Modular Monadic Meta-Theory

Benjamin Delaware  
University of Texas at Austin  
bendy@cs.utexas.edu

Steven Keuchel  
Ghent University  
{steven.keuchel,tom.schrijvers}@ugent.be

Tom Schrijvers  
The University of Hong Kong  
bruno@cs.hku.hk

Abstract

This paper presents 3MT, a framework for modular mechanized meta-theory of languages with effects. Using 3MT, individual language features and their corresponding definitions – semantic functions, theorem statements and proofs – can be built separately and then reused to create different languages with fully mechanized meta-theory. 3MT combines modular datatypes and monads to define denotational semantics with effects on a per-feature basis, without fixing the particular set of effects or language constructs.

One well-established problem with type soundness proofs for denotational semantics is that they are notoriously brittle with respect to the addition of new effects. The statement of type soundness for a language depends intimately on the effects it uses, making it particularly challenging to achieve modularity. 3MT solves this long-standing problem by splitting these theorems into two separate and reusable parts: a feature theorem that captures the well-typing of denotations produced by the semantic function of an individual feature with respect to only the effects used, and an effect theorem that adapts well-typings of denotations to a fixed superset of effects. The proof of type soundness for a particular language simply combines these theorems for its features and the combination of their effects. To establish both theorems, 3MT uses two key reasoning techniques: modular induction and algebraic laws about effects. Several effectful language features, including references and errors, illustrate the capabilities of 3MT. A case study reuses these features to build fully mechanized definitions and proofs for 28 languages, including several versions of mini-ML with effects.

Categories and Subject Descriptors D.3.1 [Programming Languages]: Formal Definitions and Theory—Semantics

General Terms Languages

Keywords mechanized meta-theory; modularity; monads; side-effects

1. Introduction

Theorem provers are actively used to mechanically verify large-scale formalizations of critical components, including programming language meta-theory [1], compilers [25], large mathematical proofs [15] and operating system kernels [23]. Due to their scale and complexity, these developments can be quite time consuming, often demanding multiple man-years of effort.

It is reasonable to expect that variations can simply extend and reuse the original development in order to leverage the large investment of resources in these formalizations. This is unfortunately often not the case, as even small extensions can require significant additional effort. Adding a new language feature to a programming language formalization or compiler, for example, involves significant redesigns that have a cross-cutting impact on nearly all definitions and proofs in the formalization. This leads to a copy-paste approach to reuse with several modified copies of the original development, making it difficult to compose new features and ultimately leading to a maintenance nightmare. Dissatisfied with this situation, several researchers [1, 15, 43, 44] have called for better ways to modularize mechanical formalizations.

This work extends the current state-of-the-art in modular mechanizations by solving a well-known and long-standing open problem with denotational semantics: type soundness proofs are notoriously brittle with respect to the addition of new effects. This is an important problem because effects are pervasive in programming language formalizations: in addition to extensions to syntax and semantics, new features usually introduce new effects to the denotations. Without a more robust formulation of type soundness, the addition of new effects requires cross-cutting changes to type soundness theorem statements and proofs.

Initially the semantics themselves were also brittle with respect to effects [24, 32], but monads [31, 50] have been found to provide the necessary robustness to denotations. Yet as far as we know, the brittleness of (denotational) type soundness proofs has remained an open problem since it was raised by Wright and Felleisen [53] to motivate their own type-soundness approach. The framework we present here, modular monadic meta-theory (3MT), is the first in 20 years to provide a substantial solution. Using 3MT, we develop a novel approach to proving type soundness for monadic denotational semantics in a way that is modular in the set of effects used. Proofs for individual features do not depend on effects they do not use and hence are robust to extension.

The solution builds on Meta-Theory à la Carte (MTC) [9], a Coq framework for the mechanization of formal programming language meta-theory that supports modular extension of existing definitions. With MTC it is possible to develop meta-theory which is modular in two dimensions: language features on the one hand and functions and proofs over these features on the other hand. MTC adapts ideas from existing programming language solutions [34, 46] to the expression problem [51] for functions and features, and adds modular induction for proofs.

3MT adds a third modularity dimension to MTC: modular addition of new effects. 3MT enables the separate definition of features with effectful semantic functions and proofs over these functions, and reuse of these features in formalizations of multiple languages.
To make denotations robust with respect to effects, 3MT uses the established solution, *monads*. In Coq, *type classes* [52] enable semantic function definitions that are constrained, yet polymorphic in the monad. This allows the inclusion of a feature in any language which supports a superset of its effects. When a language is composed from different effectful features, *monad transformers* [28] are used to instantiate the denotation’s monad with all the effects required by the modular components.

To solve the key challenge of modularizing and reusing theorems and proofs of type soundness, we split the classic type soundness theorems into three parts:

1. **Reusable feature theorems** capture the essence of type soundness for an individual feature. They depend only on that feature’s syntax, typing relation, semantic function and the effects used therein. At the same time, they abstract over the syntax, semantics and effects of other features. This means that the addition of new features with other types of effects does not affect the existing feature theorem proofs.

To achieve the abstraction over other effects, a feature uses a constrained polymorphic monad. As a consequence, it only establishes the well-typing of the resulting denotations with respect to the effects declared in the constraints.

2. **Reusable effect theorems** fix the monad of denotations and consequently the set of effects. They take well-typing proofs of monadic denotations expressed in terms of a constrained polymorphic monad and which mention only a subset of effects, and turn them into well-typings with respect to a fixed monad and all the effects it provides.

Effect theorems reason fully at the level of denotations and abstract over the details of language features like syntax and semantic functions.

3. Finally, **language theorems** establish type soundness for a particular language. They require no more effort than to instantiate the set of features and the set of effects (i.e., the monad), thus tying together the respective feature and effect theorems into an overall proof.

To establish the first two theorems, 3MT relies on modular induction and algebraic laws about effects. As far as we know, it applies the most comprehensive set of such laws to date, as each effect utilized by a feature needs to be backed up by laws and interactions between different effects must also be governed by laws. These laws are crucial for modular reasoning in the presence of effects.

