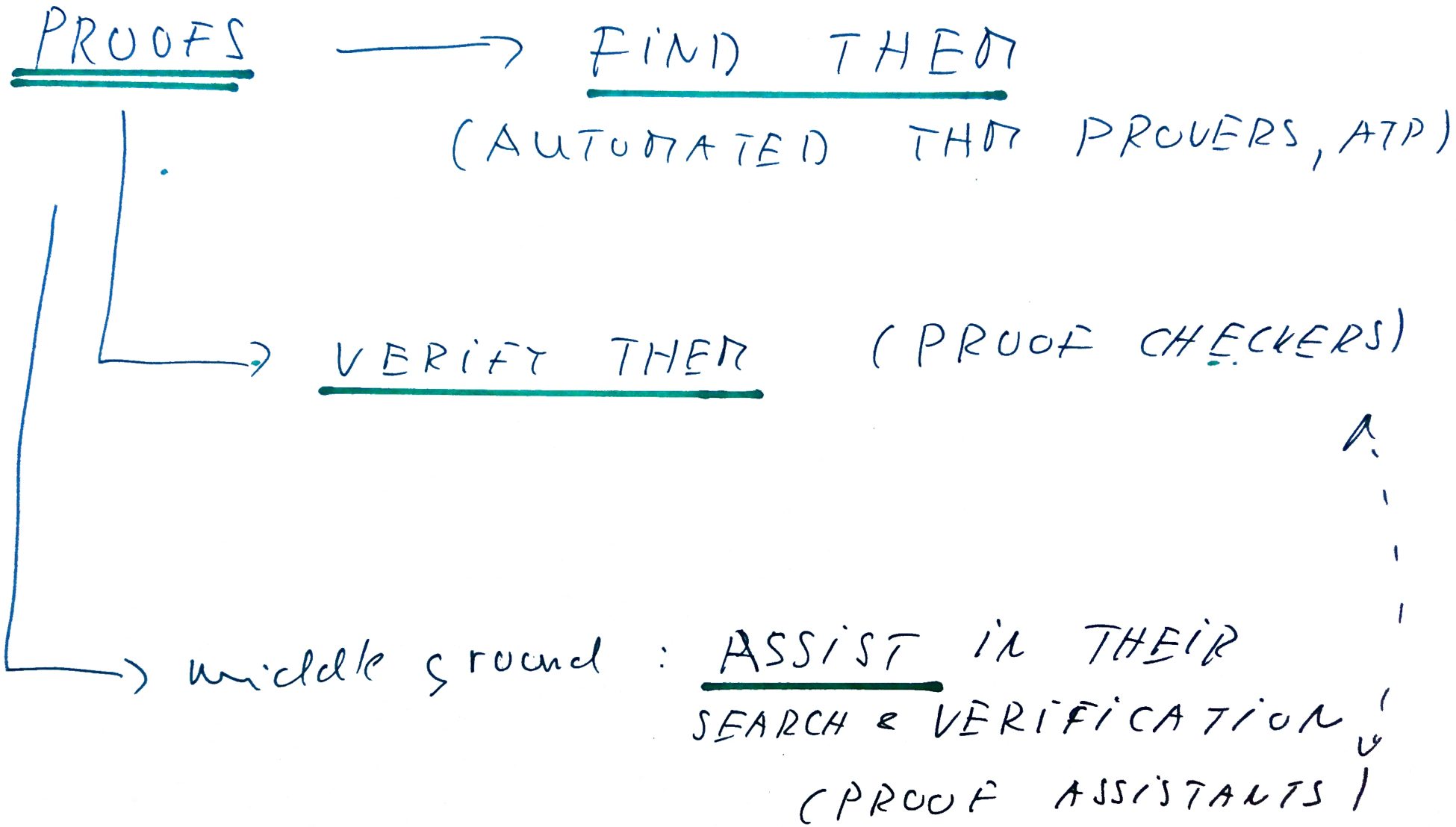
A MATHEMATICAL LOGIC PERSPECTIVE

J. K.

[seminar 8. X. 2021]


PROOFS
FIND THEM
(AUTOMATED THM PROVERS, ATP)
VERIFY THEM
(PROOF CHECKERS)
middle ground : ASSIST IN THEIR SEARCH & VERIFICATION
(PROOF ASSISTANTS!)

