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 **φML** 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 [12, 18]; 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 $x : A$. 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* $\bigcirc$ on signatures [5, 10, 24]. 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 MkSet, as pointed out by Rossberg et al. [22]. 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. [22, § 8.1], a logical version of the *stamps* of SML '90 [16]. 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 [4, 6]) 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 [24] in terms of a *syntactic–semantic* phase distinction; type refinements in the sense of Melliès and Zeilberger [15] 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* **φML** that can accommodate any number of phase distinctions simultaneously. **φML** starts with ordinary Martin-Löf type theory [19] and adds to it enough constructs to express modularity relative to a lattice of phase distinctions, denoted $\boxed{\varphi : \mathcal{O}}$.

Authors' address: Jonathan Sterling, jmsterli@cs.cmu.edu; Robert Harper, rwh@cs.cmu.edu, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA.

Each phase $\phi : \mathcal{O}$ induces a context extension (Γ, φ); types and terms in such a context are *restricted* to their φ-visible components. For instance if $\varphi :\equiv \phi_{\mathsf{st}}$ is the *static* phase, the dynamic parts of a type $\Gamma, \phi_{\mathsf{st}} \vdash A\ \mathit{type}$ are collapsed. In this sense, the weakening substitution along $\Gamma, \phi_{\mathsf{st}} \longrightarrow \Gamma$ implements the *static projection* operation $\mathsf{Fst}(-)$ from prior type theoretic accounts of modules [7], and judgmental equality $\Gamma, \phi_{\mathsf{st}} \vdash A \equiv B\ \mathit{type}$ in the extended context reconstructs the *static equivalence* judgment of Dreyer et al. [8].

2.1 Modal type structure of φML

2.1.1 The phase modality. The context extension Γ, φ is internalized as the **phase modality** $(\varphi \Rightarrow -)$; semantically, $(\varphi \Rightarrow -)$ behaves like a function space whose domain is the (subsingleton) collection of witnesses that we are "in" the φ phase.

2.1.2 The sealing modality. A type A is called *sealed* at $\varphi : \mathcal{O}$, written $\boxed{\Gamma \vdash A\ \mathsf{sealed}\ @\ \varphi}$, when it is equivalent to the *unit* type in phase φ. We include a **sealing modality** $[\varphi \setminus A]$ that seals a type A at phase φ; 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 $\varphi \vdash M : A$, we may form the **structure sharing** type $\{A \mid \varphi \hookrightarrow M\} \subseteq A$ that classifies all the elements of A equal to M at phase φ. In case $\varphi :\equiv \phi_{\mathsf{st}}$, the structure sharing type $\{A \mid \phi_{\mathsf{st}} \hookrightarrow M\} \leq A$ classifies the elements of A that are statically equivalent to M in the sense of Dreyer et al. [8] and therefore captures the *weak structure sharing* of SML '97 [17]. On the other hand, if $\varphi :\equiv \top$ is the "top" phase distinction, then $\{A \mid \top \hookrightarrow M\}$ is the true singleton type that is approximated by SML '90's *strong* structure sharing [16] via stamps, and by the F-ing Modules calculi via phantom types [22].

2.2 Applications of φML

We briefly survey a few applications of **φML**'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 $\phi_{\mathsf{st}} : \mathcal{O}$ together with a lax modality $\bigcirc A$ for effects that is always statically sealed, in the sense that $\boxed{\Gamma \vdash \bigcirc A\ \mathsf{sealed}\ @\ \phi_{\mathsf{st}}}$ holds. Given another modality T that is not sealed, one could define the effect modality by $\bigcirc A :\equiv [\phi_{\mathsf{st}} \setminus T(A)]$ in terms of the sealing modality. ML-style generative and applicative functors may then be defined like so:

$$\begin{aligned}
&\Pi^{\mathsf{gen}}, \Pi^{\mathsf{app}} : (A : \mathbf{Sig})\,(B : (\phi_{\mathsf{st}} \Rightarrow A) \to \mathbf{Sig}) \to \mathbf{Sig}\\
&\Pi^{\mathsf{gen}}(A, B) = (x : A) \to \bigcirc B(\langle \phi_{\mathsf{st}} \rangle x)\\
&\Pi^{\mathsf{app}}(A, B) = (x : A) \to B(\langle \phi_{\mathsf{st}} \rangle x)
\end{aligned}$$

We add a law to make the universe of *kinds* purely static in the sense that $(\phi_{\mathsf{st}} \Rightarrow \mathsf{Kind}) \cong \mathsf{Kind}$.

