Tracking Data-Flow with Open Closure Types

Gabriel Scherer[1] and Jan Hoffmann[2]

[1] INRIA Paris-Rocquencourt
[2] Yale University

Abstract. Type systems hide data that is captured by function closures in function types. In most cases this is a beneficial design that enables simplicity and compositionality. However, some applications require explicit information about the data that is captured in closures.
This paper introduces open closure types, that is, function types that are decorated with type contexts. They are used to track data-flow from the environment into the function closure. A simply-typed lambda calculus is used to study the properties of the type theory of open closure types. A distinctive feature of this type theory is that an open closure type of a function can vary in different type contexts. To present an application of the type theory, it is shown that a type derivation establishes a simple non-interference property in the sense of information-flow theory. A publicly available prototype implementation of the system can be used to experiment with type derivations for example programs.

Table of Contents

1 Introduction

Function types in traditional type systems only provide information about the arguments and return values of the functions but not about the data that is captured in function closures. Such function types naturally lead to simple and compositional type systems.

Recently, syntax-directed type systems have been increasingly used to statically verify strong program properties such as resource usage [8,7,6], information flow [5,14], and termination [1,3,2]. In such type systems, it is sometimes necessary and natural to include information in the function types about the data that is captured by closures. To see why, assume that we want to design a type system to verify resource usage. Now consider for example the curried append function for integer lists which has the following type in OCaml.

$$\texttt{append} : \mathit{int\ list} \to \mathit{int\ list} \to \mathit{int\ list}$$

At first glance, we might say that the time complexity of `append` is $O(n)$ if n is the length of the first argument. But a closer inspection of the definition of `append` reveals that this is a gross simplification. In fact, the complexity of the partial function call `app_par = append` ℓ is constant. Moreover, the complexity of the function `app_par` is linear—not in the length of the argument but in the length of the list ℓ that is captured in the function closure.

In general, we have to describe the resource consumption of a curried function $f : A_1 \to \cdots \to A_n \to A$ with n expressions $c_i(a_1, \ldots, a_i)$ such that c_i describes the complexity of the computation that takes place after f is applied to i arguments $a_1, \ldots, a_i$. We are not aware of any existing type system that can verify a statement of this form.

To express the aforementioned statement in a type system, we have to decorate the function types with additional information about the data that is captured in a function closure. It is however not sufficient to directly describe the complexity of a closure in terms of its arguments and the data captured in the closure. Admittedly, this would work to accurately describe the resource usage in our example function `append` because the first argument is directly captured in

the closure. But in general, the data captured in a closure $f a_1 \cdots a_i$ can be any data that is computed from the arguments $a_1, \ldots, a_i$ (and from the data in the environment). To reference this data in the types would not only be meaningless for a user, it would also hamper the compositionality of the type system. It is for instance unclear how to define subtyping for closures that capture different data (which is, e.g., needed in the two branches of a conditional.)

To preserve the compositionality of traditional type systems, we propose to describe the resource usage of a closure as a function of its argument and the data that is visible in the current environment. To this end we introduce *open closure types*, function types that refer to their arguments and to the data in the current environment.

More formally, consider a typing judgment of the form $\Gamma \vdash e : \sigma$, in a type system that tracks fine-grained intensional properties characterizing not only the shape of values, but the behavior of the reduction of e into a value (e.g., resource usage). A typing rule for open closure types, $\Gamma, \Delta \vdash e : [\Gamma'](x{:}\sigma) \to \tau$, captures the idea that, under a weak reduction semantics, the computation of the closure itself, and later the computation of the closure *application*, will have very different behaviors, captured by two different typing environments Γ and Γ' of the same domain, the free variables of e. To describe the complexity of `append`, we might for instance have a statement

$$\ell{:}\mathit{int\ list} \vdash \texttt{append}\ \ell : [\ell{:}\mathit{int\ list}](y{:}\mathit{int\ list}) \to \mathit{int\ list}\ .$$

This puts us in a position to use type annotations to describe the resource usage of `append` ℓ as a function of ℓ and the future argument y. For example, using type-based amortized analysis [6], we can express a bound on the number of created list notes in `append` with the following open closure type.

$$\texttt{append} : []({x{:}\mathit{int\ list}}^0) \to [x{:}{\mathit{int\ list}}^1](y{:}{\mathit{int\ list}}^0) \to {\mathit{int\ list}}^0\ .$$

The intuitive meaning of this type for `append` is as follows. To pay for the cons operations in the evaluation of `append` ℓ_1 we need $0{\cdot}|\ell_1|$ resource units and to pay for the cons operations in the evaluation of `append` $\ell_1\ \ell_2$ we need $0{\cdot}|\ell_1| + 1{\cdot}|\ell_2|$ resource units.

The development of a type system for open closure types entails some interesting technical challenges: term variables now appear in types, which requires mechanisms for scope management not unlike dependent type theories. If x appears in σ, the context $\Gamma, x{:}\tau, y{:}\sigma$ is not exchangeable with $\Gamma, y{:}\sigma, x{:}\tau$. Similarly, the judgment $\Gamma, x{:}\tau \vdash e_2 : \sigma$ will not entail $\Gamma \vdash \texttt{let}\, x = e_1\, \texttt{in}\, e_2 : \sigma$, as the return type σ may contain open closures scoping over x, so we need to substitute variables in types.

The main contribution of this paper is a type theory of open closure types and the proof of its main properties. We start from the simply-typed lambda calculus, and consider the simple intensional property of data-flow tracking, annotating each simply-typed lambda-calculus type with a single boolean variable. This allows us to study the metatheory of open closure types in clean and straightforward way. This is the first important step for using such types in more sophisticated type systems for resource usage and termination.

Our type system for data-flow tracking captures higher-order data-flow information. As a byproduct, we get our secondary contribution, a non-interference property in the sense of information flow theory: high-level inputs do not influence the (low-level) results of computations.

To experiment with of our type system, we implemented a software prototype in OCaml (see Section 5).

Related Work In our type system we maintain the invariant that open closure types only refer to variables that are present in the current typing context. This is a feature that distinguishes open closure types from existing formalisms for closure types.

Contextual types [11,13,15] also decorate types with context information. However, it is not necessary in contextual modal type theory that the context that is captured in a type is related to the current context. Furthermore, our goal of describing properties that may depend on previous function arguments and other visible variables is quite different from the main applications of contextual types in programming language support for manipulating proof terms and meta-variables.

Having closure types carry a set of captured variables has been done in the literature, as for example in Leroy [9], which use closure types to keep track of of *dangerous type variables* that can not be generalized without breaking type safety, or in the higher-order lifetime analysis of Hannan et al. [4], where variable sets denote variables that must be kept in memory. However, these works have no need to vary function types in different typing contexts and subtyping can be defined using set inclusion, which makes the metatheory significantly simpler. On the contrary, our scoping mechanism allows to study more complex properties, such as value dependencies and non-interference.

The classical way to understand value capture in closures in a typed way is through the *typed closure conversion* of Minamide et al. [10]. They use existential types to account for hidden data in function closures without losing compositionality, by abstracting over the difference between functions capturing from different environments. Our system retains this compositionality, albeit in a less apparent way: we get finer-grained information about the dependency of a closure on the ambient typing environment. Typed closure conversion is still possible, and could be typed in a more precise way, abstracting only over values that are outside the lexical context.

Petricek et al. [12] study *coeffects* systems with judgments of the form $C^r\Gamma \vdash e : \tau$ and function types $C^s\sigma \to \tau$, where r and s are coeffect annotations over a indexed comonad C. Their work is orthogonal to the present one as they cover very different topics: on one side, the comonadic semantics structure of coarse-grained effect indexes, and on the other the syntactic scoping rules that arise from tracking each variable of the context separately. We believe that our dependency of types on term variables would make a semantic study significantly more challenging, and conversely that use cases of open closure types are not in general characterized by a comonadic structure.

The non-interference property that we prove is different from the usual treatment in type systems for information flow like the SLam Calculus [5]. In SLam, the information flow into closure is accounted for at abstraction time. In contrast, we account for the information flow into the closure at application time.

2 A Type System for Open Closures

We define a type system for the simplest problem domain that exhibits a need for open closure types. Our goal is to determine statically, for an open term e, on which variables of the environment the value of e depends.

We are interested in weak reduction, and assume a call-by-value reduction strategy. In this context, an abstraction $\lambda x.e$ is already a value, so reducing it does not depend on the environment at all. More generally, for a term e evaluating to a function (closure), we make a distinction between the part of the environment the reduction of e depends on, and the part that will be used when the resulting closure will be applied. For example, the term $(y, \lambda x.z)$ depends on the variable y at evaluation time, but will not need the variable z until the closure in the right pair component is applied.

This is where we need open closure types. Our function types are of the form $[\Gamma^\Phi](x{:}\sigma^\phi) \to \tau$, where the mapping Φ from variables to Booleans indicates on which variables the evaluation depends at application time. The Boolean ϕ indicates whether the argument x is used in the function body. We call Φ the dependency annotation of Γ. Our previous example would for instance be typed as follows.

$$y{:}\sigma^1, z{:}\tau^0 \vdash (y, \lambda x.z) : \sigma * ([y{:}\sigma^0, z{:}\tau^1](x{:}\rho^0) \to \tau)$$

The typing expresses that the result of the computation depends on the variable y but not on the variable z. Moreover, result of the function in the second component of the pair depends on z but not on y.

In general, types are defined by the following grammar.

$$\begin{array}{lll} \texttt{Types} \ni \sigma, \tau, \rho ::= & & \text{types} \\ \quad | & \alpha & \text{atoms} \\ \quad | & \tau_1 * \tau_2 & \text{products} \\ \quad | & [\Gamma^\Phi](x{:}\sigma^\phi) \to \tau & \text{closures} \end{array}$$

The closure type $[\Gamma^\Phi](x{:}\sigma^\phi) \to \tau$ binds the new argument variable x, but not the variables occurring in Γ which are reference variables bound in the current typing context. Such a type is *well-scoped* only when all the variables it closes over are actually present in the current context. In particular, it has no meaning in an empty context, unless Γ is itself empty.

