A metalanguage for multi-phase modularity

JONATHAN STERLING and ROBERT HARPER, Carnegie Mellon University, USA

Type abstraction, the phase distinction, and computational effects all play an important role in the design and implementation of ML-style module systems. We propose a simple type theoretic metalanguage \( \Phi_{\text{ML}} \) for multi-phase modularity in which these concepts are treated individually, supporting the definition of high-level modular constructs such as generative and applicative functors, as well as all extant forms of structure sharing.

In most accounts of ML modules, the phase distinction between static code and dynamic code is enforced pervasively throughout the language [10, 16]; for instance, in a functor signature of the form \( (x : A) \to B(x) \), the signature \( B(x) \) is only allowed to depend on the “static part” of \( A \). The purpose of this restriction is to ensure that the judgmental equality of types and other static constructs can be decided independently of the existence of any notion of equality for programs.

Recently several authors have advanced a monadic presentation of ML modules in which both generativity and other effects are treated using a lax modality \( \circ \) on signatures [3, 8, 22]. When effects are treated monadically, there is however no obstacle to formulating a (conservative and tractable) notion of judgmental equality for programs, hence it is appropriate to revisit the global restriction that types shall never depend on runtime code.

1 THE NEED FOR VALUE-DEPENDENCY

In order to preserve abstraction, it is often necessary for types to depend on runtime identity; generativity of ML functors is one way to achieve this in the context of effects, but the need for this kind of dependency also occurs even for applicative functors such as \( \text{MkSet} \), as pointed out by Rossberg et al. [20]. This shows that one needs to depend on runtime value identity to achieve abstraction regardless of whether computational effects are in play; generative functors capture specifically the case where modules (potentially) exhibit dynamic initialization effects.

Static dependency on runtime identity can be approximated using phantom types as in the elaboration of Rossberg et al. [20, § 8.1], a logical version of the stamps of SML ’90 [14]. While phantom types have a definite role to play, providing the most conservative possible static approximation of value identity, experience implementing and compiling full-spectrum dependently typed programming languages (e.g. Idris 2 and Lean 4 [2, 4]) suggests that there is no longer any reason to make this the only way that types can depend on values.

2 LET A HUNDRED PHASE DISTINCTIONS BLOOM!

The venerable static–dynamic phase distinction is not the only phase distinction that can be considered. For instance, logical relations arguments can be reformulated à la Sterling and Harper [22] in terms of a syntactic–semantic phase distinction; type refinements in the sense of Melliès and Zeilberger [13] evince a phase distinction between computation (extraction) and logic (specification); security typing and information flow can be seen to exhibit a lattice of phase distinctions.

Because these are surely not the only phase distinctions that will play a role in future programming languages, we propose an adequate type theoretic metalanguage \( \Phi_{\text{ML}} \) that can accommodate any number of phase distinctions simultaneously. \( \Phi_{\text{ML}} \) starts with ordinary Martin-Löf type theory [17] and adds to it enough constructs to express modularity relative to a lattice of phase distinctions, denoted \( \Phi : \cal{O} \). (The rules of \( \Phi_{\text{ML}} \) are summarized in Fig. 1.)

Authors’ address: Jonathan Sterling, jmsterli@cs.cmu.edu; Robert Harper, rwh@cs.cmu.edu, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA.
Each phase $\phi : \emptyset$ induces a context extension $(\Gamma, \phi)$; types and terms in such a context are restricted to their $\phi$-visible components. For instance if $\phi := \phi_{st}$ is the static phase, the dynamic parts of a type $\Gamma, \phi_{st} \vdash A$ type are collapsed. In this sense, the weakening substitution along $\Gamma, \phi_{st} \rightarrow \Gamma$ implements the static projection operation $\text{Fst}(\_)$ from prior type theoretic accounts of modules [5], and judgmental equality $\Gamma, \phi_{st} \vdash A \equiv B$ type in the extended context reconstructs the static equivalence judgment of Dreyer et al. [6].

2.1 Modal type structure of $\phi$ML

2.1.1 The phase modality. The context extension $\Gamma, \phi$ is internalized as the phase modality $(\phi \Rightarrow \_)$; semantically, $(\phi \Rightarrow \_)$ behaves like a function space whose domain is the collection of proofs that we are “in” the $\phi$ phase. Such a modality corresponds in the topological frame semantics of intuitionistic logic to the local operator induced by an open subspace.

2.1.2 The sealing modality. A type $A$ is called sealed at $\phi : \emptyset$, written $\Gamma \vdash A\text{ sealed }@\phi$, when it is equivalent to the unit type in phase $\phi$. We include a sealing modality $[\phi \setminus A]$ that seals a type $A$ at phase $\phi$; the laws for this modality are similar to those of the protection modality in the dependency core calculus of Abadi et al. [1], but they actually come from those of the local operator induced by a closed subspace in the topological semantics of intuitionistic logic. Indeed, the relationship between the phase and sealing modalities is essentially that of open subspace (e.g. static fragment) and closed complement (e.g. dynamic fragment).

