Revisiting SAD

Steffen Frerix and Peter Koepke, University of Bonn, Germany

AITP 2018, March 25–30, 2018, Aussois, France

Tuesday, March 27

On Correctness of Mathematical Texts from a Logical and Practical Point of View

Konstantin Verchinine[1], Alexander Lyaletski[2],
Andrei Paskevich[2], and Anatoly Anisimov[2]

[1] Université Paris 12, IUT Sénart/Fontainebleau,
77300 Fontainebleau, France
[2] Kyiv National Taras Shevchenko University, Faculty of Cybernetics,
03680 Kyiv, Ukraine*

[integer/-s] [program/-s] [code/-s] [succeed/-s] [decide/-s] [halt/-s]

Signature PrgSort. A program is a notion. Let U,V stand for programs.

Signature IntSort. An integer is a notion. Let x,y,z stand for integers.

Signature CodeInt. A code of W is an integer.

Axiom ExiCode. Every program has a code.

Signature HaltRel. W halts on x is an atom.

Signature SuccRel. W succeeds on x and y is an atom.

Definition DefDH. W decides halting iff

for every z and every code x of every V

W succeeds on x and z iff V halts on z.

Axiom Cantor. Let W decide halting.

Then there exists V such that for every y

V halts on y iff W does not succeed on y and y.

Proposition. No program decides halting.

Evidence Algorithm

V.M. Glushkov – 1966 – Institute of Cybernetics – Kiev, Ukraine

Task: assistance to a working mathematician

Form: mathematical text processing, proof verification

Research:

- formal languages for mathematical text's presentation
- deductive routines which determine what is «evident»
- information environment, a library of mathematical knowledge
- interactive proof search

Principles:

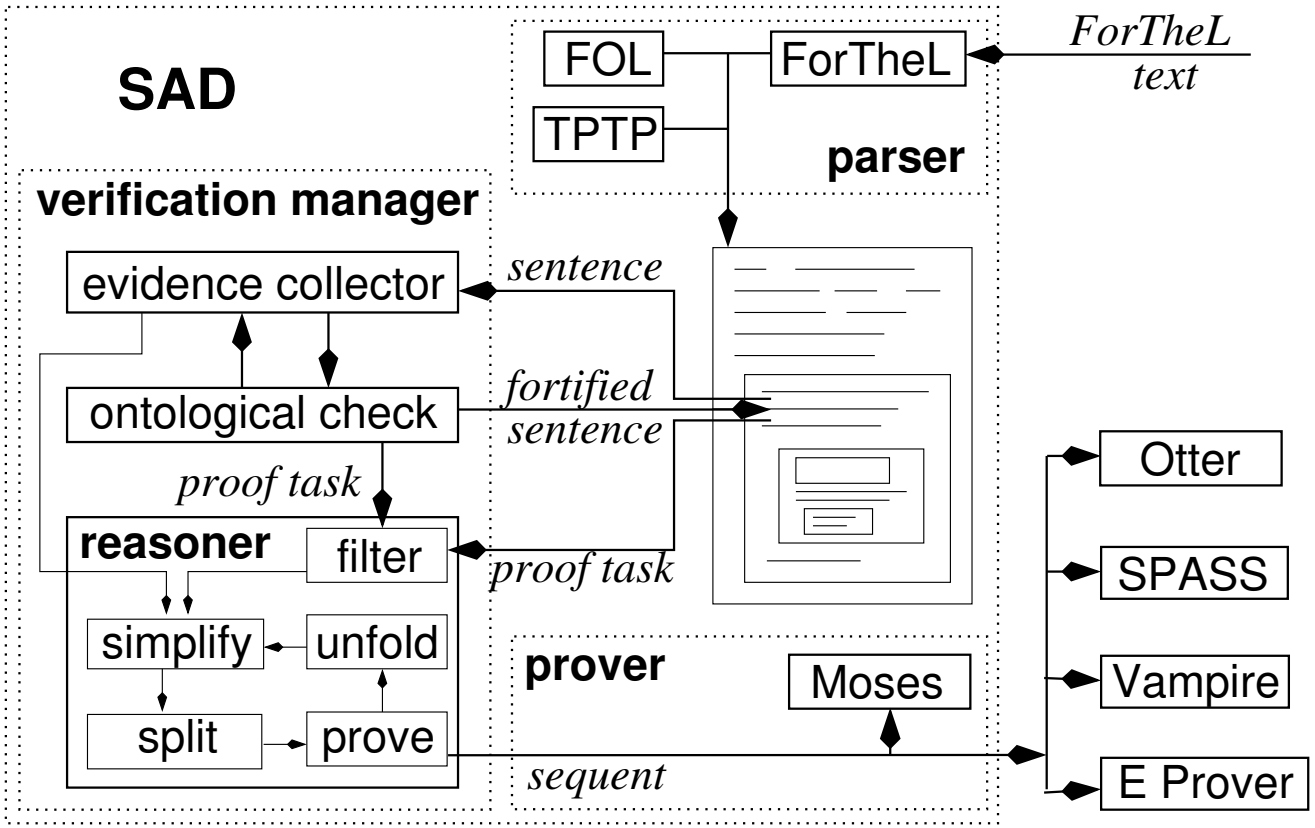
- closeness to a natural language
- closeness to a natural reasoning