We define well-scoping judgments on contexts ($\Gamma \vdash$) and types ($\Gamma \vdash \sigma$). The judgments are defined simultaneously in Figure 1 and refer to each another. They use non-annotated contexts: the dependency annotations characterize data-flow information of *terms*, and are not needed to state the well-formedness of static types and contexts.

$$\textsc{Scope-Context-Nil}\quad \emptyset \vdash \qquad \textsc{Scope-Context}\quad \frac{\Gamma \vdash \sigma}{\Gamma, x{:}\sigma \vdash}$$

$$\textsc{Scope-Atom}\quad \frac{\Gamma \vdash}{\Gamma \vdash \alpha} \qquad \textsc{Scope-Product}\quad \frac{\Gamma \vdash \tau_1 \qquad \Gamma \vdash \tau_2}{\Gamma \vdash \tau_1 * \tau_2}$$

$$\textsc{Scope-Closure}\quad \frac{\Gamma_0, \Gamma_1 \vdash \qquad \Gamma_0 \vdash \sigma \qquad \Gamma_0, x{:}\sigma \vdash \tau}{\Gamma_0, \Gamma_1 \vdash [\Gamma_0^\Phi](x{:}\sigma^\phi) \to \tau}$$

Fig. 1: Well-scoping of types and contexts

Notice that the closure contexts appearing in the return type of a closure, τ in our rule Scope-Closure, may capture the variable x corresponding to the function argument, which is why we chose the dependent-arrow–like notation $(x{:}\sigma) \to \tau$ rather than only $\sigma \to \tau$. There is no dependency of types on terms in this system, this is only used for scope tracking.

Note that $\Gamma \vdash \sigma$ implies $\Gamma \vdash$ (as proved by direct induction until an atom or a function closure is reached). Note also that a context type $[\Gamma_0](x{:}\sigma) \to \tau$ is well-scoped in any larger environment Γ_0, Γ_1: the context information may only mention variables existing in the typing context, but it need not mention all of them. As a result, well-scoping is preserved by context extension: if $\Gamma_0 \vdash \sigma$ and $\Gamma_0, \Gamma_1 \vdash$, then $\Gamma_0, \Gamma_1 \vdash \sigma$.

A Term Language, and a Naive Attempt at a Type System Our term language, is the lambda calculus with pairs, let bindings and fixpoints. This language is sufficient to discuss the most interesting problems that arise in an application of closure types in a more realistic language.

$\texttt{Terms} \ni t, u, e ::=$		terms
$\mid$	x	variables
$\mid$	(e_1, e_2)	pairs
$\mid$	$\pi_i(e)$	projections $(i \in \{1, 2\})$
$\mid$	$\lambda x.e$	lambda abstractions
$\mid$	$t\ u$	applications
$\mid$	$\texttt{let}\, x = e_1\, \texttt{in}\, e_2$	let declarations

For didactic purposes, we start with an intuitive type system presented in Figure 2. The judgment $\Gamma^\Phi \vdash e : \sigma$ means that the expression e has type σ, in the context Γ carrying the intensional information Φ. Context variable mapped to 0 in Φ are not used during the reduction of e to a value. We will show that the rules App-Tmp and Let-Tmp are not correct, and introduce a new judgment to develop correct versions of the rules.

In a judgment $\Gamma^0 \vdash \lambda x.t : [\Gamma^\Phi](x{:}\sigma^0) \to \tau$, Γ is bound only in one place (the context), and α-renaming any of its variable necessitates a mirroring change in its right-hand-side occurrences (Γ^Φ but also in σ and τ), while x is independently bound in the term and in the type, so the aforementioned type is equivalent to $[\Gamma^\Phi](y{:}\sigma) \to \tau[y/x]$. In particular, variables occurring in types do *not* reveal implementation details of the underlying term.

$$\textsc{Var}\ \frac{}{\Gamma, x{:}\sigma, \Delta \vdash}{\Gamma^0, x{:}\sigma^1, \Delta^0 \vdash x : \sigma} \qquad \textsc{Product}\ \frac{\Gamma^{\Phi_1} \vdash e_1 : \tau_1 \qquad \Gamma^{\Phi_2} \vdash e_2 : \tau_2}{\Gamma^{\Phi_1+\Phi_2} \vdash (e_1, e_2) : \tau_1 * \tau_2} \qquad \textsc{Proj}\ \frac{\Gamma^{\Phi} \vdash e : \tau_1 * \tau_2}{\Gamma^{\Phi} \vdash \pi_i(e) : \tau_i}$$

$$\textsc{Lam}\ \frac{\Gamma^{\Phi}, x{:}\sigma^{\phi} \vdash t : \tau}{\Gamma^0 \vdash \lambda x.t : [\Gamma^{\Phi}](x{:}\sigma^{\phi}) \to \tau} \qquad \textsc{Fix}\ \frac{\Gamma^{\Phi}, f{:}([\Gamma^{\Psi}](x{:}\sigma^{\phi}) \to \tau)^{\chi}, x : \sigma^{\phi} \vdash e : \tau}{\Gamma^0 \vdash \mathtt{fix}\, f\, x.e : [\Gamma^{\Psi}](x{:}\sigma^{\phi}) \to \tau}$$

$$\textsc{App-Tmp}\ \frac{(\Gamma_0, \Gamma_1)^{\Phi_{\mathsf{fun}}} \vdash t : [\Gamma_0^{\Phi_{\mathsf{clos}}}](x{:}\sigma^{\phi}) \to \tau \qquad (\Gamma_0, \Gamma_1)^{\Phi_{\mathsf{arg}}} \vdash u : \sigma}{(\Gamma_0, \Gamma_1)^{\Phi_{\mathsf{fun}}+\Phi_{\mathsf{clos}}+\phi.\Phi_{\mathsf{arg}}} \vdash t\ u : \tau} \qquad \textsc{Let-Tmp}\ \frac{\Gamma^{\Phi_{\mathsf{def}}} \vdash e_1 : \sigma \qquad \Gamma^{\Phi_{\mathsf{body}}}, x{:}\sigma^{\phi} \vdash e_2 : \tau}{\Gamma^{\phi.\Phi_{\mathsf{def}}+\Phi_{\mathsf{body}}} \vdash \mathtt{let}\, x = e_1\, \mathtt{in}\, e_2 : \tau}$$

Fig. 2: Naive rules for the type system

The syntax $\phi.\Phi$ used in the App-Tmp and Let-Tmp rules is a product, or conjunction, of the single boolean dependency annotation ϕ, and of the vector dependency annotation Φ. The sum $\Phi_1 + \Phi_2$ is the disjunction. In the Let-Tmp rule for example, if the typing of e_2 determines that the evaluation of e_2 does not depend on the definition $x = e_1$ (ϕ is 0), then $\phi.\Phi_{\mathsf{def}}$ will mark all the variables used by e_1 as not needed as well (all 0), and only the variables needed by e_2 will be marked in the result annotation $\phi.\Phi_{\mathsf{def}} + \Phi_{\mathsf{body}}$.

In the introduction we present closure types of the form $[\Gamma](x{:}\sigma) \to \tau$, while we here use the apparently different form $[\Gamma^{\Phi}](x{:}\sigma^{\phi}) \to \tau$. This new syntax is actually a simpler special case of the previous one: we could consider a type grammar of the form σ^{ϕ}, and the type $[\Gamma](x{:}\sigma) \to \tau$ would then capture all the needed information, as each type in Γ would come with its own annotation. Instead, we don't embed dependency information in the types directly, and use annotated context Γ^{Φ} to carry equivalent information. This simplification makes it easier to control the scoping correctness: it is easier to notice that Γ^{Φ} and Γ^{Ψ} are contexts ranging over the same domain than if we wrote Γ and Γ'. It is made possible by two specific aspects of this simple system:

- Our intensional information has a very simple structure, only a boolean, that does not apply to the types in depth. The simplification would not work, for example, in a security type system where products could have components of different security levels ($\tau^l * \sigma^r$), but the structure of the rules would remain the same.
- In this example, we are interested mostly in intensional information on the contexts, rather than the return type of a judgment. The general case rather suggests a judgment of the form $\Gamma^{\Phi} \vdash e : \sigma^{\phi}$, but with only boolean annotations this boils to a judgment $\Gamma^{\Phi} \vdash e : \sigma^1$, when we are interested in the value being type-checked, and a trivial judgment $\Gamma^0 \vdash e : \sigma^0$, used to type-check terms that will not be used in the rest of the computation, and which degenerates to a check in the simply-typed lambda-calculus. Instead, we define a single judgment $\Gamma^{\Phi} \vdash e : \sigma$ corresponding to the case where ϕ is 1, and use the notation $\phi.\Phi$ to nullify the dependency information coming of from e when the outer computation does not actually depend on it (ϕ is 0).

While dependency annotations make the development easier to follow, they do not affect the generality of the type theory, as the common denominator of open closure type systems is more concerned with the scoping of closure contexts than the structure of the intensional information itself.

Maintaining Closure Contexts As pointed out, the rule App-Tmp and Let-Tmp of the system above are wrong (hence the "temporary" name): the left-hand-side of the rule App-Tmp assumes that the closure captures the same environment Γ that it is computed in. This property is initially true in the closure of the rule Lam, but is not preserved by Let-Tmp (for the body type) or App-Tmp (for the return type). This means that the intensional information in a type may become stale, mentioning variables that have been removed from the context. We will now fix the type system to never mention unbound variables.

We need a *closure substitution mechanism* to explain the type $\tau_f = [\Gamma^\Phi, y{:}\rho^\chi](x{:}\sigma^\phi) \to \tau^\psi$ of a closure f in the smaller environment Γ, given dependency information for y in Γ. Assume for example that y was bound in a let binding $\texttt{let}\ y = e \ldots$ and that the type τ_f leaves the scope of y. Then we have to adapt the type rules to express the following. "If f depends on y (at application time) then f depends on the variables of Γ that e depends on."

