Abstract

We report on the *Equational Theories Project* (ETP), an online collaborative project to determine the implication graph between short equational laws on magmas, by a combination of human-generated and automated proofs, all validated by the formal proof assistant language *Lean*. **state key outcomes**

The Equational Theories Project

Author Names (in Alphabetical Order)

November 20, 2024

Contents

1 Introduction

1.1 Magmas and equational laws

A *magma* $M = (M, \diamond)$ is a set M (known as the *carrier*) together with a binary operation $\diamond \colon M \times M \to M$. An *equational law* for a magma, or *law* for short, is an identity involving $\diamond$ and some indeterminates, which we will typically denote using the symbols x, y, z, u, v, w. Familiar examples of equational laws include the *commutative law*

$$x \diamond y = y \diamond x \tag{E43}$$

and the *associative law*

$$(x \diamond y) \diamond z = x \diamond (y \diamond z). \tag{E4512}$$

For our project we have assigned a unique number to each equational law, which we describe in Appendix A. Formally, one can represent an equational law syntactically as a string $w_1 \simeq w_2$, where w_1, w_2 are words in a free magma generated by formal indeterminate symbols; see ???.

A magma M obeys a law E if the law E holds for all possible assignments of the indeterminate to M, in which case we write $M \models E$. Thus for instance $M \models E43$ if one has $x \diamond y = y \diamond x$ for all $x, y \in M$.

We place a pre-order on laws by writing $E \leq E'$ or $E \vdash E'$ if every magma that obeys E, also implies E': $(M \models E) \implies (M \models E')$. We say that two laws are *equivalent* if they imply each other. For instance, the constant law

$$x \diamond y = z \diamond w \tag{E46}$$

can easily be see to be equivalent to the law

$$x \diamond x = y \diamond z. \tag{E41}$$

In this pre-ordering, a maximal element is given by the trivial law

$$x = x \tag{E1}$$

and a minimal element is given by the singleton law

$$x = y. \tag{E2}$$

The *order* of an equational law is the number of occurrences of the magma operation. For instance, the commutative law (E43) has order 2, while the associative law (E4512) has order 4. We note some selected laws of small order that have previously appeared in the literature:

- The *central groupoid law*

  $$x = (y \diamond x) \diamond (x \diamond z) \tag{E168}$$

  is an order 3 law introduced by Evans [2] and studied further by Knuth [5] and many further authors, being closely related to central digraphs (also known as unique path property diagraphs), and leading in particular to the discovery of the Knuth-Bendix algorithm [6]; see [7] for a more recent survey

- *Tarski's axiom*

  $$x = y \diamond ((z \diamond (x \diamond (y \diamond z)))) \tag{E543}$$

  is an order 4 law that was shown by Tarski [12] to characterize the operation of subtraction in an abelian group; that is to say, a magma M obeys (E543) if and only if there is an abelian group structure on M for which $x \diamond y = x - y$ for all $x, y \in M$.

- In a similar vein, it was shown in [11] that the order 4 law

  $$x = (y \diamond z) \diamond (y \diamond (x \diamond z)) \tag{E1571}$$

  characterizes addition (or subtraction) in an abelian group of exponent 2; it was shown in [9] that the order 4 law

  $$x = (y \diamond ((x \diamond y) \diamond y)) \diamond (x \diamond (z \diamond y)) \tag{E345169}$$

characterizes the Sheffer stroke in a boolean algebra, and it was shown in [3] that the order 8 law

$$x = y \diamond ((((y \diamond y) \diamond x) \diamond z) \diamond (((y \diamond y) \diamond y) \diamond z)) \tag{E42323216}$$

characterizes division in a (not necessarily abelian) group.

The Birkhoff completeness theorem [1, Th. 3.5.14] implies that an implication $E \vdash E'$ of equational laws holds if and only if the left hand side of E' can be transformed into the right-hand side by a finite number of substitution rewrites using the law E. However, the problem of determining whether such an implication holds is undecidable in general [10].Even when the order is small, some implications[1] can require lengthy computer-assisted proofs; for instance, it was noted in [4] that the order 4 law

$$x = (y \diamond x) \diamond ((x \diamond z) \diamond z) \tag{E1689}$$

was equivalent to the singleton law (E2), but all known proofs are computer-assisted.

