

Varieties of Semiring Solvers via Multicategorical and Algebraic Constructions

MAZOYER Amaury

ENS de Lyon

May 4 – July 31 2026

supervised by Ohad Kammar of the University of Edinburgh, School of Informatics

Motivation

Problem

Prove formally that $\forall a, b \in \mathbb{R}, (a + b)^2 = a^2 + 2ab + b^2$.

Formal proof: 10 axiom invocations.

Motivation

Problem

Prove formally that $\forall a, b \in \mathbb{R}, (a + b)^2 = a^2 + 2ab + b^2$.

Formal proof: 10 axiom invocations.

Automation:

```
Require Import Ring.
```

```
Goal forall a b : R, (a + b)^2 = a^2 + 2*a*b + b^2.
```

```
Proof. intro a b. ring. Qed.
```

Motivation

Problem

Prove formally that $\forall a, b \in \mathbb{R}, (a + b)^2 = a^2 + 2ab + b^2$.

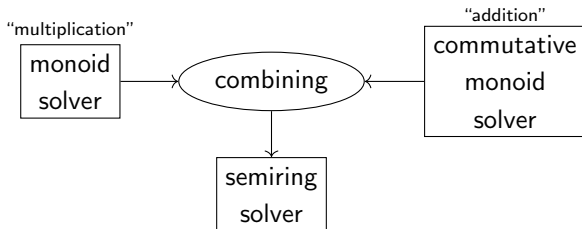
Formal proof: 10 axiom invocations.

Automation:

Require Import Ring.

Goal forall a b : R, (a + b)^2 = a^2 + 2*a*b + b^2.

Proof. intro a b. ring. Qed.



Original FREX framework

Free algebras / free extensions for equational reasoning¹

¹ “Partially-static data as free extension of algebras”, Yallop et al., 2018

State of the art

Original F_RE_X framework

Free algebras / free extensions for equational reasoning¹

Subsequent work

Using F_RE_X to build solvers, with an Idris 2 formalisation²

¹ “Partially-static data as free extension of algebras”, [Yallop et al.](#), 2018

² “Frex: Dependently Typed Algebraic Simplification”, [Allais et al.](#), 2025

State of the art

Original FREX framework

Free algebras / free extensions for equational reasoning¹

Subsequent work

Using FREX to build solvers, with an Idris 2 formalisation²

Existing modular constructions

Modular frex construction for involutive algebras³

¹ “Partially-static data as free extension of algebras”, [Yallop et al.](#), 2018

² “Frex: Dependently Typed Algebraic Simplification”, [Allais et al.](#), 2025

³ “Modular construction of multi-sorted free extensions”, [Allais et al.](#), 2023

State of the art

Original FREX framework

Free algebras / free extensions for equational reasoning¹

Subsequent work

Using FREX to build solvers, with an Idris 2 formalisation²

Existing modular constructions

Modular frex construction for involutive algebras³

Gap before this work

No modular construction for distributive combinations

¹ “Partially-static data as free extension of algebras”, [Yallop et al.](#), 2018

² “Frex: Dependently Typed Algebraic Simplification”, [Allais et al.](#), 2025

³ “Modular construction of multi-sorted free extensions”, [Allais et al.](#), 2023

State of the art

Original F_{REX} framework

Free algebras / free extensions for equational reasoning¹

Subsequent work

Using F_{REX} to build solvers, with an Idris 2 formalisation²

Existing modular constructions

Modular frex construction for involutive algebras³

Gap before this work

No modular construction for distributive combinations

Other solvers

Rocq's reflexion-based semiring/ring solver, state of the art⁴

¹ “Partially-static data as free extension of algebras”, [Yallop et al.](#), 2018

² “Frex: Dependently Typed Algebraic Simplification”, [Allais et al.](#), 2025

³ “Modular construction of multi-sorted free extensions”, [Allais et al.](#), 2023

⁴ “Proving Equalities in a Commutative Ring Done Right in Coq”, [Grégoire and](#)

