On a repository of formalized mathematics

Piotr Rudnicki*

Dept. of Computing Science, University of Alberta, Edmonton, Canada
piotr@cs.ualberta.ca

Abstract. We argue for more effort in developing a data base of formal mathematics with a long-term perspective in mind.

I am interested in certain pragmatic aspects of building a repository of formalized, machine-checked mathematics. I take it for granted that the value gained from building such a repository or repositories is self evident. This is a bold assumption in light of the thin response to the QED Manifesto [9], particularly thin from core mathematicians.

It puzzles me why we have so many different automated proof assistant systems for doing formalized mathematics and yet the body of formalized mathematics organized in a systematic way is so pathetically small. I have been involved in the Mizar [8] project for the last 30 years. The Mizar Mathematical Library (MML) is considered the largest of such formalized repositories, yet it is minuscule with respect to the body of established mathematics. Interestingly, even within the Mizar system, people more frequently propose changes to the system rather than, say, volunteer to complete the long ago started formalization of the Jordan curve theorem.

When Bill Farmer invited me to participate in the NA-MKM in Phoenix and told me to prepare a 10 (or so) minute presentation, I was really puzzled about what to say. When I was boarding the plane in Edmonton in the early hours of a very cold day (2004-01-05), I had to spend 2 hours in line in order to cross the American border because of the extra security. While waiting, I grabbed the latest edition of *Discover* magazine, Vol. 25 No. 01, January 2004, containing *Discover's* guide to the top 100 science stories of 2003. Entry number 8 in the guide was contributed by Keith Devlin and titled "2003: Mathematicians Face Uncertainty". Here are some excerpts:

> Early in the year, American mathematician Daniel Goldston and his Turkish colleague Cem Yildirim announced a proof of the twin prime conjecture, ... Although experts around the world initially agreed that the new proof was correct, a few weeks later an insurmountable error was discovered.
>
> In late 2002 the Russian mathematician Grigori Perelman posted on the Internet what he claimed was an outline for a proof of the Poincaré conjecture, ... But after months of examining the argument mathematicians are still unsure whether it is right or wrong.

* Partially supported by NSERC grant OGP9207.

> Never mind a delay of weeks or months—poor Thomas Hales, an American mathematician who has been waiting for *five years* to hear whether the mathematical community has accepted his 1998 proof of astronomer Johannes Kepler's 390-year-old conjecture that the most efficient way to pack equal-size spheres (such as cannonballs on a ship, which is how the question arose) is to stack them in the familiar pyramid fashion that greengrocers use to stack oranges on the counter. After examining Hales's argument for give years, in the spring of 2003 a review panel of world experts appointed by the prestigious journal *Annals of Mathematics* finally declared that, whereas they had not found any irreparable error in the proof, they were still not sure that it was correct. The journal agreed to publish Hales's proof, but only with a disclaimer saying they were not sure that it was right.
>
> ...
>
> So where does all this leave the field of mathematics? ...

Where, indeed?

In light of the existence of so many automated proof assistants one may ask: *Why do the "uncertain" mathematicians not use them?* There are probably many reasons. It might take an exorbitant amount of time to formalize any of the above-mentioned proofs to such a detailed level that known proof checkers could swallow them. It may as well take an exorbitant amount of effort, even if the time could be somewhat curtailed. Would it be worth it?

At the beginning of 2003, Matthias Baaz suggested rewriting into Mizar and mechanically checking Witt's proof of the Wedderburn theorem: *Every finite division ring is commutative.* We followed the brilliant presentation of the proof in Chapter 5 of [1]. Wedderburn published the theorem in 1905 [10], Witt published his proof in 1931 [11], and the theorem and the proof can be found in many algebra textbooks. That is, we are dealing with well-established mathematics. However, Matthias expected that proving this theorem would constitute a challenge as the proof involves aspects of quite diverse areas: algebra, complex numbers, integers, roots of unity, cyclotomic polynomials and polynomials in general. We formulated the theorem easily since MML contained all the needed terminology. In Mizar it is stated as:

```
theorem  for R being finite Skew-Field holds R is commutative;
```

The proof was a different matter altogether and even a cursory look through the proof and MML convinced us that we had a small challenge at hand. As Matthias and I were busy with other stuff, a more serious attempt at the proof was undertaken by Broderick Arneson, a summer student working under my supervision. Broderick did not know Mizar when he started in May of 2003. Since I was in Japan and Matthias was in Vienna, Broderick learned Mizar on his own with some help from Gilbert Lee (another student who in 2001 working as a summer student proved the Dickson lemma). In June we sketched the formalization of the main proof relegating all needed facts to the yet unproven lemmas. While I was away through most of July and August, Broderick finished the main proof, leaving for me more than 100 auxiliary facts of wildly varying weights.

Whereas MML contained a lot algebraic material, the following "higher" algebraic level notions and facts that we needed were missing:

- the multiplicative group of a division ring; we need a separate notion as the carriers of the two structures are different.
- center of a division ring and centralizer of an element understood as division rings;
- centralizer of an element of a group (the center of a group was available);
- division ring as a vector space over the center of the ring;
- conjugate classes of a group.

Of the auxiliary theorems involving the above notions we had to prove the class formula for groups and several basic facts about the cardinality of finite dimensional vector spaces.