Developed:

- languages of formal theories
- goal-driven sequent calculi
- ...

Result: System for Automated Deduction (SAD) — 1978, 2003

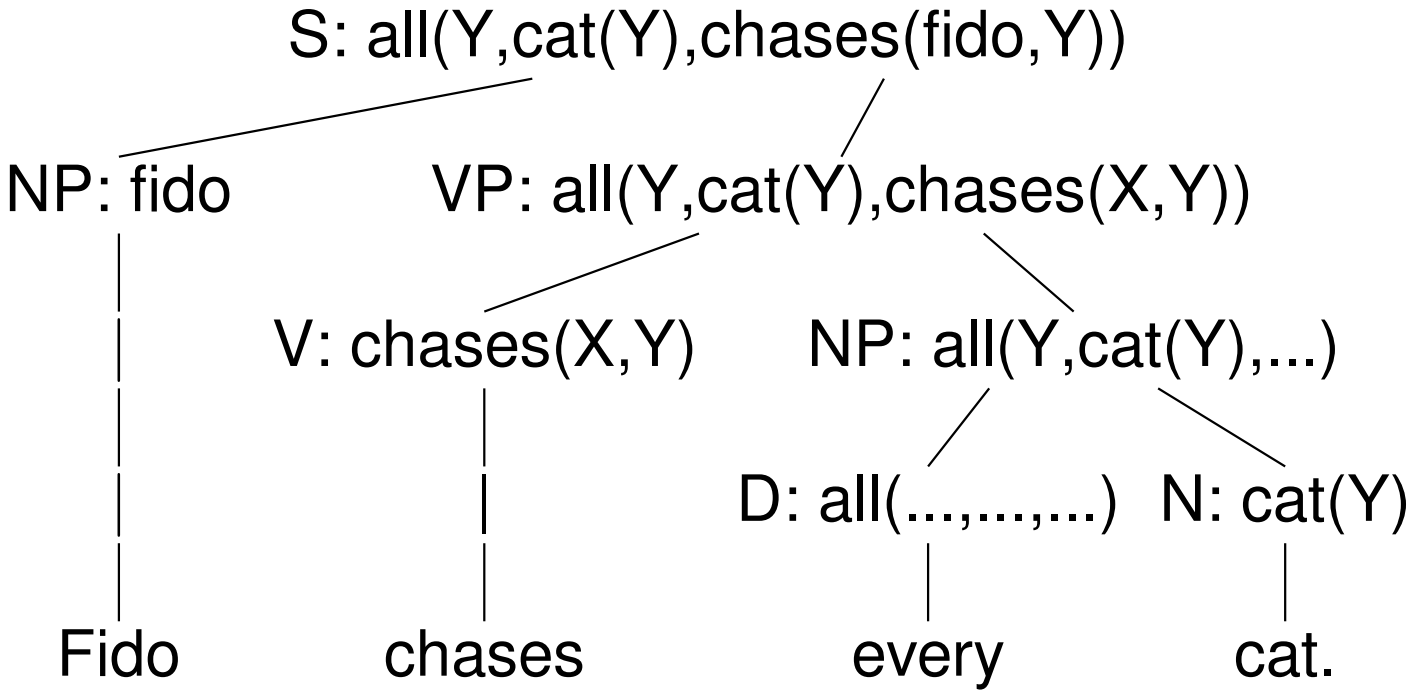
System for Automated Deduction



- **manager**: decompose input text into separate proof tasks
- **reasoner**: big steps of reasoning, heuristic proof methods
- **prover**: inference search in a sound and complete calculus

