Equational Theories

Contributors of the Equational Theories Project

May 23, 2025

Chapter 1

Basic theory of magmas

Definition 1.1 (Magma)**.** A *magma* is a set G equipped with a binary operation $\diamond : G \times G \to G$. A *homomorphism* $\varphi : G \to H$ between two magmas is a map such that $\varphi(x \diamond y) = \varphi(x) \diamond \varphi(y)$ for all $x, y \in G$. An *isomorphism* is an invertible homomorphism.

Groups, semi-groups, and monoids are familiar examples of magmas. However, in general we do not expect magmas to have any associative properties. In some literature, magmas are also known as groupoids, although this term is also used for a slightly different object (a category with inverses).

A magma is called *empty* if it has cardinality zero, *singleton* if it has cardinality one, and *non-trivial* otherwise.

The number of magma structures on a set G of cardinality n is of course n^{n^2}, which is [1]

$$1, 1, 16, 19683, 4294967296, 298023223876953125, ...$$

(OEIS A002489). Up to isomorphism, the number of finite magmas of cardinality n up to isomorphism is the slightly slower growing sequence

$$1, 1, 10, 3330, 178981952, 2483527537094825, 1432559000331889152227568 0, ...$$

(OEIS A001329). As there are $n!$ ways to rearrange the elements of a set of cardinality n, the number of non-isomorphic magmas on a set of cardinality n is at least $n^{n^2}/n!$; as it turns out, most magmas are idemprimal (which implies in particular that there are no non-trivial isomorphisms), so the number of non-isomorphic magmas is fairly close to this lower bound.

Definition 1.2 (Free Magma)**.** The *free magma* M_X generated by a set X (which we call an *alphabet*) is the set of all finite formal expressions built from elements of X and the operation $\diamond$. An element of M_X will be called a *word* with alphabet X. The *order* of a word is the number of $\diamond$ symbols needed to generate the word. Thus for instance X is precisely the set of words of order 0 in M_X.

For sake of concreteness, we will take the alphabet X to default to the natural numbers $\mathbb{N}$ if not otherwise specified.

For instance, if $X = \{0, 1\}$, then M_X would consist of the following words:

- 0, 1 (the words of order 0);

[1] All sequences start from $n = 0$ unless otherwise specified.

- $0 \diamond 0$, $0 \diamond 1$, $1 \diamond 0$, $1 \diamond 1$ (the words of order 1);
- $0 \diamond (0 \diamond 0)$, $0 \diamond (0 \diamond 1)$, $0 \diamond (1 \diamond 0)$, $0 \diamond (1 \diamond 1)$, $1 \diamond (0 \diamond 0)$, $1 \diamond (0 \diamond 1)$, $1 \diamond (1 \diamond 0)$, $1 \diamond (1 \diamond 1)$, $(0 \diamond 0) \diamond 0$, $(0 \diamond 0) \diamond 1$, $(0 \diamond 1) \diamond 0$, $(0 \diamond 1) \diamond 1$, $(1 \diamond 0) \diamond 0$, $(1 \diamond 0) \diamond 1$, $(1 \diamond 1) \diamond 0$, $(1 \diamond 1) \diamond 1$ (the words of order 2);
- etc.

Lemma 1.3. *For a finite alphabet X, the number of words of order n is $C_n|X|^{n+1}$, where C_n is the n^{th} Catalan number and X is the cardinality of X.*

Proof. Follows from standard properties of Catalan numbers. □

The first few Catalan numbers are

$$1, 1, 2, 5, 14, 42, 132, ...$$

(OEIS A000108).

Definition 1.4 (Induced homomorphism)**.** Given a function $f : X \to G$ from an alphabet X to a magma G, the *induced homomorphism* $\varphi_f : M_X \to G$ is the unique extension of f to a magma homomorphism. Similarly, if $\pi \colon X \to Y$ is a function, we write $\pi_* \colon M_X \to M_Y$ for the unique extension of π to a magma homomorphism.

For instance, if $f : \{0, 1\} \to G$ maps $0, 1$ to x, y respectively, then

$$\varphi_f(0 \diamond 1) = x \diamond y$$

$$\varphi_f(1 \diamond (0 \diamond 1)) = y \diamond (x \diamond y)$$

and so forth. If $\pi \colon \mathbb{N} \to \mathbb{N}$ is the map $\pi(n) := n + 1$, then

$$\pi_*(0 \diamond 1) = 1 \diamond 2$$

$$\pi_*(1 \diamond (0 \diamond 1)) = 2 \diamond (1 \diamond 2)$$

and so forth.

Definition 1.5 (Law)**.** Let X be a set. A *law* with alphabet X is a formal expression of the form $w \simeq w'$, where $w, w' \in M_X$ are words with alphabet X (thus one can identify laws with alphabet X with elements of $M_X \times M_X$). A magma G *satisfies* the law $w \simeq w'$ if we have $\varphi_f(w) = \varphi_f(w')$ for all $f : X \to G$, in which case we write $G \vDash w \simeq w'$.

Thus, for instance, the commutative law

$$0 \diamond 1 \simeq 1 \diamond 0 \tag{1.1}$$

is satisfied by a magma G if and only if

$$x \diamond y = y \diamond x \tag{1.2}$$

for all $x, y \in G$. We refer to Equation (1.2) as the *equation* associated to the law Equation (1.1). One can think of equations as the "semantic" interpretation of a "syntactic" law. However, we shall often abuse notation and identify a law with its associated equation. In particular, we shall (somewhat carelessly) also refer to Equation (1.2) as "the commutative law" (rather than "the commutative equation").

Definition 1.6 (Models)**.** A *theory* is a set Γ of laws. Given a theory Γ, a magma G is a *model* of Γ with the (overloaded) notation $G \models \Gamma$ if $G \models w \simeq w'$ for every $w \simeq w'$ in Γ; we also say that G *obeys* Γ. Given a law E, we write $\Gamma \models E$ if every magma G that models Γ, also models E.

Definition 1.7 (Derivation)**.** Given a theory Γ and a law $w \simeq w'$ over a fixed alphabet X, we say that Γ *derives* $w \simeq w'$, and write $\Gamma \vdash w \simeq w'$, if the law can be obtained using a finite number of applications of the following rules:

1. if $w \simeq w' \in \Gamma$, then $\Gamma \vdash w \simeq w'$.
2. $\Gamma \vdash w \simeq w$ for any word w.
3. if $\Gamma \vdash w \simeq w'$, then $\Gamma \vdash w' \simeq w$.
4. if $\Gamma \vdash w \simeq w'$ and $\Gamma \vdash w' \simeq w''$, then $\Gamma \vdash w \simeq w''$.
5. if $\Gamma \vdash w \simeq w'$, then $\Gamma \vdash \varphi_f(w) \simeq \varphi_f(w')$ for every $f : X \to M_X$.
6. if $\Gamma \vdash w_1 \simeq w_2$ and $\Gamma \vdash w_3 \simeq w_4$, then $\Gamma \vdash w_1 \diamond w_3 \simeq w_2 \diamond w_4$.

This definition is useful because of the following theorem:

Theorem 1.8 (Birkhoff's completeness theorem)**.** *For any theory Γ and words w, w' over a fixed alphabet*

$$\Gamma \vdash w \simeq w' \text{ iff } \Gamma \models w \simeq w'.$$

Proof. (Sketch) The 'only if' component is soundness, and follows from verifying that the rules of inference in Theorem 1.7 holds for $\models$. The 'if' part is completeness, and is proven by constructing the magma of words, quotiented out by the relation $\Gamma \vdash w \simeq w'$, which is easily seen to be an equivalence relation respecting the magma operation. □

Corollary 1.9 (Compactness theorem)**.** *Let Γ be a theory, and let E be a law. Then $\Gamma \models E$ if and only if there exists a finite subset Γ' of Γ such that $\Gamma' \models E$.*

Proof. The claim is obvious for $\vdash$, and the claim then follows from Theorem 1.8. □

Lemma 1.10 (Pushforward)**.** *Let $w \simeq w'$ be a law with some alphabet X, G be a magma, and $\pi : X \to Y$ be a function. If $G \models w \simeq w'$, then $G \models \pi_*(w) \simeq \pi_*(w')$. In particular, if π is a bijection, the statements $G \models w \simeq w'$ and $G \models \pi_*(w) \simeq \pi_*(w')$ are equivalent.*

Proof. Trivial. □

If π is a bijection, we will call $\pi_*(w) \simeq \pi_*(w')$ a *relabeling* of the law $w \simeq w'$. Thus for instance

$$5 \diamond 7 \simeq 7 \diamond 5$$

is a relabeling of the commutative law Equation (1.1). By the above lemma, relabeling does not affect whether a given magma satisfies a given law.

Lemma 1.11 (Equivalence)**.** *Let G be a magma and X be an alphabet. Then the relation $G \models w \simeq w'$ is an equivalence relation on M_X.*

Proof. Trivial. □

Define the total order of a law $w \simeq w'$ to be the sum of the orders of w and w'.

Lemma 1.12 (Counting laws up to relabeling)**.** *Up to relabeling, the number of laws $w \simeq w'$ of total order n is $C_{n+1}B_{n+2}$.*

Proof. Follows from the properties of Catalan and Bell numbers. □

The first few Bell numbers are

$$1, 1, 2, 5, 15, 52, 203, ...$$

(OEIS A000110).

The sequence in Theorem 1.12 is

$$2, 10, 75, 728, 8526, 115764, ...$$

(OEIS A289679).

Now we would also like to count laws up to relabeling and symmetry.

Lemma 1.13 (Counting laws up to relabeling and symmetry)**.** *Up to relabeling and symmetry, the number of laws $w \simeq w'$ of total order n is*

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

when n is odd, and

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

when n is even, where D_n is the number of partitions of $[n]$ up to reflection.

Proof. Elementary counting. □

The sequence D_n is

$$1, 1, 2, 4, 11, 32, 117, ...$$

(OEIS A103293), and the sequence in Theorem 1.13 is

$$2, 5, 41, 364, 4294, 57882, 888440, ...$$

(OEIS A376620).

We can also identify all laws of the form $w \simeq w$ with the trivial law $0 \simeq 0$. The number of such laws of total order n is zero if n is odd, and $C_{n/2}B_{n/2+1}$ if n is even. We conclude:

Lemma 1.14 (Counting laws up to relabeling, symmetry, and triviality)**.** *Up to relabeling, symmetry, and triviality, the number of laws of total order n is*

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

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 $n \geq 2$ is even.

Proof. Routine counting. □

This sequence is

$$2, 5, 39, 364, 4284, 57882, 888365, ...$$

(OEIS A376640).

In particular, up to relabeling, symmetry, and triviality, there are exactly $2 + 5 + 39 + 364 + 4284 = 4694$ laws of total order at most 4. A list can be found here. A script for generating them may be found here. The ordering of these equations is according to the following rules. First, an ordering on expressions with placeholder variables $*$ (such as $* \diamond (* \diamond *)$):

- (i) Expressions of lower order come before expressions of higher order.
- (ii) Expressions $w_L \diamond w_R$ of a given total order that is at least one are ordered lexicographically first by the ordering on the left component w_L, and then by the ordering on the right component w_R if the left components agree.

For instance, $* \diamond *$ is less than $* \diamond (* \diamond *)$, which is less than $(* \diamond *) \diamond *$.

Then, we order placeholder equations such as $* \diamond (* \diamond *) \simeq (* \diamond *) \diamond *$, where both sides are given placeholder variables:

- (i) Equations of lower total order come before equations of higher total order.
- (ii) Equations $w \simeq w'$ of a given total order are ordered lexicographically first by the ordering on the left-hand side w, and then by the ordering on the right hand side w' if the left-hand sides agree.

For instance, $* \diamond * \simeq * \diamond (* \diamond *)$ is less than $* \diamond * \simeq (* \diamond *) \diamond *$.

Finally, we order (and reduce) equations of the form $w \simeq w'$ as follows. Define the *shape* of an equation to be the equation in which all variables are replaced by placeholders $*$.

- (i) Equations of lower shape will be of lower order. For instance, any equation of shape $* \diamond * \simeq * \diamond (* \diamond *)$ is less than any equation $* \diamond * \simeq (* \diamond *) \diamond *$.
- (ii) Among equations of equations of equal shape, equations whose variables are first in the lexicographical ordering will be lower. For instance, $0 * 0 \simeq 0 \diamond (0 \diamond 0)$ is less than $0 * 0 \simeq 1 \diamond (1 \diamond 1)$, which is in turn less than $0 * 1 \simeq 0 \diamond (0 \diamond 0)$.
- (iii) Only the arrangement of the equation (up to relabeling and symmetry) which is minimal in this ordering is retained in the list. For instance, we do not retain $1 \diamond 2 \simeq 1$ because it can be replaced by $0 \simeq 0 \diamond 1$, which is earlier in the ordering.
- (iv) Any trivial equation $w \simeq w$, other than the order zero law $0 \simeq 0$, is discarded.

1.1 Alternate formula

For integers $0 \leq a \leq b$ let $E(a, b)$ be the number of magma equations $t_1 = t_2$ with t_1 of order a, t_2 of order b, counting up to relabelling, up to switching terms, and only allowing the equation $x = x$ of the form $t = t$. Then one has

- $E(0, 0) = 2$.
- If $a \neq b$:

$$E(a,b) = T(a) \cdot T(b) \cdot \sum_{\substack{1 \leq p \leq a+1 \\ 1 \leq q \leq b+1 \\ 0 \leq s \leq \min(p,q)}} \left\{ \begin{matrix} a+1 \\ p \end{matrix} \right\} \left\{ \begin{matrix} b+1 \\ q \end{matrix} \right\} \binom{p}{s} \binom{q}{s} s! \ .$$

- If $a = b > 0$:

$$E(a,b) = \frac{1}{2}T(a)^2 \cdot \sum_{\substack{1\le p,q\le a+1\\ 0\le s\le \min(p,q)}} \left\{ \begin{matrix} a+1 \\ p \end{matrix} \right\} \left\{ \begin{matrix} a+1 \\ q \end{matrix} \right\} \binom{p}{s}\binom{q}{s} s!$$
$$+ \frac{1}{2}T(a) \cdot \sum_{\substack{1\le p\le a+1\\ 0\le s\le p}} \left\{ \begin{matrix} a+1 \\ p \end{matrix} \right\} \binom{p}{s} \mathsf{Invol}(s)$$
$$- T(a) \cdot \sum_{1\le p\le a+1} \left\{ \begin{matrix} a+1 \\ p \end{matrix} \right\}.$$

Here the *Stirling numbers* $\left\{ \begin{matrix} n \\ m \end{matrix} \right\}$ *of the second kind* count the number of ways to partition a set of n elements into m non-empty subsets,

$$T(n) = \frac{1}{n+1} \cdot \binom{2n}{n}$$

counts the number of plane binary trees of order n, and.

$$\mathsf{Invol}(n) = \sum_{0\le k\le \lfloor n/2 \rfloor} \binom{n}{2k} (2k-1)!!$$

counts the number of involutions on n elements.

The number of magma equations of order n (under the given constraints) is then equal to

$$\sum_{0\le a\le \lfloor n/2 \rfloor} E(a, n-a).$$

For further details, as well as Maple calculations for $E(a,b)$, see this folder.

Chapter 2

Selected laws

In this project we study the 4694 laws (up to symmetry and relabeling) of total order at most 4.

Selected laws of interest are listed below, as well as in this file. As will be discussed in Chapter 4, every equational law comes with a dual.

Definition 2.1 (Equation 1)**.** Equation 1 is the law $0 \simeq 0$ (or the equation $x = x$).

This is the trivial law, satisfied by all magmas. It is self-dual.

Definition 2.2 (Equation 2)**.** Equation 2 is the law $0 \simeq 1$ (or the equation $x = y$).

This is the singleton law, satisfied only by the empty and singleton magmas. It is self-dual.

Definition 2.3 (Equation 3)**.** Equation 3 is the law $0 \simeq 0 \diamond 0$ (or the equation $x = x \diamond x$).

This is the idempotence law. It is self-dual.

Definition 2.4 (Equation 4)**.** Equation 4 is the law $0 \simeq 0 \diamond 1$ (or the equation $x = x \diamond y$).

This is the left absorption law.

Definition 2.5 (Equation 5)**.** Equation 5 is the law $0 \simeq 1 \diamond 0$ (or the equation $x = y \diamond x$).

This is the right absorption law (the dual of Theorem 2.4).

Definition 2.6 (Equation 6)**.** Equation 6 is the law $0 \simeq 1 \diamond 1$ (or the equation $x = y \diamond y$).

This law is equivalent to the singleton law.

Definition 2.7 (Equation 7)**.** Equation 7 is the law $0 \simeq 1 \diamond 2$ (or the equation $x = y \diamond z$).

This law is equivalent to the singleton law.

Definition 2.8 (Equation 8)**.** Equation 8 is the law $0 \simeq 0 \diamond (0 \diamond 0)$ (or the equation $x = x \diamond (x \diamond x)$).

Definition 2.9 (Equation 14)**.** Equation 14 is the law $0 \simeq 1 \diamond (0 \diamond 1)$ (or the equation $x = y \diamond (x \diamond y)$).

Appears in Problem A1 from Putnam 2001. See Theorem 5.2.

Definition 2.10 (Equation 16)**.** Equation 16 is the law $0 \simeq 1 \diamond (1 \diamond 0)$ (or the equation $x = y \diamond (y \diamond x)$).

Definition 2.11 (Equation 23)**.** Equation 23 is the law $0 \simeq (0 \diamond 0) \diamond 0$ (or the equation $x = (x \diamond x) \diamond x$).

This is the dual of Theorem 2.8.

Definition 2.12 (Equation 29)**.** Equation 29 is the law $0 \simeq (1 \diamond 0) \diamond 1$ (or the equation $x = (y \diamond x) \diamond y$).

Appears in Problem A1 from Putnam 2001. Dual to Theorem 2.9. See Theorem 5.2.

Definition 2.13 (Equation 38)**.** Equation 38 is the law $0 \diamond 0 \simeq 0 \diamond 1$ (or the equation $x \diamond x = x \diamond y$).

This law asserts that the magma operation is independent of the second argument.

Definition 2.14 (Equation 39)**.** Equation 39 is the law $0 \diamond 0 \simeq 1 \diamond 0$ (or the equation $x \diamond x = y \diamond x$).

This law asserts that the magma operation is independent of the first argument (the dual of Theorem 2.13).

Definition 2.15 (Equation 40)**.** Equation 40 is the law $0 \diamond 0 \simeq 1 \diamond 1$ (or the equation $x \diamond x = y \diamond y$).

This law asserts that all squares are constant. It is self-dual.

Definition 2.16 (Equation 41)**.** Equation 41 is the law $0 \diamond 0 \simeq 1 \diamond 2$ (or the equation $x \diamond x = y \diamond z$).

This law is equivalent to the constant law, Theorem 2.20.

Definition 2.17 (Equation 42)**.** Equation 42 is the law $0 \diamond 1 \simeq 0 \diamond 2$ (or the equation $x \diamond y = x \diamond z$).

Equivalent to Theorem 2.13.

Definition 2.18 (Equation 43)**.** Equation 43 is the law $0 \diamond 1 \simeq 1 \diamond 0$ (or the equation $x \diamond y = y \diamond x$).

The commutative law. It is self-dual.

Definition 2.19 (Equation 45)**.** Equation 45 is the law $0 \diamond 1 \simeq 2 \diamond 1$ (or the equation $x \diamond y = z \diamond y$).

This is the dual of Theorem 2.17.

Definition 2.20 (Equation 46)**.** Equation 46 is the law $0 \diamond 1 \simeq 2 \diamond 3$ (or the equation $x \diamond y = z \diamond w$).

The constant law: all products are constant. It is self-dual.

Definition 2.21 (Equation 63)**.** Equation 63 is the law $0 \simeq 1 \diamond (0 \diamond (0 \diamond 1))$ (or the equation $x = y \diamond (x \diamond (x \diamond y))$).

The "Dupont" law, studied further in Section 7.6.

Definition 2.22 (Equation 65)**.** Equation 65 is the law $0 \simeq 1 \diamond (0 \diamond (1 \diamond 0))$ (or the equation $x = y \diamond (x \diamond (y \diamond x))$).

The "Asterix" law, studied further in Section 7.2.

Definition 2.23 (Equation 168)**.** Equation 168 is the law $0 \simeq (1 \diamond 0) \diamond (0 \diamond 2)$ (or the equation $x = (y \diamond x) \diamond (x \diamond z)$).

The law of a central groupoid. It is self-dual.

Definition 2.24 (Equation 206)**.** Equation 206 is the law $0 \simeq (0 \diamond (0 \diamond 1)) \diamond 1$ (or the equation $x = (x \diamond (x \diamond y)) \diamond y$).

Our project located this law as one member of an "Austin pair"; see Chapter 3. The infinite counterexample is constructed using the infinite 3-regular tree.

Definition 2.25 (Equation 381)**.** Equation 381 is the law $0 \diamond 1 \simeq (0 \diamond 2) \diamond 1$ (or the equation $x \diamond y = (x \diamond z) \diamond y$).

Appears in Putnam 1978, Problem A4, part (b).

Definition 2.26 (Equation 387)**.** Equation 387 is the law $0 \diamond 1 \simeq (1 \diamond 1) \diamond 0$ (or the equation $x \diamond y = (y \diamond y) \diamond x$).

Introduced in MathOverflow. See Theorem 5.1

Definition 2.27 (Equation 477)**.** Equation 477 is the law $0 \simeq 1 \diamond (0 \diamond (1 \diamond (1 \diamond 1)))$ (or the equation $x = y \diamond (x \diamond (y \diamond (y \diamond y)))$).

An example of a confluent law; see Theorem 10.8.

Definition 2.28 (Equation 854)**.** Equation 854 is the law $0 = 0 \diamond ((1 \diamond 2) \diamond (0 \diamond 2))$ (or the equation $x = x \diamond ((y \diamond z) \diamond (x \diamond z))$).

Studied in Chapter 14

Definition 2.29 (Equation 953)**.** Equation 953 is the law $0 = 1 \diamond ((2 \diamond 0) \diamond (2 \diamond 2))$ (or the equation $x = y \diamond ((z \diamond x) \diamond (z \diamond z))$).

An example of a trivial law; see Theorem 5.7.

Definition 2.30 (Equation 1485)**.** Equation 1485 is the law $0 \simeq (1 \diamond 0) \diamond (0 \diamond (2 \diamond 1))$ (or the equation $x = (y \diamond x) \diamond (x \diamond (z \diamond y))$).

The weak central groupoid law, implied by the central groupoid law Theorem 2.23. Studied in Chapter 12.

Definition 2.31 (Equation 1491)**.** Equation 1491 is the law $0 \simeq (1 \diamond 0) \diamond (1 \diamond (1 \diamond 0))$ (or the equation $x = (y \diamond x) \diamond (y \diamond (y \diamond x))$).

The "Obelix" law, studied further in Section 7.2.

Definition 2.32 (Equation 1571)**.** Equation 1571 is the law $0 \simeq (1 \diamond 2) \diamond (1 \diamond (0 \diamond 2))$ (or the equation $x = (y \diamond z) \diamond (y \diamond (x \diamond z))$).

Introduced in [11]. As shown in Theorem 5.6, this law characterizes abelian groups of exponent two.

Definition 2.33 (Equation 1648)**.** Equation 1648 is the law $0 \simeq (0 \diamond 1) \diamond ((0 \diamond 1) \diamond 1)$ (or the equation $x = (x \diamond y) \diamond ((x \diamond y) \diamond y)$).

The golden ratio is a coefficient of the linearization of this law.

Definition 2.34 (Equation 1657)**.** Equation 1657 is the law $0 \simeq (0 \diamond 1) \diamond ((1 \diamond 1) \diamond 0)$ (or the equation $x = (x \diamond y) \diamond ((y \diamond y) \diamond x)$).

Definition 2.35 (Equation 1659)**.** Equation 1659 is the law $0 \simeq (0 \diamond 1) \diamond ((1 \diamond 1) \diamond 2)$ (or the equation $x = (x \diamond y) \diamond ((y \diamond y) \diamond z)$).

Definition 2.36 (Equation 1661)**.** Equation 1661 is the law $0 \simeq (0 \diamond 1) \diamond ((1 \diamond 2) \diamond 1)$ (or the equation $x = (x \diamond y) \diamond ((y \diamond z) \diamond y)$).

These two laws admit infinite models on the natural numbers arising from the modified base model construction. See Section 7.5.

Definition 2.37 (Equation 1689)**.** Equation 1689 is the law $0 \simeq (1 \diamond 0) \diamond ((0 \diamond 2) \diamond 2)$ (or the equation $x = (y \diamond x) \diamond ((x \diamond z) \diamond z)$).

Mentioned in [5]. See Theorem 5.5.

Definition 2.38 (Equation 1701)**.** Equation 1701 is the law $0 \simeq (1 \diamond x) \diamond ((2 \diamond 0) \diamond 0)$ (or the equation $x = (y \diamond x) \diamond ((z \diamond x) \diamond x)$).

This law admits infinite models on the natural numbers arising from the modified base model construction. See Section 7.5.

Definition 2.39 (Equation 2662)**.** Equation 2662 is the law $0 \simeq ((0 \diamond 1) \diamond (0 \diamond 1)) \diamond 0$ (or the equation $x = ((x \diamond y) \diamond (x \diamond y)) \diamond x$).

Appears in [11].

Definition 2.40 (Equation 3167)**.** Equation 3167 is the law $0 \simeq (((1 \diamond 1) \diamond 2) \diamond 2) \diamond 0$ (or the equation $x = (((y \diamond y) \diamond z) \diamond z) \diamond x$).

Definition 2.41 (Equation 3588)**.** Equation 3588 is the law $0 \diamond 1 \simeq 2 \diamond ((0 \diamond 1) \diamond 2)$ (or the equation $x \diamond y = z \diamond ((x \diamond y) \diamond z)$).

Our project located this law as one member of an "Austin pair"; see Chapter 3.

Definition 2.42 (Equation 3722)**.** Equation 3722 is the law $0 \diamond 1 \simeq (0 \diamond 1) \diamond (0 \diamond 1)$ (or the equation $x \diamond y = (x \diamond y) \diamond (x \diamond y)$).

Appears in Putnam 1978, Problem A4, part (a). It is self-dual.

Definition 2.43 (Equation 3744)**.** Equation 3744 is the law $0 \diamond 1 \simeq (0 \diamond 2) \diamond (3 \diamond 1)$ (or the equation $x \diamond y = (x \diamond z) \diamond (w \diamond y)$).

This law is called a "bypass operation" in Putnam 1978, Problem A4. It is self-dual. See Theorem 5.4.

Definition 2.44 (Equation 3994)**.** Equation 3994 is the law $0 \diamond 1 \simeq (2 \diamond (0 \diamond 1)) \diamond 2$ (or the equation $x \diamond y = (z \diamond (x \diamond y)) \diamond z$).

Our project located this law as one member of an "Austin pair"; see Chapter 3.

Definition 2.45 (Equation 4315)**.** Equation 4315 is the law $0 \diamond (1 \diamond 0) \simeq 0 \diamond (1 \diamond 2)$ (or the equation $x \diamond (y \diamond x) = x \diamond (y \diamond z)$).

Definition 2.46 (Equation 4512)**.** Equation 4512 is the law $0 \diamond (1 \diamond 2) \simeq (0 \diamond 1) \diamond 2$ (or the equation $x \diamond (y \diamond z) = (x \diamond y) \diamond z$).

The associative law. It is self-dual.

Definition 2.47 (Equation 4513)**.** Equation 4513 is the law $0 \diamond (1 \diamond 2) \simeq (0 \diamond 1) \diamond 3$ (or the equation $x \diamond (y \diamond z) = (x \diamond y) \diamond w$).

Definition 2.48 (Equation 4522)**.** Equation 4522 is the law $0 \diamond (1 \diamond 2) \simeq (0 \diamond 3) \diamond 4$ (or the equation $x \diamond (y \diamond z) = (x \diamond w) \diamond u$).

Dual to Theorem 2.50.

Definition 2.49 (Equation 4564)**.** Equation 4564 is the law $0 \diamond (1 \diamond 2) \simeq (3 \diamond 1) \diamond 2$ (or the equation $x \diamond (y \diamond z) = (w \diamond y) \diamond z$).

Dual to Theorem 2.47.

Definition 2.50 (Equation 4579)**.** Equation 4579 is the law $0 \diamond (1 \diamond 2) \simeq (3 \diamond 4) \diamond 2$ (or the equation $x \diamond (y \diamond z) = (w \diamond u) \diamond z$).

Dual to Theorem 2.48.

Definition 2.51 (Equation 4582)**.** Equation 4582 is the law $0 \diamond (1 \diamond 2) \simeq (3 \diamond 4) \diamond 5$ (or the equation $x \diamond (y \diamond z) = (w \diamond u) \diamond v$).

This law asserts that all triple constants (regardless of bracketing) are constant.

2.1 Equations of order greater than 4

We note some selected laws of order more than 5, which are used in some later chapters of the blueprint.

Definition 2.52 (Equation 5093)**.** Equation 5093 is the law $0 \simeq 1 \diamond (1 \diamond (1 \diamond (0 \diamond (2 \diamond 1))))$ (or the equation $x = y \diamond (y \diamond (y \diamond (x \diamond (z \diamond y))))$).

This law of order 5 was mentioned in [5]. See Theorem 3.3.

Definition 2.53 (Equation 26302)**.** Equation 26302 is the law $0 \simeq (1 \diamond ((2 \diamond 0) \diamond 3)) \diamond (0 \diamond 3)$ (or the equation $x = (y \diamond ((z \diamond x) \diamond w)) \diamond (x \diamond w)$).

A law that characterizes natural central groupoids; see Theorem 5.9.

Definition 2.54 (Equation 28770)**.** Equation 28770 is the law $0 \simeq (((1 \diamond 1) \diamond 1) \diamond 0) \diamond (1 \diamond 2)$ (or the equation $x = (((y \diamond y) \diamond y) \diamond x) \diamond (y \diamond z)$).

This law of order 5 was introduced by Kisielewicz [6]. See Theorem 3.2.

Definition 2.55 (Equation 345169)**.** Equation 345169 is the law $0 \simeq (1 \diamond ((0 \diamond 1) \diamond 1)) \diamond (0 \diamond (2 \diamond 1))$ (or the equation $x = (y \diamond ((x \diamond y) \diamond y)) \diamond (x \diamond (z \diamond y))$).

This law of order 6 was shown in [10] to characterize the Sheffer stroke in a boolean algebra; see Theorem 5.8.

Definition 2.56 (Equation 374794)**.** Equation 374794 is the law $0 \simeq (((1 \diamond 1) \diamond 1) \diamond 0) \diamond ((1 \diamond 1) \diamond 2)$ (or the equation $x = (((y \diamond y) \diamond y) \diamond x) \diamond ((y \diamond y) \diamond z)$).

This law of order 6 was introduced by Kisielewicz [6]; see Theorem 3.1.

Chapter 3

Infinite models

In this chapter we consider non-implications which are refuted only on infinite models, as those are more challenging to prove—they can't be proved by directly giving an operation table and checking which laws it satisfies.

The singleton or empty magma obeys all equational laws. One can ask whether an equational law admits nontrivial finite or infinite models. An *Austin law* is a law which admits infinite models, but no nontrivial finite models. Austin [1] established the first such law, namely the order 9 law

$$(((1 \diamond 1) \diamond 1) \diamond 0) \diamond (((1 \diamond 1) \diamond ((1 \diamond 1) \diamond 1)) \diamond 2) \simeq 0.$$

A shorter Austin law of order 6 was established in [6]:

Theorem 3.1 (Kisielewicz's first Austin law)**.** *Theorem 2.56 is an Austin law.*

Proof. First we show that every finite model of Theorem 2.56 is trivial. Write $y^2 := y \diamond y$ and $y^3 := y^2 \diamond y$. For any y, z, introduce the functions $f_y : x \mapsto y^3 \diamond x$ and $g_{yz} : x \mapsto x \diamond (y^2 \diamond z)$. Theorem 2.56 says that $g_{yz}(f_y(x)) = x$, hence by finiteness $g_{yz} = f_y^{-1}$, showing that g_{yz} does not depend on the value of z. Since

$$f_y(y^2 \diamond z) = g_{yz}(y^3),$$

it follows that $f_y(y^2 \diamond z) = f_y(y^3)$ which by injectivity of f_y implies that $z \mapsto y^2 \diamond z$ is a constant function (with y fixed). Substituting y^2 for y shows that the same is true for $z \mapsto (y^2 \diamond y^2) \diamond z$, and since

$$f_y(z) = (y^2 \diamond y) \diamond z = (y^2 \diamond y^2) \diamond z$$

we conclude that f_y is also a constant function. But this function is already known to be injective, thus there do not exist distinct elements in its domain, showing that the model must be trivial.

To construct an infinite model, consider the magma of positive integers $\mathbb{Z}^+$ with the operation $x \diamond y$ defined by

$$x \diamond y = \begin{cases} 2^y, & x = y \\ 3^y, & x = 1,\ y \neq 1 \\ z, & x = 3^z,\ y \neq x \\ 1, & else \end{cases}.$$

Then $y \diamond y = 2^y$ and $(y \diamond y) \diamond y = 1$ for all y. If $x \neq 1$ we have that

$$((y \diamond y) \diamond y) \diamond x = 3^x,$$

and since $(y \diamond y) \diamond z$ is a power of two for all y, z it follows that

$$3^x \diamond ((y \diamond y) \diamond z) = x.$$

The case $x = 1$ requires a further argument: observe that $w = (y \diamond y) \diamond z$ evaluates to one unless $z = 2^y$, in which case it evaluates to 2^{2^y} (which is greater than or equal to four). In particular, w never takes the value two. Thus

$$(((y \diamond y) \diamond y) \diamond 1) \diamond ((y \diamond y) \diamond z) = 2 \diamond w = 1,$$

concluding our proof that this magma is a model of Theorem 2.56 □

An even shorter law (order 5) was obtained by the same author in a follow-up paper [5]:

Theorem 3.2 (Kisielewicz's second Austin law)**.** *Theorem 2.54 is an Austin law.*

Proof. Using the y^2 and y^3 notation as before, the law reads

$$x = (y^3 \diamond x) \diamond (y \diamond z). \tag{3.1}$$

In particular, for any y, the map $T_y \colon x \mapsto y^3 \diamond x$ is injective, hence bijective in a finite model G. In particular we can find a function $f : G \to G$ such that $T_y f(y) = y^3$ for all y Applying Equation (3.1) with $x = f(y)$, we conclude

$$T_y(y \diamond z) = y^3 \diamond (y \diamond z) = f(y)$$

and thus $y \diamond z$ is independent of z by injectivity of T_y. Thus, the left-hand side of Equation (3.1) does not depend on x, and so the model is trivial. This shows there are no non-trivial finite models.

To establish an infinite model, use $\mathbb{N}$ with $x \diamond y$ defined by requiring

$$y \diamond y = 2^y; \quad 2^y \diamond y = 3^y$$

and

$$3^y \diamond x = 3^y 5^x$$

for $x \neq 3^y$, and

$$(3^y 5^x) \diamond z = x$$

for $z \neq 3^y 5^x$. Finally set

$$2^{3^y} \diamond z = 3^y$$

for $z \neq 3^y, 2^{3^y}$. All other assignments of $\diamond$ may be made arbitrarily. It is then a routine matter to establish Equation (3.1). □

In that paper a computer search was also used to show that no law of order four or less is an Austin law.

An open question is whether Theorem 2.52 is an Austin law. We have the following partial result from [5]:

Theorem 3.3 (Equation 5093 has no non-trivial finite models)**.** *Theorem 2.52 has no non-trivial finite models.*

Proof. From Theorem 2.52 we see that the map $w \mapsto y \diamond w$ is onto, hence injective in a finite model. Using this injectivity four times in Theorem 2.52, we see that $z \diamond y$ does not depend on z, hence the expression $x \diamond (z \diamond y)$ does not depend on x. By Theorem 2.52 again, this means that x does not depend on x, which is absurd in a non-trivial model. □

We also have such a non-implication involving two laws of order 4:

Theorem 3.4 (3994 implies 3588 for finite models)**.** *All finite magmas which satisfy Theorem 2.44 also satisfy Theorem 2.41.*

Proof. For a finite magma M, consider the set $S = \{x \diamond y | x, y \in M\}$. Now $f_z : x \mapsto z \diamond x$ and $g_z : x \mapsto x \diamond z$. They both map S to S, and due to the hypothesis $g_z \diamond f_z$ is the identity on S, so because S is finite f_z and g_z must be inverse bijections on it, and therefore they commute. □

Theorem 3.5 (3994 does not imply 3588 for infinite models)**.** *There exists a magma which satisfies Theorem 2.44 and not Theorem 2.41.*

Proof. Consider $\mathbb{N}$, with $x \diamond y$ defined as $x \oplus y$ (bitwise XOR) if x and y are even, $y+2$ if only y is even, $x \dot{-} 2$ if only x is even, and 0 if both are odd. Note that the range of the operation is the set of even naturals. Theorem 2.44 is satisfied, because for even z we get $z \oplus (x \diamond y) \oplus z = x \diamond y$ and for odd z we get $(x \diamond y) + 2 \dot{-} 2 = x \diamond y$. Setting $x = y = z = 1$, Theorem 2.41 isn't satisfied. □

The following result was established in [2]:

Theorem 3.6 (Austin's finite model theorem)**.** *Any law with at most two variables has a non-trivial finite model.*

Proof. If neither side of the law is a single variable then the zero law $x \diamond y = 0$ will work, so one can assume the law takes the form $x = f(x, y)$. Consider a finite field F with the operation $x \diamond y := ax + by$ for some coefficients $a, b \in F$. Then the law becomes a pair of equations $P(a, b) = 0$, $Q(a, b) = 1$ in the coefficients for some polynomials P, Q with integer coefficients, which one can verify to not divide each other (they have the same degree, and do not have the same set of non-zero monomials). From Bezout's theorem, this equation has a solution in some field, and hence by the Lefschetz principle it has a solution in a finite field. □

Many implications for finite magmas rely on the fact that if $f, g : X \to X$ are functions on a finite set X, then $f \circ g = I$ if and only if $g \circ f = I$. Two more complicated variants of this are as follows.

Lemma 3.7. *Let X be finite, and let $f, g : X \to X$ be such that $f = f \circ f \circ g$. Then $f = f \circ g \circ f$.*

Proof. Call a point $x \in X$ *periodic* if $f^n(x) = x$ for some $n > 0$. Because the forward orbit $x, f(x), f^2(x), ...$ in a finite space X must repeat, we see that for each x there exists an n such that $f^n(x)$ is periodic. Let n_x be the first n for which this occurs. If $n_x > 1$, then $g(x), f(g(x)), f(f(g(x))$ cannot be periodic (as this would imply $f(x)$ periodic), and then we can see that $n_{g(x)} = n_x + 1$. Hence the maximal value of n_x is at most 1, which implies that $f(x)$ is periodic for every x. Thus there is an $n > 1$ such that $f^n = f$. Since $f = f^2 \circ g$, we have $f^n = f^{n-2} \circ f \circ f = f^{n-2} \circ (f^2 \circ g) \circ f = f^n \circ g \circ f = f \circ g \circ f$, as desired. □

Lemma 3.8. *Let X be finite, and let $f, g : X \to X$ be such that $f = g \circ f \circ f$. Then $f = f \circ g \circ f$.*

Proof. By hypothesis, $f^2(x)$ uniquely determines $f(x)$. This prevents $n_x = 2$ for any x (because if $n > 2$ is such that $f^{n+2}(x) = f^2(x)$, then $f^{n+1}(x) \neq f(x)$), and hence also prevents $n_x > 2$ for any x. So again we have $f(x)$ periodic for all x, so $f^n = f$ for some $n > 1$. Then $f = f^n = f \circ (g \circ f^2) \circ f^{n-2} = f \circ g \circ f^n = f \circ g \circ f$ as required. □

This can be used to obtain a few positive finite magma implications, for instance by setting f, g to be left and right multiplication operators. Another useful lemma is

Lemma 3.9 (Eventual period)**.** *Let X be finite and $f : X \to X$. Then there exists $n \geq 1$ such that $f^{2n} = f^n$.*

Proof. By the pigeonhole principle, there exists $n \geq 1$, $m \geq 0$ such that $f^{m+n} = f^m$, which implies on iteration that $f^{m+mn} = f^m$ and hence $f^{2mn} = f^{mn}$, giving the claim. □

As a sample application, we have

Corollary 3.10 (3342)**.** *On a finite magma M, equation 3342, $x \diamond y = y \diamond (x \diamond (x \diamond x))$, implies equation 3522, $x \diamond y = x \diamond ((y \diamond y) \diamond y)$, as well as equation 4118, $x \diamond y = ((x \diamond x) \diamond x) \diamond y$.*

Proof. Write $Sx := x\diamond$, $fx := x \diamond Sx$ and $Cx = Sx \diamond x$, then we have $x \diamond y = y \diamond fx$, and our task is to show $x \diamond y = Cx \diamond y$ and $x \diamond y = x \diamond Cy$ for finite magmas, giving the four open implications.

