x_{n-k}\} \vdash \varphi$ și $\{x_1^e, \ldots, x_{n-k-1}^e, \neg x_{n-k}\} \vdash \varphi$. Aplicăm acum o propoziție anterioară pentru a concluziona că $\{x_1^e, \ldots, x_{n-k-1}^e\} \vdash \varphi$.

Teorema de completitudine medie

Pentru orice $\Delta \subseteq E(Q)$ **finită** și $\varphi \in E(Q)$ cu $\Delta \models \varphi$, avem $\Delta \vdash \varphi$.

Demonstrație

Demonstrăm prin inducție după cardinalul lui Δ. Cazul $|\Delta| = 0$, i.e. $\Delta = \emptyset$, este exact Teorema de completitudine slabă.

Presupunem acum că există $n \in \mathbb{N}$ astfel încât $|\Delta| = n^+$. Atunci există $\Gamma \subseteq E(Q)$ și $\psi \in E(Q)$ cu $|\Gamma| = n$ și $\Delta = \Gamma \cup \{\psi\}$. Cum $\Gamma \cup \{\psi\} \models \varphi$, avem $\Gamma \models \psi \to \varphi$. Din ipoteza de inducție, avem $\Gamma \vdash \psi \to \varphi$. Aplicând Teorema deducției, obținem $\Gamma \cup \{\psi\} \vdash \varphi$, i.e. $\Delta \vdash \varphi$.

Teorema de completitudine extinsă (tare)

Teorema de completitudine tare

Pentru orice $\Gamma \subseteq E(Q)$ și $\varphi \in E(Q)$ cu $\Gamma \models \varphi$, avem $\Gamma \vdash \varphi$.

Demonstrație

Din Teorema de compacitate, există $\Delta \subseteq \Gamma$ finită cu $\Delta \models \varphi$. Din Teorema de completitudine medie, avem $\Delta \vdash \varphi$, deci $\Gamma \vdash \varphi$.

Teorema de completitudine tare – versiunea 2

Orice mulțime consistentă este satisfiabilă.

Demonstrație

Fie $\Gamma \subseteq E(Q)$ consistentă. Atunci $\Gamma \nvdash \perp$, deci, din Teorema de completitudine tare, $\Gamma \not\models \perp$. Ca urmare, Γ este satisfiabilă.

A se observa (din nou) că numai în forma tare a Teoremei de completitudine s-a folosit Axioma alegerii (via apelul la Teorema de compacitate).

În unele cărți, prin Teorema de completitudine se înțelege enunțul cumulat al Teoremei de corectitudine și al Teoremei de completitudine tare.

Teorema de completitudine – sumar

- Pentru orice $\Gamma \subseteq E(Q)$ și $\varphi \in E(Q)$, avem

$$\Gamma \vdash \varphi \Leftrightarrow \Gamma \models \varphi.$$

- O mulțime este consistentă dacă și numai dacă este satisfiabilă.

Logica predicatelor

sau

Logica de ordinul I

Motto

"Predicate logic – funny you should mention that.

There is this incredibly toxic view of predicate logic that I first encountered in Good Old-Fashioned A[rtificial] I[ntelligence]. And then [there is] this entirely different, highly useful and precise view of the uses and bounds of logic that I encountered when I started studying mathematical logic and learned about things like model theory.

[...] I'm guessing that the GOFAI people made the terrible, horrible, no good, very bad mistake of getting their views of logic from the descendants of Bertrand Russell who still called themselves philosophers instead of those descendants who considered themselves part of the thriving edifice of mathematics."

– Eliezer Yudkowsky

După cum am spus și în Introducerea istorică, cealaltă abordare clasică studiată în liceu asupra logicii, pe lângă logica propozițiilor compuse (corespunzătoare în acest curs logicii propoziționale), a fost logica silogistică, unde întâlneam raționamente de genul următor:

$$\frac{\begin{array}{c}\textit{Toți iepurii au blană.}\\ \textit{Unele animale sunt iepuri.}\end{array}}{\textit{Deci, unele animale au blană.}}$$

Formalizarea clasică a argumentului de mai sus era:

$$\frac{\begin{array}{c}MaP\\ SiM\end{array}}{SiP}$$

Șirul format, *a*-*i*-*i*, dădea (printre altele) denumirea acestui tip de raționament: DARII.

Cuantificatori

Metode de a formaliza diverse aserțiuni s-au întâlnit și la materiile matematice – de pildă, folosirea cuantificatorilor. Puteam exprima faptul că într-un corp orice element nenul este inversabil prin:

$$\forall x(\neg(x = 0) \to \exists y(x \cdot y = 1)),$$

iar faptul că o relație de ordine admite un element maximal prin:

$$\exists x \forall y(x \leq y \to x = y).$$

Putem formaliza și argumentul prezentat anterior folosind cuantificatori, în felul următor:

$$\frac{\begin{array}{c}\forall x(I(x) \to B(x)) \\ \exists x(A(x) \land I(x))\end{array}}{\exists x(A(x) \land B(x))}$$

Aceste observații conduc la ideea de a defini un nou sistem logic, ce se va numi **logica predicatelor** sau **logica de ordinul I**, unde să avem la dispoziție cuantificatori și variabile, precum și simboluri prin care să exprimăm relații sau operații.

Deși logica propozițiilor compuse a fost prezentată în liceu ca o variantă mai dezvoltată a logicii silogistice (numită la acel moment și logica propozițiilor simple), observăm în exemplele anterioare că, dimpotrivă, logica propozițională, cu operatorii ei ca $\neg$, $\rightarrow$, este cea care va fi înglobată în acest sistem logic cuantificat.

Logica de ordinul I nu doar permite exprimarea riguroasă a enunțurilor de mai devreme (și, după cum am prefigurat, va putea exprima și axiomele teoriei mulțimilor), dar și, într-un anume sens precis (pe care nu îl vom detalia), este cel mai puternic sistem logic utilizabil practic – orice alt sistem mai puternic (cum ar fi, firește, logica de ordinul II) posedă neajunsuri esențiale.

Vom fixa patru obiecte $\neg$, $\rightarrow$, $\forall$, $=$, diferite două câte două și o mulțime numărabilă

$$V = \{x_0, x_1, \ldots\},$$

cu $V \cap \{\neg, \rightarrow, \forall, =\} = \emptyset$, ale cărei elemente le vom numi **variabile**.

Atenție, însă, aceste variabile **nu** au un rol analog simbolurilor propoziționale. Ne putem întreba, totuși, care este, într-adevăr, analogul acestora din urmă. Observăm că în logica propozițională, dacă schimbam mulțimea simbolurilor, obțineam și o altă mulțime de formule. Și aici, după cum am văzut în exemplele anterioare, avem nevoie de mulțimi de formule diferite pentru a vorbi despre domenii de discurs diferite. Ceea ce dădea diferența între acele domenii era faptul că se foloseau simboluri diferite pentru a exprima obiecte specifice lor, anume $\cdot$, 0, 1; $\leq$; respectiv I, A, B. (Anumite simboluri, ca $\rightarrow$, erau comune – precum în logica propozițională – și de aceea au fost fixate mai sus.)

Signaturi și structuri

Definim, așadar, o **signatură de ordinul I** ca fiind un triplet $\sigma = (F, R, r)$ astfel încât $F \cap R = \emptyset$, $(F \cup R) \cap (V \cup \{\neg, \rightarrow, \forall, =\}) = \emptyset$ și $r : F \cup R \rightarrow \mathbb{N}$.

Dacă $\sigma = (F, R, r)$ este o signatură de ordinul I, atunci numim elementele lui R **simbolurile de relație** ale lui σ, iar elementele lui F **simbolurile de funcție** ale lui σ; pentru orice $s \in F \cup R$, numim $r(s)$ **aritatea** lui s; în particular, acele $s \in F$ pentru care $r(s) = 0$ se numesc **constantele** lui σ. Mai definim și mulțimea

$$S_\sigma := \{\neg, \rightarrow, \forall, =\} \cup V \cup F \cup R.$$

Dacă $\sigma = (F, R, r)$ este o signatură de ordinul I, atunci o σ-**structură** va fi o pereche $(A, \{A_s\}_{s \in F \cup R})$, unde $A \neq \emptyset$ (și se va numi **universul**, **mulțimea suport** sau **mulțimea subiacentă** a structurii), pentru orice $s \in F$, $A_s : A^{r(s)} \rightarrow A$ și pentru orice $s \in R$, $A_s \subseteq A^{r(s)}$. Structurile vor reprezenta domeniile despre care vor vorbi formulele corespunzătoare signaturilor.

Exemple

Putem obține signaturile sugerate mai devreme dacă punem $\sigma := (F, R, r)$, iar F, R, r sunt, pe rând:

- $F = \{\cdot, 0, 1\}$, $R = \emptyset$, $r(\cdot) = 2$, $r(0) = r(1) = 0$ – atunci σ-structurile vor fi tuplurile $(A, \cdot, 0, 1)$ unde $\cdot : A^2 \to A$, iar 0, $1 \in A$, de exemplu $(\mathbb{Z}, +, 2, 7)$. Observăm că nu impunem în definiția structurii ca ea să respecte anumite legi, precum inversabilitatea de mai devreme – acest lucru se va face eventual ulterior, după ce vom defini riguros formulele și satisfacerea lor.
- $F = \emptyset$, $R = \{\leq\}$, $r(\leq) = 2$ – atunci σ-structurile vor fi perechi $(A, \leq)$ unde $\leq$ este o relație binară pe A, de exemplu $(\mathbb{N}, >)$.
- $F = \emptyset$, $R = \{I, A, B\}$, $r(I) = r(A) = r(B) = 1$.

Dacă punem $F = R = \emptyset$, atunci obținem o signatură care, dat fiind că singurele fapte pe care le vom putea exprima peste ea vor folosi semnul $=$, se va numi **signatura egalității**.

De asemenea, vom defini **signatura aritmeticii** ca fiind

$$\sigma_{ar} := (\{\dot{+}, \dot{\times}, \dot{S}, \dot{0}\}, \{\dot{<}\}, r),$$

unde $r(\dot{+}) = r(\dot{\times}) = r(\dot{<}) = 2$, $r(\dot{S}) = 1$, iar $r(\dot{0}) = 0$. Dacă definim funcția $S : \mathbb{N} \to \mathbb{N}$, pentru orice $n \in \mathbb{N}$, prin $S(n) := n^+$, iar

$$\mathcal{N} := (\mathbb{N}, (N_s)_{s \in F \cup R}),$$

unde $N_{\dot{+}} = +$, $N_{\dot{\times}} = \cdot$, $N_{\dot{S}} = S$, $N_{\dot{0}} = 0$, iar $N_{\dot{<}} =<$, avem că $\mathcal{N}$ este o σ_{ar}-structură.

De remarcat că există și alte σ_{ar}-structuri, de exemplu putem înzestra mulțimea 2 cu $\wedge$, $\vee$, $\neg$, 0 și $<$ pentru a obține o altă σ_{ar}-structură.

Reduse și expansiuni

Dacă $\sigma = (F, R, r)$ și $\sigma' = (F', R', r')$ sunt signaturi, spunem că $\sigma \leq \sigma'$ dacă $F \subseteq F'$, $R \subseteq R'$ și $r = r'_{|F \cup R}$. În această situație, dacă $\mathcal{A} = (A, (A_s)_{s \in F \cup R})$ este o σ-structură, iar $\mathcal{B} = (B, (B_s)_{s \in F' \cup R'})$ este o σ'-structură, spunem că $\mathcal{A}$ este **redusa** lui $\mathcal{B}$ la σ sau că $\mathcal{B}$ este o **expansiune** a lui $\mathcal{A}$ la σ' dacă $A = B$, iar pentru orice $s \in F \cup R$, $A_s = B_s$. Se observă că:

- Redusa oricărei σ'-structuri la σ există și este unică (de aceea am folosit articolul hotărât).
- Există mereu o expansiune a unei σ-structuri $\mathcal{A} = (A, (A_s)_{s \in F \cup R})$ la σ', obținută în felul următor: se fixează $a \in A \neq \emptyset$, simbolurilor de relație din $R' \setminus R$ li se asociază relații vide, iar simbolurilor de funcție din $F' \setminus F$ li se asociază funcții constante ce iau valoarea a.

Termeni

Formulele corespunzătoare unei signaturi $\sigma = (F, R, r)$ vor fi cuvinte peste alfabetul S_σ. Înainte de a defini formulele, va trebui să definim **termenii** (de pildă, $x \cdot y$ de mai devreme). Ei se definesc ca fiind cea mai mică mulțime $A \subseteq \mathrm{Seq}(S_\sigma)$ astfel încât:

- $V \subseteq A$;
- pentru orice $s \in F$ și orice $t_1, \ldots, t_{r(s)} \in A$, avem $st_1 \ldots t_{r(s)} \in A$ (în particular, dacă $r(s) = 0$, $s \in A$).

Mulțimea termenilor peste σ se va nota cu T_σ.

Principiul inducției pe termeni

Fie $B \subseteq T_\sigma$ astfel încât:

- $V \subseteq B$;
- pentru orice $s \in F$ și orice $t_1, \ldots, t_{r(s)} \in B$, avem $st_1 \ldots t_{r(s)} \in B$.

Atunci $B = T_\sigma$.

Principiul recursiei pe termeni

Fie A o mulțime și $G_0 : V \to A$, iar pentru orice $s \in F$, $G_s : A^{r(s)} \to A$. Atunci există și este unică $F : T_\sigma \to A$ astfel încât:

- pentru orice $x \in V$, $F(x) = G_0(x)$;
- pentru orice $s \in F$ și orice $t_1, \ldots, t_{r(s)} \in T_\sigma$, $F(st_1 \ldots t_{r(s)}) = G_s(F(t_1), \ldots, F(t_{r(s)}))$.

Mulțimea variabilelor unui termen

Ca exemplu, putem defini recursiv mulțimea variabilelor unui termen. Practic, definim funcția $Var : T_\sigma \to \mathcal{P}(V)$, prin:

- pentru orice $x \in V$, $Var(x) := \{x\}$;
- pentru orice $s \in F$ și orice $t_1, \ldots, t_{r(s)} \in T_\sigma$, $Var(st_1 \ldots t_{r(s)}) := Var(t_1) \cup \ldots \cup Var(t_{r(s)})$ (în particular, dacă $r(s) = 0$, $Var(s) = \emptyset$).

Evaluarea termenilor

Fie $\mathcal{A} = (A, (A_s)_{s \in F \cup R})$ o σ-structură. Atunci pentru orice $v : V \to A$ există și este unică o funcție $(\cdot)_v^{\mathcal{A}} : T_\sigma \to A$ astfel încât

- pentru orice $x \in V$, $x_v^{\mathcal{A}} = v(x)$;
- pentru orice $s \in F$ și orice $t_1, \ldots, t_{r(s)} \in T_\sigma$, $(st_1 \ldots t_{r(s)})_v^{\mathcal{A}} = A_s((t_1)_v^{\mathcal{A}}, \ldots, (t_{r(s)})_v^{\mathcal{A}})$ (în particular, dacă $r(s) = 0$, $s_v^{\mathcal{A}} = A_s$).

