Improving Legibility of Proof Scripts in Mizar*

Karol Pąk

Institute of Informatics,
University of Bialystok, Poland
pakkarol@uwb.edu.pl

Abstract. When faced with the question of how to translate the expression of the informal mathematical language to the formal one, every author has to solve difficult multi-level problems of adaptation. Often mathematical concepts developed in a proof assistance library are not compatible with these that occur in every known approach to prove some theorem. In consequence, the proof script authors often have to create a new, so far unknown reasoning or having little common with the original one, even if they tried to reconstruct an informal proof. Additionally, their formalized proofs are commonly regarded as ones of minor value due to their obscurity, even though the process of their creation is usually more laborious.
Therefore, it is important to better understand how we can facilitate the work of script writers and readers improving the proof scripts legibility.

Key words: Operations on languages, Legibility of proofs, Determinants of legibility

Through analyzing the existing formalized proofs collected in a database as the Mizar Mathematical Library (MML) [1], we can find more and more often well-known theorems that require especially long and complex justifications [6, 11]. However, when we try to compare the main idea in formal proof of some theorems with these that occur in an informal textbook reasoning, we encounter a problem. Often mathematical concepts used in a formal proof is not compatible with these that occur in every known informal approach. It is a consequence of the fact that the effort of formalization forced the proof script authors to compare informal proof variants to choose the easiest approach for formalization or even to create a new, so far unknown, and sometimes simpler, reasoning. Nonetheless, the contribution of the work in the process of formalization is commonly regarded as one of minor value due to the obscurity of obtained proof scripts. Obviously proof scripts do not have to be readable for human, if we use a verification system to check their correctness. Therefore, we can easily find proof scripts collected in MML, where the legibility might be very far from the general goal, even if the majority of authors spent a lot of time over their legibility [2, 7]. This concerns especially systems such as Isabelle/Isar [12] or Mizar [5], where

* The paper has been financed by the resources of the Polish National Science Center granted by decision n°DEC-2012/07/N/ST6/02147.

the proof script language is close to the natural language. The experience of big proof formalization developments shows that database of formalized proofs, both easily readable and obscure ones, are often used as libraries, which require reading proof scripts [4], e.g., to adapt or modify the existing proofs to obtain stronger theorems or even as an in-depth tutorial for new-users. Therefore, it comes as no surprise that formal systems as Mizar develop in many directions to improve the legibility of obscure scripts. One of the directions focused on the human process of understanding. Models of cognitive perception of read material and informal mathematical practice stress that an appropriate modification of the proof steps order in reasoning or lemmas extraction are a significant factor in the process of understanding. Therefore, it is important to obtain the standards of readable proof development and to organize the existing library according to a consistent style. The availability of such tools may enhance the culture of proof development and bring closer the idea that formalized proofs not only give strong guarantee for the final theorem validity, but also can be used as patterns to follow.

The main part of these methods based on the *locality of references*. Generally, if a proof step uses some information in the justification then this information has to be derived before in the proof. But this information can be located somewhere far away in the proof or in close neighborhood of the step. It is more natural for the reader if at least some of the required information is available in the directly preceding step or in several preceding steps. However, if we want to obtain a modification of the proof step order, called also *proof linearization* where the number of required information that is located in at most n directly preceding step is maximal we have to solve generally NP-hard problem, regardless how we choice n [10]. Similarly, if we want to increase the length of a linear fragment of reasoning in a selected linearization, i.e., where every step refers to the preceding one is also NP-hard [10]. We obtain the same level of complexity if we minimize the total number of references pointing out of maximal linear fragment or the total length of jumps to distant, not located in the last n directly preceding step, previously justified facts (for more detail see [8–10]). It is important to notice that not every natural determinant of legibility defined on the proof linearization is associated with NP-hard problem. If we concentrate on the number of steps decorated by labels, taking into consideration the Mizar language limitations, we obtain that this minimization problem is solvable in a polynomial time. Note that these restrictions can be easily removed, but there was no need to remove them. However, in the Isabelle/Isar proof scrips, where these restrictions do not occur, it is possible to create deductions for which this minimization is NP-hard [9]. The initial results obtained with the application of a SMT-solver Z3 [3] show that we can generally "fast" optimize the determinants of a proof linearization for reasonings collected in the MML. Additionally, these results show that there exist reasonings where it is certainly impossible to obtain the optimal value for several determinants in the same time. Therefore, it is important to establish one hierarchy of the determinants to obtain the standards of readable proof scripts. However results of survey show that the set of proposed criteria is still not suf-

ficiently closed, since a significant group of respondents highlighted unexplored properties of proof linearization. Additionally, in their opinion the readability of improved proof scripts in accordance with popular criteria's hierarchies, can be significantly degrade, since these *new* properties are not considered.

References

1. G. Bancerek and P. Rudnicki. Information Retrieval in MML. In A. Asperti, B. Buchberger, and J.H.Davenport, editors, *Proc. of Mathematical Knowledge Management 2003*, volume 2594, page 119–131. Springer, Heidelberg, 2003.
2. Grzegorz Bancerek. The Fundamental Properties of Natural Numbers. *Formalized Mathematics*, 1(1):41–46, 1990.
3. L. de Moura and N. Bjørner. Z3: An effcient SMT solver. In C. R. Ramakrishnan and J. Rehof, editors, *Tools and Algorithms for the Construction and Analysis of Systems, 14th International Conference, TACAS 2008*, volume 4963 of *Lecture Notes in Computer Science*, pages 337–340. Springer-Verlag, 2008.
4. G. Gonthier. Formal Proof—The Four-Color Theorem. *Notices of the AMS*, 55(11):1382–1393, 2008.
5. A. Grabowski, A. Korniłowicz, and A. Naumowicz. Mizar in a Nutshell. *Journal of Formalized Reasoning*, 3(2):153–245, 2010.
6. A. Korniłowicz and Y. Shidama. Brouwer Fixed Point Theorem for Disks on the Plane. *Formalized Mathematics*, 13(2):333–336, 2005.
7. A. Korniłowicz. The definition and basic properties of topological groups. *Formalized Mathematics*, 7(2):217–225, 1998.
8. K.Pąk. Improving Legibility of Proof Scripts Based on Quantity of Introduced Labels. In A. Gomolinska, A. Grabowski, M. Hryniewicka, M. Kacprzak, , and E. Schmeidel, editors, *Trends in Contemporary Computer Science, Podlasie 2014*, pages 71–81. Bialystok University of Technology, 2014.
9. K. Pąk. Automated Improving of Proof Legibility in the Mizar System. In Stephen M. Watt, James H. Davenport, Alan P. Sexton, Petr Sojka, and Josef Urban, editors, *Intelligent Computer Mathematics - International Conference, CICM 2014, Coimbra, Portugal, July 7-11, 2014. Proceedings*, pages 373–387, 2014.
10. K. Pąk. Improving Legibility of Natural Deduction Proofs is not Trivial. *Logical Methods in Computer Science*, 10(3:23):1–30, 2014.
11. K. Pąk. Topological Manifolds. *Formalized Mathematics*, 22(2):179–186, 2014.
12. M. Wenzel. *The Isabelle/Isar Reference Manual*. University of Cambridge, 2011.