Note that $x \diamond y = y \diamond fx = fx \diamond fy$, hence f is a homomorphism. By Theorem 3.9, there is $n \geq 1$ with $f^n = f^{2n}$. From 3342 we have $Sx = Sfx$ and $Cx = Sx \diamond x = f^n Sx \diamond f^n x = f^n Sx \diamond f^{2n} x = f^{2n-1} x \diamond f^n Sx = f^{n-1} x \diamond Sx = f(f^{n-1} x) = f^n x$. Then

$$Cx \diamond y = f^n x \diamond y = f^{2n} x \diamond f^n y = f^n x \diamond f^n y = x \diamond y$$

and a similar argument gives $x \diamond Cy = x \diamond y$. □

Proposition 3.11 (1167 implies 1096)**.** *For finite magmas, Equation 1167,*

$$x = y \diamond ((z \diamond (y \diamond y)) \diamond x)$$

implies Equation 1096,

$$x = y \diamond ((x \diamond (z \diamond y)) \diamond x).$$

Proof. We write 1167 as

$$L_y L_{z \diamond Sy} = I,$$

hence L_y is invertible and $L_{z \diamond Sy} L_y = I$. In particular $L_{z \diamond Sy} Sy = y$, hence squaring is injective, hence surjective. So 1167 can be rewritten as $L_{S^{-1} y} L_{z \diamond y} = I$, hence $L_{z \diamond y}$ is independent of z. In particular

$$L_{x \diamond (z \diamond y)} = L_{S^{-2} z \diamond (z \diamond y)} = L_{L_{S^{-2} z} L_{S^{-1} z \diamond S S^{-2} z} y} = L_y$$

by 1167, hence the right-hand side of 1096 is independent of z. Replacing z with y, the claim now follows from 1167. □

Proposition 3.12 (1133 implies 1167)**.** *For finite magmas, Equation 1133,*

$$x = y \diamond ((y \diamond (z \diamond y)) \diamond x)$$

implies Equation 1167,

$$x = y \diamond ((z \diamond (y \diamond y)) \diamond x).$$

Proof. 1133 asserts that $L_y L_{y \diamond (z \diamond y)} = I$, hence L_y is invertible and $L_{y \diamond (z \diamond y)} = L_y^{-1}$ does not depend on z. Setting $z = y \diamond Sy$ we see from 1133 that $y \diamond (z \diamond y) = y$ and hence we have left-involution: $L_y = L_y^{-1}$. Replacing y with $L_z y$ in 1133 we now get $L_{L_z y} L_{L_z y \diamond y} = I$, which since $L_{L_z y}$ is its own inverse gives

$$L_{L_z y \diamond y} = L_{L_z y}. \tag{3.2}$$

In particular

$$R_y^3 z = L_{L_z y \diamond y} y = L_{L_z y} y = R_y^2 z$$

hence as $L_{R_y^2 z}$ is its own inverse

$$y = L_{R_y^2 z} L_{R_y^2 z} y = L_{R_y^2 z} R_y^3 z = L_{R_y^2 z} R_y^3 z = S(R_y^2 z).$$

Thus squaring is surjective, hence invertible.

Next, by (3.2) we have $L_{z \diamond Sy} = L_w$ where $w = R_{Sy}^2 z$. By (3.2) and the fact that L_w is its own inverse, we have

$$L_w^2 w = w = L_{z \diamond Sy} Sy = L_w Sy,$$

hence $Sw = L_w w = Sy$. As S is injective, we have $L_w = L_y$, and then $L_y L_{z \diamond Sy} = L_y^2 = I$, giving 1167. □

Proposition 3.13 (1441 implies 4067, 1443 implies 3055)**.** *For finite magmas, Equation 1441,*

$$x = (x \diamond y) \diamond (x \diamond (x \diamond x))$$

implies Equation 4067,

$$x \diamond x = ((x \diamond x) \diamond y) \diamond x,$$

and equation 1443,

$$x = (x \diamond y) \diamond (x \diamond (x \diamond z))$$

implies Equation 3055,

$$x = (((x \diamond x) \diamond y) \diamond x) \diamond x.$$

Proof. Write $\tilde{C}x = x \diamond Sx$, then 1441 asserts that $R_{\tilde{C}x} R_y x = x$. Setting

$$y = Sx$$

we get $x = S\tilde{C}x$, so by finiteness $\tilde{C}Sx = x$. Replacing x with Sx in 1441 we conclude $R_x R_y Sx = Sx$ which is 4067.

Clearly 1443 implies 1441, hence 4067 by the previous implication, so that 3055 simplifies to $x = Sx \diamond x$. Meanwhile, 1443 also implies $x = S(x \diamond (x \diamond z))$. On taking square roots and using $S\tilde{C} = x$, we obtain $x \diamond (x \diamond z) = \tilde{C}x$. Applying this with $z = Sx$ we conclude $L_x \tilde{C}x = \tilde{C}x$, hence on replacing x with Sx we get $L_{Sx} x = x$ as required. □

Proposition 3.14 (1681 implies 3877, 1701 implies 1035)**.** *For finite magmas, Equation 1681,*

$$x = (y \diamond x) \diamond ((x \diamond x) \diamond x)$$

implies Equation 3877,

$$x \diamond x = (y \diamond (x \diamond x)) \diamond x,$$

and Equation 1701,

$$x = (y \diamond x) \diamond ((z \diamond x) \diamond x)$$

implies Equation 1035,

$$x = x \diamond ((y \diamond (x \diamond x)) \diamond x).$$

Proof. This is very similar to the previous proof. Write $Cx = Sx \diamond x$, then 1681 asserts $R_{Cx} L_y x = x$. Again setting $y = Sx$ yields $x = SCx$ hence $x = CSx$, and on replacing x with Sx in 1681 one obtains 3877.

For the second part, we simplify to $x = x \diamond Sx$, while 1701 gives $x = S((z \diamond x) \diamond x)$ hence $(z \diamond x) \diamond x = Cx$, so $R_x Cx = Cx$, so $R_{Sx} x = x$ as required. □

Chapter 4

General implications

We will be interested in seeing which laws imply which other laws, in the sense that magmas obeying the former law automatically obey the latter. We will also be interested in *anti-implications* showing that one law does *not* imply another, by producing examples of magmas that obey the former law but not the latter. Here is a formal definition.

Definition 4.1 (Implication)**.** A law E is said to *imply* another law E' if $\{E\} \vDash E'$, or equivalently:

$$G \vDash w \simeq w' \implies G \vDash w'' \simeq w''' \text{ for all magmas } G$$

Two laws are said to be *equivalent* if they imply each other.

Lemma 4.2 (Pre-order)**.** *If we define $E \leq E'$ if E implies E', then this is a pre-order on the set of laws, and equivalence is an equivalence relation.*

Note that we view the stronger law as less than or equal to the weaker law. This is because the class of magmas that obey the stronger law is a subset of the class of magmas that obey the weaker law. It is also consistent with the conventions of Lean's Mathlib.

Proof. Trivial. □

Implications between the laws from Chapter 2 are depicted in Figure 4.1.

Lemma 4.3 (Maximal element)**.** *The law $0 \simeq 0$ is the maximal element in this pre-order.*

Proof. Trivial. □

Lemma 4.4 (Minimal element)**.** *The law $0 \simeq 1$ is the minimal element in this pre-order.*

Proof. Trivial. □

Every magma G has a *reversal* G^{op}, formed by by replacing the magma operation $\diamond$ with its opposite $\diamond^{\mathrm{op}} : (x, y) \mapsto y \diamond x$. There is a natural isomorphism between these magmas, which induces an involution $w \mapsto w^{\mathrm{op}}$ on words $w \in M_X$. Every law $w \simeq w'$ then has a *dual* $w^{\mathrm{op}} \simeq (w')^{\mathrm{op}}$.

For instance, the dual of the law $0 \diamond 1 = 0 \diamond 2$ is $1 \diamond 0 = 2 \diamond 0$, which after relabeling is $0 \diamond 1 = 2 \diamond 1$. A list of equations and their duals can be found here. Of the 4694 equations under consideration, 84 are self-dual, leaving 2305 pairs of dual equations.

The pre-ordering on laws has a duality symmetry:

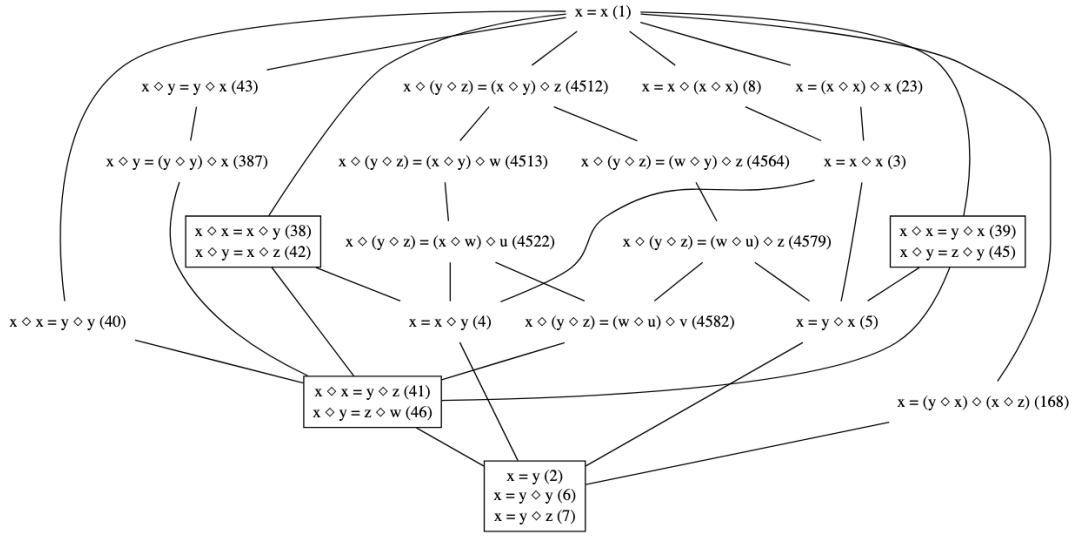

Figure 4.1: Implications between the above equations, displayed as a Hasse diagram.

Lemma 4.5 (Duality of laws)**.** *The law $w \simeq w'$ implies $w'' \simeq w'''$, if and only if $w^{\mathrm{op}} \simeq (w')^{\mathrm{op}}$ implies $w''^{\mathrm{op}} \simeq (w''')^{\mathrm{op}}$.*

Proof. This follows from the fact that a magma G satisfies a law $w \simeq w'$ if and only if G^{op} satisfies $w^{\mathrm{op}} \simeq (w')^{\mathrm{op}}$. □

Some equational laws can be "diagonalized":

Theorem 4.6 (Diagonalization)**.** *An equational law of the form*

$$F(x_1, \dots, x_n) = G(y_1, \dots, y_m), \tag{4.1}$$

where $x_1, \dots, x_n$ and $y_1, \dots, y_m$ are distinct elements of the alphabet, implies the diagonalized law

$$F(x_1, \dots, x_n) = F(x'_1, \dots, x'_n).$$

where $x'_1, \dots, x'_n$ are distinct from $x_1, \dots, x_n$ In particular, if $G(y_1, \dots, y_m)$ can be viewed as a specialization of $F(x'_1, \dots, x'_n)$, then these two laws are equivalent.

Proof. From two applications of Equation (4.1) one has

$$F(x_1, \dots, x_n) = G(y_1, \dots, y_m)$$

and

$$F(x'_1, \dots, x'_n) = G(y_1, \dots, y_m)$$

whence the claim. □

Thus for instance, Theorem 2.7 is equivalent to Theorem 2.2.

Theorem 4.7 (Laws implied by the constant law)**.** *If w, w' each have order at least one, then the law $w \simeq w'$ is implied by the constant law (Theorem 2.20). If exactly one of w, w' has order zero, and the law $w \simeq w'$ is not implied by the constant law.*

Proof. Routine. □

Theorem 4.8 (Criterion for implication)**.** *If $w \simeq w'$ is such that every variable appears the same number of times in both w and w', and $w \simeq w'$ implies another law $w'' \simeq w'''$, then every variable appears the same number of times in both w'' and w'''.*

Proof. Consider the magma MS of multisets over an arbitrary set A (which can be seen as finitely supported maps $A \to \mathbb{N}$), with the multiset addition law $+$. By hypothesis, this magma obeys $w \simeq w'$, and hence $w'' \simeq w'''$, giving the claim by comparing the orders of the elements of A appearing in w'' and w''' in this magma. □

Chapter 5

Implications between selected laws

We collect here some notable implications between the the selected laws in Chapter 2. By Theorem 1.8, every implication can basically be established by a finite number of rewrites. In most cases, the sequence of rewrites is quite straightforward, and the implication is very easy, but we record some less obvious examples.

Theorem 5.1 (387 implies 43)**.** *Theorem 2.26 implies Theorem 2.18.*

Proof. (From MathOverflow). By Theorem 2.26, one has the law

$$(x \diamond x) \diamond y = y \diamond x. \tag{5.1}$$

Specializing to $y = x \diamond x$, we conclude

$$(x \diamond x) \diamond (x \diamond x) = (x \diamond x) \diamond x$$

and hence by another application of Theorem 2.26 we see that $x \diamond x$ is idempotent:

$$(x \diamond x) \diamond (x \diamond x) = x \diamond x. \tag{5.2}$$

Now, replacing x by $x \diamond x$ in Equation (5.1) and then using Equation (5.2) we see that

$$(x \diamond x) \diamond y = y \diamond (x \diamond x)$$

so in particular $x \diamond x$ commutes with $y \diamond y$:

$$(x \diamond x) \diamond (y \diamond y) = (y \diamond y) \diamond (x \diamond x). \tag{5.3}$$

Also, from two applications of Equation (5.1) one has

$$(x \diamond x) \diamond (y \diamond y) = (y \diamond y) \diamond x = x \diamond y.$$

Thus Equation (5.3) simplifies to $x \diamond y = y \diamond x$, which is Theorem 2.18. □

Theorem 5.2 (29 equivalent to 14)**.** *Theorem 2.12 is equivalent to Theorem 2.9.*

This result was posed as Problem A1 from Putnam 2001.

Proof. By Theorem 4.5 it suffices to show that Theorem 2.12 implies Theorem 2.9. From Theorem 2.12 one has

$$x = ((x \diamond y) \diamond x) \diamond (x \diamond y)$$

and also

$$y = (x \diamond y) \diamond x$$

giving $x = y \diamond (x \diamond y)$, which is Theorem 2.9. □

Theorem 5.3 (14 implies 29)**.** *Theorem 2.9 implies Theorem 2.12.*

This result was posed as Problem A1 from Putnam 2001.

Proof. □

The following result was Problem A4 on Putnam 1978.

Theorem 5.4 (3744 implies 3722, 381)**.** *Theorem 2.43 implies Theorem 2.42 and Theorem 2.25.*

Proof. By hypothesis, one has

$$x \diamond y = (x \diamond z) \diamond (w \diamond y)$$

for all x, y, z, w. Various specializations of this give

$$x \diamond y = (x \diamond z) \diamond (y \diamond y) \tag{5.4}$$
$$x \diamond z = (x \diamond z) \diamond (x \diamond z) \tag{5.5}$$
$$(x \diamond z) \diamond y = ((x \diamond z) \diamond (x \diamond z)) \diamond (y \diamond y). \tag{5.6}$$

Equation (5.5) gives Theorem 2.42, while Equation (5.4), Equation (5.5), Equation (5.6) gives

$$x \diamond y = (x \diamond z) \diamond y$$

which is Theorem 2.25. □

Theorem 5.5 (1689 is equivalent to 2)**.** *Theorem 2.37 is equivalent to Theorem 2.2.*

Proof. The implication of Theorem 2.37 from Theorem 2.2 is trivial. The converse is a surprisingly long chain of implications; see pages 326–327 of [5]. With some computer assistance, we found the following human-readable proof. We denote $y^1 = y$ and $y^{n+1} = y^n \diamond y$ for $n \geq 1$. We also introduce the notation

$$f(x, y) = (x \diamond y) \diamond y, \qquad g(x, y) = x \diamond f(x, y) = x \diamond ((x \diamond y) \diamond y). \tag{5.7}$$

The initial equation states $x = (y \diamond x) \diamond f(x, z)$. Our main step will be to prove that for all $t \in M$ there exists $w \in M$ such that $f(t, w) = t$. The rest of the proof is then straightforward. Indeed, the initial equation gives $t = (y \diamond t) \diamond f(t, w) = (y \diamond t) \diamond t = f(y, t)$ for any $t, y \in M$. With such a simple expression of f the initial equation becomes $x = (y \diamond x) \diamond z$, which easily implies the singleton law, for instance by writing $x = ((y \diamond w) \diamond x) \diamond z = w \diamond z$ for any $w, x, y, z \in M$.

There remains to prove $f(t, w) = t$ for a well-chosen $w \in M$, explicitly, $w = g(t, t^5) = t \diamond t^7$. For any $t, u, v \in M$, the combinations $x = f(t, u)$ and $y = v \diamond t$ obey $y \diamond x = t$. Inserting these values into the initial equation yields the identity

$$f(t, u) = t \diamond f(f(t, u), z). \tag{5.8}$$

Specialize to $z = f(u,v)$ and note that $f(t,u) \diamond z = (\cdots \diamond u) \diamond f(u,v) = u$ by the initial equation so that $f(f(t,u),z) = (f(t,u) \diamond z) \diamond z = u \diamond z = g(u,v)$. Inserting this into (5.8) yields

$$f(t,u) = t \diamond g(u,v). \tag{5.9}$$

On the one hand, (5.8) with $z = u = t$ states that $t^3 = t \diamond t^5$, so (using $f(t^n,t) = t^{n+2}$)

$$f(t,t^5) = (t \diamond t^5) \diamond t^5 = t^3 \diamond t^5 = t^3 \diamond f(t^3,t) = g(t^3,t), \tag{5.10}$$

and (5.9) with $(u,v) = (t^3,t)$ then implies $f(t,t^3) = t \diamond g(t^3,t) = t \diamond f(t,t^5) = g(t,t^5)$. On the other hand, (5.9) with $(u,v) = (t,t^5)$ implies $t^3 = t \diamond g(t,t^5)$. We deduce

$$f(t,g(t,t^5)) = (t \diamond g(t,t^5)) \diamond g(t,t^5) = t^3 \diamond f(t,t^3) = (\cdots \diamond t) \diamond f(t,\ldots) = t. \tag{5.11}$$

□

The following result was established in [11].

Theorem 5.6 (Consequences of 1571)**.** *Magmas obeying Theorem 2.32 also obey Theorem 2.39, Theorem 2.15, Theorem 2.11, Theorem 2.8, Theorem 2.10, Theorem 2.9, Theorem 2.18, and Theorem 2.46, and are in fact abelian groups of exponent two. Conversely, all abelian groups of exponent two obey Theorem 2.32.*

Proof. Suppose that a magma G obeys Theorem 2.32, thus

$$x = (y \diamond z) \diamond (y \diamond (x \diamond z)). \tag{5.12}$$

$$x = ((x \diamond y) \diamond (x \diamond y)) \diamond ((x \diamond y) \diamond (x \diamond (x \diamond y)))$$

and

$$x = (x \diamond y) \diamond (x \diamond (x \diamond y))$$

whence

$$x = ((x \diamond y) \diamond (x \diamond y)) \diamond x$$

which is Theorem 2.39. This gives

$$y = ((y \diamond z) \diamond (y \diamond z)) \diamond y$$

while from Equation (5.12) one has

$$(y \diamond z) \diamond (y \diamond z) = (x \diamond y) \diamond (x \diamond ((y \diamond z) \diamond (y \diamond z) \diamond y))$$

whence

$$(x \diamond y) \diamond (x \diamond y) = (y \diamond z) \diamond (y \diamond z).$$

This implies that $(x \diamond y) \diamond (x \diamond y)$ does not depend on x, or on y, hence is equal to some constant e:

$$(x \diamond y) \diamond (x \diamond y) = e.$$

From Equation (5.12) the magma operation is surjective, hence

$$x \diamond x = e \tag{5.13}$$

which gives Theorem 2.15. Applying Equation (5.12) with $x = y = z$ we conclude

$$x = e \diamond (x \diamond e)$$

while if we instead take $y = z = e$ we have

$$x = e \diamond (e \diamond (x \diamond e))$$

hence

$$x = e \diamond x$$

and then also

$$x = x \diamond e$$

from which we readily conclude Theorem 2.11, Theorem 2.8; thus e is an identity element. From Equation (5.12) with $z = e$ we now have

$$x = y \diamond (y \diamond x) \tag{5.14}$$

which is Theorem 2.10. If instead we take $y = e$ we have

$$x = z \diamond (x \diamond z) \tag{5.15}$$

which is Theorem 2.9. So if we substitute $z = x \diamond y$ and use Equation (5.14) we obtain

$$x = (x \diamond y) \diamond y$$

and hence

$$y \diamond x = y \diamond ((x \diamond y) \diamond y) = x \diamond y$$

thanks to Equation (5.15). This gives Theorem 2.18, thus G is now commutative. From Equation (5.12) once more one has

$$x \diamond (y \diamond z) = (y \diamond x) \diamond (z \diamond ((x \diamond (y \diamond z)) \diamond x))$$

which one can simplify using commutativity and Equation (5.14) (or Equation (5.15)) to eventually obtain

$$x \diamond (y \diamond z) = (x \diamond y) \diamond z$$

which is Theorem 2.46. G is now commutative and associative, and every element is its own inverse and of exponent 2, hence is an abelian group thanks to Equation (5.13), so G is an abelian group of exponent 2 as claimed. The converse is easily verified. □

Theorem 5.7 (953 is equivalent to 2)**.** *Theorem 2.29 is equivalent to Theorem 2.2.*

Proof. It suffices to show that Theorem 2.29 implies Theorem 2.2. Pick an element 0 of G and define $1 = 0 \diamond 0$ and $2 = 1 \diamond 1$ (we do not require $0, 1, 2$ to be distinct). From Theorem 2.29 with $x = z = 0$ we have

$$0 = y \diamond 2.$$

If we then apply Theorem 2.29 with $z = 1$ we conclude that

$$x = y \diamond 0$$

for all x, y, from which one concludes $x = x'$ for any $x, x' \in G$, giving Theorem 2.2. □

Theorem 5.8 (Sheffer stroke axiom)**.** *Definition Theorem 2.55 axiomatizes the Sheffer stroke operation $x \diamond y = \overline{xy}$ in a Boolean algebra.*

Proof. See [10]. In fact this is the shortest law with this property.

A sketch of proof follows. One can easily verify that the Sheffer stroke operation obeys this law. Conversely, if this law holds, then automated theorem provers can show that the three Sheffer axioms

$$(x \diamond x) \diamond (x \diamond x) = x$$
$$x \diamond (y \diamond (y \diamond y)) = x \diamond x$$
$$(x \diamond (y \diamond z)) \diamond (x \diamond (y \diamond z)) = ((y \diamond y) \diamond x) \diamond ((z \diamond z) \diamond x)$$

are satisfied. A classical result of Sheffer [12] then allows one to conclude. □

A *natural central groupoid* is, up to isomorphism, a magma with carrier $S \times S$ for some set S and operation

$$(a, b) \diamond (c, d) = (b, c).$$

These are examples of central groupoids (Theorem 2.23).

Theorem 5.9 (Natural central groupoid axiom)**.** *Theorem 2.53 characterizes natural central groupoids.*

Proof. See [7, Theorem 5]. The proof is quite lengthy; a sketch is as follows. It is easy to see that natural central groupoids obey Theorem 2.53. Conversely, if this law holds, then

$$\begin{aligned}(y \diamond z) \diamond (z \diamond w) &= ((x \diamond ((w \diamond (y \diamond z)) \diamond w)) \diamond ((y \diamond z) \diamond w)) \diamond (z \diamond w) \\ &= z\end{aligned}$$

so we have a central groupoid. Setting $y = (t \diamond t) \diamond t$, $z = t \diamond (t \diamond t)$, $w = t \diamond t$ in Theorem 2.53 we also obtain

$$(x \diamond t) \diamond t = (t \diamond t) \diamond t.$$

Using the notation

$$x^{(1)} := (x \diamond x) \diamond x, \quad x^{(2)} := x \diamond (x \diamond x)$$

we then have

$$\begin{aligned}x \diamond t &= ((x \diamond x) \diamond (x \diamond t)) \diamond ((x \diamond t) \diamond t) \\ &= x \diamond t^{(1)}.\end{aligned}$$

A lengthy computer-assisted argument then gave the dual identity

$$t^{(2)} \diamond x = t \diamond x$$

Together, these give

$$x^{(2)} \diamond y^{(1)} = x \diamond y.$$

Multiplying on the left by $x = x^{(1)} \diamond x^{(2)}$, one can conclude that

$$x^{(2)} = x \diamond (x \diamond y).$$

One then has

$$\begin{aligned}(x \diamond y)^{(1)} &= ((y \diamond x) \diamond (x \diamond y)) \diamond (x \diamond y) \\ &= x \diamond (x \diamond y) \\ &= x^{(2)}\end{aligned}$$

and a similar argument gives

$$(x \diamond y)^{(2)} = y^{(1)}.$$

Since $(x \diamond x)^{(1)} = x^{(2)}$ and $(x \diamond x)^{(2)} = x^{(1)}$, we conclude that $x^{(1)}$ and $x^{(2)}$ are idempotent. Since $x = x^{(1)} \diamond x^{(2)}$, we see that every x is the product of two idempotents. One can show that this representation is unique, and gives a canonical identification with a natural central groupoid. $\square$

Chapter 6

Selected magmas

Each magma can be used to establish anti-implications: if Γ is the set of all laws obeyed by a magma G, then we have $\neg E \leq E'$ whenever $E \in \Gamma$ and $E' \notin \Gamma$. Large numbers of implications can already be obtained from

- All magmas of order at most 4, up to isomorphism (of which there are $178,985,294$);
- All commutative magmas of order 5, up to isomorphism **determine their count**;
- Cyclic groups $\mathbb{Z}/N\mathbb{Z}$ with $2 \leq N \leq 12$ and $x \diamond y = ax^2 + bxy + cy^2 + dx + ey$ for randomly chosen a, b, c, d, e.
- There are only 1410 distinct cancellative magmas of order 5 (up to isomorphism), and Mace4 can generate all of them in under 20 seconds. A shell script to do this is available here. A magma is cancellative if $xy = xz$ implies $y = z$ and $yx = zx$ implies $y = z$.

We also note that a systematic (computer-assisted) study of magmas of order 3 was performed in [4], though with current computational resources it was feasible to iterate over all magmas of order up to 4 by a brute force approach.

Some other magmas have been used to establish counterexamples:

- The cyclic group $\mathbb{Z}/6\mathbb{Z}$ with the addition law.
- The natural numbers with law $x \diamond y = x + 1$.
- The natural numbers with law $x \diamond y = xy + 1$.
- The reals with $x \diamond y = (x + y)/2$.
- The natural numbers with $x \diamond y$ equal to x when $x = y$ and $x + 1$ otherwise.
- The set of strings with $x \diamond y$ equal to y when $x = y$ or when x ends with yyy, or xy otherwise (see this Zulip thread).
- Vector spaces $\mathbb{F}_2^n$ over $\mathbb{F}_2$, which obey Theorem 2.32 (and hence all the subsequent laws mentioned in Theorem 5.6).

- Knuth's construction [7] of a central groupoid (Theorem 2.23) as follows. Let S be a (finite) set with a distinguished element 0, and a binary operation $*$ such that $x*0 = 0$ and $0*x = x$ for all x, and for each x, y there is a unique z with $x * z = y$. One can then define a central groupoid on $S \times S$ by defining $(a, b) \diamond (c, d)$ to equal (b, c) if $c, d \neq 0$; (b, e) if $b * e = c$ is non-zero and $d = 0$; and $(a * b, 0)$ if $c = 0$. One such example in [7] is when $S = \{0, 1, 2\}$ with $1 * 1 = 2 * 1 = 2$ and $1 * 2 = 2 * 2 = 1$.
- Cancellative magmas of orders 7 to 9, found by hand-guided search using various solvers.
- Two magmas of cardinality 8 were constructed by Z3.
- A large number of ad-hoc finite magmas were constructed using the Vampire theorem prover. In some cases, inputting theoretical information is useful: see this discussion.
- Linear magmas $x \diamond y = ax + by$ on various fields, such as $\mathbb{F}_p$ for small primes p, have also been used to establish counterexamples. One such choice is $(p, a, b) = (11, 1, 7)$. See this discussion. For a noncommutative example, see this discussion. For a more systematic exploration of the implications that can be obtained by both commutative and noncommutative linear models, see this discussion.
- A variation of the translation-invariant magma construction which resolved the Asterix / Obelix anti-implication is used to show that Theorem 2.36 does not imply Theorem 2.34.

Chapter 7

Infinite magma constructions

The need to construct infinite magmas primarily arises in the context of *Austin laws* and *Austin pairs*. An Austin law admits infinite models but no nontrivial finite ones, while an Austin pair consists of laws P and Q such that every finite model obeying the law P also obeys Q, but some infinite magma obeys P without also obeying Q. Examples are given in Chapter 3.

Here we survey techniques for constructing infinite magmas that serve as counterexamples for implications between laws. Many of the techniques presented trace their origins to the first analysis of the Asterix equation (Theorem 2.22), reviewed in Section 7.2.

7.1 Translation-invariant magmas

A *translation-invariant magma* is a magma whose carrier G is an Abelian group $G = (G, +)$, and whose magma operation takes the form

$$y \diamond x = x + f(x - y)$$

for some function $f : G \to G$. Thus the translations on G become magma isomorphisms.

Example 1. *A magma G satisfying the left (Theorem 2.4) or right (Theorem 2.5) absorption laws is translation-invariant. Equip the carrier G with an Abelian group structure $(G, +, -, 0)$ and define $f : G \to G$ as either $f(x) = -x$ or $f(x) = 0$.*

Example 2. *Linear magmas $x \diamond y = ax + by$ on a field $(\mathbb{F}, +, -, \cdot, 0, 1)$ are translation-invariant if $a + b = 1$, since $(\mathbb{F}, +, -, 0)$ forms an Abelian group, and one can set $f(x) = -ax$.*

Note that if an example of the latter sort suffices to refute the implication between P and Q then by the Lefschetz principle one can construct a counterexample where the field $\mathbb{F}$ is finite. Consequently, P and Q cannot constitute an Austin pair. However, these linear magmas can still serve as starting points for the *modified translation-invariant* models studied in Section 7.5.

7.2 The Asterix equation

Over translation-invariant magmas, equational laws simplify to univariate functional equations.

For instance, writing $x = y + h$, we have

$$y \diamond x = x + f(h)$$

$$x \diamond (y \diamond x) = x + f(h) + f^2(h)$$
$$y \diamond (x \diamond (y \diamond x)) = x + f(h) + f^2(h) + f(h + f(h) + f^2(h))$$

where $f^2 = f \circ f$, so the Asterix equation (Theorem 2.22) for such magmas simplifies to the univariant functional equation

$$f(h) + f^2(h) + f(h + f(h) + f^2(h)) = 0 \tag{7.1}$$

for $h \in G$.

This equation has some degenerate solutions, for instance we can take $f(h) = c$ for any constant c of order 3 in G. It is challenging to construct more interesting solutions to this equation; however, we can do this if $G = \mathbb{Z}$ by a greedy algorithm. We need the following technical definition.

Definition 7.1. A *partial solution* (E_0, E_1, E_2, f) to Equation (7.1) consists of nested finite sets

$$E_0 \subset E_1 \subset E_2 \subset \mathbb{Z}$$

together with a function $f : E_1 \to E_2$ with the following properties:

(a) If $h \in E_0$, then $f(h) \in E_1$, so that $f^2(h)$ is well-defined as an element of E_2; furthermore, $h + f(h) + f^2(h)$ lies in E_1, so that the left-hand side of Equation (7.1) makes sense; and Equation (7.1) holds.

(b) The function f is a bijection from $E_1 \backslash E_0$ to $E_2 \backslash E_1$.

We partially order the space of partial solutions to Equation (7.1) by writing $(E_0, E_1, E_2, f) \leq (E_0', E_1', E_2', f')$ if the following properties hold:

- $E_i \subset E_i'$ for $i = 0, 1, 2$.
- f agrees with f' on E_0.

When this occurs we say that the partial solution (E_0', E_1', E_2', f') *extends* the partial solution (E_0, E_1, E_2, f).

We define the *empty partial solution* (E_0, E_1, E_2, f) by setting $E_0 = E_1 = E_2$ to be the empty set, and f to be the empty function; it is the minimal element of the above partial order.

We have the following iterative construction, that lets us add arbitrary elements to the core domain E_0:

Lemma 7.2 (Enlarging a partial solution)**.** *Let (E_0, E_1, E_2, f) be a partial solution to Equation (7.1), and let h be an element of $\mathbb{Z}$ that does not lie in E_0. Then there exists a partial solution (E_0', E_1', E_2', f') to Equation (7.1) that extends (E_0, E_1, E_2, f), such that $h \in E_0'$.*

Proof. Because f maps $E_1 \backslash E_0$ bijectively to $E_2 \backslash E_1$, there are three cases:

- h is equal to an element h_0 of $G \backslash E_2$.
- h is equal to an element h_0 of $E_1 \backslash E_0$.
- h is equal to $h_1 = f(h_0)$ for some $h_0 \in E_1 \backslash E_0$, so that $h_1 \in E_2 \backslash E_1$.

We deal with these three cases in turn.

First suppose that $h = h_0 \in G \backslash E_2$. We perform the following construction.

- Choose an element $h_1 \in \mathbb{Z}$ that does not lie in $E_2 \cup \{h_0\}$; this is possible because E_2 is finite.
- Choose an element $h_2 \in \mathbb{Z}$ such that $h_2, h_0 + h_1 + h_2$, and $-h_1 - h_2$ are all distinct from each other and lie outside of $E_2 \cup \{h_0, h_1\}$; this is possible because E_2 is finite.
- Promote h_0 to E_0, promote $h_1, h_0 + h_1 + h_2$ to E_1, and promote $h_2, -h_1 - h_2$ to E_2, creating new sets

$$\begin{aligned} E_0' &:= E_0 \cup \{h_0\} \\ E_1' &:= E_1 \cup \{h_0, h_1, h_0 + h_1 + h_2\} \\ E_2' &:= E_2 \cup \{h_0, h_1, h_0 + h_1 + h_2, h_2, -h_1 - h_2\}. \end{aligned}$$

  Clearly we still have nested finite sets $E_0' \subset E_1' \subset E_2'$.
- Extend $f : E_1 \to E_0$ to a function $f' : E_1' \to E_0'$ by defining

$$\begin{aligned} f'(h_0) &:= h_1 \\ f'(h_1) &:= h_2 \\ f'(h_0 + h_1 + h_2) &:= -h_1 - h_2 \end{aligned}$$

  while keeping $f'(h) = f(h)$ for all $h \in E_1$.

It is then a routine matter to verify that (E_0', E_1', E_2', f') is a partial solution to Equation (7.1) extending (E_0, E_1, E_2, f) and that E_0' contains h_0, as required.

Now suppose that $h = h_0 \in E_1 \backslash E_0$, then the quantity $h_1 := f(h_0)$ lies in $E_2 \backslash E_1$. We perform the following variant of the above construction:

- Choose an element $h_2 \in \mathbb{Z}$ such that $h_2, h_0 + h_1 + h_2$, and $-h_1 - h_2$ are all distinct and lie outside of E_2. This is possible because E_2 is finite.
- Promote h_0 to E_0, promote h_1 and $h_0 + h_1 + h_2$ to E_1, and promote $h_2, -h_1 - h_2$ to E_2, thus creating new sets

$$\begin{aligned} E_0' &:= E_0 \cup \{h_0\} \\ E_1' &:= E_1 \cup \{h_1, h_0 + h_1 + h_2\} \\ E_2' &:= E_2 \cup \{h_0 + h_1 + h_2, h_2, -h_1 - h_2\}. \end{aligned}$$

  Clearly we still have nested finite sets $E_0' \subset E_1' \subset E_2'$.
- Extend $f : E_1 \to E_0$ to a function $f' : E_1' \to E_0'$ by defining

$$\begin{aligned} f'(h_1) &:= h_2 \\ f'(h_0 + h_1 + h_2) &:= -h_1 - h_2 \end{aligned}$$

  while keeping $f'(h) = f(h)$ for all $h \in E_1$.

It is then a routine matter to verify that (E_0', E_1', E_2', f') is a partial solution to Equation (7.1) extending (E_0, E_1, E_2, f) and that E_0' contains h_0, as required.

Finally, suppose that $h = h_1 = f(h_0)$ for some $h_0 \in E_1 \backslash E_0$, so that $h_1 \in E_2 \backslash E_1$. Then we perform the following algorithm.

- Choose an element $h_2 \in \mathbb{Z}$ such that $h_2, h_0+h_1+h_2$, and $-h_1-h_2$ are all distinct and lie outside of E_2. This is possible because E_2 is finite.
- Choose an element $h_3 \in \mathbb{Z}$ such that $h_3, h_1+h_2+h_3$, and $-h_2-h_3$ are all distinct and lie outside of $E_2 \cup \{h_2, h_0+h_1+h_2, -h_1-h_2\}$. This is possible because E_2 is finite.
- Promote h_0, h_1 to E_0, promote $h_2, h_0+h_1+h_2, h_1+h_2+h_3$ to E_1, and promote $h_3, -h_1-h_2, -h_2-h_3$ to E_2, creating new sets

$$\begin{aligned} E_0' &:= E_0 \cup \{h_0, h_1\} \\ E_1' &:= E_1 \cup \{h_1, h_2, h_0+h_1+h_2, h_1+h_2+h_3\} \\ E_2' &:= E_2 \cup \{h_2, h_3, h_0+h_1+h_2, h_1+h_2+h_3, -h_1-h_2, -h_2-h_3\}. \end{aligned}$$

  Clearly we still have nested finite sets $E_0' \subset E_1' \subset E_2'$.
- Extend $f : E_1 \to E_0$ to a function $f' : E_1' \to E_0'$ by defining

$$\begin{aligned} f'(h_1) &:= h_2 \\ f'(h_0+h_1+h_2) &:= -h_1-h_2 f'(h_2) \qquad := h_3 \\ f'(h_1+h_2+h_3) &:= -h_2-h_3 \end{aligned}$$

  while keeping $f'(h) = f(h)$ for all $h \in E_1$.

It is then a routine matter to verify that (E_0', E_1', E_2', f') is a partial solution to Equation (7.1) extending (E_0, E_1, E_2, f) and that E_0' contains h_0, as required. □

Corollary 7.3. *Every partial solution (E_0, E_1, E_2, f) to Equation (7.1) can be extended to a full solution $\tilde{f} : \mathbb{Z} \to \mathbb{Z}$.*

Proof. If we arbitrarily well-order the integers, and iterate Theorem 7.2 to add the least element of $\mathbb{Z} \backslash E_0$ in this well-ordering to E_0, we obtain an increasing sequence $(E_0^{(n)}, E_1^{(n)}, E_2^{(n)}, f^{(n)})$ of partial solutions to Equation (7.1), where the $E_0^{(n)}$ exhaust $\mathbb{Z}$: $\bigcup_{n=1}^{\infty} E_0^{(n)} = \mathbb{Z}$. Taking limits, we obtain a full solution $\tilde{f}$. □

Corollary 7.4. *There exists a solution $f : \mathbb{Z} \to \mathbb{Z}$ to Equation (7.1) such that the map $h \mapsto h + f(h)$ is not injective.*

Proof. Select integers $h_0, h_1, h_2, h_0', h_1', h_2'$ such that the quantities

$$h_0, h_1, h_2, h_0+h_1+h_2, -h_1-h_2, h_0', h_1', h_2', h_0'+h_1'+h_2', -h_1'-h_2'$$

are all distinct, but such that

$$h_0 + h_1 = h_0' + h_1'$$

(there are many assignments of variables that accomplish this). Then set

$$\begin{aligned} E_0 &:= \{h_0, h_0'\} \\ E_1 &:= E_0 \cup \{h_1, h_1', h_0+h_1+h_2, h_0'+h_1'+h_2'\} \\ E_2 &:= E_2 \cup \{-h_1-h_2, -h_1'-h_2'\} \end{aligned}$$

and define $f : E_1 \to E_2$ by the formulae

$$\begin{aligned} f(h_0) &:= h_1 \\ f(h_1) &:= h_2 \\ f(h_0 + h_1 + h_2) &:= -h_1 - h_2 \\ f(h'_0) &:= h'_1 \\ f(h'_1) &:= h'_2 \\ f(h'_0 + h'_1 + h'_2) &:= -h'_1 - h'_2. \end{aligned}$$

One can then check that (E_0, E_1, E_2, f) is a partial solution to Equation (7.1), and by construction $h \mapsto h + f(h)$ is not injective on E_1. Using Theorem 7.2 to extend this partial solution to a full solution, we obtain the claim. □

Corollary 7.5 (Asterix does not imply Obelix)**.** *There exists a magma obeying the Asterix law (Theorem 2.22) with carrier $\mathbb{Z}$ such that the left-multiplication maps $L_y : x \mapsto y \diamond x$ are not injective for any $y \in \mathbb{Z}$. In particular, it does not obey the Obelix law (Theorem 2.31).*

Proof. Note that $L_y(y + h) = y + h + f(h)$, so the injectivity of the left-multiplication maps is equivalent to the injectivity of the map $h \mapsto h + f(h)$. The non-injectivity then follows from Theorem 7.4. Note that the Obelix law clearly expresses x as a function of y and $L_y x = y \diamond x$, forcing injectivity of left-multiplication, so the Obelix law fails. □

On the other hand, for finite magmas the situation is different:

Proposition 7.6 (Asterix implies Obelix for finite magmas)**.** *Any finite magma obeying the Asterix law (Theorem 2.22) also is left-cancellative and obeys the Obelix law (Theorem 2.31).*

Proof. From Theorem 2.22 we see the map $z \mapsto y \diamond z$ is surjective, hence injective on a finite magma; thus the magma is left-cancellative. Replacing x by $y \diamond x$ in this law, we see that

$$y \diamond x = y \diamond ((y \diamond x) \diamond (y \diamond (y \diamond x)));$$

using injectivity, we conclude

$$x = (y \diamond x) \diamond (y \diamond (y \diamond x))$$

which is Theorem 2.31. □

A very similar argument shows that a finite magma that obeys the Obelix law has $z \mapsto y \diamond z$ injective, hence surjective, and then obeys the Asterix law.