In summary, the specific contributions of this work are:

- A reusable framework, 3MT, for mechanized meta-theory of languages with effects. This framework includes a mechanized library for monads, monad transformers and corresponding algebraic laws in Coq. Besides several laws for specific types of effects, the library also includes laws for the interactions between different types of effects.
- A new modular proof method for type-soundness proofs of denotational semantics.
- A case study of a family of fully mechanized languages, including a mini-ML variant with errors and references. The case study comprises 28 languages, 8 different effect theorems and 5 features with their feature theorems.

3MT is implemented in the Coq proof assistant and the code is available at [http://www.cs.utexas.edu/~bendy/3MT](http://www.cs.utexas.edu/~bendy/3MT).

**Code and Notational Conventions** While all the code underlying this paper has been developed in Coq, the paper adopts a terser syntax for its many code fragments. For the computational parts, this syntax exactly coincides with Haskell syntax, while it is an extrapolation of Haskell syntax style for propositions and proof concepts. Following MTC, the Coq code requires the impredicative-set option due to the use of Church encodings.

**2. Background: Meta-Theory à la Carte**

This section summarizes the necessary parts of the *Meta-Theory à la Carte* (MTC) approach to modular datatypes in Coq. For the full details of MTC, we refer the reader to the original paper [9].

**2.1 Mendler Church Encodings and Folds for Semantics**

MTC encodes data types and folds with a variant of Church encodings [5, 36] based on Mendler folds [47]. The advantage of Mendler folds is that recursive calls are explicit, allowing the user to precisely control the evaluation order. The Mendler-Church encodings represent (least) fixpoints and folds as follows:

$$
\text{type } \text{Type } \text{Alg}_M f \ a = \forall r. (r \to a) \to f \ r \to a \\
\text{type } \text{Fix}_M f = \forall a. \text{Type } \text{Alg}_M f \ a \to a \\
\text{fold}_M :: \text{Type } \text{Alg}_M f \ a \to \text{Fix}_M f \ a \to a \\
\text{fold}_M \text{alg } fa = fa \text{ alg}
$$

Mendler algebras \((\text{Type } \text{Alg}_M f \ a)\) use a function argument of type \((r \to a)\) for their recursive calls. To enforce structurally recursive calls, arguments which appear at recursive positions have a polymorphic type \(r\). Using this polymorphic type prevents case analysis, or any type of inspection, on those arguments. Mendler-Church encodings \((\text{Fix}_M f)\) are functions of type \(\forall a. \text{Type } \text{Alg}_M f \ a \to a\).

Mendler folds are defined by directly applying a Church encoded value \(fa\) to a Mendler algebra \(\text{alg}\). All these definitions are non-recursive and can thus be expressed in Coq.

**Example** As a simple example, consider a language for boolean expressions supporting boolean literals and conditionals:

$$
\text{data } \text{Logic } e = \text{Blit } \text{Bool} \mid \text{If } e \ e \ e \\
\text{type } \text{Value } = \text{Bool}
$$

The evaluation algebra for this language is defined as follows:

$$
\text{ifAlg :: } \text{Type } \text{Alg}_M \text{Logic } e \text{ Value} \\
\text{ifAlg } \text{[] } \text{Blit } b \text{ } = b \\
\text{ifAlg } \text{[} e_1 e_2 e_3 \text{]} \text{ if } \text{[} e_1 \text{]} \text{ then } \text{[} e_2 \text{]} \text{ else } \text{[} e_3 \text{]}
$$

Unlike conventional Church encodings and folds, the recursive calls ([·]) are explicit and indicate the evaluation order.

The evaluation function simply folds the \(\text{ifAlg}\) algebra:

$$
\text{eval } :: \text{Fix}_M \text{Logic } e \to \text{Value} \\
\text{eval } = \text{fold}_M \text{ifAlg}
$$

**2.2 Modular Composition of Features**

MTC adapts the *Data Types à la Carte* (DTC) [46] approach for composing \(f\)-algebras to Mendler algebras.

**Modular Functors** Because feature syntax is defined by means of functors, such as \(\text{Logic } e\), it can easily be composed with functor composition:

$$
\text{data } \text{Arith } e = \text{Lit } \text{Int} \mid \text{Add } e \ e
$$

The syntax of a language of both conditional and simple arithmetic expressions, for example, is \(\text{Fix } (\text{Arith } e \oplus \text{Logic } e)\) where:

$$
\text{data } \text{Arith } e = \text{Lit } \text{Int} \mid \text{Add } e \ e
$$

Semantic functions are expressed as Mendler algebras and can be composed in a similar way.

**Type Classes** Unlike DTC, MTC defines a number of type classes with laws in order to support proofs. These classes and laws are summarized in the table in Figure 1. The second column notes whether the base instances of a particular class are provided by the user or are automatically inferred with a default instance. Importantly, instances of all these classes for feature compositions (using \(\odot\)) are built automatically.
The class \( \text{inj} \) in DTC and it includes two additional laws which govern the be-

dings, so MTC adapts the proof methods used in the

2.3 Modular Proofs

The main novelty of MTC is its modular approach to inductive
proofs. Regular structural induction is not available for Church en-
codings, so MTC adapts the proof methods used in the initial algebra semantics of data types [14, 29] – in particular universal properties – to support modular inductive proofs over Church encodings. Proofs are written in the same modular style as functions, using proof algebras (class \( \text{PAlg} \) in Figure 1). These algebras are folded over the terms and can be modularly combined. Unlike func-
tion algebras, proof algebras are subject to an additional constraint which ensures the validity of the proofs (\( \text{proj}_eq \)).

\section{The 3MT Monad Library}

3MT includes a monad library to support effectful semantic func-
tions using \textit{monads} and \textit{monad transformers}, and provides alge-
braic laws for reasoning. Monads provide a uniform representation for encapsulating computational effects such as mutable state, exception handling, and non-determinism. Monad transformers allow monads supporting the desired set of effects to be built. Algebraic laws are the key to modular reasoning about monadic definitions.