2.2.2 Compile-time inlining without breaking abstraction. Under a separate compilation discipline, *e.g.* that of Swasey et al. [28], 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 [25, § 1.5.3] and Leroy [13, § 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 $\phi_{\mathsf{cmpl}} : \mathcal{O}$ between *compile-time* and *runtime*.[1] Value identities are exposed for inlining by means of the the structure sharing type $\{A \mid \phi_{\mathsf{cmpl}} \hookrightarrow M\}$; programmers will not be able to rely on the identities so-exposed, but the compiler will be executed in the ϕ_{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 [9].

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 $\phi_{\mathsf{dbg}} : \mathcal{O}$ and, by default, expose the identities of all modules within the debug phase by means of the structure sharing type $\{A \mid \phi_{\mathsf{dbg}} \hookrightarrow M\}$; then we may add a primitive operation to the standard basis library that allows a ϕ_{dbg}-phase string to be printed, $\mathsf{debug} : (\phi_{\mathsf{dbg}} \Rightarrow \mathsf{string}) \to \bigcirc\mathsf{unit}$. Then in the presence of an element $a : M.\mathsf{t}$ whose (hidden) representation type is int, we may freely debug by executing the side effect $\mathsf{debug}(\langle\phi_{\mathsf{dbg}}\rangle\mathsf{Int.toString}(a))$.

2.2.4 Representation independence. Following the **Logical Relations As Types** principle of Sterling and Harper [24], we may capture *binary parametricity* [20] by adding two phases $\phi^{\mathsf{L}}_{\mathsf{syn}}, \phi^{\mathsf{R}}_{\mathsf{syn}} : \mathcal{O}$ with $\phi^{\mathsf{L}}_{\mathsf{syn}} \sqcap \phi^{\mathsf{R}}_{\mathsf{syn}} \equiv \bot$ and defining $\phi_{\mathsf{syn}} :\equiv \phi^{\mathsf{L}}_{\mathsf{syn}} \sqcup \phi^{\mathsf{R}}_{\mathsf{syn}}$. Then representation independence results can be proved: a simulation between queue implementations $M, N : \mathsf{QUEUE}$ is given by a third implementation $O : \{\mathsf{QUEUE} \mid \phi_{\mathsf{syn}} \hookrightarrow [\phi^{\mathsf{L}}_{\mathsf{syn}} \hookrightarrow M, \phi^{\mathsf{R}}_{\mathsf{syn}} \hookrightarrow N]\}$. This method is used by *op. cit.* to prove a generalized Reynolds Abstraction Theorem for a module calculus, and by Sterling and Angiuli [23] to prove normalization and decidability of judgmental equality for cubical type theory.

REFERENCES

[1] Martín Abadi, Anindya Banerjee, Nevin Heintze, and Jon G. Riecke. 1999. A Core Calculus of Dependency. In *Proceedings of the 26th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL '99)*. Association for Computing Machinery, San Antonio, Texas, USA, 147–160. https://doi.org/10.1145/292540.292555

[2] Andreas Abel, Thierry Coquand, and Miguel Pagano. 2009. A Modular Type-Checking Algorithm for Type Theory with Singleton Types and Proof Irrelevance. In *Typed Lambda Calculi and Applications*, Pierre-Louis Curien (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 5–19.

[3] David Aspinall. 1995. Subtyping with singleton types. In *Computer Science Logic*, Leszek Pacholski and Jerzy Tiuryn (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 1–15.

[4] Edwin Brady. 2021. Idris 2: Quantitative Type Theory in Practice. (2021). arXiv:2104.00480 [cs.PL] To appear in the proceedings of ECOOP 2021.

[5] Karl Crary. 2020. A focused solution to the avoidance problem. *Journal of Functional Programming* 30 (2020), e24. https://doi.org/10.1017/S0956796820000222 *Bob Harper Festschrift Collection.*

[6] Leonardo De Moura and Sebastian Ullrich. 2021. The Lean 4 Theorem Prover and Programming Language (System Description). (2021). To appear in the proceedings of the 28th International Conference on Automated Deduction.