G.W. LEIBNIZ (1646-1716)

- CHARACTERISTICA UNIVERSALIS
  (general lang. / formal)
- CALCULUS RATIOCINATOR
  (logical calculus)

G. FREGE

↳ 1879 : BEGRIFFSSCHRIFT

(≈ CONCEPT SCRIPT)

INTRODUCES PREDICATE CALCULUS

AS WE KNOW IT

[PEANO 1892 : Formulario matematico.]

↳ used by him only

G. CANTOR

└→ 1878+ : NAIVE SET TH.,
INFINITE CARDINALITIES, DIAGONAL
ARGUMENT, ...

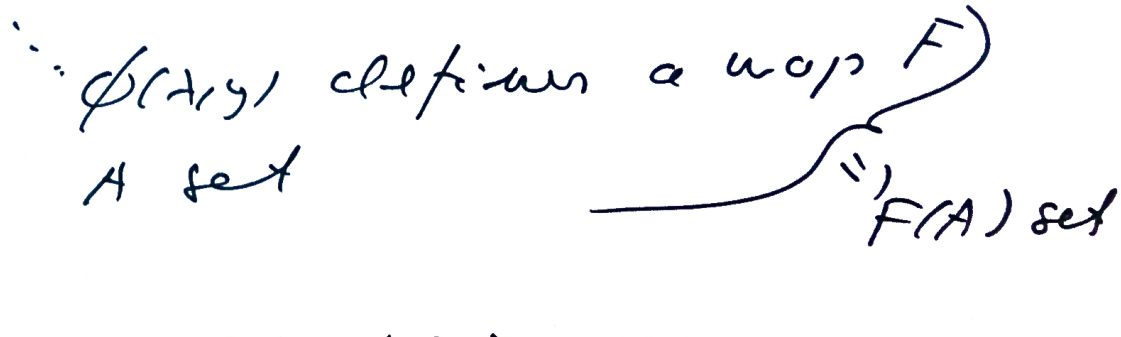
→ ANTINOMIES (= INCONSISTENCY), E.G.
RUSSELL'S 1901:
If $r := \{x \mid x \notin x\}$ then $r \in r \equiv r \notin r$.

[Bolzano : 1800+, .. "Paradoxes of infinity"]

E. ZERMELO

↳ 1908 : SET TH. AXIOMS INCLUDING AX. OF CHOICE (AC)

↳ REPLACEMENT AX. MISSING



↓

FRAENKEL, SKOLEM 1920s

Th. ZFC

[Hilbert, -----]

B. RUSSELL

↳ SIMPLE TYPE TH.

objects have types : 0, 1, 2, ... (x', ...)

"COMPREHENSION": $\phi(x')$ MENTIONS ONLY TYPE i

$\Rightarrow \{x' \mid \phi(x')\}$ EXISTS AND IT IS OF TYPE $i+1$.

✓

[THIS AVOIDS RUSSELL'S PARADOX]

B. RUSSELL – A. N. WHITEHEAD

↳ 1910, -12, -13 : 3-volumes of PRINCIPIA MATHEMATICA

- ATTEMPTS TO REDUCE MATH TO LOGIC
- USES TYPE TH.
- FORMAL

---> [Statement 1 + 1 = 2 appears after almost 400 pp and is fully proved in Vol. 2 only.]

TODAY STANDARD [AFTER BOURBAKI]

↳ MATH ≈ FO-LOGIC + SET TH.

ALTERNATIVES :

↳ CATEGORICAL FOUNDATIONS
(Topoi, ...)

↳ TYPE TH. / λ-CALC.