Atenție, din nou: funcția v din definiția de mai sus **nu** are un rol similar cu cel al funcțiilor $e : Q \to 2$ din logica propozițională, cu toate că ar putea părea astfel.

Lema de coincidență

Fie $\mathcal{A} = (A, (A_s)_{s \in F \cup R})$ o σ-structură, $v_1, v_2 : V \to A$ și $t \in T_\sigma$ astfel încât $v_{1|Var(t)} = v_{2|Var(t)}$. Atunci $t^{\mathcal{A}}_{v_1} = t^{\mathcal{A}}_{v_2}$.

Demonstrație

Demonstrăm prin inducție după termeni. Dacă $x \in V$, atunci $x \in \{x\} = Var(x)$ și deci $v_1(x) = v_2(x)$, i.e. $x^{\mathcal{A}}_{v_1} = x^{\mathcal{A}}_{v_2}$.

Fie acum $s \in F$ și $t_1, \ldots, t_{r(s)} \in T_\sigma$ ce verifică concluzia lemei. Fie $i \in \{1, \ldots, r(s)\}$. Atunci $Var(t_i) \subseteq Var(t)$ și deci $v_{1|Var(t_i)} = v_{2|Var(t_i)}$. Din ipoteza de inducție, avem $(t_i)^{\mathcal{A}}_{v_1} = (t_i)^{\mathcal{A}}_{v_2}$ și așadar:

$$\begin{aligned}
(st_1 \ldots t_{r(s)})^{\mathcal{A}}_{v_1} &= A_s((t_1)^{\mathcal{A}}_{v_1}, \ldots, (t_{r(s)})^{\mathcal{A}}_{v_1}) \\
&= A_s((t_1)^{\mathcal{A}}_{v_2}, \ldots, (t_{r(s)})^{\mathcal{A}}_{v_2}) \\
&= (st_1 \ldots t_{r(s)})^{\mathcal{A}}_{v_2}.
\end{aligned}$$

Formule

Fie $\sigma = (F, R, r)$ o signatură. Numim **formulă atomică** peste σ un șir de forma $= tu$, cu t, $u \in T_\sigma$ sau un șir de forma $st_1 \dots t_n$ cu $s \in R$, $n = r(s)$ și $t_1, \dots, t_n \in T_\sigma$. Mulțimea formulelor atomice peste σ se va nota cu Fa_σ. Mulțimea **formulelor** peste σ se definește ca fiind cea mai mică mulțime $A \subseteq \mathrm{Seq}(S_\sigma)$ astfel încât:

- formulele atomice aparțin lui A;
- dacă $\varphi \in A$, atunci $\neg\varphi \in A$;
- dacă φ, $\psi \in A$, atunci $\to \varphi\psi \in A$;
- dacă $\varphi \in A$ și $x \in V$, atunci $\forall x \varphi \in A$.

Mulțimea formulelor peste σ se va nota cu F_σ.

Notație infixată și conectori derivați

Vom folosi aceeași metodă pe care am folosit-o la logica propozițională pentru a putea nota formulele infixat – pentru orice $\varphi, \psi \in F_\sigma$, $\varphi \to \psi$ în loc de $\to \varphi\psi$, dar și, pentru orice $t, u \in T_\sigma$, $t = u$ în loc de $= tu$.

De asemenea, vom nota, ca mai înainte, pentru orice $\varphi, \psi \in F_\sigma$,

$$\varphi \wedge \psi := \neg(\varphi \to \neg\psi), \quad \varphi \vee \psi := (\neg\varphi) \to \psi,$$

$$\varphi \leftrightarrow \psi := (\varphi \to \psi) \wedge (\psi \to \varphi),$$

dar și, pentru orice $x \in V$ și $\varphi \in F_\sigma$,

$$\exists x\varphi := \neg\forall x\neg\varphi.$$

Inducție pe formule

Principiul inducției pe formule

Fie $B \subseteq F_\sigma$ astfel încât:

- formulele atomice aparțin lui B;
- dacă $\varphi \in B$, atunci $\neg\varphi \in B$;
- dacă $\varphi, \psi \in B$, atunci $\varphi \rightarrow \psi \in B$;
- dacă $\varphi \in B$ și $x \in V$, atunci $\forall x \varphi \in B$.

Atunci $B = F_\sigma$.

Recursie pe formule

Principiul recursiei pe formule

Fie A o mulțime și $G_0 : Fa_\sigma \to A$, $G_\neg : A \to A$, $G_\to : A^2 \to A$, $G_\forall : V \times A \to A$. Atunci există și este unică $F : F_\sigma \to A$ astfel încât:

- pentru orice $\varphi \in Fa_\sigma$, $F(\varphi) = G_0(\varphi)$;
- pentru orice $\varphi \in F_\sigma$, $F(\neg\varphi) = G_\neg(F(\varphi))$;
- pentru orice φ, $\psi \in F_\sigma$, $F(\varphi \to \psi) = G_\to(F(\varphi), F(\psi))$;
- pentru orice $\varphi \in F_\sigma$ și $x \in V$, $F(\forall x\varphi) = G_\forall(x, F(\varphi))$.

Mulțimea variabilelor libere ale unei formule

Ca exemplu, putem defini recursiv mulțimea variabilelor **libere** ale unei formule. Definim funcția $FV : F_\sigma \to \mathcal{P}(V)$, prin:

- pentru orice $t, u \in T_\sigma$, $FV(t = u) := Var(t) \cup Var(u)$;
- pentru orice $s \in R$ și orice $t_1, \ldots, t_{r(s)} \in T_\sigma$, $FV(st_1 \ldots t_{r(s)}) := Var(t_1) \cup \ldots \cup Var(t_{r(s)})$;
- pentru orice $\varphi \in F_\sigma$, $FV(\neg\varphi) := FV(\varphi)$;
- pentru orice $\varphi, \psi \in F_\sigma$, $FV(\varphi \to \psi) := FV(\varphi) \cup FV(\psi)$;
- pentru orice $\varphi \in F_\sigma$ și $x \in V$, $FV(\forall x \varphi) := FV(\varphi) \setminus \{x\}$.

Dacă $\varphi \in F_\sigma$ cu $FV(\varphi) = \emptyset$, atunci φ se numește **enunț**.
Mulțimea enunțurilor peste σ se notează cu E_σ.

Spre evaluarea formulelor

Fie $\mathcal{A} = (A, (A_s)_{s \in F \cup R})$ o σ-structură. Pentru orice $v : V \to A$, $x \in V$, $a \in A$, definim $v_{x \leftarrow a} : V \to A$, pentru orice $y \in V$, prin

$$v_{x \leftarrow a}(y) := \begin{cases} v(y), & \text{dacă } y \neq x, \\ a, & \text{dacă } y = x. \end{cases}$$

Observăm că pentru orice variabile x, y cu $x \neq y$, orice $v : V \to A$ și orice a, $b \in A$, avem că

$$(v_{y \leftarrow b})_{x \leftarrow a} = (v_{x \leftarrow a})_{y \leftarrow b}.$$

În acest caz, notăm valoarea lor comună cu $v_{x \leftarrow a, y \leftarrow b}$. Așadar, pentru orice $z \in V$,

$$v_{x \leftarrow a, y \leftarrow b}(z) = \begin{cases} v(z) & \text{dacă } z \neq x \text{ și } z \neq y, \\ a & \text{dacă } z = x, \\ b & \text{dacă } z = y. \end{cases}$$

Evaluarea formulelor

Avem că există și este unică o funcție $\|\cdot\|^{\mathcal{A}} : F_\sigma \to 2^{A^V}$ astfel încât, pentru orice $v : V \to A$, avem:

- pentru orice t, $u \in T_\sigma$, $\|t = u\|_v^{\mathcal{A}} = 1 \Leftrightarrow t_v^{\mathcal{A}} = u_v^{\mathcal{A}}$;
- pentru orice $s \in R$ și orice $t_1, \ldots, t_{r(s)} \in T_\sigma$, $\|st_1 \ldots t_{r(s)}\|_v^{\mathcal{A}} = 1 \Leftrightarrow ((t_1)_v^{\mathcal{A}}, \ldots, (t_{r(s)})_v^{\mathcal{A}}) \in A_s$;
- pentru orice $\varphi \in F_\sigma$, $\|\neg\varphi\|_v^{\mathcal{A}} = \neg\|\varphi\|_v^{\mathcal{A}}$;
- pentru orice φ, $\psi \in F_\sigma$, $\|\varphi \to \psi\|_v^{\mathcal{A}} = \|\varphi\|_v^{\mathcal{A}} \to \|\psi\|_v^{\mathcal{A}}$;
- pentru orice $\varphi \in F_\sigma$ și $x \in V$, $\|\forall x\varphi\|_v^{\mathcal{A}} = 1 \Leftrightarrow$ pentru orice $a \in A$, $\|\varphi\|_{v_{x \leftarrow a}}^{\mathcal{A}} = 1$.

Dacă $\varphi \in F_\sigma$ este astfel încât pentru orice $\mathcal{A}$ și v, $\|\varphi\|_v^{\mathcal{A}} = 1$, spunem că φ este **validă**.

Fie $\mathcal{A} = (A, (A_s)_{s \in F \cup R})$ o σ-structură. Este acum imediat că pentru orice $v : V \to A$, avem:

- pentru orice φ, $\psi \in F_\sigma$, $\|\varphi \wedge \psi\|_v^{\mathcal{A}} = \|\varphi\|_v^{\mathcal{A}} \mathbin{\pmb{\wedge}} \|\psi\|_v^{\mathcal{A}}$;
- pentru orice φ, $\psi \in F_\sigma$, $\|\varphi \vee \psi\|_v^{\mathcal{A}} = \|\varphi\|_v^{\mathcal{A}} \mathbin{\pmb{\vee}} \|\psi\|_v^{\mathcal{A}}$;
- pentru orice φ, $\psi \in F_\sigma$, $\|\varphi \leftrightarrow \psi\|_v^{\mathcal{A}} = \|\varphi\|_v^{\mathcal{A}} \mathbin{\pmb{\leftrightarrow}} \|\psi\|_v^{\mathcal{A}}$;
- pentru orice $\varphi \in F_\sigma$ și $x \in V$,
  $\|\exists x \varphi\|_v^{\mathcal{A}} = 1 \Leftrightarrow$ există $a \in A$ cu $\|\varphi\|_{v_{x \leftarrow a}}^{\mathcal{A}} = 1$.

Tautologii

Definiție

Spunem că $\chi \in F_\sigma$ se numește **tautologie** dacă pentru orice $F : F_\sigma \to 2$ astfel încât pentru orice $\varphi \in F_\sigma$, $F(\neg\varphi) = \neg F(\varphi)$ și pentru orice $\varphi, \psi \in F_\sigma$, $F(\varphi \to \psi) = F(\varphi) \to F(\psi)$, avem $F(\chi) = 1$.

Propoziție

Orice tautologie este formulă validă.

Demonstrație

Fie χ o tautologie. Fie $\mathcal{A}$ și v. Definim $F : F_\sigma \to 2$, pentru orice $\varphi \in F_\sigma$, prin $F(\varphi) := \|\varphi\|_v^{\mathcal{A}}$. Atunci F verifică condițiile din definiția tautologiei, deci $F(\chi) = 1$, i.e. $\|\chi\|_v^{\mathcal{A}} = 1$.

Lema de coincidență

Fie $\mathcal{A} = (A, (A_s)_{s \in F \cup R})$ o σ-structură, $v_1, v_2 : V \to A$ și $\varphi \in F_\sigma$ astfel încât $v_{1|FV(\varphi)} = v_{2|FV(\varphi)}$. Atunci $\|\varphi\|^{\mathcal{A}}_{v_1} = \|\varphi\|^{\mathcal{A}}_{v_2}$.

Demonstrație

Demonstrăm prin inducție după formule. Vom demonstra doar cazul cel mai greu, anume atunci când știm că concluzia lemei este valabilă pentru un $\varphi \in F_\sigma$, avem $x \in V$ și vrem să o demonstrăm pentru $\forall x \varphi$. Dat fiind că $\|\forall x \varphi\|^{\mathcal{A}}_{v_1} = 1$ dacă și numai dacă pentru orice $a \in A$, $\|\varphi\|^{\mathcal{A}}_{(v_1)_{x \leftarrow a}} = 1$, iar $\|\forall x \varphi\|^{\mathcal{A}}_{v_2} = 1$ dacă și numai dacă pentru orice $a \in A$, $\|\varphi\|^{\mathcal{A}}_{(v_2)_{x \leftarrow a}} = 1$, este suficient să arătăm că pentru orice $a \in A$, $\|\varphi\|^{\mathcal{A}}_{(v_1)_{x \leftarrow a}} = \|\varphi\|^{\mathcal{A}}_{(v_2)_{x \leftarrow a}}$. Fie $a \in A$. Din ipoteza de inducție, este suficient să arătăm că $((v_1)_{x \leftarrow a})_{|FV(\varphi)} = ((v_2)_{x \leftarrow a})_{|FV(\varphi)}$. Fie $y \in FV(\varphi)$. Atunci, fie $y = x$, iar atunci $(v_1)_{x \leftarrow a}(y) = a = (v_2)_{x \leftarrow a}(y)$, fie $y \neq x$, iar atunci $y \in FV(\varphi) \setminus \{x\} = FV(\forall x \varphi)$. Avem $(v_1)_{x \leftarrow a}(y) = v_1(y) = v_2(y) = (v_2)_{x \leftarrow a}(y)$.

Așadar, dacă $\mathcal{A} = (A, (A_s)_{s \in F \cup R})$ este o σ-structură și φ este enunț, pentru orice v_1, $v_2 : V \to A$, avem $\|\varphi\|^{\mathcal{A}}_{v_1} = \|\varphi\|^{\mathcal{A}}_{v_2}$, deci este echivalent faptul că pentru orice $v : V \to A$, $\|\varphi\|^{\mathcal{A}}_{v} = 1$ cu faptul că există $v : V \to A$ cu $\|\varphi\|^{\mathcal{A}}_{v} = 1$. Numim această stare de fapt cu

$$\mathcal{A} \models \varphi$$

și spunem că $\mathcal{A}$ **satisface** φ sau că $\mathcal{A}$ este **model** pentru φ.

Iată, deci, că structurile de ordinul I reprezintă analogul funcțiilor $e : Q \to 2$ întâlnite în logica propozițională. De aici provine și numele acelei ramuri a logicii care studiază structurile de ordinul I în conjuncție cu enunțurile satisfăcute de ele, anume **teoria modelelor**.