We define in Figure 3 the judgment $\Gamma, y{:}\rho, \Delta \vdash \sigma \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta' \vdash \tau$. Assuming that the variable y in the context $\Gamma, y{:}\rho, \Delta$ was let-bound to an definition with usage information Γ^Ψ, this judgment transforms any type σ in this context in a type τ in a context Γ, Δ' that does not mention y anymore. Note that Δ and Δ' have the same domain, only their intensional information changed: any mention of y in a closure type of Δ was removed in Δ'. Also note that $\Gamma, y{:}\rho, \Delta$ and Γ, Δ', or σ and τ, are not annotated with dependency annotations themselves: this is only a scoping transformation that depends on the dependency annotations of y *in the closures* of σ and Δ.

As for the scope-checking judgment, we simultaneously define the substitutions on contexts themselves $\Gamma, y{:}\rho, \Delta \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta'$. There are two rules for substituting a closure type. If the variable being substituted is not part of the closure type context (rule Subst-Closure-Notin), this closure type is unchanged. Otherwise (rule Subst-Closure) the substitution is performed in the closure type, and the neededness annotation for y is reported to its definition context Γ_0.

The following lemma verifies that this substitution preserves well-scoping of contexts and types.

Lemma 1 (Substitution preserves scoping). *If* $\Gamma, y{:}\rho, \Delta \vdash$ *and* $\Gamma, y{:}\rho, \Delta \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta'$ *hold, then* $\Gamma, \Delta' \vdash$ *holds. If* $\Gamma, y{:}\rho, \Delta \vdash \sigma$ *and* $\Gamma, y{:}\rho, \Delta \vdash \sigma \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta' \vdash \tau$ *hold, then* $\Gamma, \Delta' \vdash \tau$ *holds.*

Proof. By mutual induction on the judgments $\Gamma, y{:}\rho, \Delta \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta'$ and $\Gamma, y{:}\rho, \Delta \vdash \sigma \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta' \vdash \tau$.

$$\textsc{Subst-Context-Nil}\quad \Gamma, y{:}\rho, \emptyset \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma$$

$$\textsc{Subst-Context}\quad \frac{\Gamma, y{:}\rho, \Delta \vdash \sigma \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta' \vdash \tau}{\Gamma, y{:}\rho, \Delta, x{:}\sigma \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta', x{:}\tau}$$

$$\textsc{Subst-Atom}\quad \frac{\Gamma, y{:}\rho, \Delta \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta'}{\Gamma, y{:}\rho, \Delta \vdash \alpha \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta' \vdash \alpha}$$

$$\textsc{Subst-Product}\quad \frac{\Gamma, y{:}\rho, \Delta \vdash \sigma_1 \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta' \vdash \tau_1 \qquad \Gamma, y{:}\rho, \Delta \vdash \sigma_2 \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta' \vdash \tau_2}{\Gamma, y{:}\rho, \Delta \vdash \sigma_1 * \sigma_2 \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta' \vdash \tau_1 * \tau_2}$$

$$\textsc{Subst-Closure-Notin}\quad \frac{\Gamma_0, \Gamma_1, y{:}\rho, \Delta \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma_0, \Gamma_1, \Delta'}{\Gamma_0, \Gamma_1, y{:}\rho, \Delta \vdash [\Gamma_0^{\Phi}](x{:}\sigma_1^{\phi}) \to \sigma_2 \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma_0, \Gamma_1, \Delta' \vdash [\Gamma_0^{\Phi}](x{:}\sigma_1^{\phi}) \to \sigma_2}$$

$$\textsc{Subst-Closure}\quad \frac{\begin{array}{c}\Gamma, y{:}\rho, \Delta, \Gamma_1 \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta', \Gamma_1' \\ \Gamma, y{:}\rho, \Delta \vdash \sigma_1 \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta' \vdash \sigma_1 \qquad \Gamma, y{:}\rho, \Delta, x{:}\sigma_1 \vdash \sigma_2 \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta', x{:}\sigma_1 \vdash \tau_2\end{array}}{\Gamma, y{:}\rho, \Delta, \Gamma_1 \vdash [\Gamma^{\Phi_1}, y{:}\rho^{\chi}, \Delta^{\Phi_2}](x{:}\sigma_1^{\phi}) \to \sigma_2 \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta', \Gamma_1' \vdash [\Gamma^{\Phi_1 + \chi.\Psi}, \Delta'^{\Phi_2}](x{:}\sigma_1^{\phi}) \to \tau_2}$$

Fig. 3: Type substitution

Case Subst-Context-Nil: using Scope-Context-Nil, $\Gamma, x{:}\sigma \vdash$ implies $\Gamma \vdash \sigma$, which in turn implies $\Gamma \vdash$.

Case Subst-Context: from our hypothesis $\Gamma, y{:}\rho, \Delta, x{:}\sigma \vdash$ we deduce $\Gamma, y{:}\rho, \Delta \vdash \sigma$. By induction we can deduce $\Gamma, \Delta' \vdash \tau$, which gives context well-formedness $\Gamma, \Delta' \vdash$.

Case Subst-Atom: direct by Scope-Atom and induction hypothesis.

Case Subst-Product: by inversion, the last rule of the derivation of $\Gamma, y{:}\rho \vdash (\sigma_1 * \sigma_2)$ is Scope-Product, so we can proceed by direct induction on the premises of both judgments.

Case Subst-Closure: Using our induction hypothesis on $\Gamma, y{:}\rho, \Delta, \Gamma_1 \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, \Delta', \Gamma_1'$ we can deduce that $\Gamma, \Delta', \Gamma_1' \vdash$ and in particular $\Gamma, \Delta' \vdash$.

By inversion, the last rule of the derivation of $\Gamma, y{:}\rho, \Delta, \Gamma_1 \vdash [\Gamma^{\Phi_1}, y{:}\rho^{\chi}, \Delta^{\Phi_2}](y : \sigma_1^{\phi_1}) \to \sigma_2$ is Scope-Closure. Its premises are $\Gamma, y{:}\rho, \Delta \vdash \sigma_1$ and $\Gamma, y{:}\rho, \Delta, x{:}\sigma_1 \vdash \sigma_2$, from which we deduce by induction hypothesis $\Gamma, \Delta' \vdash \tau_1$ and $\Gamma, \Delta', x{:}\tau_1 \vdash \tau_2$ respectively, allowing to deduce that $\Gamma, \Delta' \vdash [\Gamma^{\Phi_1 + \chi.\Psi}, \Delta'^{\Phi_2}](x : \tau_1) \to \tau_2$, which allows to conclude by weakening with the well-scoped Γ_1'.

Case Subst-Closure-Notin: direct by induction and inversion.

□

We can now give the correct rules for binders:

$$\textsc{Let}\quad \frac{\Gamma^{\Phi_{\mathsf{def}}} \vdash e_1 : \sigma \qquad \Gamma^{\Phi_{\mathsf{body}}}, x{:}\sigma^{\phi} \vdash e_2 : \tau \qquad \Gamma, x{:}\sigma \vdash \tau \overset{x \setminus \Phi_{\mathsf{def}}}{\rightsquigarrow} \Gamma \vdash \tau'}{\Gamma^{\phi.\Phi_{\mathsf{def}} + \Phi_{\mathsf{body}}} \vdash \mathtt{let}\, x = e_1\, \mathtt{in}\, e_2 : \tau'}$$

$$\textsc{App}\quad \frac{\begin{array}{c}(\Gamma_0, \Gamma_1)^{\Phi_{\mathsf{fun}}} \vdash t : [\Gamma_0^{\Phi_{\mathsf{clos}}}](x{:}\sigma^{\phi}) \to \tau \\ (\Gamma_0, \Gamma_1)^{\Phi_{\mathsf{arg}}} \vdash u : \sigma \qquad \Gamma_0, \Gamma_1, x{:}\sigma \vdash \tau \overset{x \setminus \Phi_{\mathsf{arg}}}{\rightsquigarrow} \Gamma_0, \Gamma_1 \vdash \tau'\end{array}}{(\Gamma_0, \Gamma_1)^{\Phi_{\mathsf{fun}} + \Phi_{\mathsf{clos}} + \phi.\Phi_{\mathsf{arg}}} \vdash t\ u : \tau'}$$

Lemma 2 (Typing respects scoping). *If $\Gamma \vdash t : \sigma$ holds, then $\Gamma \vdash \sigma$ holds.*

This lemma guarantees that we fixed the problem of stale intensional information: types appearing in the typing judgment are always well-scoped.

Proof. By induction on the derivation of $\Gamma \vdash t : \sigma$.

Case Var: from the premise $\Gamma^0, x : \sigma^1, \Delta^0 \vdash$ we have $\Gamma \vdash \sigma$.
Case Prod: direct by induction.
Case Proj: the induction hypothesis is $\Gamma \vdash \tau_1 * \tau_2$, from which we get $\Gamma \vdash \tau_i$ (for $i \in \{1, 2\}$) by inversion.
Case Lam: the induction hypothesis is $\Gamma, x{:}\sigma \vdash \tau$. From this we get $\Gamma, x{:}\sigma$ and therefore $\Gamma \vdash \sigma$, which allows to conclude with Scope-Closure.
Case Fix: the hypothesis implies $\Gamma, f{:}[\Gamma^{\Psi}](x{:}\sigma^{\phi}) \to \tau \vdash$, which in turn implies $\Gamma \vdash [\Gamma^{\Psi}](x{:}\sigma^{\phi}) \to \tau$.
Case App: Using our induction hypothesis on the first premise give us that $\Gamma_0, \Gamma_1 \vdash [\Gamma_0^{\Phi_{\mathsf{clos}}}](x{:}\sigma) \to \tau$, so by inversion $\Gamma_0, \Gamma_1 \vdash$ and $\Gamma_0, x{:}\sigma \vdash \tau$. The latter fact can be weakened into $\Gamma_0, \Gamma_1, x{:}\sigma \vdash \tau$, and then combined with the last premise $\Gamma_0, \Gamma_1, x{:}\sigma \vdash \tau \overset{x \setminus \Phi_{\mathsf{arg}}}{\rightsquigarrow} \Gamma_0, \Gamma_1 \vdash \tau'$ and Lemma 1 to get our goal $\Gamma_0, \Gamma_1 \vdash \tau'$.
Case Let: reasoning similar to the App case. By induction on the middle premise, we have $\Gamma, x{:}\sigma \vdash \tau$, combined with the right premise $\Gamma, x{:}\sigma \vdash \tau \overset{x \setminus \Phi_{\mathsf{def}}}{\rightsquigarrow} \Gamma \vdash \tau'$ we get $\Gamma \vdash \tau'$.