1.2 The Equational Theories Project

As noted in Appendix A, there are 4694 equational laws of order at most 4. In September of 2024, we launched the *Equational Theories Project* (ETP)[2] to completely determine the implication pre-ordering $\leq$ for this set of laws. Ostensibly, this determining the truth or falsity of $4694 \times 4693 = 22028942$ implications; while one can use properties such as the transitivity of the pre-ordering to reduce the work somewhat, this is clearly a task that requires significant automation.

MORE EXPLANATION HERE

2 Results

While a large number of theoretically interesting results are not expected, some notable ones can be listed here with links to blueprints/Lean as necessary. Proofs can be deferred to the appendix.

- A new short Austin pair: Equation 3944 implies Equation 3588 [**?**], but not for infinite magmas [**?**].

[1] Another contemperaneous example of this phenomenon was the solution of the Robbins problem [8].
[2] `https://teorth.github.io/equational_theories/`

3 Mathematical Foundations

This section covers topics like free magmas (including those relative to theories), a completeness theorem, and confluence (unique simplification).

4 Formal Foundations

Here we describe the Lean framework used to formalize the project, covering technical issues such as:

- Magma operation symbol issues
- Syntax (‘LawX‘) versus semantics (‘EquationX‘)
- ”Universe hell” issues
- Additional verification (axiom checking, Leanchecker, etc.)
- Use of the ‘conjecture‘ keyword

4.1 Contributions to Mathlib

None yet, but presumably, some of what we do will be uploadable and should be mentioned.

5 Project Management

Shreyas Srinivas and Pietro Monticone have volunteered to take the lead on this section.

Discuss topics such as:

- Project generation from template
- Github issue management with labels and task management dashboard
- Continuous integration (builds, blueprint compilation, task status transition)
- Pre-push git hooks
- Use of Lean Zulip and polls

5.1 Handling Scaling Issues

Mention early human-managed efforts and the need for forethought in setting up a GitHub organizational structure. Discuss the use of transitive reduction to keep the Lean codebase manageable.

5.2 Other Design Considerations

Explain the meaning of "trusting Lean" in a large project and highlight human issues that may arise, tools for external checks, PR reviews, and good practices like branch protection.

6 Finite Magmas and Other Sources of Counterexamples

Describe various sources of example magmas, including finite and linear magmas, and their role in ruling out implications. Also, discuss the computational and memory efficiencies needed.

7 Metatheorems

List some notable metatheorems, including those that did not mature in time for deployment but may still be useful in the future.

8 Automated Theorem Proving

Describe the automated theorem provers used in the project (Z3, Vampire, egg, etc.) and performance statistics. Explore semi-automated vs. fully automated methods and how these were integrated into the project.

9 AI-assisted Contributions

Current contributions include Claude's assistance with front-end coding, with potential for more as the project progresses.

10 User Interface

Describe visualizations and explorer tools used in the project.

11 Statistics and Experiments

Analyze the implication graph and discuss test sets of implication problems for benchmarking theorem provers. Challenge: How can one automatically assign a difficulty level to an implication?

12 Data Management

Describe how data was handled during the project and how it will be managed going forward.

13 Reflections

Include testimonies from participants and reflections on the project, discussing the balance between automation and human input.

14 Conclusions and Future Directions

Summarize insights and future directions for the project, including potential databases and interesting equational laws.

Acknowledgments

Acknowledgments to the broader Lean Zulip community and smaller contributors not listed as authors.

A Numbering system

In this section we record the numbering conventions we use for equational laws.

For this formal definition we use the natural numbers $0, 1, 2, \ldots$ to represent and order indeterminate variables; however, in the main text, we use the symbols $x, y, z, w, u, v, r, s, t$ instead (and do not consider any laws with more than eight variables).

We requiring extend the ordering on indeterminate variables to a well-ordering on words w in the free magma generated by these variables by declaring $w > w'$ if one of the following holds:

- w has a larger order than w'.
- $w = w_1 \diamond w_2$ and $w' = w_1' \diamond w_2'$ have the same order $n \geq 1$ with $w_1 > w_1'$.
- $w = w_1 \diamond w_2$ and $w' = w_1' \diamond w_2'$ have the same order $n \geq 1$ with $w_1 = w_1'$ and $w_2 > w_2'$.

