On Higher-Order Algebra

Marcelo Fiore

Computer Laboratory
University of Cambridge

SCTS III
2.XII.2010

Programme

$^{(1)}$ mathematical models $\overset{(2)}{\rightsquigarrow}$ algebraic meta-theories

for: <u>higher-order</u>,

type dependency,

polymorphism,

linearity,

. . .

Meta-Theory of Algebraic Structure

[Linton 1966] **[Lawvere 1963]**

$$\begin{tikzcd}
 & \text{Cat. Alg.} \arrow[dl, leftrightarrow] \arrow[dr, leftrightarrow] & \\
\text{Univ. Alg.} \arrow[rr, leftrightarrow] & & \text{Eq. Log.}
\end{tikzcd}$$

[Birkhoff 1935]

- Soundness & completeness (Birkhoff)
  - term rewriting
- Algebraic theories (Lawvere)
  - translations & constructions
- Finitary monads (Linton)
  - initial-algebra semantics (compositionality & induction)

This Talk (1)

Algebraic framework and methodology
for the synthesis of deduction systems
for equational reasoning
and computation by rewriting.

This Talk (2)

Extension of the algebraic first-order mathematical theory to second-order; that is, to *languages with variable binding*.

$$
\begin{tikzcd}
 & \text{Cat. Alg.} \arrow[dl, leftrightarrow] \arrow[dr, leftrightarrow] \arrow[d, phantom, "2^{\mathrm{nd}}\text{-order}"] & \\
\text{Univ. Alg.} \arrow[rr, leftrightarrow] & {} & \text{Eq. Log.}
\end{tikzcd}
$$

I

Universal Algebra and Equational Logic

Universal Algebra

Syntax	Semantics

signatures:

$$\Sigma = \{\, \Sigma_n \in \boldsymbol{Set} \,\}_{n \in \mathbb{N}}$$

algebras:

$$\underline{A} = \{\, \Sigma_n \times A^n \to A \,\}_{n \in \mathbb{N}}$$

free constructions:

$$\begin{tikzcd} V \arrow[r] \arrow[dr, "\forall\, \rho"'] & T(V) \arrow[d, dashed, "\exists!\, \rho^{\#}"] \\ & \underline{A} \end{tikzcd}$$

terms, variables,
and substitution:

$$\begin{array}{ccc} T(V) \times \underline{A}^V & \longrightarrow & \underline{A} \\ t, \rho & \longmapsto & t[\rho] \end{array}$$

equations:

$$V \vdash t \equiv t'$$

validity:

$$\underline{A} \models t \equiv t'$$
$$\text{iff } \forall \rho \in \underline{A}^V.\, t[\rho] = t'[\rho]$$

Birkhoff's Deduction Problem

Devise a deduction system such that

$t \equiv t'$ is derivable from a set of equations $\mathcal{E}$

soundness $\Downarrow$ $\qquad$ $\Uparrow$ completeness

for all $\underline{A} \models \mathcal{E}$, $\underline{A} \models t \equiv t'$

Birkhoff's Equational Logic of Universal Algebra

$$\frac{(t \equiv t') \in \mathcal{E}}{t \equiv t'}$$

$$\frac{t_i \equiv t_i' \quad (i = 1, \ldots, n)}{\mathsf{o}(t_1, \ldots, t_n) \equiv \mathsf{o}(t_1', \ldots, t_n')} \quad (\mathsf{o} : n)$$

$$\frac{t \equiv t'}{t[\rho] \equiv t'[\rho]} \quad (\rho \text{ a substitution})$$

Analysis of Universal Algebra

Syntax	Semantics
signatures: $\Sigma = \{\, \Sigma_n \in \boldsymbol{Set} \,\}_{n \in \mathbb{N}}$	
	algebras: $\underline{A} = \{\, \Sigma_n \times A^n \to A \,\}_{n \in \mathbb{N}}$
	free constructions: (see diagram below)
terms, variables, and substitution: $\begin{array}{ccc} \mathsf{T}(V) \times \underline{A}^V & \to & \underline{A} \\ t, \rho & \mapsto & t[\rho] \end{array}$	
equations: $V \vdash t \equiv t'$	
	validity: $\underline{A} \models t \equiv t'$ iff $\forall \rho \in \underline{A}^V .\, t[\rho] = t'[\rho]$

free constructions:

$$\begin{tikzcd} V \arrow[r] \arrow[dr, "\forall\, \rho"'] & \mathsf{T}(V) \arrow[d, dashed, "\exists!\, \rho^{\#}"] \\ & \underline{A} \end{tikzcd}$$