7.3 Obelix

Obelix magmas are those obeying equation 1491, Theorem 2.31:

$$x = (y \diamond x) \diamond (y \diamond (y \diamond x))$$

Obelix is not particularly *structurally* similar to an Asterix, besides their shared resistance to small counterexamples. A related set of ideas can be used to construct an Obelix that does not obey some given other equations. The common idea is to define the magma operation

$$x \diamond y = x + f(y - x) = x + f(h)$$

on some underlying Abelian group. For the case of Obelix, the resulting functional equation is

$$f(f^2(h) - f(h)) = h - f(h) \tag{7.2}$$

What differs is how we must proceed in order to satisfy this equation. We again start with a partial function f, picking some initial support that will suffice to invalidate the other equation we want to show a nonimplication for. We will progressively add more elements to the support (assuming our group is countable) until the function is total, and we will maintain some invariants:

Definition 7.7. A *partial solution* for an Obelix is a partial function $f : G \to G$ with the properties:

- f has finite domain.
- f is injective.
- f maps the identity (of G, so, 0) to the identity.
- If x is in the domain of f, and $f(x)$ is in the domain, then so is $f^2(x) - f(x)$.
- If x is in the domain of f, and $f(x)$ is in the domain, then $f(f^2(x) - f(x)) = f(x) - x$. This is well-defined by property (4).
- The function $x - f(x)$, which is defined on the same domain as f, is injective.
- If x is in the domain of f but $f(x)$ isn't in the domain, then $x - f(x)$ isn't in the domain or image of f.

It's easiest to work over the group of finitely supported functions from $\mathbb{N}$ (or any other countable set) to $\mathbb{Z}$. When picking fresh elements, it's important not only to take something outside of the group closure of the elements already in f, but actually out of their $\mathbb{Q}$-span, because we need guarantees that the fresh element g doesn't obey relations like $2g = x$ as well.

Any partial solution can be extended to a complete solution.

Lemma 7.8. *For any $E \in \mathcal{E}$ and any $a \in G$, there is an extension $E \subseteq E' \in \mathcal{E}$ where the functional equation holds for a.*

Proof. **Case 1**: Assume $(a, b) \in E$ for some $b \in G$.

If $b \in \mathrm{dom}(E)$, then by condition (4) we are already done. So reduce to the case when $b \notin \mathrm{dom}(E)$. In particular, by (2) and (3) we know $a, b \neq 1$, and also by (6) we know that $ab^{-1} \notin \mathrm{dom}(E) \cup \mathrm{im}(E)$ (and is not 1).

Take c to be a generator of G not appearing in the reduced form of any entry in E, and set $E' := E \cup \{(b, c), (cb^{-1}, ab^{-1}\}$. Conditions (1), (3), and (5) are immediate. Condition (2) is also clear, where injectivity needs $ab^{-1} \notin \mathrm{im}(E)$. Condition (4) is also easy to check, using the fact that E is injective, $cb^{-1} \neq c$, and $ab^{-1} \notin \mathrm{dom}(E)$.

Finally, for condition (6), a finite check works. The main case is checking that $ca^{-1} \notin \mathrm{dom}(E') \cup \mathrm{im}(E')$. This is clear since $a \neq 1$ and $a \neq b$ (by condition (5) for E). One should also note that by condition (5) (and the fact that E is a function), there is no pair $(x, y) \in E$ with $(x, y) \neq (a, b)$ and $xy^{-1} = ab^{-1}$, so we don't ruin condition (6) for pairs already in E.

Case 2: Assume $a \notin \mathrm{dom}(E)$. If $(x, a) \in E$ for some (unique by (2)) $x \in G$, then applying Case 1 to x, we reduce to the case when $a \in \mathrm{dom}(E)$.

Thus, we may consider the case when $a \notin \mathrm{dom}(E) \cup \mathrm{im}(E)$. If $(x, y) \in E$ with $xy^{-1} = a$, then by applying Case 1 to x, we get $a \in \mathrm{im}(E)$, and reduce to a previously considered case. So,

we may assume there is no such pair (x, y). Fixing b to be a generator of G not appearing in the reduced forms for the entries in E, nor in a, then after passing to $E \cup \{(a, b)\} \in \mathcal{E}$ we again reduce to Case 1. □

The actual mechanical proof requires checking roughly a few dozen statements of the form "the fresh element is not related linearly to the existing elements". Each is individually obvious, and easily discharged.

By picking an appropriate partial solution, we can then show that there are Obelix magmas that are not Asterix.

Corollary 7.9. *There is an Obelix magma that is not Asterix (equation 65).*

Proof. This requires picking an initial set that still obeys the correct initial closure properties. Letting x_1, x_2, x_3 and x_4 be independent elements, then taking the function

$$\{(0, 0), (x_1, x_2), (x_2 - x_1, x_3), (x_1 + x_3, x_4)\}$$

already has elements that contradict the Asterix equation, and it's a valid partial solution. By extending it, we can get an Obelix that does not obey the Asterix equation. □

7.4 Greedy algorithm constructions

In Section 7.2 a magma obeying one law and refuting another was obtained by using the fact that over translation-invariant magmas, equational laws simplify to univariate functional equations, and solving the resulting equation using a greedy algorithm.

One way to construct infinite magmas obeying specific laws is via a greedy algorithm construction not on a one-variable functional equation, but on the operation table of the magma itself.

Here, it is best to work with *partially defined magma operations* on some carrier G. These can be interpreted as ternary relations $R(x, y, z)$ in three variables $x, y, z \in G$ which pass the following "vertical line test":

(VLT) If $R(x, y, z)$ and $R(x, y, z')$ both hold for some $x, y, z, z' \in G$, then $z = z'$.

Such an operation is then associated (via a one-to-one correspondence) to a partially defined operation $\diamond : S \to G$ for some $S \subset G \times G$, with $R(x, y, z)$ holding if and only if $x \diamond y$ is well-defined (i.e., $(x, y) \in S$) and equal to z. By abuse of notation, we shall also refer to R as a partially defined magma operation. Genuine magmas then correspond to the special case where $S = G \times G$, that is to say $x \diamond y$ is well-defined for all $x, y \in G$.

Given a word $w(x_1, \ldots, x_n)$ in variables $x_1, \ldots, x_n$ (so w is an element of the free magma on n generators), we can say that $w(x_1, \ldots, x_n)$ is *well-defined* with respect to a partially defined magma operation R if it can be fully evaluated using R. For instance, the word $(x \diamond y) \diamond z$ is well-defined if there exists $w, u \in G$ such that $R(x, y, w)$ and $R(w, z, u)$ both hold, in which case $(x \diamond y) \diamond z$ evaluates to u. Note from the axiom (VLT) that this evaluation is unique, if it exists. Of course, in a genuine magma, all expressions are well-defined. We say that an expression $w(x_1, \ldots, x_n)$ is *almost well-defined* if all strict subexpressions of w are well-defined. For instance, $(x \diamond y) \diamond z$ is almost well-defined if there exists $w \in G$ such that $R(x, y, w)$ holds.

An equational law $w_1 \simeq w_2$ involving some variables $x_1, \ldots, x_n$ is said to be *locally obeyed* by R if, whenever $w_1(x_1, \ldots, x_n)$, $w_2(x_1, \ldots, x_n)$ are almost well-defined, and one of the two expressions is well-defined and evaluates to some output y, then the other expression is also well-defined and evaluates to the same output y. For instance, in order for R to locally obey the associative law $(x \diamond y) \diamond z = x \diamond (y \diamond z)$ (Theorem 2.46), we require the following two axioms:

(4512-1) If $R(x,y,w)$, $R(w,z,u)$, and $R(y,z,v)$, then $R(x,v,u)$.

(4512-2) If $R(y,z,w)$, $R(x,w,u)$, and $R(x,y,v)$, then $R(v,z,u)$.

If a law involves a single variable on one side, then we only need one axiom. For instance, the Asterix law (Theorem 2.22) is locally obeyed by R if and only if the following axiom holds:

(65) If $R(y,x,z)$ and $R(x,z,u)$, then $R(y,u,x)$.

Note that if the relation R is associated to a genuine magma operation $\diamond$, then it locally obeys a law $w_1 \simeq w_2$ if and only if the magma operation $\diamond$ obeys the law $w_1 \simeq w_2$. For instance, the relation R associated to a globally defined magma operation $\diamond$ obeys (4512-1) and (4512-2) if and only if the magma is associative.

More generally, one can ask for a ternary relation R to obey some theory Γ of universal laws, using the language of one ternary relation R, the equality symbol $=$, and possibly some constants (we will shortly introduce three constants a,b,c for this purpose).

Suppose we have a relation R obeying some theory Γ (for instance, (VLT) together with (65)), but which is only finitely supported (there are only finitely many triples (x,y,z) for which $R(x,y,z)$ holds). Then one can find $a,b \in G$ such that $a \diamond b$ is currently undefined. If the carrier G is infinite (e.g., if $G = \mathbb{N}$), one can then find another element c which is *novel*: it is not equal to a,b, or any of the x,y,z for which $R(x,y,z)$ hold. In other words, the relation R and the constants a,b,c obey the following additional axioms:

(novel-1) $c \neq a$ and $c \neq b$.

(novel-2) If $R(x,y,z)$, then $c \neq x$, $c \neq y$, and $c \neq z$.

(undefined) $R(a,b,x)$ does not hold for any x.

Let us say that a theory Γ is *greedily extensible* if, whenever R is a finitely supported ternary relation obeying Γ, and a,b,c are constants obeying (novel-1), (novel-2), (undefined), then there exists an extension R' of R, thus

(extend) $R(x,y,z) \implies R'(x,y,z)$ for all x,y,z,

which is also finitely supported and obeys Γ, and which also obeys the additional axiom

(define) $R'(a,b,c)$.

Informally, R' is formed from R by "forcing" $a \diamond b = c$ and then adding other axioms as needed. (Indeed, our construction here can be viewed as a simple analogue of the forcing construction in set theory.)

Observe that if a theory Γ containing (VLT) is greedily extensible, then any finitely supported ternary relation R obeying Γ on a countably infinite carrier G can be extended to a globally defined relation obeying Γ, by iteratively selecting the first (a,b) (in some fixed enumeration of $G \times G$) for which $a \diamond b$ is undefined, and then selecting a novel element c to define as $a \diamond b$, and applying the greedily extensible property, and then taking a direct limit of the countable sequence of relations thus produced. This gives a flexible way to construct magmas that obey a given theory Γ, but which violate some other law $w_1 \simeq w_2$, as the task then reduces to just finding a partial solution R to Γ and some constants $x_1, \ldots, x_n$ for which the expressions $w_1(x_1,\ldots,x_n), w_2(x_1,\ldots,x_n)$ are already well-defined, but not equal to each other.

Unfortunately, most theories are not greedily extensible without further modification. Consider for instance the theory Γ consisting of (VLT) and the Asterix law (65). Given a,b,c and a finitely supported R obeying Γ as well as (novel-1), (novel-2), (undefined), we would like to

construct a finitely supported R' obeying Γ, (extend), (define). The naive guess would just be to take the minimal construction

$$R'(x,y,z) \text{ iff } R(x,y,z) \text{ or } (x,y,z) = (a,b,c).$$

This can work, but there is an obstruction: if $R(w,a,b)$ for some w, then (65) forces $R'(w,c,a)$. So one would have to enlarge the definition of $R'(x,y,z)$, to hold true if one of the following statements holds:

- $R(x,y,z)$ holds.
- $(x,y,z) = (a,b,c)$.
- $(x,y,z) = (w,c,a)$ for some w with $R(w,a,b)$.

This works more often, but there is then a second obstruction: if $R(b,a,b)$, then we now have $R'(b,c,a)$, and (65) then forces $R'(a,a,b)$. So we need to add a fourth item to the above list defining R':

- $(x,y,z) = (a,a,b)$, assuming $R(b,a,b)$ holds.

But now if we had $R(a,a,z)$ for some $z \neq b$, this would then create a violation of (VLT). To fix this, we need to extend Γ by adding an additional axiom:

- (65') If $R(y,x,y)$, then $R(x,x,y)$.

With this modification to Γ, if we run the above analysis, we now see that if $R(b,a,b)$ hold (so that $R(a,a,b)$ also holds), then (65) will force $R'(a,c,a)$, $R'(b,c,a)$, and $R'(c,c,a)$. So now the modified definition of R' is that $R'(x,y,z)$ holds if one of the following statements holds:

- $R(x,y,z)$ holds.
- $(x,y,z) = (a,b,c)$.
- $(x,y,z) = (w,c,a)$ for some w with $R(w,a,b)$.
- $(x,y,z) = (a,c,a)$, (b,c,a), or (c,c,a), assuming $R(b,a,b)$ holds.

One can then finally (for instance, with the assistance of a automated theorem prover) verify that if R is finitely supported and obeys $\Gamma = (VLT) + (65) + (65')$ and a,b,c obey (novel-1), (novel-2), (undefined), then the R' defined above is also finitely supported and obeys Γ, (extend), (define). This shows that the theory Γ is greedily extensible.

Using this, one can for instance find a magma obeying Theorem 2.22 that fails the left-cancellative property

$$y \diamond x = y \diamond x' \implies x = x'$$

or in terms of ternary relations

$$R(y,x,z) \text{ and } R(y,x',z) \implies x = x' \tag{7.3}$$

simply by starting with a partial solution, say on the natural numbers in which (e.g.) $R(1,2,0)$, $R(1,3,0)$ are the only situations in which R holds. One can easily verify that this obeys (VLT) and (65), (65'), but not Equation (7.3), and so any magma constructed by the above greedy construction will not be left-cancellative. Since the Obelix law Theorem 2.31 forces left-cancellativity, this gives an alternate proof of Theorem 7.5.

7.4.1 Equation 1722

We illustrate the above technique by constructing solutions to equation 1722,

$$(y \diamond y) \diamond ((x \diamond y) \diamond y) = x. \tag{7.4}$$

We abbreviate $Sy := y \diamond y$.

Define a *partial solution* to be a partial function $\diamond : E \to \mathbb{N}$ on some finite subset E of $\mathbb{N} \times \mathbb{N}$ (which one can also think of as a finitely supported ternary relation $R(x, y, z)$ obeying VLT) obeying the following axioms:

- (Law 1) If $(x \diamond y) \diamond y$ is defined, then $Sy \diamond ((x \diamond y) \diamond y)$ is defined and equal to x.
- (Law 2) If If $x \diamond y$ and $z \diamond y$ are defined and equal to each other, then $x = z$.
- (Law 3) If Sx is defined, then $(Sx \diamond x) \diamond x$ is defined.
- (Law 4) If there exists a z such that $z \diamond x = x$ then $x \diamond x$ is defined.

Lemma 7.10 (1722 extension)**.** *Suppose that $\diamond$ is a partial solution, and $a \diamond b$ is currently undefined. Then there exists an extension $\diamond'$ of $\diamond$ for which $a \diamond' b$ is defined.*

Proof. Suppose first that $b = a$, so $a \diamond a$ is undefined, then by Law 4 we have $d \diamond a \neq a$ for all d with $d \diamond a$ defined. Set $a_0 = a$ and find nine distinct elements $a_1, a_2, a_3, a_4, b_0, b_1, b_2, b_3, b_4$ not previously appearing in the domain or range of $\diamond$. Extend the indices periodically by setting $a_{i+4} = a_i, b_{i+4} = b_i$ for $i \geq 1$, and define $a_i \diamond' a_i = a_{i+1}$ (so $a_i = S^i a$), $a_{i+1} \diamond' a_i = b_i$, $b_i \diamond' a_i = a_{i+2}$, $a_{i+3} \diamond' a_{i+1} = a_{i+1}$, $a_{i+1} \diamond' a_{i+2} = a_{i+1}$, $a_{i+1} \diamond' b_i = a_i$. We also define $x \diamond' y = x \diamond y$ whenever the right-hand side is defined. It is easy to see that laws 2,3,4 are preserved (though for law 2 note that we have not defined $a_2 \diamond' a_0$ due to the way indices are extended). Now we case check Law 1.

- Case 1. y is fresh, that is $y \in \{a_1, a_2, a_3, a_4, b_0, b_1, b_2, b_3, b_4\}$. If $x \diamond' y$ is not defined, we are done, so assume this is so. In particular, $x \in \{a_1, a_2, a_3, a_4, b_0, b_1, b_2, b_3, b_4\}$. If $x, y \in \{a_1, a_2, a_3, a_4\}$ we are done by construction. If $x = b_i$ for some i, then $y = a_i$ and we are again done by construction. Finally, if $y = b_i$ for some i, then $x = a_{i+1}$ and $(x \diamond' y) \diamond' y$ is undefined.
- Case 2. x is fresh, that is $x \in \{a_1, a_2, a_3, a_4, b_0, b_1, b_2, b_3, b_4\}$. If we are not in Case 1 and $x \diamond' y$ is defined, we must have $y = a_0$ and $x \in \{a_1, b_0\}$. The case $x = a_1$ holds by construction, and the case $x = b_0$ holds as $a_2 \diamond' a_0$ is not defined.
- Case 3. $x, y \notin \{a_1, a_2, a_3, a_4, b_0, b_1, b_2, b_3, b_4\}$ and $x \diamond y$ was undefined. Then $x \diamond' y$ is undefined unless $x = y = a_0$, in which case Law 1 holds by construction.
- Case 4. $x, y \notin \{a_1, a_2, a_3, a_4, b_0, b_1, b_2, b_3, b_4\}$, $x \diamond y$ was defined, and $(x \diamond y) \diamond y$ was not defined. Then $(x \diamond' y) \diamond' y$ is undefined unless $(x \diamond y) = a = y$, but this is impossible by Law 4 as already observed.
- Case 5. $x, y \notin \{a_1, a_2, a_3, a_4, b_0, b_1, b_2, b_3, b_4\}$ and $x \diamond y$ and $(x \diamond y) \diamond y$ were defined. Then the claim follows from Law 1 applied to $\diamond$.

Now suppose that $a \diamond b$ is undefined for some $a \neq b$. By applying the previous construction, we may assume without loss of generality that Sb is defined. We may assume that $a \diamond b$ remains undefined after doing so, since we are done otherwise. By Law 3, $a \neq Sb \diamond b$. By Law 2, we have

$d \diamond b = a$ for at most one d, which is necessarily different from Sb. Choose a c not previously appearing in the domain or range of $\diamond$, and set $a \diamond' b = c$. If a d exists as before, we additionally set $Sb \diamond' c = d$. Finally we define $x \diamond' y = x \diamond y$ whenever the right-hand side is defined. It is again routine to check that $\diamond'$ obeys Laws 2,3,4. Now we case check Law 1.

- Case 1. $x = c$ or $x \diamond' y = c$. Not possible since no left multiplication by c is defined.
- Case 2. $y = c$. This would force $x = Sb$ and $d = Sb$, but this is not possible since d is different from Sb.
- Case 3: $(x \diamond' y) \diamond' y = c$. This forces $x = d$ and $y = b$, and the claim follows from construction.
- Case 4: None of the terms in $(x \diamond' y) \diamond' y$ are equal to c. Then the claim follows from Law 1 applied to $\diamond$.

□

By the greedy algorithm, this implies that any partial solution can be extended to a 1722 magma on $\mathbb{N}$. We can now refute the implication to equation 1832

$$x = (x \diamond Sx) \diamond Sx,$$

equation 2644

$$x = S^2 x \diamond x,$$

and equation 3050,

$$x = ((Sx \diamond x) \diamond x) \diamond x$$

by using the partial solution

$$0 \diamond 0 = 1, 0 \diamond 1 = 2, 1 \diamond 0 = 2, 1 \diamond 1 = 3, 1 \diamond 2 = 0, 1 \diamond 3 = 1, 1 \diamond 4 = 2$$

$$2 \diamond 0 = 3, 2 \diamond 1 = 4, 3 \diamond 0 = 4, 3 \diamond 1 = 1, 3 \diamond 3 = 3, 3 \diamond 4 = 0$$

which violates all three equations at $x = 0$.

7.4.2 Equation 713

Similar arguments can actually handle 713: $x = y \diamond (y \diamond ((y \diamond x) \diamond x))$. Here, the laws defining a partial solution are

- (Law 1) If $(y \diamond x) \diamond x$ is defined, then $y \diamond (y \diamond ((y \diamond x) \diamond x))$ is defined and equal to x.
- (Law 2) $x \diamond y \neq y$ for all x, y.
- (Law 3) If Sx is defined, then so is $Sx \diamond x$.

Lemma 7.11 (713 extension)**.** *Suppose that $\diamond$ is a partial solution, and $a \diamond b$ is currently undefined. Then there exists an extension $\diamond'$ of $\diamond$ for which $a \diamond' b$ is defined.*

Proof. First suppose that $a \diamond a$ is not defined. Set $a_0 := a$ and select three new elements a_1, a_2, a_3. Define $a_0 \diamond a_0 = a_1$, $a_1 \diamond a_0 = a_2$, $a_0 \diamond a_2 = a_3$, $a_0 \diamond a_1 = a_3$, $a_0 \diamond a_3 = a_0$. It is a routine but tedious matter to check that Laws 1,2,3 are preserved by these operations. (The trickiest case is the $x = a_0$ case of Law 1; here we need Law 2 to prevent $y \diamond a_0$ from equalling a_0.)

Now suppose that $a \diamond b$ is undefined for some $a \neq b$. Let $d_1, d_2, \ldots, d_n$ be all the elements with $d_i \diamond b = a$. Note from Law 3 that none of the d_i can be equal to b. Choose a new element c, as well as c_i for each d_i, and set $a \diamond b = c$, $d_i \diamond c = c_i$, and $d_i \diamond c_i = b$. It is easy to see that this preserves Laws 2,3. For Law 1 ,we do the usual case analysis:

- Case 1: $y = c$, $y = c_i$, $y \diamond x = c$, or $y \diamond x = c_i$. This case cannot occur because we have not defined left multiplication with c or c_i.
- Case 2: $x = c$ or $x = c_i$. Because $d_i \neq b$, it is easy to see that $(y \diamond x) \diamond x$ is not defined for any x.
- Case 3: $(y \diamond x) \diamond x = c$ or $(y \diamond x) \diamond x = c_i$. This is only possible if $x = b$ and $y = d_j$ for some j, and the claim then follows from construction.
- Case 4: None of the terms in $(y \diamond x) \diamond x$ are equal to c or c_i. This follows from the previous seed.

□

One can now refute the implications of the equations $x = x \diamond ((x \diamond x) \diamond (x \diamond x))$ (817), $x = (x \diamond x) \diamond (x \diamond (x \diamond x))$ (1426), $x \diamond x = (x \diamond (x \diamond x)) \diamond x$ (3862), $x \diamond x = ((x \diamond x) \diamond x) \diamond x$ (4065) by using the partial solution

$$0 \diamond 0 = 1, 0 \diamond 1 = 3, 0 \diamond 2 = 3, 0 \diamond 3 = 0$$

$$1 \diamond 0 = 2, 1 \diamond 1 = 0, 1 \diamond 2 = 1, 1 \diamond 3 = 2, 1 \diamond 4 = 3$$

$$2 \diamond 0 = 2, 2 \diamond 2 = 4, 2 \diamond 4 = 0$$

$$4 \diamond 1 = 2, 4 \diamond 2 = 4, 4 \diamond 3 = 2, 4 \diamond 4 = 1.$$

which violates 3862 at $x = 2$ and the other three laws at $x = 0$.

7.4.3 Equation 1289

For $x = y \diamond (((x \diamond y) \diamond y) \diamond y)$ (1289), one can similarly argue using the rules

- (Law 1) If $((x \diamond y) \diamond y) \diamond y$ is already defined, then $y \diamond (((x \diamond y) \diamond y) \diamond y)$ is also defined and equals x.
- (Law 2) R_x is injective for all x currently in the table.
- (Law 3) $x \diamond x = x$ for all x currently in the table.

Lemma 7.12 (1289 extension)**.** *Suppose that $\diamond$ is a partial solution, and $a \diamond b$ is currently undefined. Then there exists an extension $\diamond'$ of $\diamond$ for which $a \diamond' b$ is defined.*

Proof. If $a \diamond b$ is currently undefined, introduce a new element c and define $a \diamond b = c$ and $c \diamond c = c$. If furthermore $a = (d \diamond b) \diamond b$ for some d, then also define $b \diamond c = d$ (This last step is well defined by injectivity of R_b).

We now check that the three axioms still hold. Law 3 is obvious, law 2 follows since $d \neq c$. For law 1, we first make the observation that $a \neq b$, for otherwise $a \diamond b$ would have been defined. This has the consequence that if d exists, then $d \neq b$, for otherwise $a = (b \diamond b) \diamond b = b$. In particular, the product $d \diamond c$ remains undefined after running the algorithm once.

We now work by cases on the values of the variables x, y appearing in law 1:

- Case 1: $y = c$. In this case, for the product $x \diamond y$ to be defined, we require $x = b$ or $x = c$. In the former case either $b \diamond c$ or $(b \diamond c) \diamond c = d \diamond c$ is not defined. In the latter case, law 1 holds as c is idempotent.

- Case 2: $y = b$. For $((x \diamond b) \diamond b) \diamond b$ to be defined now but not have been defined before, we require one of $x = a, (x \diamond b) = a, ((x \diamond b) \diamond b) = a$. The first two cases are eliminated as $c \diamond b$ is not yet defined. The last case holds as then d exists and equals x, so $b \diamond (((x \diamond b) \diamond b) \diamond b) = b \diamond (a \diamond b) = b \diamond c = x$.
- Case 3: $y \neq c, y \neq b$. We have introduced no new products with a right-hand side other than c or b, so if $((x \diamond y) \diamond y) \diamond y$ was undefined before it remains undefined now.

□

To refute $x \diamond (y \diamond x) = (x \diamond y) \diamond x$ (4435) and $x = (((y \diamond x) \diamond y) \diamond y) \diamond y$ (3316) we use the partial solution

$$0 \diamond 0 = 0; 0 \diamond 1 = 2; 0 \diamond 2 = 1; 0 \diamond 4 = 1$$

$$1 \diamond 0 = 2; 1 \diamond 1 = 1$$

$$2 \diamond 0 = 3; 2 \diamond 2 = 2$$

$$3 \diamond 0 = 4; 3 \diamond 3 = 3$$

$$4 \diamond 4 = 4$$

which violates 4435 at $(x, y) = (0, 1)$ and 3116 at $(x, y) = (2, 0)$.

7.4.4 Equation 73

For $x = y \diamond (y \diamond (x \diamond y))$ (73), we argue similarly, now with laws

- Law 1. If $y \diamond (x \diamond y)$ is defined, then $y \diamond (y \diamond (x \diamond y))$ is defined and equal to x.
- Law 2. R_y is injective for all y currently in the table.
- Law 3. $x \diamond y \neq y$ for all x, y currently in the table.

Lemma 7.13 (73 extension)**.** *Suppose that $\diamond$ is a partial solution, and $a \diamond b$ is currently undefined. Then there exists an extension $\diamond'$ of $\diamond$ for which $a \diamond' b$ is defined.*

Proof. If $a \diamond b$ is undefined, set it equal to a new element c. If we also have $b = d \diamond a$ for some d (unique by Law 2, and only possible for $a \neq b$ by Law 3), set $a \diamond c = d$.

It is obvious that Laws 2, 3 are preserved. Now we case check Law 1:

- Case 1: $x = c$ or $y = c$. Not possible since no left multiplication with c is defined.
- Case 2: $x \diamond y = c$. Only possible when $x = a$, $y = b$, but then $y \diamond (x \diamond y)$ is undefined since $y = b \neq a$ if d is defined.
- Case 3. $y \diamond (x \diamond y) = c$. Only possible when $y = a$ and $x = d$, and holds in this case.
- Case 4: $x, y, x \diamond y, y \diamond (x \diamond y) \neq c$: this case is already covered by the previous seed.

□

One can obtain various refutations by using the countermodels here.

7.4.5 Equation 63

For $x = y \diamond (x \diamond (x \diamond y))$ (63), we argue similarly, now with laws

- Law 1. If $x \diamond (x \diamond y)$ is defined, then $y \diamond (x \diamond (x \diamond y))$ is defined and equal to x.
- Law 2. If $x \diamond y = x \diamond z$ with y, z distinct, then $y \diamond x$ (if defined) is not equal to z or to $z \diamond x$ (if defined).
- Law 3: If $x \diamond x$ is defined, it is equal to x.
- Law 4: If $x \neq y$, then $x \diamond y$ is not equal to x.

Lemma 7.14 (63 extension)**.** *Suppose that $\diamond$ is a partial solution, and $a \diamond b$ is currently undefined. Then there exists an extension $\diamond'$ of $\diamond$ for which $a \diamond' b$ is defined.*

Proof. If $a = b$, set $a \diamond' a = a$. This clearly does not destroy Laws 3 or 4, and because of Law 4, Law 2 will also be retained. Finally, using Law 4, we can check that this addition does not break Law 1.

Now suppose $a \neq b$. Let $d_1, d_2, ..., d_n$ be all the elements with $b = a \diamond d_i$, and note from Law 3 and $a \neq b$ that we have the crucial inequality $d_i \neq a$ for all i. If $d_i \diamond a$ is defined, let $e_i = d_i \diamond a$. From Law 4 and $d_i \neq a$, we have $e_i \neq d_i$. From Law 2 and $a \diamond d_i = a \diamond d_j$, we further have $e_i \neq e_j$ and $e_i \neq d_j$ for $i \neq j$.

For the algorithm, we set $a \diamond' b = c$ for some new c, $d_i \diamond' c = a$, and $c \diamond' e_i = d_i$ (This is well defined as we have just argued $e_i \neq e_j$ for $i \neq j$).

This creates a new partial function. Law 2 is verified as follows: The case $x = c$ cannot occur because $c \diamond' e_i \neq c \diamond' e_j$ for $i \neq j$. If $y = c$, then $x = d_i$ for some i, but then $y \diamond' x = c \diamond' d_i$ is undefined as $d_i \neq e_j$, so this case is vacuous. If $z = c$ and $x, y \neq c$, then similarly $z \diamond' x$ is undefined, and $y \diamond' x$ is not equal to $c = z$, so we are ok in this case also.

Law 3 is clearly unaffected, and it is also straightforward to check that Law 4 is also not invalidated (here it is essential that $d_i \neq a$).

Now we verify Law 1.

- Case 1: $x = c$. Then for $x \diamond' y$ to be defined we must have $y = e_i$ for some i, but then $x \diamond' (x \diamond' y) = c \diamond' d_i$ is undefined as $d_i \neq e_j$ for all j.
- Case 2: $y = c$. Then for $x \diamond' y$ to be defined we must have $x = d_i$ for some i. Then $d_i \diamond' (d_i \diamond' c)$ is either undefined or is equal to e_i, in which case Law 1 holds as $c \diamond' e_i = d_i$.
- Case 3: $x \diamond' y = c$. Then $x = a$ and $y = b$. Since $d_i \neq a$ for all i, $x \diamond (x \diamond y)$ is undefined.
- Case 4: $x \diamond' (x \diamond' y) = c$. Then $x = a$ and $y = d_i$ for some i, and Law 1 holds as $d_i \diamond' c = a$.
- Case 5: None of $x, y, x \diamond' y, x \diamond' (x \diamond' y)$ are equal to c. Then this case is covered by the previous seed.

□

One can obtain various refutations by using the countermodels here.

7.4.6 Equation 1076

For $x = y \diamond ((x \diamond (x \diamond y)) \diamond y)$ (1076), we argue similarly. There are just two laws:

- Law 1. If $x \diamond (x \diamond y)$ is defined and equal to some z, then $y \diamond (z \diamond y)$ is defined and equal to x.
- Law 2. $x \diamond x$ is not equal to x.

Lemma 7.15 (1076 extension)**.** *Suppose that $\diamond$ is a partial solution, and $a \diamond b$ is currently undefined. Then there exists an extension $\diamond'$ of $\diamond$ for which $a \diamond' b$ is defined.*

Proof. Set $a \diamond' b = c$ for some new element c. If $d_1, d_2, ..., d_n$ are the elements for which $a \diamond d_i = b$, set $c \diamond' d_i = c'_i$ for some new element c'_i, and also set $d_i \diamond' c'_i = a$. If $d_i \diamond a$ is equal to some e_i, set $e_i \diamond' c'_i = c''_i$ and $c'_i \diamond' c''_i = d_i$, where c''_i is equal to a if $e_i = d_i$, or is some new element otherwise.

One can verify that no collisions are caused by this construction (this is why we have to take $c''_i = a$ when $e_i = d_i$), and that Law 2 is preserved.

We need to verify that these constructions preserve Law 1. There are several cases:

- $y = c$. Not possible since there are no right multiplications by c defined.
- $x = c$. Not possible since it forces $y = d_i$, $x \diamond y = c'_i$ for some i.
- $y = c'_i$, $x = d_i$. True by construction.
- $y = c'_i$, $x \neq d_i$. This forces $x = e_i \neq d_i$ and $x \diamond' y = c''_i$, but then $x \diamond' (x \diamond' y)$ is undefined.
- $x = c'_i$. Not possible because this forces $x \diamond' y = d_i$, and $x \diamond' (x \diamond' y)$ will be undefined. (Here we use the fact that $e_i = d_i$ can only occur when $d_i \neq a$, by Law 2.)
- $x = c''_i$ is new. Not possible as no left multiplications by c''_i are defined.
- $y = c''_i$ is new. This forces $x = c'_i$ and $x \diamond' y = d_i$, but then $x \diamond' (x \diamond' y)$ is undefined.
- x and y are not new and $x \diamond y$ was undefined. This requires $x = a, y = b$, but then $x \diamond' (x \diamond' y)$ is undefined since right multiplication by c is undefined.
- x, y are not new and $x \diamond y$ was defined, but $x \diamond (x \diamond y)$ was undefined. This requires $x = a$, $x \diamond y = b$, and hence $y = d_i$ for some i. The claim now follows from construction.
- x, y, are not new and $x \diamond y$, $x \diamond (x \diamond y)$ were defined. This then follows from the previous seed.

□

One can obtain various refutations by using the countermodels here.

7.4.7 Equation 3308

Similar: see here and here.

7.5 A survey of examples

7.5.1 Translation-invariant models

The implication between the laws Theorem 2.33 and Theorem 2.24 can be refuted by a translation-invariant magma on the integers. Define the function $f : \mathbb{Z} \to \mathbb{Z}$ by

$$f(x) = \begin{cases} -1 & \text{if } x > 0, \\ 0 & \text{if } x = 0, \\ 1 & \text{if } x < 0, \end{cases}$$

and consider the translation-invariant magma on $\mathbb{Z}$ given by the operation $x \diamond y = x + f(y - x)$.

The resulting magma satisfies Equation 1648: one can show this by a case analysis on $f(y-x)$. If $f(y - x) = 1$ we have $x \diamond y = x + f(y - x) = x + 1$, so

$$(x \diamond y) \diamond ((x \diamond y) \diamond y) = (x + 1) \diamond ((x + 1) \diamond y) = (x + 1) \diamond (x + 2) = (x + 1) - 1 = x.$$

Similar computations verify the other two cases.

However, setting $x = 0$ and $y = -1$ in Equation 206, we get

$$(x \diamond (x \diamond y)) \diamond y = (x \diamond 1) \diamond y = (-1) \diamond y = -1 \neq x$$

so the magma does not obey Theorem 2.24. We can conclude

Theorem 7.16 (1648 does not imply 206)**.** *There exists a magma which satisfies Theorem 2.33 and not Theorem 2.24.*

There are variation of the translation-invariant constructions refuting implications: e.g. in some cases, similar constructions are carried out starting with a non-Abelian group. Translation-invariant models are also useful building blocks for the *modified base model* constructions explained below.

7.5.2 Modified base models

For some pairs of laws P and Q, it is possible to start with an infinite model $(M, \diamond)$ obeying both P and Q, then modify the operation $\diamond$ in a limited way, resulting in a model $(M, \diamond')$ of P that does not obey Q.

This works especially well when this *base model* $(M, \diamond)$ is a translation-invariant magma in which the function f takes finitely many different values. This is common: e.g. the translation-invariant model refuting the implication above is of the required sort!

The strategy is to first modify the magma operation in a naive way, by introducing a counterexample to the consequent Q. This generally yields one or more counterexamples to the antecedent P, but one can *trace* the effects of this initial modification and make further adjustments which restore the antecedent.

A model refuting the implication between the laws Theorem 2.35 and Theorem 2.45 can be constructed using the modified base model technique. Start with the infinite model $(\mathbb{Z}, \diamond)$ of Theorem 2.35 given by the following operation:

$$x \diamond y = \begin{cases} x + 1 & \text{if } x, y \text{ have the same parity} \\ x - 1 & \text{otherwise} \end{cases}$$

A case analysis shows that the magma $(\mathbb{Z}, \diamond)$ satisfies both Theorem 2.35 and Theorem 2.45. We will eventually *modify* it by setting

$$x \diamond' y = \begin{cases} 0 & \text{if } x = 0,\ x, y \text{ do not have the same parity} \\ x + 1 & \text{if } x, y \text{ have the same parity} \\ x - 1 & \text{otherwise} \end{cases}$$

and checking that $(\mathbb{N}, \diamond')$ satisfies Theorem 2.35 but refutes Theorem 2.45.

One finds these modifications using the following strategy:

First, choose some element (tuple) of the carrier M that will constitute a counterexample to the consequent in the modified model. In this specific case, the consequent, Theorem 2.45, can be written as

$$x \diamond (y \diamond x) = x \diamond (y \diamond z)$$

in equational form, which always holds when $x = z$. So let's choose the tuple $(0, 0, 1)$ to constitute the required counterexample. Computing $0 \diamond (0 \diamond 0) = 0 \diamond 1 = -1$ and similarly $0 \diamond (0 \diamond 1) = -1$ suggest that we could force this tuple to be a counterexample by defining a new operation $\diamond''$ and setting $0 \diamond'' 1$ to something other than -1. One seemingly has many choices here: should we take $0 \diamond'' 1 = 0$, $0 \diamond'' 1 = 1$, $0 \diamond'' 1 = 2$, or perhaps even $0 \diamond'' 1 = -1$?

It's easy to rule out some of the possibilities. For instance, setting $0 \diamond'' 1 = 1$ would yield $0 \diamond'' (0 \diamond'' 0) = 0 \diamond'' 1 = 0 \diamond'' (0 \diamond'' 1)$ again. The simplest possibility which results in a counterexample to Theorem 2.45 sets $0 \diamond'' 1 = 0$ and $x \diamond'' y = x \diamond y$ for any $x \neq 0, y \neq 1$.

Unfortunately, the resulting $(M, \diamond'')$ would not then obey Theorem 2.35. For any $z \in M$, one would have

$$(0 \diamond'' 1) \diamond'' ((1 \diamond'' 1) \diamond'' z) = 0 \diamond'' (2 \diamond'' z)$$

which equals $0 \diamond'' 1 = 0$ as desired for even z, but equals $0 \diamond'' 3 = -1 \neq 0$ for odd z.

However, since f takes finitely many values in the base model, the breakage is tightly controlled: by considering what happens if $x \neq 0$ and $y \neq 1$, we see that all new counterexamples to Theorem 2.45 have this form. The calculation now suggests defining yet another $\diamond'''$, where setting $0 \diamond''' 3 = 0$ would eliminate this counterexample. But doing that just moves the issue one level higher: one then has

$$(0 \diamond''' 3) \diamond''' ((3 \diamond''' 3) \diamond''' z) = 0 \diamond''' (4 \diamond''' z)$$

which equals $0 \diamond''' 3 = 0$ as desired for even z, but equals $0 \diamond''' 5 = -1 \neq 0$ for odd z.

Instead, the infinitely many counterexamples arising from the iterated redefinition can be eliminated all at once by setting:

$$x \diamond' y = \begin{cases} 0 & \text{if } x = 0,\ x, y \text{ do not have the same parity} \\ x + 1 & \text{if } x, y \text{ have the same parity} \\ x - 1 & \text{otherwise} \end{cases}$$

At this point one might as well truncate the model to $\mathbb{N}$ since the result of the $\diamond'$ operation is nonnegative whenever the operands are nonnegative. This finishes the construction and proves

Theorem 7.17 (1659 does not imply 4315)**.** *There exists a magma which satisfies Theorem 2.35 and not Theorem 2.45.*

The result of a modified base model construction can be a finite modification (when $\diamond$ and $\diamond'$ differ in finitely many inputs) or one in which they differ in infinitely many coefficients. Note

that if the base model $(M, \diamond)$ was obtained by a greedy construction, and $(M, \diamond')$ is a finite modification, then the modified model could also have been obtained using the same greedy construction. It is not surprising that more difficult refutations using this construction tend to require the latter sort of modification.

7.6 The Dupont equation

Now we consider the Dupont equation, Theorem 2.21, which can be treated by a greedy translation invariant construction that is more complicated than the one considered for the Asterix law in Section 7.2.

If we adopt a translation-invariant model

$$x \diamond y = x + f(y - x)$$

on some abelian group G, then with $y = x + h$, we have

$$x \diamond y = x + f(h)$$

$$x \diamond (x \diamond y) = x + f^2(h)$$

$$y \diamond (x \diamond (x \diamond y)) = y + f(f^2(h) - h)$$

and so the Dupont law $x = y \diamond (x \diamond (x \diamond y))$ becomes the functional equation

$$f(f^2(h) - h) = -h. \tag{7.5}$$

One way to solve this equation is to have an automorphism $T : G \to G$ that obeys the identity

$$T^3 - T = -I,$$

then one can just take $f(h) = T(h)$. For instance, if $G = \mathbb{Z}^3$, one can take the automorphism $T : \mathbb{Z}^3 \to \mathbb{Z}^3$ defined by

$$T(x, y, z) := (-z, x + z, y).$$

We now extend this greedily to $\mathbb{Z}^3 \times \mathbb{Z}$ as follows. Define a *partial solution* (E_1, E_2, f) to be a pair $\mathbb{Z}^3 \subset E_1 \subset E_2 \subset \mathbb{Z}^3 \times \mathbb{Z}$, and a function $f : E_2 \to E_1$ obeying the following axioms.