Vom defini următoarele concepte, precum și noi semnificații ale semnului $\models$, prin analogie cu logica propozițională:

- Dacă $\varphi \in E_\sigma$ și φ este valid, vom scrie $\models \varphi$.
- Spunem că $\varphi \in E_\sigma$ este **satisfiabil** dacă există $\mathcal{A}$ cu $\mathcal{A} \models \varphi$.
- Spunem că un enunț φ este **nesatisfiabil** dacă φ nu este satisfiabil.
- Fie $\varphi, \psi \in E_\sigma$. Spunem că din φ **se deduce semantic** ψ și scriem $\varphi \models \psi$ dacă pentru orice $\mathcal{A}$ cu $\mathcal{A} \models \varphi$ avem $\mathcal{A} \models \psi$.

Un exemplu

Vom ilustra în continuare toate conceptele de până acum. Fie σ prima signatură dată ca exemplu în curs și considerăm σ-formula

$$\varphi := \forall x_0 (x_0 \cdot 1 = x_0).$$

Atunci

$$\begin{aligned} FV(\varphi) &= FV(x_0 \cdot 1 = x_0) \setminus \{x_0\} \\ &= (Var(x_0 \cdot 1) \cup Var(x_0)) \setminus \{x_0\} \\ &= (Var(x_0) \cup Var(1) \cup Var(x_0)) \setminus \{x_0\} \\ &= (\{x_0\} \cup \emptyset \cup \{x_0\}) \setminus \{x_0\} = \emptyset, \end{aligned}$$

deci φ este enunț.

Un exemplu

Fie acum $\mathcal{A}$ o σ-structură având pe A ca univers și $v : V \to A$. Avem că

$$\begin{aligned}
\|\varphi\|_v^{\mathcal{A}} = 1 &\Leftrightarrow \|\forall x_0(x_0 \cdot 1 = x_0)\|_v^{\mathcal{A}} = 1 \\
&\Leftrightarrow \text{pentru orice } a \in A,\ \|x_0 \cdot 1 = x_0\|_{v_{x_0 \leftarrow a}}^{\mathcal{A}} = 1 \\
&\Leftrightarrow \text{pentru orice } a \in A,\ (x_0 \cdot 1)_{v_{x_0 \leftarrow a}}^{\mathcal{A}} = (x_0)_{v_{x_0 \leftarrow a}}^{\mathcal{A}} \\
&\Leftrightarrow \text{pentru orice } a \in A,\ A.((x_0)_{v_{x_0 \leftarrow a}}^{\mathcal{A}}, 1_{v_{x_0 \leftarrow a}}^{\mathcal{A}}) = (x_0)_{v_{x_0 \leftarrow a}}^{\mathcal{A}} \\
&\Leftrightarrow \text{pentru orice } a \in A,\ A.(v_{x_0 \leftarrow a}(x_0), A_1) = v_{x_0 \leftarrow a}(x_0) \\
&\Leftrightarrow \text{pentru orice } a \in A,\ A.(a, A_1) = a,
\end{aligned}$$

deci $\mathcal{A} \models \varphi$ dacă și numai dacă pentru orice $a \in A$, $A.(a, A_1) = a$.

În orice signatură σ, are sens să definim (din nou, prin analogie cu logica propozițională)

$$\perp := \neg(\forall x_0(x_0 = x_0) \to \forall x_0(x_0 = x_0))$$

și avem, clar, că $\perp$ este enunț, iar pentru orice σ-structură $\mathcal{A}$, avem $\mathcal{A} \not\models \perp$, i.e. $\perp$ este nesatisfiabil.

Numărul de elemente

Tot în orice signatură σ, are sens să definim, pentru orice $n \geq 2$, enunțul

$$\exists^{\geq n} := \exists x_1 \ldots \exists x_n (\neg(x_1 = x_2) \wedge \neg(x_1 = x_3) \wedge \ldots),$$

iar pentru orice σ-structură $\mathcal{A}$, și orice $n \geq 2$, avem $\mathcal{A} \models \exists^{\geq n}$ dacă și numai dacă universul lui $\mathcal{A}$ are cardinalul cel puțin n. Putem defini și $\exists^{\geq 1}$ ca fiind $\exists x_1 (x_1 = x_1)$, care va fi un enunț valid, dat fiind că am presupus că orice structură are universul nevid. De asemenea, vom mai defini, pentru orice $n \geq 1$:

$$\exists^{\leq n} := \neg \exists^{\geq n^+},$$
$$\exists^{= n} := \exists^{\geq n} \wedge \exists^{\leq n},$$

ce vor avea semnificațiile lor firești.

Complet analog celor din logica propozițională, vom introduce noțiuni de satisfiabilitate pentru mulțimi de formule, precum și semnificații corespunzătoare ale semnului $\models$.

Fie $\Gamma \subseteq E_\sigma$. Pentru orice σ-structură $\mathcal{A}$, spunem că $\mathcal{A}$ **satisface** Γ sau că $\mathcal{A}$ este **model** pentru Γ, și scriem $\mathcal{A} \models \Gamma$, dacă pentru orice $\varphi \in \Gamma$, $\mathcal{A} \models \varphi$.

Spunem că Γ este **satisfiabilă** dacă există o σ-structură $\mathcal{A}$ cu $\mathcal{A} \models \Gamma$; că este **nesatisfiabilă** dacă nu este satisfiabilă; și că este **finit satisfiabilă** dacă orice submulțime finită a sa este satisfiabilă.

Ca exemplu, fie $\Gamma := \{\exists^{\geq n} \mid n \geq 1\}$. Atunci o structură satisface Γ dacă și numai dacă mulțimea ei subiacentă este infinită.

Proprietăți

Următoarele proprietăți se demonstrează perfect analog celor din logica propozițională.

Proprietăți

Fie $\Gamma \subseteq E_\sigma$, $\Delta \subseteq \Gamma$ și $\mathcal{A}$ o σ-structură. Avem următoarele:

- Dacă $\mathcal{A} \models \Gamma$, atunci $\mathcal{A} \models \Delta$.
- Dacă Δ este nesatisfiabilă, atunci Γ este nesatisfiabilă.
- Avem că $\mathcal{A} \models \Gamma$ dacă și numai dacă pentru orice $\Sigma \subseteq \Gamma$ finită, $\mathcal{A} \models \Sigma$.

Deducție semantică din mulțimi

Fie $\Gamma \subseteq E_\sigma$ și $\varphi \in E_\sigma$. Spunem că din Γ **se deduce semantic** φ, și scriem $\Gamma \models \varphi$, dacă pentru orice σ-structură $\mathcal{A}$ cu $\mathcal{A} \models \Gamma$ avem $\mathcal{A} \models \varphi$. Această noțiune are următoarele proprietăți analoage celor din logica propozițională și demonstrabile similar.

Proprietăți

Fie $\Gamma \subseteq E_\sigma$, $\Delta \subseteq \Gamma$ și φ, $\psi \in E_\sigma$. Avem următoarele:

- Dacă $\Delta \models \varphi$, atunci $\Gamma \models \varphi$.
- Mulțimea Γ este nesatisfiabilă dacă și numai dacă $\Gamma \models \bot$.
- Avem $\Gamma \models \varphi$ dacă și numai dacă $\Gamma \cup \{\neg\varphi\}$ este nesatisfiabilă.
- Avem $\Gamma \cup \{\varphi\} \models \psi$ dacă și numai dacă $\Gamma \models \varphi \to \psi$.

Teorema de compacitate

Din nou ca în logica propozițională, vom putea enunța Teorema de compacitate, în cele două variante ale ei. Această teoremă reprezintă temelia întregii teorii a modelelor logicii de ordinul I.

Teorema de compacitate

- Fie $\Gamma \subseteq E_\sigma$ și $\varphi \in E_\sigma$. Atunci $\Gamma \models \varphi$ dacă și numai dacă există $\Delta \subseteq \Gamma$ finită cu $\Delta \models \varphi$.
- O mulțime de enunțuri este satisfiabilă dacă și numai dacă este finit satisfiabilă.

Precum în cazul logicii propoziționale, fiecare dintre variante are câte o implicație imediată, iar implicațiile care rămân sunt echivalente între ele (cu demonstrații perfect analoage). Ceea ce ne rămâne va fi demonstrarea următorului rezultat.

Teoremă (TK2$\Leftarrow$)

Orice mulțime de enunțuri finit satisfiabilă este satisfiabilă.

Instrumentul cu care s-a demonstrat acel rezultat la logica propozițională a fost **ultraprodusul**. Vom indica în continuare cum se definește această noțiune pentru structuri de ordinul I, definiția fiind mai elaborată decât cea pentru evaluări propoziționale (cronologic, ea a apărut, însă, anterior).

Considerăm $\sigma = (F, R, r)$ signatura peste care lucrăm. Fie I o mulțime nevidă, $\mathcal{A} = (\mathcal{A}_i)_{i \in I}$ o familie de σ-structuri, astfel încât, pentru orice $i \in I$, $\mathcal{A}_i = (A_i, (A_{i,s})_{s \in F \cup R})$ și U un ultrafiltru pe I. Vom nota cu $\mathcal{A}^U = (A^U, (A_s^U)_{s \in F \cup R})$ σ-structura care va reprezenta ultraprodusul familiei $\mathcal{A}$ relativ la U și pe care o vom defini în continuare.

Cum, pentru orice $i \in I$, $A_i \neq \emptyset$, aplicând Axioma alegerii, avem că $\prod_{i \in I} A_i \neq \emptyset$.

Vom defini o relație de echivalență pe $\prod_{i\in I} A_i$, notată cu $\sim_U$, în felul următor: pentru orice $(f_i)_{i\in I}, (g_i)_{i\in I} \in \prod_{i\in I} A_i$, spunem că $(f_i)_{i\in I} \sim_U (g_i)_{i\in I}$ dacă

$$\{i \in I \mid f_i = g_i\} \in U,$$

și vom pune $A^U := \prod_{i\in I} A_i / \sim_U$.

Pentru orice $s \in F \cup R$ și orice $(a_{1,i})_{i\in I}, \ldots, (a_{r(s),i})_{i\in I}$, punem, dacă $s \in F$,

$$A^U_s(\widehat{(a_{1,i})_{i\in I}}, \ldots, \widehat{(a_{r(s),i})_{i\in I}}) := (A_{i,s}(a_{1,i}, \widehat{\ldots,} a_{r(s),i}))_{i\in I},$$

iar dacă $s \in R$,

$$(\widehat{(a_{1,i})_{i\in I}}, \ldots, \widehat{(a_{r(s),i})_{i\in I}}) \in A^U_s :\Leftrightarrow \{i \in I \mid (a_{1,i}, \ldots, a_{r(s),i}) \in A_{i,s}\} \in U.$$

Se poate demonstra că aceste definiții sunt corecte (nu depind de reprezentanți) și, deci, am terminat de definit ultraprodusul $\mathcal{A}^U$.

Funcții cu valori într-un produs cartezian

Având în vedere că în definirea ultraprodusului se folosește produsul cartezian (de aici îi vine și denumirea, lucru care nu era vizibil în logica propozițională), vom da niște definiții ce se referă la funcții cu valori într-o asemenea mulțime.

Fie I o mulțime și $(A_i)_{i \in I}$. Fie $v : V \to \prod_{i \in I} A_i$ și U un ultrafiltru pe I. Pentru orice $i \in I$, definim $v_i : V \to A_i$, punând, pentru orice $x \in V$, $v_i(x) := v(x)_i$, și mai definim $v^U : V \to A^U$, punând, pentru orice $x \in V$, $v^U(x) := \widehat{v(x)}$.

Proprietăți

Fie $x \in V$ și $a = (a_i)_{i \in I} \in \prod_{i \in I} A_i$. Avem următoarele:

- Pentru orice $i \in I$, $(v_{x \leftarrow a})_i = (v_i)_{x \leftarrow a_i}$.
- Avem $(v_{x \leftarrow a})^U = (v^U)_{x \leftarrow \widehat{a}}$.

Teorema fundamentală a ultraproduselor (Łoś)

Fie I o mulțime nevidă, $\mathcal{A} = (\mathcal{A}_i)_{i \in I}$ o familie de σ-structuri astfel încât pentru orice $i \in I$, notăm cu A_i universul lui $\mathcal{A}_i$, $v : V \to \prod_{i \in I} A_i$ și U un ultrafiltru pe I. Atunci:

- Pentru orice $t \in T_\sigma$,

$$t_{v^U}^{\mathcal{A}^U} = \widehat{(t_{v_i}^{\mathcal{A}_i})_{i \in I}}.$$

- Pentru orice $\chi \in F_\sigma$,

$$\|\chi\|_{v^U}^{\mathcal{A}^U} = 1 \Leftrightarrow \{i \in I \mid \|\chi\|_{v_i}^{\mathcal{A}_i} = 1\} \in U.$$

Demonstrația depășește cadrul cursului. Ea poate fi, însă, un exercițiu pentru cei interesați – se face prin inducție structurală; cazul oarecum mai netrivial este cel al cuantificatorului universal, unde se vor folosi și proprietățile care au fost (cu acest scop) indicate anterior ale funcțiilor cu valori într-un produs cartezian.

Corolar

Fie I o mulțime nevidă, $\mathcal{A} = (\mathcal{A}_i)_{i \in I}$ o familie de σ-structuri și U un ultrafiltru pe I. Atunci, pentru orice $\chi \in E_\sigma$,

$$\mathcal{A}^U \models \chi \Leftrightarrow \{i \in I \mid \mathcal{A}_i \models \chi\} \in U.$$

Următorul rezultat se deduce întocmai ca la logica propozițională.

Teorema fundamentală a ultraproduselor – versiunea 2

Fie I o mulțime nevidă, $\mathcal{A} = (\mathcal{A}_i)_{i \in I}$ o familie de σ-structuri și U un ultrafiltru pe I. Atunci, pentru orice $\Delta \subseteq E_\sigma$ finită,

$$\mathcal{A}^U \models \Delta \Leftrightarrow \{i \in I \mid \mathcal{A}_i \models \Delta\} \in U.$$

Trucul lui Scott

Pentru a demonstra Teorema de compacitate, mai avem nevoie de un rezultat, anume o formă mai tare a Axiomei alegerii.

Teoremă (Axioma alegerii pentru proprietăți)

Fie P o proprietate ce are două argumente și I o mulțime astfel încât pentru orice $i \in I$, există x cu $P(i,x)$. Atunci există o familie $(x_i)_{i \in I}$ astfel încât pentru orice $i \in I$, $P(i, x_i)$.

Demonstrație

Vom folosi faptul că orice mulțime are rang. Pentru orice $i \in I$, punem α_i să fie acel ordinal α **minim** cu proprietatea că există $x \in V_\alpha$ cu $P(i,x)$ și apoi punem

$$X_i := \{x \in V_{\alpha_i} \mid P(i,x)\} \neq \emptyset.$$

(Acest procedeu de formare a mulțimilor X_i se numește **trucul lui Scott**.) Aplicăm, apoi, Axioma alegerii pe familia $(X_i)_{i \in I}$ și obținem familia cerută.

Demonstrația teoremei de compacitate

Putem, acum, demonstra acea implicație rămasă a Teoremei de compacitate.

Teoremă (TK2$\Leftarrow$)

Fie $\Gamma \subseteq E_\sigma$ finit satisfiabilă. Atunci Γ este satisfiabilă.

