From the Universality of Mathematical Truth to the Interoperability of Proof Systems

Gilles Dowek

From the Universality of Mathematical Truth to the Interoperability of Proof Systems

Gilles Dowek

Inria and ENS Paris-Saclay, France
gilles.dowek@ens-paris-saclay.fr

1 Yet another crisis of the universality of mathematical truth

The development of computerized proof systems, such as Coq, Matita, Agda, Lean, HOL 4, HOL Light, Isabelle/HOL, Mizar, etc. is a major step forward in the never ending quest of mathematical rigor. But it jeopardizes the universality of mathematical truth [5]: we used to have proofs of Fermat's little theorem, we now have Coq proofs of Fermat's little theorem, Isabelle/HOL proofs of Fermat's little theorem, PVS proofs of Fermat's little theorem, etc. Each proof system: Coq, Isabelle/HOL, PVS, etc. defining its own language for mathematical statements and its own truth conditions for these statements.

This crisis can be compared to previous ones, when mathematicians have disagreed on the truth of some mathematical statements: the discovery of the incommensurability of the diagonal and side of a square, the introduction of infinite series, the non-Euclidean geometries, the discovery of the independence of the axiom of choice, and the emergence of constructivity. All these past crises have been resolved.

2 Predicate Logic and other logical frameworks

One way to resolve a crisis, such as that of non-Euclidean geometries, or that of the axiom of choice, is to view geometry, or set theory, as an axiomatic theory. The judgement that the statement *the sum of the angles in a triangle equals the straight angle* is true evolves to that that it is a consequence of the parallel axiom and of the other axioms of geometry. Thus, the truth conditions must be defined, not for the statements of geometry, but for arbitrary sequents: pairs $\Gamma \vdash A$ formed with a theory, a set of axioms, Γ and a statement A.

This induces a separation between the definition of the truth conditions of a sequent: the logical framework and the definition of the various geometries as theories in this logical framework. This logical framework, Predicate logic, was made precise by Hilbert and Ackermann [13], in 1928, more than a century after the beginning of the crisis of non-Euclidean geometries. The invention of Predicate Logic was a huge step forward. But Predicate Logic also has some limitations.

To overcome these limitation, it has been modernized in various ways in the last decades. First, λ-Prolog [15] and Isabelle [17] have extended Predicate logic with variable binding function symbols, such as the symbol λ in the term $\lambda x\ x$. Then, the $\lambda\Pi$-calculus [12] has permitted to explicitly represent proof-trees, using the so-called Brouwer-Heyting-Kolmogorov algorithmic interpretation of proofs and Curry-de Bruijn-Howard correspondence. In a second stream of research, Deduction modulo theory [4, 6] has introduced a distinction between computation and deduction, in such a way that the statement $27 \times 37 = 999$ computes to $999 = 999$, with the algorithm of multiplication, and then to $\top$, with the algorithm of natural number comparison. It thus has a trivial proof. A third stream of research has extended classical Predicate logic to an Ecumenical predicate logic [10, 14, 3, 19, 18, 9, 11] with both constructive and classical logical constants.

These streams of research have merged, to provide a logical framework, the $\lambda\Pi$-calculus modulo theory [2], also called Martin-Löf's logical framework [16]. This framework permits function symbols to bind variables, it includes an explicit representation for proof-trees, it distinguishes computation from deduction, and it permits to define both constructive and classical logical constants. It is the basis of the language Dedukti, where Simple type theory, Martin-Löf's type theory, the Calculus of constructions, etc. can easily be expressed.

3 The theory $\mathcal{U}$

The expression in Dedukti of Simple type theory, Simple type theory with polymorphism, Simple type theory with predicate subtyping, the Calculus of constructions, etc. use symbol declarations and computation rules that play the *rôle* of axioms in Predicate logic. But, just like the various geometries or the various set theories share a lot of axioms and distinguish by a few, these theories share a lot of symbols and rules. This remark leads to defining a large theory, the theory $\mathcal{U}$ [1], that contains Simple type theory, Simple type theory with polymorphism, Simple type theory with predicate subtyping, and the Calculus of constructions, etc. as sub-theories.

Many proofs developed in proof processing systems can be expressed in the theory $\mathcal{U}$ and depending on the symbols and rules they use they can be translated to more common formulations of the theories implemented in these systems.