□

It is handy to introduce a convenient derived notation $\Gamma^{\Phi} \vdash \tau \overset{y \setminus \Psi}{\rightsquigarrow} \Gamma'^{\Phi'} \vdash \tau'$ that is defined below. This substitution relation does not only remove y from the open closure types in Γ, it also updates the dependency annotation on Γ to add the dependency Ψ, corresponding to all the variables that y depended on – if it is itself marked as needed.

$$\frac{\Gamma, y{:}\rho, \Delta \vdash \tau \overset{y \setminus \Psi}{\rightsquigarrow} \Gamma, \Delta' \vdash \tau'}{\Gamma^{\Phi_1}, y{:}\rho^{\chi}, \Delta^{\Phi_2} \vdash \tau \overset{y \setminus \Psi}{\rightsquigarrow} \Gamma^{\Phi_1 + \chi.\Psi}, \Delta'^{\Phi_2} \vdash \tau'}$$

It is interesting to see that substituting y away in $\Gamma^{\Phi_1}, y{:}\rho, \Delta^{\Phi_2}$ changes the annotation on Γ, but not its types (Γ is unchanged in the output as its types

may not depend on y), while it changes the types in Δ but not its annotation (Φ_2 is unchanged in the output as a value for y may only depend on variables from Γ, not Δ).

The following technical results allow us to permute substitutions on unrelated variables. They will be used in the typing soundness proof of the next section (Theorem 1).

Lemma 3 (Confluence). *If* $\Gamma_1 \vdash \tau_1 \overset{x_a \backslash \Psi_a}{\rightsquigarrow} \Gamma_{2a} \vdash \tau_{2a}$ *and* $\Gamma_1 \vdash \tau_1 \overset{x_b \backslash \Psi_b}{\rightsquigarrow} \Gamma_{2b} \vdash \tau_{2b}$ *then there exists a unique* $\Gamma_3 \vdash \tau_3$ *such that*

$$\Gamma_{2a} \vdash \tau_{2a} \overset{x_b \backslash (\Psi_b + \Psi_a.\Psi_b(x_a))}{\rightsquigarrow} \Gamma_3 \vdash \tau_3 \qquad \textit{and} \qquad \Gamma_{2b} \vdash \tau_{2b} \overset{x_a \backslash (\Psi_a + \Psi_b.\Psi_a(x_b))}{\rightsquigarrow} \Gamma_3 \vdash \tau_3$$

Proof. Without loss of generality we can assume that x_a appears before x_b in Γ_1, so in particular $\Psi_a(x_b) = 0$. For any subcontext of the form

$$\Delta_1{}^{\Psi_1}, x_a{:}\sigma_a{}^{\rho_a}, \Delta_2{}^{\Psi_2}, x_b{:}\sigma_b{}^{\rho_b}$$

, assume that substituting Ψ_a for x_a first results in

$$\Delta_1{}^{\Psi_1 + \rho_a.\Psi_a}, \Delta_{2a}{}^{\Psi_2}, x_b{:}\sigma_{ba}{}^{\rho_b}$$

, while substituting Ψ_b for x_b first results in

$$\Delta_1{}^{\Psi_1 + \rho_b.\Psi_b(\Delta_1)}, x_a{:}\sigma_a{}^{\rho_a + \rho_b.\Psi_b(x_a)}, \Delta_2{}^{\Psi_2 + \rho_b.\Psi_b(\Delta_2)}$$

. Substituting $\Psi_b + \Psi_a.\Psi_b(x_a)$ for x_b in

$$\Delta_1{}^{\Psi_1 + \rho_a.\Psi_a}, \Delta_{2a}{}^{\Psi_2}, x_b{:}\sigma_{ba}{}^{\rho_b}$$

results in

$$\Delta_1{}^{\Psi_1 + \rho_a.\Psi_a + \rho_b.(\Psi_b + \Psi_a.\Psi_b(x_a))(\Delta_1)}, \Delta_{2a}{}^{\Psi_2 + \rho_b.(\Psi_b + \Psi_a.\Psi_b(x_a))(\Delta_{2a})}$$

which simplifies to

$$\Delta_1{}^{\Psi_1 + \rho_a.\Psi_a + \rho_b.\Psi_b(\Delta_1) + \rho_b.\Psi_b(x_a).\Psi_a}, \Delta_{2a}{}^{\Psi_2 + \rho_b.\Psi_b(\Delta_{2a})}$$

Substituting $\Psi_a + \Psi_b.\Psi_a(x_b) = \Psi_a$ for x_a in

$$\Delta_1{}^{\Psi_1 + \rho_b.\Psi_b(\Delta_1)}, x_a{:}\sigma_a{}^{\rho_a + \rho_b.\Psi_b(x_a)}, \Delta_2{}^{\Psi_2 + \rho_b.\Psi_b(\Delta_2)}$$

results in

$$\Delta_1{}^{\Psi_1 + \rho_b.\Psi_b(\Delta_1) + (\rho_a + \rho_b.\Psi_b(x_a)).\Psi_a}, \Delta_{2a}{}^{\Psi_2 + \rho_b.\Psi_b(\Delta_2)}$$

which simplifies to

$$\Delta_1{}^{\Psi_1 + \rho_b.\Psi_b(\Delta_1) + \rho_a.\Psi_a + \rho_b.\Psi_b(x_a).\Psi_a}, \Delta_{2a}{}^{\Psi_2 + \rho_b.\Psi_b(\Delta_2)}$$

Given that Δ_2 and Δ_{2a} have the same domain (only different types), the restrictions $\Psi_b(\Delta_2)$ and $\Psi_b(\Delta_{2a})$ are equal, allowing to conclude that the two substitutions indeed end in the same sequent

$$\Delta_1{}^{\Psi_1 + (\rho_a + \rho_b.\Psi_b(x_a)).\Psi_a + \rho_b.\Psi_b(\Delta_1)}, \Delta_{2a}{}^{\Psi_2 + \rho_b.\Psi_b(\Delta_2)}$$

Note that we can make sense, informally, of this resulting sequent. The variable used by this final contexts are

- the variables used of Δ_1 used in the initial judgment (Ψ_1)
- the variables of Δ_2 (updated in Δ_{2a} to remove references to the substituted variable x_a) used in the initial judgment (Ψ_2)
- the variables used by Ψ_b, if it is used (ρ_b is 1)
- the variables used by Ψ_a if either x was used (ρ_a is 1), or if x_b is used (ρ_b is 1) and itself uses x_a ($\Psi_b(x_a)$ is 1).

To get this intuition, we considered again the annotations as booleans, but note that the equivalence proof was done in a purely algebraic manner. It should therefore be preserved in future work where the intensional information has a richer structure.

□

Corollary 1 (Reordering of substitutions). *If Ψ_a and Ψ_b have domain Γ, and*

$$\Gamma_1{}^{\Phi_1} \vdash \tau_1 \overset{x_a \backslash \Psi_a}{\rightsquigarrow} \Gamma_2{}^{\Phi_2} \vdash \tau_2 \overset{x_b \backslash (\Psi_b + \Psi_b(x_a).\Psi_a)}{\rightsquigarrow} \Gamma_3{}^{\Phi_3} \vdash \tau_3$$

then there exists $\Gamma'_2{}^{\Phi'_2} \vdash \tau'_2$ such that

$$\Gamma_1{}^{\Phi_1} \vdash \tau_1 \overset{x_b \backslash \Psi_b}{\rightsquigarrow} \Gamma'_2{}^{\Phi'_2} \vdash \tau'_2 \overset{x_a \backslash (\Psi_a + \Psi_a(x_b).\Psi_b)}{\rightsquigarrow} \Gamma_3{}^{\Phi_3} \vdash \tau_3$$

On open closure types on the left of function types Note that the Subst-Closure handles the function type on the left-hand-side of the arrow, σ_1, is a specific and subtle way: it must be unchanged by the substitution judgment. Under a slightly simplified form, the judgment reads:

$$\frac{\Gamma, y{:}\rho, \Delta \vdash \sigma_1 \overset{y \backslash \Psi}{\rightsquigarrow} \Gamma, \Delta' \vdash \sigma_1 \qquad \Gamma, y{:}\rho, \Delta, x{:}\sigma_1 \vdash \sigma_2 \overset{y \backslash \Psi}{\rightsquigarrow} \Gamma, \Delta', x{:}\sigma_1 \vdash \tau_2}{\Gamma, y{:}\rho, \Delta \vdash [\Gamma^{\Phi_1}, y{:}\rho^{\chi}, \Delta^{\Phi_2}](x{:}\sigma_1^{\phi}) \to \sigma_2 \overset{y \backslash \Psi}{\rightsquigarrow} \Gamma, \Delta' \vdash [\Gamma^{\Phi_1 + \chi.\Psi}, \Delta'^{\Phi_2}](x{:}\sigma_1^{\phi}) \to \tau_2}$$

This corresponds to the usual "change of direction" on the left of arrow type. A substitution $\Gamma, y{:}\rho \vdash \tau \overset{y \backslash \Psi}{\rightsquigarrow} \Gamma \vdash \tau'$ is a lossy transformation, as we forget how y is used in τ and instead mix its definition information with the rest of the context information in τ'. Such a loss makes sense for the return type of a function: we forget information about the return value. But by contravariance of input argument, we should instead *refine* the argument types.

But as the gain or loss or precision correspond to variables going out of scope, such a refinement could only happen in smaller nested scopes. On the contrary, when going out to a wider scope, the only possibility is that the closure type does not depend on the particular variable being substituted (so the type σ is preserved, $\Gamma, y{:}\rho, \Delta \vdash \sigma \overset{y \backslash \Psi}{\rightsquigarrow} \Gamma, \Delta' \vdash \sigma$) . If the variable was used, a loss of precision would be possible: this substitution must be rejected.