Demonstrație

Fie $I := \mathcal{P}_{\text{fin}}(\Gamma) = \{\Delta \in \mathcal{P}(\Gamma) \mid \Delta \text{ finită}\}$. Cum $\emptyset \in I$, $I \neq \emptyset$. Pentru orice $\Delta \in I$, există o σ-structură $\mathcal{A}$ cu $\mathcal{A} \models \Delta$. Din teorema precedentă, există o familie de σ-structuri $(\mathcal{A}_\Delta)_{\Delta \in I}$ astfel încât, pentru orice $\Delta \in I$, $\mathcal{A}_\Delta \models \Delta$.

Demonstrația **curge** apoi întocmai ca la logica propozițională. **A se observa** că avem nevoie de Axioma alegerii de multe ori (inclusiv în Teorema fundamentală a ultraproduselor, pe care nu am demonstrat-o!).

Ultima semnificație a lui $\models$

Fie Γ, $\Delta \subseteq E_\sigma$. Vom nota:

- prin $\Gamma \models \Delta$ faptul că pentru orice σ-structură $\mathcal{A}$ cu $\mathcal{A} \models \Gamma$ avem $\mathcal{A} \models \Delta$;
- prin $\Gamma \sim \Delta$ faptul că pentru orice σ-structură $\mathcal{A}$, $\mathcal{A} \models \Gamma$ dacă și numai dacă $\mathcal{A} \models \Delta$.

Observăm că $\Gamma \sim \Delta$ dacă și numai dacă $\Gamma \models \Delta$ și $\Delta \models \Gamma$.

Știind aceste noțiuni, vom putea prezenta câteva aplicații ale Teoremei de compactitate.

Propoziție

Fie $\Gamma, \Sigma \subseteq E_\sigma$ cu $\Gamma \models \Sigma$ și Σ finită. Atunci există $\Delta \subseteq \Gamma$ finită cu $\Delta \models \Sigma$.

Demonstrație

Demonstrăm prin inducție după cardinalul lui Σ. Pentru cazul $|\Sigma| = 0$, i.e. $\Sigma = \emptyset$, putem lua $\Delta := \emptyset$.

Presupunem acum că există $n \in \mathbb{N}$ astfel încât $|\Sigma| = n^+$ și luăm $\Sigma' \subseteq E_\sigma$ și $\varphi \in E_\sigma$ cu $|\Sigma'| = n$ și $\Sigma = \Sigma' \cup \{\varphi\}$. Atunci avem $\Gamma \models \Sigma'$ și $\Gamma \models \varphi$. Din prima afirmație, aplicând ipoteza de inducție, avem că există $\Delta' \subseteq \Gamma$ finită cu $\Delta' \models \Sigma'$, iar din a doua, aplicând Teorema de compacitate, avem că există $\Delta'' \subseteq \Gamma$ finită cu $\Delta'' \models \varphi$. Atunci $\Delta := \Delta' \cup \Delta''$ este mulțimea finită căutată.

Corolar

Fie $\Gamma, \Sigma \subseteq E_\sigma$ cu $\Gamma \sim \Sigma$ și Σ finită. Atunci există $\Delta \subseteq \Gamma$ finită cu $\Gamma \sim \Delta$, sau, echivalent, $\Sigma \sim \Delta$.

Demonstrație

Cum $\Gamma \models \Sigma$ și Σ este finită, din propoziția precedentă obținem că există $\Delta \subseteq \Gamma$ finită cu $\Delta \models \Sigma$. Dar $\Sigma \models \Gamma$, deci $\Delta \models \Gamma$. Mai mult, cum $\Delta \subseteq \Gamma$, avem $\Gamma \models \Delta$, deci $\Gamma \sim \Delta$.

Aplicații ale teoremei de compactitate

Propoziție

Fie $\Gamma \subseteq E_\sigma$ astfel încât pentru orice $m \in \mathbb{N}$ există $\mathcal{A} \models \Gamma$ astfel încât universul lui $\mathcal{A}$ are cardinalul mai mare sau egal cu m. Atunci Γ are un model cu universul infinit.

Demonstrație

Fie $\Sigma := \Gamma \cup \{\exists^{\geq n} \mid n \geq 1\}$. Clar, dacă Σ ar fi satisfiabilă, atunci un model al său ar fi un model al lui Γ cu universul infinit. Din Teorema de compactitate, este suficient să arătăm că Σ este finit satisfiabilă.

Fie $\Delta \subseteq \Sigma$ finită și vrem să arătăm că Δ este satisfiabilă. Avem că există $m \in \mathbb{N}$ astfel încât $\Delta \subseteq \Gamma \cup \{\exists^{\geq n} \mid 1 \leq n \leq m\}$.

Știm că există $\mathcal{A} \models \Gamma$ astfel încât universul lui $\mathcal{A}$ are cardinalul mai mare sau egal cu m. Atunci $\mathcal{A} \models \Delta$, deci Δ este satisfiabilă.

Aplicații ale teoremei de compacitate

Propoziție

Nu există $\Gamma \subseteq E_\sigma$ astfel încât pentru orice σ-structură $\mathcal{A}$, avem $\mathcal{A} \models \Gamma$ dacă și numai dacă universul lui $\mathcal{A}$ este finit (altfel spus, logica de ordinul I nu poate captura finitudinea).

Demonstrație

Presupunem că ar exista un asemenea Γ. Din propoziția precedentă, este suficient să arătăm că pentru orice $m \in \mathbb{N}$ există $\mathcal{A} \models \Gamma$ astfel încât universul lui $\mathcal{A}$ are cardinalul mai mare sau egal cu m. Fie $\mathcal{A}$ o σ-structură având ca univers pe m (de ce există așa ceva?). Atunci $\mathcal{A}$ are universul finit, deci, din ipoteză, $\mathcal{A} \models \Gamma$ și $\mathcal{A}$ este cea căutată.

Aplicații ale teoremei de compacitate

Propoziție

Nu există $\Gamma \subseteq E_\sigma$ **finită** astfel încât pentru orice σ-structură $\mathcal{A}$, avem $\mathcal{A} \models \Gamma$ dacă și numai dacă universul lui $\mathcal{A}$ este infinit.

Demonstrație

Presupunem că ar exista un asemenea Γ. Atunci $\Gamma \sim \{\exists^{\geq n} \mid n \geq 1\}$. Dintr-o propoziție anterioară, există $m \in \mathbb{N}$ cu $\Gamma \sim \{\exists^{\geq n} \mid 1 \leq n \leq m\}$. Fie $\mathcal{A}$ o σ-structură având ca univers mulțimea m. Atunci $\mathcal{A} \models \{\exists^{\geq n} \mid 1 \leq n \leq m\}$, deci $\mathcal{A} \models \Gamma$. Însă $\mathcal{A}$ are universul finit, ceea ce contrazice ipoteza făcută despre Γ.

Teorema Löwenheim-Skolem în sus

Fie $\Gamma \subseteq E_\sigma$ astfel încât Γ are un model cu universul infinit și κ un cardinal. Atunci Γ are un model cu universul de cardinal mai mare sau egal decât κ.

Demonstrație

Aplicând o propoziție veche, fie C o mulțime astfel încât $C \cap S_\sigma = \emptyset$ și $|C| = \kappa$. Fixăm o bijecție $f : \kappa \to C$ și notăm, pentru orice $\alpha \in \kappa$, $f(\alpha)$ cu c_α. Dacă avem $\sigma = (F, R, r)$, notăm $\sigma' := (F \cup C, R, r')$ unde $r'_{|F \cup R} = r$ și, pentru orice $c \in C$, $r'(c) = 0$. Atunci σ' este o signatură cu $\sigma \leq \sigma'$. Notăm

$$\Sigma := \Gamma \cup \{\neg(c_\alpha = c_\beta) \mid \alpha, \beta \in \kappa,\ \alpha \neq \beta\} \subseteq E_{\sigma'}.$$

Vom arăta că Σ este satisfiabilă.

Demonstrație (cont.)

De ce ne rezolvă problema faptul că Σ este satisfiabilă? Dacă avem $\mathcal{B}' \models \Sigma$, atunci $\mathcal{B}' \models \Gamma$. Fie $\mathcal{B}$ redusa lui $\mathcal{B}'$ la σ. Atunci $\mathcal{B} \models \Gamma$ (exercițiu!), iar $\mathcal{B}$ și $\mathcal{B}'$ au același univers, pe care îl notăm cu B. Considerăm funcția $g : \kappa \to B$, definită, pentru orice $\alpha \in \kappa$, prin $g(\alpha) := B'_{c_\alpha}$. Atunci g este injectivă și, deci, $\kappa \leq |B|$. Ca urmare, $\mathcal{B}$ este modelul căutat.

Din Teorema de compacitate, este suficient să arătăm că Σ este finit satisfiabilă. Fie $\Delta \subseteq \Sigma$ finită și vrem să arătăm că Δ este satisfiabilă. Avem că există $D \subseteq \kappa$ finită astfel încât

$$\Delta \subseteq \Gamma \cup \{\neg(c_\alpha = c_\beta) \mid \alpha,\ \beta \in D,\ \alpha \neq \beta\}.$$

Demonstrație (cont.)

Fie $\mathcal{A}$ un model al lui Γ cu universul infinit A și $h : D \to A$ injectivă. Fie $a \in A$ arbitrar. Fie $\mathcal{A}'$ o expansiune a lui $\mathcal{A}$ la σ' (avem $\mathcal{A}' \models \Gamma$ – exercițiu!), unde, pentru orice $\alpha \in \kappa$, avem

$$A'_{c_\alpha} := \begin{cases} h(\alpha), & \text{dacă } \alpha \in D, \\ a, & \text{dacă } \alpha \notin D. \end{cases}$$

Atunci $\mathcal{A}' \models \Delta$ și deci Δ este satisfiabilă.

Pentru orice t, $u \in T_\sigma$ și $y \in V$, vom defini termenul $t[y := u]$ (citim, de pildă, „t în care y a fost substituit prin u"), în mod recursiv, astfel:

- dacă $t \in V$,

$$t[y := u] = \begin{cases} u, & \text{dacă } y = t, \\ t, & \text{dacă } y \neq t. \end{cases}$$

- pentru orice $s \in F$, $t_1, \ldots, t_{r(s)} \in T_\sigma$,

$$(st_1 \ldots t_{r(s)})[y := u] = s(t_1[y := u]) \ldots (t_{r(s)}[y := u]).$$

Substituția pe formule

Pentru orice $\chi \in F_\sigma$, $y \in V$ și $u \in T_\sigma$, vom defini formula $\chi[y := u]$ (citim, de pildă, „χ în care y a fost substituit prin u”), în mod recursiv, astfel:

- pentru orice t, $v \in T_\sigma$,
  $(t = v)[y := u] = ((t[y := u) = (v[y := u]))$;
- pentru orice $s \in R$, $t_1, \ldots, t_{r(s)} \in T_\sigma$,
  $$(st_1 \ldots t_{r(s)})[y := u] = s(t_1[y := u]) \ldots (t_{r(s)}[y := u]);$$
- pentru orice $\varphi \in F_\sigma$, $(\neg\varphi)[y := u] = \neg(\varphi[y := u])$;
- pentru orice φ, $\psi \in F_\sigma$,
  $(\varphi \to \psi)[y := u] = (\varphi[y := u]) \to (\psi[y := u])$;
- pentru orice $\varphi \in F_\sigma$ și $x \in V$,
  $$(\forall x\varphi)[y := u] := \begin{cases} \forall x(\varphi[y := u]), & \text{dacă } y \neq x, \\ \forall x\varphi, & \text{dacă } y = x. \end{cases}$$

Deziderate

Am dori ca pentru orice χ, y, u, formula

$$\forall y \chi \to (\chi[y := u])$$

să fie validă.

Din păcate, acest lucru nu este adevărat. De pildă, luăm $\chi := \neg\forall x_0(x_0 = x_1)$, $y := x_1$, $u := x_0$. Atunci

$$\begin{aligned}
\chi[y := u] &= (\neg\forall x_0(x_0 = x_1))[x_1 := x_0] \\
&= \neg((\forall x_0(x_0 = x_1))[x_1 := x_0]) \\
&= \neg\forall x_0((x_0 = x_1)[x_1 := x_0]) \\
&= \neg\forall x_0(x_0[x_1 := x_0] = x_1[x_1 := x_0]) \\
&= \neg\forall x_0(x_0 = x_0).
\end{aligned}$$

Deziderate

Formula despre care vrem să fie validă va fi

$$\forall x_1 \neg \forall x_0 (x_0 = x_1) \to \neg \forall x_0 (x_0 = x_0).$$

Dar dacă luăm $\mathcal{A}$ o σ-structură al cărei univers este mulțimea $2 = \{0, 1\}$, iar $v : V \to 2$ oarecare, cum pentru orice $a \in 2$ există $b \in 2$ cu $a \neq b$, avem

$$\|\forall x_1 \neg \forall x_0 (x_0 = x_1)\|_v^{\mathcal{A}} = 1,$$

iar cum nu este adevărat că există $a \in 2$ cu $a \neq a$, avem

$$\|\neg \forall x_0 (x_0 = x_0)\|_v^{\mathcal{A}} = 0.$$

Ca urmare,

$$\begin{aligned}
&\|\forall x_1 \neg \forall x_0 (x_0 = x_1) \to \neg \forall x_0 (x_0 = x_0)\|_v^{\mathcal{A}} \\
&= \|\forall x_1 \neg \forall x_0 (x_0 = x_1)\|_v^{\mathcal{A}} \to \|\neg \forall x_0 (x_0 = x_0)\|_v^{\mathcal{A}} \\
&= 1 \to 0 = 0,
\end{aligned}$$

deci formula nu este validă.

Soluționare

Problema este că în termenul u apare variabila x_0 care este apoi „capturată accidental" de cuantificatorul $\forall x_0$ ce apare în formula χ. Soluția va fi să păstrăm definiția dată doar pentru situațiile în care acest fenomen nu poate apărea. Aceste situații „bune", ce depind, firește, de χ, y și u, vor fi definite în continuare sub titulatura „y este **liber pentru** u în χ".

Definiția lui „y este liber pentru u în χ" este recursivă și are forma următoare:

- y este liber pentru u în orice formulă atomică;
- y este liber pentru u în $\neg\varphi$ dacă y este liber pentru u în φ;
- y este liber pentru u în $\varphi \to \psi$ dacă y este liber pentru u în φ și y este liber pentru u în ψ;
- y este liber pentru u în $\forall x \varphi$ dacă fie $y \notin FV(\varphi)$, fie $y \in FV(\varphi)$, dar în acest caz avem $x \notin Var(u)$ și y este liber pentru u în φ.