3MT implements the necessary definitions of \textit{monads} and \textit{monad transformers} as a Coq library inspired by the Haskell \textit{monad transformer library} (MTL) [28]. Our library refines the MTL in two key ways in order to support modular reasoning using algebraic laws. While algebraic laws can only be documented informally in

\begin{center}
\begin{tabular}{|c|l|}
\hline
Class Definition & Description \\
\hline
\texttt{class Functor f where} & \texttt{Functors Supplied by the user} \\
\hline
\texttt{fmap :: (a \to b) \to (f a \to f b)} & \\
\texttt{fmap\_id :: fmap \_id \equiv id} & \\
\texttt{fmap\_fusion :: \_\_g h,} & \\
\texttt{fmap \_h \circ \_g} & \\
\hline
\texttt{class f \_<\ g where} & \texttt{Function Subtyping Inferred} \\
\texttt{inj :: f a \to g a} & \\
\texttt{prj :: g a \to \_f (f a)} & \\
\texttt{inj\_prj :: inj \_prj} & \\
\texttt{prj\_inj :: prj \_inj} & \\
\hline
\texttt{class (Functor f, \textit{Functor} g, f <\ g) \Rightarrow} & \texttt{Function Delegation Inferred} \\
\texttt{WF.Functor f g where} & \\
\texttt{wf \_functor :: \_a b \equiv (\_a \to \_b).} & \\
\texttt{fmap \_h \circ \_g} & \\
\hline
\texttt{class (Functor h, f <\ h, g <\ h) \Rightarrow} & \texttt{Function Discrimination Inferred} \\
\texttt{DistinctSubFunctor f g h where} & \\
\texttt{inj\_discriminate :: \_a (\_f :: f a)} & \\
\texttt{\_g :: g (g a), inj \_fe \not\equiv inj \_ge} & \\
\hline
\texttt{class \textit{FAlg} name t a f where} & \texttt{Function Algebras Supplied by the user} \\
\texttt{f\_algebra :: Mixin t f a} & \\
\hline
\texttt{class (f <\ g, \textit{FAlg} n t a f, \textit{FAlg} n t a g) \Rightarrow} & \texttt{Algebra Delegation Inferred} \\
\texttt{WF.FAAlg n t a f g where} & \\
\texttt{wf\_algebra :: \_\_a (\_\_a :: f t),} & \\
\texttt{f\_algebra \_rec (inj \_fa)} & \\
\texttt{f\_algebra \_rec \_fa} & \\
\hline
\texttt{class (Functor f, \textit{Functor} g, f <\ g) \Rightarrow} & \texttt{Proof Algebras Supplied by the User} \\
\texttt{\textit{PAlg} name f g a where} & \\
\texttt{p\_algebra :: Algebra f a} & \\
\texttt{proj\_eq :: \_\_\_1 (p\_algebra \_e)} & \\
\texttt{id \_\_ (inj (fmap \_p \_a))} & \\
\hline
\end{tabular}
\end{center}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure1.png}
\caption{Type classes provided by 3MT}
\end{figure}

The \textit{Functor} class provides the \texttt{fmap} method and is an adap-
tation of the corresponding type class in Haskell. In contrast with the Haskell version, the two functor laws are part of the definition.

Figure 1. Type classes provided by 3MT

\begin{itemize}
\item \texttt{eqType t} is a slight generalization of Mendler algebras, which is useful for defining non-Inductive language features such as general recursion or higher-order binders. The type class \textit{WF.FAAlg} provides a well-

\begin{enumerate}
\item \texttt{eval :: AlgebraM Ref \_ (Env \to (Value, \_\_\_))}
\item \texttt{evalErr :: AlgebraM ErrP \_ (Maybe Value, \\
\begin{itemize}
\item MTC supports the composition of two algebras over different func-
tors as long as they have the same carrier. That is not the case here,
\end{itemize}
\end{enumerate}

\subsection{Sublemmas}

Each feature builds extensible datatypes by abstracting

\subsection{No Effect Modularity}

Unfortunately, effect modularity is not supported in MTC. Consider two features: mutable references \textit{Ref} and errors \textit{ErrP}. Both of these introduce an effect to any language, the former state and the

\section{The 3MT Monad Library}

3MT includes a monad library to support effectful semantic func-
tions using \textit{monads} and \textit{monad transformers}, and provides alge-

Supporting two instances of the same effect requires extra machinery [41].

The particular implementation of a type class, we can still modularly reason about its behavior via these laws. This is crucial for supporting modular reasoning [35].

The first three laws for the Monad class are standard, while the last law (fmap bind) relates fmap and bind in the usual way. Each monad subclass also includes its own set of laws. The laws for various subclasses can be found scattered throughout the functional programming literature, such as for failure [13] and state [13, 35]. Yet, as far as we know, 3MT is the first to systematically bring them together. Furthermore, although most laws have been presented in the semantics literature in one form or another, we have not seen some of the laws in the functional programming literature. One such example are the laws for the exception class:

- The bind throw law generalizes the bind fail law: a sequential computation is aborted by throwing an exception.
- The catch throw law states that the exception handler is invoked when an exception is thrown in a catch.
- The catch throw law 2 indicates that an exception handler is redundant if it just re-throws the exception.
- The catch return law states that a catch around a pure computation is redundant.
- The fmap catch law states that pure functions (fmap f) distribute on the right with catch.

Other definitions. Our monad library contains a number of other classes, definitions and laws apart from the definitions discussed here. This includes infrastructure for other types of effects (e.g. writer effects), as well as other infrastructure from the MTL. There are roughly 30 algebraic laws in total.

4. Modular Monadic Semantics

Features can utilize the monad library included with 3MT to construct algebras for semantic functions which are compatible with a range of effects. These modular monadic algebras have the form:

\[ \text{eval}_{\text{ref}} :: S_\text{m} \text{Store} m \Rightarrow \text{Algebra}_{\text{mt}} \text{Ref } f (m a) \]
\[ \text{eval}_{\text{error}} :: E_\text{m} \Rightarrow \text{Algebra}_{\text{mt}} \text{Error } f (m a) \]

These algebras use monad subclasses such as \( S_\text{m} \) and \( E_\text{m} \) to constrain the monad required by the feature, allowing the monad to
have more effects than those used in the feature. These two algebras can be combined to create a new evaluation algebra with type:

\[(S_m, m, s, E_m, x) \Rightarrow \text{Algebra}_{m} \ (\text{Ref}_m \oplus \text{Err}_m) (m, a)\]

The combination imposes both type class constraints while the monad type remains extensible with new effects. The complete set of effects used by the evaluation algebras for the five language features used in our case study of Section 7 are given in Figure 4.