[7] Derek Dreyer. 2005. *Understanding and Evolving the ML Module System.* Ph.D. Dissertation. Carnegie Mellon University, USA.

[8] Derek Dreyer, Karl Crary, and Robert Harper. 2003. A Type System for Higher-Order Modules. In *Proceedings of the 30th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL '03)*. Association for Computing Machinery, New Orleans, Louisiana, USA, 236–249. https://doi.org/10.1145/604131.604151

[9] Robert Harper. 2013. The Future of Standard ML. (2013). https://www.cs.cmu.edu/~rwh/talks/mlw13.pdf Talk given at the ML Workshop.

[1] Here compile-time refers to a stage subsequent to typechecking/elaboration, and is therefore semantically different from a static phase.

[10] Robert Harper. 2020. ***PFPL** Supplement: Types for Program Modules.* http://www.cs.cmu.edu/~rwh/pfpl/supplements/modules.pdf

[11] Robert Harper and Mark Lillibridge. 1994. A Type-Theoretic Approach to Higher-Order Modules with Sharing. In *Proceedings of the 21st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. Association for Computing Machinery, Portland, Oregon, USA, 123–137. https://doi.org/10.1145/174675.176927

[12] Robert Harper, John C. Mitchell, and Eugenio Moggi. 1990. Higher-Order Modules and the Phase Distinction. In *Proceedings of the 17th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. Association for Computing Machinery, San Francisco, California, USA, 341–354. https://doi.org/10.1145/96709.96744

[13] Xavier Leroy. 2000. A Modular Module System. *Journal of Functional Programming* 10, 3 (May 2000), 269–303. https://doi.org/10.1017/S0956796800003683

[14] David MacQueen, Robert Harper, and John Reppy. 2020. The History of Standard ML. *Proceedings of the ACM on Programming Languages* 4, HOPL (June 2020). https://doi.org/10.1145/3386336

[15] Paul-André Melliès and Noam Zeilberger. 2015. Functors are Type Refinement Systems. In *POPL '15: Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. ACM, Mumbai, India. https://hal.inria.fr/hal-01096910

[16] Robin Milner, Mads Tofte, and Robert Harper. 1990. *The Definition of Standard ML*. MIT Press.

[17] Robin Milner, Mads Tofte, Robert Harper, and David MacQueen. 1997. *The Definition of Standard ML (Revised)*. MIT Press.

[18] Eugenio Moggi. 1989. A Category-Theoretic Account of Program Modules. In *Category Theory and Computer Science*. Springer-Verlag, Berlin, Heidelberg, 101–117.

[19] Bengt Nordström, Kent Peterson, and Jan M. Smith. 1990. *Programming in Martin-Löf's Type Theory*. International Series of Monographs on Computer Science, Vol. 7. Oxford University Press, NY.

[20] John C. Reynolds. 1983. Types, Abstraction, and Parametric Polymorphism. In *Information Processing*.

[21] Egbert Rijke, Michael Shulman, and Bas Spitters. 2020. Modalities in homotopy type theory. *Logical Methods in Computer Science* Volume 16, Issue 1 (Jan. 2020). https://doi.org/10.23638/LMCS-16(1:2)2020 arXiv:1706.07526 [math.CT]

[22] Andreas Rossberg, Claudio Russo, and Derek Dreyer. 2014. F-ing modules. *Journal of Functional Programming* 24, 5 (2014), 529–607. https://doi.org/10.1017/S0956796814000264

[23] Jonathan Sterling and Carlo Angiuli. 2021. Normalization for Cubical Type Theory. In *Proceedings of the 36th Annual ACM/IEEE Symposium on Logic in Computer Science*. ACM, New York, NY, USA. arXiv:2101.11479 [cs.LO] To appear.

[24] Jonathan Sterling and Robert Harper. 2021. Logical Relations As Types: Proof-Relevant Parametricity for Program Modules. *J. ACM* (2021). arXiv:2010.08599 [cs.PL] To appear.

[25] Christopher Allen Stone. 2000. *Singleton Kinds and Singleton Types*. Ph.D. Dissertation. Carnegie Mellon University.