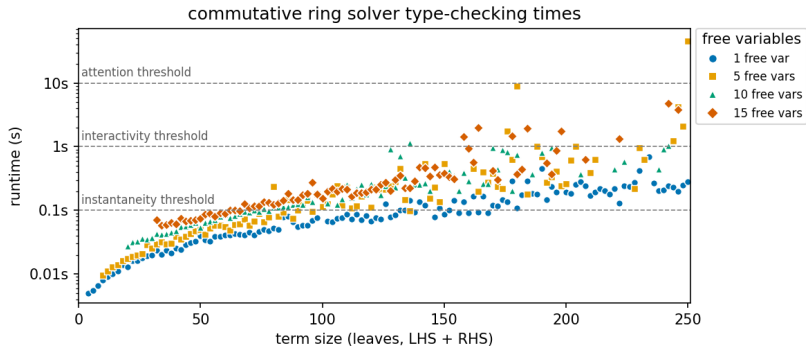
[Mahboubi](#), 2005

Practical payoff

Multiplicative structure			Additive structure		
Theory	Comm.	Inv.	Comm. Semigroup	Comm. Monoid	Abelian Group
Semigroup	Mere	Mere	$\mathcal{P}(\Sigma^+) \setminus \{\emptyset\}$	$\mathcal{P}(\Sigma^+)$	$\mathbb{Z}\langle\Sigma^+\rangle$
		Inv.	$(\mathcal{P}(\Sigma^+) \setminus \{\emptyset\}, -^R)$	$(\mathcal{P}(\Sigma^+), -^R)$	$(\mathbb{Z}\langle\Sigma^+\rangle, \text{rev})$
	Comm.	Mere	$2\mathbb{N}_{>0}$	$2\mathbb{N}$	$2\mathbb{Z}$
		Inv.	$\mathfrak{m}_n^\sigma \setminus \{0\}$	$\mathfrak{m}_n^\sigma$	$(2\mathbb{Z}[\mathbf{i}], -)$
Monoid	Mere	Mere	$\mathcal{P}(\Sigma^*) \setminus \{\emptyset\}, M_n(\mathbb{N}_{>0})$	$\mathcal{P}(\Sigma^*), M_n(\mathbb{N})$	$M_n(\mathbb{Z})$
		Inv.	$(M_n(\mathbb{N}_{>0}), -^T),$ $(\mathcal{P}(\Sigma^*) \setminus \{\emptyset\}, -^R)$	$(M_n(\mathbb{N}), -^T),$ $(\mathcal{P}(\Sigma^*), -^R), \text{Rel}(X)$	$(M_n(\mathbb{Z}), -^T)$
	Comm.	Mere	$\mathbb{N}_{>0}$	$\textcircled{\mathbb{N}}$	$\textcircled{\mathbb{Z}, \mathbb{R}, \mathbb{C}}$
		Inv.	$\mathbb{N}_\sigma \llbracket X_1, \dots, X_n \rrbracket \setminus \{0\}$	$\mathbb{N}_\sigma \llbracket X_1, \dots, X_n \rrbracket$	$(\mathbb{C}, -),$ $\mathbb{Z}_\sigma \llbracket X_1, \dots, X_n \rrbracket$
Group	Mere	Mere	$T_{n, \Delta_{>0}}(\mathbb{R})$	impossible nontrivially	impossible nontrivially
		Inv.	$(T_{n, \Delta_{>0}}(\mathbb{R}), -^\dagger)$	impossible nontrivially	impossible nontrivially
	Comm.	Mere	$\mathbb{R}_{>0}$	impossible nontrivially	impossible nontrivially
		Inv.	$(\mathbb{C}_{>0}, -)$	impossible nontrivially	impossible nontrivially

Models: see slide 43 in appendix

Practical payoff



Equational theories

Equational theories

Presentation $\mathcal{T} = (\Sigma_{\mathcal{T}}, \text{Ax}_{\mathcal{T}})$

- ▶ *signature* $\Sigma_{\mathcal{T}}$: operation symbols with arity.
- ▶ *axioms* $\text{Ax}_{\mathcal{T}}$: axioms between $\Sigma_{\mathcal{T}}$ -terms.

A $\mathcal{T}$ -model interprets the operations and satisfies the axioms.

Equational theories

Presentation $\mathcal{T} = (\Sigma_{\mathcal{T}}, Ax_{\mathcal{T}})$

- ▶ *signature* $\Sigma_{\mathcal{T}}$: operation symbols with arity.
- ▶ *axioms* $Ax_{\mathcal{T}}$: axioms between $\Sigma_{\mathcal{T}}$ -terms.

A $\mathcal{T}$ -model interprets the operations and satisfies the axioms.

Example: monoids

- ▶ operations: $\{(\cdot) : 2, 1 : 0\}$
- ▶ axioms:

$$x, y, z \vdash x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad \text{associativity}$$

$$x \vdash 1 \cdot x = x \quad \text{left neutrality}$$

$$x \vdash x \cdot 1 = x \quad \text{right neutrality}$$

- ▶ $(\mathbb{N}, (+), 0)$, $(\mathbb{N}, (\times), 1)$ are models.

The distributive combination of theories

Additive part

Presentation $\mathcal{A} = \langle \Sigma_{\mathcal{A}}, \text{Ax}_{\mathcal{A}} \rangle$

Multiplicative part

Presentation $\mathcal{M} = \langle \Sigma_{\mathcal{M}}, \text{Ax}_{\mathcal{M}} \rangle$

Distributive combination $\mathcal{M} \triangleright \mathcal{A}$

$$\Sigma_{\mathcal{M} \triangleright \mathcal{A}} = \Sigma_{\mathcal{A}} \sqcup \Sigma_{\mathcal{M}}$$

$$\text{Ax}_{\mathcal{M} \triangleright \mathcal{A}} = \text{Ax}_{\mathcal{A}} \sqcup \text{Ax}_{\mathcal{M}}$$

$\sqcup$ distributivity axioms of every $\mathcal{M}$ -operation over every $\mathcal{A}$ -operation

The distributive combination of theories

Additive part

Presentation $\mathcal{A} = \langle \Sigma_{\mathcal{A}}, \text{Ax}_{\mathcal{A}} \rangle$

Multiplicative part

Presentation $\mathcal{M} = \langle \Sigma_{\mathcal{M}}, \text{Ax}_{\mathcal{M}} \rangle$

Distributive combination $\mathcal{M} \triangleright \mathcal{A}$

$$\Sigma_{\mathcal{M} \triangleright \mathcal{A}} = \Sigma_{\mathcal{A}} \sqcup \Sigma_{\mathcal{M}}$$

$$\text{Ax}_{\mathcal{M} \triangleright \mathcal{A}} = \text{Ax}_{\mathcal{A}} \sqcup \text{Ax}_{\mathcal{M}}$$

$\sqcup$ distributivity axioms of every $\mathcal{M}$ -operation over every $\mathcal{A}$ -operation

Example

Semiring = monoid $\triangleright$ commutative monoid

Distributivity axioms:

$$\begin{aligned} x, y, z \vdash x \cdot (y + z) &= (x \cdot y) + (x \cdot z) & x, y, z \vdash (x + y) \cdot z &= (x \cdot z) + (y \cdot z) \\ x \vdash x \cdot 0 &= 0 & x \vdash 0 \cdot x &= 0 \end{aligned}$$

Free algebras

Presentation $\mathcal{T}$, set of variables X .