Linguistic analysis

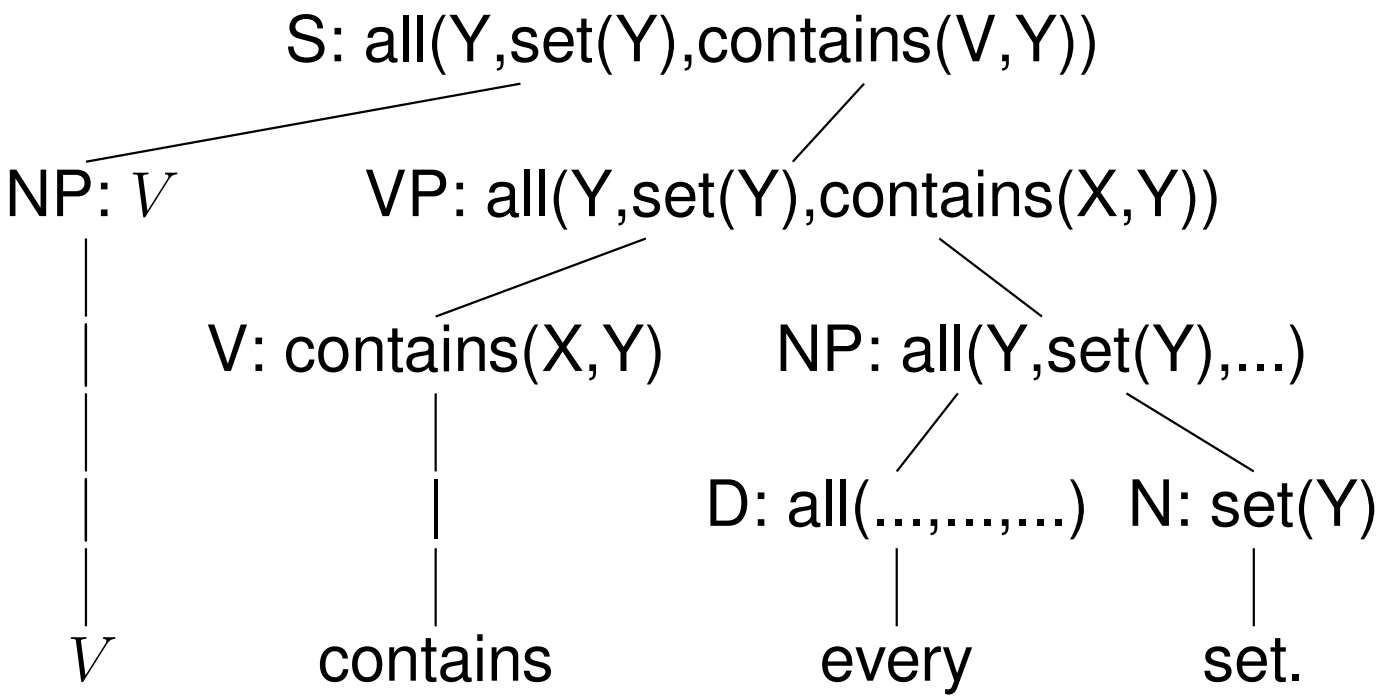
“Fido chases every cat.”



$\forall Y\,(\mathrm{cat}(Y) \rightarrow \mathrm{chases}(\mathrm{fido}, Y))$.

Linguistic analysis

"V contains every set."



$\forall Y\,(\mathrm{set}(Y) \rightarrow V \supseteq Y)$.

Theorem 4. *The set of prime numbers is infinite.*

Proof. Let A be a finite set of prime numbers. Take a function p and a number r such that p lists A in r steps. $\mathrm{ran}p \subseteq \mathbb{N}^+$. $\prod_{i=1}^{r} p_i \neq 0$. Take $n = \prod_{i=1}^{r} p_i + 1$. n is nontrivial. Take a prime divisor q of n.

Let us show that q is not an element of A. Assume the contrary. Take i such that $(1 \leq i \leq r$ and $q = p_i)$. p_i divides $\prod_{i=1}^{r} p_i$ (by MultProd). Then q divides 1 (by DivMin). Contradiction. qed.

Hence A is not the set of prime numbers. □