Position paper: A real Semantic Web for mathematics deserves a real semantics

P. Corbineau, H. Geuvers, C. Kaliszyk, J. McKinna, F. Wiedijk

ICIS, Radboud University Nijmegen, the Netherlands

Abstract. Mathematical documents, and their instrumentation by computers, have rich structure at the layers of presentation, metadata and semantics, as objects in a system for formal mathematical logic. Semantic Web tools [2] support the first two of these, with little, if any, contribution to the third, while Proof Assistants [17] instrument the third layer, typically with bespoke approaches to the first two. Our position is that a web of mathematical documents, definitions and proofs should be given a fully-fledged semantics in terms of the third layer. We propose a "MathWiki" to harness Web 2.0 tools and techniques to the rich semantics furnished by contemporary Proof Assistants.

1 Background and state of the art

We can identify four worlds of mathematical discourse available on the Web:

- Traditional mathematical practice: a systematic body of knowledge, organised around documents written by experts, most often in LaTeX, to varying degrees of sophistication. The intended audience is an expert readership, and the content is of high quality and reliability, having been through a rigorous editorial process. Indexing and cross-referencing is managed externally by journals themselves, augmented by tools such as CiteSeer, Google Scholar, and archival sites such as ArXiv;
- Wikipedia, MathWorld, *etc.*: universal readership and authorship, wide coverage, but relatively shallow and of variable reliability, with little systematic development of larger theories, and little or no critical gloss on the material;
- The Semantic Web, with the OMDoc standard [9] and tools like SWiM [11], for organising structured documents around a basic notion of "falling under a concept" (such concepts then further organised into content dictionaries);
- The language and (checked) libraries of *proof assistants*, in which concepts, definitions, statements, and most importantly, *proofs* of theorems are represented in a machine-checkable format.

We focus in this paper on the fourth world, as we expect it to be least familiar to readers of the paper, but more importantly because we believe that proof assistants offer a real, that is to say, formal *mathematical* semantics to (a Semantic Web of) mathematical documents. Our aim, and that of our partners in a European consortium, is to integrate all four worlds into a coherent whole, and develop a "MathWiki", a system for the collaborative authoring and communication of computer mathematics to the world.

Proof Assistants The basic idea of using computer programs to check mathematical proofs goes back to the archaeology of AI research. The 1960s saw the emergence of two basic paradigms: de Bruijn's AUTOMATH [16], and Milner's LCF. Both provide highly generic foundational approaches to representing mathematics: as a series of checked objects (definitions etc.) extending a body of knowledge from an initial axiomatisation (e.g. of arithmetic or set theory). In LCF the objects, including proofs of their properties, are obtained by running programs to produce values of an abstract datatype `thm`, that is to say they are *ephemeral* phenomena associated to the persistent program texts which give rise to them. In AUTOMATH, the objects — λ-terms in a dependently-typed language uniformly representing definitions and proofs — are themselves persistent and in principle may be independently rechecked, or otherwise processed.

Modern systems have elaborated these ideas with great sophistication, extensive libraries, and highly non-trivial formalisations:

- The HOL Light system [8] is an LCF-style checker for higher-order logic; Harrison recently announced a proof of the analytic Prime Number Theorem;
- The Isabelle system [15] is also LCF-like, but adds a generic twist in terms of an AUTOMATH-like theory of representation: it is a *logical framework*, that is, it is generic over the underlying choice of logic and axiomatisation. It is available with libraries for both higher-order logic, and for ZF set theory. It has been used to formalise Gödel's completeness theorem, the consistency of the axiom of choice, the Prime Number Theorem, etc.;
- The Coq system [3] is type-theoretic, within which objects and proofs are λ-terms in a calculus of inductive and coinductive definitions; a notable development is Gonthier's formalisation of the Four Colour Theorem [6];
- The Mizar system [13], a proof checker for a strong version of set theory, emphasises developing a formalised library of standard, classical mathematics.

The decisive semantic advantage of all these systems over existing approaches to mathematical documents comes from the infrastructure of a formalised meta-level: names and binding to support substitutive definitions, definitional equality, hypothetical and general reasoning. The Proof Assistant and Semantic Web communities seem to differ over what constitutes a (mathematical) definition:

- in the Semantic Web a definition is a reference to a (canonical) textual description of the defined object; while
- for the proof assistant community a definition is a binding with a dynamic semantics given by a substitutive notion of *definitional equality*, namely the replacement of the named object (*definiendum*) by a body (*definiens*).

