François Garillot
Generic Proof Tools and Finite Group Theory

a report by Conor McBride

October 31, 2011

1 Overview

Garillot's thesis represents a substantial contribution to formalized mathematics in its development of finte group theory, but is at least as strong a contribution to the study of tools and techniques for large scale proof engineering. The development is mediated via the Coq system, and while the author has clearly made a considerable study of Coq's quirks and subtleties, the better to play his games of automation, he does not lose sight of the point: he argues cogently for the engineering principles he uses in his development, whatever the tricks he must play to deliver them. He addresses key isses of structure management which any designer of proof systems and libraries must face, working at a scale where the cost of exponentially bad representation choices does become prohibitive and only the scalable can serve at all.

The thesis begins with a compact and helpful introduction to the Calculus of Inductive Constructions by incremental augmentation of Pure Type Systems. From there, we see a careful analysis of the representation of mathematical structures as records carrying sets, their operations, and proof of relevant structural properties. The rest of the first chapter deals extensively with mechanisms outside the Coq kernel which support abbreviation, and particularly with 'canonical structures'. Garillot develops his 'packed classes' methodology for modelling concept hierarchies and demonstrates the principles of its usage on small examples.

The second chapter introduces the techniques Garillot exploits to manage developments in finite group theory, dividing labour efficiently between human and machine, favouring reflection (using the computational power of the kernel) over tactics (computing outside the kernel). He takes considerable advantage of the domain's finiteness to work with certified Boolean decision procedures wherever possible, exploiting the proof irrelevance which naturally accompanies propositions reflected as Boolean values. He demonstrates the effectiveness of these techniques by giving a pleasingly algebraic development of the Chinese Remainder Theorem, leading to a delightfully compact verification of RSA public key encryption.

The third chapter takes the algebraic approach still further, developing a toolkit for subgroup computations which are characteristic *by construction*. This compositional method hinges on recognizing that characteristicity can be seen as functoriality, baking preservation of structure into the operations on sets. This is Mathematics conducted with the engineering discipline of Computer Science, leading to an adventurous formalization of torsion theories for groups. This investigation of "by construction" reasoning finishes with a speculative section on the possibility of exploiting parametricity in a reflective way, indicating a strong and potentially valuable strand of future work.