

Computer-checked mathematics: a formal proof of the Odd Order theorem

Assia Mahboubi

Inria – Inria - Microsoft Joint Centre

assia.mahboubi@inria.fr

Abstract

The Odd Order Theorem is a landmark result in finite group theory, due to W. Feit and J. G. Thompson [1], which states that every finite group of odd order is solvable. It is famous for its crucial role in the classification of finite simple groups, for the novel methods introduced by its original proof but also for the striking contrast between the simplicity of its statement and the unusual length and complexity of its proof. After a six year collaborative effort, we managed to formalize and machine-check a complete proof of this theorem [2] using the Coq proof assistant [3]. The resulting collection of libraries of formalized mathematics covers a wide variety of topics, mostly in algebra, as this proof relies on a sophisticated combination of local analysis and character theory. In this tutorial we comment on the role played by the different features of the proof assistant, from the meta-theory of its underlying logic to the implementation of its various components. We will also discuss some issues raised by the translation of mathematical textbooks into formal libraries and the perspectives it opens on the use of a computer to do mathematics.

Categories and Subject Descriptors F.4.1 [*Mathematical Logic and Formal Languages*]: Mathematical Logic

General Terms Theory

References

- [1] FEIT, W., AND THOMPSON, J. G. Solvability of Groups of Odd Order. *Pacific Journal of Mathematics* 13, 3 (1963), 775–1029.
- [2] GONTHIER, G., ASPERTI, A., AVIGAD, J., BERTOT, Y., COHEN, C., GARILLOT, F., LE ROUX, S., MAHBOUBI, A., O’CONNOR, R., OULD BIHA, S., PASCA, I., RIDEAU, L., SOLOVYEV, A., TASSI, E., AND THÉRY, L. A Machine-Checked Proof of the Odd Order Theorem. In *ITP 2013* (2013), vol. 7998 of *LNCS*, pp. 163–179.
- [3] THE COQ DEVELOPMENT TEAM. *The Coq proof assistant reference manual*. Inria, 2004. Version 8.0.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

CSL-LICS 2014, July 14–18, 2014, Vienna, Austria.

Copyright is held by the owner/author(s). Publication rights licensed to ACM.

ACM 978-1-4503-2886-9...\$15.00.

<http://dx.doi.org/10.1145/2603088.2603090>