4.1 Example: References

Figure 3 illustrates this approach with definitions for the functor for expressions and the evaluation and typing algebras for the reference feature. Other features have similar definitions.

For the sake of presentation the definitions are slightly simplified from the actual ones in Coq. For instance, we have omitted issues related to the extensibility of the syntax for values (\text{Value}) and types (\text{Type}). We refer the interested reader to MTC [9] and the 3MT Coq code for these details. \text{Value} and \text{Type} are treated as abstract datatypes with a number of constructor functions: \text{loc}, \text{stack}, \text{unit}, \text{tRef} and \text{tUnit} denote respectively reference locations, stuck values, unit values, reference types and unit types. There are also matching functions \text{isLoc} and \text{isTRef} for checking whether a term is a location value or a reference type, respectively.

The type \text{Ref}_m is the functor for references. It has constructors for creating references (\text{Ref}) dereferencing (\text{DeRef}) and assigning (\text{Assign}) references. The evaluation algebra \text{eval}_{m} uses the state monad for its reference environment, which is captured in the type class constraint $S_m \text{Store}_m$. The typing algebra ($\text{typeof}_{m}$) is also monadic, using the failure monad to denote ill-typing.

4.2 Effect-Dependent Theorems

Monadic semantic function algebras are compatible with new effects and algebraic laws facilitate writing extensible proofs over these monadic algebras. Effects introduce further challenges to proof reuse, however: each combination of effects induces its own type soundness statement. Consider the theorem for a language with references which features a store $\sigma$ and a store typing $\Sigma$ that are related through the store typing judgement $\Sigma \vdash \sigma$:

\[
\forall e, t, \Sigma, \sigma. \left\{\begin{array}{l}
\text{typeof } e \equiv \text{return } t \\
\Sigma \vdash \sigma
\end{array}\right\} \Rightarrow
\exists v, \Sigma', \sigma'. \left\{\begin{array}{l}
\text{put } \sigma \triangleright \triangleright \varepsilon \equiv \text{put } \sigma' \triangleright \triangleright \text{return } v \\
\Sigma' \supseteq \Sigma \\
\Sigma' \vdash v : t
\end{array}\right\}
\]

(LSOUND$_S$)

Contrast this with the theorem for a language with errors, which must account for the computation possibly ending in an exception being thrown:

\[
\forall e, t. \text{typeof } e \equiv \text{return } t \\
(\exists v. [e] \equiv \text{return } v \land \vdash v : t) \lor (\exists x. \varepsilon \equiv \text{throw } x)
\]

(LSOUND$_E$)

Clearly, the available effects are essential for the formulation of the theorem. A larger language which involves both exceptions and state requires yet another theorem where the impact of both effects cross-cut one another:

\[
\forall e, t, \Sigma, \sigma. \left\{\begin{array}{l}
\text{typeof } e \equiv \text{return } t \\
\Sigma \vdash \sigma
\end{array}\right\} \Rightarrow
\exists v, \Sigma', \sigma'. \left\{\begin{array}{l}
\text{put } \sigma \triangleright \triangleright \varepsilon \equiv \text{put } \sigma' \triangleright \triangleright \text{return } v \\
\Sigma' \supseteq \Sigma \\
\Sigma' \vdash v : t
\end{array}\right\} \lor
\exists x. \text{put } \sigma \triangleright \triangleright \varepsilon \equiv \text{throw } x
\]

(LSOUND$_ES$)

Modular formulations of LSOUND$_E$ and LSOUND$_S$ are useless for proving a modular variant of LSOUND$_ES$ because their

\footnote{A similar proliferation of soundness theorems can be found in TAPL [37].}
induction hypotheses have the wrong form. The hypothesis for LSOUNDₐ requires the result to be of the form return v, disallowing put σ ꞌ⇒ return v (the form required by LSOUNDₐ). Similarly, the hypothesis for LSOUNDₐ does not account for exceptions occurring in subterms. In general, without anticipating additional effects, type soundness theorems with fixed sets of effects cannot be reused modularly.

5. Modular Monadic Type Soundness

In order to preserve a measure of modularity, we do not prove type soundness directly for a given feature, but by means of a more generic theorem. The technique of proving a theorem of interest by means of a more general theorem is well-known. For a conventional monolithic language, for instance, type soundness is often established for any well-formed typing context, even though the main interest lies with the more specific initial, empty context. In that setting, the more general theorem produces a weaker induction hypothesis for the theorem’s proof.

Our approach to type soundness follows the core idea of this technique and relies on three theorems:

- **FSOUND**: a reusable feature theorem that is only aware of the effects that a feature uses
- **ESOUND**: an effect theorem for a fixed set of known effects, and
- **LSOUND**: a language theorem which combines the two to prove soundness for a specific language.

In order to maximize compatibility, the statement of the reusable feature theorem cannot hardwire the set of effects. This statement must instead rephrase type soundness in a way that can adapt to any superset of a feature’s effects. Our solution is to have the feature theorem establish that the monadic evaluation and typing algebras of a feature satisfy an extensible well-formedness relation, defined in terms of effect-specific typing rules. Thus, a feature’s proof of FSOUND uses only the typing rules required for the effects specific to that feature. The final language combines the typing rules of all the language’s effects into a closed relation.

Figure 6 illustrates how these reusable pieces fit together to build a proof of soundness. Each feature provides a proof algebra for FSOUND which relies on the typing rules (WFM-X) for the effects it uses. Each unique statement of soundness for a combination of effects requires a new proof of ESOUND. The proof of LSOUND for a particular language is synthesized entirely from a single proof of ESOUND and a combination of proof algebras for FSOUND.

Note that there are several dimensions of modularity here. A feature’s proof of FSOUND only depends on the typing rules for the effects that feature uses and can thus be used in any language which includes those typing rules. The typing rules themselves can be reused by any number of different features. ESOUND depends solely on a specific combination of effects and can be reused in any language which supports that combination, e.g. both LSOUNDₐ and LSOUNDₐR use ESOUNDₐES.

5.1 Soundness for a Pure Feature

The reusable feature theorem FSOUND states that [] and TypeError are related by the extensible typing relation:

\[ \forall e, \Sigma. \; \Sigma \vdash_M \llbracket e \rrbracket : \text{typeof } e \]  \hspace{1cm} (∗)

Figure 5. Typing rules for pure monadic values.