[26] Christopher A. Stone and Robert Harper. 2000. Deciding Type Equivalence in a Language with Singleton Kinds. In *Proceedings of the 27th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. Association for Computing Machinery, Boston, MA, USA, 214–227. https://doi.org/10.1145/325694.325724

[27] Christopher A. Stone and Robert Harper. 2006. Extensional equivalence and singleton types. *ACM Transactions on Computational Logic* 7, 4 (2006), 676–722. https://doi.org/10.1145/1183278.1183281

[28] David Swasey, Tom Murphy, Karl Crary, and Robert Harper. 2006. A Separate Compilation Extension to Standard ML. In *Proceedings of the 2006 Workshop on ML (ML '06)*. Association for Computing Machinery, Portland, Oregon, USA, 32–42. https://doi.org/10.1145/1159876.1159883

A SELECTED RULES

A.1 Judgments of φML

We specify **φML** parametrically in a meet semilattice $\mathcal{O}$ of phases, writing $\boxed{\varphi : \mathcal{O}}$ to mean that φ is an element of $\mathcal{O}$. We begin by recapitulating the ordinary judgments of type theory:

1. $\boxed{\Gamma\ \mathit{ctx}}$ means that Γ is a context.
2. $\boxed{\Gamma \vdash A\ \mathit{type}}$ presupposes $\Gamma\ \mathit{ctx}$ and means that A is a type in context Γ.
3. $\boxed{\Gamma \vdash A \equiv B\ \mathit{type}}$ presupposes $\Gamma\ \mathit{ctx}$ and $\Gamma \vdash A, B\ \mathit{type}$, and means that A and B are equal types in context Γ.

To the above, **φML** adds the following forms of judgment that pertain to the structure of phases:

1. $\boxed{\Gamma \vdash \varphi}$ presupposes $\Gamma\ \mathit{ctx}$ and $\varphi : \mathcal{O}$, and means that Γ entails that the φ phase is activated.
2. $\boxed{\Gamma \vdash A\ \text{sealed}\ @\ \varphi}$ presupposes $\Gamma\ \mathit{ctx}$, $\Gamma \vdash A\ \mathit{type}$, and $\varphi : \mathcal{O}$, and means that Γ entails that A is *sealed* at phase φ. Intuitively this means that the type A can expose no information to clients at phase φ, *i.e.* is a singleton type at phase φ.

Contexts in **φML** are totally structural; all the judgments of **φML** specified above are stable under weakening, contraction, and exchange.

A.2 Contexts and phases

To activate a given phase, **φML** has a context extension Γ, φ governed by the following rules:

$$\textsc{cx/emp}\ \frac{}{\cdot\ \mathit{ctx}} \qquad \textsc{cx/var}\ \frac{\Gamma\ \mathit{ctx} \qquad \varphi : \mathcal{O}}{\Gamma, \varphi\ \mathit{ctx}} \qquad \textsc{cx/ph}\ \frac{\Gamma\ \mathit{ctx} \qquad \Gamma \vdash A\ \mathit{type}}{\Gamma, x : A\ \mathit{ctx}} \qquad \textsc{ph/var}\ \frac{\varphi \in \Gamma}{\Gamma \vdash \varphi}$$

We impose rules to make the judgment $\boxed{\Gamma \vdash \varphi}$ preserve meets:

$$\textsc{top/intro}\ \frac{}{\Gamma \vdash \top} \qquad \textsc{meet/intro}\ \frac{\Gamma \vdash \varphi \qquad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi} \qquad \textsc{meet/elim}\ \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi \qquad \Gamma \vdash \psi}$$

Observation A.1. The following monotonicity law is derivable:

$$\textsc{ph/mono}\ \frac{\varphi \leq_{\mathcal{O}} \psi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \psi}$$

Proof. If $\varphi \leq_{\mathcal{O}} \psi$, then $\varphi \wedge \psi = \varphi$; to derive $\Gamma \vdash \psi$ we therefore may apply meet/elim. □

A.3 The phase modality

We include a modality $\varphi \Rightarrow A$ that governs programs that can be written at phase φ; semantically, this *phase modality* is just a dependent function space over the (subsingleton) collection of witnesses that the phase φ is active.