Free $\mathcal{T}$ -model over X $\langle F_{\mathcal{T}}X, \eta^{\mathcal{T}} \rangle$: “most general” $\mathcal{T}$ -model generated by X .

Intuition:

- ▶ elements of $F_{\mathcal{T}}X = \mathcal{T}$ -expressions modulo the axioms of $\mathcal{T}$
- ▶ the *unit* $\eta^{\mathcal{T}} : X \rightarrow \underbrace{F_{\mathcal{T}}X}_{\text{carrier set}}$ embeds the variables in X in $F_{\mathcal{T}}X$

Free algebras

Presentation $\mathcal{T}$, set of variables X .

Free $\mathcal{T}$ -model over X $\langle F_{\mathcal{T}}X, \eta^{\mathcal{T}} \rangle$: “most general” $\mathcal{T}$ -model generated by X .

Intuition:

- ▶ elements of $F_{\mathcal{T}}X = \mathcal{T}$ -expressions modulo the axioms of $\mathcal{T}$
- ▶ the *unit* $\eta^{\mathcal{T}} : X \rightarrow \underbrace{F_{\mathcal{T}}X}_{\text{carrier set}}$ embeds the variables in X in $F_{\mathcal{T}}X$

Universal property:

for every $\mathcal{T}$ -model A and function $e : X \rightarrow \underline{A}$, there exists a unique $\mathcal{T}$ -homomorphism $h : F_{\mathcal{T}}X \rightarrow A$ such that:

$$\begin{array}{ccc} X & \xrightarrow{\eta^{\mathcal{T}}} & \underline{F_{\mathcal{T}}X} \\ & \searrow e & \downarrow h \\ & & \underline{A} \end{array}$$

Free algebras

Example: free monoid over X

► $\underline{F_{\text{Mon}}X} := \text{List } X \quad u \cdot v := u \mathbin{++} v \quad 1 := [] \quad \eta^{\text{Mon}} x := [x]$

► **Monoid**-model A , function $e : X \rightarrow \underline{A}$

$\Rightarrow$ unique monoid homomorphism h :

$$\underline{h} [x_1, \dots, x_n] := 1 \cdot (e x_1) \cdot \dots \cdot (e x_n)$$

$$\underline{h}(\eta^{\text{Mon}} x) = \underline{h} [x] = 1 \cdot (e x) = e x$$

Free algebras

Example: free monoid over X

► $F_{\mathbf{Mon}}X := \text{List } X \quad u \cdot v := u \mathbin{\dot{+}} v \quad 1 := [] \quad \eta^{\mathbf{Mon}} x := [x]$

► **Monoid**-model A , function $e : X \rightarrow \underline{A}$

⇒ unique monoid homomorphism h :

$$\underline{h} [x_1, \dots, x_n] := 1 \cdot (e x_1) \cdot \dots \cdot (e x_n)$$

$$\underline{h}(\eta^{\mathbf{Mon}} x) = \underline{h} [x] = 1 \cdot (e x) = e x$$

Example: free commutative monoid over X

► $F_{\mathbf{CMon}}X := \text{Bag } X \quad u + v := u \mathbin{\dot{+}} v \quad 0 := \{\}$ $\eta^{\mathbf{CMon}} x := \{x : 1\}$

► **CMonoid**-model A , function $e : X \rightarrow \underline{A}$

⇒ unique commutative monoid homomorphism h :

$$\underline{h} \text{ bag} := 0 + \sum_{(x:n) \in \text{bag}} n \cdot (e x) \quad \text{notation: } n \cdot x := \underbrace{x + \dots + x}_{n \text{ times}}$$

$$\underline{h}(\eta^{\mathbf{CMon}} x) = \underline{h} \{x : 1\} = 0 + (e x) = e x$$

Free algebras and normalisation

Theorem (Extensional normalisation, informally)

Let $\langle F_{\mathcal{T}}X, \eta^{\mathcal{T}} \rangle$ be a free $\mathcal{T}$ -model over the set X , and s, t be expressions with variables from X .

The equation $s = t$ is valid in every $\mathcal{T}$ -model iff their interpretations in $F_{\mathcal{T}}X$ are equal.

Free algebras and normalisation

Theorem (Extensional normalisation, informally)

Let $\langle F_{\mathcal{T}}X, \eta^{\mathcal{T}} \rangle$ be a free $\mathcal{T}$ -model over the set X , and s, t be expressions with variables from X .

The equation $s = t$ is valid in every $\mathcal{T}$ -model iff their interpretations in $F_{\mathcal{T}}X$ are equal.