Extensible Typing Relation The extensible typing relation has the form:

\[ \Sigma \vdash_M v_m : t_m \]  \hspace{1cm} (∗)

The relation is polymorphic in an environment type env and an evaluation monad type m. The parameters \( \Sigma, v_m, t_m \) are related by the extensible typing relation, defined in terms of effect-specific typing rules. Thus, a feature’s proof of FSOUND uses only the typing rules required for the effects specific to that feature. The final language combines the typing rules of all the language’s effects into a closed relation.

Figure 6 lists the two base typing rules of this relation. These do not constrain the evaluation monad and environment types and are the only rules needed for pure features. The (WFM-ILLTYPED) rule ensures that nothing can be said about computations (\( m_c \)) which are ill-typed. The (WFM-RETURN) rule ensures that well-typed computations only yield values of the expected type.

To see how the reusable theorem works for a pure feature, consider the proof of soundness for the boolean feature.

**Proof** Using the above two rules, we can show that FSOUND holds for the boolean feature. The proof has two cases. The boolean literal case is handled by a trivial application of (WFM-RETURN). The second case, for conditionals, is more interesting³.

\[
\begin{align*}
\Gamma & \vdash_M [\epsilon_c] : \text{typeof } \epsilon_c \\
\Gamma & \vdash_M [\epsilon_l] : \text{typeof } \epsilon_l \\
\Gamma & \vdash_M [\epsilon_e] : \text{typeof } \epsilon_e \\
\Gamma \vdash \text{do } v \leftarrow [\epsilon_c] \\
\Gamma \vdash \text{case } \text{isBool } v \text{ of} \\
\Gamma \vdash \text{Just } b \rightarrow \text{t_l} \\
\Gamma \vdash \text{if } b \text{ then } [\epsilon_l] \text{ else } [\epsilon_e] \\
\Gamma \vdash \text{Nothing } \rightarrow \text{stuck} \\
\end{align*}
\]

³ We omit the environment \( \Sigma \) to avoid clutter.
ever, perform case analysis on the derivations of the proofs produced by the induction hypothesis that the subexpressions are well-formed, \( \vdash_M [e_c] : \text{typeof } e_c, \vdash_M [e_z] : \text{typeof } e_z \) and \( \vdash_M [e_v] : \text{typeof } e_v \). The final rule used in each derivation determines the shape of the monadic value produced by \([e_c]\) and \(\text{typeof } e_v\). Assumingly that only the pure typing rules of Figure 5 are used for the derivations, we can divide the proof into two cases depending on whether \(e_c, e_z\), or \(e_v\) was typed with \((\text{WFM-ILLTYPED})\).

- If any of the three derivations uses \((\text{WFM-ILLTYPED})\), the result of \(\text{typeof } e\) is \(\text{fail}\). As \(\text{fail}\) is the zero of the typing monad, \((\text{WFM-ILLTYPED})\) resolves the case.
- Otherwise, each of the subderivations was built with \((\text{WFM-RETURN})\) and the evaluation and typing expressions can be simplified using the \(\text{return bind}\) monad law.

\[
\vdash_M \begin{cases} \text{isBool } v_c \text{ of} \\
\text{Just } b \quad \rightarrow \quad \text{return } v_t \\
\text{else } \quad \text{return } v_c \\
\text{Nothing} \quad \rightarrow \quad \text{stuck}
\end{cases}
\]

After simplification, the typing expression has replaced the bind with explicit values which can be reasoned with. If \(\text{isBool } t_e\) is \(\text{false}\), then the typing expression reduces to \(\text{fail}\) and well-formedness again follows from the \((\text{WFM-ILLTYPED})\) rule. Otherwise \(t_e \equiv TBool\), and we can apply the inversion lemma

\[
\vdash v : TBOOL \rightarrow \exists b. \text{Just } b
\]

Figure 7. Typing rules for exceptional monadic values.

to establish that \(v_c\) is of the form \(\text{Just } b\), reducing the evaluation to either \(\text{return } v_t\) or \(\text{return } v_c\). A similar case analysis on \(\text{eqT } t_c, t_x\) will either produce \(\text{fail}\) or \(\text{return } t_t\). The former is trivially true, and both \(\vdash_M \text{return } v_c : \text{return } t_t\) and \(\vdash_M \text{return } v_c : \text{return } t_t\) hold in the latter case from the induction hypotheses.

### Modular Sublemmas

The above proof assumed that only the pure typing rules of Figure 5 were used to type the subexpressions of the \(\text{if}\) expression, which is clearly not the case when the boolean feature is included in an effectful language. Instead, case analyses are performed on the extensible typing relation in order to make the boolean feature theorem compatible with new effects. Case analyses over the extensible \(\vdash_M\) relation are accomplished using extensible proof algebras which are folded over the derivations provided by the induction hypothesis, as outlined in Section 2.3.

In order for the boolean feature’s proof of \(\text{FSOUND}\) to be compatible with a new effect, each extensible case analysis requires a proof algebra for the new typing rules the effect introduces to the \(\vdash_M\) relation. These proof algebras are examples of feature interactions \(\text{[3]}\) from the setting of modular component-based frameworks. In essence, a feature interaction is functionality (e.g., a function or a proof) that is only necessary when two features are combined. Importantly, these proof algebras do not need to be provided up front when developing the boolean algebra, but can instead be modularly resolved by a separate feature for the interaction of boolean and the new effect.

The formulation of the properties proved by extensible case analysis has an impact on modularity. The conditional case of the previous proof can be dispatched by folding a proof algebra for the property \(\text{WFM-If-Vc}\) over \(\vdash_M [v_c] : \text{typeof } t_c\). Each new effect induces a new case for this proof algebra, however, resulting in an interaction between boolean and every effect. \(\text{WFM-If-Vc}\) is specific to the proof of \(\text{FSOUND}\) in the boolean feature; proofs of \(\text{FSOUND}\) for other features require different properties and thus different proof algebras. Relying on such specific properties can lead to a proliferation of proof obligations for each new effect.