$$\textsc{phmod/formation}\ \frac{\varphi : \mathcal{O} \qquad \Gamma, \varphi \vdash A\ \mathit{type}}{\Gamma \vdash \varphi \Rightarrow A\ \mathit{type}} \qquad \textsc{phmod/intro}\ \frac{\Gamma, \varphi \vdash M : A}{\Gamma \vdash \langle\varphi\rangle M : \varphi \Rightarrow A} \qquad \textsc{phmod/elim}\ \frac{\Gamma \vdash M : \varphi \Rightarrow A \qquad \Gamma \vdash \varphi}{\Gamma \vdash M\ @\ \varphi : A}$$

$$\textsc{phmod/beta}\ \frac{\Gamma, \varphi \vdash M : A \qquad \Gamma \vdash \varphi}{\Gamma \vdash (\langle\varphi\rangle M)\ @\ \varphi \equiv M : A} \qquad \textsc{phmod/eta}\ \frac{\Gamma \vdash M : \varphi \Rightarrow A}{\Gamma \vdash \langle\varphi\rangle(M\ @\ \varphi) \equiv M : \varphi \Rightarrow A}$$

A.4 Structure sharing

To model *structure sharing* from ML languages, **φML** includes a connective $\{A \mid \varphi \hookrightarrow M\}$ that classifies the elements of type A that are equal to M in phase φ.

$$\textsc{sh/formation}\quad \frac{\varphi : \mathcal{O} \qquad \Gamma \vdash A\ \mathit{type} \qquad \Gamma, \varphi \vdash M : A}{\Gamma \vdash \{A \mid \varphi \hookrightarrow M\}\ \mathit{type}}$$

$$\textsc{sh/intro}\quad \frac{\Gamma \vdash M : A \qquad \Gamma, \varphi \vdash M \equiv N : A}{\Gamma \vdash \lfloor M \rfloor : \{A \mid \varphi \hookrightarrow N\}}$$

$$\textsc{sh/elim}\quad \frac{\Gamma \vdash M : \{A \mid \varphi \hookrightarrow N\}}{\Gamma \vdash \lceil M \rceil : A}$$

$$\textsc{sh/elim/bdry}\quad \frac{\Gamma \vdash M : \{A \mid \varphi \hookrightarrow N\} \qquad \Gamma \vdash \varphi}{\Gamma \vdash \lceil M \rceil \equiv N : A}$$

$$\textsc{sh/beta}\quad \frac{\Gamma \vdash M : A \qquad \Gamma, \varphi \vdash M \equiv N : A}{\Gamma \vdash \lceil \lfloor M \rfloor \rceil \equiv M : A}$$

$$\textsc{sh/eta}\quad \frac{\Gamma \vdash M : \{A \mid \varphi \hookrightarrow N\}}{\Gamma \vdash \lfloor \lceil M \rceil \rfloor \equiv M : \{A \mid \varphi \hookrightarrow N\}}$$

Example A.2. Using the top element of the phase lattice, the structure sharing connective can express *singleton* types [2, 3, 25–27]. In particular, given $\Gamma \vdash A\ \mathit{type}$ and $\Gamma \vdash M : A$, we define $\mathcal{S}_A(M) :\equiv \{A \mid \top \hookrightarrow M\}$.

A.5 Judgmental sealing

A type is *sealed* at phase φ when it has exactly one element at that phase and hence can leak no information. This is expressed by the following rules:

$$\textsc{sl/point}\quad \frac{\Gamma \vdash A \text{ sealed @ } \varphi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \star_A : A}$$

$$\textsc{sl/glue}\quad \frac{\Gamma \vdash A \text{ sealed @ } \varphi \qquad \Gamma \vdash \varphi \qquad \Gamma \vdash M : A}{\Gamma \vdash M \equiv \star_A : A}$$

Function types are sealed when their codomains are sealed; product types (including unit, the nullary product) are sealed when all their conjuncts are sealed; structure sharing types are sealed at the phase of their constraint:

$$\textsc{fun/sealed}\quad \frac{\Gamma \vdash A\ \mathit{type} \qquad \Gamma \vdash B \text{ sealed @ } \varphi}{\Gamma \vdash A \to B \text{ sealed @ } \varphi}$$

$$\textsc{unit/sealed}\quad \frac{}{\Gamma \vdash \text{unit sealed @ } \varphi}$$