2 A project proposal: MathWiki

The MathWiki project proposes to combine a Wikipedia-like encyclopedia of mathematical notions and results, with a web-based integrated formal environment for collaboratively working with multiple proof assistants. Wikipedia has

shown that it is possible to create large bodies of coherent knowledge, by providing lightweight (web-based) functionality to add material. In the MathWiki project we similarly want to provide lightweight web-based functionality to contribute to a repository of formalised mathematics. This should provide both a means to do large joint formalisations in a distributed way, but also the means to search and retrieve material, both at a low level, in terms of proof assistant-specific text, and at the high level of standard mathematical documents.

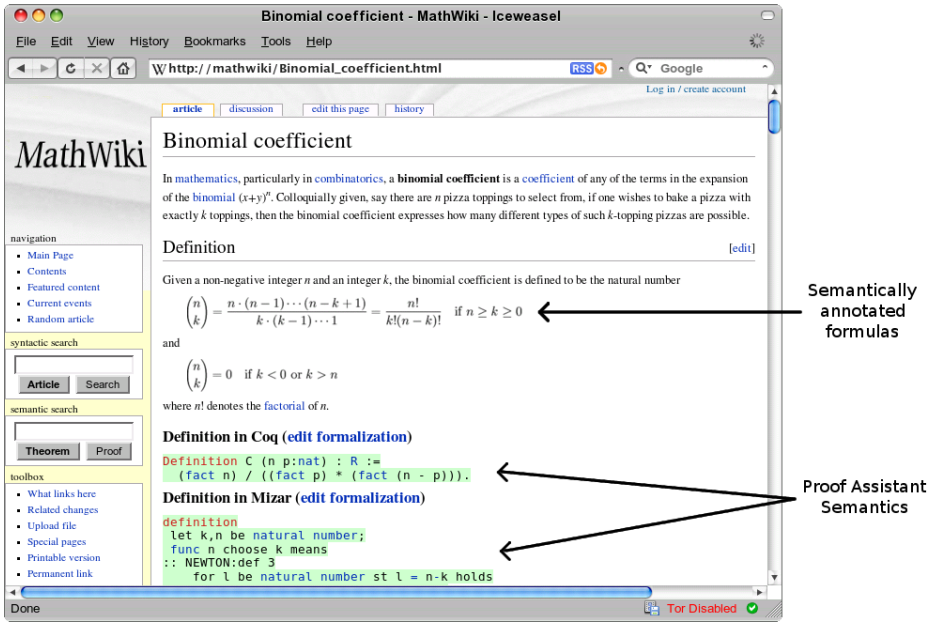

Fig. 1. An example MathWiki page for the binomial coefficient

The MathWiki repository will include knowledge about mathematical concepts by the means of high level concept description pages. Those pages will include links to pages containing the finer details, which are, in the end, checked proof assistant code. We plan to directly incorporate into our project a certain number of state-of-the-art proof assistants. But the MathWiki itself will be open to other systems and it should be easy to incorporate them. The repository will contain all the large libraries of formal mathematics that already exist for the included proof assistants, like the Coq user contributions (*contribs*) and the Archive of Formal Proofs for Isabelle, in order to facilitate access to them.

We have created a prototype [4] that only supports Coq (without any semantic aspects yet), which suggests the project is technically feasible. In Figure 1 we sketch how the eventual system might look (including quoted material from Wikipedia for illustrative purposes).

Our first claim is that a mathematical semantic web where the mathematical notions refer to objects with a real formal semantics in a proof assistant will be profitable for users of mathematics because it improves preciseness and correctness. Our planned MathWiki system should substantiate that claim and open up to a wider community the rich collections of knowledge stored in the repositories of proof assistants and to facilitate the extension and editing of these repositories by outside users.

Our second claim is that the "medium" of *computer checkable formal proofs* will become a valuable asset in ICT, notably in verification and correctness of software and systems. At this moment there is not *one* type of medium for computer checkable formal proofs: basically each proof assistant has its own "media type". We think that in the future these media types will more and more converge and become exchangeable. A real mathematical semantic web is the platform for studying, comparing and exchanging these media types.

3 Why now: QED 15 years later?

The motivation for initiating this project precisely now is the convergence of several decisive factors. One of them is the success of the Wiki approach in general, and mostly the success of its application to the encyclopedic endeavour. This example shows that the collaborative approach is a good way of developing bodies of shared knowledge.

Another key factor is the availability of mature proof assistants with solid reputations and a certain quantity of formal developments. These proof assistants are way past toy examples and now allow outstanding results; they can handle large developments spanning hundreds of files.