Example: monoids

The equation

$$x, y \vdash x \cdot (y \cdot 1) = 1 \cdot (x \cdot y)$$

holds in every monoid since

$$[x] \mathbin{+} ([y] \mathbin{+} []) = [x, y] = [] \mathbin{+} ([x] \mathbin{+} [y])$$

Free algebra for the distributive combination

Free additive algebra

- ▶ $\mathcal{A}$ commutative:
every operation commutes with
every other operation
- ▶ $F_{\mathcal{A}} = \langle F_{\mathcal{A}}X, \eta^{\mathcal{A}} \rangle$

Free multiplicative algebra

- ▶ $\mathcal{M}$ arbitrary
- ▶ $F_{\mathcal{M}} = \langle F_{\mathcal{M}}X, \eta^{\mathcal{M}} \rangle$

Free distributive combination algebra (hypothesis)

- ▶ $\underline{F_{\mathcal{M} \triangleright \mathcal{A}} X} := \underline{F_{\mathcal{A}} \underline{F_{\mathcal{M}} X}}$
- ▶ additive operations from $F_{\mathcal{A}} \underline{F_{\mathcal{M}} X}$
- ▶ “lifted” multiplicative operations of $F_{\mathcal{M}} X$
- ▶ $\eta^{\mathcal{M} \triangleright \mathcal{A}} := \eta^{\mathcal{A}} \circ \eta^{\mathcal{M}}$

Free algebra for the distributive combination

Example: semirings

► $F_{\mathbf{Mon} \triangleright \mathbf{CMon}} X := \text{Bag List } X$

► $u + v := u \uplus v$

► lifted multiplication:

$$2xy \cdot (3xz + t) = 6xyxz + 2xyt$$

$$\wr [x, y] : 2 \wr [x, z] : 3, [t] : 1 \wr = \wr [x, y, x, z] : 6, [x, y, t] : 2 \wr$$

$$u \cdot v := \biguplus_{(l_1 : n_1) \in u} \biguplus_{(l_2 : n_2) \in v} \wr l_1 \uplus l_2 : n_1 \times n_2 \wr$$

► $\eta^{\mathbf{Mon} \triangleright \mathbf{CMon}}_X := \wr [x] : 1 \wr$

► $x \in \text{Bag List } X, \underline{h} \, x := 0 + \sum_{([x_1, \dots, x_n] : n) \in x} n \cdot (1 \cdot (e_{x_1}) \cdot \dots \cdot (e_{x_n}))$

Failure: no-go results

[Zwart & Marsden, 2018]: the previous construction doesn't work if any of these 3 hypotheses hold:

1. $\mathcal{M}$ has an idempotent operator
(i.e. there exists $(* : 2) \in \Sigma_{\mathcal{M}}$ such that $x \vdash x * x = x$ holds)
2. $\mathcal{A}$ has two or more distinct constants
3. $a, b, c, d \vdash (a * b) * (c * d) = (a * c) * (b * d)$ does not hold for every $(* : 2) \in \Sigma_{\mathcal{A}}$

Failure: no-go results

[Zwart & Marsden, 2018]: the previous construction doesn't work if any of these 3 hypotheses hold:

1. $\mathcal{M}$ has an idempotent operator
(i.e. there exists $(* : 2) \in \Sigma_{\mathcal{M}}$ such that $x \vdash x * x = x$ holds)
2. $\mathcal{A}$ has two or more distinct constants
3. $a, b, c, d \vdash (a * b) * (c * d) = (a * c) * (b * d)$ does not hold for every $(* : 2) \in \Sigma_{\mathcal{A}}$

Free additive algebra

- ▶ $\mathcal{A}$ **commutative**:
every operation commutes with
every other operation

Free multiplicative algebra

- ▶ $\mathcal{M}$ arbitrary

2. and 3. are false under the commutativity hypothesis

Failure: no-go results

[Zwart & Marsden, 2018]: the previous construction doesn't work if any of these 3 hypotheses hold:

1. $\mathcal{M}$ has an idempotent operator
(i.e. there exists $(* : 2) \in \Sigma_{\mathcal{M}}$ such that $x \vdash x * x = x$ holds)
2. $\mathcal{A}$ has two or more distinct constants
3. $a, b, c, d \vdash (a * b) * (c * d) = (a * c) * (b * d)$ does not hold for every $(* : 2) \in \Sigma_{\mathcal{A}}$

Free additive algebra

- ▶ $\mathcal{A}$ **commutative**:
every operation commutes with
every other operation

Free multiplicative algebra

- ▶ $\mathcal{M}$ arbitrary

2. and 3. are false under the commutativity hypothesis

Problem: What about 1.?

Failure: no-go results

[Zwart & Marsden, 2018]: the previous construction doesn't work if any of these 3 hypotheses hold:

1. $\mathcal{M}$ has an idempotent operator
(i.e. there exists $(* : 2) \in \Sigma_{\mathcal{M}}$ such that $x \vdash x * x = x$ holds)
2. $\mathcal{A}$ has two or more distinct constants
3. $a, b, c, d \vdash (a * b) * (c * d) = (a * c) * (b * d)$ does not hold for every $(* : 2) \in \Sigma_{\mathcal{A}}$

Free additive algebra

- ▶ $\mathcal{A}$ **commutative**:
every operation commutes with
every other operation

Free multiplicative algebra

- ▶ $\mathcal{M}$ **arbitrary affine**

2. and 3. are false under the commutativity hypothesis

Problem: What about 1.? $\Rightarrow$ *affinity* hypothesis for $\mathcal{M}$

Corrected theorem

Affine presentation

- ▶ $\mathcal{T}$ presentation
- ▶ such that in every axiom, each variable appears at most once **on each side**

Examples:

- ▶ $x, y \vdash x + y = y + x$ is affine
- ▶ $x \vdash x \cdot 0 = 0$ is affine
- ▶ $x \vdash x \vee x = x$ is *not* affine

Semigroups, monoids, groups: all affine theories

Corrected theorem

Affine presentation

- ▶ $\mathcal{T}$ presentation
- ▶ such that in every axiom, each variable appears at most once **on each side**

Examples:

- ▶ $x, y \vdash x + y = y + x$ is affine
- ▶ $x \vdash x \cdot 0 = 0$ is affine
- ▶ $x \vdash x \vee x = x$ is *not* affine

Semigroups, monoids, groups: all affine theories

Theorem (Informally stated)

If the additive theory is commutative and the multiplicative theory is affine, then the free algebra of the distributive combination is given by composition of the component free algebras.