(a) The set $E_2 \backslash \mathbb{Z}^3$ is finite.

(b) For $h \in \mathbb{Z}^3$, $f(h) = Th$; in particular, f is a bijection on $\mathbb{Z}^3$.

(c) For $h \in E_1 \backslash \mathbb{Z}^3$, $f(h) \in E_1$. Also, $-h + f^2(h) \in E_1$ and $f(-h + f^2(h)) = -h$. Note that this (and (b)) implies that $-h \in E_1$, thus E_1 is symmetric around the origin.

(d) For $h \in E_2 \backslash E_1$, $f(h) \in E_1$.

(e) The elements $-h$, $h - f^2(h)$, and $f^2(h) - h$ for $h \in E_2 \backslash E_1$ are all distinct from each other, and all lie outside of E_2. In particular this forces $f^2(h) \neq 0$, hence $f(h) \neq 0$. It also forces $f^2(h) \neq h$, hence $f(h) \neq h$.

Thus for instance one can take $(\mathbb{Z}^3, \mathbb{Z}^3, T)$ as a partial solution. We say that a partial solution (E_1', E_2', f') is an *extension* of (E_1, E_2, f) if $E_1 \subset E_1'$, $E_2' \subset E_2$, and f' agrees with f on E_2.

Informally, E_1 represents the portion of $\mathbb{Z}^3 \times \mathbb{Z}$ where we have completely resolved the Dupont equation; the set $E_2 \backslash E_1$ represents the portion for which f (and all forward iterates of f) have been defined, but the Dupont equation has not yet been verified; and the elements $-h$, $h - f^2(h)$, and $f^2(h) - h$ for $h \in E_2 \backslash E_1$ are the portion where f is not yet defined, but for which one is ready to "promote" these elements to E_2 or E_1 by defining f appropriately.

The key lemmas are then

Lemma 7.18 (Promoting to E_1)**.** *If (E_1, E_2, f) is a partial solution and $h \in E_2 \backslash E_1$, then there exists an extension (E_1', E_2', f') of (E_1, E_2, f) such that $h \in E_1'$.*

Proof. This will be a greedy construction, but we have to introduce a rather large number of additional elements to ensure that certain non-degeneracy conditions are maintained (in particular, the new elements h' introduced have to be such that $f^2(h') - h'$ avoids E_2 and hence $\mathbb{Z}^3$, which requires a certain amount of complexity in the construction).

Let $\tilde{E}_2$ denote the set E_2 together with all the elements of the form $-h'$, $h' - f^2(h')$, and $f^2(h') - h'$ for $h' \in E_2 \backslash E_1$; this is $\mathbb{Z}^3$ with a finite number of additional elements.

Let a be an element of $\mathbb{Z}^3$ such that the quantities

$$\pm Ta, \pm(Ta + a)$$

are distinct from each other and from

$$0, \pm h, \pm(h - f(h)), \pm(f^2(h) - h);$$

this is possible since $T, T + 1$ are invertible.

Next, we pick an $x \in \mathbb{Z}^3 \times \mathbb{Z}$ such that the quantities

$$\pm x, \pm x + Ta, \pm x - Ta, \pm 2x + Ta, \pm x + Ta + a, \pm(h + x), \pm(h - f(h) + x), \pm(f^2(h) - h + x + Ta)$$

are all distinct from each other and from $\tilde{E}_2$; indeed, from the choice of a (and the non-zero nature of h, $f(h)$, $h - f(h)$, and $f^2(h) - h$) there are only finitely many x for which a collision can occur between any pair of these expressions.

We now promote $\pm h, \pm x, \pm x + Ta, \pm x - Ta$ to E_1, and also promote $h + x$, $h - f^2(h)$, $\pm 2x + Ta$, $\pm x + Ta + a$ to E_2. That is to say, we define

$$E_1' := E_1 \cup \{\pm h, \pm x, \pm x + Ta, \pm x - Ta\}$$

and

$$E_2' := E_2 \cup \{-h, \pm x, \pm x + Ta, \pm x - Ta, h + x, h - f^2(h), \pm 2x + Ta\}.$$

We then define an extension f' of f to E_2' by setting

$$\begin{aligned}
f'(\pm x) &:= a \\
f'(\pm x + Ta) &:= \pm x \\
f'(\pm x - Ta) &:= \mp x + Ta \\
f'(\pm x + Ta + a) &:= \pm x - Ta \\
f'(\pm 2x + Ta) &:= \pm x + Ta \\
f'(\pm x + Ta + a) &:= \pm x - Ta \\
f'(-h) &:= x + Ta \\
f'(h + x) &:= h \\
f'(h - f^2(h)) &:= -h.
\end{aligned}$$

It is easy to see that (E_1', E_2', f') obeys properties (a), (b), (d). By construction, we have

$$f'((f')^2(h') - h') = -h'$$

for

$$h' = \pm h, \pm x, \pm x + Ta, \pm x - Ta$$

giving property (c). By construction, the quantities

$$-h', h' - f^2(h'), f^2(h') - h'$$

are distinct from each other and lie outside of $\tilde{E}_2 \cup E'_2$ for

$$h' = h + x, h - f^2(h), \pm 2x + Ta, \pm x + Ta + a$$

while these quantities are distinct from each other and lie in $\tilde{E}_2 \backslash E'_2$ for $h' \in E_2 \backslash E'_1$ (note that this forces $h' \neq \pm h$). This gives property (e). □

Lemma 7.19 (Promoting to E_2)**.** *If (E_1, E_2, f) is a partial solution and $h \in (\mathbb{Z}^3 \times \mathbb{Z}) \backslash E_2$, then there exists an extension (E'_1, E'_2, f') of (E_1, E_2, f) such that $h \in E'_2$.*

Proof. Let $\tilde{E}_2$ denote the set E_2 together with all elements of the form

$$-h', h' - f^2(h'), f^2(h') - h' \tag{7.6}$$

for some $h' \in E_2 \backslash E_1$; this is $\mathbb{Z}^3$ with a finite number of elements attached, and is symmetric around the origin.

First suppose that h lies outside of $\tilde{E}_2$. Then we can find $a \in \mathbb{Z}^3$ such that the quantities

$$-h, \pm(h - Ta)$$

are distinct from each other, and lie outside of $\tilde{E}_2$. We now promote h to E_2, thus setting

$$E'_1 := E_1$$

and

$$E'_2 := E_2 \cup \{h\}$$

and define an extension f' of f to E'_2 by setting

$$f'(h) := a.$$

It is then a routine matter to check that (E'_1, E'_2, f') is an extension of (E_1, E_2, f).

Now suppose that h lies in $\tilde{E}_2$. Then h is of one of the forms Equation (7.6) for some $h' \in E_2 \backslash E_1$. Suppose it is of the form $-h'$ or $f^2(h') - h'$. We invoke Theorem 7.18 to promote h' to E_1 by using a suitable extension (E'_1, E'_2, f'); and now h will lie in E'_2, giving the claim. If instead h is of the form $h' - f^2(h')$, then this procedure might not place h in E'_2; but if it does not, it will be of the form $-h''$ for $h'' = f^2(h') - h' \in E'_2 \backslash E'_1$. Applying Theorem 7.18 one more time to now promote h'' to E_1, we will obtain a larger extension (E''_1, E''_2, f'') with $h \in E''_2$, giving the claim. □

Iterating these lemmas in the usual fashion, we can conclude that any partial solution can be completed to a global model of Theorem 2.21.

Among other things, this permits one to generate models in which the function f is not injective. To see this, let a be a non-zero element of $\mathbb{Z}^3$, let x be an element of $\mathbb{Z}^3 \times \mathbb{Z}$ outside of $\mathbb{Z}^3$, and consider the partial solution $(\mathbb{Z}^3, \mathbb{Z}^3 \cup \{x\}, f)$ where $f(h) = Th$ for $h \in \mathbb{Z}^3$ and $f(x) = a$. One can check that this is a partial solution and is not injective, since $f(x) = f(T^{-1}a)$. This non-injectivity implies in particular that the model is not left-cancellative, and hence does not obey the law

$$x = (y \diamond x) \diamond ((y \diamond x) \diamond y)$$

(equation 1692).

7.6.1 Second construction

We now give a second construction, with works on the integers $G = \mathbb{Z}$.

We first define a seed solution $f_0 : E_0 \to \mathbb{Z}$ defined on the set $E_0 := \{-7, -3, -2, -1, 0, 1, 3, 4, 6\}$ with

$$f(-7) = -4, f(-3) = 4, f(-2) = -3, f(-1) = -1, f(0) = 1, f(1) = 3, f(3) = 0, f(4) = -2, f(6) = 2.$$

In this construction, we define a partial solution to be a function $f : E \to \mathbb{Z}$ defined on a finite subset of E obeying the following axioms:

(i) E contains E_0, and f agrees with f_0 on E_0.

(ii) If $h \in E$ and $f(h) \in E$, then $f^2(h) - h$ is also in E, and $f(f^2(h) - h) = -h$.

(iii) If $h \in E$ and $h \neq 3$, then $f(h) \neq 0$.

(iv) If $a \neq a'$ are distinct elements of E with $f(a) = f(a')$, and $-a \in E$, then $a' \neq a + f(-a)$.

(v) If $a \neq a'$ are distinct elements of E with $f(a) = f(a')$, and $-a, -a' \in E$, then $a' + f(-a') \neq a + f(-a)$.

We say that a partial solution $f' : E' \to \mathbb{Z}$ *extends* another $f : E \to \mathbb{Z}$ if E' contains E and f' agrees with f on E.

Lemma 7.20 (Seed solution)**.** *$f_0 : E_0 \to \mathbb{Z}$ is a partial solution.*

Proof. Finite check. □

Lemma 7.21 (Extension)**.** *If $f : E \to \mathbb{Z}$ is a partial solution and $h_0 \in \mathbb{Z}$, then there exists an extension $f' : E' \to \mathbb{Z}$ for which axiom (ii) applies, i.e., $h_0 \in E'$, $f'(h_0) \in E'$, $(f')^2(h_0) - h_0 \in E'$, and $f'((f')^2(h_0) - h_0) = -h_0$.*

Proof. We divide into cases.

Case 1: $h_0 \in E$ and $f(h_0) \in E$. In this case we are already done thanks to axiom (ii).

Case 2: $h_0 \in E$ but $f(h_0) \notin E$. This is the main case. Let H be the set of all $h \in E$ such that $f(h) = f(h_0)$; this is a finite set containing h_0. Let $H' \subset H$ be the set of all $h' \in H$ such that $-h' \in E$. We make the following observations:

(a) All elements h of H are non-zero. For if $h = 0$ then $f(h_0) = f(h) = 1 \in E$, contradicting the hypothesis $f(h_0) \notin E$.

(b) If $h' \in H'$ then $h' \neq h' + f(-h')$. Otherwise we would have $f(-h') = 0$, then by axiom (iii) we have $h' = -3$, hence $f(h_0) = f(h') = 4 \in E$ by axiom (i). But this again contradicts the hypothesis $f(h_0) \notin E$. (This is the main reason we take E_0 to be so large.)

(c) If $h_1 \in H$ and $h_2 \in H'$ are distinct then $h_1 \neq h_2 + f(-h_2)$. This follows from axiom (iv).

(d) If $h_1, h_2 \in H'$ are distinct then $h_1 + f(-h_1) \neq h_2 + f(-h_2)$. This follows from axiom (v).

From these observations, we see that if we take c to be a sufficiently large integer, the following claims hold:

1. The expressions $\pm c$, $\pm(c - h)$ for $h \in H$, and $\pm(c - h' - f(-h'))$ for $h \in H'$ are all distinct from each other.

2. c is not expressible as the sum of four or fewer elements of $\pm(E \cup f(E))$.

We select such a c. We then promote $f(h_0)$, $c-h$ for $h \in H$, and $-c+h'+f(-h')$ for $h' \in H'$, thus setting

$$E' := E \cup \{f(h_0)\} \cup \{c-h : h \in H\} \cup \{-c+h'+f(-h') : h' \in H'\}.$$

We then extend f to $f' : E' \to \mathbb{Z}$ by setting

$$\begin{aligned} f(f(h_0)) &:= c \\ f(c-h) &:= -h \\ f(-c+h'+f(-h')) &:= h'-c \end{aligned}$$

for all $h \in H$ and $h' \in H'$. Axiom (i) is then obvious. Axiom (ii) needs to be verified for the new elements h_0 and $c-h'$, $h' \in H'$ of E' (the other elements will not obey the hypotheses of this axiom), but this is routine. In particular h_0 obeys the required conclusion of this lemma.

We need to verify (iii) for the new elements of E', but this is clear from property (a) and claim 2.

Now we need to verify (iv). It suffices to do so when at least one of $a, a', -a$ are new elements of E'. If neither of a, $-a$ are new, then the only new elements a' for which $f(a')$ could equal $f(a)$ take the form $c-h$ (thanks to claim 2), but then a' cannot equal $a+f(-a)$, again thanks to claim 2. If instead one of $a, -a$ is new, then from claim 1 the new element must be $f(h_0)$. There is no old element a' with $f(a') = c = f(f(h_0))$, so we must have $a = -f(h_0)$, but then $a+f(-a) = -f(h_0)+c$ will not equal a', again thanks to claim 2.

Finally, we need verify to (v). We may assume that at least one of $a, a', -a, -a'$ are new elements of E'. As before, this forces the new element to be $f(h_0)$, and this cannot be a or a', so without loss of generality we have $a = -f(h_0)$ and $a' \in E$. But then $a+f(-a) = -f(h_0)+c$ will not equal $a'+f(-a')$, again thanks to claim 2.

Case 3: $h_0 \notin E$ but $h_0 \in f(E)$. Here we can write $h_0 = f(h_1)$ where h_1 is of the form in Case 2. Applying the Case 2 construction, we can pass to an extension in which $f(h_1) = h_0$ lies in E, and so we are now in either Case 1 or Case 2, and so we can again conclude.

Case 4: $h_0 \notin E$ and $h_0 \notin f(E)$. We let c be an integer so large that it is not expressible as the sum of four or fewer elements of $\pm(E \cup f(E))$. We then promote h_0 to E by setting

$$E' := E \cup \{h_0\}$$

and define an extension $f' : E' \to \mathbb{Z}$ by setting $f'(h_0) := c$. Axioms (i)-(iii) are obvious. For axiom (iv), since $f'(h_0)$ is not equal to any other value of f', the only new case introduced is if $-a = h_0$, but then $a+f(-a) = -h_0+c$ is distinct from a' by choice of c. A similar argument yields axiom (v). With this extension, we are now in Case 2, and so we repeat the previous analysis to conclude. □

Iterating this lemma, we conclude

Corollary 7.22 (Greedy completion of Dupont)**.** *Every partial solution $f : E \to \mathbb{Z}$ can be extended to a global solution $f' : \mathbb{Z} \to \mathbb{Z}$ of Equation (7.5).*

Corollary 7.23 (Non-injective Dupont solution)**.** *The Dupont equation admits non-injective solutions, and hence can violate Equation 1692.*

Proof. It suffices to find a partial solution that violates injectivity. This can be done for instance by adjoining $\{-13, 10\}$ to E_0 and defining $f(10) = 2 = f(6)$, $f(-13) = -10$, and performing a finite check to verify that this is still a partial solution. □

7.7 An ad hoc model

Theorem 7.24. *There exists a magma which satisfies Equation 3342,*

$$x \diamond y = y \diamond (x \diamond (x \diamond x)),$$

but such that none of the laws

$$x \diamond x = x \diamond ((x \diamond x) \diamond x)$$
$$x \diamond y = x \diamond ((y \diamond y) \diamond y)$$
$$x \diamond x = ((x \diamond x) \diamond x) \diamond x$$
$$x \diamond y = ((x \diamond x) \diamond x) \diamond y.$$

hold.

Proof. We begin with some informal motivation. Writing

$$f(x) := x \diamond (x \diamond x), \tag{7.7}$$

we conclude that

$$x \diamond y = y \diamond f(x) \tag{7.8}$$

and hence on iteration

$$x \diamond y = f(x) \diamond f(y).$$

In particular, $x \diamond x = f(x) \diamond f(x)$, and

$$f(x) = x \diamond (x \diamond x) = (x \diamond x) \diamond f(x) = (f(x) \diamond f(x)) \diamond f(x).$$

If f is surjective, this would imply

$$x = (x \diamond x) \diamond x$$

and hence the four laws stated above would hold in this case.

This motivates the use of a non-surjective f. We will take G to be the space of polynomials $\mathbb{Z}[t]$ of one variable with integer coefficients, and let $f : G \to G$ be the multiplication by t map:

$$f(P) := tP.$$

This is of course non-surjective. The magma operation will be constructed as follows:

- If P is a polynomial with $P(0) \neq 0$, then $t^n P \diamond t^n P = t^n P \diamond t^{n+1} P = 2P$ for all $n \geq 0$, and $t^{n+m} P \diamond 2t^n P = 2t^n P \diamond t^{n+m+1} P = t^{m+1} P$ for all $n, m \geq 0$. (This is well-defined since the $t^n P$, $2t^n P$ are all distinct polynomials.)
- We define $P \diamond Q = 0$ if not covered by the above laws.

It is a routine matter to verify Equation (7.7) and Equation (7.8), so that equation 3342 holds. However, one can check that the four laws in the conclusion fail with $x = y = 1$. □

Theorem 7.25 (1437 example)**.** *There exists a magma that obeys Equation 1437,*

$$x = (x \diamond x) \diamond (y \diamond (z \diamond x)),$$

but does not obey equation 4269,

$$x \diamond (x \diamond x) = x \diamond (y \diamond x).$$

Proof. A first attempt would be the operation $i \diamond j := j + 1$ on $\mathbb{Z}/3\mathbb{Z}$; this obeys 1437, but unfortunately also obeys 4269. However, an "extension" of this operation will work. Namely, we take the carrier $G = \mathbb{N} \times \mathbb{Z}/3\mathbb{Z}$ and define $(a, i) \diamond (b, j)$ to equal

- $(a - 1, j + 1)$ if $i = j + 2$ and $a > 0$;
- $(b, j + 1)$ if $i = j + 2$ and $a = 0$;
- $(a + 1, j + 1)$ otherwise.

Note that $(a, i) \diamond (a, i) = (a + 1, i + 1)$, and that $(b, j) \diamond ((c, k) \diamond (a, i))$ will be of the form $(d, i + 2)$ for some d. Hence

$$((a, i) \diamond (a, i)) \diamond ((b, j) \diamond ((c, k) \diamond (a, i))) = (a + 1 - 1, i + 3) = (a, i),$$

giving 1437. On the other hand,

$$(0, i) \diamond ((b, i) \diamond (0, i)) = (0, i) \diamond (b + 1, i + 1) = (b + 1, i + 2)$$

and so equation 4269 fails. □

Chapter 8

Equivalence with the constant and singleton laws

85 laws have been shown to be equivalent to the constant law (Theorem 2.20), and 815 laws have been shown to be equivalent to the singleton law (Theorem 2.2).

These are the laws up to 4 operations that follow from diagonalization of Theorem 2.2 and Theorem 2.20.

To formalize these in Lean, a search was run on the list of equations to discover diagonalizations of these two specific laws: equations of the form $x = R$ where R doesn't include x, and equations of the form $x \circ y = R$ where R doesn't include x or y.

The proofs themselves all look alike, and correspond exactly to the two steps described in the proof of Theorem 4.6. The Lean proofs were generated semi-manually, using search-and-replace starting from the output of `grep` that found the diagonalized laws.

In the case of the constant law, Theorem 2.16 ($x \circ x = y \circ z$) wasn't detected using this method. It was added manually to the file with the existing proof from the sub-graph project.

Chapter 9

Metatheorems from Invariants

For the purposes of this chapter, a *theorem* is a (true) statement about particular equations, for example '(387 implies 43)' is a theorem. A *metatheorem* is a general statement about implications; one can usually get many theorems from a single metatheorem. This chapter is all about generating many interesting metatheorems using a *meta-metatheorem*, called the fundamental property of invariants. If all this is making your head spin, don't worry. Look at the sections below for examples of metatheorems you can probably agree are both concrete and interesting. Once you have done that, come back here and we will show you how to prove these and other metatheorems using *invariants*.

9.1 Invariants

Let E, E_1, and E_2 be equations. If $E \Rightarrow E_1$ and $E_1 \Rightarrow E_2$, then $E \Rightarrow E_2$. Very trivial. Rephrasing this, we see that if $E \Rightarrow E_1$ and $E \not\Rightarrow E_2$, then $E_1 \not\Rightarrow E_2$.

Extending this idea, suppose we compute the set of all equations which are implied by E; we will call this set $\mathcal{Y}(E)$ (we use $\mathcal{Y}$ because this is an example of a Yoneda embedding). Then $\mathcal{Y}(E)$ is upwards closed, or closed under forward implication: no equation in $\mathcal{Y}(E)$ can imply an equation not in $\mathcal{Y}(E)$. If we know $\mathcal{Y}(E)$ well, this already settles a potentially large number of implications in the negative.

While computing $\mathcal{Y}(E)$ for an arbitrary equation E may seem daunting, for some nice equations we can find *invariants*, which makes the task manageable. An *invariant* for E is some sort of data associated with expressions w so that

$$\mathcal{Y}(E) = \{w = w' \mid \text{Invariant}(w) = \text{Invariant}(w')\}$$

If we can find an invariant which is computable for each term w, then we can easily describe $\mathcal{Y}(E)$. The fact that $\mathcal{Y}(E)$ is upwards closed is rephrased as follows; this is called **the fundamental property of invariants**. Remember that an invariant is a function taking expressions and outputting some data.

Meta-metatheorem 9.1 (Fundamental property of invariants)**.** *Let I be an invariant of E. If $w = w'$ implies $w'' = w'''$ and $I(w) = I(w')$ (that is, E implies $w = w'$), then $I(w'') = I(w''')$.*

More succinctly, for an invariant I of E we must have

$$(w = w' \Rightarrow w'' = w''') \implies (I(w) = I(w') \Rightarrow I(w'') = I(w''')).$$

When using this result, we commonly take the contrapositive: if $I(w) = I(w')$ and $I(w'') \neq I(w''')$, then $w = w'$ cannot imply $w'' = w'''$. Note that the conclusion is independent of the equation E; all we need to know is that I is an invariant.

Note for category theorists. Let Π denote the preorder of magma equations ordered by implication. If I is an invariant then define

$$I(w = w') := \begin{cases} \texttt{true} & \text{if } I(w) = I(w') \\ \texttt{false} & \text{otherwise} \end{cases}.$$

(In programming languages we would say $I(w = w') := I(w) == I(w')$). Let $\mathbf{Bool} = \{\texttt{true}, \texttt{false}\}$ be the poset where $\texttt{false} \leq \texttt{true}$. Then I becomes a function $\Pi \to \mathbf{Bool}$, and the fundamental property of invariants just says that this function is monotone, i.e. functorial. Thus for every invariant I we obtain a functor $\Pi \to \mathbf{Bool}$.

Question 1: Does every functor $\Pi \to \mathbf{Bool}$ come from an invariant?

Question 2: What can we say about the category of functors $\Pi \to \mathbf{Bool}$? Give a nice interpretation of natural transformations between invariants. □

The fundamental property of invariants is not a theorem, nor a metatheorem: it is a meta-metatheorem, in the sense that it will allow us to get a metatheorem for every invariant we find.

Example: absorption law

Let E be the equation $x \diamond y = x$. Intuitively, we must have

$$\mathcal{Y}(E) = \{w = w' \mid \text{the leftmost variable is the same for } w \text{ and } w'\}.$$

We will talk about proving statements like this one (say in Lean) later on; take it as given for now. The invariant is clear: we define $I(w)$ to be the leftmost variable of w. Instantiating this invariant in the fundamental property of invariants, we get the following metatheorem.

Metatheorem 9.2. *Let $w = w'$ be an equation such that the leftmost variable of w is the same as the leftmost variable of w'. Then $w = w'$ cannot imply an equation that does not have the property from the last sentence.*

Example: associativity

For a more complicated example, let E be the associativity equation $x \diamond (y \diamond z) = (x \diamond y) \diamond z$. Intuitively, we must have

$$\mathcal{Y}(E) = \{\text{equations that, when we remove all parentheses, are of the form } w = w\}.$$

There is an invariant lurking behind: it is the (ordered) list of variables appearing in an expression, counting repetitions. More formally, we define $I(w)$ to be the tuple of variables appearing in w, listed from left to right, say. Again, from the fundamental property of invariants we get the following.

Metatheorem 9.3. *Let $w = w'$ be an equation such that the variables appearing in w, taking into account order and repetitions, are the same ones that appear in w'. Then $w = w'$ cannot imply an equation that does not have the property from the last sentence.*

If we were coding a computer program that computes $I(w)$ given w, one could take the string of symbols that is w, ignore all parentheses, replace all symbols $\diamond$ by commas, and surround with an appropriate delimiter. (I imagine one could easily do this using regular expressions.)

We can compute other examples, but the invariant can get complicated even for simple equations. Exercise: what is the invariant for commutativity? Answer: To compute $I(w)$ from w replace all parentheses with curly braces and all symbols $\diamond$ with commas, and interpret the result as nested sets.

9.2 Expanding the language

The method of invariants really shines when we expand our formal language. Right now our language consists of variables, parentheses, the equal sign, and $\diamond$ (there is also an implicit use of $\forall$ but let's ignore that for now). Let Π denote the preorder of equations (built from the language described) ordered by implication.

We will add the symbol $\wedge$ ('and') to our language. Then we consider a bigger preorder $\Pi' \supseteq \Pi$ which includes equations and also conjunctions of equations. Even if we only care about Π it will be apparent that studying invariants in Π' gives us useful metatheorems about Π. Equations and conjunctions of equations are examples of *formulas* (or formulae, according to taste).

If φ is a formula, we can define $\mathcal{Y}(\varphi)$ to be the set of all formulae implied by φ; this agrees with our previous definition. Now define an invariant of φ to be a function I on terms such that

$$\mathcal{Y}(\varphi) \cap \Pi = \{w = w' \mid I(w) = I(w')\}.$$

Again, this clearly agrees with our previous definition. Although $\mathcal{Y}(\varphi) \cap \Pi$ might not be upwards closed in Π', it is upwards closed in Π, which is enough to get the fundamental property of invariants *verbatim*. This leads to more metatheorems we didn't have access to before.

Example: associativity and idempotency

Let φ be the conjunction of the associative law and the idempotency law ($x \diamond x = x$). Again, we will rely on our intuition, which says that an invariant I defined by taking $I(w)$ to be the set of all variables appearing in w, works. The corresponding metatheorem is the following

Metatheorem 9.4. *Let $w = w'$ be an equation such that the set of variables appearing in w is equal to the set of variables appearing on w'. Then $w = w'$ cannot imply an equation that does not have the property from the last sentence.*

Example: associativity and commutativity

For a similar example, we can let φ be the conjunction of the associative and the commutative laws. Here we can define $I(w)$ to be the multiset of variables appearing in w. We obtain the following metatheorem.

Metatheorem 9.5. *Let $w = w'$ be an equation such that the variables appearing in w, taking into account multiplicity, are the same ones that appear in w'. Then $w = w'$ cannot imply an equation that does not have the property from the last sentence.*

Trivia: this was the first example of a metatheorem obtained by use of an invariant.

Example: associativity and commutativity with a twist

We can keep expanding our language if it helps us express more intricate invariants. For instance, we can add the symbol '1' to our language. Let φ be the conjunction of associativity, commutativity, the equations $1 \diamond x = x$, and

$$\underbrace{x \diamond x \diamond \cdots \diamond x}_{m \text{ times}} = 1,$$

for some fixed positive integer m. Pause to guess the invariant before we move on.

The invariant $I(w)$ is the multiset of variables appearing in w but multiplicities are computed modulo m. Thus we have the pretty metatheorem:

Metatheorem 9.6. *Fix some positive integer m. Let $w = w'$ be an equation such that every variable appearing in w appears the same number of times in w' modulo m. Then $w = w'$ cannot imply an equation that does not have the property from the last sentence.*

9.3 Proving metatheorems from invariants in Lean

For the rest of this chapter we readopt the convention of calling 'theorem' an important result, not necessarily pertaining to specific equations.

An invariant is generally a *syntactic* property of an expression. However, invariants can also be described and calculated *semantically* through the notion of a *lifting magma family*, described below. The general idea is that the value of an invariant for an expression can be computed by substituting specific values for the variables in the expression and evaluating the result in a certain magma in the lifting magma family; additional requirements ensure that the fundamental property of invariants is satisfied.

Definition 9.7 (Lifting Magma Family)**.** A *lifting magma family* is a family of magmas $\{G_\alpha\}$, one for each type α, satisfying the following properties:

- For each type α, there is a function $\iota_\alpha : \alpha \to G_\alpha$.
- Given a function $f : \alpha \to G_\alpha$, there is a magma homomorphism lift $f : G_\alpha \to G_\alpha$ such that lift $f(\iota_\alpha(x)) = f(x)$ for all x in α.

Example 3. *The free Abelian groups form a lifting magma family. When the underlying set is finite, the groups are isomorphic to $\mathbb{Z}^n$.*

Example 4. *Lists form a lifting magma family.*

The key consequence of the Theorem 9.7 is that it is significantly easier to check whether an equation is satisfied in a lifting magma family.

Theorem 9.8 (Evaluation theorem for lifting magma families)**.** *Suppose E is an equation involving a set of variables X, and let G be a lifting magma family.*

Determining whether E is satisfied by G_X is equivalent to checking that E is true with the specific substitution ι_X.

Proof. For the forward direction, suppose E is satisfied by G_X. Then, by definition, any substitution of the variables in E with elements of G_X will yield a true equation. In particular, substituting according to ι_X will yield a true equation.

For the reverse direction, suppose that E is true when evaluated with the substitution ι_X. Now, consider an arbitrary substitution of variables $f : X \to G_X$. By the lifting magma family

property, there is a magma homomorphism $\operatorname{lift} f : G_X \to G_X$ such that $\operatorname{lift} f(\iota_X(x)) = f(x)$ for all x in X. In other words, applying the substitution f is equivalent to first applying to substitution ι_X and then applying the homomorphism $\operatorname{lift} f$. Since E is true when evaluated with the substitution ι_X, it is also true after applying the homomorphism $\operatorname{lift} f$. Thus, E is satisfied by G_X. □

Theorem 9.9 (The fundamental property of invariants)**.** *Let E and E' be equations involving a set of variables X, and let G be a lifting magma family.*

If E is true with the substitution ι_X, and E implies E', then so is E'.

Proof. Applying the evaluation Theorem 9.8, we see that E is satisfied by G_X. Since E implies E', E' is also satisfied by G_X, and in particular, E' is true with the substitution ι_X. □

Remark 1. *The result of evaluating an expression along the function $\iota_X : X \to G_X$ is the invariant.*

In the case of Abelian groups, the result of evaluation is the variables in the expression with multiplicity. In the case of lists, the result of evaluation is the variables in the expression in the order they appear.

When the lifting magma family has good computational properties, calculating the invariant becomes easy.

Remark 2. *Given an equation ϕ in the language of magmas (possibly involving logical operations other than equality and universal quantification), the initial (i.e., most general) magmas satisfying ϕ (provided they exist) form a lifting magma family.*

However, for the purpose of generating invariants, we are interested in lifting magma families with convenient descriptions that are computationally tractable.

Remark 3. *Suppose S is a finite set of equations in the language of magmas that is a confluent term rewriting system under a certain ordering of the terms (in the sense of the Knuth-Bendix algorithm). Then the initial magmas satisfying S form a lifting magma family where equality of elements in the magma is decidable.*

This offers a way of generating examples of lifting magma families with good computational properties for computing invariants of expressions.

9.4 Generating laws from equations

The invariants defined in this chapter are properties of the *syntax* of the equations being considered. In other words, they are properties of the laws associated with the equations, rather than of the equations themselves. Proving non-implications using invariants requires a way to operate on the syntax of the equations and then translate the reasoning back to results about the original equations.

A magma law can be generated from an equation by accessing the syntax used in its definition and converting it to a declaration representing a magma law through metaprogramming. There is a choice in the variable set of the magma law – one one hand, it can be a finite set whose size matches the number of variables, and on the other hand, it can be the set of natural numbers. The advantage of the former is that one can generate proofs that the satisfiability of the magma law is equivalent to the satisfiability of the original equation (this only needs to be done for variable sets of size up to six, since that is the maximum size currently being considered in the project; it's convenient to prove individual lemmata for each variable set size establishing this equivalence). The advantage of the latter is that it bypasses the need to cast between various finite sets while constructing a model as a counter-example.

One approach is to generate both forms of the law, using the first to establish the equisatisfiability of the law and the equation and then transporting this result to the second form of the law. The conversion from the first form to the second is summarised in the lemma below.

Lemma 9.10. *[Compatibility between magma laws over finite sets and the natural numbers] Let E be a magma law defined over n variables and let $\tilde{E}$ be the same equation with variables ranging over the natural numbers (formally, $\tilde{E}$ is the image of E under the canonical map from the finite set with n elements to the natural numbers). Then any magma M satisfies E if and only if it satisfies $\tilde{E}$.*

Proof. In the forward direction, suppose $\phi : \mathbb{N} \to M$ is a substitution. Then the restriction of ϕ to the first n natural numbers is a substitution for the variables of E, and since M satisfies E, the law E is true in M under this substitution. Since $\tilde{E}$ is the same as E under the substitution ϕ, M satisfies $\tilde{E}$.

In the reverse direction, suppose $\phi : \{0, 2, \dots, n-1\} \to M$ is a substitution. Then ϕ can be extended to a substitution $\tilde{\phi} : \mathbb{N} \to M$ by setting $\tilde{\phi}(i) = \phi(i)$ for $i \leq n$ and $\tilde{\phi}(i) = 0$ for $i \geq n$. Since M satisfies $\tilde{E}$ under the substitution $\tilde{\phi}$, it satisfies E under the restriction of $\tilde{\phi}$ to the first n natural numbers, which is precisely ϕ. The special case where $n = 0$ is in fact impossible, since there cannot be an expression with no variables. □

9.5 Conclusion: Beyond Invariants

We are still lacking:

- A large collection of invariants.
- An estimate for how many implications the resulting metatheorems will settle.
- Algorithms (in Lean, Python, or otherwise) to compute known invariants.
- General results about lifting magmas.
- Formalization of the method of invariants and resulting metatheorems.
- Knowledge about the category-theoretic interpretation of invariants (see the questions in the note for category theorists).

Related to the last bullet point, we note the following. If all that matters about invariants is the fundamental property, we can apply the old French trick of turning a (meta-meta)theorem into a definition.

Q: If we were to define invariants as any functions satisfying the fundamental property, would anything change? (For those who read the note for category theorists: an equivalent redefinition is to consider invariants as functors $\Pi \to \mathbf{Bool}$).

Chapter 10

Some abstract nonsense

This is an alternate presentation of the material of the previous section, where we use the "abstract nonsense" of free magmas in the presence of a theory as the conceptual foundation.

Definition 10.1 (Free magma relative to a theory)**.** Let Γ be a theory with an alphabet X. A *free magma* with alphabet X subject to the theory Γ is a magma $M_{X,\Gamma}$ together with a function $\iota_{X,\Gamma} : X \to M_{X,\Gamma}$, with the following properties:

(i) $M_{X,\Gamma}$ obeys the theory Γ: $M_{X,\Gamma} \vDash \Gamma$.

(ii) For any magma M obeying the theory Γ and any function $f : X \to M$, there exists a unique magma homomorphism $\tilde{f} : M_{X,\Gamma} \to M$ such that $\tilde{f} \circ \iota_{X,\Gamma} = f$.

Such magmas exist and are unique up to a suitable isomorphism:

Theorem 10.2 (Existence and uniqueness of free magmas)**.** *Let Γ be a theory with alphabet X.*

(i) *There exists a free magma $M_{X,\Gamma}$ with alphabet X subject to the theory Γ.*

(ii) *If $M_{X,\Gamma}$ and $M'_{X,\Gamma}$ are two free magmas with alphabet X subject to the theory Γ, then there exists a unique magma isomorphism $\phi : M_{X,\Gamma} \to M'_{X,\Gamma}$ such that $\phi \circ \iota_{X,\Gamma} = \iota'_{X,\Gamma}$.*

We remark that the ordinary free magma M_X corresponds to the case when Γ is the empty theory.

Proof. For (i), we define $M_{X,\Gamma} = M_X/\sim$, where the equivalence relation $\sim$ is defined by requiring $w \sim w'$ if and only if $\Gamma \vDash w \simeq w'$; this is an equivalence relation thanks to Theorem 1.11, and from Theorem 1.8 we see that this relation respects the magma operations, so that $M_{X,\Gamma}$ is a magma. The map $\iota_{X,\Gamma} : X \to M_{X,\Gamma}$ is defined by setting $\iota_{X,\Gamma}(x)$ to be the equivalence class of x in $M_{X,\Gamma}$ for each $x \in X$.

We first check that $M_{X,\Gamma}$ obeys Γ. Let $w \simeq w'$ be a law in Γ, and let $f : X \to M_{X,\Gamma}$ be a function. We may lift this function to a function $\tilde{f} : X \to M_X$. From Theorem 1.7, we have $\Gamma \vdash w \simeq w'$ and hence $\Gamma \vdash \varphi_{\tilde{f}}(w) \simeq \varphi_{\tilde{f}}(w')$. By Theorem 1.8, we conclude $\Gamma \vDash \varphi_{\tilde{f}}(w) \simeq \varphi_{\tilde{f}}(w')$. Quotienting by $\sim$, we conclude that $\varphi_f(w) = \varphi(w')$, giving the claim by Theorem 1.6.

Now we check the universal property (ii). Let M be a magma obeying the theory Γ, and let $f : X \to M$ be a function, then we have a magma homomorphism $\varphi_f : M_X \to M$. If $w, w' \in M_X$ are such that $w \sim w'$, then $\Gamma \vDash w \simeq w'$ and hence $\varphi_f(w) = \varphi_f(w')$. Hence φ_f descends to a map $\tilde{f} : M_{X,\Gamma} \to M$, which one can check to be a magma homomorphism with $\tilde{f} \circ \iota_{X,\Gamma} = f$. By construction, $M_{X,\Gamma}$ is generated by $\iota_{X,\Gamma}(X)$, and so this homomorphism is unique. □

Example 5 (Free associative magma)**.** *Let Γ consist solely of the associative law, Theorem 2.46 (so X contains $0, 1, 2$). Then one can take $M_{X,\Gamma}$ to be the set of nonempty strings with alphabet X, with magma operation given by concatenation, and $\iota_{X,\Gamma}(x)$ being the length one string x. It is a routine matter to verify that this obeys the axioms of a free magma subject to Γ.*

Example 6 (Free associative commutative magma)**.** *Let Γ consist of the associative law (Theorem 2.46) and the commutative law (Theorem 2.18). Then one can take $M_{X,\Gamma}$ to be the free abelian monoid $\mathbb{N}_0^X \backslash 0$ of tuples $(n_x)_{x \in X}$ with the n_x natural numbers, not all zero, with all but finitely many of the n_x vanishing, with the magma operation given by vector addition, and with $\iota_{X,\Gamma}(x)$ being the standard generator of $\mathbb{N}^X$ associated to $x \in X$; one can think of this space as the space of formal non-empty commuting associating sums of X. It is a routine matter to verify that this obeys the axioms of a free magma subject to Γ.*

Example 7 (Free left absorptive magma)**.** *Let Γ consist of the left absorptive law (Theorem 2.4). Then one can take $M_{X,\Gamma}$ to be X with the law $x \diamond y = x$, and $\iota_{X,\Gamma}$ to be the identity map. It is easy to see that this is indeed a free magma subject to Γ.*

Example 8 (Free constant magma)**.** *Let Γ consist of the constant law (Theorem 2.20). Then one can take $M_{X,\Gamma}$ to be the disjoint union $X \uplus \{0\}$ of X and another object 0, with $\iota_{X,\Gamma}$ being the identity embedding, and with the zero magma law $x \diamond y = 0$ for all $x, y \in X \uplus \{0\}$.*

Free magmas can be used to characterize entailment by Γ in terms of a canonical invariant.

Theorem 10.3 (Canonical invariant)**.** *Let Γ be a theory with some alphabet X, and let $M_{X,\Gamma}$ be a free magma with alphabet X subject to Γ, with associated map $\iota_{X,\Gamma} : X \to M_{X,\Gamma}$. Then for any $w, w' \in M_X$, we have*

$$\Gamma \vDash w \simeq w' \text{ if and only if } \varphi_{\iota_{X,\Gamma}}(w) = \varphi_{\iota_{X,\Gamma}}(w').$$

Proof. By Theorem 10.2 we may take $M_{X,\Gamma}$ to be the canonical free magma constructed in the proof of that theorem. The claim is then clear from expanding out definitions. □

Every theory Γ then gives a metatheorem about anti-implication:

Corollary 10.4 (Criterion for anti-implication)**.** *Let Γ be a theory with some alphabet X, and let $M_{X,\Gamma}$ be a free magma with alphabet X subject to Γ, with associated map $\iota_{X,\Gamma} : X \to M_{X,\Gamma}$. Let $w \simeq w'$ and $w'' \simeq w'''$ be laws with alphabet X. If one has*

$$\varphi_{\iota_{X,\Gamma}}(w) = \varphi_{\iota_{X,\Gamma}}(w')$$

but

$$\varphi_{\iota_{X,\Gamma}}(w'') \neq \varphi_{\iota_{X,\Gamma}}(w'''),$$

then the law $w \simeq w'$ cannot imply the law $w'' \simeq w'''$.