II

Monadic Equational Systems and Equational Metalogic

Monadic Equational Systems

Generalised Syntax	Semantics

$\mathbb{T}$ a strong monad

E-M algebras:

$$\underline{A} = (TA \to A)$$

generalised terms:

$$t : U \to TV$$

(Kleisli maps)

variables:

$$V \to TV$$

substitution:

$$\sigma : TV \otimes [V, \underline{A}] \to \underline{A}$$

interpretation:

$$\begin{tikzcd} U \otimes [V, \underline{A}] \arrow[r, "[\![t]\!]"] \arrow[d, "t \otimes \mathrm{id}"'] & \underline{A} \\ TV \otimes [V, \underline{A}] \arrow[ur, "\sigma"'] & \end{tikzcd}$$

generalised equations:

$$t \equiv t' : U \to TV$$

validity:

$$\underline{A} \models t \equiv t' \text{ iff } [\![t]\!] = [\![t']\!]$$

Deduction Problem

Devise a deduction system such that

$\mathsf{t} \equiv \mathsf{t}' : \mathsf{U} \to \mathsf{TV}$ is derivable from a set of generalised equations $\mathcal{E}$

$$\text{soundness} \Downarrow \qquad \Uparrow \text{completeness}$$

for all $\underline{A} \models \mathcal{E}$, $\underline{A} \models \mathsf{t} \equiv \mathsf{t}'$

Equational Metalogic

$$(\mathrm{Subst})\ \frac{\begin{array}{c} t_1 \equiv t_1' : U \to TV \\ t_2 \equiv t_2' : V \to TW \end{array}}{t_1[t_2] \equiv t_1'[t_2'] : U \to TW}$$

$$(\mathrm{LocChar})\ \frac{\begin{array}{c} \{\, e_i : U_i \longrightarrow U \,\}_{i \in I} \text{ jointly epi} \\ t\, e_i \equiv t'\, e_i : U_i \to TV \quad (i \in I) \end{array}}{t \equiv t' : U \to TV}$$

$$(\mathrm{Ext})\ \frac{t \equiv t' : U \to TV}{\langle W \rangle t \equiv \langle W \rangle t' : W \otimes U \to T(W \otimes V)}$$

Soundness

If $t \equiv t' : U \to TV$ is derivable from $\mathcal{E}$

then $\underline{A} \models t \equiv t'$, for all $\underline{A} \models \mathcal{E}$.

Internal Soundness and Completeness

For

$\widetilde{T}V$ the free algebra satisfying $\mathcal{E}$

and

$q : TV \to \widetilde{T}V$ the associated quotient map,

the following are equivalent:

1. $\underline{A} \models t \equiv t' : U \to TV$, for all $\underline{A} \models \mathcal{E}$
2. $\widetilde{T}V \models t \equiv t' : U \to TV$
3. $q\, t = q\, t' : U \to \widetilde{T}V$

Methodology

Model

universe of discourse

$\mathbb{S}$

abstract syntax

$\mathbb{T}$

Theory

Deductive System

axioms

arities

$$\mathcal{A} \rhd f \equiv f' : C \to TA$$

co-arities

sound for a canonical algebraic model theory
+
framework for completeness

interpretation

concretion

syntactic structure

Equational Logical Framework

$$\mathcal{A} \rhd \Gamma \vdash t \equiv t'$$

Applications

- Rational reconstruction of mono-sorted and multi-sorted equational logic.
- Synthetic Nominal Equational Logic.
- Metalogic for the enriched algebraic theories of Kelly and Power.
- Algebraic model theory for rewriting modulo equations.