Consider the following example:

```
(* in context Γ *)
 let x : int = e_x in
  let y : bool = e_y in
   let f (g : [Γ⁰, x:int¹](z : unit⁰) → int) : int = g () in
   f (λz. x);
   f
```

In the environment $\Gamma, x{:}\texttt{int}, y{:}\texttt{bool}$, the type of `f`'s function argument `g` describes a function whose result depends on `x`. We can still express this dependency when substituting the variable `y` away, that is when considering the type of the expression `(let y = ... in let f g = ... in f)` as a whole: the argument type will still have type $[\Gamma^0, x{:}\texttt{int}^1](z : \texttt{unit}) \to \texttt{int}$. However, this dependency on `x` cannot make sense anymore if we remove `x` itself from the context, the substitution does not preserve this function type. This makes the whole expression `(let x = ... in (let y = ... in let f g = ... in f))` ill-typed, as `x` escapes its scope in the argument function type.

One way to understand this requirement is that there are two parts to having an analysis be fully "higher-order". Fist, it handles programs that take functions as input, and second, it handles programs that return functions as result of computations. Some languages only pass functions as parameters (this is in particular the case of C with pointers to global functions), some constructions such as currying fundamentally rely on function creation with environment capture. Our system proposes a new way to handle this second part, and is intensionally simplistic, to the point of being restrictive, on the rest.

In a non-toy language one would want to add subtyping of context information, that would allow controlled loss of precision to, for example, create lists of functions with slightly different context information. Another useful feature would be context information polymorphism to express functions being parametric with respect to the context information of their argument. This is intentionally left to future work.

3 A Big-Step Operational Semantics

In this section, we will define an operational semantics for our term language, and use it to prove the soundness of the type system (Theorem 1). Our semantics is equivalent to the usual call-by-value big-step reduction semantics for the lambda-calculus in the sense that computation happens at the same time. There is however a notable difference.

Function closures are not built in the same way as they are in classical big-step semantics. Usually, we have a rule of the form $V \vdash \lambda x.t \implies (V, \lambda x.t)$ where the closure for $\lambda x.t$ is a pair of the value environment V (possibly restricted to its subset appearing in t) and the function code. In contrast, we capture no values at closure creation time in our semantics: $V \vdash \lambda x.t \implies (\emptyset, \lambda x.t)$. The captured values will be added to the closure incrementally, during the reduction of binding forms that introduced them in the context.

Consider for example the following two derivations; one in the classic big-step reduction, and the other in our alternative system.

$$\textsc{Classic-Red-Let}\quad \frac{x{:}v \vdash x \overset{c}{\Longrightarrow} v \qquad x{:}v, y{:}v \vdash \lambda z.y \overset{c}{\Longrightarrow} ((x \mapsto v, y \mapsto v), \lambda z.y)}{x{:}v \vdash \mathtt{let}\, y = x\, \mathtt{in}\, \lambda z.y \overset{c}{\Longrightarrow} ((x \mapsto v, y \mapsto v), \lambda z.y)}$$

$$\textsc{Our-Red-Let}\quad \frac{x{:}v \vdash x \implies v \qquad x{:}v, y{:}v \vdash \lambda z.y \implies ([x,y], \emptyset, \lambda z.y) \qquad (\emptyset, \lambda z.y) \overset{y\backslash v}{\rightsquigarrow} ([x], y \mapsto v, \lambda z.y)}{x{:}v \vdash \mathtt{let}\, y = x\, \mathtt{in}\, \lambda z.y \implies ([x], y \mapsto v, \lambda z.y)}$$

Rather than capturing the whole environment in a closure, we store none at all at the beginning (merely record their names), and add values incrementally, just before they get popped from the environment. This is done by the *value substitution* judgment $w \overset{x\backslash v}{\rightsquigarrow} w'$ that we will define in this section. The reason for this choice is that this closely corresponds to our typing rules, value substitution being a runtime counterpart to substitution in types $\Gamma \vdash \sigma \overset{x\backslash \Phi}{\rightsquigarrow} \Gamma' \vdash \sigma'$; this common structure is essential to prove of the type soundness (Theorem 1).

Note that derivations in this modified system and in the original one are in one-to-one mapping. It should not be considered a new dynamic semantics, rather a reformulation that is convenient for our proofs as it mirrors our static judgment structure.

Values and Value Substitution Values are defined as follows.

$\mathtt{Val} \ni v, w ::=$		values
$\mid$	$\mathtt{v}_\alpha$	value of atomic type
$\mid$	(v, w)	value tuples
$\mid$	$([x_j]_{j\in J}, (x_i \mapsto v_i)_{i\in I}, \lambda x.t)$	function closures
$\mid$	$([x_j]_{j\in J}, (x_i \mapsto v_i)_{i\in I}, \mathtt{fix}\, f\, x.t)$	recursive function closures

The set of variables bound in a closure is split into an ordered mapping $(x_i \mapsto v_i)_{i\in I}$ for variables that have been substituted to their value, and a simple list $[x_j]_{j\in J}$ of variables whose value has not yet been captured. They are both binding occurrences of variables bound in t; α-renaming them is correct as long as t is updated as well.

To formulate our type soundness result, we define a typing judgment on values $\Gamma \vdash v : \sigma$ in Figure 4. An intuition for the rule Value-Closure is the following. Internally, the term t has a dependency Γ^Φ on the ambient context, but also dependencies $(\tau_i^{\psi_i})$ on the captured variables. But externally, the type may not mention the captured variables, so it reports a different dependency $\Gamma^{\Phi'}$ that corresponds to the internal dependency Γ^Φ, combined with the dependencies (Ψ_i) of the captured values. Both families $(\psi_i)_{i\in I}$ and $(\Psi_i)_{i\in I}$ are existentially quantified in this rule.

$$\textsc{Value-Atom}\ \frac{\Gamma \vdash}{\Gamma \vdash \mathtt{v}_\alpha : \alpha} \qquad \textsc{Value-Product}\ \frac{\Gamma \vdash v_1 : \tau_1 \qquad \Gamma \vdash v_2 : \tau_2}{\Gamma \vdash (v_1, v_2) : \tau_1 * \tau_2}$$

$$\textsc{Value-Closure}\ \frac{\Gamma, \Gamma_1 \vdash \qquad \forall i \in I,\ \Gamma, (x_j{:}\tau_j)_{j<i} \vdash v_i : \tau_i \qquad \Gamma^\Phi, (x_i{:}\tau_i^{\psi_i})_{i\in I}, x{:}\sigma^\phi \vdash t : \tau \qquad \Gamma^\Phi, (x_i{:}\tau_i^{\psi_i})_{i\in I}, x{:}\sigma^\phi \vdash \tau \overset{(x_i)\backslash(\Psi_i)}{\rightsquigarrow} \Gamma^{\Phi'}, x{:}\sigma^\phi \vdash \tau'}{\Gamma, \Gamma_1 \vdash (\mathrm{dom}\,\Gamma, (x_i \mapsto v_i)_{i\in I}, \lambda x.t) : [\Gamma^{\Phi'}](x{:}\sigma^\phi) \to \tau'}$$

$$\textsc{Value-Closure-Fix}\ \frac{\Gamma, \Gamma_1 \vdash \qquad \forall i \in I,\ \Gamma, (x_j{:}\tau_j)_{j<i} \vdash v_i : \tau_i \qquad \Gamma^\Phi, (x_i{:}\tau_i^{\psi_i})_{i\in I}, f{:}([\Gamma, (x_i{:}\tau_i^{\psi_i})](x{:}\sigma^\phi) \to \tau)^\chi, x{:}\sigma^\phi \vdash t : \tau \qquad \Gamma^\Phi, (x_i{:}\tau_i^{\psi_i})_{i\in I}, x{:}\sigma^\phi \vdash \tau \overset{(x_i)\backslash(\Psi_i)}{\rightsquigarrow} \Gamma^{\Phi'}, x{:}\sigma^\phi \vdash \tau'}{\Gamma, \Gamma_1 \vdash (\mathrm{dom}\,\Gamma, (x_i \mapsto v_i)_{i\in I}, \mathtt{fix}\, f\, x.t) : [\Gamma^{\Phi'}](x{:}\sigma^\phi) \to \tau'}$$

Fig. 4: Value typing

$$\textsc{Subst-Value-Atom}\ \mathtt{v}_\alpha \overset{y\backslash v}{\rightsquigarrow} \mathtt{v}_\alpha \qquad \textsc{Subst-Value-Product}\ \frac{w_1 \overset{y\backslash v}{\rightsquigarrow} w_1' \qquad w_2 \overset{y\backslash v}{\rightsquigarrow} w_2'}{(w_1, w_2) \overset{y\backslash v}{\rightsquigarrow} (w_1', w_2')}$$

$$\textsc{Subst-Value-Closure}\ ([x_{j_1}, \ldots, x_{j_n}, y], (x_i \mapsto w_i)_{i\in I}, t) \overset{y\backslash v}{\rightsquigarrow} ([x_{j_1}, \ldots, x_{j_n}], (y \mapsto v)(x_i \mapsto w_i)_i, t)$$

$$\textsc{Subst-Value-Closure-Notin}\ \frac{y \notin (x_j)_{j\in J}}{([x_j]_{j\in J}, (x_i \mapsto w_i)_{i\in I}, t) \overset{y\backslash v}{\rightsquigarrow} ([x_j]_{j\in J}, (x_i \mapsto w_i)_{i\in I}, t)}$$

Fig. 5: Value substitution

In the judgment rule, the notation $(x_j : \tau_j)_{j<i}$ is meant to define the environment of each $(x_i : \tau_i)$ as Γ^Φ, plus all the $(x_j : \tau_j)$ that come before x_i in the typing judgment $\Gamma^\Phi, (x_i : \tau_i)_{i\in I}, x : \sigma^\phi \vdash t$. The notation $\ldots \overset{(x_i)\backslash(\Psi_i)}{\rightsquigarrow} \ldots$ denotes the sequence of substitutions for all (x_i, Ψ_i), with the rightmost variable (introduced last) substituted first: in our dynamic semantics, values are captured by the closure in the LIFO order in which their binding variables enter and leave the lexical scope.

