Proof Assistants and Proof Formalization

Nicolas Trutmann

Contents

1. Introduction

"unfinished"

what is a proof assistant, why do proofs "hold" in a proof assistant, are there options, which option have we chosen and why, what are we doing with it, (eventually) what have we gotten out of this endeavor
Avigad 2021

2. simply typed lambda calculus as a model of higher order logic

The formulation of simple type theory resembles models[1] where models of first order logic formulas are built from sets, but using ((many?) sorted?) expressions from lambda calculus.

We build the axiom of choice by a choice operator ε_α of type $(\alpha \to Prop) \to \alpha$. So for any predicate $P : (\alpha \to Prop)$, $\varepsilon_\alpha P$ chooses an x such that Px. It is convenient to hold a double viewpoint, with P as a function on the type α and another where P is viewed as a subset of the set of all elements of type α, namely the subset of all x such that Px holds.

This is fine, but impractical. This is usually extended byproof assistants by allowing the user to create definitions, variable substitutions on terms and variable substitution on types. In simple type theory, the last point is not even a semantically meaningful sentence, as we'll soon see.

This establishes simple type theory as a model, alongside set theory, of logic. Halbeisen 2025 This has an immense shortcoming. The language we have described so far doesn't allow us to talk *about* types, only *with* types. Take for example an algebraic structure like a group. While we may be able to talk about the elements of such a group, we do not have the tools necessary to generalize this to statements about *all types which are groups*. Types and terms are kept strictly separate and we can't quantify over them. This distinction of therms and types is not present in set theory. Think for example, of the symbol $\mathbb{Z}$, which, in type theory, would be clearly categorized as a type, however this renders common notations such as "$n\mathbb{Z}$" syntactically meaningless. In set theory on the other hand, both $\mathbb{Z}$ and $n\mathbb{Z}$ are clearly sets (for lack of options) and the second expressions is simply a slight abuse of notation for a perfectly legal construction of a set.

3. dependent type theory

4. setoid hell

5. implementations of extensionality

comparing lean and Rocq with respect to metatheoretical properties that the rocq people care about.

6. SR failures

7. Sylvester's Theorem

Cite the theorem in the form that we prove, big picture overview of the proof, side by side comparison of "semantic" proof vs "formal" proof (vs formal proof?)

[1] in the strict sense of the definition of model theory for set theory

"unfinished"

7.1. Prelude. definitions and such
bilinear form, notation

"unfinished"

The original theorem is over 170 years old but remains reasonably legible to modern readers. Perhaps less familiar to the modern reader is the presentation of the theorem, where the statement is entirely contained in the title of the paper, and the body of the paper is devoted entirely to the proof of the statement.
The title reads:

> A DEMONSTRATION OF THE THEOREM THAT EVERY HOMOGENEOUS QUADRATIC POLYNOMIAL IS REDUCIBLE BY REAL ORTHOGONAL SUBSTITUTIONS TO THE FORM OF A SUM OF POSITIVE AND NEGATIVE SQUARES. [sic.]

We'll be following the more modern approach of Lang, whose theorem reads like this:

THEOREM 7.1 (Sylvester). *Let E be a real vector space with a nondegenerate bilinear form g. There exists an integer $r \in \mathbb{Z}$, $r \geq 0$, if $\{v_1, \ldots, v_n\}$ is an orthogonal basis of E then for r of them we have $v_i^2 > 0$ and for $n - r$ of them $v_i^2 < 0$.*

PROOF. Suppose $v_1, \ldots, v_n$ and $w_1, \ldots, w_n$ were two orthogonal bases.
Let $a_i = v_i^2$ and $b_i = w_i^2$,
of which $a_1, \ldots, a_r > 0$, and $a_{r+1}, \ldots, a_n < 0$
and $b_1, \ldots, b_r > 0$, bnd $b_{r+1}, \ldots, b_n < 0$ for some integers r, s.
It suffices to show that $r = s$.
To that end we'll show that the set $\{v_1, \ldots, v_r, w_{s+1}, \ldots, w_n\}$ is linearly independent. Because then we get that $r + (n - s) \leq n$, and therefore $r \leq s$ and by symmetry, $r = s$.
Suppose that

$$(x_1 v_1 + \cdots + x_r v_r) + (y_{s+1} w_{s+1} + \cdots + y_n w_n) = 0$$

Then

$$x_1 v_1 + \cdots + x_r v_r = -y_{s+1} w_{s+1} - \cdots - y_n w_n$$

squaring both sides yields

$$x_1^2 a_1 + \cdots + x_r^2 a_r = y_{s+1}^2 b_{s+1} + \cdots + y_n^2 b_n$$

.
The left hand side is ≥ 0 and the right hand side is ≤ 0, and therefore 0. It follows that all coefficients are 0, which shows that they are linearly independent.
□

"unfinished"

The original reference is Sylvester 1852.
It is presented in Lang 2002, Thm. 4.1 in a modern way.
Also Norman 1986, Theorem 10.43, which is what's cited on wikipedia.

8. Comparison to existing theorem

I accidentally implemented the existence theorem of an orthogonal basis. This invites for comparison. The underlying structure of the theorem is essentially the same. It requires an existence proof of one nonisotropic vector, and then proceeds by induction on the dimension.

9. timetravelling bugs

Bibliography

Avigad, Jeremy (Aug. 30, 2021). *Foundations*. DOI: 10.48550/arXiv.2009.09541. arXiv: 2009.09541[cs]. URL: http://arxiv.org/abs/2009.09541 (visited on 08/13/2025).

Halbeisen, Lorenz J. (2025). *Combinatorial Set Theory: With a Gentle Introduction to Forcing*. Springer Monographs in Mathematics. Cham: Springer Nature Switzerland. ISBN: 978-3-031-91751-6 978-3-031-91752-3. DOI: 10.1007/978-3-031-91752-3. URL: https://link.springer.com/10.1007/978-3-031-91752-3 (visited on 11/28/2025).

Lang, Serge (2002). *Algebra*. en. Vol. 211. Graduate Texts in Mathematics. New York, NY: Springer. ISBN: 978-1-4612-6551-1. DOI: 10.1007/978-1-4613-0041-0. URL: https://link.springer.com/10.1007/978-1-4613-0041-0.

Norman, C. W. (1986). *Undergraduate algebra: a first course*. en. Oxford : New York: Clarendon Press ; Oxford University Press. ISBN: 978-0-19-853249-1.

Sylvester, J.J. (Aug. 1852). "XIX. A demonstration of the theorem that every homogeneous quadratic polynomial is reducible by real orthogonal substitutions to the form of a sum of positive and negative squares". en. In: *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 4.23, pp. 138–142. ISSN: 1941-5982, 1941-5990. DOI: 10.1080/14786445208647087.