III

Second-Order Equational Logic

Beyond First-Order

Computer Science

- $(\lambda x.\, M)\, N = M[{}^{N}\!/\!{}_{x}]$
- $\lambda x.\, M\, x \ = M \quad \big(x \notin \mathsf{FV}(M)\big)$

Logic

- $\neg(\forall x.\, P) = \exists x.\, \neg P$
- $(\forall x.\, P) \vee Q = \forall x.\, (P \vee Q) \quad \big(x \notin \mathsf{FV}(Q)\big)$

Mathematics

- $\int \Big(\int f(x, y)\, dx \Big)\, dy = \int \Big(\int f(x, y)\, dy \Big)\, dx$
- $P(c) \simeq \int^{z \in \mathbb{C}} \mathbb{C}(c, z) \times P(z)$

[Church 1940]

A formulation of the simple theory of types.

Simple Type Theory

	algebraic	simply typed	dependently typed
		theories	
types	unstructured	algebraic	algebraic with binding
terms	algebraic	algebraic with binding	algebraic with binding

The syntactic theory should account for:

- variables and meta-variables
- variable binding and α-equivalence
- capture-avoiding and meta substitution
- mono and multi sorting

Synthesis of Second-Order Equational Logic

- Development in the spirit of Birkhoff:
  from model theory to deductive system.

- *Second-Order Equational Logic* is synthesised from an *Equational Metalogic* by means of a syntactic concretisation of a monadic model theory.

- *Soundness* is guaranteed by construction; *completeness* is established by an explicit description of free constructions as syntactic quotients under (bidirectional) term rewriting.

Algebraic Model Theory

finite sets (contexts)
and functions (renamings)

$$\mathcal{S}et^{\mathbb{F}}$$

Σ

$$\Sigma(X) = \coprod_{\vec{n}=(n_1,\ldots,n_k)\in\mathbb{N}^*} \Sigma_{\vec{n}} \times \prod_{i=1}^{k} X^{V^{n_i}}$$

$X \in \mathcal{S}et^{\mathbb{F}}$ provides $\begin{cases} X\Gamma \ (\Gamma \in \mathbb{F}) \\ \mathbb{F}(\Gamma, \Delta) \longrightarrow \mathcal{S}et(X\Gamma, X\Delta) \end{cases}$

E.g. the object of variables is $V\Gamma = \Gamma$

interpretation

syntactic structure =

- arities: an operator of arity $\vec{n} = (n_1, \ldots, n_k)$ takes k arguments, respectively binding n_i variables.
- signature: $\Sigma = \{\, \Sigma_{\vec{n}} \in \mathcal{S}et^{\mathbb{F}} \,\}_{\vec{n}\in\mathbb{N}^*}$

+

- **substitution**

Algebras with Substitution

(Σ-monoids)

- algebra structure:

$$\Sigma X \xrightarrow{\xi} X$$

- substitution structure:

$$\text{monoid} \quad V \xrightarrow{e} X \xleftarrow{m} X \bullet X$$

$$\left(\equiv \quad \begin{array}{c} \Gamma \longrightarrow X\Gamma \longleftarrow X\Delta \times (X\Gamma)^{\Delta} \\ \text{subject to the laws of substitution} \end{array} \right)$$

subject to the compatibility condition:

$$\begin{tikzcd}
\Sigma(X) \bullet X \arrow[r] \arrow[d, "\xi \bullet X"'] & \Sigma(X \bullet X) \arrow[r, "\Sigma m"] & \Sigma X \arrow[d, "\xi"] \\
X \bullet X \arrow[rr, "m"'] & & X
\end{tikzcd}$$

Monadic Model Theory

$$\begin{tikzcd} \mathbf{\Sigma\text{-Mon}} \arrow[d, shift left] \\ \mathcal{S}et^{\mathbb{F}} \arrow[u, shift left] \arrow[u, phantom, "\dashv"] \arrow["\mathcal{M}_\Sigma"', loop below] \end{tikzcd}$$

Thm:

1. $$\mathcal{M}_\Sigma(X) \cong V + X \bullet \mathcal{M}_\Sigma(X) + \Sigma(\mathcal{M}_\Sigma X)$$

2. For Σ induced by a binding signature,

   $\mathcal{M}_\Sigma$ is a strong monad .

   (Needed to develop a theory of strengths.)

concretion

Syntactic theory.

