Universal Algebra in HoTT

Andreas Lynge[1] and Bas Spitters[2]

[1] Aarhus University, Aarhus, Denmark
andreaslynge@cs.au.dk
[2] Aarhus University, Aarhus, Denmark
b.a.w.spitters@gmail.com

Introduction

Universal algebra is a mathematical theory of algebraic structures. The isomorphism theorems in universal algebra are generalizations of the isomorphism theorems known from group theory and ring theory. In universal algebra these theorems apply to all algebras, e.g. groups, rings, groups acting on sets, etc.

Universal algebra has been developed in type theory before [6, 4, 2]. To model quotient types and function extensionality, these developments are using setoids. This leads to well-known problems.

We formalize universal algebra in the HoTT library [1] using Coq's type class mechanism [5] in the style of the math-classes library [6]. Propositional truncation and quotient types are defined in terms of HITs [7, Chapter 6] and the univalence axiom implies function extensionality [7, Section 4.9]. By using this we avoid the need for setoids. We show that there is a univalent category of algebras and homomorphisms for a signature. The development contains the three fundamental isomorphism theorems, which become identification theorems in HoTT.

The following sections give a brief overview of the work. A longer explanation is available at https://github.com/andreaslyn/Work/blob/master/Math-Bachelor.pdf.

Fundamental definitions

A (multi-sorted) *algebra* $A : \mathrm{Algebra}(\sigma)$ for a signature $\sigma : \mathrm{Signature}$ consists of

- A *carrier* type $A_s : \mathcal{U}$ for each $s : \mathrm{Sort}(\sigma)$, where $\mathrm{Sort}(\sigma)$ is a type of sorts corresponding to the signature σ. It is required that A_s is a set for all $s : \mathrm{Sort}(\sigma)$.
- An *operation* $u^A : \mathrm{Operation}(A, u)$ for each $u : \mathrm{Symbol}(\sigma)$. Here $\mathrm{Symbol}(\sigma)$ is a type of function symbols corresponding to σ, and

$$\mathrm{Operation}(A, u) \equiv (A_{s_1} \to A_{s_2} \to \cdots \to A_{s_n}),$$

  where $n : \mathbb{N}$ and $s_1, \ldots, s_n : \mathrm{Sort}(\sigma)$ depends on u.

For example, a group G acting on a set S is an algebra with two carrier types, the group G and the set S. This algebra has the usual group operations: the identity element $e : G$, the binary operation $\cdot : G \to G \to G$, and the inverse operation $(-)^{-1} : G \to G$. Additionally there is the action of G on S, an operation $\alpha : G \to S \to S$.

A *homomorphism* $f : A \to B$ between algebras $A, B : \mathrm{Algebra}(\sigma)$ is a family of functions $f_s : A_s \to B_s$, indexed by $s : \mathrm{Sort}(\sigma)$, that preserves operations in the sense that

$$f_{s_{n+1}}(u^A(x_1, x_2, \ldots, x_n)) = u^B(f_{s_1}(x_1), f_{s_2}(x_2), \ldots, f_{s_n}(x_n)),$$

for all $u : \mathrm{Symbol}(\sigma)$ and $x_i : A_{s_i}$.

An *isomorphism* is a homomorphism $f : A \to B$ where, for all $s : \mathrm{Sort}(\sigma)$, f_s is both injective and surjective, or equivalently f_s is an equivalence.

A property of homomorphisms $f : A \to B$ is that equational laws involving operations, such as $u^A(v^A(x), y) = w^A(x, y)$, are always preserved,

$$u^B(v^B(f_r(x)), f_s(y)) = f_t(u^A(v^A(x), y)) = f_t(w^A(x, y)) = w^B(f_r(x), f_s(y)).$$

Results

For generic single-sorted (single carrier type) algebraic structures, Coquand and Danielsson show that isomorphic structures are equal [3]. This leads us to a central theorem about multi-sorted algebras:

If there is an isomorphism $A \to B$ between two algebras $A, B : \mathrm{Algebra}(\sigma)$, then $A = B$.

This is in fact an equivalence, which we use to show that there is a (univalent) category σ-**Alg** of algebras and homomorphisms for signature σ. This was previously formalized in HoTT for single-sorted algebraic structures [7, Section 9.8]. We have generalized this to multi-sorted algebraic structures, but with a more specific notion of algebraic structure and homomorphism.

We define product algebra, subalgebra and quotient algebra. Product algebras are used to construct products in the category σ-**Alg**, equalisers are subalgebras, and coequalisers are quotient algebras. We prove the three isomorphism theorems. The first isomorphism theorem states that:

Given a homomorphism $f : A \to B$ between algebras $A, B : \mathrm{Algebra}(\sigma)$,

- *The kernel of f, defined by $\ker(f)(s, x, y) :\equiv (f_s(x) = f_s(y))$, gives rise to a quotient algebra $A/\ker(f)$ of A by $\ker(f)$.*
- *Set $\mathrm{inim}(f)(s, y) :\equiv \left\| \sum_{(x:A_s)} (f_s(x) = y) \right\|$, where $\|-\|$ denotes propositional truncation. It induces a subalgebra $B\&\,\mathrm{inim}(f)$ of B, the homomorphic image of f.*
- *There is an isomorphism $A/\ker(f) \to B\&\,\mathrm{inim}(f)$, and hence $A/\ker(f) = B\&\,\mathrm{inim}(f)$.*

It follows that any morphism $f : A \to B$ in σ-**Alg** image factorizes $A \to B\&\,\mathrm{inim}(f) \hookrightarrow B$. Images are stable under pullback, so the category σ-**Alg** of algebras for signature σ is regular.

References

[1] A. Bauer, J. Gross, P. L. Lumsdaine, M. Shulman, M. Sozeau, and B. Spitters. The HoTT Library: A Formalization of Homotopy Type Theory in Coq. In *Proceedings of the 6th ACM SIGPLAN Conference on Certified Programs and Proofs*, CPP 2017, pages 164–172. ACM, 2017. http://doi.acm.org/10.1145/3018610.3018615.

[2] V. Capretta. Universal Algebra in Type Theory. In Y. Bertot, G. Dowek, A. Hirschowits, C. Paulin, and L. Théry, editors, *Theorem Proving in Higher Order Logics, 12th International Conference, TPHOLs '99*, volume 1690 of *LNCS*, pages 131–148. Springer, 1999.

[3] T. Coquand and N. A. Danielsson. Isomorphism is equality. *Indagationes Mathematicae*, 24(4):1105 – 1120, 2013. In memory of N.G. (Dick) de Bruijn (19182012), http://www.sciencedirect.com/science/article/pii/S0019357713000694.

[4] E. Gunther, A. Gadea, and M. Pagano. Formalization of Universal Algebra in Agda. *Electronic Notes in Theoretical Computer Science*, 338:147–166, 10 2018.

[5] M. Sozeau and N. Oury. First-Class Type Classes. In *Proceedings of the 21st International Conference on Theorem Proving in Higher Order Logics*, TPHOLs '08, pages 278–293, Berlin, 2008. Springer. http://dx.doi.org/10.1007/978-3-540-71067-7_23.

[6] B. Spitters and E. van der Weegen. Type Classes for Mathematics in Type Theory. *MSCS, special issue on 'Interactive theorem proving and the formalization of mathematics'*, 21:1–31, 2011.

[7] The Univalent Foundations Program. *Homotopy Type Theory: Univalent Foundations for Mathematics*. http://homotopytypetheory.org/book, Institute for Advanced Study, 2013.