Proof. By Theorem 10.3, the hypothesis $\iota_{X,\Gamma}(w) = \iota_{X,\Gamma}(w')$ is equivalent to $\Gamma \vDash w \simeq w'$, and the hypothesis $\iota_{X,\Gamma}(w'') \neq \iota_{X,\Gamma}(w''')$ is equivalent to $\Gamma \not\vDash w'' \simeq w'''$. The claim follows. □

Example 9. *Let Γ be the associative and commutative law, so that we can take $M_{X,\Gamma} = \mathbb{N}_0^X \backslash 0$ as in Example 6. One can then check that for any word $w \in M_X$, that $\varphi_{\iota_{X,\Gamma}}(w)$ is the tuple that assigns to each letter x of the alphabet, the number of times x appears in w. We conclude that if w, w' have the same number of occurrences of each letter of the alphabet, but w'', w''' do not, then $w \simeq w'$ cannot imply $w'' \simeq w'''$. This recovers Theorem 4.8.*

Example 10. *Let Γ consist of the left absorption law, so we can take $M_{X,\Gamma} = X$ as in Example 7. Then $\varphi_{\iota_{X,\Gamma}}(w)$ is the first letter of w. We conclude that if w, w' have the same first letter, but w'', w''' do not, then $w \simeq w'$ cannot imply $w'' \simeq w'''$.*

Example 11. *Let Γ consist of the constant law, so we can take $M_{X,\Gamma} = X \uplus \{0\}$ as in Example 8. Then $\varphi_{\iota_{X,\Gamma}}(w)$ is x if w is just a letter x of the alphabet, and 0 otherwise. We conclude that if w, w', w''' have order at least one, but w'' has order zero, then $w \simeq w'$ cannot imply $w'' \simeq w'''$; this is basically Theorem 4.7.*

Example 12. *Let Γ be the theory consisting of the commutative and associative laws, and an additional law $x^n \simeq y^n$ for a fixed n, where x^n denotes the magma operation applied to n copies of x (the order is irrelevant thanks to associativity), then one can check (for finite X) that the free magma $M_{X,\Gamma}$ can be taken to be $(\mathbb{Z}/n\mathbb{Z})^X$ with the addition operation, and $\iota_{X,\Gamma}(x)$ being the standard generator associated to x. Then for any word w, $\varphi_{\iota_{X,\Gamma}}(w)$ corresponds to a tuple that assigns to each letter x of the alphabet, the number of times x occurs in w modulo n. We conclude that if w, w' have the same number of occurrences modulo n of each letter of the alphabet, but w'', w''' do not, then $w \simeq w'$ cannot imply $w'' \simeq w'''$. This is a stronger version of Theorem 4.8.*

10.1 Confluent theories

One promising source of theories Γ for which the free magma $M_{X,\Gamma}$ can be understood are the *confluent theories*.

Definition 10.5 (Confluent theory)**.** Let Γ be a theory. A word w can be *reduced* to another w' if one can get from w to w' by a series of substitutions of laws in Γ, where no substitution increases the length of the word **this is a working definition, might not be the best one to keep.**. A theory Γ is *confluent* if whenever a word w can be reduced to both w' and w'', then both w' and w'' can be reduced further to a common reduction $\tilde{w}$. As such, each word $w \in M_X$ should have a *unique simplification* to a reduced word w_Γ in some normal form, for instance the shortest reduction that is minimal with respect to some suitable ordering such as lexicographical ordering.

Example 13. *The associative law, Theorem 2.46, appears to be confluent* **check this**.

Example 14. *The theory consisting of both the associative and commutative laws, Theorem 2.46, Theorem 2.18, appears to be confluent* **check this**.

Example 15. *The idempotent law, Theorem 2.3, appears to be confluent* **check this**.

The significance of confluent theories lies in

Theorem 10.6 (Free magma of a confluent theory)**.** *Let Γ be a confluent theory. Then the free magma $M_{X,\Gamma}$ subject to this theory can be described as the space of reduced words in M_X in normal form, where the operation $w \diamond_\Gamma w'$ on this magma is defined as the normal form reduction of $w \diamond w'$, and $\iota_{X,\Gamma}$ is the identity embedding (note that every single-letter word is already in normal form).*

Proof. Should just be a matter of expanding definitions properly. □

Corollary 10.7 (Criterion for anti-implication)**.** *Let Γ be a confluent theory. Then a law $w \simeq w'$ is a consequence of Γ if and only if w, w' have the same normal form reduction. In particular, a law with this property cannot imply a law without this property.*

Proof. Follows from Theorem 10.4. □

It is thus of interest to locate some confluent laws. Here is a non-trivial example:

Theorem 10.8 (477 confluent)**.** *Theorem 2.27 is confluent.*

Proof. See the notes here. A sketch of proof is as follows. We induct on the length of the term. As before we consider terms of the form XY. Also, in both sequences if a simplification is applied to the whole term, then we can assume the sequence is simply final.

By Theorem 10.9, if any of the two sequences is final, then right before the last step, the two factors of the outermost product are both simple. This is also true for the result of the non-final sequence. By the induction hypothesis, they can be identified correspondingly, so the two sequences are either both final or both non-final, and in the first case, the same simplification is applied to give the same result. □

Lemma 10.9 (477 lemma)**.** *If Z and W are simple, then $Z(W\cdots(WW))$ is simple.*

Proof. Assume the contrary. Then we have 2 cases.

Case 1: $W\cdots(WW)$ matches the pattern $y(x(y\cdots(yy)))$, with k occurrences of W ($k \leq n$). Since $|x(y\cdots(yy))| > n|y|$, but $|\cdots(WW)| \leq (n-1)|W|$, this is impossible.

Case 2: $Z(W\cdots(WW))$ matches the pattern $y(x(y\cdots(yy)))$. Since $n \geq 3$, we have $Z = y = W$, so $|W\cdots(WW)| = n|W| = n|Z|$, contradicting $|x(y\cdots(yy))| > n|y|$. □

Chapter 11

Magma cohomology

Group cohomology is a theory that constructs certain abelian groups $H^n(G, M)$ to a group G acting as a module on an abelian group M, via a chain complex

$$0 \to C^0(G, M) \xrightarrow{d} C^1(G, M) \xrightarrow{d} C^2(G, M) \xrightarrow{d} C^3(G, M) \xrightarrow{d} ...$$

where $C^n(G, M)$ is the space of functions $f : G^n \to M$, and the coboundary maps $d : C^n(G, M) \to C^{n+1}(G, M)$ are explicit maps obeying the relation $d^2 = 0$. The cohomology group $H^2(G, M)$ is of particular relevance in constructing extensions of the group G by M.

It turns out that part of this formalism can be extended to more general magmas G that obey a different law than the associative law.

Let G be a magma obeying some equation E of the form $w_{E,1}(x_1, ..., x_n) = w_{E,2}(x_1, ..., x_n)$. We let $M = (M, +)$ be an abelian group that also has a linear magma operation

$$s \diamond t = as + bt$$

obeying E for some $a, b \in \mathrm{End}(M)$ in the endomorphism ring of M. Note that in such a linear magma, any word $w(s_1, ..., s_n)$ takes the form

$$w(s_1, ..., s_n) = \sum_{i=1}^{n} P_{w,i}(a, b)s_i$$

for some (non-commutative) polynomials $P_{w,i}(a, b)$ in a, b with natural number coefficients. For instance,

$$s \diamond s = (a + b)s$$
$$t \diamond (s \diamond s) = (ba + b^2)s + at$$
$$(t \diamond (s \diamond s)) \diamond t = (aba + ab^2)s + (a^2 + b)t$$
$$t \diamond ((t \diamond (s \diamond s)) \diamond t) = (baba + bab^2)s + (ba^2 + b^2 + a)t.$$

The law E is then obeyed when

$$P_{w_{E,1},i}(a, b) = P_{w_{E,2},i}(a, b)$$

for $i = 1, ..., n$. For instance, the law 1110,

$$x = y \diamond ((y \diamond (x \diamond x)) \diamond y) \tag{11.1}$$

would be obeyed if one has

$$baba + bab^2 = 1; \quad ba^2 + b^2 + a = 0. \tag{11.2}$$

A solution here would be provided by $(a, b) = (\phi, -1)$, where ϕ solves the golden ratio equation $\phi^2 = \phi + 1$.

We consider *extensions* of G by M, which are magmas with carrier $G \times M$ with an operation of the form

$$(x, s) \diamond (y, t) = (x \diamond y, as + bt + f(x, y)) \tag{11.3}$$

for some function $f : G \times G \to M$. An easy induction then shows that for any word $w(x_1, \ldots, w_n)$, one has

$$w((x_1, s_1), \ldots, (x_n, s_n)) = (w(x_1, \ldots, x_n), \sum_{i=1}^{n} P_{w,i}(a, b)x_i$$

$$+ \sum_{w_1 \diamond w_2 \leq w} Q_{w,w_1 \diamond w_2}(a, b) f(w_1(x_1, \ldots, x_n), w_2(x_1, \ldots, x_n)))$$

where $w_1 \diamond w_2$ ranges over all subterms of w that are not single variables, and $Q_{w,w_1 \diamond w_2}(a, b)$ is a suitable (noncommutative) monomial in a, b. For instance

$$(x, s) \diamond (x, s) = (x \diamond x, (a + b)s + f(x, x))$$

$$(y, t) \diamond ((x, s) \diamond (x, s)) = (y \diamond (x \diamond x), (ba + b^2)s + at + bf(x, x) + f(y, x \diamond x))$$

$$((y, t) \diamond ((x, s) \diamond (x, s))) \diamond (y \diamond t) = ((y \diamond (x \diamond x)) \diamond y,$$

$$(aba + ab^2)s + (a^2 + b)t + abf(x, x) + af(y, x \diamond x) + f(y \diamond (x \diamond x), y))$$

$$(y \diamond t) \diamond (((y, t) \diamond ((x, s) \diamond (x, s))) \diamond (y \diamond t)) = (y \diamond ((y \diamond (x \diamond x)) \diamond y),$$

$$(baba+bab^2)s+(ba^2+b^2+a)t+babf(x,x)+baf(y,x\diamond x)+bf(y\diamond(x\diamond x),y)+f(y,(y\diamond(x\diamond x))\diamond y)).$$

Assuming Equation (11.2), we conclude that this extension obeys the law Equation (11.1) if and only if one has

$$babf(x, x) + baf(y, x \diamond x) + bf(y \diamond (x \diamond x), y) + f(y, (y \diamond (x \diamond x)) \diamond y) = 0 \tag{11.4}$$

for all $x, y \in G$. More generally, an extension obeys a law E provided that

$$\sum_{w_1 \diamond w_2 \leq w_{E,1}} Q_{w_{E,1},w_1 \diamond w_2}(a, b) f(w_1(x_1, \ldots, x_n), w_2(x_1, \ldots, x_n))$$

$$= \sum_{w_1 \diamond w_2 \leq w_{E,2}} Q_{w_{E,2},w_1 \diamond w_2}(a, b) f(w_1(x_1, \ldots, x_n), w_2(x_1, \ldots, x_n))$$

for all $x_1, \ldots, x_n \in G$. We call f a *E-cocycle* if this equation holds, and denote the space of such E-cocycles as $Z^2_E(G, M)$. This is an abelian group, and each E-cocycle defines a magma on $G \times M$ obeying E. For instance, when $f = 0$ we obtain the direct product of the G and M magmas.

Given any function $g : G \to M$, one can define a bijection $(x, s) \mapsto (x, s + g(x))$ on $G \times M$, which conjugates the law Equation (11.3) to the law

$$(x, s) \diamond (y, t) = (x \diamond y, as + bt + f(x, y) + g(x \diamond y) - ag(x) - bg(y)).$$

Being conjugate, this new operation will obey E if and only if the original operation does. Thus if one defines a *coboundary* to be a function $f : G \times G \to M$ of the form $f(x, y) =$

$g(x \diamond y) - ag(x) - bg(y)$ for some $g : G \to M$, we can add a coboundary to an E-cocycle and still obtain a E-cocycle. So if we let $B^2(G, M)$ be the space of coboundaries, we see that $B^2(G, M)$ is a subgroup of $Z^2_E(G, M)$. We define the *E-cohomology* $H^2_E(G, M)$ to be the quotient

$$H^2_E(G, M) := Z^2_E(G, M)/B^2(G, M).$$

Observe that if E implies E', then $H^2_E(G, M)$ is a subgroup of $H^2_{E'}(G, M)$. Thus, to refute an implication $E \implies E'$, it suffices to locate a magma G and a linear magma M obeying both E and E' such that

$$H^2_E(G, M) \not\subset H^2_{E'}(G, M). \tag{11.5}$$

This leads to a computational approach to refutations, as these groups can be computed by linear algebra.

For instance, let us consider the law Equation (11.1) together with a putative consequence, equation 1629:

$$x = (x \diamond x) \diamond ((x \diamond x) \diamond x). \tag{11.6}$$

A simultaneous (linear) model for both Equation (11.1) and Equation (11.6) is given by carrier $G = M = \mathbb{F}_5$ with $x \diamond y = 3x - y$. Then the coboundaries $f : \mathbb{F}_5 \times \mathbb{F}_5 \to \mathbb{F}_5$ are of the form $f(x, y) = g(3x - y) - 3g(x) + g(y)$ for $g : \mathbb{F}_5 \to \mathbb{F}_5$, the 1110-cocycles solve the equation

$$3f(x, x) - 3f(y, 2x) - f(3y - 2x, y) + f(y, 3y - x) = 0$$

for $x, y \in \mathbb{F}_5$, and the 1629-cocycles solve the equation

$$f(2x, 0) - f(2x, x) = 0.$$

A function $g : \mathbb{F}_5 \to \mathbb{F}_5$ has vanishing derivative, $g(3x - y) - 3g(x) + g(y) = 0$, if and only if g is linear, which is a one-dimensional space; so, by the rank-nullity theorem, the space $B^2(G, M)$ of coboundaries is four-dimensional. One can check computationally that the space $Z^2_{1110}(G, M)$ is six-dimensional, so $H^2_{1110}(G, M)$ is two-dimensional. One can check numerically that it contains an element not in $H^2_{1629}(G, M)$, leading to a finite counterexample on the 25-element carrier $G \times M$ to the implication of 1629 from 1110.

Remark 4. *In the case the associative law (and taking $a = b = 1$), the cocycle law becomes the familiar*

$$f(x, y) + f(x \diamond y, z) = f(x, y \diamond z) + f(y, z)$$

and we recover the usual group cohomology (if G is a group). The same occurs for Tarski's law 543 $x = y \diamond (z \diamond (x \diamond (y \diamond z)))$.

Remark 5. *One can interpret the above cohomology group in terms of a partial chain complex*

$$0 \to C^0(G, M) \xrightarrow{d^0} C^1(G, M) \xrightarrow{d^1} C^2(G, M) \xrightarrow{d^2_E} C^n(G, M)$$

where the zeroth coboundary map $d^0 : C^0(G, M) \to C^1(G, M)$ is the zero map, the first coboundary map $d : C^1(G, M) \to C^2(G, M)$ (which does not depend on the equation E) is defined by the formula

$$d^1 vf(x, y) := f(x \diamond y) - (f(x) \diamond f(y)) = f(x \diamond y) - af(x) - bf(y)$$

and the second coboundary map $d^2_E : C^2(G, M) \to C^n(G, M)$ (which does depend on E) is defined by the formula

$$d^2_E f(x_1, \ldots, x_n) := \sum_{w_1 \diamond w_2 \leq w_{E,1}} Q_{w_{E,1}, w_1 \diamond w_2}(a, b) f(w_1(x_1, \ldots, x_n), w_2(x_1, \ldots, x_n))$$

$$- \sum_{w_1 \diamond w_2 \leq w_{E,2}} Q_{w_{E,2}, w_1 \diamond w_2}(a,b) f(w_1(x_1, \ldots, x_n), w_2(x_1, \ldots, x_n)).$$

The fact that coboundaries are cocycles can then be rewritten as the chain complex relations $d^1 d^0 = 0$, $d_E^2 d^1 = 0$. *The group* $H_E^2(G,M)$ *is then just the second cohomology group of this chain complex. The first cohomology group* $H_E^1(G,M)$ *is the kernel of* d^1, *or equivalently the abelian group of magma homomorphisms from the magma* G *to the linear magma* M.

When E *is the associative law, this partial chain complex can be extended to the usual group cohomology chain complex; however, it is not clear if any such extension exists for a general law* E.

Remark 6. *Suppose that* $G = M = \mathbb{F}_p$ *is a field of prime order, and* a, b *are coefficients in that field, with the magma operation on* G *also given in a linear form* $x \diamond y = a'x + b'y$. *Then one can view a cocycle* $f : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$ *as a bivariate polynomial of degree at most* $2p-2$ *with coefficients in* $\mathbb{F}_p$. *The coboundary maps* d, d_E *preserve degree, and so one can decompose (or "grade") the cohomology group* $H_E^2(G,M)$ *as* $\bigoplus_{d=0}^{2p-2} H_E^2(G,M)_d$, *where* $H_E^2(G,M)_d$ *are defined as with* $H_E^2(G,M)$ *but with the cocycles and coboundaries required to be homogeneous polynomials of degree at most* d. *To disprove an implication* $E \implies E'$, *it thus suffices to establish a non-inclusion* $H_E^2(G,M)_d \not\subset H_{E'}^2(G,M)_d$ *at a single degree* d, *which may be slightly easier computationally, and also provides for more compactly described counterexamples.*

Chapter 12

Weak central groupoids

In this chapter we study weak central groupoids Theorem 2.30,

$$x = (y \diamond x) \diamond (x \diamond (z \diamond y)). \tag{12.1}$$

The first observation is that this law is equivalent to its dual:

Lemma 12.1 (1485 equivalent to 2162)**.** *Theorem 2.30 is equivalent to the dual law*

$$x = ((y \diamond z) \diamond x) \diamond (x \diamond y) \tag{12.2}$$

(equation 2162).

Proof. It suffices to prove that Equation (12.1) implies Equation (12.2). Write $w = y \diamond z$, then from Equation (12.1) we can write $z = z_1 \diamond z_2$ with $z_1 = z \diamond z$ and $z_2 = z \diamond (z \diamond z)$, and then by Equation (12.1)

$$y = (z_2 \diamond y) \diamond (y \diamond (z_1 \diamond z_2)) = (z_2 \diamond y) \diamond w.$$

From another application of Equation (12.1) we have

$$x = (w \diamond x) \diamond (x \diamond ((z_2 \diamond y) \diamond w)) = ((y \diamond z) \diamond x) \diamond (x \diamond y)$$

as required. □

Given a weak central groupoid G, define a directed graph with vertices in G by declaring $x \to y$ if and only if $y = x \diamond z$ for some z. There is an equivalent characterization of this graph:

Lemma 12.2 (Equivalent characterization of graph)**.** *One has $x \to y$ if and only if $x = w \diamond y$ for some w.*

Proof. If $x \to y$ then $y = x \diamond z$, then writing $z = z_1 \diamond z_2$ as before we obtain

$$x = (z_2 \diamond x) \diamond (x \diamond (z_1 \diamond z_2)) = (z_2 \diamond x) \diamond y$$

giving the forward implication. The backwards implication follows by duality. □

Define a *good path* in G to be a path of the form

$$x \to x \diamond y \to y$$

for some $x, y \in G$ (we allow loops). By the above lemma, this is a path in G. The following claims are clear from definition and the above lemma:

Claim 1: If $x, y \in G$ then there is exactly one good path $x \to z \to y$ from x to y.

Claim 2: Any edge $x \to y$ in the directed graph is the initial segment of some good path $x \to y \to z$.

Claim 3: Any edge $x \to y$ in the directed graph is the final segment of some good path $w \to x \to y$.

Slightly more non-trivial is

Lemma 12.3 (Claim 4)**.** *If $a \to b \to c \to d \to e \to a$ is a 5-cycle in the directed graph, and $a \to b \to c$ and $c \to d \to e$ are good paths, then $b \to c \to d$ is also good.*

Proof. If $a \to b \to c$ is good then $b = a \diamond c$; if $c \to d \to e$ is good then $d = c \diamond e$; and if $e \to a$ then $a = e \diamond z$ for some z by definition. By Equation (12.2) we then have

$$c = ((e \diamond z) \diamond c) \diamond (c \diamond e) = b \diamond d$$

so $b \to c \to d$ is good. □

Conversely, we have

Lemma 12.4 (Reversing the claims)**.** *Let G be a directed graph, with some paths of length two in the graph designated as "good", in such a way that Claims 1-4 hold. Then there is a weak central groupoid structure on the vertices of G such that the good paths are precisely the paths of the form $x \to x \diamond y \to y$.*

Proof. Define an operation $\diamond : G \times G \to G$ by defining $x \diamond y$ to be the unique vertex z for which one has a good path $x \to z \to y$; this is well-defined by Claim 1, and by Claims 2-3, the property $x \to y$ holds if and only if $y = x \diamond z$ for some z, and also if and only if $x = w \diamond y$ for some w. In particular, for all x, y, z, we have a 5-cycle

$$y \to y \diamond x \to x \to x \diamond (z \diamond y) \to (z \diamond y) \to y$$

with $y \to y \diamond x \to x$ and $x \to x \diamond (z \diamond y) \to (z \diamond y)$ good, hence by Claim 4 we have Equation (12.1) as required. □

This gives us a graph-theoretical route to construct weak central groupoids. We first introduce a weaker version of Claim 1:

Claim 1': If $x, y \in G$ then there is at least one good path $x \to z \to y$ from x to y.

Let us call a *relaxed weak central groupoid* a directed graph with some paths of length 2 designated as "good" that obeys Claims 1', 2, 3, 4.

We also define a *partial weak central groupoid* to be a directed graph with some paths of length 2 that obeys Claim 4 as well as the following opposite weakening of Claim 1:

Claim 1": If $x, y \in G$ then there is at most one good path $x \to z \to y$ from x to y.

If we can upgrade Claim 1" to Claim 1, and we also have Claim 2 and Claim 3, then we call this a *complete weak central groupoid*, and by the previous proposition this is in correspondence with Equation (12.1).

Let G_0 be a relaxed weak central groupoid. A *partial extension* of G_0 is a partial weak central groupoid G with a "projection map" $\pi : G \to G_0$, which is a homomorphism in the sense that the image $\pi(x) \to \pi(y)$ of any edge $x \to y$ in G is an edge in G_0, the image $\pi(x) \to \pi(y) \to \pi(z)$ of any good path $x \to y \to z$ in G is a good path in G_0, and the image $\pi(x) \to \pi(y) \to \pi(z)$ of any bad path $x \to y \to z$ in G is a bad path in G_0. Note that Claim 4 for G is then automatic from Claim 4 of the base G_0. The extension is *complete* if the partial weak central groupoid is complete.

We have the following convenient completion property:

Proposition 12.5 (Completion property)**.** *Let G_0 be a directed graph obeying claims 1', 2, 3, 4. Then any finite partial extension of G_0 with carrier $G_0 \times \mathbb{N}$ (and projection map $\pi(a,n) = a$) can be completed to a complete extension.*

Proof. By the previous comments, we can ignore Claim 4 as it is automatic, and focus on completing the partial weak central groupoid on G to a complete weak central groupoid by ensuring Claims 1, 2, 3 hold. By the usual greedy algorithm, it suffices to show that any individual failure of Claim 1, 2 or 3 can be resolved by adding some finite number of edges to the graph.

Suppose first that Claim 2 fails, that is to say the partial weak central groupoid contains an edge $(a,n) \to (b,m)$ that is not the initial segment of any good path. Since the base relaxed weak central groupoid G_0 obeys Claim 2, we can find a good path $a \to b \to c$ in the base. We then pick a natural number l not previously occurring in the partial weak central groupoid, and adjoin the edge $(b,m) \to (c,l)$ to that partial weak central groupoid. All new paths created in this way are declared good or bad depending on whether their images in G_0 are good or bad, in particular $(a,n) \to (b,m) \to (c,l)$ is good. This can be checked to still be a partial extension of G_0 (no violation of Claim 1" is created), and now Claim 2 is resolved at for the edge $(a,n) \to (b,m)$. A similar argument permits one to resolve any violations of Claim 3.

If Claim 1 is violated, then there is a pair $(a,n), (b,m)$ that currently has no good path of length two in the partial weak central groupoid. As the base relaxed weak central groupoid G_0 obeys Claim 1', we can find a good path $a \to c \to b$ in G_0. We then pick a natural number l not previously occurring, and adjoin the edges $(a,n) \to (c,l) \to (b,m)$. All new paths created in this way are declared good or bad depending on whether their images in G_0 are good or bad, in particular $(a,n) \to (c,l) \to (b,m) \to (c,l)$. One can check that this is still a partial extension of G_0 (no violation of Claim 1" is created), and now Claim 1 is resolved at the pair $(a,n), (b,m)$. □

Theorem 12.6 (1485 does not imply 1483)**.** *Theorem 2.30 does not imply any of the following laws:*

- *Equation 3457:* $x \diamond x = x \diamond ((x \diamond x) \diamond y)$.
- *Equation 2087:* $x = ((y \diamond x) \diamond x) \diamond (x \diamond x)$.
- *Equation 2124:* $x = ((y \diamond y) \diamond x) \diamond (x \diamond x)$.
- *Equation 3511:* $x \diamond y = x \diamond ((x \diamond y) \diamond x)$.

Proof. Computer check reveals that the carrier $G_0 = \{0,1,2,3,4\}$ with incidence matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

is a relaxed weak central groupoid if we declare the paths $0 \to 0 \to 0$, $0 \to 0 \to 1$, $0 \to 1 \to 1$, $1 \to 0 \to 0$, $1 \to 1 \to 0$, $1 \to 1 \to 1$ to be bad, and all other paths in the directed graph to be good. We can also check the following axioms:

- Anti-3457: There exist x, y, z, w with $x \to z \to x$, $z \to w \to y$ both good, and $x \to z \to w$ bad. (One can take $x = 1$, $y = 4$, $z = 0$, $w = 0$.)
- Anti-2087: There exist x, y, z, w, u with $y \to z \to x$, $z \to w \to x$, and $x \to u \to x$ good, and $w \to x \to u$ is bad. (One can take $x = 1, y = 2$, $z = 4$, $w = 1$, $u = 0$.)

- Anti-2124: There exists x, y, z, w, u with $y \to z \to y$, $z \to w \to x$ and $x \to u \to x$ good, and $w \to x \to u$ bad. (One can take $x = 1$, $y = 2$, $z = 4$, $w = 1$, $u = 0$.)
- Anti-3511: There exists x, y, z, w with $x \to z \to y$ and $z \to w \to x$ good, and $x \to z \to w$ bad. (One can take $x = 1$, $y = 3$, $z = 1$, $w = 0$.)

Let G_* be a finite partial extension of G_0 to be chosen later. By Theorem 12.5, we can complete this to a complete weak central groupoid G with carrier $G_0 \times \mathbb{N}$. Depending on how we choose G_*, we can ensure that this G refutes one of the four laws 3457, 2087, 2124, 3511:

- Refuting 3457: Let x, y, z, w be as in the claim Anti-3457, then select G_* to be the directed graph with edges $(x,0) \to (z,2) \to (x,0) \to (z,2) \to (w,3) \to (y,1)$. One can check that this is a partial extension, and that G will refute 3457 with x, y replaced by $(x,0), (y,1)$.
- Refuting 2087: Let x, y, z, w, u be as in the claim Anti-2087, then select G_* to be the directed graph with edges $(y,1) \to (z,2) \to (x,0)$ and $(z,2) \to (w,3) \to (x,0) \to (u,4) \to (x,0)$. One can check that this is a partial extension, and that G will refute 2087 with x, y replaced by $(x,0), (y,1)$.
- Refuting 2124: Let x, y, z, w, u be as in the claim Anti-2124, then select G_* to be the directed graph with edges $(y,1) \to (z,2) \to (y,1)$ and $(z,2) \to (w,3) \to (x,0) \to (u,4) \to (x,0)$. One can check that this is a partial extension, and that G will refute 2124 with x, y replaced by $(x,0), (y,1)$.
- Refuting 3511: Let x, y, z, w be as in the claim Anti-3511, then select G_* to be the directed graph with edges $(x,0) \to (z,2) \to (y,1)$ and $(z,2) \to (w,3) \to (x,0)$. One can check that this is a partial extension, and that G will refute 3511 with x, y replaced by $(x,0), (y,1)$.

□

12.1 Twisting a weak central groupoid

Occasionally, an equational law is preserved under a "twist" operation in which one replaces the magma operation $x \diamond y$ by $x \diamond' y := Tx \diamond Uy$ for some automorphisms T, U of the magma G that obey additional relations. In the case of the weak central groupoid law Equation (12.1), we see that

$$(y \diamond' x) \diamond' (x \diamond' (z \diamond' y)) = (T^2 y \diamond TUx) \diamond (UTx \diamond (UTUz \diamond U^3 y))$$

so if T is an automorphism of order 5 and $U = T^{-1}$ (so that $T^2 = U^3$), we conclude that this twisted magma is also a weak central groupoid. This can be used to generate further counterexamples. For instance, let M_2 be the order two weak central groupoid with carrier $\mathbb{F}_2$ and with the NAND operation $x \diamond y := 1 - xy$; this can easily be verified to be a weak central groupoid. It does not have any nontrivial automorphisms, but its fifth power $M_2^{\otimes 5}$ has a cyclic shift T of order 5: $T((x_i)_{i \in \mathbb{Z}/5\mathbb{Z}}) = (x_{i+1})_{i \in \mathbb{Z}/5\mathbb{Z}}$. If we twist $M_2^{\otimes 5}$ by T and T^{-1}, we obtain a weak central groupoid M with carrier $\mathbb{F}_2^5$ and magma operation

$$(x_i)_{i \in \mathbb{Z}/5\mathbb{Z}} \diamond (y_i)_{i \in \mathbb{Z}/5\mathbb{Z}} = (1 - x_{i+1} y_{i-1})_{i \in \mathbb{Z}/5\mathbb{Z}}.$$

In particular, if $x = (x_i)_{i \in \mathbb{Z}/5\mathbb{Z}}$, then

$$x \diamond x = (1 - x_{i+1} x_{i-1})_{i \in \mathbb{Z}/5\mathbb{Z}}$$

and

$$(x \diamond x) \diamond (x \diamond x) = (1 - (1 - x_{i+2}x_i)(1 - x_i x_{i-2}))_{i \in \mathbb{Z}/5\mathbb{Z}}$$

which by the laws of boolean algebra simplify to

$$(x \diamond x) \diamond (x \diamond x) = (x_i(x_{i-2} + x_i + x_{i+2}))_{i \in \mathbb{Z}/5\mathbb{Z}}$$

from which one can easily refute equation 151,

$$x = (x \diamond x) \diamond (x \diamond x).$$

Informally, the reason for this is that equation 151 has a different semigroup twist symmetries: $T^2 = 1, T = U^{-1}$ instead of $T^5 = 1, T = U^{-1}$.

Chapter 13

Equation 677

In this chapter we study finite magmas that obey equation 677,

$$x = y \diamond (x \diamond ((y \diamond x) \diamond y)) \tag{13.1}$$

for all x, y, and whether this implies equation 255,

$$x = ((x \diamond x) \diamond x) \diamond x. \tag{13.2}$$

Using the usual notation $L_y x = y \diamond x$, $R_y x = x \diamond y$, $Sx = x \diamond x$, we can rewrite equation 677 as

$$x = L_y L_x L_{L_y x} y = L_y(x \diamond R_y L_y x) \tag{13.3}$$

and 255 as

$$x = (Sx \diamond x) \diamond x.$$

Lemma 13.1 (Basic properties of 677 magma)**.** *Let M be a finite magma obeying (13.1).*

- *(i) The left multiplication operators $L_y : M \to M$ are all invertible, with $L_y^{-1} x = x \diamond R_y L_y x$.*
- *(ii) If $x, y \in M$ and $y \diamond x = x$, then $y = Sx \diamond x$. In particular, 255 holds if and only if the equation $y \diamond x = x$ is solvable for every x.*
- *(iii) For all $x, y \in M$, we have $x = L_y x \diamond R_y L_y^2 x$.*

Proof. From (13.3) we see that L_y is surjective, hence invertible on finite magmas, giving (i) (the formula for $L_y^{-1} x$ being immediate from (13.3)).

For (ii), using the fact that $L_y x = x$, (i) becomes $x = x \diamond R_y x = L_x L_x y$, then, using the invertibility of L_x given by (i) we have

$$y = L_x^{-1} L_x^{-1} x \overset{(i)}{=} L_x^{-1}(x \diamond R_x L_x x) = L_x^{-1}(L_x R_x L_x x) = R_x L_x x = Sx \diamond x.$$

For (iii), we apply (i) with x replaced by $L_y x$. □

We have the following equivalent characterizations of 255:

Lemma 13.2. *Let M be a finite magma obeying (13.1), and let $x \in M$. Then the following are equivalent:*

- *(i) 255 holds for x, that is to say $R_x(Sx \diamond x) = x$.*
- *(ii) The equation $R_x y = x$ has the unique solution $y = Sx \diamond x$.*
- *(iii) The equation $R_x y = x$ has a solution.*
- *(iv) The equation $R_x L_x z = x$ has a solution.*
- *(v) The equation $L_x R_x z = z$ has a solution.*
- *(vi) The equation $R_x L_x y = y$ has a solution.*
- *(vii) The equation $L_x S y = y$ has a solution.*

Proof. Clearly (ii) implies (i), which implies (iii). If (iii) holds, we apply (13.3) to conclude that

$$y \diamond x = x = y \diamond (x \diamond (x \diamond y))$$

and hence by left invertibility

$$x = x \diamond (x \diamond y).$$

On the other hand, from (13.1) with y replaced by x we have

$$x = x \diamond (x \diamond (Sx \diamond x))$$

and hence by left invertibility $y = Sx \diamond x$, giving (ii).

From left cancellativity we see that (v) and (vi) are equivalent, as are (iii) and (iv).

If (vii) holds, then $L_x L_y y = y$, but from (13.3) we have $y = L_x L_y R_x L_x y$, so (vi) follows from left-cancellativity; the converse implication follows by reversing the steps. If (v) holds, then we have $L_x L_z x = z$, but from (13.3) one has $z = L_x L_z R_x L_x z$, giving the (iv) by left-cancellativity; the converse implication follows by reversing the steps. □

This for instance gives the implication for linear magmas:

Lemma 13.3 (No linear counterexamples)**.** *Suppose we have a finite magma M obeying 677 which is linear in the sense that M is an abelian group and $x \diamond y = \alpha x + \beta y + c$ for some endomorphisms $\alpha, \beta : M \to M$ and constant c. Then M obeys 255.*

Proof. By the previous lemma, it suffices to show that right multiplication R_x is surjective, or equivalently injective by finiteness. If this is not the case, then we can find distinct y, y' such that $R_x y = R_x y'$, hence $L_y x = L_{y'} x$. But in this linear model, L_y and $L_{y'}$ differ by a constant, hence we have $L_y = L_{y'}$. Applying (13.3) we have

$$L_y L_x L_{L_y x} y = x = L_y L_x L_{L_y x} y'$$

and hence by left-invertibility $y = y'$, a contradiction. □

In fact the argument gives a stronger obstruction to refuting 255:

Lemma 13.4 (No counterexamples via linear extension)**.** *Suppose that we have a magma with carrier $G \times M$ obeying 677, where G already is a magma obeying 677 and 255, M is an abelian group, and the multiplication operation on $G \times M$ is of the form*

$$(x, s) \diamond (y, t) = (x \diamond y, \alpha_{x,y} s + \beta_{x,y} t + c_{x,y})$$

for some endomorphisms $\alpha_{x,y}, \beta_{x,y} : M \to M$ and constants $c_{x,y}$. Then $G \times M$ obeys 255.

Proof. By Theorem 13.1, it suffices to show that for any (y,t), the equation $(x,s) \diamond (y,t) = (y,t)$ is solvable. Since G already obeys 255, we know that we can find x such that $x \diamond y = y$, so it suffices to show that the operation $s \mapsto \alpha_{x,y} s + \beta_{x,y} t + c_{x,y}$ is surjective, or equivalently injective. If this were not the case, then we could find s, s' such that $\alpha_{x,y} s = \alpha_{x,y} s'$, and hence $L_{(x,s)}(y,t') = L_{(x,s')}(y,t')$ for all $t' \in M$. Since

$$x \diamond y = y = x \diamond (y \diamond ((x \diamond y) \diamond x))$$

from (13.1), we have $y = y \diamond ((x \diamond y) \diamond x)$, and hence $L_{(y,t)} L_{L_{(x,s)}(y,t)}(x,s)$ is of the form (y,t') for some t', and similarly with (x,s) replaced by (x,s'). We conclude that

$$L_{(x,s)} L_{(y,t)} L_{L_{(x,s)}(y,t)}(x,s) = (y,t) = L_{(x,s)} L_{(y,t)} L_{L_{(x,s)}(y,t)}(x,s')$$

and hence by left invertibility $s = s'$, a contradiction. □

Linear models $x \diamond y = \alpha x + \beta y + c$ on the finite field F_p turn out to be classified into two types:

- (Type 1) $\alpha = 1 - \beta$, β is a primitive tenth root of unity, and $c = 0$. (These models are also translation-invariant.)
- (Type 2) α is a primitive third root of unity, c is arbitrary, and β solves $\beta^3 + \beta + 1 = -\alpha$ and $\beta^4 + \beta^3 + 2\beta^2 + 2\beta + 1 = 0$.

An example of a Type I model is $x \diamond y = 2x - y$ on F_5. Examples of Type II models include $x \diamond y = 4x + 3y$ and $x \diamond y = 4x + y$ on F_7. An exceptional class of Type II models are $x \diamond y = 5x - 4y + c$ on F_{31}, these are the only Type II models that are translation-invariant and do not have idempotents (if $c \neq 0$).

13.1 A finite non-right-cancellative example

Suppose G is already a 677 magma, and to each pair $x, y \in G$ we assign a binary operation $\diamond_{x,y} : M \times M \to M$ such that one has the functional equation

$$s = t \diamond_{y, L_y^{-1} x} (s \diamond_{x,(y \diamond x) \diamond y} ((t \diamond_{y,x} s) \diamond_{y \diamond x, y} t)) \tag{13.4}$$

for all $x, y \in G$, then the operation

$$(x,s) \diamond (y,t) := (x \diamond y, s \diamond_{x,y} t)$$

is easily seen to be a 677 magma. It is right-injective if G and all of the $\diamond_{y,x}$ are right-injective.

Suppose M is a field that admits a primitive cube root of unity ω as well as a primitive fifth root of unity ζ (for instance, M could be a field of order 16). Then the three operations

$$s \diamond^0 t := s - \zeta(t - s)$$

$$s \diamond^+ t := t$$

$$s \diamond^- t := s - \omega(t - s)$$

can easily be seen to obey the identities

$$s = t \diamond^0 (s \diamond^0 ((t \diamond^0 s) \diamond^0 t))$$

$$s = t \diamond^+ (s \diamond^+ ((t \diamond^- s) \diamond^- t))$$
$$s = t \diamond^- (s \diamond^- ((t \diamond^+ s) \diamond^+ t))$$

for all t, s.

Now suppose that G is also a field with a primitive fifth root of unity β (so that $\beta = \beta^4$ is a quadratic residue), but -1 and $\beta + 1$ are non-zero quadratic non-residues (for instance, G could be the field of order 31, with $\beta = 2$). If we define $x \diamond y = x - \beta(y - x)$, and then define $\diamond_{x,y}$ to be $\diamond^0$ when $y = x$, $\diamond^+$ when $y - x$ is a non-zero quadratic residue, and $\diamond^-$ when $y - x$ is a non-zero quadratic non-residue, one can then check that (13.4) holds. Since $\diamond^0$ is not right-cancellative, this gives a finite 677 magma that is not right-cancellative.

13.2 The free 677 magma

In this section we construct the free 677 magma $M_{X,677}$ generated by some set of generators X. First let M_X be the free magma generated X with operation given by pairing $x, y \mapsto (x, y)$; one can think of elements of M_X as finite trees with leaves in X. If $w = (x, y)$ we write $x = w_L$ and $y = w_R$ for the left and right components of w; we also define w_{LL}, w_{LR}, etc. iteratively if they are defined, for instance if $w = ((x, y), z)$ then $w_{LR} = y$. We define a partial order $<$ on M_X by declaring $w < w'$ if w is a subtree of w', thus $w < w'$ if one of $w \leq w'_L$, $w \leq w'_R$ holds.

We define an operation $\diamond$ recursively on M_X by the following rule:

- If $x, y \in M_X$ is such that $x < y = (y_L, (x \diamond y_L) \diamond x)$, then $x \diamond y := y_L$. Otherwise, $x \diamond y = (x, y)$.

Note that to define $x \diamond y$, one only needs to be able to compute $x' \diamond y'$ for $y' < y$. Since there are no infinite descending chains in the partial order $<$, we see that $\diamond$ is well-defined. By construction, we observe the following properties:

Lemma 13.5 (Properties of operation)**.** *Let $x, y \in M_X$ be such that $x \diamond y = z$. Then either*

$$x, y < z = (x, y)$$

or

$$x, z < y = (z, (x \diamond z) \diamond x).$$

In particular, x is strictly upper bounded by one of y, z.

Next, we observe

Lemma 13.6 (Additional property)**.** *If $x, y \in M_X$, then*

$$x \diamond ((y \diamond x) \diamond y) = (x, (y \diamond x) \diamond y).$$

Proof. Write $z := y \diamond x$, $u = z \diamond y$, $v = x \diamond u$. Our task is to show that $v = (x, u)$.