↳ INTUITIONISTIC LOGIC

+ VARIOUS BLENDS

A PARTICULARLY LOCAL RECENT ATTEMPT

→ UNIVALENT FOUNDATIONS

SEE THE SEMINAR SOURCE PAGE FOR THE ITEM ABOUT VOEVODSKY'S WORK

A. CHURCH

↳ 1930s : λ-calculus

- OBJECTS ARE NOT SETS BUT <u>FUNCTIONS</u>

(ALSO ARGUMENTS & VALUES, SO A FUNCTION CAN BE APPLIED TO A FUNCTION)

[MENTAL IM. : OBJECTS = COMPUTER CODES]

(more later)

SOME HISTORY OF ATP

↳ 1950s : M. DAVIS, P.C. GILMORE, H. WANG

↳ 1960s : FORMALLY PROOFS ALL PM THMS

↳ 1967 : de BRUIJN : AUTOMATH

↳ 1994 : THE QED MANIFESTO

... died out

.
.
.

1975 : K. APPEL + W. HAKEN : ASSISTED PRF OF THE 4-COLOR THM

1998 : T. HALES : KEPLER'S CONJECTURE

(referees 99% sure)

FLYSPECK/HOL : 2017 FULLY PC CHECKED FORMAL PROOF

→ "essentially" exhaustive search after a reduction

2009 : J. AVIGAD + coauthors : the PRIME NB. THM

(ERDÖS-SELBERG PRF)

I SUGGEST WE CONCENTRATE ON THE FORMALIZATION/CHECKING SIDE AND ON LEAN IN PARTICULAR: IT HAS THE MOST ELABORATE & ELEMENTARY INFO PAGE AIMED AT BEGINNERS

↳ SEE THE SEMINAR SOURCE PAGE

↳ OFFERS FURTHER POPULAR ARTICLES AND TALK'S, E.G.:

NATHANSON', ALIGAH', SCHOLZE'

SOFTWARE USES A LOT OF LOGIC (esp. PROOF TA.)

EX:

- RESOLUTION
- S - CALCULUS
- UNIFICATION
- NORMALIZATION

+ CS TECHNIQUES

- TYPED λ - CALC.
- HIGHER ORDER LOGIC
- NATURAL DEDUCTION
- CALCULUS OF CONSTRUCTION
- NON - CLASSICAL LOGIC

NEXT: A VERY BRIEF BASIC BACKGROUND ON

- FO LOGIC

- SIMPLE TYPED λ-calculus.

FO PREDICATE CALCULUS

lang. : $\wedge, \vee, \neg, \rightarrow, \ldots$
$x, y, z, \ldots$
$\exists, \forall$
$(,), \ldots$
$=$

} common

constants : $0, 1$

rel. symb. : $x < y$

funct. symb. : $x + y, \; x \cdot y$

} SPECIFIC VOCABULARY

EX : lang. of real closed fields

[Chpt. 2 in van den Dries - see Ito pox]

Terms: $(x + 0) \cdot 1$

formulas: $\forall x\ (x > c \to (\exists y, y \cdot y = x))$

Theory: a set of sentences

↳ Σ_x: RCF (real closed fields)

↳ Ax's: - ax.'s of ordered fields

- "every odd-deg poly has a root"

- "every positive nb. is a $\square$"

ALL SYNTAX ENCODED BY BINARY STRINGS

$Prf_T(x,y)$: "x is a T-proof of y"

FACT : If "$z \in T$" is ALGORITHMICALLY DECIDABLE,
so is $Prf_T(x,y)$.

If "$z \in T$" $\in$ PTIME, also $Prf_T(x,y) \in P$.

TRUE FOR ZFC, PA, RCF, ...

COROLLARY: WE CAN VERIFY FORMAL ZFC-PROOFS IN P-TIME (≃ quadratic).

=

A LIMITING FACTOR COULD BE THE LENGTH OF FORMAL PROOFS BUT:

$$|\text{FORMAL PRF}| \leq (\text{small const.}) \cdot |\text{ENGLISH PRF}|$$

$$\vdots$$

$$\simeq 4$$

PROOF SEARCH ?

FACT: $\exists x \, Prf_{ZFC}(x, y)$ IS ALG. UNDECIDABLE.

HENCE $|x|$ CANNOT BE COMPUTABLY BOUNDED IN TERMS OF y.

$\Leftarrow$ HALTING PROBLEM

$\Leftarrow$ ENTSCHEIDUNGSPROBLEM: $\exists x \, Prf_{\varphi}(x, y)$ ALSO UNDEC.