Syntactic Theory

- *Canonical specification* and derived *correct definition* of
  - variable renaming,
  - capture-avoiding simultaneous substitution,
  - meta-variable renaming,
  - meta-substitution.
- Canonical *algebraic model theory*.

- **Contexts**

$$\mathsf{M}_1 : [m_1], \ldots, \mathsf{M}_k : [m_k] \rhd x_1, \ldots, x_n \ \left(\forall_{1 \leq i \leq k}\, m_i \in \mathbb{N}\right)$$

- **Terms**

(Variables)

For $x \in \Gamma$,

$$\frac{}{\Theta \rhd \Gamma \vdash x}$$

(Parameterised metavariables)

For $(\mathsf{M} : [m]) \in \Theta$,

$$\frac{\Theta \rhd \Gamma \vdash t_i \ (1 \leq i \leq m)}{\Theta \rhd \Gamma \vdash \mathsf{M}[t_1, \ldots, t_m]}$$

(Operators)

$$\mathsf{o} : (m_1, \ldots, m_k) \quad \left(\forall_{1 \le i \le k} \ m_i \in \mathbb{N}\right)$$

o is an operator taking k arguments each of which binds m_i variables

$$\frac{\Theta \rhd \Gamma, \vec{x_i} \vdash t_i \ \ (1 \le i \le k)}{\Theta \rhd \Gamma \vdash \mathsf{o}\big((\vec{x_1})\, t_1, \ldots, (\vec{x_k})\, t_k\big)}$$

Second-Order Equational Logic

- **Equational presentations**

  An *equational presentation* is a set of axioms each of which is a pair of terms in context.

λ-calculus

$$\lambda : (1)\,,\ @ : (0,0)$$

$$(\beta) \qquad \mathsf{M} : [1]\,,\ \mathsf{N} : [0] \ \rhd\ \cdot$$
$$\vdash\ \lambda\big(\,(x)\mathsf{M}[x]\,\big)\,@\,\mathsf{N}[\,] \equiv \mathsf{M}\big[\mathsf{N}[\,]\big]$$

$$(\eta) \qquad \mathsf{F} : [0] \ \rhd\ \cdot$$
$$\vdash\ \lambda\big(\,(x)\mathsf{F}[\,]\,@\,x\,\big) \equiv \mathsf{F}[\,]$$

Typed λ-calculus

$$\lambda^{\sigma,\tau} \quad : \quad (\sigma)\tau \to \sigma \Rightarrow \tau$$

$$@^{\sigma,\tau} \quad : \quad \sigma \Rightarrow \tau, \sigma \to \tau$$

$$(\beta) \quad \mathsf{M} : [\sigma]\tau\,,\ \mathsf{N} : [\,]\sigma \ \rhd\ \cdot$$
$$\vdash\ \lambda^{\sigma,\tau}\big((x)\mathsf{M}[x]\big)\,@^{\sigma,\tau}\mathsf{N}[\,] \equiv \mathsf{M}\big[\mathsf{N}[\,]\big] : \tau$$

$$(\eta) \quad \mathsf{F} : [\,](\sigma \Rightarrow \tau)\ \rhd\ \cdot$$
$$\vdash\ \lambda^{\sigma,\tau}\big((x)\,\mathsf{F}[\,]\,@^{\sigma,\tau}x\big) \equiv \mathsf{F}[\,] : \sigma \Rightarrow \tau$$

Classical first-order logic

Connectives	$\bot, \top$	:	o
	$\vee, \wedge$	:	$o, o \to o$
	$\neg$	:	$o \to o$
Quantifier	$\forall$	:	$(\iota)o \to o$
Functions	$f_i^{(m)}$	:	$\underbrace{\iota, \ldots, \iota}_{m} \to \iota$
Predicates	$P_j^{(n)}$	:	$\underbrace{\iota, \ldots, \iota}_{n} \to o$

Boolean algebra axioms for $(\bot, \vee, \top, \wedge, \neg)$

$$P : [\iota]o\,,\;\; X : [\,]\iota \;\; \rhd \;\; \cdot$$
$$\vdash \;\forall\big(\,(x)P[x]\,\big) \equiv \forall\big(\,(x)P[x]\,\big) \wedge P\big[X[\,]\big] \;\; : o$$

$$P : [\iota]o\,,\;\; Q : [\,]o \;\; \rhd \;\; \cdot$$
$$\vdash \;\forall\big(\,(x)\;P[x] \vee Q[\,]\,\big) \equiv \forall\big(\,(x)P[x]\,\big) \vee Q[\,] \;\; : o$$