From Theorem 13.5 we know that y is upper bounded by one of z, x, z is upper bounded by one of u, y, and x is upper bounded by one of u, v. So out of x, y, z, u, v, the only elements that can be maximal in this set are u and v. If v is maximal, then by Theorem 13.5 we have $v = (x, u)$ as required, hence we may assume for contradiction that u is maximal. From Theorem 13.5, this implies that $u = (z, y)$ and $u = (u_L, (x \diamond u_L) \diamond x)$, hence $u_L = z$ and $y = (x \diamond z) \diamond x$.

From Theorem 13.5, x is upper bounded by one of $x \diamond z$ and z, and $x \diamond z$ is upper bounded by one of y and x. We also recall that y was upper bounded by one of z, x. We conclude that out of $x, y, z, x \diamond z$, the only one that can be maximal is z. In particular z is not bounded by x, hence by Theorem 13.5 $z = (y, x)$. z is also not bounded by $x \diamond z$, hence by Theorem 13.5 $x \diamond z = z_L = y$, hence $y = y \diamond x = z$, contradicting the fact that y was not maximal. This gives the required contradiction. □

Corollary 13.7. *The operation* $\diamond$ *obeys* (13.1).

Proof. By the previous lemma and definition of $\diamond$, it suffices to show that $y < (x, (y \diamond x) \diamond y)$. Defining z, u, v as before, this amounts to showing that $y < v$. We already have $v = (x, u)$, hence by Theorem 13.5 $x < v$. Also recall that y is bounded by one of x, z, and z is bounded by one of y, u. Since u is also bounded by v, we obtain the claim. □

Corollary 13.8. *Let* $M_{X,677}$ *be the magma generated by* X *with operation* $\diamond$. *Then* $M_{X,677}$ *is the free magma for* (13.1) *generated by* X.

Proof. By the previous corollary, it suffices to show that every function $f : X \to M$ into a 677 magma M can be extended to a unique homomorphism $\varphi_f : M_{X,677} \to X$. Uniqueness is clear since $M_{X,677}$ is generated by X. For existence, we define φ_f by first extending f to the unique homomorphism from M_X to X (using the pairing map) and then restricting to $M_{X,677}$. To verify the homomorphism property $\varphi_f(x \diamond y) = \varphi_f(x) \diamond \varphi_f(y)$, we are already done when $x \diamond y = (x, y)$. The only remaining case is when $x \diamond y = y_L$ and $x < y = (y_L, (x \diamond y_L) \diamond x)$. If we assume inductively that the homomorphism property $\varphi_f(x' \diamond y') = \varphi_f(x') \diamond \varphi_f(y')$ has already been verified for $y' < y$, then we have

$$\varphi_f(y) = \varphi_f(y_L) \diamond \varphi_f(y_R) = \varphi_f(y_L) \diamond (\varphi_f(x \diamond y_L) \diamond \varphi_f(x)) = \varphi_f(y_L) \diamond ((\varphi_f(x) \diamond \varphi_f(y_L)) \diamond \varphi_f(x))$$

and the claim now follows since M obeys 677. □

By construction, we have $x \diamond y > y$ or $x \diamond y < y$ for any x, y. In particular, $M_{X,677}$ does not obey (13.2).

Chapter 14

Equation 854

In this chapter we study magmas that obey Theorem 2.28, thus

$$x = x \diamond ((y \diamond z) \diamond (x \diamond z)) \tag{14.1}$$

for all x, y, z. In particular we have

$$x = x \diamond (x \diamond z)^2;$$

substituting $z = (x \diamond x)^2$ we have in particular that

$$x = x \diamond x^2. \tag{14.2}$$

We then have

$$\begin{aligned} y &= y \diamond ((x \diamond y) \diamond y^2) \\ &= (y \diamond y^2) \diamond ((x \diamond y) \diamond y^2) \end{aligned}$$

and thus by another application of Equation (14.1) we conclude the useful law

$$(x \diamond y) \diamond y = x \diamond y \tag{14.3}$$

(equation 378). We introduce the notation $y \to x$ to denote the relation that $x = z \diamond y$ for some z, then from Equation (14.3) we see that

$$y \to x \iff x = x \diamond y. \tag{14.4}$$

From Equation (14.1) we have

$$(y \diamond z) \diamond (x \diamond z) \to x \tag{14.5}$$

for all x, y, z.

Now let X be an alphabet, and M_X the free magma. We let Γ be the theory consisting just of the law Equation (14.1), then as in Theorem 10.2 we have the equivalence relation $\sim$ on M_X defined by setting $w \sim w'$ iff $\Gamma \models w \simeq w'$, then $M_X/\sim$ is a free magma for Γ. We can then also define a directed graph on M_X by declaring $w' \to w$ if $w \sim w'' \diamond w'$ for some w'', or equivalently (by applying Equation (14.4) to $M_X/\sim$) that $w \sim w \diamond w'$.

Call a word w *irreducible* if it is not of the form $w = w_1 \diamond w_2$ with $w_2 \to w_1$, and *reducible* otherwise. Clearly if a word $w = w_1 \diamond w_2$ is reducible, then it is equivalent to the shorter word w_1. Iterating, we conclude that every word is equivalent to an irreducible word. Such a word is either a generator in X, or else a product $w_1 \to w_2$ with $w_2 \not\to w_1$.

We can describe the words equivalent to an irreducible word as follows.

Theorem 14.1 (Description of equivalence)**.** *Let w be an irreducible word, and let w' be a word equivalent to w.*

(i) If w is a product $w = w_1 \diamond w_2$, then w' takes the form

$$w' = (((w'_1 \diamond w'_2) \diamond v_1) \diamond ... \diamond v_n)$$

for some $w'_1 \sim w_1$, $w'_2 \sim w_2$, some $n \geq 0$, and some words $v_1, ..., v_n$ such that for all $0 \leq i < n$, v_{i+1} is of the form

$$v_{i+1} \sim (y_i \diamond z_i) \diamond (x_i \diamond z_i)$$

for some x_i, y_i, z_i with

$$x_i \sim (((w'_1 \diamond w'_2) \diamond v_1) \diamond ... \diamond v_i).$$

In particular, $v_{i+1} \to x_i$.

(ii) Similarly, if w is a generator, then w' takes the form

$$w' = ((w \diamond v_1) \diamond ... \diamond v_n)$$

for some $n \geq 0$, and some words $v_1, ..., v_n$ such that for all $0 \leq i < n$, v_{i+1} is of the form

$$v_{i+1} \sim (y_i \diamond z_i) \diamond (x_i \diamond z_i)$$

for some x_i, y_i, z_i with

$$x_i \sim ((w \diamond v_1) \diamond ... \diamond v_i).$$

In particular, $v_{i+1} \to x_i$.

Conversely, any word of the above forms is equivalent to w.

Proof. We just verify claim (i), as claim (ii) is similar. The converse direction is clear from Equation (14.5) (after quotienting down to $M_X/\sim$), so it suffices to prove the forward claim. By Theorem 1.8, it suffices to prove that the class of words described by (i) is preserved by any term rewriting operation, in which a term in the word is replaced by an equivalent term using Equation (14.1). Clearly the term is in w'_1 or w'_2 then the form of the word is preserved, and similarly if the term is in one of the v_i. The only remaining case is if we are rewriting a term of the form

$$x_i = (((w'_1 \diamond w'_2) \diamond v_1) \diamond ... \diamond v_i).$$

If $i > 0$ we can rewrite this term down to x_{i-1}, and this still preserves the required form (decrementing n by one). If $i = 0$ then we cannot perform such a rewriting because of the irreducibility of $w_1 \diamond w_2$ and hence $w'_1 \diamond w'_2$. Finally, we can rewrite x_i to $x_i \diamond v$ where v is of the form

$$v_i = (y \diamond z) \diamond (x_i \diamond z),$$

and after some relabeling we are again of the required form (now incrementing n by one). □

We have two useful corollaries:

Corollary 14.2 (Unique factorization)**.** *Two irreducible words w, w' are equivalent if and only if they are either the same generator of X, or are of the form $w = w_1 \diamond w_2$, $w' = w'_1 \diamond w'_2$ with $w_1 \sim w'_1$ and $w_2 \sim w'_2$.*

Proof. Immediate from Theorem 14.1. □

Corollary 14.3 (Description of graph)**.** *If w, w' are words, then $w' \to w$ holds if and only if $w' \sim (Y \diamond Z) \diamond (w \diamond Z)$ for some words Y, Z.*

Proof. By replacing w, w' with irreducible equivalents, we may assume without loss of generality that w, w' are irreducible. By hypothesis, w is equivalent to $w \diamond w'$. The claim now follows from Theorem 14.1. □

We can now prove some anti-implications.

Theorem 14.4 (854 does not imply 3316, 3925)**.** *The laws*

$$x \diamond y = x \diamond (y \diamond (x \diamond y)) \tag{14.6}$$

and

$$x \diamond y = (x \diamond (y \diamond x)) \diamond y \tag{14.7}$$

are not implied by Theorem 2.28.

Proof. We work in the free group M_X on two generators $X = \{x, y\}$. It suffices to show that

$$x \diamond y \nsim x \diamond (y \diamond (x \diamond y))$$

and

$$x \diamond y \nsim (x \diamond (y \diamond x)) \diamond y.$$

We begin with the first claim. Suppose this were not the case, then by Theorem 14.2 one of the following statements must hold:

- (i)
$$y \to x$$
.
- (ii)
$$(y \diamond (x \diamond y)) \to x$$
.
- (iii)
$$y \diamond (x \diamond y) \sim y.$$

If (i) holds, then we have $x \diamond y = x$ (Equation 4) in $M_X/\sim$, hence in every magma obeying Theorem 2.28. But we have examples of such magmas in which this fails.

Similarly, if (iii) holds, then $y \diamond (x \diamond y) = y$ (Equation 10) holds in $M_X/\sim$, hence in every magma obeying Theorem 2.28. But we have examples of such magmas in which this fails.

Finally, if (ii) holds, then the claim

$$x \diamond y \sim x \diamond (y \diamond (x \diamond y))$$

to refute simplifies to

$$x \diamond y \sim x$$

and we are back to (i), which we already know not to be the case.

For the latter equation, we similarly have the cases

- (iv)
$$y \to x$$
.
- (v)
$$y \to x \diamond (y \diamond x)$$
.
- (vi)
$$x \sim x \diamond (y \diamond x).$$

(iv) is (i), which was already ruled out, and (vi) is similarly a relabeled version of (iii). In case (v) holds, the claim to refute simplifies to

$$x \diamond y \sim x \diamond (y \diamond x)$$

and using Theorem 14.2 we reduce to either $y \sim y \diamond x$, $y \to x$, or $y \diamond x \to x$, and each of these is already known to fail. □

14.1 Some further properties of 854 magmas

As in the previous section, we write $y \to x$ if $x = x \diamond y$.

Lemma 14.5 (854 equivalences, I)**.** *For x, y in a 854 magma, the following are equivalent.*

- *(i)* $y \to x$.
- *(ii)* $x = x \diamond y$.
- *(iii)* $x = z \diamond y$ *for some* z.
- *(iv)* $z, x \diamond z \to y$ *for some* z.
- *(v)* $x \diamond y^2 \to y$.
- *(vi)* $y \diamond (x \diamond y^2) = y$.
- *(vii)* $y = (w \diamond z) \diamond (x \diamond z)$ *for some* w, z.
- *(viii)* $y \to x \diamond y^2$.

Proof. The equivalence of (i) and (ii), or (v) and (vi), is by definition. (iii) trivially implies (ii), and the converse comes from Equation (14.3). Using Equation (14.2) we see that (v) implies (iv). If (iv) is true, then $y = (y \diamond z) \diamond (x \diamond z)$, giving (vii). From Equation (14.1) we see that (vii) implies (ii). If (ii) is true, then $y \diamond (x \diamond y^2) = y \diamond ((x \diamond y) \diamond (y \diamond y)) = y$, giving (vi). Finally, to show the equivalence of (i) and (viii), use the already established equivalence of (i) and (v), together with Equation (14.3) which gives $(x \diamond y^2) \diamond y^2 = x \diamond y^2$. □

Introduce the notation $y \leq x$ for $x \diamond y \to y$.

Lemma 14.6 (854 equivalences, II)**.** *For x, y in a 854 magma, the following are equivalent.*

- *(i)* $y \leq x$.

- *(ii)* $x \diamond y \to x$.
- *(iii) For all* z, $y \to z$ *implies* $x \to z$.
- *(iv)* $x \to x \diamond y$.

Proof. The equivalence of (i) and (ii) is by definition. If (ii) holds and $y \to z$, then by Theorem 14.5 we have $x = u \diamond (x \diamond y)$ and $z = v \diamond y$ for some u, v, hence

$$z \diamond x = z \diamond (x \diamond ((v \diamond y) \diamond (x \diamond y))) = z \diamond ((u \diamond (x \diamond y)) \diamond (z \diamond (x \diamond y))) = z,$$

giving the desired claim $x \to z$. Now if (iii) holds, note from Theorem 14.5 that $y \to x \diamond y$, hence $x \to x \diamond y$ by (iii), so that $(x \diamond y) \diamond x = x \diamond y$, giving (iv). Finally, if (iv) holds, note that

$$\begin{aligned} x \diamond ((x \diamond y) \diamond x) &= x \diamond (((x \diamond y) \diamond ((y \diamond y) \diamond ((x \diamond y) \diamond y))) \diamond x) \\ &= x \diamond (((x \diamond y) \diamond ((y \diamond y) \diamond (x \diamond y))) \diamond (x \diamond ((y \diamond y) \diamond (x \diamond y)))) \\ &= x \end{aligned}$$

and hence by (iv) $x \diamond (x \diamond y) = x$, giving (ii). □

Corollary 14.7. *The relation* $\leq$ *is a pre-order, and for each* z*, the sets* $\{x : x \to z\}$ *are upward closed in this preorder.*

14.2 Running a greedy algorithm

Define a *partial 854 magma* to be a partial function $\diamond : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ obeying the following axioms:

- (Equation 854) If $x, y, z \in \mathbb{N}$ are such that $(y \diamond z) \diamond (x \diamond z)$ is well-defined, then $x \diamond ((y \diamond z) \diamond (x \diamond z))$ is well-defined and equal to x.
- (Equation 8) If $x \in \mathbb{N}$ are such that $x \diamond x$ is well-defined, then $x \diamond (x \diamond x)$ is well-defined and equal to x.
- (Equation 101) If $x, y \in \mathbb{N}$ are such that $(x \diamond y) \diamond x$ is well-defined, then $x \diamond ((x \diamond y) \diamond x)$ is well-defined and equal to x.
- (Equation 46155) If $x, y \in \mathbb{N}$ are such that $x \diamond (x \diamond y)$ is well-defined, then $(x \diamond y) \diamond (x \diamond (x \diamond y))$ is well-defined and equal to $x \diamond y$.
- (Equation 378) If $x, y \in \mathbb{N}$ is such that $x \diamond y$ is well-defined, then $(x \diamond y) \diamond y$ is well-defined and equal to $x \diamond y$.
- (No idempotence) If $x \in \mathbb{N}$ is such that $x \diamond x$ is well-defined, then $x \diamond x \neq x$.
- (Auxiliary law) If $x, y \in \mathbb{N}$ are such that $x \diamond (x \diamond y)$ is well-defined and equal to x, then $x = y$.
- (Unique factorization) If $x, y, x', y' \in \mathbb{N}$ are such that $x \diamond y$, $x' \diamond y'$ are well-defined and equal to each other, then at least one of the assertions $x \diamond y = x$, $x' \diamond y' = x'$, or $(x, y) = (x', y')$ is true.
- (Monotonicity) If $x, y \in \mathbb{N}$ is such that $x \diamond y$ is defined, then either $x \diamond y = x$ or $x \diamond y > x, y$.

The first five laws are known consequences of 854. The no idempotence law was known for the free magma M_{854} because it maps to finite magmas without idempotents, such as $\mathbb{Z}/3\mathbb{Z}$ with law $x \diamond y = x - 1_{x=y}$. The unique factorization law is also known for the free magma by Theorem 14.2. The auxiliary law is a "leap of faith" that helped close the greedy argument, and the monotonicity property is a technical consequence of the greedy construction that will also help close the argument.

The following observation is key.

Proposition 14.8 (Greedy construction)**.** *Suppose one has a partial 854 magma on $\mathbb{N}$ that is only finitely defined, and let $a, b \in G$ be such that $a \diamond b$ is currently undefined. Then it is possible to extend the magma to a larger partial 854 magma, such that $a \diamond b$ is now defined.*

Proof. Define a directed graph by writing $x \to y$ if $y \diamond x$ is defined and equal to y. By Equation 378, we see that $x \to y$ if and only if $z \diamond x$ is well-defined and equal to y for some z.

From unique factorization, we see that b has at most one representation of the form $b = b_1 \diamond b_2$ with $b_1 \neq b$, or equivalently $b_2 \not\to b_1$. We define b_1, b_2 accordingly if such a representation exists, otherwise we leave b_1, b_2 undefined. We say that b_1 is *relevant* if $b_2 \to a$. Note that this forces $a \neq b_1$ since $b_2 \not\to b_1$. Also, if b_1, b_2 exist, we see from monotonicity that $b = b_1 \diamond b_2 > b_1, b_2$.

Let c be a natural number that is larger than any number appearing in anywhere in the partial 854 magma multiplication table (in particular it is larger than a, b, as well as b_1, b_2 if they are defined). We then extend the multiplication table by defining $a \diamond b = c$, $b \diamond c = b$, and $c \diamond b = c$. If b_1 exists and is relevant, we also define $b_1 \diamond c = b_1$. Finally, if b_1 exists and is relevant, and additionally $b \to b_1$, then we also define $c \diamond b_1 = c$. We remark that all new entries added are of the left absorptive form $x \diamond y = x$, except for $a \diamond b = c$.

We now verify that all of the axioms of a partial 854 magma continue to hold. We begin with all the axioms except for 854:

- Monotonicity: Observe that all the new values $x \diamond y$ of the multiplication table introduced are either equal to x, or larger than both x and y, so the monotonicity property is preserved.
- Unique factorization: the only way unique factorization breaks is if there is an element z that has two distinct factorizations $z = x \diamond y = x' \diamond y'$ with neither $x \diamond y$ nor $x' \diamond y'$ a left absorptive product. Since the only non-left-absorptive product introduced is $a \diamond b = c$, and c has no prior representation as a product, we see that the unique factorization property is preserved.
- No idempotence: The only possible product $x \diamond x$ that could be introduced here is $a \diamond b$ if $x = a = b$, but in that case $x \diamond x = a \diamond b = c$ is clearly not equal to x, so the no idempotence property is preserved.
- Equation 8: If $x \diamond x$ were already defined in the previous magma, the claim would already be established, so $x \diamond x$ must be one of the new products $a \diamond b$, $b \diamond c$, $c \diamond b$, $b_1 \diamond c$, or $c \diamond b_1$. As $c \neq a, b, b_1$, the only option is $x = a = b$, but then $x \diamond (x \diamond x) = b \diamond c = b = x$, as required.
- Equation 101: By Equation 8, we may assume $x \diamond y \neq x$, which implies $y \neq c$ since $x \diamond c = x$ whenever the left-hand side is defined. We can also assume $x \neq c$, since we have $c \diamond z = c$ whenever the left-hand side is defined. If $x \diamond y = c$, then $(x, y) = (a, b)$; as $(x \diamond y) \diamond x = c \diamond x$ is well-defined, $x = a$ is then either equal to b, or equal to b_1 if the latter exists and is relevant. But the second case cannot occur since $a \neq b_1$, so we have $x = b$, and then $x \diamond ((x \diamond y) \diamond x) = b \diamond (c \diamond b) = b = x$, giving the claim. So we may assume $x \diamond y \neq c$. If $(x \diamond y, x) \neq (a, b)$, then $(x \diamond y) \diamond x$ was already defined in the original partial magma,

and the claim follows from Equation 101; hence we may assume $(x \diamond y, x) = (a, b)$, then $x \diamond ((x \diamond y) \diamond x) = b \diamond c = b = x$, giving the claim.

- Equation 46155: By Equation 8, we may assume $x \diamond y \neq x$ and hence $y \neq c$ as before. The case $x = c$ is not possible, as this forces $x \diamond y = c$ and then $x \diamond (x \diamond y)$ is undefined. If $x \diamond y = c$, then $(x, y) = (a, b)$; in order for $x \diamond (x \diamond y) = a \diamond c$ to be defined, either $a = b$ or $a = b_1$ with b_1 relevant, but the latter is impossible since $a \neq b_1$; thus $x = y = a = b$ and $(x \diamond y) \diamond (x \diamond (x \diamond y)) = c \diamond (b \diamond c) = c = (x \diamond y)$, giving the claim. Thus we may assume $x \diamond y \neq c$. If $(x, x \diamond y) \neq (a, b)$ then $x \diamond (x \diamond y)$ was already defined in the original partial magma, and the claim follows from Equation 46155; hence we may assume $(x, x \diamond y) = (a, b)$, and we have $(x \diamond y) \diamond (x \diamond (x \diamond y)) = b \diamond c = b = x \diamond y$, giving the claim.

- Equation 378: We can assume $x \diamond y \neq x$, since the claim is trivial otherwise. This rules out the $y = c$ and $x = c$ cases. The only new case is then if $x \diamond y = c$, but forces $(x, y) = (a, b)$, and then $(x \diamond y) \diamond y = c \diamond b = c = x \diamond y$, giving the claim.

- Auxiliary law: if $x = c$, then the only possible value for $x \diamond y$ is c, and $c \diamond c$ is undefined, contradiction; thus $x \neq c$. If $y = c$, then the only possible value for $x \diamond y$ is x, and then $x \diamond (x \diamond y)$ cannot equal x by the no idempotence law. Thus $y \neq c$. Since $x \diamond (x \diamond y) = x$ is not equal to c, $(x, x \diamond y)$ is not equal to (a, b). If $(x, y) \neq (a, b)$, then both $x \diamond y$ and $x \diamond (x \diamond y)$ were already defined in the original partial magma, and the claim follows from the auxiliary law for that magma. Thus we may assume $(x, y) = (a, b)$, in which case $a \diamond c = a$, hence by construction either $a = b$ or $a = b_1$. If $a = b$ then we are done. If $a = b_1$, then b_1 cannot be relevant, and then $a \diamond c = b_1 \diamond c$ remains undefined, a contradiction.

Now we tackle the most difficult verification, which is 854. This splits into a large number of cases.

- Case 1: $x = c$. Then $x \diamond z$ can only equal c, hence z equals b or b_1; and $y \diamond z$ can also only equal b or b_1, and $(y \diamond z) \diamond (x \diamond z)$ is equal to $y \diamond z$. If $y \diamond z = b$, then we are done since $c \diamond b = c$. If $y \diamond z = b_1$, then $b_1 \diamond c$ needs to be defined, so b_1 is relevant. Furthermore, from equation 378 we have $b_1 \diamond z = b_1$, hence by the no idempotence property z must equal b, so $b \to b_1$, and hence $c \diamond b_1 = c$, giving the claim.

- Case 2: $x \neq c$, $z = c$. This forces $x, y = b, b_1$ with $y \diamond z = y$ and $x \diamond z = x$, thus $y \diamond x$ is well-defined and we need $x \diamond (y \diamond x)$ well-defined and equal to x. If $x = y$, this follows from Equation 8; otherwise, either $x = b_1 \diamond b_2$ and $y = b_1$ or $x = b_1$ and $y = b_1 \diamond b_2$, and the claim follows from Equation 101 or Equation 46155 respectively.

- Case 3: $x, z \neq c$, $y = c$. Then z must equal b or b_1, $y \diamond z$ must equal c, and $x \diamond z$ must equal b or b_1, and $(y \diamond z) \diamond (x \diamond z)$ must equal c, with the b_1 options only available if b_1 is relevant. If $x \diamond z = z$ then by equation 378, $z \diamond z = z$, contradicting the no idempotence law. Thus we either have $z = b_1, x \diamond z = b$ or $z = b, x \diamond z = b_1$, and in either case b_1 must be relevant. If $z \to x$, then either have $x = b$, or $x = b_1$ and b_1 is relevant, and in either case we have $x \diamond c = x$ as required. So we may assume $z \not\to x$. In the case $z = b_1, x \diamond z = b = b_1 \diamond b_2$ we may then apply unique factorization to conclude that $z = b_2$ and $x = b_1$, thus $x \diamond c = x$ as required. In the opposite case $z = b$, $x \diamond z = b_1$ with $z \not\to x$, we see from monotonicity that $b_1 = x \diamond z > z = b$; but from monotonicity again $b = b_1 \diamond b_2 > b_1$, a contradiction.

- Case 4: $x, y, z \neq c$, $(y, z) = (a, b)$. Here, $y \diamond z$ and $(y \diamond z) \diamond (x \diamond z)$ must equal c, and $x \diamond z$ must then equal b or b_1, with the latter an option only if b_1 is relevant. If $x \diamond z = b$, then by Equation 378, $b \diamond b = b$, contradicting idempotence, thus $x \diamond z = b_1$ and b_1 is relevant,

and then $b \to b_1$ by Equation 378 again. If $z \to x$, then $x = b_1$, and the claim follows since $b_1 \diamond c = c$, so we may assume $z \not\to x$. By monotonicity, this forces $b_1 = x \diamond z > z = b$ and $b = b_1 \diamond b_2 > b_1$, a contradiction.

- Case 5: $x, y, z \neq c$, $(y, z) \neq (a, b)$, $(x, z) = (a, b)$. Now $x \diamond z = c$, and $y \diamond z$ must equal b or b_1. If $y \diamond z = b$, then by Equation 378, $b \diamond b = b$, contradicting idempotence, thus $y \diamond z = b_1$ and b_1 is relevant, and then $b \to b_1$ by Equation 378 again, so $b_1 \diamond (b_1 \diamond b_2) = b_1$. By the auxiliary law, this forces $b_1 = b_2$, so $x = b_1$, and then we are done since $b_1 \diamond c = b_1$.
- Case 6: $x, y, z \neq c$, $(y, z), (x, z) \neq (a, b)$, $(y \diamond z, x \diamond z) = (a, b)$. Here $x \diamond z = b$ and $(y \diamond z) \diamond (x \diamond z) = c$. If $z \to x$, then $x = b$ and we are done since $b \diamond c = b$. If $z \not\to x$, then by unique factorization applied to $x \diamond z = b_1 \diamond b_2$ we have $(x, z) = (b_1, b_2)$. By Equation 378, we have $z \to y \diamond z$, hence $b_2 \to a$, so b_1 is relevant. We are now done since $b_1 \diamond c = b_1$.
- Case 7: $x, y, z \neq c$, $(y, z), (x, z) \neq (a, b), (y \diamond z, x \diamond z) \neq (a, b)$. In this case $x \diamond ((y \diamond z) \diamond (x \diamond z))$ would already have been defined and equal to x in the previous partial magma, thanks to Equation 854.

□

Iterating this in the usual fashion, we obtain

Corollary 14.9 (854 extension)**.** *Suppose one has a partial 854 magma on $\mathbb{N}$ that is only finitely defined. Then it can be extended to a complete 854 magma that additionally obeys the no idempotence law, the monotonicity law, the auxiliary law, and the unique factorization law.*

Proof. Apply the usual greedy algorithm. □

Corollary 14.10 (854 does not not imply 413)**.** *There is an 854 magma which does not obey the 413 law $x = x \diamond (x \diamond (x \diamond (y \diamond x)))$.*

Proof. Create a partial magma by imposing the laws $1 \diamond 0 = 2$, $0 \diamond 2 = 3$, $2 \diamond 0 = 2$, $3 \diamond 2 = 3$. One can check that this is a partial magma. We then extend it to a global magma using Theorem 14.9. We claim that we have the 413 violation

$$0 \diamond (0 \diamond (0 \diamond (1 \diamond 0))) = 0$$

or equivalently

$$0 \diamond (0 \diamond 3) = 0.$$

Indeed this is immediate from the auxiliary law. □

Corollary 14.11 (854 does not not imply 1045)**.** *There is an 854 magma which does not obey the 1045 law $x = x \diamond ((y \diamond (y \diamond x)) \diamond x)$.*

Proof. Similar to previous, but start with the seed

$$0 \diamond 0 = 2; 0 \diamond 1 = 0 \diamond 2 = 0; 1 \diamond 2 = 3; 2 \diamond 0 = 2 \diamond 1 = 2 \diamond 3 = 2; 3 \diamond 2 = 3$$

which already violates the law with $x = 1, y = 0$, and can be verified to be a partial 854 magma. □

14.3 The free 854 magma

In this section we explicitly describe the free magma $M_{X,854}$ on some set X of generators relative to the 854 law.

We recall the free magma M_X from Theorem 1.2, though to avoid confusion we will denote the magma operation on M_X by $*$ rather than $\diamond$. Recall that every word w in M_X has a length in $\mathbb{N}$, which is zero if w is a generator in X, and is the sum of the lengths of w_L and w_R plus one if instead w is of the form $w_L * w_R$ for the left and right components w_L, w_R of w (which are uniquely defined by w). We iterate this notation, for instance w_{RL} is the left-component of w_R (if it exists), thus $w = w_L * (w_{RL} * w_{RR})$ in this case.

We shall shortly define a relation $\to$ on M_X. To motivate this relation, we make the following observation about 854 magmas:

Lemma 14.12 (The 854 relation)**.** *Let M be an 854 magma, and let $\to$ be the associated operation, thus $x \to y$ if $y \diamond x = y$. Then $x \to y$ holds under any of the following assumptions:*

- *(i) $y = a \diamond x$ for some a.*
- *(ii) $x = a \diamond (y \diamond b)$ for some a, b with $b \to a$.*
- *(iii) $y = a \diamond (x \diamond b)$ for some a, b with $b \to a$ and $x \diamond b \to x$.*
- *(iv) $x = a \diamond y$ for some a, z with $z \to a, y$.*
- *(v) $x = a \diamond y$ for some a, with either $a = y$, $a = y \diamond z$, or $y = a \diamond z$ for some z.*

Proof. Case (i) follows from Equation (14.3). For (ii), we observe

$$y \diamond x = y \diamond ((a \diamond b) \diamond (y \diamond b)) = y$$

as required. For (iii), we see from (ii) that $y \to x$, and from (i) we have $x \diamond b \to y$, and then

$$y \diamond x = y \diamond ((x \diamond (x \diamond b)) \diamond (y \diamond (x \diamond b))) = y$$

as required. For (iv), we have

$$y \diamond x = y \diamond ((a \diamond z) \diamond (y \diamond z)) = y$$

as required. Finally, for (v), in the $a = y$ case we have from Equation (14.2) that

$$y \diamond x = y \diamond ((y \diamond y^2) \diamond (y \diamond y^2)) = y,$$

in the $a = y \diamond z$ case we have from Equation (14.2) that

$$y \diamond x = y \diamond (((y \diamond z) \diamond (y \diamond z)^2) \diamond (y \diamond (y \diamond z)^2)) = y,$$

and finally in the $y = a \diamond z$ case we have from Equation (14.2) that

$$y \diamond x = y \diamond ((a \diamond (a \diamond z)^2) \diamond ((a \diamond z) \diamond (a \diamond z)^2)) = y,$$

so the claim follows in all cases. □

Now we define the operation $\to$ on M_X by the following rule.

Definition 14.13 (Relation on the free group)**.** For $x, y \in M_X$, we have $x \to y$ if and only if one of the following holds:

- (i) $x = y_R$.
- (ii) $y = x_{RL}$ and $x_{RR} \to x_L$.
- (iii) $x = y_{RL}$, $y_{RR} \to y_L$, and $y_R \to y_{RL}$.
- (iv) $y = x_R$, and there exists $z \in \{x_{LR}, x_{LRL}, x_{RR}, x_{RRL}\}$ such that $z \to x_L$ and $z \to x_R$.
- (v) $y = x_R$, and one of the claims $x_L = x_R$, $x_L = x_{RL}$, or $x_R = x_{LL}$ holds.

Here we adopt the convention that a claim can only hold if all terms in it are well-defined, for instance claim (ii) can only hold if x_{RL} is well-defined.

If we define the "max-length" of a claim $x \to y$ to be the maximum of the length of x and the length of y, we see that the verification of a claim $x \to y$ only involves claims $x' \to y'$ of strictly smaller max-length. Thus this definition is well-defined. We also see that if $x \to y$, then exactly one of

$$x = y_R, x = y_{RL}, y = x_R, y = x_{RL} \tag{14.8}$$

hold; in particular, we cannot have $x \to x$ for any x.

We then define a new operation $\diamond$ on M_X by the rule $x \diamond y = x$ if $y \to x$, and $x \diamond y = x * y$ otherwise. Thus, by definition, $y \to x$ if and only if $x \diamond y = x$. We then define $M_{X,854}$ to be the magma generated by X with the operation $\diamond$; thus, $w \in M_{X,854}$ if and only if either $w \in X$, or else $w_L, w_R \in M_{X,854}$ and $w_R \not\to w_L$.

Theorem 14.14 (Free 854 magma)**.** *The magma $M_{X,854}$ is a free 854 magma on X.*

Proof. Let $f : X \to M$ be a function from X to an 854 magma M, then φ_f is a homomorphism from M_X (with the operation $*$) to M. We claim that the restriction of φ_f to $M_{X,854}$ is a homomorphism from $M_{X,854}$ (with operation $\diamond$) to M. Since φ_f was already a homomorphism for $*$, it suffices to show that φ_f preserves $\to$: that is to say, for any $x, y \in M_{X,854}$, that $x \to y$ implies $\varphi_f(x) \to \varphi_f(y)$. By definition, one of the five scenarios (i)-(v) in Theorem 14.13 holds, and in each case one can establish the claim from the corresponding claim of Theorem 14.12 and an induction on the max-length of the claim $x \to y$.

It remains to show that M_{854} actually obeys 854, that is to say that

$$(y \diamond z) \diamond (x \diamond z) \to x$$

for all $x, y, z \in M_{854}$. Writing $w = y \diamond z$, we have $z \to w$ by Theorem 14.13(i), and we need to show that $w \diamond (x \diamond z) \to x$. We divide into four cases.

Case 1: $x \diamond z \to w$, $z \to x$. Here we have $x \diamond z = x$ and $w \diamond (x \diamond z) = w$. We now have $z \to x, w$ and $x \to w$, and we need to show that $w \to x$.

From Equation (14.8) we know that one of

$$z = x_R, z = x_{RL}, x = z_R, x = z_{RL} \tag{14.9}$$

holds, one of

$$z = w_R, z = w_{RL}, w = z_R, w = z_{RL} \tag{14.10}$$

holds, and one of

$$x = w_R, x = w_{RL}, w = x_R, w = x_{RL} \tag{14.11}$$

holds.

We split into subcases using Equation (14.11).

- If $x = w_R$ then the claim follows from Theorem 14.13(i).
- If $w = x_{RL}$ then from Theorem 14.13(iii) we have $x_{RR} \to x_L$, and then the claim follows from Theorem 14.13(ii).
- If $x = w_{RL}$, then $w_{RR} \to w_L$ by Theorem 14.13(ii) and from Theorem 14.13(iii) we will be done if we can show that $w_R \to w_{RL}$. If $z = w_R$ then this follows from $z \to x$. The claim $z = w_{RL}$ is not compatible with Equation (14.9), since $z = x$ in that case. If $w = z_R$ then $x = z_{RRL}$, and this is only compatible with Equation (14.9) if $x = z_{RL}$, thus $z = a * (x * (x * b))$ and $w = x * (x * b)$ for some a, b. In order to have $x = w_{RL}$ in Equation (14.11), we must have $b \to x$ by Theorem 14.13(iii), but then $x * b$ would not lie in M_{854}, a contradiction.
- If $w = x_R$, then we cannot then have $z = x_R$ as then $z = w$ which is incompatible with Equation (14.10). If $z = x_{RL} = w_L$ then $x_{RR} \to x_L$ by Theorem 14.13(ii), and the only available options from Equation (14.10) are $z = w_R$ and $z = w_{RL}$. For $z = w_R$ we have $w = z * z$ and $x = a * (z * z)$ for some a with $z \to a = x_L$. Since $z \to z * z = x_R$ as well by Theorem 14.13(i), and $z = x_{RR}$, we obtain $w \to x$ as required from Theorem 14.13(iv).

Case 2: $x \diamond z \to w$, $z \not\to x$. We now have $x * z, z \to w$, and we need to show that $w \to x$. From Equation (14.8) we know that one of

$$w = (x * z)_R, w = (x * z)_{RL}, x * z = w_R, x * z = w_{RL} \tag{14.12}$$

holds, and that one of

$$w = z_R, w = z_{RL}, z = w_R, z = w_{RL} \tag{14.13}$$

holds.

We split into cases depending on Equation (14.12).

- If $w = (x * z)_R$ then $w = z$, which is incompatible with Equation (14.13).
- If $w = (x * z)_{RL}$ then $w = z_L$ and $z_R \to x$ by Theorem 14.13(ii). Only the first two possibilities of Equation (14.13) are compatible with $w = z_L$. In the first case we are done since $z_R \to x$ and $w = z_R$. In the second case, we have $z = w*(w*a)$ for some a with $a \to w$ (from Theorem 14.13(ii) and $z \to w$), but then $w * a$ will not lie in M_{854}, contradiction.
- If $x * z = w_R$ then w is longer than z and $z \neq w_R$. Comparing this with Equation (14.13) we see that the only compatible option is $z = w_{RL}$, thus $x = z$, and then $w = a * (x * x)$ and $x \to a$ by Theorem 14.13(iii), and the claim follows from Theorem 14.13(ii).
- If $x * z = w_{RL}$, then $w = a * ((x * z) * b)$ for some a, b. Then w, w_R, and w_{RL} are all longer than z and none of the options in Equation (14.13) can hold, a contradiction.

Case 3: $x \diamond z \not\to w$, $z \to x$. We now have $z \to x, w$, and we need to show that $w * x \to x$.

If $z \in \{w_R, w_{RL}, x_R, x_{RL}\}$, then the claim follows from Theorem 14.13(iv), so we may assume that this is not the case. By Equation (14.8), we then know that one of

$$x = z_R, x = z_{RL}$$

holds, and also one of

$$w = z_R, w = z_{RL}$$

holds. Thus, we either have one of

$$w = x, w = x_L, x = w_L.$$

But in any of these three cases the claim follows from Theorem 14.13(v).

Case 4: $x \diamond z \not\to w$, $z \not\to x$. Then $x = (w \diamond (x \diamond z))_{RL}$ and $z \to w$, so the claim follows from Theorem 14.13(ii).

□

With the explicit description of $M_{X,854}$ we can now refute various laws. Suppose for instance that x, y are generators in X. We cannot have $y \to x$ (as none of Equation (14.8) hold), so $y * x \in M_{X,854}$. We also cannot have $y * x \to x$ (by inspection of the cases in Theorem 14.13(iv), Theorem 14.13(v)), so $x * (y * x)$ lies in $M_{X,854}$. Then $x * (y * x) \not\to x$ (by Equation (14.8)), so $x * (x * (y * x))$ lies in $M_{X,854}$; finally, $x * (x * (y * x)) \not\to x$ (this follows from Theorem 14.13(ii) since $y * x \not\to x$), so $x * (x * (x * (y * x)))$ lies in $M_{X,854}$. This gives an alternate proof of Theorem 14.10. One can similarly establish Theorem 14.11.

Chapter 15

Equation 906

In this chapter we study finite magmas that obey equation 906,

$$x = y \diamond ((y \diamond x) \diamond (x \diamond x)) \tag{15.1}$$

for all x, y. We can write this as

$$L_y(L_y x \diamond Sx) = x. \tag{15.2}$$

This implies that L_y is surjective, hence invertible by finiteness, so

$$L_y x \diamond Sx = L_y^{-1} x. \tag{15.3}$$

Corollary 15.1 (Edge disjointness of left cycles)**.** *For any integer n,*

$$L_y x = L_z x \implies L_y^n x = L_z^n x.$$

Proof. This is trivial for $n = 0, 1$, and $n = -1$ follows from Equation (15.3). Observe that if the claim holds for $n = 0, -1, \ldots, -m$ for any $m \geq 1$ then it also holds for $n = -m - 1$. Finally, since there is a common period to all the L_y by finiteness (or Legendre's theorem), the set of n for which the claim holds is periodic. The claim follows. □

Setting $n = N - 2$ for $N > 2$ a common period of L_y, L_z (which exists by finiteness) we conclude that

$$L_y x = L_z x \implies L_y^2 x = L_z^2 x. \tag{15.4}$$

Theorem 15.2. *For finite magmas, equation 906 implies equation 3862,*

$$(x \diamond (x \diamond x)) \diamond x = x \diamond x. \tag{15.5}$$

Proof. Observe from Equation (15.2) that

$$L_x S^2 x = L_x(L_x x \diamond Sx) = x$$

while from Equation (15.3) we have

$$L_{L_x Sx} S^2 x = L_x Sx \diamond SSx = L_x^{-1} Sx = x.$$

Thus

$$L_x S^2 x = L_{L_x Sx} S^2 x = x$$

and hence by the $n = 2$ case of Theorem 15.1

$$L_x x = L_{L_x Sx} x$$

giving the claim. □

Chapter 16

Equation 1323

In this chapter we study magmas that obey equation 1323,

$$x = y \diamond (((y \diamond y) \diamond x) \diamond y) \tag{16.1}$$

for all x, y. Using the squaring operator $Sy := y \diamond y$ and the left and right multiplication operators $L_y x := y \diamond x$ and $R_y x = x \diamond y$, this law can be written as

$$L_y R_y L_{Sy} x = x.$$

In particular, this gives a way to construct these magmas:

Lemma 16.1 (Construction of 1323 magmas)**.** *Suppose that M is a magma such that*

$$R_{Sy} L_{Sy} = 1 \tag{16.2}$$

and

$$L_y R_y = R_{Sy} \tag{16.3}$$

hold. Then the magma obeys 1323.