PROPOSITIONAL LOGIC CASE

$\Rightarrow$ COMPUTATIONAL COMPLEXITY TH.

$\exists x \; Prf_{PC}(x, y)$: SOLVABLE IN EXP. TIME

PC : prop. calc.

(EXH. SEARCH OVER TRUTH ASSIGN.'S)

- P vs NP problem : ~~SAT~~ TAUT IN P-TIME ?

- NP vs coNP problem : $\exists x \; (|x| \leq poly(|y|) \; Prf_P(x, y)$

some P ?

CLASSICAL SEMANTICS (TARSKIAN)

$\mathcal{IR} \models \varphi$

TRUE or FALSE

BUT HOW DO WE KNOW?

↳ BY HAVING A PROOF ONLY.

CONSTRUCTIVE MATHEMATICS

≈ "PROOFS INSTEAD OF STRUCTURES"

(AND "CONSTRUCTIONS INSTEAD OF $\exists x$")

↳ BROUWER'S INTUITIONISM

(Heyting, Kolmogorov, Poincaré, ...)

↳ MARKOV'S CONSTRUCTIVE LOGIC

(many VARIANTS)

SIMPLY TYPED λ-CALCULUS

Types: NOT JUST 0, 1, ... BUT MORE COMPLEX AND NOT LINEARLY ORDERED.

Some basic types:

$\mathbb{N}$: natural nb's

$\mathbb{B}$: Boolean values 0, 1

⋮

(SIMPLE) TYPE FORMATION

A, B types

$A \to B$ IS A TYPE

→ OBJECTS ARE FUNCTIONS FROM A-TYPE OBJ'S WITH VALUES IN B-TYPE OBJ'S.

Ex's:

$\mathbb{N} \to \mathbb{B}$: subsets of $\mathbb{N}$ $(= \mathcal{P}(\mathbb{N}))$

$(\mathbb{N} \to \mathbb{B}) \to \mathbb{B}$: $\mathcal{P}(\mathcal{P}(\mathbb{N}))$

$\mathbb{N} \to \mathbb{N}$: unary arith. functions

$\mathbb{N} \to (\mathbb{N} \to \mathbb{N})$: binary ...

$(\mathbb{N} \to \mathbb{N}) \to \mathbb{N}$: functionals

⋮

TERMS :

VARIABLES : $x, y, \ldots, s, t, \ldots$ e.g. $\boxed{x : A}$ $\Rightarrow$ "x has type A"

COMPOSITION : IF $a : A$ AND $t : A \to B$

THEN ta is A TERM OF TYPE B

SOME CONSTANTS :

$id_A : A \longrightarrow A$ ("identity f.")

$K_{A,y} : A \to (B \to A)$: to any $y : B$

assigns $x : A$

(constant in B)

λ - EXPRESSIONS

$\lambda x.t$: a function assigning to x the value computed by term t (types should match)

Ex's:

$\lambda x.x$: identity

$\lambda x.y$: constant y

[many variants, β-conversion, Curry etc., ...]

OBSERVATION :

$id_A : A \to A$

$K : A \to (B \to A)$

formation rule:

$$\frac{a : A \qquad t : A \to B}{ta : B}$$

$\Longrightarrow$

PROP. TAUTOLOGIES

$p \to p$

$p \to (q \to p)$

AND INFER. RULE

MODUS PONENS

$$\frac{p \qquad p \Rightarrow q}{q}$$

(rather a miracle)

CURRY - HOWARD ISO

types $\rightleftharpoons$ formulas

terms $\rightleftharpoons$ proofs

slogan: "proofs as types"

[many variants & extensions, relates to functional progr. languages]

SUMMARY: λ-CALC SPEAKS AT THE SAME TIME ABOUT PROOFS AND COMPUTATIONS

SOME Q's :

- IS THERE SOME FUNDAMENTAL REASON WHY "ORDINARY" FORMALIZATION BASED ON FOL LOGIC + ZFC CANNOT BE USE?
- OR IS IT "JUST" PROGRAMMERS CONVENIENCE?