For instance, F. Thiré has expressed a large library of arithmetic, originally developed in Matita, in an sub-theory of the theory $\mathcal{U}$, corresponding to Simple type theory with polymorphism and translated these proofs to the language of seven proof systems [20], Y. Géran has expressed the first book of Euclid's elements originally developed in Coq, in a sub-theory of the theory $\mathcal{U}$, corresponding to Predicate logic, and translated these proofs to the language of many proof systems, including predicate logic ones [8], and T. Felicissimo has shown that a large library of proofs originally developed in Matita, including a proof of Bertrand's postulate, could be expressed in predicative type theory and expressed in Agda [7].

References

1. F. Blanqui, G. Dowek, É. Grienenberger, G. Hondet, and F. Thiré. Some axioms for mathematics. In N. Kobayashi, editor, *Formal Structures for Computation and Deduction*, volume 195 of *LIPIcs*, pages 20:1–20:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.
2. D. Cousineau and G. Dowek. Embedding Pure Type Systems in the lambda-Pi-calculus modulo. In S. Ronchi Della Rocca, editor, *Typed lambda calculi and applications*, volume 4583 of *Lecture Notes in Computer Science*, pages 102–117. Springer, 2007.
3. G. Dowek. On the definition of the classical connectives and quantifiers. In E.H. Haeusler, W. de Campos Sanz, and B. Lopes, editors, *Why is this a Proof?, Festschrift for Luiz Carlos Pereira*. College Publications, 2015.
4. G. Dowek, Th. Hardin, and C. Kirchner. Theorem proving modulo. *Journal of Automated Reasoning*, 31:33–72, 2003.
5. G. Dowek and F. Thiré. The universality of mathematical truth jeopardized by the development of computerized proof systems. In A. Arana and F. Pataut, editors, *Proofs*. To be published.
6. G. Dowek and B. Werner. Proof normalization modulo. *The Journal of Symbolic Logic*, 68(4):1289–1316, 2003.
7. T. Felicissimo, F. Blanqui, and A. Kumar Barnawal. Predicativize: Sharing proofs with predicative systems. Manuscript, 2022.
8. Y. Géran. Mathématiques inversées de Coq. l'exemple de GeoCoq. Master thesis, 2021.
9. F. Gilbert. *Extending higher-order logic with predicate subtyping: Application to PVS. (Extension de la logique d'ordre supérieur avec le sous-typage par prédicats)*. PhD thesis, Sorbonne Paris Cité, France, 2018.
10. J.-Y. Girard. On the unity of logic. *Annals of Pure and Applied Logic*, 59(3):201–217, 1993.
11. É. Grienenberger. A logical system for an ecumenical formalization of mathematics. Manuscript, 2020.
12. R. Harper, F. Honsell, and G. Plotkin. A framework for defining logics. *Journal of the ACM*, 40(1):143–184, 1993.
13. D. Hilbert and W. Ackermann. *Grundzüge der theoretischen Logik*. Springer-Verlag, 1928.
14. C. Liang and D. Miller. Unifying classical and intuitionistic logics for computational control. In *28th Symposium on Logic in Computer Science*, pages 283–292, 2013.
15. D. Miller and G. Nadathur. *Programming with Higher-Order Logic*. Cambridge University Press, 2012.
16. B. Nordström, K. Petersson, and J.M. Smith. *Programming in Martin-Löf's type theory*. Oxford University Press, 1990.
17. L.C. Paulson. Isabelle: The next 700 theorem provers. In P. Odifreddi, editor, *Logic and Computer Science*, pages 361–386. Academic Press, 1990.
18. L.C. Pereira and R.O. Rodriguez. Normalization, soundness and completeness for the propositional fragment of prawitz'ecumenical system. *Revista Portuguesa de Filosofia*, 73(3-4):1153–1168, 2017.
19. D. Prawitz. Classical versus intuitionistic logic. In E.H. Haeusler, W. de Campos Sanz, and B. Lopes, editors, *Why is this a Proof?, Festschrift for Luiz Carlos Pereira*. College Publications, 2015.

20. F. Thiré. Sharing a library between proof assistants: Reaching out to the HOL family. In F. Blanqui and G. Reis, editors, *Proceedings of the 13th International Workshop on Logical Frameworks and Meta-Languages*, volume 274 of *EPTCS*, pages 57–71, 2018.