Possible extensions

- ▶ free extensions

like free algebras but also embed constants from an existing model

Possible extensions

- ▶ **free extensions**
like free algebras but also embed constants from an existing model
- ▶ **full mechanisation**
complete the Idris 2 proof of the main theorem

Possible extensions

- ▶ **free extensions**
like free algebras but also embed constants from an existing model
- ▶ **full mechanisation**
complete the Idris 2 proof of the main theorem
- ▶ **optimality of the hypothesis**
something weaker than affinity?

Possible extensions

- ▶ **free extensions**
like free algebras but also embed constants from an existing model
- ▶ **full mechanisation**
complete the Idris 2 proof of the main theorem
- ▶ **optimality of the hypothesis**
something weaker than affinity?
- ▶ **multi-sorted theories**
examples: non-square matrices, linear transformations, modules

Conclusion

- ▶ free algebras:
normal forms modulo axioms
- ▶ solving:
extensional normalisation
- ▶ distributive combination of theories:
disjoint union + distributivity axioms
- ▶ free algebra for the distributive combination of theories:
composition of the component free algebras
 - ▶ commutative additive theory
 - ▶ affine multiplicative theory
- ▶ modularity:
already 28 non-trivial solvers

Section 1

Appendices

Appendix outline

- Category theory
- Universal algebra
- Proof
- Misc

Subsection 1

Category theory

Monads

A *monad* on a category $\mathcal{C}$ is a triple (T, η, μ) where:

- ▶ $T : \mathcal{C} \rightarrow \mathcal{C}$
- ▶ $\eta : 1_{\mathcal{C}} \Rightarrow T$
- ▶ $\mu : T^2 \Rightarrow T$

and such that the following diagrams commute:

$$\begin{array}{ccc} T & \xrightarrow{T\eta} & T^2 \\ \eta T \downarrow & \searrow & \downarrow \mu \\ T^2 & \xrightarrow{\mu} & T \end{array} \qquad \begin{array}{ccc} T^3 & \xrightarrow{T\mu} & T^2 \\ \mu T \downarrow & & \downarrow \mu \\ T^2 & \xrightarrow{\mu} & T \end{array}$$

Distributive laws

A *distributive law* of (T, η^T, μ^T) over (S, η^S, μ^S) is a natural transformation $\lambda : TS \Rightarrow ST$ such that the following diagrams commute:

$$\begin{array}{ccc} & T & \\ T\eta^S \swarrow & & \searrow \eta^S T \\ TS & \xrightarrow{\lambda} & ST \end{array}$$

$$\begin{array}{ccc} & S & \\ \eta^T S \swarrow & & \searrow S\eta^T \\ TS & \xrightarrow{\lambda} & ST \end{array}$$

$$\begin{array}{ccccc} T^2S & \xrightarrow{T\lambda} & TST & \xrightarrow{\lambda T} & ST^2 \\ \mu^T S \downarrow & & & & \downarrow S\mu^T \\ TS & \xrightarrow{\lambda} & & & ST \end{array}$$

$$\begin{array}{ccccc} TS^2 & \xrightarrow{\lambda S} & STS & \xrightarrow{S\lambda} & S^2T \\ T\mu^S \downarrow & & & & \downarrow \mu^S T \\ TS & \xrightarrow{\lambda} & & & ST \end{array}$$

Subsection 2

Universal algebra

Finitary signature $\Sigma = (\text{op } \Sigma, \text{arity}_\Sigma)$

describes the operators of a theory

- ▶ *operator set*: $\text{op } \Sigma \in \mathbf{Set}$
- ▶ *arity assignment*: $\text{arity}_\Sigma : \text{op } \Sigma \rightarrow \mathbb{N}$

Example: monoid signature $\Sigma_{\mathbf{Mon}}$

- ▶ $\text{op } \Sigma_{\mathbf{Mon}} := \{(\cdot), 1\}$
- ▶ $\text{arity}_{\Sigma_{\mathbf{Mon}}}(\cdot) := 2$, i.e., $(\cdot)$ is a binary operator
- ▶ $\text{arity}_{\Sigma_{\mathbf{Mon}}}1 := 0$, i.e., 1 is a constant

Written succinctly: $\Sigma_{\mathbf{Mon}} := \{(\cdot) : 2, 1 : 0\}$

Interpretation

Algebra $A = (\underline{A}, A[[-]])$ over a signature Σ

- ▶ *carrier set*: $\underline{A} \in \mathbf{Set}$
- ▶ *operations or interpretations*: $A[[f]] : \underline{A}^n \rightarrow \underline{A}$ for all $(f : n) \in \Sigma$

Example: monoids

- ▶ $(\mathbb{N}, (+), 0)$
- ▶ $(\mathbb{N}, (\cdot), 1)$
- ▶ $(\mathbb{N}, \max, 0)$
- ▶ $(\mathbb{C}, (+), 0)$
- ▶ $(\mathbb{C}, (\cdot), 1)$

Structure-preserving maps

Homomorphism $h : A \rightarrow B$

between Σ -algebras A, B :

- ▶ function $\underline{h} : \underline{A} \rightarrow \underline{B}$
- ▶ such that:

$$B \llbracket f \rrbracket (h(a_1), \dots, h(a_n)) = h(A \llbracket f \rrbracket (a_1, \dots, a_n))$$

for all $(f : n) \in \Sigma$ and $a_1, \dots, a_n \in \underline{A}$

Example: complex conjugation

- ▶ $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \quad \overline{0} = 0$
- ▶ $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}, \quad \overline{1} = 1$