Theory axioms $\;\; \cdot \rhd \cdot \vdash \varphi_k \equiv \top : o$

- **Deductive system**

  (Extended metasubstitution)

$$\frac{\mathsf{M}_1 : [m_1], \ldots, \mathsf{M}_k : [m_k] \rhd \Gamma \vdash s \equiv t \qquad \Theta \rhd \Delta, \vec{x_i} \vdash s_i \equiv t_i \quad (1 \leq i \leq k)}{\Theta \rhd \Gamma, \Delta \vdash s\{\mathsf{M}_i := (\vec{x_i})s_i\}_{1 \leq i \leq k} \equiv t\{\mathsf{M}_i := (\vec{x_i})t_i\}_{1 \leq i \leq k}}$$

<u>Metasubstitution</u>:

- $x\{\mathsf{M}_i := (\vec{x_i})t_i\}_{1 \leq i \leq k} = x$
- $\big(\mathsf{M}_\ell[s_1, \ldots, s_m]\big)\{\mathsf{M}_i := (\vec{x_i})t_i\}_{1 \leq i \leq k}$

  $= \; t_\ell[s'_j/x_{i,j}]_{1 \leq j \leq m}$

  where $s'_j = s_j\{\mathsf{M}_i := (\vec{x_i})t_i\}_{1 \leq i \leq k}$
- $\big(\mathsf{o}(\ldots, (\vec{x})s, \ldots)\big)\{\mathsf{M}_i := (\vec{x_i})t_i\}_{1 \leq i \leq k}$

  $= \; \mathsf{o}\big(\ldots, (\vec{x})s\{\mathsf{M}_i := (\vec{x_i})t_i\}_{1 \leq i \leq k}, \ldots\big)$

Theorems

- Categories of models are monadic, and complete and cocomplete. The induced monads are finitary and preserve epimorphisms.

- Second-order equational logic is a conservative extension of Birkhoff's (first-order) equational logic.

- Two completeness results.
  1. Semantic completeness of second-order derivability.
  2. Derivability completeness of (bidirectional) second-order term rewriting.

IV

Second-Order Algebraic Theories

Second-Order Theory of Equality

- Terms

$$M_1 : [m_1], \ldots, M_k : [m_k] \rhd x_1, \ldots, x_n \vdash s$$

where

$$\begin{array}{rcll} s & ::= & x_j & (1 \leq j \leq n) \\ & \mid & M_i[s_1, \ldots, s_{m_i}] & (1 \leq i \leq k) \end{array}$$

under the metasubstitution mechanism.

- The category $\mathbb{M}$ has set of objects $\mathbb{N}^*$ and morphisms

$$(m_1, \ldots, m_k) \to (n_1, \ldots, n_\ell)$$

given by tuples

$$\langle\, M_1 : [m_1], \ldots, M_k : [m_k] \rhd x_1, \ldots, x_{n_i} \vdash s_i \,\rangle_{1 \leq i \leq \ell}$$

that compose by *metasubstitution*.

The Structure of Second-Order Equality

Universal property of $\mathbb{M}$.

The category $\mathbb{M}$ is universally characterised as the free (strict) cartesian category on an exponentiable object, *viz.* (0).

- Products:

$$(m_1, \ldots, m_k) = (m_1) \times \cdots \times (m_k)$$

- Exponentiability:

$$(m) = (0)^m \Rightarrow (0)$$

Second-Order Algebraic Theories

- A (mono-sorted) *second-order algebraic theory* consists of a small cartesian category $\mathbb{T}$ and a strict cartesian identity-on-objects functor $\mathbb{M} \longrightarrow \mathbb{T}$ that preserves the exponentiable object (0).

- The category $\mathcal{M}od(\mathbb{T})$ of (set-theoretic) *functorial models* of a second-order algebraic theory $\mathbb{T}$ is the category of cartesian functors $\mathbb{T} \longrightarrow \mathcal{S}et$ and natural transformations between them.