Proof. Trivial. □

So now we would like to construct magmas satisfying Equation (16.2) and Equation (16.3). We need some bijections:

Lemma 16.2 (Bijections)**.** *Let G be a countably infinite abelian torsion group of exponent 2. Then there exists a bijection $\phi_a : G \to \mathbb{Q}^\times$ for each $a \in G \backslash \{0\}$ such that $\phi_a(0) = 1$ and $\phi_a(a + b) = -\phi_a(b)$ for all $b \in G$, so in particular $\phi_a(a) = -1$.*

Proof. Such a bijection can be easily constructed from the axiom of choice and a greedy algorithm, defining ϕ_a one pair $\{b, a + b\}$ at a time. □

Lemma 16.3 (Building a magma)**.** *Let G be a countably infinite abelian torsion group of exponent 2, and let ϕ_a be as in the previous lemma. Let N be the set of pairs (x, a) with $x \in \mathbb{Q}^\times$ and $a \in G \backslash \{0\}$, and let $M = G \uplus N$ be the disjoint union of G and N. Suppose that we have an operation $\diamond : M \times M \to M$ obeying the following axioms:*

- *(i) We have*

$$a \diamond b = a + b \tag{16.4}$$

  for $a, b \in G$.

- *(ii) We have*
$$(x,a)\diamond b = (\phi_a(b)x, a) \tag{16.5}$$
$$b\diamond (x,a) = (x/\phi_a(b), a) \tag{16.6}$$
and
$$(\phi_a(b)x,a)\diamond(x,a) = a+b \tag{16.7}$$
for $x\in\mathbb{Q}^\times$, $b\in G$, and $a\in G\backslash\{0\}$.

- *(iii) If $a,b,0\in G$ are distinct and $(x,a)\diamond(y,b) = (z,c)$ for some $x,y,z\in\mathbb{Q}^\times$ and $c\in G$, then $(y,b)\diamond(z,c) = (\phi_a(b)x,a)$.*

Then Equation (16.2), Equation (16.3) and hence Equation (16.1) holds.

Proof. With these rules, 0 is a unit, and the squaring operator is given by $Sa = 0$ and $S(x,a) = a$, so the set of squares is G. If $a\in G$ is a square number, we have
$$L_a b = R_a b = a+b$$
and
$$L_a(x,b) = (x/\phi_b(a), b);\quad R_a(x,b) = (x\phi_b(a), b)$$
so Equation (16.2) is satisfied.

Now we verify Equation (16.3). If y is a square, then the claim already follows from Equation (16.2) since $Sy = 0$ is a unit. Otherwise, for $y\in\mathbb{Q}^\times$ and $b\in G\backslash\{0\}$, we have to show that
$$L_{(y,b)}R_{(y,b)}a = R_b a = a+b$$
for $a\in G$ and
$$L_{(y,b)}R_{(y,b)}(x,a) = R_b(x,a) = (\phi_a(b)x,a)$$
for $x\in\mathbb{Q}^\times$ and $a\in G\backslash\{0\}$. In the first case, we have from Equation (16.6) that
$$R_{(y,b)}a = (y/\phi_a(b), b)$$
and then from Equation (16.7) we have
$$L_{(y,b)}R_{(y,b)}a = a+b$$
as required. In the second case, if $a = b$, then by the bijective nature of ϕ_a, we can write $x = \phi_a(c)y$ for some $c\in G$, then from Equation (16.7) we have
$$R_{(y,b)}(x,a) = a+c$$
and then by Equation (16.5)
$$L_{(y,b)}R_{(y,b)}(x,a) = (\phi_a(a+c)y, a)$$
but from construction we have $\phi_a(a+c) = -\phi_a(c) = \phi_a(b)\phi_a(c)$ and hence $\phi_a(a+c)y = \phi_a(b)x$ as required.

It remains to handle the case when a,b are distinct elements of $G\backslash\{0\}$. But this follows from (iii). □

Definition 16.4 (Partial solution)**.** A *partial solution* is a finite family $\mathcal{F}$ of tuples $(x,y,z,a,b,c)\in(\mathbb{Q}^\times)^3\times G^6$ with $a,b,c,0$ distinct, such that the tuples $(\phi_a(b)^n x, a, \phi_b(c)^n y, b)$, $(\phi_b(c)^n y, b, \phi_c(a)^n z, c)$, $(\phi_c(a)^n z, c, \phi_a(b)^{n+1}x, a)$ for $(x,y,z,a,b,c)\in\mathcal{F}$ and $n\geq 0$ are all distinct.

Lemma 16.5 (Soundness)**.** *Let $\mathcal{F}$ be a partial solution. Then if one defines a partial operation $\diamond$ on M by requiring axioms (i), (ii), imposing the additional operations*

$$(\phi_a(b)^n x, a) \diamond (\phi_b(c)^n y, b) = (\phi_c(a)^n z, c)$$

$$(\phi_b(c)^n y, b) \diamond (\phi_c(a)^n z, c) = (\phi_a(b)^{n+1} x, a)$$

$$(\phi_c(a)^n z, c) \diamond (\phi_a(b)^{n+1} x, a) = (\phi_b(c)^{n+1} y, b)$$

for all $n \geq 0$ and $(x, y, z, a, b, c) \in \mathcal{F}$, and no other operations, then this is a well-defined partial operation that obeys axiom (iii) whenever it is defined.

Proof. Routine. □

Lemma 16.6 (Greedy extension)**.** *If $\diamond$ is defined by a partial solution, and $(x, a) \diamond (y, b)$ is undefined for some $x, y \in \mathbb{Q}^\times$ and distinct $a, b \in G \backslash \{0\}$, then it is possible to extend the partial solution so that $(x, a) \diamond (y, b)$ is now defined.*

Proof. We select a $c \in G \backslash \{0\}$ that has not previously been used by the partial solution, let $z \in \mathbb{Q}^\times$ be arbitrary, (e.g., one could take $z = 1$ if desired), and add (x, y, z, a, b, c) to $\mathcal{F}$, thus we now also assign

$$(\phi_a(b)^n x, a) \diamond (\phi_b(c)^n y, b) = (\phi_c(a)^n z, c)$$

$$(\phi_b(c)^n y, b) \diamond (\phi_c(a)^n z, c) = (\phi_a(b)^{n+1} x, a)$$

$$(\phi_c(a)^n z, c) \diamond (\phi_a(b)^{n+1} x, a) = (\phi_b(c)^{n+1} y, b)$$

for all natural numbers n. As the a, b, c are distinct, the $\phi_a(b), \phi_b(c), \phi_c(a)$ are not equal to ± 1, and the members of this infinite sequence do not collide with each other. The second and third equations in this family cannot collide with previous assignments because c is novel. If we arrange matters so that $\phi_b(c)$ involves primes in the numerator or denominator that do not appear in any previous $\phi_a(b), \phi_b(c), \phi_c(a), x, y, z$ used by the greedy algorithm, or the current x, y, z, then we also see that the first infinite sequence does not collide with any previously assigned value of $\diamond$ either. □

Corollary 16.7 (Iterated greedy extension)**.** *Every partial solution can be extended to a complete solution that obeys Equation (16.2) and Equation (16.3), and hence 1323.*

Proof. Apply the usual greedy algorithm. □

Corollary 16.8 (1323 does not imply 2744)**.** *There exists a 1323 magma which does not obey the 2744 equation $R_y L_{Sy} L_y x = x$.*

Proof. It suffices to produce a partial solution in which L_y is not injective. Pick distinct a, b, b', c with $\phi_a(b)$, $\phi_a(b')$ having no prime factors in common in the numerator or denominator. We take the partial solution consisting of $(1, 1, 1, a, b, c)$ and $(1, 1, 1, a, b', c)$, that is to say we impose the conditions

$$(\phi_a(b)^n, a) \diamond (\phi_b(c)^n, b) = (\phi_c(a)^n, c)$$

$$(\phi_b(c)^n, b) \diamond (\phi_c(a)^n, c) = (\phi_a(b)^{n+1}, a)$$

$$(\phi_c(a)^n, c) \diamond (\phi_a(b)^{n+1}, a) = (\phi_b(c)^{n+1}, b)$$

and

$$(\phi_a(b)^n, a) \diamond (\phi_{b'}(c)^n, b') = (\phi_c(a)^n, c)$$

$$(\phi_{b'}(c)^n, b') \diamond (\phi_c(a)^n, c) = (\phi_a(b')^{n+1}, a)$$

$$(\phi_c(a)^n, c) \diamond (\phi_a(b')^{n+1}, a) = (\phi_b(c)^{n+1}, b').$$

One can check that no collisions occur; on the other hand, as $L_{(1,a)}(1, b) = L_{(1,a)}(1, b') = (1, c)$, we already have a violation of left injectivity. Completing this seed to a full magma using Theorem 16.7, we obtain the claim. □

Chapter 17

Equation 1516

In this chapter we study magmas that obey equation 1516,

$$x = (y \diamond y) \diamond (x \diamond (x \diamond y)) \tag{17.1}$$

for all x, y. Using the squaring operator $Sy := y \diamond y$ and the left and right multiplication operators $L_y x := y \diamond x$ and $R_y x = x \diamond y$, this law can be written as

$$L_{Sy} L_x L_x y = x.$$

We begin by studying a greedily constructed translation invariant model

$$x \diamond y = x + f(y - x) \tag{17.2}$$

on the carrier $\mathbb{Z}$ with some function $f : \mathbb{Z} \to \mathbb{Z}$ with $f(0) = 0$. This ensures that $Sx = x$. If $y = x + h$, then $L_x y = x + f(h)$, $L_x^2 y = x + f^2(h)$, and $L_y L_x^2 y = y + f(f^2(h) - h)$, so the law Equation (17.1) simplifies to

$$f(f^2(h) - h) = -h. \tag{17.3}$$

Thus, if we let $E = \{(h, f(h))\}$ be the graph of f, then we have the following property: if $(a, b), (b, c) \in E$, then $(c - a, -a) \in E$. This helps motivate the following definition.

Definition 17.1 (1516 seed)**.** A *1516 seed* is a finite collection E of pairs (a, b) with $a, b \in \mathbb{Z}$ obeying the following axioms:

- Axiom 1: $(0, 0) \in E$.
- Axiom 2: If $(a, b) \in E$ and $a \neq 0$, then $b \neq 0, -a$.
- Axiom 3: If $(a, b), (a, b') \in E$, then $b = b'$.
- Axiom 4: If $(a, b), (b, c) \in E$, then $(c - a, -a) \in E$.
- Axiom 5: If $(b, a), (b', a), (-b, d), (-b', d') \in E$ with $b \neq b'$, then $b + d \neq d', b' + d'$.

An *extension* of a 1516 seed E is a 1516 seed E' that contains E.

This definition has an extension property:

Lemma 17.2 (1516 extension)**.** *Let E be a 1516 seed, and let $a_0 \in \mathbb{Z}$. Then there exists an extension E' of E that contains (a_0, c_0) for some c_0.*

Proof. We may assume that E does not already contain any pair of the form (a_0, c), since we are done otherwise. By Axiom 1 implies that $a_0 \neq 0$. Let $b_1, \dots, b_n$ denote all the integers b_i such that $(b_i, a) \in E$, then $n \geq 0$ is finite, and by Axiom 2 all the b_i are non-zero and not equal to $-a$. Let c_0 be a sufficiently large integer to be chosen later. We then add the pairs (a_0, c_0) and $(c - b_i, -b_i)$ to E for all i. Furthermore, if i is such that $(-b_i, d_i) \in E$ for some (necessarily unique and non-zero) d_i, we also add $(d_i + b + i - c_0, b_i - c_0)$ to E. Let E' be the resulting set of pairs. Axioms 4, 5 for E ensure that (for c_0 large enough) the addition of these pairs do not cause a violation of Axioms 2 or 3 for E', and of course Axiom 1 for E' will also be retained. As for Axiom 4, one can check that the only new pairs of pairs $(', b), (b, c)$ that would trigger these axioms either take the form $(b_i, a_0), (a_0, c_0)$ or $(c_0 - b_i, -b_i), (-b_i, d_i)$, and in either case we see from construction that Axiom 4 remains in effect for E'. Finally, the new quadruples of pairs $(b, a), (b', a), (-b, d), (-b', d') \in E'$ only arise when either $(-b, d)$, $(-b', d')$ is equal to (a_0, c_0) and the other three pairs in the quadruple were already in E, and for c_0 large enough we see that Axiom 5 remains valid. □

For technical reasons (which will be helpful later when we expand the magma) we also give a variant that will ensure a useful "double surjectivity" property:

Lemma 17.3 (1516 extension variant)**.** *Let E be a 1516 seed, and let $h \in \mathbb{Z}$ be non-zero. Then there exists an extension E' of E that contains $(a_i, a_i + h)$ for $i = 1, 2, 3, 4$, for some distinct a_1, a_2, a_3, a_4.*

Proof. If we choose a sufficiently large, and set $a_i = ia$ (say) for $i = 1, 2, 3, 4$, the claim simply follows by adding $(a_i, a_i + h)$ to E and verifying that none of the axioms are violated. □

Corollary 17.4 (Base magma)**.** *There exists a 1516 magma with carrier $\mathbb{Z}$ with the properties that*

- *(i) $Sa = a$ for all a.*
- *(ii) For any distinct $a, b \in \mathbb{Z}$, the equation $R_a c = b$ has at least four solutions c.*
- *(iii) For each $a \in \mathbb{Z}$, there exist at least two $b \neq a$ such that $L_a R_a b = b$.*

Note from Equation (17.1) and the hypothesis $Sa = a$ that $R_a c = a$ if and only if $c = a$. Thus, the requirement that a, b be distinct in (ii) is necessary.

Proof. By Theorem 17.2, Theorem 17.3 and the greedy algorithm starting with the seed consisting of $(0, 0)$, $(-1, 2)$, $(3, 1)$, $(-10, 20)$, $(30, 10)$, we obtain a graph $\{(a, f(a)) : a \in \mathbb{Z}\}$ of a function $f : \mathbb{Z} \to \mathbb{Z}$ with $f(0) = 0$, $f(-1) = 2$, $f(3) = 1$, $f(-10) = 20$, $f(30) = 10$ and the property that if $f(a) = b$ and $f(b) = c$, then $f(c - a) = -a$, and also with the property that for every non-zero h there are distinct $a_{h,1}, a_{h,2}, a_{h,3}, a_{h,4}$ with $f(a_{h,i}) = a_{h,i} + h$ for $i = 1, 2, 3, 4$. We then have that Equation (17.3) holds. If we then define the magma operation $\diamond$ by Equation (17.2), we obtain Equation (17.1), and since $f(0) = 0$ we have (i). Also, from construction we see that $R_d(d - a_{h,i}) = d + h$ for any d, h, i, giving (ii). Finally, from construction we have $R_a(a + 1) = a + 1 + f(-1) = a + 3$, so $L_a R_a(a + 1) = a + f(3) = a + 1$, and similarly $L_a R_a(a + 10) = a + 10$, giving (iii). □

Let us denote by A the free group over $\mathbb{N}$. Note that a magma with the same properties as in Theorem 17.4 but having carrier A can be constructed similarly. The same thing is true for the following results. In fact, the Lean implementation has A whenever $\mathbb{Z}$ is; this has been done to reuse some preexisting code.

Now we construct a more complex 1516 magma, whose carrier G is $\mathbb{Z} \cup G'$, where

$$G' := \{(a,c,n) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N} : a \neq c\}.$$

The first component $\mathbb{Z}$ will represent the squares, and the second component G' will represent the non-squares. The most important coordinate of an element (a,c,n) of G' is a; the other two components c, n are technical, with n being needed to ensure a certain infinite surjectivity property, and c being such that $L_c(a,c,n)$ remains at one's disposal to select at certain stages of the inductive process.

The 1516 magma constructed in Theorem 17.4 will be the restriction of G to $\mathbb{Z}$; thus $a \diamond b$ is already defined in G for $a, b \in \mathbb{Z}$, but the rest of the multiplication table is not currently defined. By construction, S is already defined and equal to the identity on $\mathbb{Z}$, and we have the 1516 equation

$$L_{Sa} L_b L_b a = b$$

for $a, b \in \mathbb{Z}$, with the left multiplication operators L_b currently only defined as maps from $\mathbb{Z}$ to $\mathbb{Z}$. Among other things, this means that $L_a = L_{Sa}$ is surjective as a map from $\mathbb{Z}$ to $\mathbb{Z}$ for any $a \in \mathbb{Z}$.

We extend the squaring map S to all of G by declaring $S(a,c,n) := a$, thus S maps G to $\mathbb{Z}$. To create a 1516 magma structure on all of G, we need to extend the left multiplication operators L_b, $b \in \mathbb{Z}$ as maps from G to G, and also introduce additional maps $L_x : G \to G$ for $x \in G'$, obeying the following axioms:

- Axiom A: For any $x \in G'$, $L_x x = Sx$.
- Axiom B: For any $x \in G'$ and $b \in \mathbb{Z}$, $L_{Sx} L_b L_b x = b$.
- Axiom C: For any $x \in G$ and $y \in G'$, $L_{Sx} L_y L_y x = y$.

We first address Axiom B, which purely concerns how to extend the L_b operators for $b \in \mathbb{Z}$, and also impose an additional technical "infinitely surjective" requirement that will help us satisfy Axiom C later. We first need some preparatory lemmas. We begin by locating some useful elements $c_{y,b}$ of $\mathbb{Z}$ for all $y \in G'$ and $b \in \mathbb{Z}$.

Lemma 17.5 (Useful elements)**.** *One can assign $c_{y,b} \in \mathbb{Z}$ for each $y = (a,c,n) \in G'$ and $b \in \mathbb{Z}$ with the following properties:*

- *(i) For all $y = (a,c,n) \in G'$ and $b \in \mathbb{Z}$, $c_{y,b} \neq a, b, c$ and $L_a L_{c_{y,b}} b = c_{y,b}$.*
- *(ii) For all $y \in G'$, the map $b \mapsto c_{y,b}$ is injective.*

Proof. Let $y = (a,c,n)$. By Theorem 17.4 (iii), we can find $c_{y,a} \neq a, c$ such that $L_a R_a c_{y,a} = c_{y,a}$, or equivalently $L_a L_{c_{y,a}} a = c_{y,a}$. Next, for any $b \neq a$, we can apply Theorem 17.4 (ii) to find $c_{y,b} \neq b, c, c_{y,a}$ such that $R_a c_{y,b} = b$; note that as $R_a a = Sa = a \neq b$, this also implies that $c_{y,b} \neq a$, and that the $c_{y,b}$ are distinct as b variables. We now have $L_a L_{c_{y,b}} b = L_{Sa} L_{c_{y,b}} L_{c_{y,b}} a = c_{y,b}$ for such b, giving the claim. □

Let $c_{y,b}$ be as above. Define a *partial solution* to be a partial assignment of $L_{c'} y \in G$ for $c' \in \mathbb{Z}$ and $y \in G$ that obeys the following properties:

- (a) If $y \in \mathbb{Z}$, then $L_{c'} y$ agrees with the operation defined in Theorem 17.4.
- (b) If $y = (a,c,0) \in G'$, then $L_a y = a$.

- (c) If $y = (a, c, n) \in G'$ and $n \neq 0$, then $L_a y = (a, c, 0)$.
- (d) If $y = (a, c, n) \in G'$ and $b \in \mathbb{Z}$, then $L_{c_{y,b}} y = b$.
- (e) For any a, c, $L_c(a, c, n)$ is only defined for finitely many n.
- (f) If $y = (a, c, n) \in G'$ and $c' \in \mathbb{Z}$ are such that $L_{c'} y$ is defined, then $L_{c'} L_{c'} y$ and $L_a L_{c'} L_{c'} y$ are defined, with $L_a L_{c'} L_{c'} y$ equal to c'.
- (g) If $y = (a, c, n) \in G'$ and $c' \in \mathbb{Z}$ are such that $c' \neq a$ and $L_{c'} y$ is defined, then $L_{c'} y \neq c'$.

Lemma 17.6 (Existence of partial solution)**.** *A partial solution exists.*

Proof. We define $L_{c'} y$ for $y = (a, c, n) \in G'$ as follows:

- (i) If $c' = a$ and $n = 0$, then $L_{c'} y := a$.
- (ii) If $c' = a$ and $n \neq 0$, then $L_{c'} y := (a, c, 0)$.
- (iii) If $c' = c_{y,b}$ for some b, then $L_{c'} y := b$.
- (iv) In all other cases, $L_{c'} y$ is undefined.

We of course also define $L_{c'} y$ for $y \in \mathbb{Z}$ using Theorem 17.4.

From Lemma 17.5 we see that this is a well-defined operation, with $L_c y$ undefined for any $y = (a, c, n) \in G'$. So properties (a)-(e) and (g) are clear from construction. Property (e) is also clear from construction in each of the three cases (i), (ii), (iii) (for (i), (ii) we also use the fact that $L_a a = a$). □

We can make $L_{c'} y$ defined in a partial solution:

Lemma 17.7 (First extension)**.** *Suppose we have a partial solution for which $L_{c'} y$ is currently undefined for some $c' \in \mathbb{Z}$ and $y \in G$. Then one can extend this partial solution in such a manner that $L_{c'} y$ is now defined.*

Proof. Write $y = (a, c, n)$. Because $L_a : \mathbb{Z} \to \mathbb{Z}$ and $L_{c'} : \mathbb{Z} \to \mathbb{Z}$ are surjective, we can find $b \in \mathbb{Z}$ such that $L_a L_{c'} b = c'$. If we had $b = c'$, then $L_a c' = c'$, which from (17.1) (and $Sc' = c'$) implies that $a = c'$, which contradicts the undefined nature of $L_{c'} y$ thanks to properties (b), (c) of a partial solution. Hence, $b \neq c'$. We then set $L_{c'} y := b$. It is then clear that all the properties (a)-(g) of a partial solution are maintained. □

We can also insert inverses of $L_{c'}$:

Lemma 17.8 (Second extension)**.** *Suppose we have a partial solution, and let $c' \in \mathbb{Z}$ and $y = (a, c, n) \in G$. Then, unless one is in the case when $c' = a$ and $n = 0$, then one can find $z \in G$ such that $L_{c'} z$ is currently undefined, but for which one can find an extension of the partial solution for which $L_{c'} z$ is now equal to y.*

Proof. Write $y = (a, c, n)$. There are several cases.

- Case 1: $L_{c'} y = w$ for some $w \in G'$. By Lemma 17.5, $c_{w,c'}$ is distinct from c', and from property (d) of a partial solution, $L_{c_{w,c'}} w = c'$. By property (e) of a partial solution, we can find $z = (c_{w,c'}, c', n')$ such that $L_{c'} z$ is currently undefined. Then set $L_{c'} z := y$, so that we have $L_{c_{w,c'}} L_{c'} L_{c'} z = c'$. One then verifies that all the axioms (a)-(g) of a partial solution are valid in this case.

- Case 2: $c' \neq a$ and $L_{c'}y = b$ for some $b \in \mathbb{Z}$. By property (g) of a partial solution, $c' \neq b$. By Theorem 17.4, we can find a' such that $L_{a'}b = R_b a' = c'$ and $a' \neq c'$. By property (e) of a partial solution, we can find $z = (a', c', n')$ such that $L_{c'}z$ is currently undefined. Then set $L_{c'}z = y$, so that we have $L_{a'}L_{c'}L_{c'}z = c'$. One then verifies that all the axioms (a)-(g) of a partial solution are valid in this case.
- Case 3: $c' \neq a$ and $L_{c'}y$ is currently undefined. Use Lemma 17.7 set $L_{c'}y$ equal to some $b \in \mathbb{Z}$, then apply the Case 2 analysis.
- Case 4: $c' = a$. Because we are excluding the case $n = 0$, we are now in Case 1 thanks to property (c) of a partial solution.

□

Now we can establish Axiom B.

Proposition 17.9 (Obtaining Axiom B)**.** *There exists a way to extend $L_b : \mathbb{Z} \to \mathbb{Z}$ to $L_b : G \to G$ for all $b \in \mathbb{Z}$, in such a way that Axiom B holds, and furthermore for each $b \in \mathbb{Z}$ and $x \in G'$, the set $\{y \in G' : L_b y = x\}$ is infinite. Also, we can ensure that $L_b x \neq x$ for any $b \in \mathbb{Z}$ and $x \in G'$.*

Proof. By iterating Theorem 17.7 and Theorem 17.8 in alternation, we can find an increasing chain of partial solutions with the property that for any $y = (a, c, n) \in G'$ and $c' \in \mathbb{Z}$ and any natural number k, excluding the case where $c' = a$ and $n = 0$, that one can find a partial solution on this chain for which $L_{c'}y$ is defined, and such that $L_{c'}z = y$ for at least k distinct choices of $z \in G'$. Taking the limit of this chain, we can then find a fully defined operation $L_{c'}y$ for $c' \in \mathbb{Z}$ and $y \in G$ obeying the properties (a)-(d), (f), (g) (but not (e)) of a partial solution, with the property that $y = (a, c, n) \in G'$ and $c' \in \mathbb{Z}$, excluding the case $c' = a$ and $n = 0$, that there are infinitely many $z \in G'$ such that $L_{c'}z = y$. The excluded case $c' = a, n = 0$ is also covered by property (b) of a partial solution. The claim follows. □

Finally, we construct the remaining L_x.

Proposition 17.10 (Obtaining Axioms A, C)**.** *One can find maps $L_x : G \to G$ for each "non-square" $x \in G'$, such that Axioms A, C hold.*

Proof. We can work with a single $x \in G'$. Our task is to find a function L_x for which

$$L_x x = Sx \tag{17.4}$$

and

$$L_{Sy}L_x L_x y = x \tag{17.5}$$

for all $y \in G$ (note that L_{Sy} is already fully constructed).

Define a *seed* to be an injective partial function L_x defined on finitely many values and obeying Equation (17.4), as well as Equation (17.5) whenever $L_x L_x y$ is defined. If there is a $y \in G$ for which $L_x y$ is currently undefined, then by hypothesis y is equal to $L_x z$ for at most one z. If such a z exists, we set $L_x y$ to be an element of $\{w : L_{Sz}w = x\}$ different from y that is not already in the domain or range of L_x; we are able to do so thanks to the infinite surjectivity (Theorem 17.4 (ii)) and the fact that the domain and the range of L_x are finite. If no such z exists, we set $L_x y$ to be arbitrary element of G not already in the domain or range. In either case, we see that the seed property is preserved. Starting from the seed in which L_x is only defined on x and maps it to Sx, we obtain the claim. □

Corollary 17.11. *There exists a 1516 magma that does not obey the 255 equation*

$$x = ((x \diamond x) \diamond x) \diamond x.$$

Proof. Let us define the element $x_0 := (0, 1, 0) \in G'$. Since $Sx_0 = 0$, we know that $0 \diamond x_0 = 0$ (see the first part of the proof of Theorem 17.9). Therefore, x_0 does not obey the 255 equation, as we have

$$((x_0 \diamond x_0) \diamond x_0) \diamond x_0 = (0 \diamond x_0) \diamond x_0 = 0 \diamond x_0 = 0 \neq x_0.$$

□

Chapter 18

Equation 1729

In this chapter we study magmas that obey equation 1729,

$$x = (y \diamond y) \diamond ((y \diamond x) \diamond y). \tag{18.1}$$

for all x, y. Using the squaring operator $Sy := y \diamond y$ and the left and right multiplication operators $L_y x := y \diamond x$ and $R_y x = x \diamond y$, this law can be written as

$$L_{Sy} R_y L_y x = x.$$

This implies that L_y is injective and L_{Sy} is surjective, hence L_{Sy} is invertible. If y is a square (i.e., $y \in SM$), then L_y and L_{Sy} are both invertible, hence now R_y is also invertible, with inverse $R_y^{-1} = L_y L_{Sy}$. We rewrite this as

$$L_y = R_y^{-1} L_{Sy}^{-1} \tag{18.2}$$

for all $y \in SM$.

We have the following procedure for extending a small magma SM obeying Equation (18.1) to a larger one M:

Theorem 18.1 (Extending a 1729 magma)**.** *Let SM be a magma obeying 1729, and let N be another set disjoint from SM, and set $M := SM \uplus N$. Suppose that we have a squaring map $S' : N \to SM$ (which will complement the existing squaring map $S : SM \to SM$), and bijections $L'_a, R'_a : N \to N$ for all $a \in SM$ (which will complement the existing bijections $L_a, R_a : SM \to SM$ coming from SM), obeying the following axioms:*

- *(i) For all $a \in SM$, we have $L'_a = (R'_a)^{-1}(L'_{Sa})^{-1}$.*
- *(ii) For all $y \in N$, the elements $R'_a y \in N$ are distinct from each other and from y as $a \in SM$ varies.*
- *(iii) If $R'_a x = y$ for some $a \in SM$ and some $x, y \in N$, then $L'_{S'y} L_{L^{-1}_{S'x} a} y = x$.*
- *(iv) For all $x \in N$, we have $(L'_{S'x})^2 x = x$.*

Suppose also that we have an operation $\diamond' : N \times N \to M$ obeying the following axioms:

- *(v) For all $x \in N$, we have $x \diamond' x = S'x$.*
- *(vi) For all $y \in N$ and $a \in SM$, we have $R'_a y \diamond' y = L^{-1}_{S'y} a$.*

- *(vii) For all $x, y \in N$ with $x \diamond' y$ not already covered by rules (v) or (vi), we have $x \diamond' y = z$ for some $z \in N$. Furthermore, $z \diamond' x = (L'_{S'x})^{-1} y$.*

Then one can endow M with an operation $\diamond'' : M \times M \to M$ obeying 1729 defined as follows:

- *If $a, b \in SM$, then $a \diamond'' b = a \diamond b$.*
- *If $a \in SM$ and $x \in N$, then $a \diamond'' b := L'_a b$.*
- *If $x \in N$ and $a \in SM$, then $b \diamond'' a := R'_a b$.*
- *If $x, y \in N$, then $x \diamond'' y := x \diamond' y$.*

Furthermore, the 817 law $x \diamond'' SS'x = x$ fails for any $x \in N$.

Proof. We need to show that $\diamond''$ verifies the law Equation (18.1). In the case when $x, y \in SM$, then the claim follows from the fact that SM already obeyed this equation. If x was equal to an element $a \in SM$ and $y \in N$, then by construction the law is equivalent to $L'_{Sa} R'_a L'_a y = y$, which follows from axiom (i).

Now suppose that $x \in N$ and y is equal to some element a of SM. From axiom (v) we have $x \diamond'' x = S'x$, and then this case of Equation (18.1) becomes

$$L_{S'x}(R'_a x \diamond' x) = a$$

which follows from axiom (vi). So the only remaining case is when $x, y \in N$. Using axiom (ii), we can divide into cases:

- Case 1: $x = y$. Then by (v) we need to show that $L'_{S'x} L'_{S'x} x = x$, which follows from axiom (iv).
- Case 2: $y = R'_a x$ for some $a \in SM$. Then by axiom (vi), we need to show that $L'_{S'y} L'_{L^{-1}_{S'x} a} y = x$, which follows from axiom (iii).
- Case 3: We are not in case 1 or case 2. Then by axiom (vii), we have $y \diamond'' x = z$ for some $z \in N$ with $z \diamond'' y = (L'_{S'y})^{-1} x$. But this implies $L'_{S'y}(z \diamond'' y) = x$, which is Equation (18.1).

We have now verified that $\diamond''$ obeys 1729. For any $x \in N$, we have $x \diamond'' SS'x = R'_{SS'x} x$, and so the final claim follows from axiom (ii). □

To build a magma obeying 1729 but not 817, it thus suffices to produce

- a 1729 magma SM;
- a set N of "non-squares";
- a squaring map $S' : N \to SM$;
- bijections $L'_a, R'_a : N \to N$ for all $a \in SM$ obeying the axioms (i)-(iv); and
- an operation $\diamond' : N \times N \to SM \uplus N$ obeying the axioms (v)-(vii).

The magma SM is defined as follows:

Definition 18.2 (Definition of SM)**.** Take SM to be a countably infinite abelian group of exponent 4, generated by generators E_n for $n \in \mathbb{N}$ subject to the relations $4E_n = 0$.

Lemma 18.3 (Basic properties of SM)**.** *SM is a 1729 magma, the squaring operation $S : SM \to SM$ is just the doubling map $Sa = 2a$, and the double squaring map $S^2 : SM \to SM$ is constant: $S^2 a = 0$ for all $a \in SM$.*

Proof. Routine verification. □

We now define N, as well as some Cayley graph structures on it.

Definition 18.4 (Definition of N)**.** Take N to be the free non-abelian group with a generator e_a for each $a \in SM$, thus N is the set of reduced words using the alphabet e_a, e_a^{-1}. Two elements $x, y \in SM$ are said to be *adjacent* if $x = e_a y$ or $y = e_a x$ for some $a \in SM$; this defines a left Cayley graph on N. We make a partial ordering $\leq$ on N by declaring $y \leq x$ if y is a right subword of x (or equivalently, y is on the unique simple path from 1 to x). For instance, if $a, b, c \in SM$ are distinct, then

$$1 \leq e_c \leq e_b^{-1} e_c \leq e_a e_b^{-1} e_c.$$

If $x \in N$ is not the identity, we define the *parent* of x to be the unique element $y \in N$ adjacent to x whose reduced word is shorter. For instance, the parent of $e_a e_b^{-1} e_c$ is $e_b^{-1} e_c$.

Lemma 18.5 (Basic properties of N)**.** *N is countable, and $\leq$ is a partial ordering.*

Proof. Routine verification. □

We will define the right multiplication operators $R'_a : N \to N$ using the group action:

Definition 18.6 (Definition of R'_a)**.** We set

$$R'_a x := e_a x \tag{18.3}$$

for all $a \in SM$ and $x \in N$.

Lemma 18.7 (Basic properties of R'_a)**.** *The operators R'_a are bijective and obey axiom (ii).*

Proof. Routine verification. □

We defer construction of the squaring map $S' : N \to SM$ for now, but turn to left-multiplication. From two applications of Equation (18.2) and the exponent 4 hypothesis we have

$$L'_a = (R'_a)^{-1} (L'_{2a})^{-1} = (R'_a)^{-1} L'_0 R'_{2a}.$$

Thus, once L'_0 is specified, we can *define* L'_a for all other $a \in SM$ by the rule

$$L'_a := (R'_a)^{-1} L'_0 R'_{2a}. \tag{18.4}$$

Furthermore, from the $a = 0$ case of Equation (18.2) we must also have the axiom

- (i') $(L'_0)^2 = (R'_0)^{-1}$.

Conversely, we have

Lemma 18.8 (Using L'_0 to construct L'_a)**.** *Suppose we have a bijection $L'_0 : N \to N$ that obeys axiom (i'), and then define L'_a for all $a \in SM$ by the formula (18.4). Then this recovers L'_0 when $a = 0$ (to formalize this it may be convenient to give L'_0 and L'_a distinct names), and the L'_a are all bijections and obey axiom (i). Furthermore, we have*

$$(L'_a)^{-1} := (R'_{2a})^{-1} L'_0 R'_0 R'_a \tag{18.5}$$

for all $a \in SM$.

Proof. Routine verification. □

We now write the other remaining axioms in terms of L'_0 rather than L'_a using Equation (18.4), Equation (18.5), Equation (18.3), and the magma law on SM:

- (iii') If $R'_a x = y$ for some $a \in SM$ and some $x, y \in N$, then $(R'_{S'y})^{-1} L'_0 R'_{2S'y} (R'_{a-S'x})^{-1} L'_0 R'_{2(a-S'x)} y = x$.
- (iv') For all $x \in N$, we have $(R'_{S'x})^{-1} L'_0 R'_{2S'x} (R'_{S'x})^{-1} L'_0 R'_{2S'x} x = x$.
- (v) For all $x \in N$, we have $x \diamond' x = S'x$.
- (vi') For all $y \in N$ and $a \in SM$, we have $e_a y \diamond' y = a - S'y$.
- (vii') For all $x, y \in N$ with $x \diamond' y$ not already covered by rules (v) or (v'), we have $x \diamond' y = z$ for some $z \in N$. Furthermore, $z \diamond' x = (R'_{2S'x})^{-1} L'_0 e_0 e_{S'x} y$.

Lemma 18.9 (Reduction to new axioms)**.** *Suppose we can find a function $S' : N \to SM$, a bijection $L'_0 : N \to N$, and an operation $\diamond' : N \times N \to SM \uplus N$ obeying axioms (i'), (iii'), (iv'), (v), (vi'), (vii'). Then there exists a magma obeying 1729 but not 817.*

Proof. Construct the L'_a using Theorem 18.8. By Theorem 18.7 and direct verification we can noe verify axioms (i)-(vii), and then the claim follows from Theorem 18.1. □

Our task is now to find a function $S' : N \to SM$, a bijection $L'_0 : N \to N$, and an operation $\diamond' : N \times N \to M$ obeying axioms (i'), (iii'), (iv'), (v), (vi'), (vii').

We will again use a greedy construction for this, but with some modifications. Firstly, the axiom (i'), together with (18.3) means that we cannot restrict L'_0 to be partially defined on just finitely many values: any relation of the form

$$L'_0 x = y$$

for some $x, y \in N$ would automatically imply that

$$L'_0 (R'_0)^n x = (R'_0)^n y \tag{18.6}$$

and also

$$L'_0 (R'_0)^n y = (R'_0)^{n-1} x \tag{18.7}$$

for all $n \in \mathbb{Z}$. Thus, L'_0 becomes defined on two right cosets $\langle e_0 \rangle x$, $\langle e_0 \rangle y$ of N, where $\langle e_0 \rangle := \{e_0^n : n \in \mathbb{Z}\}$ is an infinite cyclic subgroup of N. In general, we will require that L'_0 is defined on a finite union of cosets of $\langle e_0 \rangle$.

In a somewhat similar vein, axiom (vii'), if iterated naively, would mean that a given entry $x \diamond' y = z$ of the multiplication table could potentially generate an infinite sequence of further entries, which unfortunately do not have as regular a pattern as the iterations Equation (18.6), Equation (18.7) of axiom (i'). So we will need to truncate this iteration by creating an addition category of "pending" identities $I[x, y, z]$ of the form "$z \diamond' x = (R'_{2S'x})^{-1} L'_0 R'_0 e_{S'x} y$" for some $x, y, z \in N$, which will be temporarily undefined because $S'x$ is undefined. More precisely,

Definition 18.10 (Partial solution)**.** A *partial solution* $(L'_0, \diamond', S', \mathcal{I})$ is a collection of the following data:

- A partially defined function $L'_0 : N \to N$, defined on a finite union of right cosets of $\langle e_0 \rangle$;
- A partially defined operation $\diamond' : N \times N \to M$, defined on a finite set;

- A partially defined function $S' : N \to SM$, defined on a finite set; and
- A finite collection $\mathcal{J}$ of "pending identities" $I[x,y,z]$, which one can think of either as ordered triples of elements $x,y,z \in N$, or as formal strings of the form "$z \diamond' x = (R'_{2S'x})^{-1} L'_0 R'_0 R'_{S'x} y$" for some $x,y,z \in N$.

Furthermore, the following axioms are satisfied:

- (i") $L'_0 x$ is defined and equal to y, then we have the identities Equation (18.6), Equation (18.7) for all $n \in \mathbb{Z}$.
- (S) If $S'x$ is defined for some $x \in N$, then $S'y$ is defined for all $y \leq x$.
- (iii") If $R'_a x = y$ for some $a \in SM$ and some $x,y \in N$, and $S'x, S'y$ are defined, then $(R'_{S'y})^{-1} L'_0 R'_{2S'y} (R'_{a-S'x})^{-1} L'_0 R'_{2(a-S'x)} y$ is defined and equal to x.
- (iv") If $x \in N$ is such that $S'x$ is defined, then $(R'_{S'x})^{-1} L'_0 R'_{2S'x} (R'_{S'x})^{-1} L'_0 R'_{2S'x} x$ is defined and equal to x.
- (v") If $x \in N$ and $x \diamond' x$ is defined, then $S'x$ is defined and equal to $x \diamond' x$.
- (vi") For all $y \in N$ and $a \in SM$, if $R'_a y \diamond' y$ is defined, then $a - S'y$ is defined and equal to $R'_a y \diamond' y$.
- (vii") For all $x,y \in N$ and x is not equal to y or $R'_a y$ for any $a \in SM$, and $x \diamond' y$ is defined, then it is equal to some $z \in N$. Furthermore, either $I[x,y,z]$ is a pending identity, or else $z \diamond' x$ and $(R'_{2S'x})^{-1} L'_0 R'_0 R'_{S'x} y$ are defined and equal to each other.
- (P) If $I[x,y,z]$ is a pending identity, then $x,y,z \in N$, and Sx and $z \diamond' x$ are undefined. Furthermore, z is not equal to x or $R'_a x$ for any $a \in SM$, and y is not of the form $(R'_0)^n x$ or $(R'_0)^n y_0$ for any n, where y_0 is the parent of x.
- (P') If $I[x,y,z]$ and $I[x,y',z]$ are pending identities, then $y = y'$.
- (P") If $I[x,y,z]$ is a pending identity, then $x \diamond' y = z$.
- (L) If y is the parent of x with $x = R'_a y$, and $(R'_{a-S'y})^{-1} L'_0 R'_{2(a-S'y)} x$ is defined, then it is not equal to x.

We say that one partial solution $(\tilde{L}'_0, \tilde{\diamond}', \tilde{S}', \tilde{\mathcal{J}})$ *extends* another if $(L'_0, \diamond', S', \mathcal{J})$ if $\tilde{L}'$ is an extension of L'_0, $\tilde{\diamond}'$ is an extension of $\diamond'$, and $\tilde{S}'$ is an extension of S'. (No constraint is imposed on the final components $\tilde{\mathcal{J}}, \mathcal{J}$.) This is a preordering.

