Abstract Algebra for the Alloy Analyzer

Alexander Varga

Spring 2017

1 First Isomorphism Theorem

Alloy is a software tool that alloys for the specification of models and the verification of assertions about those models with the use of SAT solvers. For my capstone, the models were abstract algebraic structures like groups, which are sets of elements with an addition operation satisfying some basic constraints. The main assertion on these models was the first isomorphism theorem. In short, the project was to 'prove' the first isomorphism theorem for groups with Alloy. Since this involved verifying claims for all possible homomorphisms between groups, the more advanced tool Alloy* was used, which allows higher-order quantification. We were successful in verifying the first isomorphism theorem for small groups with Alloy*.

2 Additional Features

Several additional utilities and group operations were provided, as well as usage demos, including a program that finds hamiltonian paths through the Cayley Graphs of groups. There is also rudimentary support for rings, which are groups augmented with a multiplication operation.

3 Modularity Proposal

Finally, in attempting to create a module for groups parameterized over the types of their elements, some limitations on the modularity of Alloy models were discovered. A simple example was put together to demonstrate this shortcoming. Alloy's macro-based approach to parametric polymorphism is insufficient. For example, it allows the definition of groups of cats and groups of dogs in the same model, but doesn't allow relations between the two. If a highly generic (large) module is defined for groups of arbitrary types of elements and a simple (small) model wishes to use this module but highly restrict it to just groups of a particular type, the resulting CNF formula is a (large) combination of the CNF formulas generated for each. The burden of constraining the model is left to the SAT-solver, which causes extreme inefficiency. The proposed solution is

for Alloy to take 'fact' statements in the model into account before reduction to CNF. This would allow for the creation of highly generic modules that can be restricted as desired in individual modules with appropriate facts. Allowing such coding practices and patterns from standard programming experience to carry over to Alloy will be helpful in reducing the overhead of modelling and encourage modular and extensible code.

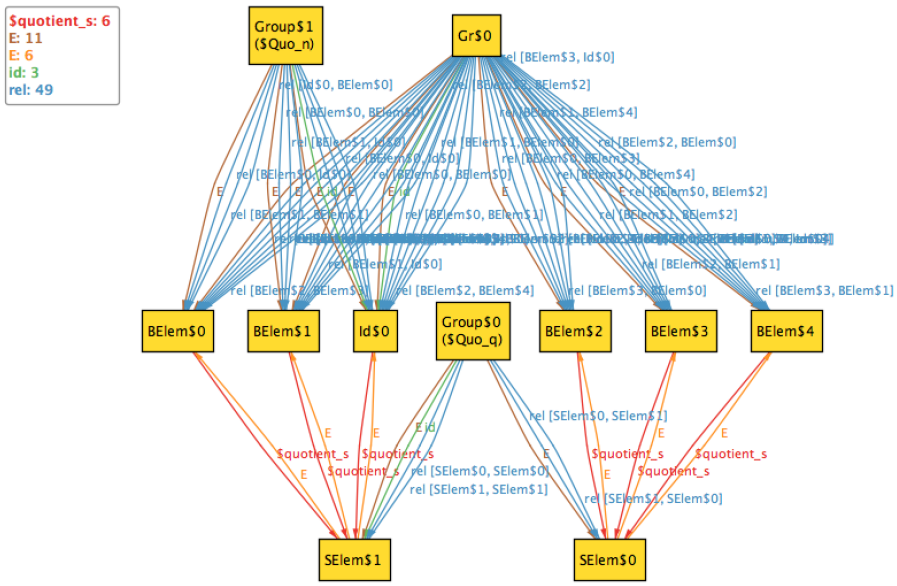

Figure 1: The quotient of a group of 6 elements and a group of 3 elements is a group of 2 sets of 3 elements each