Substituting Values In the typing rules, we use the substitution relation $\Gamma, y{:}\rho \vdash \sigma \overset{y\backslash\Phi}{\rightsquigarrow} \Gamma \vdash \tau$ to remove the variable y from the closure types in σ. Correspondingly, in our runtime semantics, we *add* the variable y to the vector stored in the closure value, by a value substitution judgment $w \overset{y\backslash v}{\rightsquigarrow} w'$ (see Figure 5) when the binding of y is removed from the evaluation context.

In the Subst-Value-Closure, the notation $, (y \mapsto v)(x_i \mapsto w_i)_i$ means that the binding $y \mapsto v$ is added in first position in the vector of captured values. The values w_i were computed in a context depending on y, so they need to appear after the binding $y \mapsto v$ for the value to be type-correct.

Lemma 4 (Value substitution preserves typing). *If* $(\Gamma \vdash v : \rho)$, $(\Gamma, y{:}\rho \vdash w : \sigma)$, $(\Gamma, y{:}\rho \vdash \sigma \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma \vdash \tau)$ *and* $(w \overset{y\backslash v}{\rightsquigarrow} w')$ *hold, then* $(\Gamma \vdash w' : \tau)$ *holds.*

Note that this theorem is restricted to substitutions of the rightmost variable of the context. While substitution in types needs to operate under binders (in rule Subst-Closure), value substitution is a runtime operation that will only be used by our (weak) reduction relation on the last introduced variable.

Proof. By induction on the value typing judgment $\Gamma, y{:}\rho \vdash w : \sigma$.

Case Value-Atom: by inversion we know that the last rule of $\Gamma, y{:}\rho \vdash \alpha \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma \vdash \tau$ is Subst-Atom. From the premise $\Gamma, y{:}\rho \vdash$ and $\Gamma, y{:}\rho \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma$ we can deduce from Lemma 1 that $\Gamma \vdash$, which allows to conclude $\Gamma \vdash \mathsf{v}_\alpha : \alpha$.

Case Value-Product: by inversion, the last rules of $\Gamma, y{:}\rho \vdash (\sigma_1 * \sigma_2) \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma \vdash \tau$ and $w \overset{y\backslash v}{\rightsquigarrow} w'$ are respectively Subst-Product and Subst-Value-Product, so by induction hypothesis we have $\Gamma \vdash w_1' : \tau_1$ and $\Gamma \vdash w_2' : \tau_2$, which allows us to conclude $\Gamma \vdash (w_1', w_2') : \tau_1 * \tau_2$.

Case Value-Closure. By inversion we know that the last substitution rules applied are either Subst-Closure and Subst-Value-Closure, or Subst-Closure-Notin and Subst-Value-Closure-Notin, depending on whether the substituted variable is part of the closure context.

In the latter case, both the types and the judgments are unchanged, so the result is immediate. If the substituted value is part of the closure context, the rules of the involved judgments are

$$\frac{\Gamma, y{:}\rho \vdash \sigma_1 \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma \vdash \sigma_1 \qquad \Gamma, y{:}\rho, x{:}\sigma_1 \vdash \sigma_2 \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma, x{:}\sigma_1 \vdash \sigma_2'}{\Gamma, y{:}\rho \vdash [\Gamma^{\Phi_1}, y{:}\rho^{\chi}](x{:}\sigma_1^{\phi}) \to \sigma_2 \overset{y\backslash\Psi}{\rightsquigarrow} \Gamma \vdash [\Gamma^{\Phi_1 + \chi.\Psi}](x{:}{\sigma_1}^{\phi}) \to \sigma_2'}$$

$$\frac{\begin{array}{c}\forall i \in I,\ \Gamma, y{:}\rho, (x_j{:}\tau_j)_{j<i} \vdash w_i : \tau_i \qquad \Gamma^{\Phi_1''}, y{:}\rho^{\chi''}, (x_i{:}\tau_i^{\psi_i})_{i\in I}, x{:}{\sigma_1}^{\phi} \vdash t : \sigma_2'' \\ \Gamma^{\Phi_1''}, y{:}\rho^{\chi''}, (x_i{:}\tau_i^{\psi_i})_{i\in I}, x{:}{\sigma_1}^{\phi} \vdash \sigma_2'' \overset{(x_i)\backslash(\Psi_i)}{\rightsquigarrow} \Gamma^{\Phi_1}, y{:}\rho^{\chi}, x{:}{\sigma_1}^{\phi} \vdash \sigma_2\end{array}}{\Gamma, y{:}\rho \vdash (\operatorname{dom}\Gamma, (x_i \mapsto w_i)_{i\in I}, \lambda x.t) : [\Gamma^{\Phi_1}, y{:}\rho^{\chi}](x{:}{\sigma_1}^{\phi}) \to \sigma_2}$$

$$([\operatorname{dom}\Gamma, y], (x_i \mapsto w_i)_{i\in I}, t) \overset{y\backslash v}{\rightsquigarrow} (\operatorname{dom}\Gamma, (y \mapsto v)(x_i \mapsto w_i)_i, t)$$

We can reach our goal by using the following inference rule:

$$\frac{\begin{array}{c}\forall i \in I,\ \Gamma, y{:}\rho, (x_j{:}\tau_j)_{j<i} \vdash w_i : \tau_i \\ \Gamma^{\Phi_1''}, y : \rho^{\chi''}, (x_i{:}{\tau_i}^{\psi_i})_{i\in I}, x{:}{\sigma_1}^{\phi} \vdash t : \sigma_2'' \\ \Gamma^{\Phi_1''}, y{:}\rho^{\chi''}, (x_i{:}\tau_i^{\psi_i})_{i\in I}, x{:}{\sigma_1}^{\phi} \vdash \sigma_2'' \overset{,y(x_i)_i\backslash,\Psi(\Psi_i)_i}{\rightsquigarrow} \Gamma^{\Phi_1+\chi.\Psi}, x{:}{\sigma_1}^{\phi} \vdash \sigma_2'\end{array}}{\Gamma \vdash (\operatorname{dom}\Gamma, , (y \mapsto v)(x_i \mapsto w_i)_{i\in I}, \lambda x.t) : [\Gamma^{\Phi_1+\chi.\Psi}](x{:}{\sigma_1}^{\phi}) \to \sigma_2'}$$

$$\textsc{Red-Var}\quad V \vdash x \implies V(x) \qquad \textsc{Red-Lam}\quad V \vdash \lambda x.t \implies (\mathrm{dom}\, V, \emptyset, \lambda x.t)$$

$$\textsc{Red-Lam-Fix}\quad V \vdash \mathtt{fix}\, f\, x.t \implies (\mathrm{dom}\, V, \emptyset, \mathtt{fix}\, f\, x.t)$$

$$\textsc{Red-Pair}\quad \frac{V \vdash e_1 \implies v_1 \qquad V \vdash e_2 \implies v_2}{V \vdash (e_1, e_2) \implies (v_1, v_2)} \qquad \textsc{Red-Proj}\quad \frac{V \vdash e \implies (v_1, v_2)}{V \vdash \pi_i(e) \implies v_i}$$

$$\textsc{Red-Let}\quad \frac{V \vdash e_1 \implies v_1 \qquad V, (x \mapsto v_1) \vdash e_2 \implies v_2 \qquad v_2 \overset{x \setminus v_1}{\rightsquigarrow} v_2'}{V \vdash \mathtt{let}\, x = e_1\, \mathtt{in}\, e_2 \implies v_2'}$$

$$\textsc{Red-App}\quad \frac{\begin{array}{c} V, V_1 \vdash t \implies (\mathrm{dom}\, V, V_2, \lambda y.t') \\ V, V_1 \vdash u \implies v_{\mathsf{arg}} \qquad V, V_1, V_2, y \mapsto v_{\mathsf{arg}} \vdash t' \implies w \qquad w \overset{y \setminus v_{\mathsf{arg}}}{\rightsquigarrow} w' \overset{V_2}{\rightsquigarrow} w'' \end{array}}{V, V_1 \vdash t\ u \implies w''}$$

$$\textsc{Red-App-Fix}\quad \frac{\begin{array}{c} V, V_1 \vdash t \implies (\mathrm{dom}\, V, (x_i \mapsto v_i)_{i \in I}, \mathtt{fix}\, f\, y.t') \\ V, V_1 \vdash u \implies v_{\mathsf{arg}} \qquad V, (x_i \mapsto v_i)_i, (f \mapsto \mathtt{fix}\, f\, y.t'), (y \mapsto v_{\mathsf{arg}}) \vdash t' \implies w \end{array}}{V, V_1 \vdash t\ u \implies w}$$

Fig. 6: Big-step reduction rules

The typing assumptions all match those of our premise. The reduction assumption is simply the composition of the reductions of the premises:

$$\begin{array}{ll} & \Gamma^{\Phi_1''}, y{:}\rho^{\chi''}, (x_i{:}\tau_i^{\psi_i})_{i \in I}, x{:}{\sigma_1}^{\phi} \vdash \sigma_2'' \\ \overset{(x_i) \setminus (\Psi_i)}{\rightsquigarrow} & \Gamma^{\Phi_1}, y{:}\rho^{\chi}, x{:}{\sigma_1}^{\phi} \vdash \sigma_2 \\ \overset{y \setminus \Psi}{\rightsquigarrow} & \Gamma^{\Phi_1 + \chi \cdot \Psi}, x{:}{\sigma_1}^{\phi} \vdash \sigma_2' \end{array}$$

□

The Big-Step Reduction Relation We are now equipped to define in Figure 6 the big-step reduction relation on well-typed terms $V \vdash e \implies v$, where V is a mapping from the variables to values that is assumed to contain at least all the free variables of e. The notation $w \overset{V_2}{\rightsquigarrow} w'$ denotes the sequence of substitutions for each (variable, value) pair in V_2, from the last one introduced in the context to the first; the intermediate values are unnamed and existentially quantified.

