

A matematika megalapozása típuselmélettel

Kaposi Ambrus

Eötvös Loránd Tudományegyetem

Az informatika napjainkban – modern megközelítések és kapcsolódások.
Az MTA Informatika- és Számítástudományi Bizottság rendezvénye

Budapest
2026. január 8.

Tartalom

1. Számítógépes bizonyításellenőrzők használói
2. Halmazelmélet és típuselmélet
 - 2.1 absztrakció
 - 2.2 konstruktivitás
 - 2.3 extenzionalitás

Írásos változat:

Kaposi Ambrus, Molnár Zoltán. Mi az a típuselmélet és mire jó?
Érintő Elektronikus Matematikai Lapok 

Számítógépes bizonyításellenőrző (proof assistant, interactive theorem prover)

- ▶ A matematikust segíti a bizonyítás leírásában és ellenőrzi a bizonyítást
 - ▶ \leftrightarrow automata tételezbizonyítók (SMT solvers, pl. Z3)
 - ▶ Példák:



- ▶ Kik használják ezeket?

Felhasználó: Vladimir Voevodsky



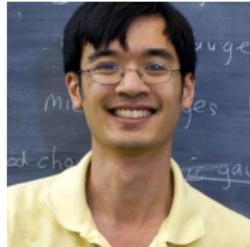
- ▶ 1989. Voevodskii, Kapranov. ∞ -groupoids as a model for a homotopy category. Communications of the Moscow Mathematical Society
- ▶ 1998. Simpson. Homotopy types of strict 3-groupoids
 - ▶ Cáfolja a fenti cikk fő eredményét
- ▶ 2013. Voevodsky elismeri a hibát
- ▶ Innentőlazzal foglalkozik, hogyan lehet számítógéppel bizonyításokat ellenőrizni, és Rocq-ban dolgozik

Felhasználó: Peter Scholze

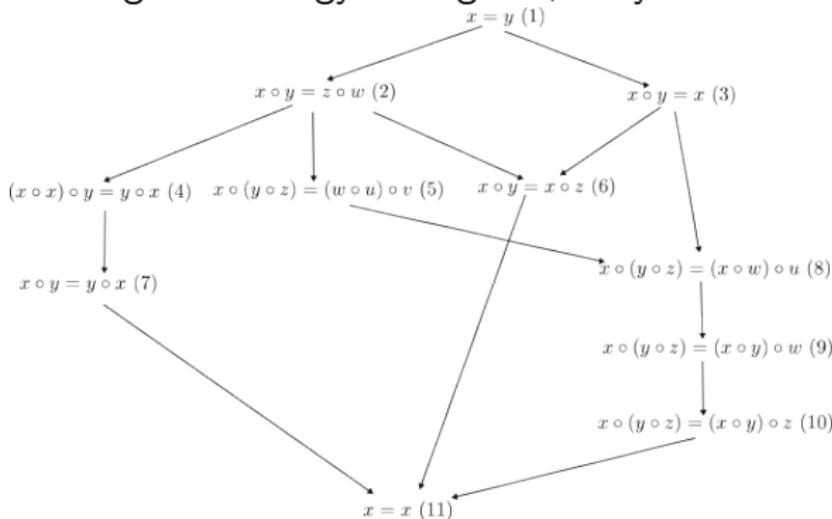


- ▶ Liquid tensor experiment: egy likvid vektorterekről szóló téTEL (Clausen–Scholze)
 - ▶ 2020 dec. Scholze eddigi legfontosabb tétele, nem teljesen biztos a helyességében, még senki sem ellenőrizte
 - ▶ 2021 jún. Lean-ben formalizálták a kérdéses részeket (Johan Commelin vezetésével)
 - ▶ 2022 júl. Teljesen kész a formalizálás.
 - ▶ Tanulságok: egyszerűsödött a bizonyítás, Scholze megértette, mitől működik

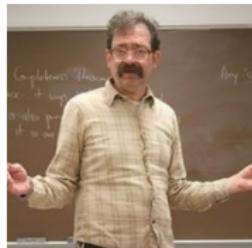
Felhasználó: Terence Tao



- ▶ Magma: egy A halmaz és egy $\circ : A \times A \rightarrow A$ függvény
- ▶ Katalogizálni az egyenlőségeket, melyekben max. 5 változó van.



Felhasználó: Randall Holmes ↗



- ▶ 2010. Bebizonyította Quine „New Foundations” halmazelméletének konzisztenciáját
- ▶ Nem bírta kivárni a bírálókat
- ▶ 2015. Sky Wilshaw segítségével Lean-ben formalizálta

Felhasználó: Kevin Buzzard ↗



- ▶ Elégedetlen, hogy 17 évet kell várni, hogy az Annals of Mathematics visszavonjon egy hibás cikket
- ▶ 2017. Az Imperial College-ben péntek esténként formalizáló klubot alapított, azóta ez nemzetközivé vált, és a teljes BSc/MSc szintű matematikát belekódolták Lean-be