Pentru a oferi un exemplu general de caz în care această situație are loc, definim mulțimea variabilelor unei formule (nu doar cele libere), prin funcția $Var : F_\sigma \to \mathcal{P}(V)$, definită recursiv prin:

- pentru orice $t, u \in T_\sigma$, $Var(t = u) := Var(t) \cup Var(u)$;
- pentru orice $s \in R$ și orice $t_1, \ldots, t_{r(s)} \in T_\sigma$, $Var(st_1 \ldots t_{r(s)}) := Var(t_1) \cup \ldots \cup Var(t_{r(s)})$;
- pentru orice $\varphi \in F_\sigma$, $Var(\neg\varphi) := Var(\varphi)$;
- pentru orice $\varphi, \psi \in F_\sigma$, $Var(\varphi \to \psi) := Var(\varphi) \cup Var(\psi)$;
- pentru orice $\varphi \in F_\sigma$ și $x \in V$, $Var(\forall x\varphi) := Var(\varphi) \cup \{x\}$.

Exemplul general

Propoziție

Fie $\chi \in F_\sigma$, $y \in V$, $u \in T_\sigma$. Atunci, dacă $Var(\chi) \cap Var(u) = \emptyset$, avem că y este liber pentru u în χ.

Demonstrație

Demonstrăm prin inducție după χ. Cazul netrivial este cel în care χ este de forma $\forall x \varphi$. Știm că $Var(\forall x \varphi) \cap Var(u) = \emptyset$, iar cum $Var(\varphi) \subseteq Var(\forall x \varphi)$, avem $Var(\varphi) \cap Var(u) = \emptyset$. Din ipoteza de inducție, avem că y este liber pentru u în φ.

Presupunem că $y \in FV(\varphi)$. Rămâne de arătat că $x \notin Var(u)$. Dar aceasta este adevărat, dat fiind că $x \in Var(\forall x \varphi)$, iar $Var(\forall x \varphi) \cap Var(u) = \emptyset$.

Proprietățile substituției libere

Pentru a arăta că, în acest caz de „substituție liberă”, formulele pe care le doream valide într-adevăr sunt așa, vom folosi următoarele proprietăți, ale căror demonstrații le lăsăm ca exercițiu.

Proprietățile substituției libere

Fie $\chi \in F_\sigma$, t, $u \in T_\sigma$, $y \in V$, $\mathcal{A}$ o σ-structură cu universul A și $v : V \to A$. Atunci:

- $(t[y := u])^{\mathcal{A}}_v = t^{\mathcal{A}}_{v_{y \leftarrow u^{\mathcal{A}}_v}}$;
- dacă y este liber pentru u în χ, $\|\chi[y := u]\|^{\mathcal{A}}_v = \|\chi\|^{\mathcal{A}}_{v_{y \leftarrow u^{\mathcal{A}}_v}}$.

Acum putem demonstra rezultatul dorit.

Propoziție

Fie $\chi \in F_\sigma$, $y \in V$, $u \in T_\sigma$, $\mathcal{A}$ o σ-structură cu universul A și $v : V \to A$. Presupunem că y este liber pentru u în χ. Atunci avem

$$\|\forall y\chi \to (\chi[y := u])\|_v^{\mathcal{A}} = 1.$$

Demonstrație

Presupunem că avem $\|\forall y\chi\|_v^{\mathcal{A}} = 1$. Atunci, pentru orice $a \in A$, $\|\chi\|_{v_{y\leftarrow a}}^{\mathcal{A}} = 1$. În particular, $\|\chi\|_{v_{y\leftarrow u_v^{\mathcal{A}}}}^{\mathcal{A}} = 1$, deci, din propoziția precedentă,

$$\|(\chi[y := u])\|_v^{\mathcal{A}} = 1.$$

Variante libere

Pentru a putea defini corect substituția în cazul general, vom defini recursiv, pentru orice formulă χ și orice $W \subseteq V$ finită, **varianta** W-**liberă** a lui χ, notată cu χ^W, în felul următor:

- dacă χ este atomică, $\chi^W := \chi$;
- $(\neg\varphi)^W := \neg(\varphi^W)$;
- $(\varphi \to \psi^W) := \varphi^W \to \psi^W$;
- $(\forall x\varphi)^W := \begin{cases} \forall z \left(\varphi^W[x := z]\right), & \text{dacă } x \in W, \\ \forall x\varphi^W, & \text{dacă } x \notin W, \end{cases}$

  unde z este variabila cu indice cel mai mic din mulțimea (nevidă) $V \setminus \left(W \cup Var\left(\varphi^W\right)\right)$.

A se observa că în acest ultim caz, cum $z \notin Var\left(\varphi^W\right)$, avem că $Var\left(\varphi^W\right) \cap Var(z) = \emptyset$, deci substituția din definiție este liberă.

Proprietăți ale variantelor libere

Aceste variante libere au următoarele proprietăți, ale căror demonstrații le lăsăm ca exercițiu.

Propoziție

Fie $\chi \in F_\sigma$.

- Fie $y \in V$, $u \in T_\sigma$. Atunci y este liber pentru u în $\chi^{Var(u)}$.
- Fie $W \subseteq V$ finită, $\mathcal{A}$ o σ-structură cu universul A și $v : V \to A$. Atunci $\left\|\chi^W\right\|_v^{\mathcal{A}} = \|\chi\|_v^{\mathcal{A}}$.

Substituții nelibere

Definim, acum, pentru orice χ, y, u astfel încât y **nu** este liber pentru u în χ,

$$\chi[y := u] := \chi^{Var(u)}[y := u].$$

Dat fiind că ne-am restrâns la cazul „neliber", nu intrăm în conflict de limbaj cu folosirea operației de substituție din cadrul definirii variantei libere (și nici cu membrul drept de mai sus).

Propoziție

Fie χ, y, u astfel încât y nu este liber pentru u în χ. Atunci avem, pentru orice $\mathcal{A}$ și v, $\|\chi[y := u]\|_v^{\mathcal{A}} = \|\chi\|_{v_{y \leftarrow u_v^{\mathcal{A}}}}^{\mathcal{A}}$ și, deci, ca mai înainte, formula $\forall y \chi \to (\chi[y := u])$ este validă.

Demonstrație

Fie $\mathcal{A}$ și v. Avem, folosind proprietățile anterioare, că

$$\|\chi[y := u]\|_v^{\mathcal{A}} = \left\|\chi^{Var(u)}[y := u]\right\|_v^{\mathcal{A}} = \left\|\chi^{Var(u)}\right\|_{v_{y \leftarrow u_v^{\mathcal{A}}}}^{\mathcal{A}} = \|\chi\|_{v_{y \leftarrow u_v^{\mathcal{A}}}}^{\mathcal{A}}.$$

Deducție în logica de ordinul I

Vom introduce sumar un sistem deductiv de tip Hilbert pentru logica de ordinul I. Axiomele sale vor fi:

- tautologiile;
- pentru orice formule φ, ψ și orice $y \in V \setminus FV(\varphi)$,
$$(\forall y(\varphi \to \psi)) \to (\varphi \to \forall y \psi);$$
- pentru orice $\chi \in F_\sigma$, $y \in V$, $u \in T_\sigma$ cu y liber pentru u în χ,
$$\forall y \chi \to (\chi[y := u]);$$
- pentru orice y, z, $w \in V$, $t \in T_\sigma$ și orice formulă **atomică** φ,
$$y = y;$$
$$z = w \to (t[y := z] = t[y := w]);$$
$$z = w \to (\varphi[y := z] \to \varphi[y := w]).$$

Pe lângă regula de deducție (MP), vom avea și regula **generalizării**: pentru orice $x \in V$ și $\varphi \in F_\sigma$, din φ se va deduce $\forall x \varphi$.

Pentru orice $\Gamma \subseteq E_\sigma$ (atenție, **nu** F_σ!) și orice $\varphi \in F_\sigma$, se vor defini, exact ca la logica propozițională, $\Gamma \vdash \varphi$ și $\vdash \varphi$. Această deducție va satisface următoarele proprietăți, pe care nu le vom demonstra.

Proprietăți

Fie $\Gamma \subseteq E_\sigma$, $\varphi \in E_\sigma$, $\psi \in F_\sigma$. Atunci:

- $\Gamma \vdash \varphi \to \psi$ dacă și numai dacă $\Gamma \cup \{\varphi\} \vdash \psi$ (**teorema deducției**);
- dacă $\Gamma \cup \{\varphi\} \vdash \perp$, atunci $\Gamma \vdash \neg\varphi$;
- dacă $\Gamma \vdash \psi$ și $\Gamma \vdash \neg\psi$, atunci $\Gamma \vdash \perp$.

Teorema de corectitudine

Precum la logica propozițională, vom avea următoarea teoremă ce se demonstrează prin inducție pe deducția sintactică. **A se observa** că validitatea uneia dintre axiome (cea care implică substituția) a fost deja demonstrată.

Teorema de corectitudine

Fie $\Gamma \subseteq E_\sigma$ și $\varphi \in F_\sigma$. Atunci, dacă $\Gamma \vdash \varphi$, avem că pentru orice σ-structură $\mathcal{A}$ cu universul A astfel încât $\mathcal{A} \models \Gamma$ și pentru orice $v : V \to A$ avem $\|\varphi\|_v^{\mathcal{A}} = 1$. În particular, dacă avem $\vdash \varphi$, atunci φ este validă.

Mulțimi consistente

Precum la logica propozițională, putem reformula teorema de corectitudine folosind noțiunea de mulțime consistentă.

Spunem că $\Gamma \subseteq E_\sigma$ este **consistentă** dacă $\Gamma \nvdash \perp$, și **inconsistentă** dacă $\Gamma \vdash \perp$.

Teorema de corectitudine – versiunea 2

Orice mulțime satisfiabilă este consistentă.

Demonstrație

Fie $\Gamma \subseteq E_\sigma$ satisfiabilă. Atunci $\Gamma \not\models \perp$, deci $\Gamma \nvdash \perp$, i.e. Γ este consistentă.

Mulțimi maximal consistente

Spunem că o mulțime consistentă de enunțuri Γ este **maximal consistentă** dacă este maximală printre mulțimile consistente relativ la incluziune, adică, pentru orice mulțime consistentă de enunțuri Σ ce include Γ, avem că $\Gamma = \Sigma$. Mulțimile maximal consistente satisfac următoarele proprietăți, pe care nu le vom demonstra.

Proprietăți

Fie Γ o mulțime maximal consistentă și φ, $\psi \in E_\sigma$. Atunci:

- $\Gamma \vdash \varphi$ dacă și numai dacă $\varphi \in \Gamma$;
- $\neg\varphi \in \Gamma$ dacă și numai dacă $\varphi \notin \Gamma$;
- $\varphi \to \psi \in \Gamma$ dacă și numai dacă $\varphi \notin \Gamma$ sau $\psi \in \Gamma$.

Teorema generală

Scopul acestor investigații este, ca în cazul logicii propoziționale, o teoremă generală care să lege noțiunile desemnate prin semnele $\vdash$ și $\models$, ce va include, așadar, Teorema de completitudine tare pentru logica de ordinul I, al cărei enunț (reamintim din Introducerea istorică) a fost pentru prima dată demonstrat de Gödel în 1929:

Teorema de completitudine – sumar

- Pentru orice $\Gamma \subseteq E_\sigma$ și $\varphi \in E_\sigma$, avem
$$\Gamma \vdash \varphi \Leftrightarrow \Gamma \models \varphi.$$
- O mulțime de enunțuri este consistentă dacă și numai dacă este satisfiabilă.

Nu vom parcurge toate detaliile demonstrației uzuale (care este datorată lui Henkin) a enunțului de mai sus (după cum se vede, deja am omis anumite demonstrații ale unor proprietăți), dar vom **schița** ideile principale care intră în componența sa.

Martori

Fie $\Gamma \subseteq E_\sigma$ și C o mulțime ale cărei elemente sunt toate constante ale lui σ. Spunem că C este o **mulțime de martori** pentru Γ dacă pentru orice $\varphi \in F_\sigma$ și $y \in V$ cu $FV(\varphi) \subseteq \{y\}$ există $c \in C$ astfel încât

$$\Gamma \vdash (\exists y \varphi) \rightarrow (\varphi[y := c]).$$

Clar, dacă $\Gamma \subseteq \Sigma$ și C este o mulțime de martori pentru Γ, atunci C este o mulțime de martori pentru Σ.

În continuare, vom arăta că mulțimile maximal consistente ce admit mulțimi de martori sunt satisfiabile, acesta putând fi văzut ca un caz particular al Teoremei de completitudine.

Teorema de existență a modelului

Considerăm signatura $\sigma = (F, R, r)$. Fie Γ o mulțime maximal consistentă și C o mulțime de martori pentru Γ. Atunci există o σ-structură $\mathcal{A} = (A, (A_s)_{s \in F \cup R})$ astfel încât $\mathcal{A} \models \Gamma$ și $|A| \leq |C|$.

Demonstrație

Ideea demonstrației, așa cum am spus, îi aparține lui Henkin. Pe mulțimea C se pune relația de echivalență $\sim$, definită, pentru orice c, $d \in C$, prin

$$c \sim d :\Leftrightarrow (c = d) \in \Gamma,$$

iar apoi se pune $A := C/\sim$.

Cum există $\pi : C \to A$ surjecția canonică, dintr-un exercițiu de seminar avem că există o injecție $g : A \to C$, deci $|A| \leq |C|$.

Demonstrație (cont.)

Pentru orice $s \in F \cup R$ și orice $a_1, \ldots, a_{r(s)} \in C$, dacă $s \in F$, cum C este mulțime de martori pentru mulțimea maximal consistentă Γ, avem că există $c \in C$ cu

$$((\exists x_0 (s a_1 \ldots a_{r(s)} = x_0)) \to (s a_1 \ldots a_{r(s)} = c)) \in \Gamma$$

și putem pune

$$A_s(\widehat{a_1}, \ldots, \widehat{a_{r(s)}}) := \widehat{c},$$

iar dacă $s \in R$, punem

$$(\widehat{a_1}, \ldots, \widehat{a_{r(s)}}) \in A_s :\Leftrightarrow s a_1 \ldots a_{r(s)} \in \Gamma.$$

Se demonstrează că toate aceste definiții sunt bune (nu depind de alegerile făcute), iar, după o lungă inducție, folosind proprietățile de martori și de maximal-consistență, se arată că $\mathcal{A} \models \Gamma$.

Signaturi numărabile

Pentru a putea atinge aceste proprietăți, ne vom restrânge temporar la cazul signaturilor numărabile.

Propoziție-Definiție

Fie $\sigma = (F, R, r)$ o signatură. Următoarele afirmații sunt echivalente:

- $F \cup R$ este cel mult numărabilă;
- F_σ este numărabilă;
- E_σ este numărabilă.

În acest caz, spunem că σ este o **signatură numărabilă**.

Proprietatea de maximal-consistență

Teoremă

Considerăm σ numărabilă. Atunci pentru orice mulțime consistentă Γ există o mulțime maximal consistentă Γ' ce include pe Γ.