Algebraic Translations

For second-order algebraic theories $\mathbb{M} \to \mathbb{T}$ and $\mathbb{M} \to \mathbb{T}'$, a second-order *algebraic translation* is a functor $\mathbb{T} \to \mathbb{T}'$ such that

$$\begin{tikzcd} & \mathbb{M} \arrow[dl] \arrow[dr] & \\ \mathbb{T} \arrow[rr] & & \mathbb{T}' \end{tikzcd}$$

Algebraic Functors

Every second-order algebraic translation $\mathrm{F} : \mathbb{T} \to \mathbb{T}'$ contravariantly induces an *algebraic functor* $\mathrm{F}^* : \mathcal{M}\boldsymbol{od}(\mathbb{T}') \to \mathcal{M}\boldsymbol{od}(\mathbb{T})$.

- Algebraic functors have left adjoints.

Theories *vs.* Presentations

Classifying categories

— the theory of a presentation

For every second-order equational presentation $\mathcal{E}$, we construct a second-order algebraic theory $\mathbb{M}(\mathcal{E})$.

Internal languages

— the presentation of a theory

For every second-order algebraic theory T, we construct a second-order equational presentation $\mathscr{E}(\mathsf{T})$.

Theorems

- **Theory/presentation correspondence.**

  Every second-order algebraic theory T is isomorphic to the second-order algebraic theory of its associated equational presentation $\mathbb{M}(\mathscr{E}(\mathsf{T}))$.

- **Presentation/theory correspondence.**

  Every second-order equational presentation $\mathcal{E}$ is isomorphic, with respect to a notion of *syntactic translation*, to the second-order equational presentation of its associated algebraic theory $\mathscr{E}(\mathbb{M}(\mathcal{E}))$.

  (An interesting example of syntactic translation is the CPS transform.)

- The above two correspondences yield an equivalence of categories.

- **Universal-algebra/categorical-algebra correspondence.**

  For every second-order equational presentation $\mathcal{E}$, the category of algebraic models $\mathcal{E}$-Mod and the category of functorial models $\mathcal{M}od(\mathbb{M}(\mathcal{E}))$ are equivalent.

- **Categorical-algebra/universal-algebra correspondence.**

  For every second-order algebraic theory T, the category of functorial models $\mathcal{M}od(\mathsf{T})$ and the category of algebraic models $\mathscr{E}(\mathsf{T})$-Mod are equivalent.

Further Directions

- Completeness of equational metalogic.
- Second-order universal algebra.
  - $\rightsquigarrow$ Second-order variety theorem.
  - $\rightsquigarrow$ Second-order algebraic categories.
- Model theory for higher-order term rewriting.
  - $\rightsquigarrow$ Second-order rewriting logic.
  - $\rightsquigarrow$ Equivalence of higher-order reductions.
- Constructions on second-order algebraic theories.
- Higher-order homotopical algebra.

Recent Developments

- Dependent types (e.g. Martin Löf Type Theory).
- Polymorphism (e.g. System F).

Papers

[1] M. Fiore and C.-K. Hur. **Term equational systems and logics**. In *Proceedings of the 24th Conference on the Mathematical Foundations of Programming Semantics (MFPS XXIV)*, ENTCS, volume 218, pages 171–192, 2008.

[2] M. Fiore. **Second-order and dependently-sorted abstract syntax**. In *Logic in Computer Science Conf. (LICS'08)*, pages 57–68. IEEE, Computer Society Press, 2008.

[3] M. Fiore. **Algebraic Meta-Theories and Synthesis of Equational Logics**. Research Programme, 2009.

[4] M. Fiore and C.-K. Hur. **Second-order equational logic**. In *Proceedings of the 19th EACSL Annual Conference on Computer Science Logic (CSL 2010)*, volume 6247 of *Lecture Notes in Computer Science*, pages 320–335. Springer-Verlag, 2010.

[5] M. Fiore and O. Mahmoud. **Second-order algebraic theories**. In *Proceedings of the 35th International Symposium on Mathematical Foundations of Computer Science (MFCS 2010)*, volume 6281 of *Lecture Notes in Computer Science*, pages 368–380. Springer-Verlag, 2010.