Formális nyelv a számítógépes bizonyításellenőrzők mögött

- ▶ Elsőrendű logika és halmazelmélet: Mizar



- ▶ Egyszerű típuselmélet:
- ▶ Martin-Löf típuselmélete: Agda Idris

LEAN
THEOREM PROVER

ROCQ

Halmazelmélet és típuselmélet

$t \in A$

$t : A$

$f : A \rightarrow B$

Absztrakció

- ▶ halmazelmélet \sim assembly,
típuselmélet \sim Java
- ▶ Benacerraf. What Numbers Could not Be (1965)
 - ▶ Zermelo: $\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \dots$
 - ▶ Neumann: $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \dots$
 - ▶ A kettőt megkülönbözteti a $0 \in 2$ állítás.
- ▶ Bourbaki: ha két halmaz bijekcióban áll, nem szabad megkülönböztetni őket
 - ▶ Általánosabban: izomorf struktúrák megkülönböztethetetlenek.
Pl. ha $M \simeq N$ monoidok, és az egyik kommutatív, a másik is
- ▶ A típuselmélet nyelve ezt úgy éri el, hogy bizonyos dolgok nem kimondhatók: nincs \in, \cup, \cap
- ▶ Lehet-e ilyen megszorított környezetben formalizálni a matematikát?
 - ▶ Hasonló próbálkozás volt a Principia Mathematica...
 - ▶ Igen: Kevin Buzzard által vezetett Lean mathlib implementáció
- ▶ Szinonímák az absztrakcióra: reprezentáció-függetlenség,
strukturalizmus, parametricitás, uniformitás, természetesség,
információ elrejtése

Technikai különbségek

elsőrendű logika
 $\wedge, \vee, \supset, \forall, \exists$

halmazelmélet
axiómái

$t \in A$

típuselmélet

$t : A$

állítások
típusként
elkódolva
 $\wedge, \vee, \supset, \forall, \exists$

Néhány példa:

$0 \in 2$ állítás

$0 : 2$ nyelvtanilag hibás

$1 \in \forall$ nyelvtanilag hibás

$t \in A$ dinamikus információ

$t : A$ statikus információ

$\mathbb{N} \subset \mathbb{Z}$

$n : \mathbb{N}$, de $n : \mathbb{Z}$ nem teljesül

részhalmaz, karakterisztikus függvény

csak karakterisztikus függvény,
pl. $\text{isNonNeg} : \mathbb{Z} \rightarrow \text{Bool}$

Konstruktivitás

- ▶ Klasszikus logika: kizárt harmadik elve (minden A állításra $A \vee \neg A$), kiválasztási axióma
- ▶ A típuselmélet általánosabb, lehetünk konstruktívak és klasszikusak is
- ▶ Ha nem használjuk a fenti klasszikus elveket, akkor a típuselmélet axióma-mentes!
 - ▶ $\forall x, y \in \mathbb{N}. \exists z \in \mathbb{N}. (z|x) \wedge (z|y) \wedge \forall z' \in \mathbb{N}. ((z'|x) \wedge (z'|y)) \supset z' \leq z$
 $\Pi x, y : \mathbb{N}. \Sigma z : \mathbb{N}. (z|x) \times (z|y) \times \Pi z' : \mathbb{N}. ((z'|x) \times (z'|y)) \rightarrow z' \leq z$
 - ▶ $2 = 2$ bizonyítása bizonyítja $(1 + 1 = 2)$ -t is.
- ▶ Bishop 1967-ben megmutatta, hogy az analízist fel lehet építeni konstruktívan is.
 - ▶ Óvatosnak kell lenni. Pl. f injektivitása: $x \neq y \rightarrow f(x) \neq f(y)$ helyett $f(x) = f(y) \rightarrow x = y$

Extenzionalitás

- ▶ Halmazelmélet: ha két halmaznak ugyanazok az elemei, akkor egyenlők
- ▶ Típuselméletben ez értelmetlen (egy term csak egy típusba tartozik)
- ▶ Helyette: Voevodsky univalence axiómája: $(A \cong B) \rightarrow (A = B)$
- ▶ Következmény: az egyenlőség már nem feltétlenül állítás!

A típus állítás, ha minden $a, a' : A$ -ra az $a =_A a'$ típusnak van eleme

A típus halmaz, ha minden $a, a' : A$ -ra az $a =_A a'$ állítás

A típus groupoid, ha minden $a, a' : A$ -ra az $a =_A a'$ halmaz

...

- ▶ Példák:

Állítások: $2 =_{\mathbb{N}} 3$, $\Pi x : \mathbb{N}. x + 1 =_{\mathbb{N}} 1 + x$, $\Pi x : \mathbb{N}. (x = 1) \times (x = 2)$

Halmazok: \mathbb{N} , \mathbb{R} , $\mathbb{N} \rightarrow \mathbb{R}$, $\mathbb{R} \times \mathbb{R}$, $\{0, 1\}$

Groupoidok: halmaz, magma, csoport, gyűrű
 $e, e' : (\{0, 1\} =_{\text{halmaz}} \{0, 1\})$

Típuselmélet és univalence

- ▶ A típuselmélet megvalósítja Benacerraf álmát: a matematika olyan megalapozása, amelyben lehet reprezentáció-függetlenül érvelni
- ▶ Voevodsky univalence axiómája $((A \cong B) \rightarrow (A = B))$ ezt belsővé teszi
- ▶ Ez azonban axióma:
 - ✓ absztrakció
 - ✓ extenzionalitás
 - ✗ konstruktivitás
- ▶ Coquand és mtsai kidolgozták a típuselmélet ∞ -groupoidokra épülő modelljét, és erre alapozva megadták a kubikális típuselmélet
 - ✓ absztrakció
 - ✓ extenzionalitás
 - ✓ konstruktivitás
 - ✗ A típuselmélet megértéséhez kellenek a ∞ -dimenziós absztrakt terek
- ▶ Saját kutatás (folyamatban): Higher Observational Type Theory
 - ✓ absztrakció
 - ✓ extenzionalitás
 - ✓ konstruktivitás
 - ✓ egyszerű szabályok, prematematikai intuíciókkal indokolhatók