Abstract syntax

$\text{Term}_\Sigma X$: terms over signature Σ and variable set X

$$\frac{x \in X}{x \in \text{Term}_\Sigma X} \qquad \frac{t_i \in \text{Term}_\Sigma X \quad (\text{op} : n) \in \Sigma}{\text{op}(t_1, \dots, t_n) \in \text{Term}_\Sigma X}$$

Term folding $A \llbracket t \rrbracket e$

- ▶ Σ -algebra A
 - ▶ environment $e : X \rightarrow \underline{A}$
- } Σ -algebra over X

Inductively:

$$A \llbracket x \rrbracket e := e\ x \qquad A \llbracket \text{op}(t_1, \dots, t_n) \rrbracket e := A \llbracket \text{op} \rrbracket (A \llbracket t_1 \rrbracket e, \dots, A \llbracket t_n \rrbracket e)$$

Example: monoid

- ▶ term $t := x \cdot (y \cdot 1)$
- ▶ interpretation with $e := \{x \mapsto 2, y \mapsto 3\}$ in $A := (\mathbb{N}, (+), 0)$

$$A \llbracket x \cdot (y \cdot 1) \rrbracket = 2 + (3 + 0) = 5$$

Equation $X \vdash_{\Sigma} \ell = r$ over signature Σ

- ▶ set X
- ▶ terms $\ell, r \in \text{Term}_{\Sigma} X$

Satisfaction $\langle A, e \rangle \models (X \vdash \ell = r)$

by Σ -algebra over X $\langle A, e \rangle$:

$$A[[\ell]] e = A[[r]] e$$

Validity $A \models (X \vdash \ell = r)$

in algebra A :

$$\forall e : X \rightarrow \underline{A}, \quad \langle A, e \rangle \models (X \vdash \ell = r)$$

Validity

Satisfaction $\langle A, e \rangle \models (X \vdash \ell = r)$

by Σ -algebra over X $\langle A, e \rangle$:

$$A[[\ell]]e = A[[r]]e$$

Validity $A \models (X \vdash \ell = r)$

in algebra A :

$$\forall e : X \rightarrow \underline{A}, \quad \langle A, e \rangle \models (X \vdash \ell = r)$$

Example:

- ▶ $\langle A := (\mathbb{N}, (+), 0), e := \{x \mapsto 2, y \mapsto 3\} \rangle$ satisfies

$$x, y \vdash x \cdot (y \cdot 1) = 1 \cdot (x \cdot y)$$

since

$$2 + (3 + 0) = 5 = 0 + (2 + 3)$$

Varieties of algebras

Presentation $\mathcal{T} = (\Sigma_{\mathcal{T}}, \text{Ax}_{\mathcal{T}})$

- ▶ signature $\Sigma_{\mathcal{T}}$
- ▶ set $\text{Ax}_{\mathcal{T}}$ of $\Sigma_{\mathcal{T}}$ -equations, the *axioms*

$\mathcal{T}$ -model: $\Sigma_{\mathcal{T}}$ -algebra validating every axiom in $\mathcal{T}$: $A \models (X \vdash \ell = r) \in \text{Ax}_{\mathcal{T}}$

Example: monoids

Monoid presentation $:= (\Sigma_{\text{Mon}}, \text{Ax}_{\text{Monoid}})$ with the axioms

$$x, y, z \vdash x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad \text{associativity}$$

$$x \vdash 1 \cdot x = x \quad \text{left neutrality}$$

$$x \vdash x \cdot 1 = x \quad \text{right neutrality}$$

monoids are **Monoid**-models

Free $\mathcal{T}$ -model over X $\langle F_{\mathcal{T}}X, \eta^{\mathcal{T}} \rangle$

- ▶ $\mathcal{T}$ -model $F_{\mathcal{T}}X$
- ▶ environment $\eta^{\mathcal{T}}$ called the *unit*
- ▶ *universal property*:
every $\mathcal{T}$ -model over X $\langle A, e \rangle$ uniquely defines
 - ▶ a homomorphism $h : F_{\mathcal{T}}X \rightarrow A$
 - ▶ that extends e along $\eta^{\mathcal{T}}$: $e = h \circ \eta^{\mathcal{T}}$

Example: free monoid over X

- ▶ $\underline{F_{\text{Mon}}}X := \text{List } X \quad u \cdot v := u \mathbin{++} v \quad 1 := [] \quad \eta^{\text{Mon}} x := [x]$
- ▶ for every **Monoid**-model over X $\langle A, e \rangle$, a unique monoid homomorphism h :

$$\underline{h} [x_1, \dots, x_n] := 1 \cdot (e x_1) \cdot \dots \cdot (e x_n)$$

$$\underline{h}(\eta^{\text{Mon}} x) = \underline{h} [x] = 1 \cdot (e x) = e x \text{ since } F_{\text{Mon}}X \text{ is a } \mathbf{Monoid}\text{-model}$$

Free algebras

Free $\mathcal{T}$ -model over X $\langle F_{\mathcal{T}}X, \eta^{\mathcal{T}} \rangle$

- ▶ $\mathcal{T}$ -model $F_{\mathcal{T}}X$
- ▶ environment $\eta^{\mathcal{T}}$ called the *unit*
- ▶ *universal property*:
every $\mathcal{T}$ -model over X $\langle A, e \rangle$ uniquely defines
 - ▶ a homomorphism $h : F_{\mathcal{T}}X \rightarrow A$
 - ▶ that extends e along $\eta^{\mathcal{T}}$: $e = h \circ \eta^{\mathcal{T}}$