Semantic web techniques now available provide a relevant presentation layer to the user. Although formal proofs are highly structured and hence easy to index, it is this extremely precise structure that can leave the user lost in the details, or unable to search or browse effectively.

The last key element we wish to stress is the availability of Web 2.0 technologies, which support the creation of web-based complex user interfaces. These technologies are important for our project since interactive proof development is by far the most popular way of using proof assistants.

Already in 1993 the authors of the QED Manifesto [1] had this vision: to let the whole world participate in creating a shared repository of formalised mathematics. We can speculate as to why this was an idea before its time: inevitably, user communities around each system felt keenly the supposed strengths of their own approach, and the perceived deficiencies of others'. The relative maturity of systems and their libraries has greatly mitigated this state of affairs.

The difficulty of formal proof also restrained the ambition of proof projects attempted, but with eyes on a bigger prize, collective development has become common practice in the formal proof community. This is how the biggest achievements were possible. Mizar and its MML are the primary example of the success of collective development though not very focused. More focused examples are

the CompCert project in which a whole team participated in the verification of a C compiler and the Nijmegen repository of formalised mathematics (CoRN) [5]. The ongoing Flyspeck project [7] is another instance.

Proof assistants proposed to be part of the MathWiki project in the initial phase are Coq, Isabelle and Mizar. They cover three different foundational theories (Type Theory, Higher-Order Logic and Set Theory), and embrace classical as well as intuitionistic mathematics. They also have three different interaction modes: de Bruijn style, LCF-style and batch-mode interaction. Thus the three of them provide an excellent coverage of the variety among existing proof assistants.

4 Conclusion

The power of Wiki technology is to make building a new encyclopedia of mathematics a truly global democratic enterprise. Contemporary proof assistant technology has reached the point where we can imagine such a richly structured web of mathematics with a fully-fledged semantics in a formal system. A real Semantic Web for mathematics deserves a real semantics.

References

1. R. Boyer et al. The QED Manifesto. In Bundy, ed., *Automated Deduction – CADE 12*, *LNAI* 814. Springer, 1994.
2. S. Buswell, O. Caprotti, D.P. Carlisle, M.C. Dewar, M. Gaëtano, and M. Kohlhase. The OpenMath Standard, version 2.0, 2002.
3. Coq Team. *The Coq Proof Assistant Reference Manual V8.1.* INRIA, 2006.
4. P. Corbineau and C. Kaliszyk. Cooperative repositories for formal proofs. In Kauers *et al.* eds., *Calculemus/MKM*, *LNCS* 4573. Springer, 2007.
5. L. Cruz-Filipe, H. Geuvers, and F. Wiedijk. C-CoRN, the constructive Coq repository at Nijmegen. In Asperti *et al.* eds., *MKM*, *LNCS* 3119. Springer, 2004.
6. G. Gonthier. A computer-checked proof of the Four Colour Theorem, 2006.
7. T. C. Hales. Introduction to the flyspeck project. In Coquand *et al.* eds., *Mathematics, Algorithms, Proofs*, *Dagstuhl Proceedings* 05021. IBFI, Germany, 2005.
8. J. Harrison. HOL light: A tutorial introduction. In Srivas and Camilleri, eds., *Proceedings of FMCAD'96*, *LNCS* 1166. Springer, 1996.
9. M. Kohlhase. *OMDoc - An Open Markup Format for Mathematical Documents [version 1.2]*, *LNCS* 4180. Springer, 2006.
10. A.P. Krowne. An architecture for collaborative math and science digital libraries. Master's thesis, Virginia Tech Dept. of Computer Science, Blacksburg, VA, 2003.
11. C. Lange. SWiM – a semantic wiki for mathematical knowledge management. In Bechhofer *et al.* eds., *ESWC*, *LNCS* 5021. Springer, 2008.
12. C. Lange, S. McLaughlin, and F. Rabe. Flyspeck in a semantic wiki. Unpublished.
13. M. Muzalewski. *An Outline of PC Mizar.* Fondation Philippe le Hodey, 1993.
14. R.P. Nederpelt, J.H. Geuvers, and R.C. de Vrijer. *Selected Papers on Automath*, *Studies in Logic and the Foundations of Mathematics* 133. Elsevier, 1994.
15. T. Nipkow, L. C. Paulson, and M. Wenzel. *Isabelle/HOL - A Proof Assistant for Higher-Order Logic*, *LNCS* 2283. Springer, 2002.
16. D.T. van Daalen. A description of Automath and some aspects of its language theory. In Nederpelt et al. [14]. Article A.3.
17. F. Wiedijk, ed. *The Seventeen Provers of the World*, *LNCS* 3600. Springer, 2006.