Demonstrație

Fie $f : \mathbb{N} \to E_\sigma$ o bijecție. Vom nota, pentru orice n, $f(n)$ cu φ_n. Definim șirul de mulțimi $(\Gamma_n)_{n\in\mathbb{N}}$ în mod recursiv, punând $\Gamma_0 := \Gamma$, iar pentru orice $n \in \mathbb{N}$,

$$\Gamma_{n+1} := \begin{cases} \Gamma_n \cup \{\varphi_n\}, & \text{dacă } \Gamma_n \cup \{\varphi_n\} \text{ este consistentă,} \\ \Gamma_n \cup \{\neg\varphi_n\}, & \text{altfel.} \end{cases}$$

Arătăm prin inducție că pentru orice n, Γ_n este consistentă. Fie n. Trebuie demonstrat că dacă $\Gamma_n \cup \{\varphi_n\} \vdash \bot$, atunci $\Gamma_n \cup \{\neg\varphi_n\}$ este consistentă. Presupunem că am avea $\Gamma_n \cup \{\neg\varphi_n\} \vdash \bot$, deci $\Gamma_n \vdash \neg\varphi_n \to \bot$. Cum $\Gamma_n \cup \{\varphi_n\} \vdash \bot$, rezultă $\Gamma_n \vdash \neg\varphi_n$ și deci $\Gamma_n \vdash \bot$, contradicție cu ipoteza de inducție.

Proprietatea de maximal-consistență

Demonstrație (cont.)

Luăm acum

$$\Gamma' := \bigcup_{n\in\mathbb{N}} \Gamma_n,$$

care, clar, este consistentă. Presupunem acum că ar exista Σ consistentă cu $\Gamma' \subsetneq \Sigma$. Fie $\varphi \in \Sigma \setminus \Gamma'$. Atunci există n cu $\varphi = \varphi_n$. Cum $\varphi_n \notin \Gamma'$, $\varphi_n \notin \Gamma_{n+1}$, deci $\neg\varphi_n \in \Gamma_{n+1} \subseteq \Sigma$. Deci $\Sigma \vdash \varphi$ și $\Sigma \vdash \neg\varphi$, iar cum

$$\varphi \to (\neg\varphi \to \bot)$$

este tautologie, avem $\Sigma \vdash \bot$, ceea ce contrazice presupunerea că Σ este consistentă.

Proprietatea de martori

Teoremă

Considerăm σ numărabilă. Fie $\Gamma \subseteq E_\sigma$ consistentă și C numărabilă astfel încât $C \cap S_\sigma = \emptyset$. Notăm cu σ' signatura numărabilă obținută prin adăugarea elementelor lui C la σ pe post de constante (precum în demonstrația teoremei Löwenheim-Skolem în sus). Atunci există o mulțime consistentă $\Gamma' \subseteq E_{\sigma'}$ astfel încât $\Gamma \subseteq \Gamma'$ și C este mulțime de martori pentru Γ'.

Demonstrație

Fie $f : \mathbb{N} \to C$ o bijecție. Vom nota, pentru orice n, $f(n)$ cu c_n. Fie

$$A := \{\varphi \in F_{\sigma'} \mid |FV(\varphi)| \leq 1\}.$$

Fie $g : \mathbb{N} \to A$ o bijecție. Vom nota, pentru orice n, $g(n)$ cu φ_n. Pentru orice n, punem y_n să fie variabila liberă a lui φ_n, în caz că aceasta există, și x_0 altfel.

Demonstrație (cont.)

Definim șirul de mulțimi $(\Gamma_n)_{n\in\mathbb{N}}$ în mod recursiv, punând $\Gamma_0 := \Gamma$, iar pentru orice $n \in \mathbb{N}$, dacă notăm cu d_n acel c_m cu m minim astfel încât c_m nu apare în enunțurile din Γ_n,

$$\Gamma_{n+1} := \Gamma_n \cup \{(\exists y_n \varphi_n) \to (\varphi_n[y_n := d_n])\}.$$

Se arată printr-o inducție **netrivială** (pe care o omitem, dar menționăm că se folosește în mod crucial faptul că, pentru orice n, d_n nu apare în enunțurile din Γ_n) că pentru orice n, Γ_n este consistentă. Luăm acum $\Gamma' := \bigcup_{n\in\mathbb{N}} \Gamma_n$. Atunci Γ' va fi și ea consistentă, iar pentru orice $\varphi \in F_{\sigma'}$ și $y \in V$ cu $FV(\varphi) \subseteq \{y\}$, avem că $\varphi \in A$, deci există n cu $\varphi = \varphi_n$, iar atunci $y_n = y$, deci

$$\Gamma' \vdash (\exists y \varphi) \to (\varphi[y := d_n]),$$

ca urmare C este mulțime de martori pentru Γ'.

Teorema de completitudine tare – varianta 2 (cazul numărabil)

Considerăm σ numărabilă. Fie $\Gamma \subseteq E_\sigma$ consistentă. Atunci Γ admite un model cu universul cel mult numărabil.

Demonstrație

Aplicând o propoziție veche, fie C o mulțime numărabilă astfel încât $C \cap S_\sigma = \emptyset$. Notăm cu σ' signatura numărabilă obținută prin adăugarea elementelor lui C la σ pe post de constante. Din propoziția precedentă, există o mulțime consistentă $\Gamma' \subseteq E_{\sigma'}$ astfel încât $\Gamma \subseteq \Gamma'$ și C este mulțime de martori pentru Γ'. Dintr-o propoziție anterioară, există $\Gamma'' \subseteq E_{\sigma'}$ maximal consistentă cu $\Gamma' \subseteq \Gamma''$. Avem că C este mulțime de martori și pentru Γ''. Din Teorema de existență a modelului, există o σ'-structură $\mathcal{A}'$ cu universul A astfel încât $\mathcal{A}' \models \Gamma''$, în particular $\mathcal{A}' \models \Gamma$, și $|A| \leq |C| = \aleph_0$, deci A este cel mult numărabilă. Redusa lui $\mathcal{A}'$ la σ va fi atunci modelul căutat.

Consecințe

Corolar

Considerăm σ numărabilă. Fie $\Gamma \subseteq E_\sigma$ satisfiabilă. Atunci Γ admite un model cu universul cel mult numărabil.

Teorema de completitudine (slabă; cazul numărabil)

Considerăm σ numărabilă. Atunci pentru orice $\varphi \in E_\sigma$ cu $\models \varphi$, avem $\vdash \varphi$.

Demonstrație

Fie $\varphi \in E_\sigma$ cu $\models \varphi$. Presupunem că $\nvdash \varphi$. Atunci $\{\neg\varphi\}$ este consistentă (dacă am avea că $\{\neg\varphi\} \vdash \bot$, atunci am avea $\vdash \varphi$, contradicție!), deci satisfiabilă. Prin urmare, există $\mathcal{A}$ cu $\mathcal{A} \models \neg\varphi$, i.e. $\mathcal{A} \not\models \varphi$, ceea ce contrazice presupunerea.

Consecințe

Teorema de completitudine (slabă; cazul general)

Considerăm σ arbitrară. Atunci pentru orice $\varphi \in E_\sigma$ cu $\models \varphi$, avem $\vdash \varphi$.

Demonstrație

Fie $\varphi \in E_\sigma$ cu $\models \varphi$. Fie σ' astfel încât $\sigma' \leq \sigma$ și σ' conține doar simbolurile din σ ce apar efectiv în φ. Avem că σ' este o signatură numărabilă. Vom pune indici semnelor $\vdash$ și $\models$ pentru a indica signatura peste care lucrăm. Așadar, avem $\models_\sigma \varphi$. De aici deducem (exercițiu!) că $\models_{\sigma'} \varphi$ și putem aplica cazul numărabil al Teoremei de completitudine pentru a deduce că $\vdash_{\sigma'} \varphi$. De aici rezultă imediat $\vdash_\sigma \varphi$, ceea ce trebuia arătat.

Teorema generală

Precum la logica propozițională, putem deduce apoi Teorema de completitudine tare în cazul general (folosind Teorema deducției și Teorema de compacitate), rezumând aceste rezultate în modul următor, pe care l-am anticipat deja.

Teorema de completitudine – sumar

- Pentru orice $\Gamma \subseteq E_\sigma$ și $\varphi \in E_\sigma$, avem

$$\Gamma \vdash \varphi \Leftrightarrow \Gamma \models \varphi.$$

- O mulțime de enunțuri este consistentă dacă și numai dacă este satisfiabilă.

Izomorfisme

Considerăm signatura $\sigma = (F, R, r)$. Fie $\mathcal{A} = (A, (A_s)_{s \in F \cup R})$ și $\mathcal{B} = (B, (B_s)_{s \in F \cup R})$ două σ-structuri. Un **izomorfism** de la $\mathcal{A}$ la $\mathcal{B}$ este o bijecție $f : A \to B$ astfel încât pentru orice $s \in F \cup R$ și orice $a_1, \ldots, a_{r(s)} \in A$, avem, dacă $s \in F$, că

$$f(A_s(a_1, \ldots, a_{r(s)})) = B_s(f(a_1), \ldots, f(a_{r(s)})),$$

iar dacă $s \in R$, că

$$(a_1, \ldots, a_{r(s)}) \in A_s \Leftrightarrow (f(a_1), \ldots, f(a_{r(s)})) \in B_s.$$

Spunem că două σ-structuri $\mathcal{A}$ și $\mathcal{B}$ sunt **izomorfe**, și notăm $\mathcal{A} \simeq \mathcal{B}$, dacă există un izomorfism de la $\mathcal{A}$ la $\mathcal{B}$.

Echivalență elementară

Spunem că două σ-structuri $\mathcal{A}$ și $\mathcal{B}$ sunt **elementar echivalente**, și notăm $\mathcal{A} \equiv \mathcal{B}$, dacă pentru orice $\varphi \in E_\sigma$ avem că $\mathcal{A} \models \varphi$ dacă și numai dacă $\mathcal{B} \models \varphi$.

Pentru orice σ-structură $\mathcal{A}$, notăm

$$Th(\mathcal{A}) := \{\varphi \in E_\sigma \mid \mathcal{A} \models \varphi\}.$$

Clar, pentru orice σ-structuri $\mathcal{A}$ și $\mathcal{B}$, avem că $\mathcal{A} \equiv \mathcal{B}$ dacă și numai dacă $\mathcal{B} \models Th(\mathcal{A})$.

Propoziție (exercițiu)

Două structuri izomorfe sunt elementar echivalente.

Apare întrebarea: există structuri elementar echivalente care nu sunt izomorfe?

Mai concret, să considerăm σ_{ar} și structura sa canonică $\mathcal{N}$. Am dori să găsim o σ_{ar}-structură $\mathcal{M}$ cu $\mathcal{N} \equiv \mathcal{M}$, deci $\mathcal{M} \models Th(\mathcal{N})$, dar cu $\mathcal{N} \not\simeq \mathcal{M}$. Un asemenea $\mathcal{M}$ se va numi **model non-standard al aritmeticii**.

Putem găsi un asemenea model destul de simplu, în felul următor. Dat fiind că $Th(\mathcal{N})$ are un model infinit (pe $\mathcal{N}$), aplicând Teorema Löwenheim-Skolem în sus, obținem că există $\mathcal{M} \models Th(\mathcal{N})$ cu universul de cardinal cel puțin $\aleph_1$. Așadar, nu poate exista un izomorfism de la $\mathcal{M}$ la $\mathcal{N}$ din motive care țin de cardinalitate.

Există, însă, vreun model non-standard al aritmeticii **numărabil**?

Modele non-standard ale aritmeticii

Vom considera σ' ca fiind acea signatură care se obține din σ_{ar} prin adăugarea unei constante $c \notin S_{\sigma_{ar}}$. Notăm

$$\Gamma := Th(\mathcal{N}) \cup \{\neg(c = \dot{0}), \neg(c = \dot{S}\dot{0}), \neg(c = \dot{S}\dot{S}\dot{0}), \ldots\} \subseteq E_{\sigma'}.$$

Arătăm că Γ este satisfiabilă. Din Teorema de compacitate, este suficient să arătăm că este finit satisfiabilă. Fie $\Delta \subseteq \Gamma$ finită. Atunci există $m \in \mathbb{N}$ astfel încât

$$\Delta \subseteq Th(\mathcal{N}) \cup \{\neg(c = \dot{S}^i\dot{0}) \mid i < m\}.$$

Fie $\mathcal{B}$ expansiunea lui $\mathcal{N}$ la σ' astfel încât c este interpretat în $\mathcal{B}$ prin m. Atunci $\mathcal{B} \models \Delta$, deci Δ este satisfiabilă. Am arătat, deci, că Γ este satisfiabilă, iar cum σ' este o signatură numărabilă, dintr-un rezultat anterior avem că Γ admite un model cu universul numărabil. Redusa acelui model la σ_{ar} va fi modelul non-standard al aritmeticii căutat.

Fundamentele matematicii

Motto

"Everyone knows what a curve is, until he has studied enough mathematics to become confused through the countless number of possible exceptions."

– Felix Klein

Demonstrații formale

Atât în logica propozițională, cât și în logica de ordinul I, avem de-a face cu următoarea echivalență (caracterizare): pentru orice mulțime de enunțuri Γ și orice formulă φ, avem că $\Gamma \vdash \varphi$ **dacă și numai dacă** există $n \in \mathbb{N}$ și un șir finit de formule $(\varphi_i)_{i \leq n}$ astfel încât $\varphi_n = \varphi$, iar pentru orice $i \leq n$, φ_i este fie axiomă a sistemului deductiv, fie element al lui Γ, fie se obține din formule care o precedă printr-una dintre regulile de deducție – regula (MP) sau regula generalizării.

Demonstrația echivalenței este aproape imediată, făcându-se într-unul din sensuri prin inducție pe deducția sintactică, iar în celălalt prin inducție după acel n.

Un șir finit ca mai sus se va numi **demonstrație formală** (relativă la Γ). Membrul drept al echivalenței se poate lua și ca definiție a semnului $\vdash$, dar, după cum s-a văzut, nu a fost nevoie. El justifică, însă, folosirea sintagmei „deducție sintactică" și este crucial în raționamentele filosofice care privesc aceste logici.

Argumentul de „strângere”

În primul rând, ne putem întreba: de ce aceste concepte formale, indicate de semnele $\vdash$ și $\models$, corespund conceptului informal de „adevăr universal”?

Un răspuns ne este dat de așa-numitul argument de „strângere” al lui Kreisel. El pornește de la următoarele premise necontroversate:

- Orice enunț demonstrabil (teoremă formală) este „universal adevărat”.
- Orice enunț „universal adevărat” este, în particular, adevărat în orice structură (deci valid).

Se obține, așadar, următoarea imagine:

$$\vdash \varphi \qquad \Rightarrow \qquad \varphi \text{ este „universal adevărat”} \qquad \Rightarrow \qquad \models \varphi$$

Teorema de completitudine (i.e. faptul că $\models \varphi$ implică $\vdash \varphi$) devine ultima premisă a argumentului, cea care „strânge” conceptul informal între cele două concepte formale, garantând egalitatea celor trei.