Alternatively, the boolean feature can use a proof algebra for a stronger property that is also applicable in other proofs, cutting down on the number of feature interactions. One such stronger, more general sublemma relates the monadic bind operation to well-typing:

\[
\begin{align*}
\Sigma &\vdash_M \text{throw } x : t_m \\
\forall \Sigma' : k : t_m &\rightarrow \Sigma' \vdash_M k_v : k_t T &\rightarrow \\
\Sigma &\vdash_M \text{catch } m : k : t_m
\end{align*}
\]

A proof of \(\text{WFM-If-Vc}\) follows from two applications of this stronger property. The advantage of \(\text{WFM-Bind}\) is clear: it can be reused to deal with case analyses in other proofs of \(\text{FSOUND}\), while a proof of \(\text{WFM-If-Vc}\) has only a single use. The disadvantage is that \(\text{WFM-Bind}\) may not hold for some new effect, while the weaker \(\text{WFM-If-Vc}\) does, possibly excluding some feature combinations. As \(\text{WFM-Bind}\) is a desirable property for typing rules, the case study focuses on that approach.

### 5.2 Type Soundness for a Pure Language

The second phase of showing type soundness is to prove a statement of soundness for a fixed set of effects. For pure effects, the soundness statement is straightforward:

\[
\forall v_m. t. \vdash_M v_m : \text{return } t \Rightarrow \exists v, v_m \equiv \text{return } v \land \vdash v : t \\
\text{Ladding to ESOUND}\text{.}
\]

Each effect theorem is proved by induction over the derivation of \(\vdash_M v_m : \text{return } t\). \(\text{ESOUND}\) fixes the irrelevant environment type to the type \(\text{()\)} and the evaluation monad to the pure monad \(\text{1}\). Since the evaluation monad is fixed, the proof of \(\text{ESOUND}\) only needs to consider the pure typing rules of Figure 5. The proof of the effect theorem is straightforward: \(\text{WFM-ILLTYPED}\) could not have been used to derive \(\vdash_M v_m : \text{return } t\), and \(\text{WFM-RETURN}\) provides both a witness for \(v\) and a proof that it is of type \(t\).

The statement of soundness for a pure language built from a particular set of features is similar to \(\text{ESOUND}\):

\[
\forall e, t. \text{typeof } e \equiv \text{return } t \Rightarrow \exists v, [e] \equiv \text{return } v \land \vdash v : t \\
\text{LSOUND.}
\]

The proof of \(\text{LSOUND}\) is an immediate consequence of the reusable proofs of \(\text{FSOUND}\) and \(\text{ESOUND}\). Folding a proof algebra for \(\text{FSOUND}\) over \(e\) provides a proof of \(\vdash_M [e] : \text{return } t\), satisfying the first assumption of \(\text{ESOUND}\). \(\text{LSOUND}\) follows immediately.

### 5.3 Errors

The evaluation algebra of the error language feature uses the side effects of the exception monad, requiring new typing rules.

#### Typing Rules

Figure 7 lists the typing rules for monadic computations involving exceptions. \(\text{WFM-Throw}\) states that \(\text{throw } x\) is typeable with any type. \(\text{WFM-Catch}\) states that binding the results of both branches of a \(\text{catch}\) statement will produce a monad with the same type. While it may seem odd that this rule is formulated in terms of a continuation \(\gg\gg k\), it is essential for compatibility with the proofs algebras required by other features. As described
in Section 5.1, extensible proof algebras over the typing derivation will now need cases for the two new rules. To illustrate this, consider the proof algebra for the general purpose WFM-BIND property. This algebra requires a proof of:

\[
\begin{align*}
\forall \gamma, \Gamma \vdash \gamma & \rightarrow \Gamma \vdash_M k \gamma : t_m \\
\exists \delta \vdash_M \delta \gamma & \rightarrow \Gamma \vdash_M k \delta \gamma : t_m \\
\end{align*}
\]  
(WFM-GET)

\[
\begin{align*}
\forall \gamma, \Gamma \vdash \gamma & \rightarrow \Gamma \vdash_M k \gamma : t_m \\
\exists \delta \vdash_M \delta \gamma & \rightarrow \Gamma \vdash_M k \delta \gamma : t_m \\
\end{align*}
\]  
(WFM-ASK)

\[
\begin{align*}
\forall \gamma, \Gamma \vdash \gamma & \rightarrow \Gamma \vdash_M k \gamma : t_m \\
\exists \delta \vdash_M \delta \gamma & \rightarrow \Gamma \vdash_M k \delta \gamma : t_m \\
\end{align*}
\]  
(WFM-PUT)

\[
\begin{align*}
\forall \gamma, \Gamma \vdash \gamma & \rightarrow \Gamma \vdash_M k \gamma : t_m \\
\exists \delta \vdash_M \delta \gamma & \rightarrow \Gamma \vdash_M k \delta \gamma : t_m \\
\end{align*}
\]  
(WFM-LOCAL)

\[
\begin{align*}
\forall \gamma, \Gamma \vdash \gamma & \rightarrow \Gamma \vdash_M k \gamma : t_m \\
\exists \delta \vdash_M \delta \gamma & \rightarrow \Gamma \vdash_M k \delta \gamma : t_m \\
\end{align*}
\]  
(WFM-BOT)

![Figure 8. Typing rules for stateful monadic values.](image)

**Effect Theorem**  The effect theorem, ESOUND₀, for a language whose only effect is exceptions reflects that the evaluation function is either a well-typed value or an exception.

\[
\forall \nu_m, t. \vdash_M \nu_m : \text{return } t \Rightarrow \\
\exists \nu_m \equiv \text{throw } x \vee \exists \nu_m \equiv \text{return } v \wedge v \vdash : t \quad \text{(ESOUND₀)}
\]

The proof of ESOUND₀ is again by induction on the derivation of \(\Gamma \vdash_M \nu_m : \text{return } t\). The irrelevant environment can be fixed to \(I\), while the evaluation monad is the exception monad \(\mathbb{E}_1 x \frac{1}{x}\).

The typing derivation is built from four rules: the two pure rules from Figure 5 and the two exception rules from Figure 7. The case for the two pure rules is effectively the same as before, and WFM-THROW is straightforward. In the remaining case, \(\nu_m \equiv \text{catch } e' h\), and we can leverage the fact that the evaluation monad is fixed to conclude that either \(\exists v. v \equiv \text{return } v\) or \(\exists x. e' \equiv \text{throw } x\). In the former case, \(\text{catch } e' h\) can be reduced using \text{catch_return}, and the latter case is simplified using \text{catchThrow}. In both cases, the conclusion then follows immediately from the assumptions of WFM-CATCH. The proof of the language theorem LSOUND₀ is similar to LSOUND and is easily built from ESOUND₀ and FSOUND.

