

Theory exploration for working algebraists

David Stanovský

Charles University, Prague, Czech Republic

stanovsk@karlin.mff.cuni.cz

Abstract

As a working algebraist, I'd like to present a personal view on how automated theory exploration could possibly be used in research in algebra.

To my knowledge, classical first order automated theorem proving is, for now, the only automated reasoning technique that helped to obtain original and fundamental results in algebra. Most of such theorems are found in the theory of loops and quasigroups (see [3] for a survey), although there are some recent results in algebraic logic and the semigroup theory. The common feature of the problems accessible to first order ATP is their equational nature: the problems are formulated within a small first order theory, and most of the axioms (usually all of them) are unit equalities.

What I just described, is not theory exploration. The user enters axioms and a conjecture, the ATP system tries to prove it. I'd like to present several problems that require more than just proving (or refuting) a given statement. Let me address two of them in here. I would find a theory exploration system solving any of them useful in my research.

Structure theorems. Let's define an abstract class of algebras, such as abelian groups, or such as algebras (A, \cdot) satisfying equations $x \cdot x = x$ and $x \cdot (y \cdot z) = x \cdot y$. The aim is, to discover a structure theorem, along specified lines. The specification could include, for instance, direct decompositions (or semidirect, or subdirect), it could search for interesting substructures, congruences, etc. In the first case, the classical structure theorem says that every finite abelian group decomposes as a direct product of cyclic groups of prime power order. In the second case, the structure theorem says that there is a congruence such that the factoralgebra and all blocks are just left projection algebras (that is, the operation is $x \cdot y = x$). Can a theory exploration system address this sort of questions? A basic theory of universal algebra could be useful in this respect, see e.g. [2], Chapter II.

Term conditions. Many important properties of algebras are equivalent to existence of a term satisfying certain equations. For example, an equationally defined class \mathcal{K} of algebras has permutable congruences (that is, $\alpha\beta = \beta\alpha$ for each pair of congruences of every algebra $A \in \mathcal{K}$), if and only if there is a term p such that $p(x, x, y) = p(y, x, x) = y$ for all x, y in every algebra $A \in \mathcal{K}$. There is a whole hierarchy of properties and corresponding term conditions, that plays an important role in universal algebra and its applications. It shall be useful to have a tool for working with such conditions. E.g., does a given (finite) algebra satisfy a term condition? (The system needs to invent a term that satisfies it.) Does one condition imply another one? (This can be proved by a series of compositions and substitutions.) Given a term condition, can you find a nicer one, equivalent to it? To learn more about term conditions, see, e.g., the presentation [4], or the paper [1].

References

- [1] L. Barto, D. Stanovský, *Polymorphisms of small digraphs*, submitted.
<http://www.karlin.mff.cuni.cz/~stanovsk/math/gpoly.pdf>
- [2] S. Burris, H.P. Sankappanavar, *A course in universal algebra*, GTM 78, Springer, 1981.
<http://www.math.uwaterloo.ca/~snburris/htdocs/ualg.html>
- [3] JD Phillips, D. Stanovský, *Automated theorem proving in quasigroup and loop theory*, Artificial Intelligence Communications 23/2-3 (2010), 267–283.

- [4] R. Willard, *Quick course in universal algebra and tame congruence theory*,
http://www.math.uwaterloo.ca/~rdwillar/documents/Slides/willard_cspworkshop_tutorial.pdf