Example: free commutative monoid over X

- ▶ $\underline{F_{\mathbf{CMon}}}X := \text{Bag } X \quad u \cdot v := u \uplus v \quad 1 := \{\}$ $\eta^{\mathbf{CMon}} x := \{x : 1\}$
- ▶ for every **CMonoid**-model over X $\langle A, e \rangle$, a unique commutative monoid homomorphism h :

$$\underline{h} \text{ bag} := 1 \cdot \sum_{(x:n) \in \text{bag}} n \cdot (e x)$$

$$\underline{h}(\eta^{\mathbf{CMon}} x) = \underline{h} \{x : 1\} = 1 \cdot (e x) = e x$$

Free algebras and normalisation

Theorem (extensional normalisation)

Let $\langle F_{\mathcal{T}}X, \text{env} \rangle$ be a free $\mathcal{T}$ -model, and let $X \vdash \ell = r$ be an equation in context. The following are equivalent:

- 1. The unit satisfies the equation: $\langle F_{\mathcal{T}}X, \text{env} \rangle \models (X \vdash \ell = r)$*
- 2. The free algebra validates the equation: $F_{\mathcal{T}}X \models (X \vdash \ell = r)$*
- 3. Every $\mathcal{T}$ -model A validates the equation: $A \models (X \vdash \ell = r)$*

Proof

3. $\Rightarrow$ 2. and 2. $\Rightarrow$ 1. hold by definition.

1. $\Rightarrow$ 3. is deduced from the universal property of the free algebra. □

Free algebras and normalisation

Theorem (extensional normalisation)

Let $\langle F_{\mathcal{T}}X, \text{env} \rangle$ be a free $\mathcal{T}$ -model, and let $X \vdash \ell = r$ be an equation in context. The following are equivalent:

1. The unit satisfies the equation: $\langle F_{\mathcal{T}}X, \text{env} \rangle \models (X \vdash \ell = r)$
2. The free algebra validates the equation: $F_{\mathcal{T}}X \models (X \vdash \ell = r)$
3. Every $\mathcal{T}$ -model A validates the equation: $A \models (X \vdash \ell = r)$

Example: monoids

The equation

$$x, y \vdash x \cdot (y \cdot 1) = 1 \cdot (x \cdot y)$$

holds in every monoid since

$$[x] \mathbin{+} ([y] \mathbin{+} []) = [x, y] = [] \mathbin{+} ([x] \mathbin{+} [y])$$

Commutative theories

Commutative theory

- ▶ $\mathcal{T}$ presentation
- ▶ such that every operator commutes with every other operator:

$$f \left(\begin{array}{c} g(x_{11}, \dots, x_{1m}) \\ \vdots \\ g(x_{n1}, \dots, x_{nm}) \end{array} \right) = g \left(f \left(\begin{array}{c} x_{11} \\ \vdots \\ x_{n1} \end{array} \right), \dots, f \left(\begin{array}{c} x_{1m} \\ \vdots \\ x_{nm} \end{array} \right) \right)$$

holds in every $\mathcal{T}$ -model for every $(f : n) \in \Sigma_{\mathcal{T}}$, $(g : m) \in \Sigma_{\mathcal{T}}$

Example: monoids

The equations are:

$$(x \cdot y) \cdot (z \cdot w) = (x \cdot z) \cdot (y \cdot w) \quad 1 \cdot 1 = 1 \quad 1 = 1$$

The theory of commutative monoids is commutative.

Affine theories

Affine theory

- ▶ $\mathcal{T}$ presentation
- ▶ such that in every axioms, each variable appears at most once

Examples:

- ▶ $x, y \vdash x + y = y + x$ is affine
- ▶ $x \vdash x \cdot 0 = 0$ is affine
- ▶ $x \vdash x \vee x = x$ is *not* affine

Semigroups, monoids, groups: all affine theories

Extensions and morphisms of extensions

Extension of A by X $\langle B, h, e \rangle$

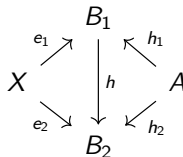
where A is a $\mathcal{T}$ -model and X a set.

- ▶ $\mathcal{T}$ -model B
- ▶ homomorphism of $\mathcal{T}$ -models $h : A \rightarrow B$
- ▶ function $e : X \rightarrow \underline{B}$

Morphism of extensions $h : b_1 \rightarrow b_2$

between extensions of A by X $b_1 = \langle B_1, h_1, e_1 \rangle$ and $b_2 = \langle B_2, h_2, e_2 \rangle$.

- ▶ homomorphism of $\mathcal{T}$ -models $h : B_1 \rightarrow B_2$
- ▶ such that the following diagram commutes:



Free extensions

Free extension of A by X $\langle A[X], \text{sta}, \text{dyn} \rangle$

- ▶ extension of A by X $\langle A[X], \text{sta}, \text{dyn} \rangle$

- ▶ *universal property*:

every extension of A by X $\langle B, h, e \rangle$ uniquely defines a morphism of extensions $[B, h, e] : \langle A[X], \text{sta}, \text{dyn} \rangle \rightarrow \langle B, h, e \rangle$