Thus for instance

$$0 < 1 < 0 \diamond 0 < 0 \diamond 1 < 1 \diamond 0$$

and

$$1 \diamond 1 < 0 \diamond (0 \diamond 0) < (0 \diamond 0) \diamond 0.$$

We similarly place a well-ordering on equational laws $w_1 \simeq w_2$ by declaring $w_1 \simeq w_2 > w_1' \simeq w_2'$ if one of the following holds: as follows:

- $w_1 \simeq w_2$ has a longer order than $w_1' \simeq w_2'$.
- If $w_1 \simeq w_2$ has the same order as $w_1' \simeq w_2'$, and $w_1 > w_1'$.
- If $w_1 \simeq w_2$ has the same order as $w_1' \simeq w_2'$, $w_1 = w_1'$, and $w_2 > w_2'$.

Two equational laws are equivalent if one can be obtained from another by some combination of relabeling the variables and applying the symmetric law $w_1 \simeq w_2 \iff w_2 \simeq w_1$. For instance, $(0 \diamond 1) \diamond 2 \simeq 1$ is equivalent to $0 \simeq (1 \diamond 0) \diamond 2$. We then eliminate all equational laws that are not minimal in their equivalence class; for instance, we would eliminate $(0 \diamond 1) \diamond 2 \simeq 1$ in favor of $0 \simeq (1 \diamond 0) \diamond 2$. Finally, we eliminate any law of the form $w \simeq w$ other than $0 \simeq 0$. We then number the remaining equations $E1, E2, \ldots$. For instance, $E1$ is the trivial law $0 \simeq 0$, $E2$ is the constant law $0 \simeq 1$, $E3$ is the idempotent law $0 \simeq 0 \diamond 0$, and so forth. Lists and code for generating these equations, or the equation number attached to a given equation, can be found at the ETP repository.

The number of equations in this list of order $n = 0, 1, 2, \ldots$ is given by

$$2, 5, 39, 364, 4284, 57882, 888365, \ldots$$

(`https://oeis.org/A376640`). The number can be computed to be

$$C_{n+1}B_{n+2}/2$$

if n is odd, 2 if $n = 0$, and

$$(C_{n+1}B_{n+2} + C_{n/2}(2D_{n+2} - B_{n+2}))/2 - C_{n/2}B_{n/2+1}$$

if $n > 2$ is even, where C_n, B_n are the Catalan and Bell numbers, and D_n is the number of partitions of $[n]$ up to reflection, which for $n = 0, 1, 2, \dots$ is

$$1, 1, 2, 4, 11, 32, 117, \dots$$

(`https://oeis.org/A103293`). A proof of this claim can be found in the ETP blueprint. In particular, there are 4694 equations of order at most 4.

B Proofs of Theoretical Results

Provide the interesting proofs mentioned in the results section, while routine proofs can refer to the blueprint or Lean.

C Author Contributions

List author contributions, using CRediT categories. Elaborate on how these categories are interpreted and add affiliations and grant acknowledgments.

References

[1] Franz Baader and Tobias Nipkow. *Term rewriting and all that.* Cambridge University Press, Cambridge, 1998.

[2] Trevor Evans. Products of points—some simple algebras and their identities. *Amer. Math. Monthly*, 74:362–372, 1967.

[3] Graham Higman and B. H. Neumann. Groups as groupoids with one law. *Publ. Math. Debrecen*, 2:215–221, 1952.

[4] A. Kisielewicz. Austin identities. *Algebra Universalis*, 38(3):324–328, 1997.

[5] Donald E. Knuth. Notes on central groupoids. *J. Combinatorial Theory*, 8:376–390, 1970.

[6] Donald E. Knuth and Peter B. Bendix. Simple word problems in universal algebras. In *Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967)*, pages 263–297. Pergamon, Oxford-New York-Toronto, Ont., 1970.

[7] André Kündgen, Gregor Leander, and Carsten Thomassen. Switchings, extensions, and reductions in central digraphs. *J. Combin. Theory Ser. A*, 118(7):2025–2034, 2011.

[8] William McCune. Solution of the Robbins problem. *J. Automat. Reason.*, 19(3):263–276, 1997.

[9] William McCune, Robert Veroff, Branden Fitelson, Kenneth Harris, Andrew Feist, and Larry Wos. Short single axioms for Boolean algebra. *J. Automat. Reason.*, 29(1):1–16, 2002.

[10] Ralph McKenzie. On spectra, and the negative solution of the decision problem for identities having a finite nontrivial model. *J. Symbolic Logic*, 40:186–196, 1975.

[11] N. S. Mendelsohn and R. Padmanabhan. Minimal identities for Boolean groups. *J. Algebra*, 34:451–457, 1975.

[12] Alfred Tarski. Ein beitrag zur axiomatik der abelschen gruppen. *Fundamenta Mathematicae*, 30(1):253–256, 1938.