5.4 References

**Typing Rules**  Figure 8 lists the two typing rules for stateful computations. To understand the formulation of these rules, consider LSOUND₀, the statement of soundness for a language with a stateful evaluation function. The statement accounts for both the typing environment \(\Sigma\) and evaluation environment \(\sigma\) by imposing the invariant that \(\sigma\) is well-formed with respect to \(\Sigma\). FSOUND however, has no such conditions (which would be anti-modular in any case).

We avoid this problem by accounting for the invariant in the typing rules themselves:

- WFM-GET requires that the continuation \(k\) of a \text{get} is well-typed under the invariant.
- WFM-PUT requires that any newly installed environment maintains this invariant.

The intuition behind these premises is that effect theorems will maintain these invariants in order to apply the rules.

6. Effect Compositions

As we have seen, laws are essential for proofs of FSOUND. The proofs so far have involved only one effect and the laws regulate the behavior of that effect’s primitive operations.
Languages often involve more than one effect, however. Hence, the proofs of effect theorems must reason about the interaction between multiple effects. There is a trade-off between fully instantiating the monad for the language as we have done previously, and continuing to reason about a constrained polymorphic monad. The former is easy for reasoning, while the latter allows the same language proof to be instantiated with different implementations of the monad. In the latter case, additional effect interaction laws are required.

6.1 Languages with State and Exceptions

Consider the effect theorem which fixes the evaluation monad to support exceptions and state. The statement of the theorem mentions both kinds of effects by requiring the evaluation function to be run with a well-formed state \( \sigma \) and by concluding that well-typed expressions either throw an exception or return a value. The WFM-CATCH case this theorem has the following goal:

\[
\forall \gamma, \delta, \eta, e E, \epsilon T. \quad \Sigma \vdash \gamma : \Sigma \quad \Rightarrow \quad \exists \gamma', \delta', \eta', e', \epsilon T.
\]

\[
\exists \gamma', \delta', \eta', e', \epsilon T. \quad \exists \gamma', \delta', \eta', e', \epsilon T. \quad \gamma, \delta \vdash e E \equiv e T
\]

\[
\Sigma \vdash \eta : \eta
\]

\[
\Sigma \vdash \delta : \delta
\]

\[
\Sigma \vdash \gamma : \Gamma
\]

\[
\text{typeof } e T \equiv \text{return } t
\]

In order to apply the induction hypothesis to \( e \) and \( h \), we need to precede them by a \( \text{put} \). Hence, \( \text{put} \) must be pushed under the catch statement through the use of a law governing the behavior of \( \text{put} \) and \( \text{catch} \). There are different choices for this law, depending on the monad that implements both \( \text{put} \) and \( \text{catch} \). We consider two reasonable choices, based on the monad and transformer compositions \( E F t \) and \( E S t (E T (E T 1)) \):

- Either \( \text{catch} \) passes the current state into the handler:
  
  \[
  \exists \gamma', \delta', \eta', e', \epsilon T. \quad \exists \gamma', \delta', \eta', e', \epsilon T. \quad \gamma, \delta \vdash e E \equiv e T
  \]

- Or \( \text{catch} \) runs the handler with the initial state:
  
  \[
  \exists \gamma', \delta', \eta', e', \epsilon T. \quad \exists \gamma', \delta', \eta', e', \epsilon T. \quad \gamma, \delta \vdash e E \equiv e T
  \]

The WFM-CATCH case is provable under either choice. As the LSOUND_E proof is written as an extensible theorem, the two cases are written as two separate proof algebras, each with a different assumption about the behavior of the interaction. Since the cases for the other rules are impervious to the choice, they can be reused with either proof of WFM-CATCH.

6.2 Full Combination of Effects

A language with references, errors and lambda abstractions features four effects: state, exceptions, an environment and failure. The language theorem for such a language relies on the effect theorem ESOUND_ESRF given in Figure 10. The proof of ESOUND_ESRF is similar to the previous effect theorem proofs, and makes use of the full set of interaction laws given in Figure 11. Perhaps the most interesting observation here is that because the environment monad only makes local changes, we can avoid having to choose between laws regarding how it interacts with exceptions. Note also that since we are representing nontermination using a failure monad \( F m \), the catch fail law conforms to our desired semantics.

7. Case Study

As a demonstration of the 3MT framework, we have built a set of five reusable language features and combined them to build a family of languages which includes a mini-ML [8] variant with references and errors. The study includes pure boolean and arithmetic features as well as effectful features for references, errors and lambda abstractions.

![Figure 10. Effect theorem statement for languages with errors, state, an environment and failure.](http://www.cs.utexas.edu/~bendy/3MT)

The study builds twenty eight different combinations of the features which are all possible combinations with at least one feature providing values. Figure 13 presents the syntax of the expressions, values, and types provided; each line is annotated with the feature that provides that set of definitions.

Four kinds of feature interactions appear in the case study.

- The PHOAS representation of binders requires an auxiliary equivalence relation, the details of which are covered in the MTC paper [9]. The soundness proofs of language theorems

![Figure 11. Interaction laws](http://www.cs.utexas.edu/~bendy/3MT)
for languages which include binders proceed by induction over this equivalence relation instead of expressions. The reusable feature theorems of other features need to be lifted over this equivalence relation.

- The effect theorems that feature an environment typing \( \Sigma \), such as those for state or environment, need a weakening sublemma which states that each well-formed value under \( \Sigma \) is also well-formed under a conservative extension:

\[
\Sigma \vdash v : t \Rightarrow \Sigma' \supseteq \Sigma \vdash v : t
\]

- Inversion lemmas for the well-formed value relation as in the proof of FS\textsc{ound} for the boolean feature in Section 5.1 are proven by induction over the relation.

The proofs of the first and second kind of feature interactions are straightforward; the inversion lemmas of the third kind can be dispatched by tactics hooked into the type class inference algorithm.