Example: commutative monoids

A commutative monoid, $X = \{x_1, x_2, x_3\}$

$$A[X] := \underline{A} \times \mathbb{N}^3$$

$$\langle a, \langle k_{11}, k_{12}, k_{13} \rangle \rangle + \langle b, \langle k_{21}, k_{22}, k_{23} \rangle \rangle := \langle a + b, \langle k_{11} + k_{21}, k_{12} + k_{22}, k_{13} + k_{23} \rangle \rangle$$

$$0 := \langle 0, \langle 0, 0, 0 \rangle \rangle \quad \text{sta } a := \langle a, \langle 0, 0, 0 \rangle \rangle$$

$$\text{dyn } x_1 := \langle 0, \langle 1, 0, 0 \rangle \rangle \quad \text{dyn } x_i := \dots$$

$$[B, h, e] \langle a, \langle k_1, k_2, k_3 \rangle \rangle := h a + k_1 \cdot e x_1 + k_2 \cdot e x_2 + k_3 \cdot e x_3$$

Subsection 3

Proof

Proof idea

Goal: construct $F_{\mathcal{M} \triangleright \mathcal{A}} X$ from $F_{\mathcal{M}} X$ and $F_{\mathcal{A}} X$

1. Start with $F_{\mathcal{M}} X$
2. Apply the free additive algebra: $F_{\mathcal{A}}(F_{\mathcal{M}} X)$
3. The additive operations are already there.
4. Use the commutativity of $\mathcal{A}$ to lift the multiplicative operations.
5. Use the affinity of $\mathcal{M}$ to prove that the lifted operations still satisfy the axioms of $\mathcal{M}$.
6. The universal properties of the two free constructions combine to show that the resulting model is free.

Underlying concepts:

operads/translations, multicategories, an adjunction used for lifting, a pullback description of models of the distributive combination

Lifting of the multiplicative operations

Theorem

Let $\mathcal{T}$ be a theory. The forgetful multi-functor $\underline{} : \mathbf{Multi}(\mathcal{T}, \mathbf{Set}) \rightarrow \langle \mathbf{Set}, \Pi \rangle$ has a left adjoint iff $\mathcal{T}$ is commutative.

Pullback square

$\mathcal{A}$ and $\mathcal{M}$ theory, $\mathcal{O}$ operad, $T : \mathcal{O} \rightarrow \mathcal{M}$ translation

$$\begin{array}{ccc}
 \mathbf{Mod}(T \triangleleft \mathcal{A}, \mathbf{Set}) & \xrightarrow{\cong_{\mathcal{O} \triangleleft \mathcal{A}}} & \mathbf{Mod}(\mathcal{O}, \mathbf{Multi}(\mathcal{A}, \mathbf{Set})) \\
 \cong_{\mathcal{M}} \downarrow & & \downarrow \mathbf{Mod}(\mathcal{O}, \cong) \\
 \mathbf{Mod}(\mathcal{M}, \mathbf{Set}) & \xrightarrow{\mathbf{Mod}(T, \mathbf{Set})} & \mathbf{Mod}(\mathcal{O}, \langle \mathbf{Set}, \Pi \rangle)
 \end{array}$$

Subsection 4

Misc

Models in the table I

- ▶ $\mathbb{N}, \mathbb{Z}, \mathbb{R}$: natural numbers, integers and real numbers with the usual operations.
- ▶ $(\mathbb{C}, -)$: complex numbers with conjugation.
- ▶ $\mathbb{C}_{>0} := \{a + b\mathbf{i} \mid a \in \mathbb{R}_{>0}, b \in \mathbb{R}\}$ are complex numbers with a strictly positive real part.
- ▶ $2\mathbb{Z}[\mathbf{i}] := \{2(a + b\mathbf{i}) \mid a, b \in \mathbb{Z}\}$ with standard addition, multiplication and conjugation as involution.
- ▶ $\mathcal{P}(\Sigma^*)$ and variants: formal languages on the alphabet Σ , with union as addition and concatenation as multiplication.
- ▶ $M_n(X)$: $n \times n$ square matrices with coefficients in X . $-^T$ denotes matrix transposition.

Models in the table II

- ▶ $\mathbb{Z}\langle\Sigma^+\rangle$: finite integer linear combinations of nonempty words, i.e, finitely supported functions from Σ^+ to $\mathbb{Z}$. Addition is pointwise function addition and multiplication is concatenation that distributes over sums. rev is word reversal.
- ▶ $\text{Rel}(X)$: the set of binary relations on X . Addition is union, and multiplication is composition. Involution is the converse $R^\dagger := \{(y, x) \mid (x, y) \in R\}$.
- ▶ $Y_\sigma \llbracket X_1, \dots, X_n \rrbracket$: multivariate generating functions in the variables $X_1, \dots, X_n$ with coefficients in Y . Addition and multiplication are the standard operations, the involution is defined by $f(x_1, \dots, x_n)^{* \sigma} := f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ where $\sigma \in \mathfrak{S}_n$ is a permutation of order 2, i.e, $\sigma^2 = \text{id}$ and $\sigma \neq \text{id}$.

Models in the table III

- ▶ $\mathfrak{m}_n^\sigma := \{f \in \mathbb{N}_\sigma \llbracket X_1, \dots, X_n \rrbracket \mid f(0, \dots, 0) = 0\}$: multivariate generating functions in the variables $X_1, \dots, X_n$ with coefficients in $\mathbb{N}$ and with no constant part.
- ▶ $(T_{n, \Delta_{>0}}(\mathbb{R}), -^\dagger)$: upper triangular matrices with coefficients > 0 on the diagonal. Addition and multiplication is standard matrix addition and multiplication. The involution $-^\dagger$ reverses the order of the coefficients on the diagonal, e.g. $\Delta(1, \dots, n)^\dagger = \Delta(n, \dots, 1)$.