We write $V : \Gamma \vdash$ if the context valuation V, mapping free variables to values, is well-typed according to the context Γ.

$$\textsc{Value-Env-Empty}\quad \emptyset : \emptyset \vdash \qquad \textsc{Value-Env}\quad \frac{V : \Gamma \vdash \qquad \Gamma \vdash v : \sigma}{V, x \mapsto v : \Gamma, x{:}\sigma \vdash}$$

Theorem 1 (Type soundness). *If* $\Gamma^{\Phi} \vdash t : \sigma$, $V : \Gamma \vdash$ *and* $V \vdash t \implies v$ *then* $\Gamma \vdash v : \sigma$.

Proof. By induction on the reduction derivation $V \vdash t \implies v$.

Case Red-Var: From $V : \Gamma \vdash$ we have $\Gamma \vdash V(x) : \sigma$.
Case Red-Lam, Red-Lam-Fix: in the degenerate case where there are no captured values, the value typing rule Value-Closure for $[\Gamma^{\Phi}](x{:}\sigma^{\phi}) \to \tau$ has as only premise $\Gamma^{\Phi}, x{:}\sigma^{\phi} \vdash \tau$, which is precisely our typing assumption.
Case Red-Pair, Red-Proj: direct by induction.
Case Red-Let: The involved derivations are the following:

$$\frac{V \vdash e_1 \implies v_1 \qquad V, x \mapsto v_1 \vdash e_2 \implies v_2 \qquad v_2 \overset{x \setminus v_1}{\rightsquigarrow} v_2'}{V \vdash \mathtt{let}\, x = e_1\, \mathtt{in}\, e_2 \implies v_2'}$$

$$\frac{\Gamma^{\Phi_{\mathsf{def}}} \vdash e_1 : \sigma \qquad \Gamma^{\Phi_{\mathsf{body}}}, x{:}\sigma^{\phi} \vdash e_2 : \tau \qquad \Gamma, x{:}\sigma \vdash \tau \overset{x \setminus \Phi_{\mathsf{def}}}{\rightsquigarrow} \Gamma \vdash \tau'}{\Gamma^{\phi.\Phi_{\mathsf{def}} + \Phi_{\mathsf{body}}} \vdash \mathtt{let}\, x = e_1\, \mathtt{in}\, e_2 : \tau'}$$

By induction hypothesis we have $\Gamma \vdash v_1 : \sigma$, from which we deduce that $V, x \mapsto v_1 : \Gamma, x{:}\sigma \vdash$. This allows us to use induction again to deduce that $\Gamma, x{:}\sigma \vdash v_2 : \tau$. Finally, preservation of value typing by value substitution (Lemma 4) allows to conclude that the remaining goal $\Gamma \vdash v_2' : \tau'$ holds.
Case Red-App: the involved derivations are the following.

$$\frac{\begin{array}{c} V, V_1 \vdash t \implies (\operatorname{dom} V, (x_i \mapsto v_i)_{i \in I}, \lambda y.t') \qquad V, V_1 \vdash u \implies v_{\mathsf{arg}} \\ V, V_1, (x_i \mapsto v_i)_i, y \mapsto v_{\mathsf{arg}} \vdash t' \implies w \qquad w \overset{y \setminus v_{\mathsf{arg}}}{\rightsquigarrow} w' \overset{(x_i) \setminus (v_i)}{\rightsquigarrow} w'' \end{array}}{V, V_1 \vdash t\ u \implies w''}$$

$$\frac{\begin{array}{c} (\Gamma, \Gamma_1)^{\Phi_{\mathsf{fun}}} \vdash t : [\Gamma^{\Phi_{\mathsf{clos}}}](y{:}\sigma^{\phi}) \to \tau \\ (\Gamma, \Gamma_1)^{\Phi_{\mathsf{arg}}} \vdash u : \sigma \qquad \Gamma, y{:}\sigma \vdash \tau \overset{y \setminus \Phi_{\mathsf{arg}}}{\rightsquigarrow} \Gamma \vdash \tau' \end{array}}{(\Gamma, \Gamma_1)^{\Phi_{\mathsf{fun}} + \Phi_{\mathsf{clos}} + \phi.\Phi_{\mathsf{arg}}} \vdash t\ u : \tau'}$$

By induction we have that $\Gamma, \Gamma_1 \vdash v_{\mathsf{arg}} : \sigma$ and $\Gamma \vdash ((x_i \mapsto v_i)_i, \lambda y.t') : [\Gamma^{\Phi_{\mathsf{clos}}}](y{:}\sigma^{\phi}) \to \tau$.
By inversion, we know that the derivation for this value typing judgment is of the form

$$\frac{\begin{array}{c} \Gamma, \Gamma_1 \vdash \qquad \forall i \in I,\ \Gamma, (x_j{:}\tau_j)_{j<i} \vdash v_i : \tau_i \qquad \Gamma^{\Phi}, (x_i{:}\tau_i^{\psi_i})_{i \in I}, y{:}\sigma^{\phi} \vdash t' : \tau'' \\ \Gamma^{\Phi}, (x_i{:}\tau_i^{\psi_i})_{i \in I}, y{:}\sigma^{\phi} \vdash \tau'' \overset{(x_i) \setminus (\Psi_i)}{\rightsquigarrow} \Gamma^{\Phi_{\mathsf{clos}}}, y{:}\sigma^{\phi} \vdash \tau \end{array}}{\Gamma, \Gamma_1 \vdash (\operatorname{dom} \Gamma, (x_i \mapsto v_i)_{i \in I}, \lambda y.t') : [\Gamma^{\Phi_{\mathsf{clos}}}](y{:}\sigma^{\phi}) \to \tau}$$

From our result $\Gamma, \Gamma_1 \vdash v_{\mathsf{arg}}$ and the premises $\Gamma, (x_j{:}\tau_j)_{j<i} \vdash v_i : \tau_i$ we deduce that the application valuation is well-typed with respect to the application environment: $V, V_1, (x_i \mapsto v_i)_i, y \mapsto v_{\mathsf{arg}} : \Gamma, \Gamma_1, (x_i{:}\tau_i), \sigma \vdash$. It is used in the premise of the body computation judgment, so by induction we get that $\Gamma, \Gamma_1, (x_i{:}\tau_i), y{:}\sigma \vdash w : \tau''$.

$$\textsc{Classic-Red-Var}\quad W \vdash x \overset{c}{\Longrightarrow} W(x) \qquad \textsc{Classic-Red-Lam}\quad W \vdash \lambda x.t \overset{c}{\Longrightarrow} (W, \lambda x.t)$$

$$\textsc{Classic-Red-Lam-Fix}\quad W \vdash \mathtt{fix}\, f\, x.t \overset{c}{\Longrightarrow} (W, \mathtt{fix}\, f\, x.t)$$

$$\textsc{Classic-Red-Pair}\quad \frac{W \vdash e_1 \overset{c}{\Longrightarrow} w_1 \qquad W \vdash e_2 \overset{c}{\Longrightarrow} w_2}{W \vdash (e_1, e_2) \overset{c}{\Longrightarrow} (w_1, w_2)} \qquad \textsc{Classic-Red-Proj}\quad \frac{W \vdash e \overset{c}{\Longrightarrow} (w_1, w_2)}{W \vdash \pi_i(e) \overset{c}{\Longrightarrow} w_i}$$

$$\textsc{Classic-Red-Let}\quad \frac{W \vdash e_1 \overset{c}{\Longrightarrow} w_1 \qquad W, x \mapsto w_1 \vdash e_2 \overset{c}{\Longrightarrow} w_2}{W \vdash \mathtt{let}\, x = e_1\, \mathtt{in}\, e_2 \overset{c}{\Longrightarrow} w_2}$$

$$\textsc{Classic-Red-App}\quad \frac{W \vdash t \overset{c}{\Longrightarrow} (W', \lambda y.t') \qquad W \vdash u \overset{c}{\Longrightarrow} w_{\mathsf{arg}} \qquad W', y \mapsto w_{\mathsf{arg}} \vdash t' \overset{c}{\Longrightarrow} w}{W \vdash t\ u \overset{c}{\Longrightarrow} w}$$

$$\textsc{Classic-Red-App-Fix}\quad \frac{W \vdash t \overset{c}{\Longrightarrow} (W', \mathtt{fix}\, f\, y.t') \qquad W \vdash u \overset{c}{\Longrightarrow} w_{\mathsf{arg}} \qquad W', f \mapsto (W', \mathtt{fix}\, f\, y.t'), y \mapsto w_{\mathsf{arg}} \vdash t' \overset{c}{\Longrightarrow} w}{W \vdash t\ u \overset{c}{\Longrightarrow} w}$$

Fig. 7: Classic big-step reduction rules

From there, we wish to use preservation of value typing on the chain of value substitutions $w \overset{y \setminus v_{\mathsf{arg}}}{\rightsquigarrow} w' \overset{(x_i) \setminus (v_i)}{\rightsquigarrow} w''$ to conclude that $\Gamma \vdash w'' : \tau'$. However, the type substitutions of our premises are in the reverse order:

$$\Gamma^{\Phi}, (x_i{:}\tau_i^{\psi_i})_{i \in I}, y{:}\sigma^{\phi} \vdash \tau'' \overset{(x_i) \setminus (\Psi_i)}{\rightsquigarrow} \Gamma^{\Phi_{\mathsf{clos}}}, y{:}\sigma^{\phi} \vdash \tau \overset{y \setminus \Phi_{\mathsf{arg}}}{\rightsquigarrow} \Gamma^{\Phi_{\mathsf{clos}} + \phi.\Phi_{\mathsf{arg}}} \vdash \tau'$$

we therefore need to use our Reordering Lemma (1) to get them in the right order — note that the annotations $(\Psi_i)_{i \in I}$ and Φ_{arg} are not changed as they are independent from each other: for any i, we have $\Psi_i(y) = \Phi_{\mathsf{arg}}(x_i) = 0$.

$$\Gamma^{\Phi}, (x_i{:}\tau_i^{\psi_i})_{i \in I}, y{:}\sigma^{\phi} \vdash \tau'' \overset{y \setminus \Phi_{\mathsf{arg}}}{\rightsquigarrow} \Gamma^{\Phi'_{\mathsf{clos}}}, (x_i{:}\tau_i^{\psi_i})_{i \in I} \vdash \tau \overset{(x_i) \setminus (\Psi_i)}{\rightsquigarrow} \Gamma^{\Phi_{\mathsf{clos}} + \phi.\Phi_{\mathsf{arg}}} \vdash \tau'$$

□

Finally, we recall the usual big-step semantics for the call-by-value calculus with environments, in figure 7, and state its equivalence with our utilitarian semantics. Due to space restriction we will only mention the rules that differ, and elide the equivalence proof, but the long version contains all the details.