Mai apoi, putem să ne întrebăm cum putem realiza vechea promisiune de a fundamenta teoria mulțimilor (ZFC) pe logică.

Așa cum s-a văzut și am și evidențiat, noi am fundamentat logica de ordinul întâi pe teoria mulțimilor (inclusiv formulele erau mulțimi!), ca urmare apare problema prefigurată de a găsi un alt fundament pentru logică, pentru a nu avea referințe circulare.

În primul, să observăm că **nu putem fundamenta ceva pe nimic**. Mereu, când dorim să facem matematică și să o comunicăm altora, ne bazăm pe faptul că există anumite idei și concepte pe care le avem dinainte presupuse tacit.

Să vedem, însă, ce are de spus filosofia matematicii despre asemenea chestiuni.

Simplificând masiv, există în genere două mari moduri de a fundamenta filosofic matematica:

- **platonism**, în care obiectele matematice (chiar și infinite) „există” într-un sens abstract (în genul formelor lui Platon), iar noi avem acces la ele doar prin obiecte finite, tangibile (precum demonstrațiile);
- **formalism** (sau chiar **finitism**, deși ele diferă), în care doar despre obiectele matematice finite se poate spune că „există” cu adevărat, iar cele infinite sunt doar anumite ficțiuni, povești pe care le spunem pentru a putea avea o intuiție productivă.

Noi vom avea o abordare mai **agnostică** – după cum am spus și anterior, ne vom baza pe anumite intuiții comune pe care le avem cu toții și pe care le dorim a fi **minimale** (vezi și „jocurile de limbaj” ale lui Wittgenstein).

Vom alege să avem la bază noțiunile intuitive de număr natural și de funcție calculabilă.

După cum am spus în Introducerea istorică, există mai multe moduri de a defini funcția calculabilă (mașini Turing etc.). Acesta nefiind un curs de calculabilitate, ne vom baza pe cunoștințele de programare dobândite în liceu, anume limbajul C (sau chiar pseudocodul) și modul cum sunt implementați în el algoritmi standard, precum algoritmul lui Euclid sau cei de sortare.

Vom spune, deci, că o funcție $f : \mathbb{N} \to \mathbb{N}$ este **calculabilă** dacă există un program C care o calculează. (Aceasta nu este o definiție neriguroasă, cu condiția de a fi fost precizat în detaliu, în prealabil, cum arată și cum este rulat un program C, lucru care se poate face la un curs de semantica limbajelor de programare.) Putem extinde imediat definiția și la alte tipuri de date nenumerice (cum ar fi șirurile de caractere, cum vom vrea să fie formulele), luând în calcul că acestea pot fi (și chiar sunt, în practică) codificate ca numere.

Teza Church-Turing

Cum putem ști că aceste concepte formale de program C, mașină Turing etc. corespund celui informal de calculabilitate? Așa cum am mai spus, această corespondență poartă numele de **teza Church-Turing**.

Există argumente în favoarea tezei ce seamănă cu cel de „strângere” de mai devreme (de aceea am dorit să fie menționat). Un alt argument este că orice definiție gândită pentru calculabilitate s-a dovedit a fi echivalent cu cele ale lui Church și Turing. Mai mult, orice încercare de a fundamenta calculabilitatea pe legi mai profunde ale fizicii (avem exemplul faimos al **calculului cuantic**) nu a condus la creșterea clasei de funcții calculabile, ci doar (fapt nedemonstrat, dar bănuit puternic) la cea a **vitezei** de calcul.

Vom accepta, deci, teza Church-Turing.

Mulțimi decidabile

Spunem că $A \subseteq \mathbb{N}$ (sau, din nou, putem lucra și cu date nenumerice, ca șirurile de caractere) este **decidabilă** dacă $\chi_A : \mathbb{N} \to 2$ este calculabilă, i.e. dacă există un program (o **procedură de decizie**) care primește ca intrare un număr natural și returnează 1 dacă el este în A și 0 dacă nu este.

De exemplu, dacă Q este cel mult numărabilă, avem că $E(Q) \subseteq \mathrm{Seq}(S(Q))$ este decidabilă, iar dacă σ este o signatură de ordinul I numărabilă, avem că F_σ și E_σ, ca submulțimi ale lui $\mathrm{Seq}(S_\sigma)$, sunt decidabile.

Cum mulțimea programelor (oricum le-am formaliza) este numărabilă, iar mulțimea submulțimilor lui $\mathbb{N}$ este infinită, nenumărabilă, avem că **există mulțimi nedecidabile**.

Mulțimi recursiv enumerabile

Spunem că $A \subseteq \mathbb{N}$ (cu aceleași precizări) este **recursiv enumerabilă** dacă există un program care primește ca intrare un număr natural și returnează 1 dacă el este în A, iar în caz că nu este, nu se oprește.

Orice mulțime decidabilă este recursiv enumerabilă: putem construi un program care apelează procedura de decizie a mulțimii: în caz că aceea returnează 1, va returna și el 1, iar în caz că returnează 0, programul va intra într-o buclă infinită. Programul verifică atunci condiția din definiția enumerabilității recursive.

Deși folosim, pentru intuiție, termenul de „mulțime", noi nu avem nevoie (neapărat) de teoria mulțimilor pentru a le fundamenta, putând gândi în mare parte doar în termeni de aceste programe/proceduri concrete, formalizate, aproximativ vorbind, într-un sistem deductiv „finitar", pe care nu îl vom detalia.

Caracterizarea mulțimilor recursiv enumerabile

Propoziție

O mulțime este recursiv enumerabilă dacă și numai dacă există un program care nu acceptă date de intrare, rulează la infinit, iar pe parcursul rulării afișează exact acele numere (respectiv șiruri etc.) care sunt elemente ale mulțimii. (Un asemenea program oferă, în fond, o enumerare a mulțimii, de unde provine și termenul.)

Demonstrație

Pentru „$\Rightarrow$", rulăm în paralel (de ce putem face asta?) programul din definiția enumerabilității recursive dând ca intrare, pe rând, fiecare număr natural, iar atunci când vreuna dintre cópii returnează 1, afișăm numărul corespunzător.

Pentru „$\Leftarrow$", dacă avem un număr dat ca intrare, așteptăm ca programul din enunțul propoziției să îl afișeze, iar în acel moment, returnăm 1.

Când Q este numărabilă, mulțimea acelor șiruri din $\mathrm{Seq}(E(Q))$ ce sunt demonstrații formale este decidabilă. În particular, ea este recursiv enumerabilă. Observăm că putem modifica un program ce enumeră toate demonstrațiile formale pentru a afișa doar concluziile lor. Astfel, se observă că mulțimea **tautologiilor** este recursiv enumerabilă.

Dar, mai mult, cum pentru orice $\varphi \in E(Q)$, $Var(\varphi)$ este finită, putem decide dacă φ este tautologie doar uitându-ne la tabelul de adevăr construit de la $Var(\varphi)$. Avem, deci, o procedură de decizie pentru mulțimea tautologiilor, care este, așadar, decidabilă.

Aceste fapte ne arată că sistemul de deducție pentru logica propozițională nu este strict necesar. El a fost studiat doar pentru dobândirea intuiției asupra sistemelor de deducție în general.

Cazul logicii de ordinul I

Când avem de-a face cu o signatură de ordinul I numărabilă, prima parte a raționamentului anterior încă funcționează, iar ca urmare mulțimea demonstrațiilor este decidabilă, iar cea a formulelor valide este recursiv enumerabilă. Acesta este conținutul **real** al teoremei de completitudine, numit, uneori, **teorema de completitudine abstractă**.

Apare întrebarea: există o procedură de decizie pentru mulțimea formulelor valide? Răspunsul, după cum am spus și în Introducerea istorică, a fost dat de Church și Turing și este unul **negativ**. Este de remarcat că pentru a justifica acest fapt, avem nevoie de o definiție precisă a calculabilității (așa cum au oferit ei), nu ne mai sunt suficiente argumente informale precum cele precedente.

Cazul mulțimilor de formule

Se observă și că raționamentul inițial se păstrează și în cazul în cazul în care avem o mulțime decidabilă de enunțuri $\Gamma \subseteq E_\sigma$ ca mulțime de premise, în sensul că mulțimea demonstrațiilor relative la Γ este decidabilă, iar mulțimea consecințelor sintactice ale lui Γ este recursiv enumerabilă.

Acestea sunt, în fond, proprietățile pe care le dorim, atunci când considerăm o mulțime Γ care să poată fundamenta matematica: vrem să putem decide dacă un șir de enunțuri este o demonstrație, altfel însăși noțiunea de demonstrație nu ar avea sens!

Ce vom face este, deci, să arătăm că teoria mulțimilor ZFC se poate codifica ca o mulțime decidabilă de enunțuri peste o signatură numărabilă.

Signatura va fi notată cu $\sigma_\in$ și va conține un singur simbol, anume un simbol de relație de aritate 2, notat cu $\in$. Se observă folosirea exclusivă a sa este justificată, i.e. notațiile folosite uzual în teoria mulțimilor se pot reduce la el în logica de ordinul I, și le vom folosi drept prescurtări, de pildă:

$$\begin{array}{l|r}
\emptyset \in x & \exists y (y \in x \wedge \forall z \neg (z \in y)) \\
x = \{z\} & \forall u (u \in x \leftrightarrow u = z) \\
x = u \cap v & \forall z (z \in x \leftrightarrow (z \in u \wedge z \in v)) \\
x \subseteq y & \forall z (z \in x \rightarrow z \in y)
\end{array}$$

Axiomele ZFC

În continuare vom vedea cum sunt formalizate axiomele ZFC în această signatură.

- Axioma extensionalității:

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y).$$

- Axioma perechii:

$$\forall x \forall y \exists z (x \in z \wedge y \in z).$$

- Axioma reuniunii:

$$\forall F \exists x \forall z ((\exists y (z \in y \wedge y \in F)) \rightarrow z \in x).$$

- Axioma mulțimii părților:

$$\forall x \exists y \forall z (z \subseteq x \rightarrow z \in y).$$

Axiomele ZFC

- Axioma infinitului:

$$\exists A(\emptyset \in A \wedge \forall x(x \in A \to x \cup \{x\} \in A).$$

- Axioma regularității:

$$\forall a(\neg(a = \emptyset) \to \exists b(b \in a \wedge a \cap b = \emptyset)).$$

Axioma alegerii are o formulare mai lungă (dar nu mai complicată), drept care o vom omite.

Unde vom avea, într-adevăr, o problemă, va fi exact acolo unde am avut-o deja, anume la explicitarea acelor „proprietăți" din Axioma comprehensiunii și Axioma înlocuirii. O vom trata doar pe prima dintre ele, cealaltă formalizându-se analog.

Axioma comprehensiunii, formal

Naiv, axioma comprehensiunii s-ar scrie ca

$$\forall P \forall x \exists y \forall z (z \in y \leftrightarrow z \in x \land P(z)).$$

Însă o asemenea „cuantificare după predicate” nu este posibilă decât într-o logică de ordin superior (ceea ce, până la urmă, ne-ar conduce la o referință circulară, pe care dorim să o evităm).

Soluția este de a înlocui acea unică axiomă de mai sus cu o familie **infinită** de axiome, câte una pentru fiecare proprietate P formalizabilă ca formulă φ peste signatura $\sigma_\in$, în felul următor (simplificând puțin):

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \in x \land \varphi).$$

După ce formalizăm astfel și Axioma înlocuirii, notăm mulțimea de axiome care rezultă cu ZFC. Observăm, deci, că sistemul acesta nu are doar nouă axiome, cum ne-am fi așteptat, ci un număr numărabil. (Se poate chiar demonstra că nu există o mulțime finită $\Gamma \subseteq E_{\sigma_\in}$ cu $\Gamma \sim ZFC$.) Totuși, este adevărat lucrul pe care-l doream, anume faptul că ZFC este o mulțime decidabilă, și, prin urmare, mulțimea ZFC-demonstrațiilor este și ea decidabilă, iar mulțimea consecințelor lui ZFC este recursiv enumerabilă.

Ipoteza continuumului

În acest moment, putem formaliza, de pildă, chiar și ipoteza continuumului, i.e. faptul că $2^{\aleph_0} = \aleph_1$, ca pe un $\sigma_\in$-enunț, notat cu CH, și putem privi „metarezultatele" lui Gödel și Cohen, ce spun că

$$ZFC \not\vdash \neg CH, \text{ respectiv } ZFC \not\vdash CH,$$

ca pe niște afirmații despre proceduri definibile finit ce sunt demonstrabile în acel sistem finitar pomenit anterior.

În particular, prima afirmație este echivalentă cu faptul că $ZFC \cup \{CH\}$ este consistentă, afirmație ce se va nota prin

$$Con(ZFC + CH).$$

Consistența relativă

Totuși, acest enunț îl implică, firește, pe $Con(ZFC)$, ce exprimă faptul că ZFC este consistentă. Or, noi am văzut că a doua teoremă de incompletitudine a lui Gödel spune că aceasta nu este demonstrabilă într-un sistem finitar.

De ce, totuși, rezultatele acestea de independență nu îl contrazic pe acela de incompletitudine? Răspunsul este că nu $Con(ZFC + CH)$ este enunțul demonstrat, de fapt, ci

$$Con(ZFC) \to Con(ZFC + CH),$$

i.e. consistența **relativă** a ipotezei continuumului (și apoi, în cazul rezultatului lui Cohen, a negației ei) peste ZFC.

Consistența absolută

Un mod de a ne convinge de consistența sistemului *ZFC* este prin argumente extra-matematice (filosofice, ontologice), de exemplu prin intuiția pe care o avem asupra ierarhiei von Neumann.

Odată ce ne-am convins de ea, putem dezvolta în interiorul *ZFC* logica de ordinul I, așa cum am făcut-o în acest curs, împreună cu toate rezultatele ei – compacitate, completitudine, Löwenheim-Skolem în sus etc.

Paradoxul lui Skolem

Admițând ZFC ca fiind consistentă, îi putem adăuga pe $Con(ZFC)$ însuși ca pe o axiomă suplimentară și putem deduce, din teorema de completitudine, că există modele pentru ZFC.

Nu există aici un concept evident de model standard, dar, clar, ca și în cazul aritmeticii, se poate construi o varietate de modele cu ajutorul Teoremei Löwenheim-Skolem în sus.

Un fapt curios este că, fiind o mulțime de enunțuri într-o signatură numărabilă, ZFC admite un model numărabil, chiar dacă în interiorul unui asemenea model există în mod necesar mulțimi pe care modelul le „vede” ca fiind nenumărabile. Acest fapt este denumit **paradoxul lui Skolem** – paradox nu fiindcă exprimă o contradicție, ca în cazul paradoxul lui Russell, ci fiindcă exprimă ceva aparent neverosimil.

Logica drept unealtă

Pe de altă parte, încrederea în *ZFC* și capacitatea acesteia de a formaliza logica de ordinul întâi ne permit să o folosim pe aceasta din urmă ca pe o unealtă utilă în matematică, independent de chestiunile legate de fundamente.