2.1.3 Structure sharing. Given a type $A$ and an element $\phi \vdash M : A$, we may form the structure sharing type $\{ A \mid \phi \rightarrow M \} \subseteq A$ that classifies all the elements of $A$ equal to $M$ at phase $\phi$. In case $\phi := \phi_{st}$, the structure sharing type $\{ A \mid \phi_{st} \rightarrow M \} \subseteq A$ classifies the elements of $A$ that are statically equivalent to $M$ in the sense of Dreyer et al. [6] and therefore captures the weak structure sharing of SML ’97 [15]. On the other hand, if $\phi := \top$ is the “top” phase distinction, then $\{ A \mid \top \rightarrow M \}$ is the true singleton type that is approximated by SML ’90’s strong structure sharing [14] via stamps, and by the F-ing Modules calculi via phantom types [20].

2.2 Applications of $\phi$ML

We briefly survey a few applications of $\phi$ML’s perspective on multi-phase modularity.
2.2.1 Reconstructing ML’s static–dynamic phase distinction. The classic static–dynamic phase distinction of SML and OCaml is recovered by adding a single phase distinction \( \Phi_{\text{st}} : \emptyset \) together with a lax modality \( \bigcirc A \) for effects that is always statically sealed, in the sense that \( \Gamma \vdash \bigcirc A \text{ sealed } @ \Phi_{\text{st}} \) holds. Given another modality \( T \) that is not sealed, one could define the effect modality by \( \bigcirc A := [\Phi_{\text{st}} \setminus T(A)] \) in terms of the sealing modality. ML-style generative and applicative functionals may then be defined like so:

\[
\begin{align*}
\Pi^\text{gen}, \Pi^\text{app} : (A : \text{Sig}) (B : (\Phi_{\text{st}} \Rightarrow A) \to \text{Sig}) \to \text{Sig} \\
\Pi^\text{gen}(A, B) = (x : A) \to \bigcirc B(\langle \Phi_{\text{st}} \rangle x) \\
\Pi^\text{app}(A, B) = (x : A) \to B(\langle \Phi_{\text{st}} \rangle x)
\end{align*}
\]

We add a law to make the universe of kinds purely static in the sense that \( (\Phi_{\text{st}} \Rightarrow \text{Kind}) \equiv \text{Kind} \).

2.2.2 Compile-time inlining without breaking abstraction. Under a separate compilation discipline, e.g. that of Swasey et al. [26], a module is compiled as a function of its dependencies; unless special arrangements are made, this can obstruct the inlining of functions whose identities are not exposed by the dependencies’ interfaces. To address the inlining problem, Stone [23, § 1.5.3] and Leroy [11, § 5.3] have suggested extending the module language to support sharing of non-static phrases in module signatures; then this interface can be used by the compiler to support inlining of the exposed definitions. This is too naïve: users of module systems employ non-sharing in order to maintain abstraction and enforce their intention that a dependent module’s implementation is independent of some part of its dependency.

We propose to address the inlining problem by introducing a phase distinction \( \Phi_{\text{cmpl}} : \emptyset \) between compile-time and runtime.\(^1\) Value identities are exposed for inlining by means of the the structure sharing type \( \{A \mid \Phi_{\text{cmpl}} \Rightarrow M \} \); programmers will not be able to rely on the identities so-exposed, but the compiler will be executed in the \( \Phi_{\text{cmpl}} \) phase and can therefore exploit exposed identities for inlining. This application provides essential theoretical support for the efficient implementation of Harper’s proposal to treat datatypes as abstract types with default implementations [7].

2.2.3 Reconciling debugging with abstraction. Debugging is a common source of frustration when developing code in the presence of abstract types; many engineers today still primarily rely on so-called “printf-debugging” to diagnose broken code, but this becomes a problem in the presence of abstract types whose representations are unknown. We propose to add a new “debug” phase \( \Phi_{\text{dbg}} : \emptyset \) and, by default, expose the identities of all modules within the debug phase by means of the structure sharing type \( \{A \mid \Phi_{\text{dbg}} \Rightarrow M \} \); then we may add a primitive operation to the standard basis library that allows a \( \Phi_{\text{dbg}} \)-phase string to be printed, \( \text{debug} : (\Phi_{\text{dbg}} \Rightarrow \text{string}) \to \bigcirc \text{unit} \). Then in the presence of an element \( a : M.t \) whose (hidden) representation type is \( \text{int} \), we may freely debug by executing the side effect \( \text{debug}(\langle \Phi_{\text{dbg}} \rangle \text{int}.\text{toString}(a)) \).

2.2.4 Representation independence. Following the Logical Relations As Types principle of Sterling and Harper [22], we may capture binary parametricity [18] by adding two phases \( \Phi_{\text{syn}}^L, \Phi_{\text{syn}}^R : \emptyset \) with \( \Phi_{\text{syn}}^L \cap \Phi_{\text{syn}}^R \equiv \bot \) and defining \( \Phi_{\text{syn}} := \Phi_{\text{syn}}^L \cup \Phi_{\text{syn}}^R \). Then representation independence results can be proved: a simulation between queue implementations \( M, N : \text{QUEUE} \) is given by a third implementation \( O : \{\text{QUEUE} \mid \Phi_{\text{syn}} \leftrightarrow [\Phi_{\text{syn}}^L \leftrightarrow M, \Phi_{\text{syn}}^R \leftrightarrow N] \} \). This method is used by op. cit. to prove a generalized Reynolds Abstraction Theorem for a module calculus, and by Sterling and Angiuli [21] to prove normalization and decidability of judgmental equality for cubical type theory.

\(^1\)Here compile-time refers to a stage subsequent to typechecking/elaboration, and is therefore semantically different from a static phase.
REFERENCES