The framework itself consists of about 4,400 LoC of which about 2,000 LoC comprise the implementation of the monad transformers and their algebraic laws. The size in LoC of the implementation of semantic evaluation and typing functions and the reusable feature theorem for each language feature is given in the left box in Figure 12. The right box lists the sizes of the effect theorems. Each language needs on average 110 LoC to assemble its semantic functions and soundness proofs from those of its features and the effect theorem for its set of effects.

### 8. Related Work

While previous work has explored the basic techniques of modularizing dynamic semantics of languages with effects, our work is the first to show how to also do modular proofs. Adding the ability to do modular proofs required the development of novel techniques for reasoning about modular components with effects.

#### 8.1 Functional Models for Modular Side Effects

**Monads and Monad Transformers** Since Moggi [31] first proposed monads to model side-effects, and Wadler [50] popularized them in the context of Haskell, various researchers (e.g., [21, 45]) have sought to modularize monads. Monad transformers emerged [6, 28] from this process, and in later years various alternative implementation designs facilitating monad (transformer) implementations, have been developed, including Filinski’s layered monads [10] and Jaskelioff’s Monatron [19].

**Monads and Subtyping** Filinski’s MultiMonadic MetaLanguage (M^M\textsc{L}) [11, 12] embraces the monadic approach, but uses subtyping (or subeffecting) to combine the effects of different components. The subtyping relation is fixed at the program or language level, which does not provide the adaptability we achieve with constrained polymorphism.

**Algebraic Effects and Effect Handlers** In the semantics community the algebraic theory of computational effects [39] has been an active area of research. Many of the laws about effects, which we have not seen before in the context of functional programming, can be found throughout the semantics literature. Our first four laws for exceptions, for example, have been presented by Levy [26].

A more recent model of side effects is effect handlers. They were introduced by Plotkin and Pretnar [38] as a generalization from exception handlers to handlers for a range of computational effects, such as I/O, state, and nondeterminism. Bauer and Pretnar [4] built the language \( \text{Eff} \) around effect handlers and show how to implement a wide range of effects in it. Kammar et al. [22] showed that effect handlers can be implemented in terms of delimited continuations or free monads.

The major advantage of effect handlers over monads is that they are more easily composed, as any composition of effect operations and corresponding handlers is valid. In contrast, not every composition of monads is a monad. In the future, we plan on investigating the use of effect handlers instead of monad transformers, which could potentially reduce the amount of work involved on proofs about interactions of effects.

**Other Effect Models** Other useful models have been proposed, such as applicative functors [30] and arrows [17], each with their own axioms and modularity properties.
8.2 Modular Effectful Semantics

There are several works on how to modularize semantics with effects, although none of these works considers reasoning.

Mosses [33] modularizes structural operational semantics by means of a label transition system where extensible labels capture effects like state and abrupt termination. Swierstra [46] presents modular syntax with functor coproducts and modular semantics with algebra compositions. To support effects, he uses modular syntax to define a free monad. The effectful semantics for this free monad is not given in a modular manner; however, Jaske-loff et al. [20] present a modular approach for operational semantics on top of Swierstra’s modular syntax, although they do not cover conventional semantics with side-effects. Both Schrijvers and Oliveira [42] and Bahr and Hvitved [2] have shown how to define modular semantics with monads for effects; this is essentially the approach followed in this paper for modular semantics.

8.3 Effects and Reasoning

Non-Modular Monadic Reasoning Although monads are a purely functional way to encapsulate computational-effects, programs using monads are challenging to reason about. The main issue is that monads provide an abstraction over purely functional models of effects, allowing functional programmers to write programs in terms of abstract operations like >>=, return, or get and put. One way to reason about monadic programs is to remove the abstraction provided by such operations [18]. However, this approach is fundamentally non-modular.

Modular Monadic Reasoning Several more modular approaches to modular monadic reasoning have been pursued in the past.

One approach to modular monadic reasoning is to exploit parametricity [40, 49]. Voigtlander [48] has shown how to derive parametricity theorems for type constructor classes such as Monad. Unfortunately, the reasoning power of parametricity is limited, and parametricity is not supported by proof assistants like Coq.

A second technique uses algebraic laws. Liang and Hudak [27] present one of the earliest examples of using algebraic laws for reasoning. They use algebraic laws for reader monads to prove correctness properties about a modular compiler. In contrast to our work, their compiler correctness proofs are pen-and-paper and thus more informal than our proofs. Since they are not restricted by a termination checker or the use of positive types only, they exploit features like general recursion in their definitions. Oliveira et al. [35] have also used algebraic laws for the state monad, in combination with parametricity, for modular proofs of non-interference of aspect-oriented advice. Hinze and Gibbons discuss several other algebraic laws for various types of monads [13]. However, as far as we know, we are the first to provide an extensive mechanized library for monads and algebraic laws in Coq.

8.4 Mechanization of Monad Transformers

Huffmann [16] illustrates an approach for mechanizing type constructor classes in Isabelle/HOL with monad transformers. He considers transformer variants of the resumption, error and writer monads, but features only the generic functor, monad and transformer laws. The work tackles many issues that are not relevant for our Coq setting, such as lack of parametric polymorphism and explicit modeling of laziness.

9. Conclusion

In previous work [9] we have shown that it is possible to modularize meta-theory along two dimensions: 1) language constructs and 2) operations and proofs. A significant limitation of that work is that it only considered pure languages.

This work lifts that limitation and shows how to develop modular meta-theory for languages with effects. Our solution uses monads and corresponding algebraic laws for reasoning about different types of effects. The key challenge that we have solved is how to formulate and prove a general type-soundness theorem in a modular way that enables the reuse of feature proofs across multiple languages with different sets of effects. This turned out to be non-trivial because existing formulations of type-soundness are very sensitive to the particular effects used by the language.

As a secondary contribution, our work shows that algebraic laws about effects scale up to realistic verification tasks such as meta-theoretic proofs. As far as we know, it is their largest application to date. In this setting, the proof assistant Coq has been invaluable. While the typically smaller examples in the functional programming community can easily be dealt with by pen-and-paper proofs, that approach would not have been manageable for the large family of type-soundness proofs for mini-ML variants, as keeping track of large goals and hypotheses by hand would be too painful and error-prone.

Acknowledgements We would like to thank the anonymous reviewers for their many comments and suggestions. This work was supported by the National Science Foundation under Grant CCF 0724979.

References