Dezvoltarea teoriei modelelor logicii de ordinul I a declanșat o serie de progrese teoretice, de exemplu în algebră, după cum vom vedea în ultimul capitol.

Aplicații ale teoriei modelelor în algebră

Motto

"Every field of mathematics has its zenith and its nadir. The zenith of logic is model theory (we do not dare state what we believe will be its nadir). The sure sign that we are dealing with a zenith is that as we, ignorant and dumb non-logicians, attempt to read the stuff, we feel that the material should be rewritten for the benefit of a general audience."

– Gian-Carlo Rota, *Indiscrete Thoughts*

Mulțimi complete

Numim o mulțime $\Gamma \subseteq E_\sigma$ **completă** dacă este satisfiabilă, iar pentru orice $\varphi \in E_\sigma$, avem $\Gamma \models \varphi$ sau $\Gamma \models \neg\varphi$.

Propoziție

Fie $\mathcal{A}$ o σ-structură. Atunci $Th(\mathcal{A})$ este completă.

Demonstrație

Clar, $\mathcal{A} \models Th(\mathcal{A})$, deci $Th(\mathcal{A})$ este satisfiabilă. Fie $\varphi \in E_\sigma$. Presupunem $Th(\mathcal{A}) \not\models \varphi$. Atunci $\varphi \notin Th(\mathcal{A})$, deci $\mathcal{A} \not\models \varphi$. Avem că $\mathcal{A} \models \neg\varphi$, deci $\neg\varphi \in Th(\mathcal{A})$ și $Th(\mathcal{A}) \models \neg\varphi$.

Observăm că dacă Γ și Σ verifică $\Gamma \sim \Sigma$, avem că mulțimea consecințelor lui Γ este egală cu mulțimea consecințelor lui Σ.

Mulțimi complete

Propoziție

Fie $\mathcal{A}$ o σ-structură. Avem că mulțimea consecințelor lui $Th(\mathcal{A})$ este $Th(\mathcal{A})$.

Demonstrație

Fie φ cu $Th(\mathcal{A}) \models \varphi$. Cum $\mathcal{A} \models Th(\mathcal{A})$, avem $\mathcal{A} \models \varphi$, deci $\varphi \in Th(\mathcal{A})$.

Propoziție

Fie $\mathcal{A}$ o σ-structură și Γ completă cu $\mathcal{A} \models \Gamma$. Atunci $\Gamma \sim Th(\mathcal{A})$.

Demonstrație

Fie $\mathcal{B}$ o σ-structură. Dacă $\mathcal{B} \models \Gamma$ și $\varphi \in Th(\mathcal{A})$, atunci $\mathcal{A} \not\models \neg\varphi$, deci $\Gamma \not\models \neg\varphi$. Cum Γ este completă, $\Gamma \models \varphi$ și deci $\mathcal{B} \models \varphi$.

Dacă $\mathcal{B} \models Th(\mathcal{A})$ și $\varphi \in \Gamma$, atunci $\mathcal{A} \models \varphi$, deci $\varphi \in Th(\mathcal{A})$ și $\mathcal{B} \models \varphi$.

Consecințe decidabile

Propoziție

Fie Γ o mulțime completă astfel încât mulțimea consecințelor ei este recursiv enumerabilă. Atunci mulțimea consecințelor ei este decidabilă.

Demonstrație

Vrem să construim o procedură de decizie pentru mulțimea consecințelor lui Γ. Fie φ intrarea acelei proceduri. Rulăm programul ce enumeră mulțimea consecințelor lui Γ, iar în momentul în care îl afișează pe φ sau pe $\neg\varphi$ (ceea ce necesar se va întâmpla, Γ fiind completă), returnăm, după caz, 1 sau 0.

Teorema Löwenheim-Skolem

Teorema Löwenheim-Skolem în sus, pe care am studiat-o, este o variantă mai slabă a următorului rezultat, pe care nu îl vom demonstra.

Teorema Löwenheim-Skolem

Considerăm signatura $\sigma = (F, R, r)$. Fie $\Gamma \subseteq E_\sigma$ astfel încât Γ are un model cu universul infinit și κ un cardinal cu

$$\max(|F \cup R|, \aleph_0) \leq \kappa.$$

Atunci Γ are măcar un model cu universul de cardinal **exact** κ.

Remarcăm, totuși, că noi am întâlnit o metodă de a construi modele care au cel mult un anume cardinal, anume cardinalul $\aleph_0$ – în demonstrația Teoremei de completitudine. Demonstrația Teoremei Löwenheim-Skolem folosește idei asemănătoare.

Definiția categoricității

Definiție

Dacă $\Gamma \subseteq E_\sigma$ și κ este un cardinal infinit, spunem că Γ este κ-**categorică** dacă pentru orice σ-structuri $\mathcal{A}$ și $\mathcal{B}$ care au universul de cardinal κ, iar $\mathcal{A} \models \Gamma$ și $\mathcal{B} \models \Gamma$, avem $\mathcal{A} \simeq \mathcal{B}$.

Testul Łoś-Vaught

Teoremă (Testul Łoś-Vaught)

Considerăm signatura $\sigma = (F, R, r)$. Fie $\Gamma \subseteq E_\sigma$ satisfiabilă astfel încât Γ nu are modele finite și κ un cardinal cu $\max(|F \cup R|, \aleph_0) \leq \kappa$ astfel încât Γ este κ-categorică. Atunci Γ este completă.

Demonstrație

Presupunem prin absurd că Γ nu este completă. Atunci există φ cu $\Gamma \not\models \varphi$ și $\Gamma \not\models \neg\varphi$, deci $\Gamma \cup \{\neg\varphi\}$ și $\Gamma \cup \{\varphi\}$ au modele, ce din ipoteză au necesar universul infinit. Aplicând Teorema Löwenheim-Skolem, obținem că există σ-structuri $\mathcal{A}$ și $\mathcal{B}$ cu universul de cardinal κ astfel încât $\mathcal{A} \models \Gamma \cup \{\neg\varphi\}$, iar $\mathcal{B} \models \Gamma \cup \{\varphi\}$. Cum Γ este κ-categorică, avem că $\mathcal{A} \simeq \mathcal{B}$, deci $\mathcal{A} \equiv \mathcal{B}$, ceea ce contrazice faptul că $\mathcal{A} \models \neg\varphi$ și $\mathcal{B} \models \varphi$.

Teoria corpurilor

Considerăm signatura σ_a ce conține simbolurile de operație $+$, $-$, $\cdot$ ce au aritatea 2, precum și constantele 0 și 1. Putem codifica faptul că o σ_a-structură este inel, iar adăugând la acele enunțuri pe următoarele:

$$\neg(0 = 1)$$

$$\forall x(\neg(x = 0) \to \exists y(x \cdot y = 1))$$

obținem că acea structură este chiar corp (engl. *field*).

Un corp k se numește **algebric închis** (engl. *algebraically closed field*) dacă orice $f \in k[x]$ neconstant are o rădăcină în k. Acest lucru se codifică în felul următor – pentru orice $n \in \mathbb{N}$, notăm cu φ_n enunțul

$$\forall a_0 \ldots \forall a_n \exists x \quad x^{n+1} + \sum_{i=0}^{n} a_i x^i = 0.$$

Adăugând aceste enunțuri la mulțimea de enunțuri ce axiomatizează corpurile, obținem o mulțime pe care o notăm cu ACF. Orice corp algebric închis este infinit (exercițiu de algebră).

Cunoaștem de la algebră că, dat fiind un corp k, în cazul în care există un $n \in \mathbb{N}$ astfel încât 1 adunat cu el însuși de n ori este 0 în k, atunci acel n este prim și se numește **caracteristica** lui k, iar în cazul în care nu există un asemenea n, spunem că acea caracteristică este 0. Pentru orice număr prim p, notăm cu ψ_p enunțul

$$\underbrace{1 + \ldots + 1}_{\text{de } p \text{ ori}} = 0.$$

Vom nota apoi, pentru orice p, $ACF_p := ACF \cup \{\psi_p\}$, iar $ACF_0 := ACF \cup \{\neg\psi_q \mid q \text{ prim}\}$.

Teorema fundamentală a algebrei spune că $\mathbb{C}$ este un corp algebric închis, deci este model pentru ACF_0. Pentru orice număr prim p, există un „cel mai mic” corp algebric închis de caracteristică p, care este notat cu $\overline{\mathbb{F}}_p$. Vom folosi proprietatea ce spune că pentru orice p și orice $A \subseteq \overline{\mathbb{F}}_p$ finită, cel mai mic subcorp al lui $\overline{\mathbb{F}}_p$ ce conține pe A este tot finit.

Categoricitate

Vom mai folosi un fapt de algebră fără demonstrație, ce spune că pentru orice caracteristică și orice cardinal nenumărabil, orice două corpuri algebric închise de acel cardinal și acea caracteristică sunt izomorfe. Avem deci:

Corolar

- ACF_0 nu are modele finite, iar pentru orice cardinal nenumărabil κ, este κ-categorică.
- Pentru orice număr prim p, ACF_p nu are modele finite, iar pentru orice cardinal nenumărabil κ, este κ-categorică.

Aplicând testul Łoś-Vaught, obținem:

Corolar

- ACF_0 este completă.
- Pentru orice număr prim p, ACF_p este completă.

Acest corolar ne furnizează alte exemple de structuri neizomorfe care sunt elementar echivalente.

Mai departe, avem:

Corolar

- Mulțimea consecințelor lui ACF_0 este decidabilă.
- Pentru orice număr prim p, mulțimea consecințelor lui ACF_p este decidabilă.

Corolar

$Th(\mathbb{C})$ este decidabilă.

Demonstrație

Cum $\mathbb{C} \models ACF_0$, iar ACF_0 este completă, avem că $ACF_0 \sim Th(\mathbb{C})$, deci mulțimea consecințelor lui ACF_0 este egală cu mulțimea consecințelor lui $Th(\mathbb{C})$. Dar prima este decidabilă, iar a doua este chiar $Th(\mathbb{C})$, ceea ce ne rezolvă problema.

Echivalența

Propoziție

Fie $\varphi \in E_{\sigma_a}$. Următoarele afirmații sunt echivalente:

- $\mathbb{C} \models \varphi$;
- $ACF_0 \models \varphi$;
- există $\mathcal{A}$ cu $\mathcal{A} \models ACF_0 \cup \{\varphi\}$;
- pentru orice $m \in \mathbb{N}$, există $p > m$ prim și $\mathcal{A}$ cu $\mathcal{A} \models ACF_p \cup \{\varphi\}$;
- există $m \in \mathbb{N}$ astfel încât pentru orice $p > m$ prim, $ACF_p \models \varphi$.

Demonstrație

Echivalența primelor trei afirmații este dată de faptul că ACF_0 este completă. Demonstrăm că a doua afirmație o implică pe a cincea. Din Teorema de compacitate, avem că există $m \in \mathbb{N}$ cu $ACF \cup \{\neg\psi_q \mid q < m\} \models \varphi$. Dar pentru orice $p > m$ prim, avem că $ACF_p \models ACF \cup \{\neg\psi_q \mid q < m\}$, deci $ACF_p \models \varphi$, ceea ce trebuia demonstrat.

Echivalența

Demonstrație (cont.)

Faptul că a cincea afirmație o implică pe a patra este imediat.

Demonstrăm acum că a patra afirmație o implică pe a doua. Presupunem prin absurd că $ACF_0 \not\models \varphi$. Cum ACF_0 este completă, avem că $ACF_0 \models \neg\varphi$. Aplicând același raționament ca mai înainte, obținem că există $n \in \mathbb{N}$ astfel încât pentru orice $q > n$ prim, $ACF_q \models \neg\varphi$, ceea ce contrazice ipoteza.

Funcții injective pe mulțimi finite

Următoarea propoziție este un exercițiu de teoria mulțimilor.

Propoziție

Fie A o mulțime finită și $f : A \to A$. Următoarele afirmații sunt echivalente:

- f este injectivă;
- f este surjectivă;
- f este bijectivă.

Corolar

Fie $n \in \mathbb{N}$, k un corp finit și $f : k^n \to k^n$ polinomială injectivă. Atunci f este surjectivă.

Caracteristică primă

Propoziție

Fie $n \in \mathbb{N}$, p un număr prim și $f : (\overline{\mathbb{F}}_p)^n \to (\overline{\mathbb{F}}_p)^n$ polinomială injectivă. Atunci f este surjectivă.

Demonstrație

Presupunem prin absurd că există p prim și $f : (\overline{\mathbb{F}}_p)^n \to (\overline{\mathbb{F}}_p)^n$ polinomială injectivă nesurjectivă, deci există $x \in (\overline{\mathbb{F}}_p)^n \setminus \mathrm{Im} f$. Fie A mulțimea coeficienților componentelor lui f, iar B mulțimea componentelor lui x. Atunci $A \cup B$ este finită, iar, din cele spuse mai devreme, cel mai mic subcorp al lui $\overline{\mathbb{F}}_p$ ce conține pe $A \cup B$ este și el finit și îl notăm cu k. Atunci f induce o funcție polinomială injectivă nesurjectivă de la k^n la k^n, contradicție!

Teorema Ax-Grothendieck

Teorema Ax-Grothendieck

Fie $n \in \mathbb{N}$ și $f : \mathbb{C}^n \to \mathbb{C}^n$ polinomială injectivă. Atunci f este surjectivă.

Demonstrație

Pentru orice $n, d \in \mathbb{N}$, există (exercițiu!) un σ_a-enunț $\chi_{n,d}$ astfel încât pentru orice corp k, avem că $k \models \chi_{n,d}$ dacă și numai dacă pentru orice $f : k^n \to k^n$ polinomială injectivă astfel încât toate componentele lui f sunt de grad cel mult d, avem că f este surjectivă. Propoziția precedentă spune, deci, că pentru orice p prim și orice $n, d \in \mathbb{N}$, $\overline{\mathbb{F}}_p \models \chi_{n,d}$. Din echivalența de mai devreme, avem că pentru orice $n, d \in \mathbb{N}$, avem $\mathbb{C} \models \chi_{n,d}$, ceea ce trebuia demonstrat.

Pentru a pune punct

Dacă doriți să știți mai multe

Acest curs a acoperit, firește, doar o mică parte din logica matematică, însă pe pagina cursului:

https://cs.unibuc.ro/~asipos/lm/

am indicat anumite referințe bibliografice suplimentare, dintre care evidențiez acum ghidul exhaustiv al lui Peter Smith, intitulat *Beginning Mathematical Logic: A Study Guide*, accesibil la adresa:

https://www.logicmatters.net/tyl/

În FMI

De asemenea, în facultatea noastră există un număr de profesori care își desfășoară activitatea științifică în logica matematică, o parte dintre ei fiind grupați în Centrul de Cercetare în Logică, Optimizare și Securitate (LOS):

https://los.cs.unibuc.ro/

care organizează și seminarul științific de logică:

https://los.cs.unibuc.ro/seminar-logic.html

Vă mulțumesc pentru atenție.

Succes la examen!