$$\textsc{prod/sealed}\quad \frac{\Gamma \vdash A, B \text{ sealed @ } \varphi}{\Gamma \vdash A \times B \text{ sealed @ } \varphi}$$

$$\textsc{sh/sealed/1}\quad \frac{\psi : \mathcal{O} \qquad \Gamma \vdash A\ \mathit{type} \qquad \Gamma, \psi \vdash M : A \qquad \Gamma, \varphi \vdash \psi}{\Gamma \vdash \{A \mid \psi \hookrightarrow M\} \text{ sealed @ } \varphi}$$

$$\textsc{sh/sealed/2}\quad \frac{\psi : \mathcal{O} \qquad \Gamma \vdash A\ \mathit{type} \qquad \Gamma, \psi \vdash M : A \qquad \Gamma \vdash A \text{ sealed @ } \varphi}{\Gamma \vdash \{A \mid \psi \hookrightarrow M\} \text{ sealed @ } \varphi}$$

Observation A.3. The following rules are already derivable:

$$\textsc{product point}\quad \frac{\Gamma \vdash A, B \text{ sealed @ } \varphi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \star_{A \times B} \equiv (\star_A, \star_B) : A \times B}$$

$$\textsc{function point}\quad \frac{\Gamma \vdash A\ \mathit{type} \qquad \Gamma \vdash B \text{ sealed @ } \varphi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \star_{A \to B} \equiv \lambda x : A.\star_B : A \to B}$$

A.6 The sealing modality

Not every type is sealed; for instance, the sum type $A + B$ is not sealed even if A and B are both sealed, because a single bit of information can be exposed by case analysis. To seal a non-sealed type, **φML** provides an idempotent modality $[\varphi \setminus A]$ governed by the following rules:

$$\begin{array}{l}\textsc{sl/formation}\\ \dfrac{\varphi : \mathcal{O} \qquad \Gamma \vdash A\ \mathit{type}}{\Gamma \vdash [\varphi \setminus A]\ \mathit{type}}\end{array} \qquad \begin{array}{l}\textsc{sl/sealed/1}\\ \dfrac{\psi : \mathcal{O} \qquad \Gamma \vdash A\ \mathit{type} \qquad \Gamma, \psi \vdash \varphi}{\Gamma \vdash [\psi \setminus A]\ \mathsf{sealed}\ @\ \varphi}\end{array}$$

$$\begin{array}{l}\textsc{sl/sealed/2}\\ \dfrac{\psi : \mathcal{O} \qquad \Gamma \vdash A\ \mathit{type} \qquad \Gamma \vdash A\ \mathsf{sealed}\ @\ \varphi}{\Gamma \vdash [\psi \setminus A]\ \mathsf{sealed}\ @\ \varphi}\end{array} \qquad \begin{array}{l}\textsc{sl/intro}\\ \dfrac{\Gamma \vdash M : A}{\Gamma \vdash \mathsf{seal}_{\varphi}(M) : [\varphi \setminus A]}\end{array}$$

$$\begin{array}{l}\textsc{sl/elim}\\ \dfrac{\Gamma \vdash M : [\varphi \setminus A] \qquad \Gamma \vdash B\ \mathsf{sealed}\ @\ \varphi \qquad \Gamma, x : A \vdash N(x) : B}{\Gamma \vdash x \leftarrow \mathsf{unseal}_{\varphi}(M); N(x) : B}\end{array}$$

$$\begin{array}{l}\textsc{sl/beta}\\ \dfrac{\Gamma \vdash M : A \qquad \Gamma \vdash B\ \mathsf{sealed}\ @\ \varphi \qquad \Gamma, x : A \vdash N(x) : B}{\Gamma \vdash x \leftarrow \mathsf{unseal}_{\varphi}(\mathsf{seal}_{\varphi}(M)); N(x) \equiv N(M) : B}\end{array}$$

$$\begin{array}{l}\textsc{sl/eta}\\ \dfrac{\Gamma \vdash M : [\varphi \setminus A] \qquad \Gamma \vdash B\ \mathsf{sealed}\ @\ \varphi \qquad \Gamma, x : [\varphi \setminus A] \vdash N(x) : B}{\Gamma \vdash N(M) \equiv x \leftarrow \mathsf{unseal}_{\varphi}(M); N(\mathsf{seal}_{\varphi}(x)) : B}\end{array}$$