To complete the main proof we needed primitive roots of unity and cyclotomic polynomials which were not in MML (but fortunately polynomials and the complex field were already formalized). We proved only the facts that we needed for our proof, hardly paying attention to any systematic development of the theory. And thus, among others, we proved:

- unital polynomial is a product of cyclotomic polynomials;
- coefficients of cyclotomic polynomials are integer;
- facts about the divisibility of values of cyclotomic polynomials and powers of the integer value at which they are evaluated.

All of the above lemmas required us to deal with polynomials defined by roots, and not much on the subject was available in MML. This hinged on the factor theorem (which in my high-school was called the little Bézout theorem; I remember it well as I had to prove it at the entrance exam to the university). Fortunately for us, R. Milewski [7] had proved earlier that the field of complex numbers is algebraically closed. This part required much more effort than we had anticipated and, as a community service, we also proved that the cardinality of the bag of roots of a polynomial over an algebraically closed integral domain equals the degree of the polynomial (although we did not need this fact).

The entire work was completed at the end of December of 2003. The point that I would like to make is this: if MML contained all the facts typically assumed in algebra books when proving the Wedderburn theorem, then our entire effort would have taken at most several days. Indeed, once all the background material was formalized, the main proof took only ca. 250 lines of formal, Mizar text, see [2]. This is roughly 5 to 10 times more than in an algebra textbook like [3, p. 178–179]. (5 to 10 because the number of lines is a ridiculous metric for such comparisons).

Now, imagine that MML (or rather a database for a similar system offering more computational, yet trusted, facilities) contained all the background material needed for the proof of the twin prime conjecture. Would Goldston and Yildirim consider using it in order to proof-check their claims? While only they

can answer, I somehow suspect they might be willing to do so the second time around.

In the QED Manifesto that appeared on web at some point in 1993 we read:

> QED is the very tentative title of a project to build a computer system that effectively represents all important mathematical knowledge and techniques. The QED system will conform to the highest standards of mathematical rigor, including the use of strict formality in the internal representation of knowledge and the use of mechanical methods to check proofs of the correctness of all entries in the system.
>
> The QED project will be a major scientific undertaking requiring the cooperation and effort of hundreds of deep mathematical minds, considerable ingenuity by many computer scientists, and broad support and leadership from research agencies. ...

The truth of the above remains unchanged and in the last 10 years we have seen no new ideas on how this "dream" could materialize.

But there is good news: Thomas Hales has started a project aiming at the formalization of his proof of Kepler's conjecture and we think that Hales's effort may change the picture substantially. His Flyspeck project [5] calls upon a mechanical proof assistant to help convince people about the correctness of a very long and complicated proof of a long open problem (it does not matter that relatively little depends on the conjecture being resolved). His effort requires a lot of computer algebra done under the supervision of a mechanized proof-checker where the paradigms of *Mathematica* and *Maple* are unsatisfactory. It is important to realize that Hales himself decided to rely on HOL-light which provides proof-checking/generating tools in order to dispel all(?) doubts concerning the computation-based parts of his proof.

I think that further success of automated proof assistants among mathematicians heavily depends on employing such systems in current mathematical research (like Hales's effort); and there are many open problems for which, now and then, someone claims to have found a proof; the earlier mentioned twin prime conjecture and the Poincaré conjecture are cases in point.

There are also some systematization efforts that can benefit from using proof assistants. Among large proofs that require some clean-up, although nobody doubts their correctness, one could mention the classification of simple groups and the graph minors theorem. Both proofs are scattered over hundreds of papers and thousands of pages. Also, efforts like building an information system on graph class inclusions [6] might find it beneficial to use some formal reasoning system just at the level of formulating their claims and then extracting the web-presentation automatically.

On a not so grande scale I am planning to put some effort into formalizing the complicated proof of correctness of the interval graph recognition algorithm of [4].

References

1. M. Aigner and G. M. Ziegler. *Proofs from THE BOOK.* 2nd ed., Springer 1999.

2. B. Arneson, M. Baaz and P. Rudnicki. Witt's Proof of the Wedderburn Theorem. `http://mizar.org/JFM/Vol15/weddwitt.html`.
3. P. M. Cohn *Classic Algebra.* 3rd ed., Wiley, 2000.
4. D. G. Corneil, S. Olariu, and L. Stewart. The Ultimate Interval Graph Recognition Algorithm? *Proc. 9th Annual ACM-SIAM Symposium on Discrete Algorithms, SODA'98*, 1998.
5. T. Hales. The Flyspeck Project Fact Sheet. `http://www.math.pitt.edu/ thales/flyspeck/index.html`
6. Information System on Graph Class Inclusions. `http://http://wwwteo.informatik.uni-rostock.de/isgci`.
7. R. Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001. See also `http://mizar.org/JFM/Vol12/polynom5.html`.
8. The Mizar system. `http://mizar.org`.
9. The QED Project. `http://www-unix.mcs.anl.gov/qed`.
10. J. H. M. Wedderburn. A theorem on finite algebras. *Trans. Amer. Math. Soc*, (**4**):349–352, 1905.
11. E. Witt. Über die Kommutativität endlicher Schiefkörper. *Abh. Math. Sem. Univ. Hamburg*, (**8**):413, 1931.

January 22, 2004