Lemma 18.11 (Existence of partial solution)**.** *There exists a partial solution.*

Proof. Set $L'_0, \diamond', S'$ to be empty functions, and have the set of pending identities to also be empty. The verification of the required axioms is then routine. □

Lemma 18.12 (Chain of partial solutions)**.** *Suppose that one has a sequence $(L'_{0,n}, \diamond'_n, S'_n, \mathcal{J}_n)$ of partial solutions, each one an extension of the previous, such that for any $x,y \in N$, $L'_{0,n} x$, $x \diamond'_n y$, and $S'_n x$ are defined for some n. Then there exists a 1729 magma that does not obey 817.*

Proof. Take the direct limit of the chain to obtain total functions $L'_0, \diamond', S'$. The axioms (i'), (iii'), (iv"), (v"), (vi"), (vii") of the partial solutions then easily imply that the direct limit obeys the axioms (i'), (iii'), (iv'), (v), (vi'), (vii') (one also uses axiom (P) to note that all pending identities disappear in the direct limit). The claim now follows from Theorem 18.9. □

Now we seek to enlarge a partial solution. We first make an easy observation:

Proposition 18.13 (Enlarging L'_0)**.** *Suppose one has a partial solution in which $L'_0 x$ is undefined for some $x \in N$. Then one can extend the partial solution so that $L'_0 x$ is now defined.*

Proof. By axiom (i"), $L'_0 (R'_0)^n x$ is undefined for every integer n. Let $d = E_m$ be a generator of SM that does not appear as a component of any index of any of the generators e_a appearing anywhere in the partial solution; such a d exists due to the finiteness hypotheses. We set $L'_0 x := e_d$, and then extend by Equation (18.6), Equation (18.7), thus

$$L'_0 (R'_0)^n x := (R'_0)^n e_d$$

and

$$L'_0 (R'_0)^n e_d := (R'_0)^{n-1} x.$$

Because of the new nature of d, no collisions in the partial function L_0 are created by this operation. It is then easy to check that axiom (i") is preserved by this operation, whereas none of the other axioms (S), (iii"), (iv"), (v"), (vi"), (vii"), (P), (P'), (P") are affected by this extension. With some effort, axiom (L) can also be verified. □

As a corollary, we have

Proposition 18.14 (Enlarging L'_0 many times)**.** *Suppose one has a partial solution. Let A be a finite subset of N. Then one can extend the partial solution so that $L'_0 x$ is now defined for all $x \in A$.*

Proof. Iterate Proposition 18.13 in the obvious fashion. □

Next, we provide a tool for enlarging the domain of definition of S'. The main step is the following inductive one with extra axioms.

Proposition 18.15 (Enlarging S' with induction hypothesis and axioms)**.** *Suppose one has a partial solution in which $S'x$ is undefined for some $x \in N$, but $S'y$ is defined for all $y < x$. (This hypothesis is vacuous for $x = 1$.) Let y_0 be the parent of x (if $x \neq 1$), and assume the following additional axioms:*

- *(A) If $R'_a x = y_0$ for some $a \in SM$, then $L'_0 R'_{S'y_0} x$ is defined.*
- *(B) If $x = R'_a y_0$ for some $a \in SM$, then $L'_0 R'_{2(a - S'y_0)} x$ is defined.*
- *(C) If $I[x, y, z]$ for some $y, z \in N$, and $S'z$ is defined, then $L'_0 R'_0 R'_{S'z} x$ is defined.*

Then one can extend the partial solution so that $S'x$ is now defined.

Proof. Let $d_0, d_1 \in SM$ be generators E_{n_0} of SM that do not appear in the index a of any e_a that currently appears in the partial solution (of which there are only finitely many). We also set some further distinct generators $d'_{y,z} \in SM$ for $y, z \in SM$ that are distinct from each other and all previous generators (this is possible as we have infinitely many generators). We set $S'x, x \diamond' x := d_0$; this preserves axiom (S) and (v"). We set

$$L'_0 R'_{2d_0} x := e_{d_1}$$

$$L'_0 R'_{2d_0} (R'_{d_0})^{-1} e_{d_1} := R'_{d_0} x$$

and then extend these choices using Equation (18.6), Equation (18.7) to recover axiom (i'), thus for instance

$$L'_0 (R'_0)^n R'_{2d_0} x := (R'_0)^n e_{d_1}$$

and

$$L'_0 (R'_0)^n e_{d_1} := (R'_0)^{n-1} R'_{2d_0} x$$

for all $n \in \mathbb{Z}$.

To retain axiom (iii"), we perform the following actions:

- If y_0 is undefined, do nothing.
- If $R'_a x = y_0$ for some $a \in SM$ (so that $L'_0 R'_{S'y_0} x$ is defined, by hypothesis (A)), set $L'_0 R'_{2(a-d_0)} y_0 := R'_{a-d_0} (R'_{2S'y_0})^{-1} R'_0 L'_0 R'_{S'y_0} x$. Then extend using Equation (18.6), Equation (18.7).
- If $x = R'_a y_0$ for some $a \in SM$ (so that $L'_0 R'_{2(a-Sy_0)} x$ is already defined, by hypothesis (B)), set $L'_0 R'_{2d_0} (R'_{a-S'y_0})^{-1} L'_0 R'_{2(a-Sy_0)} x := R'_{d_0} y_0$, and extend using Equation (18.6), Equation (18.7).

To retain axiom (P), we perform the following actions for each pending identity of the form $I[x,y,z]$ for some y, z, executed in some arbitrary order.

- Remove this identity $I[x,y,z]$ from the list of pending identities.
- Set $L'_0 R'_0 R'_{d_0} y := e_{d'_{y,z}}$, and $x' \diamond y' := z'$, where $(x', y', z') := (z, x, (R'_{2d_0})^{-1} e_{d'_{y,z}})$. Extend all the new definitions of L'_0 using Equation (18.6), Equation (18.7).
- If $S'x'$ is undefined, add $I[x', y', z']$ as a pending identity.
- If instead $S'x'$ is defined (which makes $L'_0 R'_0 R'_{S'x'} y'$ defined, by axiom (C)), set $x'' \diamond y'' = z''$, where $(x'', y'', z'') := (z', x', (R'_{2S'x'})^{-1} L'_0 R'_0 R'_{S'x'} y')$. Then add $I[x'', y'', z'']$ as a pending identity.

One can check that these definitions do not cause any collisions in the partial function L'_0, and that axioms (i'), (iii'), (iv"), (v"), (vii"), (P), (P'), (P") are preserved; the remaining axiom (vi") is unaffected by this extension. Axiom (L) can also be shown to be preserved after a tedious calculation. □

Proposition 18.16 (Enlarging S' with induction hypothesis)**.** *Suppose one has a partial solution in which $S'x$ is undefined for some $x \in N$, but $S'y$ is defined for all $y < x$. (This hypothesis is vacuous for $x = 1$.) Then one can extend the partial solution so that $S'x$ is now defined.*

Proof. Let y_0 be the parent of x, that is to say the unique neighbor of x in the path to 1 (this is only defined for $x \neq 1$), then by axiom (i") y_0 is the unique neighbor for which $S'y_0$ is defined, and we either have $x = R'_a y_0$ or $R'_a x = y_0$ for some unique $a \in SM$.

By using Theorem 18.14, we may impose axioms (A), (B), (C) without loss of generality, as this only imposes a finite set of conditions. The claim now follows from Theorem 18.15. □

As a corollary, we have

Proposition 18.17 (Enlarging S')**.** *Suppose one has a partial solution in which $S'x$ is undefined for some $x \in N$. Then one can extend the partial solution so that $S'x$ is now defined.*

Proof. Obtained by induction from Proposition 18.16, using the fact that there are no infinite descending chains in N. □

Finally, we give a tool for enlarging $\diamond$:

Proposition 18.18 (Enlarging $\diamond$)**.** *Suppose one has a partial solution in which $x \diamond' y$ is undefined for some $x, y \in N$. Then one can extend the partial solution so that $x \diamond' y$ is now defined.*

Proof. By applying Theorem 18.17 as needed, we may assume without loss of generality that $S'x$ and $S'y$ are already defined (among other things, this removes the possibility that $x \diamond' y$ is part of a pending identity). If this makes $x \diamond' y$ defined, then we are done, so we may assume that this is not the case.

Similarly, by using Theorem 18.13, we may assume without loss of generality that $L'_0 R'_0 R'_{S'x} y$ is defined.

We now divide into cases:

Case 1: $x = y$. In this case we set $x \diamond' y := S'x$. It is clear that this preserves axiom (v"), and no other axiom is impacted.

Case 2: If $x = R'_a y$ for some $a \in SM$, then we set $x \diamond' y := a - S'y$. This preserves axiom (vi"), and no other axiom is impacted.

Case 3: If x is not equal to y or $R'_a y$ for any $a \in SM$. Let $d_0 \in SM$ be a generator that does not appear as a component of any index of any of the generators e_a appearing anywhere in the partial solution. We set $x \diamond' y := z$ with $z := e^2_{d_0}$.

This temporarily disrupts axiom (vii"). To recover it, we perform the following actions.

- Set $x' \diamond' y' = z'$, where $(x', y', z') := (z, x, (R'_{2S'x})^{-1} L_0 R'_0 R'_{Sx} y)$.
- Add $I[x', y', z']$ as a pending identity.

One can check that these definitions do not cause any collisions in the partial function L'_0, and that axioms (i'), (vii'), (P), (P') are preserved; the remaining axioms (S), (iii"), (iv"), (v"), (vi") are unaffected by this extension. □

Theorem 18.19 (1729 does not imply 817)**.** *There exists a magma that obeys equation 1729 but not equation 817.*

Proof. Starting from Theorem 18.11 and applying Theorem 18.13, Theorem 18.17, Theorem 18.18 alternatingly, one can find a chain of partial solution that are total in the limit. The claim now follows from Theorem 18.12. □

Chapter 19

Rewriting theory

We briefly recall the basics of rewrite theory necessary to our exposition, following mostly Baader and Nipkow [3], and generally omitting proofs when they can be found there.

We first work in the abstract taking an arbitrary set A, with a given equivalence relation over it which we denote $\approx$. We consider a relation R over A.

Definition 19.1. We write $a \to b$ if $a \ R \ b$ holds in A, and say that a *rewrites to* (or *reduces to*) b. We further define

- $\to^+$ as the transitive closure of R.
- $\to^*$ as the reflexive transitive closure of R.
- $\leftrightarrow^*$ as the reflexive transitive and symmetric closure of R.

We sometimes write $b \leftarrow a$, (resp. $b \ ^* \leftarrow a$ etc) to mean $a \to b$ (resp. $a \to^* b$ etc), and chain notations, e.g. $b_1 \leftarrow a \to b_2$.

Note that $\leftrightarrow^*$ is an equivalence relation and the hope is for it to be equal to $\approx$, in order to deduce properties of the latter.

One should first note that if even R is contained in $\approx$, then so are $\to^+, \to^*$ and $\leftrightarrow^*$ (as it is an equivalence relation), so we will focus on that case. Generally $a \to^* b$ can be seen as a way to *compute* the $\approx$ relation, as it is directed, in a way to constrain our search space.

However, in general, we cannot deduce the converse, so it may be the case that $a \approx b$ but neither $a \to^* b$ nor $b \to^* a$ nor even is there a single c such that $a \to^* c \ ^* \leftarrow b$, as the number of "left-right alternations" may be arbitrarily large.

The following properties are going to be very useful to deduce exactly such a converse.

Definition 19.2. We say that R is *Church-Rosser* if whenever $a \leftrightarrow^* b$, there exists some c such that

$$a \to^* c \ ^* \leftarrow b$$

We say that R is *confluent* if whenever $b_1 \ ^* \leftarrow a \to^* b_2$ there exists some c such that $b_1 \to^* c \ ^* \leftarrow b_2$.

We say that R is *locally confluent* if whenever $b_1 \leftarrow a \to b_2$ there exists some c such that $b_1 \to^* c \ ^* \leftarrow b_2$.

We say that (an arbitrary) a is in *normal form* (or a is a normal form) if there is no $a' \neq a$ such that $a \to a'$, and that R is *weakly normalizing* if for every a, there is some a' such that $a \to^* a'$ and a' is in normal form.

We say that R is *strongly normalizing* if there are no infinite rewrite sequences $a_1 \to a_2 \to \ldots$. In particular, a strongly normalizing R is also weakly normalizing.

It turns out that if R is strongly normalizing and Church-Rosser, and effective (we can "compute" with it) then the problem of equivalence is decidable! This is because of the following lemma.

Lemma 19.3. *If R is Church-Rosser, then any normal form is* unique.

This means that, in this situation, a and b reduce to an identical normal form c *if and only if* $a \leftrightarrow^* b$! This means that we have the following algorithm to decide $a \leftrightarrow^* b$ (and therefore $a \approx b$ if these relations coincide):

1. Repeatedly apply R to a and b until normal forms a' and b' are found for them (this is possible because R is strongly normalizing).
2. Compare a' and b' for exact equality (sometimes called "syntactic equality").
3. If $a' = b'$, we can conclude $a \leftrightarrow^* b$.
4. If $a' \neq b'$ can can conclude that they are *not* equivalent due to the lemma.

Note that weak normalization does not change much here except at step 1, where we need to pick reductions which eventually bring the elements to normal forms.

The strategy is therefore, for a given $\approx$ to find an R which is (strongly) normalizing and Church-Rosser, and such that $\leftrightarrow^* = \approx$. This is roughly the goal of the entire field of *completion*. We call such an R *complete for* $\approx$.

The task is helped by the following facts, which we state here also without proof.

Theorem 19.4. *1. R is Church-Rosser iff it is confluent.*

2. (Newman's lemma) if R is strongly normalizing, then R is confluent iff it is locally confluent.

This can be leveraged by looking at the particulars of the equivalence relation of interest, namely quantified equations over syntactic trees as in Chapter 10, and a theory Γ, which we will usually take to be finite (usually it will have a single equation!).

We will therefore consider relations over the set of elements of the free magma M_X, and the aim is to find a rewrite system R is complete for $\simeq$.

Certainly $\simeq$ is closed over substitutions, and be a *congruence*: if $a \simeq a'$ and $b \simeq b'$ under Γ, then $a \diamond b \simeq a' \diamond b'$ under Γ as well.

We therefore consider R to be both closed under substitutions and a congruence. A convenient way to represent this is via a *rewrite system*: simply a set of pairs of words $(l, r) \in M_X$ (we typically write $l \to r$) which represents the smallest congruence, closed by substitutions that contains those pairs.

Naturally, a set of laws $w \simeq w'$ can be seen, given a choice of orientation (left-to-right or right-to-left) for each law as such a rewrite system. In this case, it is very clear that the reflexive transitive closure $\leftrightarrow^*$ recovers the original equational theory $\Gamma \vDash \cdot \simeq \cdot$. However, it's clear that sometimes these systems will either be not strongly normalizing, or confluent, or both.

For example, it's clear that commutativity (the rule $x \cdot y \simeq y \cdot x$ cannot possibly be oriented. Here is a non-confluent example:

$$x \cdot (y \cdot z) \to y$$

We have $a \cdot (b \cdot (c \cdot d)) \to^* b$, but also $a \cdot (b \cdot (c \cdot d)) \to^* a \cdot c$ for any a, b, c, d (which are both in normal form).

Knuth and Bendix [8] described a technique by which a theory or set of equations Γ could be turned into a complete system. The crucial idea is the observation that the non-local-confluence of a rewrite system can be reduced to a finite (if the system is finite) set of "worst offenders" for confluence. If these pairs can be *joined* (reduced to the same term) then the system is confluent. It is possible to compute such pairs.

The high-level idea is therefore to identify such pairs, and add them as an unoriented equation, to be oriented if possible, and repeating until no un-joinable pairs exist. If this procedure succeeds and terminates, the system is successfully completed, and as a result the theory Γ is decidable, via the completed system as described above.

We use the intuitive notions of "position in a word" and "word at a position p". We denote by $w[w']_p$ the word w with w' inserted at position p.

Definition 19.5. Given a rewrite system R and two rules $\rho_1 : l_1 \to r_1$ and $\rho_2 : l_2 \to r_2$ in R, we say that (t, u) is a *critical pair* for ρ_1 and ρ_2 if there is some non-variable position p in l_1 such that l_2 unifies with the term at that position. We denote by σ the most general unifier thus obtained and have $t = r_1\sigma$ and $u = l_1\sigma[r_2\sigma]_p$

Note that, in the above setting, $t \leftarrow l_1\sigma \to u$, giving us a candidate for non-local-confluence. The next lemma states that these candidates are the most general ones.

Theorem 19.6. *Given a rewrite system R, if for every critical pair (t, u) of R, there is a term v such that $t \to^* v \ ^* \leftarrow u$, then R is locally confluent.*

Note that building critical pairs of a finite system is computable. Therefore the only step of the completion process which require genuine creativity is the choice of the orientation of the equations, along with the proof that that orientation is strongly normalizing.

As a capper to this section we can note that even in the event that such an orientation is not found, one can still partially apply the completion procedure, using any well-founded order on terms that is stable by substitution and congruence, to obtain a semi-decision procedure for equality. This process is sometimes called *unfailing completion* and is at the core of the *superposition calculus* used in Vampire.

Chapter 20

Order 5 Austin laws

Chapter 3 has useful background context for this chapter. As noted in Chapter 3: an *Austin law* is a law which admits infinite models, but no nontrivial finite models. Austin laws have order 5 or greater [5]. In this chapter we report partial results of a classification of laws of order 5 on whether they do or do not allow non-trivial finite or infinite models, with a particular interest in finding Austin laws. This work is also discussed in this Zulip thread with results saved on this git branch.

There are 57,882 equations of order 5 (not including the 4,694 equations of order ≤ 4).

- 19,392 (33.5%) admit only trivial models.
- 38,360 (66.2%) have known satisfying finite models (and hence, also infinite models).
- 106 allow only trivial finite models. Of these, 10 are Austin laws, and it is unknown whether the remaining 96 admit infinite models.
- In 24 cases it is unknown whether they allow nontrivial finite models.

Of the equations with known satisfying finite models, a few had a minimum satisfying model size of order 17 (the largest minimum satisfying model size in order ≤ 4 is 7.) One equation was found with a satisfying model of order 26, but the smaller orders were not exhaustively searched so it cannot be established that the order is minimal.

Equations with trivial finite models

106 equations were found that admitted only trivial finite models. Of these, Vampire's decision procedure finished without finding an implication to Equation 2 for 10 equations, allowing us to establish that they are inequivalent, e.g. they allow non-trivial infinite models. Hence, they must be Austin laws. The set of 10 Austin laws includes Theorem 2.54, an Austin law established in [5]. Note that Vampire's decision procedure also establishes that all 10 Austin laws are inequivalent to each other. These laws are listed in Table 20.1.

Of the 96 remaining equations, Vampire did not establish any implications between equations in this set. No effort was made to build infinite models for these equations. This set includes Theorem 2.52, another equation mentioned in [5] as having only trivial finite models, and it being unknown whether it allows infinite models. These laws are listed in Table 20.2.

$x = y \diamond (x \diamond (x \diamond (y \diamond (z \diamond z))))$ (4916)	$x = ((((y \diamond y) \diamond z) \diamond x) \diamond x) \diamond z$ (41082)
$x = y \diamond (((x \diamond (z \diamond z)) \diamond y) \diamond y)$ (15535)	$x = (y \diamond (y \diamond ((z \diamond z) \diamond x))) \diamond y$ (30591)
$x = (y \diamond z) \diamond (x \diamond (z \diamond (z \diamond z)))$ (17522)	$x = (((y \diamond y) \diamond y) \diamond x) \diamond (y \diamond z)$ (28770)
$x = (y \diamond y) \diamond ((z \diamond (x \diamond x)) \diamond z)$ (20034)	$x = (y \diamond ((x \diamond x) \diamond y)) \diamond (z \diamond z)$ (25964)
$x = (y \diamond (x \diamond x)) \diamond ((y \diamond z) \diamond y)$ (22455)	$x = (y \diamond (z \diamond y)) \diamond ((x \diamond x) \diamond y)$ (22818)

Table 20.1: Austin laws

Remaining unknown equations

There are 24 (12 modulo duality) remaining equations, for which we did not establish whether they do or do not admit nontrivial finite models. For one equation, Equation 17260 below, Vampire's decision procedure indicates that it admits nontrivial models, though it is unclear whether it admits nontrivial finite models. These laws are listed in Table 20.3.

$x = y \diamond (x \diamond (y \diamond (y \diamond (z \diamond y))))$ (4952)	$x = ((((y \diamond z) \diamond y) \diamond y) \diamond x) \diamond y$ (41252)
$x = y \diamond (x \diamond (y \diamond (z \diamond (x \diamond z))))$ (4957)	$x = ((((y \diamond x) \diamond y) \diamond z) \diamond x) \diamond z$ (40914)
$x = y \diamond (x \diamond (z \diamond (z \diamond (y \diamond z))))$ (5012)	$x = ((((y \diamond z) \diamond y) \diamond y) \diamond x) \diamond z$ (41253)
$x = y \diamond (y \diamond (x \diamond (y \diamond (z \diamond y))))$ (5066)	$x = ((((y \diamond z) \diamond y) \diamond x) \diamond y) \diamond y$ (41239)
$x = y \diamond (y \diamond (y \diamond (x \diamond (z \diamond y))))$ (5093)	$x = ((((y \diamond z) \diamond x) \diamond y) \diamond y) \diamond y$ (41179)
$x = y \diamond (y \diamond (y \diamond (z \diamond (x \diamond y))))$ (5107)	$x = ((((y \diamond x) \diamond z) \diamond y) \diamond y) \diamond y$ (40951)
$x = y \diamond (y \diamond (z \diamond (y \diamond (x \diamond y))))$ (5141)	$x = ((((y \diamond x) \diamond y) \diamond z) \diamond y) \diamond y$ (40917)
$x = y \diamond (z \diamond (y \diamond (y \diamond (x \diamond y))))$ (5295)	$x = ((((y \diamond x) \diamond y) \diamond y) \diamond z) \diamond y$ (40909)
$x = y \diamond (x \diamond (y \diamond ((z \diamond x) \diamond y)))$ (5833)	$x = (((y \diamond (x \diamond z)) \diamond y) \diamond x) \diamond y$ (40070)
$x = y \diamond (x \diamond (y \diamond ((z \diamond x) \diamond z)))$ (5834)	$x = (((y \diamond (x \diamond y)) \diamond z) \diamond x) \diamond z$ (40037)
$x = y \diamond (x \diamond (y \diamond ((z \diamond y) \diamond y)))$ (5837)	$x = (((y \diamond (y \diamond z)) \diamond y) \diamond x) \diamond y$ (40221)
$x = y \diamond (y \diamond (x \diamond ((z \diamond x) \diamond y)))$ (5947)	$x = (((y \diamond (x \diamond z)) \diamond x) \diamond y) \diamond y$ (40057)
$x = y \diamond (y \diamond (x \diamond ((z \diamond y) \diamond y)))$ (5951)	$x = (((y \diamond (y \diamond z)) \diamond x) \diamond y) \diamond y$ (40208)
$x = y \diamond (y \diamond ((x \diamond y) \diamond (z \diamond y)))$ (6820)	$x = (((y \diamond z) \diamond (y \diamond x)) \diamond y) \diamond y$ (39485)
$x = y \diamond (y \diamond ((z \diamond x) \diamond (x \diamond y)))$ (6878)	$x = (((y \diamond x) \diamond (x \diamond z)) \diamond y) \diamond y$ (39126)
$x = y \diamond (y \diamond ((z \diamond y) \diamond (x \diamond y)))$ (6895)	$x = (((y \diamond x) \diamond (y \diamond z)) \diamond y) \diamond y$ (39163)
$x = y \diamond (y \diamond ((z \diamond z) \diamond (x \diamond y)))$ (6912)	$x = (((y \diamond x) \diamond (z \diamond z)) \diamond y) \diamond y$ (39214)
$x = y \diamond (x \diamond ((y \diamond (z \diamond x)) \diamond y))$ (7587)	$x = ((y \diamond ((x \diamond z) \diamond y)) \diamond x) \diamond y$ (38316)
$x = y \diamond (y \diamond ((x \diamond (z \diamond x)) \diamond y))$ (7701)	$x = ((y \diamond ((x \diamond z) \diamond x)) \diamond y) \diamond y$ (38303)
$x = y \diamond (y \diamond ((z \diamond (x \diamond x)) \diamond y))$ (7755)	$x = ((y \diamond ((x \diamond x) \diamond z)) \diamond y) \diamond y$ (38249)
$x = y \diamond (y \diamond ((z \diamond (x \diamond z)) \diamond y))$ (7763)	$x = ((y \diamond ((z \diamond x) \diamond z)) \diamond y) \diamond y$ (38565)
$x = y \diamond (x \diamond (((z \diamond x) \diamond y) \diamond y))$ (8485)	$x = ((y \diamond (y \diamond (x \diamond z))) \diamond x) \diamond y$ (37519)
$x = y \diamond ((x \diamond y) \diamond (y \diamond (z \diamond y)))$ (9337)	$x = (((y \diamond z) \diamond y) \diamond (y \diamond x)) \diamond y$ (36867)
$x = y \diamond ((x \diamond y) \diamond (z \diamond (y \diamond y)))$ (9345)	$x = (((y \diamond y) \diamond z) \diamond (y \diamond x)) \diamond y$ (36713)
$x = y \diamond ((x \diamond z) \diamond (y \diamond (z \diamond z)))$ (9384)	$x = (((y \diamond y) \diamond z) \diamond (y \diamond x)) \diamond z$ (36714)
$x = y \diamond ((z \diamond x) \diamond (y \diamond (x \diamond y)))$ (9603)	$x = (((y \diamond x) \diamond y) \diamond (x \diamond z)) \diamond y$ (36514)
$x = y \diamond ((z \diamond y) \diamond (x \diamond (x \diamond y)))$ (9663)	$x = (((y \diamond x) \diamond x) \diamond (y \diamond z)) \diamond y$ (36487)
$x = y \diamond ((z \diamond y) \diamond (x \diamond (y \diamond y)))$ (9667)	$x = (((y \diamond y) \diamond x) \diamond (y \diamond z)) \diamond y$ (36638)
$x = y \diamond ((z \diamond y) \diamond (y \diamond (x \diamond y)))$ (9680)	$x = (((y \diamond x) \diamond y) \diamond (y \diamond z)) \diamond y$ (36524)
$x = y \diamond ((x \diamond y) \diamond ((z \diamond x) \diamond y))$ (10218)	$x = ((y \diamond (x \diamond z)) \diamond (y \diamond x)) \diamond y$ (35685)
$x = y \diamond ((x \diamond y) \diamond ((z \diamond y) \diamond y))$ (10222)	$x = ((y \diamond (y \diamond z)) \diamond (y \diamond x)) \diamond y$ (35836)
$x = y \diamond ((x \diamond (y \diamond x)) \diamond (z \diamond y))$ (11081)	$x = ((y \diamond z) \diamond ((x \diamond y) \diamond x)) \diamond y$ (35036)
$x = y \diamond ((x \diamond (y \diamond x)) \diamond (z \diamond z))$ (11082)	$x = ((y \diamond y) \diamond ((x \diamond z) \diamond x)) \diamond z$ (34889)
$x = y \diamond ((x \diamond (z \diamond x)) \diamond (y \diamond y))$ (11116)	$x = ((y \diamond y) \diamond ((x \diamond z) \diamond x)) \diamond y$ (34888)
$x = y \diamond ((y \diamond (x \diamond y)) \diamond (z \diamond y))$ (11205)	$x = ((y \diamond z) \diamond ((y \diamond x) \diamond y)) \diamond y$ (35100)
$x = y \diamond ((y \diamond (z \diamond y)) \diamond (x \diamond y))$ (11280)	$x = ((y \diamond x) \diamond ((y \diamond z) \diamond y)) \diamond y$ (34778)
$x = y \diamond (((y \diamond x) \diamond x) \diamond (z \diamond z))$ (12073)	$x = ((y \diamond y) \diamond (x \diamond (x \diamond z))) \diamond z$ (33998)
$x = y \diamond (((y \diamond x) \diamond z) \diamond (x \diamond z))$ (12087)	$x = ((y \diamond x) \diamond (y \diamond (x \diamond z))) \diamond z$ (33884)
$x = y \diamond (((z \diamond x) \diamond y) \diamond (x \diamond y))$ (12234)	$x = ((y \diamond x) \diamond (y \diamond (x \diamond z))) \diamond y$ (33883)
$x = y \diamond ((x \diamond (y \diamond (z \diamond z))) \diamond y)$ (12857)	$x = (y \diamond (((z \diamond z) \diamond y) \diamond x)) \diamond y$ (33436)
$x = y \diamond ((x \diamond (z \diamond (y \diamond x))) \diamond y)$ (12883)	$x = (y \diamond (((x \diamond y) \diamond z) \diamond x)) \diamond y$ (33020)
$x = y \diamond ((x \diamond ((z \diamond y) \diamond y)) \diamond y)$ (13764)	$x = (y \diamond ((y \diamond (y \diamond z)) \diamond x)) \diamond y$ (32294)
$x = y \diamond ((y \diamond ((x \diamond z) \diamond z)) \diamond z)$ (13849)	$x = (y \diamond ((y \diamond (y \diamond x)) \diamond z)) \diamond z$ (32281)
$x = y \diamond ((z \diamond ((x \diamond y) \diamond y)) \diamond y)$ (13992)	$x = (y \diamond ((y \diamond (y \diamond x)) \diamond z)) \diamond y$ (32280)
$x = (y \diamond x) \diamond (z \diamond ((x \diamond z) \diamond z))$ (18137)	$x = ((y \diamond (y \diamond x)) \diamond y) \diamond (x \diamond z)$ (27863)
$x = (y \diamond y) \diamond (x \diamond ((x \diamond z) \diamond z))$ (18212)	$x = ((y \diamond (y \diamond x)) \diamond x) \diamond (z \diamond z)$ (27859)
$x = (y \diamond y) \diamond ((x \diamond (x \diamond z)) \diamond z)$ (19966)	$x = (y \diamond ((y \diamond x) \diamond x)) \diamond (z \diamond z)$ (26105)
$x = (y \diamond (y \diamond x)) \diamond ((z \diamond z) \diamond z)$ (22619)	$x = (y \diamond (y \diamond y)) \diamond ((x \diamond z) \diamond z)$ (22634)

Table 20.2: Trivial finite models, unknown infinite models

$x = y \diamond (((z \diamond y) \diamond x) \diamond (x \diamond y))$ (12294)	$x = ((y \diamond x) \diamond (x \diamond (y \diamond z))) \diamond y$ (33856)
$x = y \diamond ((z \diamond (x \diamond (x \diamond z))) \diamond y)$ (13102)	$x = (y \diamond (((z \diamond x) \diamond x) \diamond z)) \diamond y$ (33273)
$x = (y \diamond x) \diamond (z \diamond (x \diamond (z \diamond z)))$ (17260)	$x = (((y \diamond y) \diamond x) \diamond y) \diamond (x \diamond z)$ (28740)
$x = (y \diamond x) \diamond (z \diamond (z \diamond (x \diamond z)))$ (17286)	$x = (((y \diamond x) \diamond y) \diamond y) \diamond (x \diamond z)$ (28626)
$x = (y \diamond y) \diamond (((z \diamond x) \diamond x) \diamond z)$ (20911)	$x = (y \diamond (x \diamond (x \diamond y))) \diamond (z \diamond z)$ (25087)
$x = (y \diamond (y \diamond x)) \diamond (x \diamond (x \diamond z))$ (21714)	$x = ((y \diamond x) \diamond x) \diamond ((x \diamond z) \diamond z)$ (24200)
$x = (y \diamond (z \diamond x)) \diamond (x \diamond (x \diamond y))$ (21864)	$x = ((y \diamond x) \diamond x) \diamond ((x \diamond z) \diamond y)$ (24199)
$x = (y \diamond (z \diamond x)) \diamond (x \diamond (x \diamond z))$ (21865)	$x = ((y \diamond x) \diamond x) \diamond ((x \diamond y) \diamond z)$ (24197)
$x = (y \diamond (z \diamond x)) \diamond (x \diamond (x \diamond w))$ (21866)	$x = ((y \diamond x) \diamond x) \diamond ((x \diamond z) \diamond w)$ (24201)
$x = (y \diamond (x \diamond x)) \diamond ((x \diamond z) \diamond z)$ (22446)	$x = (y \diamond (y \diamond x)) \diamond ((x \diamond x) \diamond z)$ (22591)
$x = ((y \diamond x) \diamond x) \diamond (z \diamond (x \diamond z))$ (23337)	$x = ((y \diamond x) \diamond y) \diamond (x \diamond (x \diamond z))$ (23354)
$x = ((y \diamond x) \diamond y) \diamond (x \diamond (y \diamond z))$ (23357)	$x = ((y \diamond z) \diamond x) \diamond (z \diamond (x \diamond z))$ (23653)

Table 20.3: Unknown whether they admit finite models

Chapter 21

Simple rewrites

53,905 implications were automatically generated by simple rewrites.
describe the process of automatically generating these implications here.

Chapter 22

Trivial auto-generated theorems

Approximately 4.5m transitive implications were proven by a transitive reduction of about 15k theorems. Most of these implications were derived from being the first automated run to connect the largest equivalence classes, hence creating a large set of transitively closed implications.

Scripts generated theorems to try simple combinations of equation rewrites to reach the desired goal for every unknown implication. The generated proof scripts were run with lean and the successful theorems were extracted. An example of the types of generated rewrites that were tested:

```
repeat intro
apply
```

```
repeat intro
try { rw [<-h] }
try { rw [<-h, <-h] }
try { rw [<-h, <-h, <-h] }
try { rw [<-h, <-h, <-h, <-h] }
try { rw [<-h, <-h, <-h, <-h, <-h] }
repeat rw [h]
```

```
repeat intro
try {
  nth_rewrite 1 [h]
  try { rw [h] }
  try { rw [<-h] }
}
try {
  nth_rewrite 2 [h]
  try { rw [h] }
  try { rw [<-h] }
}
try {
  nth_rewrite 3 [h]
  try { rw [h] }
  try { rw [<-h] }
}
```

```
try {
  nth_rewrite 4 [h]
  try { rw [h] }
  try { rw [<-h] }
}
try {
  nth_rewrite 1 [h]
  nth_rewrite 1 [h]
  try { rw [h] }
  try { rw [<-h] }
}
...
```

Chapter 23

Enumerating Small Finite Magmas

describe the process of automatically generating these implications here.

Chapter 24

Equation Search

Approximately 650k transitive implications were proven by a custom tool leveraging the implication graph. After previous brute force had derived many implications expressible as a small number of rewrites, this search tool uses substitutions implied by the implication graph to search further.

An example proof illustrates the logic it uses:

```
have eq3315 (x y : G) : x * y = x * (y * (x * x)) := by
  apply Apply.Equation12_implies_Equation11 at h
  apply RewriteHypothesis.Equation11_implies_Equation3323 at h
  apply Apply.Equation3323_implies_Equation3315 at h
  apply h
have eq52 (x y : G) : x = x * (y * (x * x)) := by
  apply Apply.Equation12_implies_Equation61 at h
  apply Apply.Equation61_implies_Equation54 at h
  apply Apply.Equation54_implies_Equation52 at h
  apply h
repeat intro
nth_rewrite 1 [eq3315]
nth_rewrite 1 [← eq52]
apply h
repeat assumption
```

Using the graph of implications and refutations, it identifies equivalence classes/strongly-connected components in the implication graph and possible goals by subtracting out the refutation graph. Iterating through all equivalence classes, it can perform a meet-in-the-middle graph search where it searches outwards from both hypotheses and goals by performing equation substitutions. Depending on the number of hypotheses versus goals, it dynamically adjusts the search depth on both sides based on a configured branching factor.

Due to it's naive implementation, it may only be able to perform certain substitutions in a round-about way and the graph size explodes faster than it must, so it's limited to fairly shallow search depths. Also, the tool may emit proofs without some information Lean may require, so some generated proofs have to be fixed-up afterwards.

Chapter 25

E-Graphs

For proving implications, we used another technique called equality saturation [13] with the `lean-egg` tactic, to automatically construct proofs.

A similar approach is being pursued in the MagmaEgg tool as well, which is a standalone program that only supports magma equalities, while the lean-egg tactic supports any Lean expression.

25.1 lean-egg

25.1.1 Methodology

The basic methodology of equality saturation is based on E-Graphs, a data structure that can store equivalence classes of terms efficiently. We used the `lean-egg` tactic (https://github.com/marcusrossel/lean-egg), based on equality saturation as a tactic, which (re)constructs a proof from the E-graph [9] in Lean. This means that we do not have to trust either the egg tool nor the tactic: if something goes wrong, Lean will not accept the constructed proof. In fact, we found issues with the proof reconstruction from the examples in this project.

The `lean-egg` tactic works for equational reasoning, i.e. proving equalities as consequences of other equalities (potentially universally quantified), which is exactly what we need to prove implications of laws in Magmas. In many cases, we have laws of the form $x = y$, where neither set of variables in the left- and right-hand-side of the law is a subset of each other. In this case the laws cannot be used as rewrite rules: it's not clear what it would be rewritten to, since there are unknowns on both sides of the equation. For these cases we used a simple heuristic, where we instantiate the variables with terms found in the (proof) context, as those are likely to be important for proving the equality.

25.1.2 Results

Out of the possible implications between the 34 equations considered in Chapter 2, this method found an additional 86 implications that were not found before. Some of these seem to be missing in the computation of the transitive closure of implications of the equalities (an investigation is in progress), but some of these are genuinely new theorems, and the `lean-egg` tactic finds good proofs of these (these can be rewritten using `calc` style with a different tactic, `calcify`: https://github.com/nomeata/lean-calcify). An example of this is the following proof, found by `lean-egg`:

Theorem 25.1 (14 implies 23)**.** *Theorem 2.9 is equivalent to Theorem 2.11.*

Proof.

$$x = (x \diamond x) \diamond (x \diamond (x \diamond x)) = (x \diamond x) \diamond x$$

□

It was also able to (re)prove Theorem 5.5, albeit with a manually-provided hint (guide, in the sense of [9]).

25.2 MagmaEgg

This is a simple but apparently at least somewhat effective Rust theorem prover based on egg `e-graph` library written for this project.

It proved 5574 of the 24283 implications in the `only_strongest.txt` file at the time.

The code was originally based on the `magma_search` pull request, but has been pretty much completely rewritten.

Currently search just uses the egg library in a basic fashion, except that in case there are extra variables not present in the LHS, it has code to instantiate them with all subexpressions of the original goal.

Exporting the proofs to Lean has turned out to be harder than finding the proofs, but a good solution has been implemented (modulo some issues in egg that require to sometimes turn off explanation optimization since it sometimes triggers stack overflows and assert failures) that directly produces proof terms using `let` / `have` and `Eq.refl`, `Eq.symm`, `Eq.trans`, `Magma.op`, a congruence lemma for `Magma.op` and variables and the hypothesis. I define one letter aliases for them to reduce verbosity.

Possible future work:

- Figure out which implications are important to prove and try it on them
- Replace the fork-based code with self-execution so that it works on Windows and is less of na hack
- Fork egg and fix the buggy and slow length optimization of explanations
- Maybe write Lean code directly instead of writing explanation sexps and converting to Lean code in a second run
- Fix the generation of extra variable values so it doesn't take too much time in pathological cases (i.e. goals with 4-6 variables)
- Determine whether it actually has some advantages compared to Vampire and `lean-egg`
- Support searching for multiple goal equations at once
- Write a custom elaborator for Lean to speed up elaboration
- If the Lean kernel turns out to be too slow for some large necessary proofs and thus the custom elaborator is not enough, write a custom verified typechecker
- Support having extra rewrite rules, such as other implications that have been found implied by the hypothesis, or simple equalities found by the egraph search itself
- Run it with massive computing resources if deemed useful and someone offers those, once it's a bit more mature

Chapter 26

Using the Vampire theorem prover

1,775 implications were proven using the Vampire theorem prover.

The Vampire proofs were found by iteratively trying to prove some of the remaining unknown implications, then taking the transitive closure including the newly proven theorems. At the end only the transitive reduction of the implications was kept.

The Vampire proofs were converted to Lean proofs using a term elaborator implementing the deduction step of superposition calculus.

Bibliography

[1] A. K. Austin. A note on models of identities. *Proc. Amer. Math. Soc.*, 16:522–523, 1965.

[2] A. K. Austin. Finite models for laws in two variables. *Proc. Amer. Math. Soc.*, 17:1410–1412, 1966.

[3] Franz Baader and Tobias Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.

[4] Joel Berman and Stanley Burris. A computer study of 3-element groupoids. In *Logic and algebra (Pontignano, 1994)*, volume 180 of *Lecture Notes in Pure and Appl. Math.*, pages 379–429. Dekker, New York, 1996.

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

[6] Andrzej Kisielewicz. Varieties of algebras with no nontrivial finite members. In *Lattices, semigroups, and universal algebra (Lisbon, 1988)*, pages 129–136. Plenum, New York, 1990.

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

[8] 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.

[9] Thomas Koehler, Andrés Goens, Siddharth Bhat, Tobias Grosser, Phil Trinder, and Michel Steuwer. Guided equality saturation. *Proc. ACM Program. Lang.*, 8(POPL):1727–1758, 2024.

[10] 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.

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

[12] Henry Maurice Sheffer. A set of five independent postulates for Boolean algebras, with application to logical constants. *Trans. Amer. Math. Soc.*, 14(4):481–488, 1913.

[13] Max Willsey, Chandrakana Nandi, Yisu Remy Wang, Oliver Flatt, Zachary Tatlock, and Pavel Panchekha. egg: Fast and extensible equality saturation. *Proc. ACM Program. Lang.*, 5(POPL):1–29, 2021.