There is a close correspondence between judgments of both semantics, but as the value differ slightly, in the general cases the value bindings of the environment will also differ. We state the theorem only for closed terms, but the proof will proceed by induction on a stronger induction hypothesis using an equivalence between non-empty contexts.

Theorem 2 (Semantic equivalence). *Our reduction relation is equivalent with the classic one on closed terms:* $\emptyset \vdash t \implies v$ *holds if and only if* $\emptyset \vdash t \overset{c}{\Longrightarrow} v$ *also holds.*

To formulate our induction hypothesis, we define the equivalence judgment $V \vdash v = W \overset{c}{\vdash} w$; on each side of the equal sign there is a context and a value, the right-hand side being considered in the classical semantics.

$$\emptyset \vdash \ = \emptyset \overset{c}{\vdash} \qquad \frac{V \vdash \ = W \overset{c}{\vdash} \qquad V \vdash v = W \overset{c}{\vdash} w}{V, x \mapsto v \vdash \ = W, x \mapsto w \overset{c}{\vdash}}$$

$$\frac{V \vdash \ = W \overset{c}{\vdash}}{V \vdash \mathsf{v}_\alpha = W \overset{c}{\vdash} \mathsf{v}_\alpha} \qquad \frac{V \vdash v_1 = W \overset{c}{\vdash} w_1 \qquad V \vdash v_2 = W \overset{c}{\vdash} w_2}{V \vdash (v_1, v_2) = W \overset{c}{\vdash} (w_1, w_2)}$$

$$\frac{V \vdash \ = W \overset{c}{\vdash} \qquad V, x_i \mapsto v_i \vdash \ = W' \overset{c}{\vdash}}{V \vdash ((x_i \mapsto v_i)_{i \in I}, \lambda x.t) = W \overset{c}{\vdash} (W', \lambda x.t)}$$

The stronger version of the theorem becomes the following: if $V \vdash \ = W \overset{c}{\vdash}$ and $V \vdash t \implies v$ and $W \vdash t \overset{c}{\Longrightarrow} w$, then $V \vdash v = W \overset{c}{\vdash} w$.

As for subject reduction, we first need to prove that value substitution preserves value equivalence.

Lemma 5 (Value substitution preserves value equivalence). *If* $V, y \mapsto v_0 \vdash v = W \overset{c}{\vdash} w$, $V \vdash v_0 = W \overset{c}{\vdash} w_0$, *and* $v \overset{y \setminus v_0}{\rightsquigarrow} v'$ *then* $V \vdash v' = W \overset{c}{\vdash} w$.

Proof.
Subst-Value-Atom: direct.
Subst-Value-Product: direct induction.
Subst-Value-Closure: We have $((x_i \mapsto v_i)_{i \in I}, \lambda x.t) \overset{y \setminus v_0}{\rightsquigarrow} (, y \mapsto v_0(x_i \mapsto v_i)_{i \in I}, \lambda x.t)$ and $V, y \mapsto v_0 \vdash ((x_i \mapsto v_i)_{i \in I}, \lambda x.t) = W \vdash (W', \lambda x.t)$. The latter implies $V, y \mapsto v_0, x_i \mapsto v_i \vdash \ = W' \overset{c}{\vdash}$ which which in turn implies our goal $V \vdash (, y \mapsto v_0) =$ – with the additional premise $V \vdash \ = W \overset{c}{\vdash}$ from our hypothesis $V \vdash v_0 = W \overset{c}{\vdash} w_0$. □

We can now prove the theorem proper:

Proof.
Red-Var, Classic-Red-Var: we check by direct induction on the contexts that if $V \vdash \ = W \overset{c}{\vdash}$ holds, then $V \vdash V(x) = W \overset{c}{\vdash} W(x)$.
Red-Lam, Classic-Red-Lam: The correspondence between $V \vdash (\emptyset, \lambda x.t)$ and $W \overset{c}{\vdash} (W, \lambda x.t)$ under assumption $V \vdash \ = W \overset{c}{\vdash}$ is direct from the inference rule

$$\frac{V, \emptyset \vdash \ = W \overset{c}{\vdash}}{V \vdash (\emptyset, \lambda x.t) = W \overset{c}{\vdash} (W, \lambda x.t)}$$

Red-Pair, Classic-Red-Pair and Red-Proj, Classic-Red-Proj: direct by induction.

Red-Let, Classic-Red-Let: By induction hypothesis on the e_1 premise, we deduce that $V \vdash v_1 = W \overset{c}{\vdash} w_1$, hence $V, x \mapsto v_1 \vdash \ = W, x \mapsto w_1 \overset{c}{\vdash}$. This lets us deduce, again by induction hypothesis, that $V, x \mapsto v_1 \vdash v_2 = W, x \mapsto w_1 \overset{c}{\vdash} w_2$. As value substitution preserves value equivalence, we can deduce from $v_2 \overset{x \setminus v_1}{\rightsquigarrow} v_2'$ that our goal $V \vdash v_2' = W \overset{c}{\vdash} w_2$ holds.

Red-App, Classic-Red-App: By induction hypothesis we have that $V \vdash v_{\mathsf{arg}} = W \vdash w_{\mathsf{arg}}$ and $V \vdash ((x_i \mapsto v_i)_{i \in I}, \lambda y.t') = W \overset{c}{\vdash} (W', \lambda y.t')$. By inversion on the value equivalence judgment of the latter we know that $V, x_i \mapsto v_i \vdash \ = W' \overset{c}{\vdash}$. Combined with the former value equivalence, this gives us $V, x_i \mapsto v_i, y \mapsto v_{\mathsf{arg}} \vdash \ = W', y \mapsto w_{\mathsf{arg}} \overset{c}{\vdash}$, so by induction hypothesis and preservation of value equivalence by reduction we can deduce our goal. □

4 Dependency information as non-interference

We can formulate our dependency information as a *non-interference* property. Two valuations V and V' are Φ-equivalent, noted $V =_\Phi V'$, if they agree on all variables on which they depend according to Φ. We say that e respects non-interference for Φ when, whenever $V \vdash e \implies v$ holds, then for any V' such that $V =_\Phi V'$ we have that $V' \vdash e \implies v$ also holds. This corresponds to the information-flow security idea that variables marked 1 are low-security, while variables marked 0 are high-security and should not influence the output result.

This non-interference statement requires that the two evaluations of e return the same value v. This raises the question of what is the right notion of equality on values. Values of atomic types have a well-defined equality, but picking the right notion of equality for function types is more difficult. While we can state a non-interference result on atomic values only, the inductive subcases would need to handle higher-order cases as well.

Syntactic equality (even modulo α-equivalence) is not the right notion of equality for closure values. Consider the following example: $x{:}\tau^0 \vdash \mathtt{let}\, y = x\, \mathtt{in}\, \lambda z.z : [x{:}\tau^0](z : \sigma^1) \to \sigma$. This term contains an occurrence of the variable x, but its result does not depend on it. However, evaluating it under two different contexts $x{:}v$ and $x{:}v'$, with $v \neq v'$, returns distinct closures: $(x \mapsto v, \lambda z.z)$ on one hand, and $(x \mapsto v', \lambda z.z)$ on the other. These closures are not structurally equal, but their difference is not essential since they are indistinguishable in any context. Logical relations are the common technique to ignore those internal differences and get a more observational equality on functional values. They involve, however, a fair amount of metatheoretical effort (in particular in presence of non-terminating fixpoints) that we would like to avoid.

Consider a different example: $x{:}\tau^0 \vdash \lambda y.x : [x{:}\tau^1](y{:}\sigma^0) \to \tau$. Again, we could use two contexts $x{:}v$ and $x{:}v'$ with $v \neq v'$, and we would get as a result two closures: $x{:}v \vdash \lambda y.x \implies (x \mapsto v, \lambda y.x)$ and $x{:}v' \vdash \lambda y.x \implies (x \mapsto v', \lambda y.x)$.

$$\textsc{Equiv-Atom}\quad \Gamma \vdash \mathsf{v}_\alpha =_{\Phi_0} \mathsf{v}_\alpha : \alpha$$

$$\textsc{Equiv-Pair}\quad \frac{\Gamma \vdash v_1 =_{\Phi_0} v_1' : \sigma_1 \qquad \Gamma \vdash v_2 =_{\Phi_0} v_2' : \sigma_2}{\Gamma \vdash (v_1, v_2) =_{\Phi_0} (v_1', v_2') : \sigma_1 * \sigma_2}$$

$$\textsc{Equiv-Closure}\quad \frac{\begin{array}{c}\forall i \in I,\ \Gamma, (x_j{:}\tau_j)_{j<i} \vdash v_i : \tau_i \qquad \Gamma^\Phi, (x_i{:}\tau_i^{\psi_i})_{i\in I}, x{:}\sigma^\phi \vdash t : \tau \\ \Gamma^\Phi, (x_i{:}\tau_i^{\psi_i})_{i\in I}, x{:}\sigma^\phi \vdash \tau \overset{(x_i)\setminus(\Psi_i)}{\rightsquigarrow} \Gamma^{\Phi'}, x{:}\sigma^\phi \vdash \tau' \qquad \forall i \in I, \Psi_i \subseteq \Phi_0 \implies v_i =_{\Phi_0} v_i'\end{array}}{\Gamma \vdash ((x_i \mapsto v_i)_{i\in I}, \lambda y.t) =_{\Phi_0} ((x_i \mapsto v_i')_{i\in I}, \lambda y.t) : [\Gamma^{\Phi'}](x{:}\sigma) \to \tau'}$$

Fig. 8: Value equivalence

Interestingly, these two closures are *not* equivalent under all contexts: any context applying the function will be able to observe the different results. However, our notion of interference requires that they can be considered equal. This is motivated by real-world programming languages that only output a pointer to a closure in a program that returns a function.

While the aforementioned closures are not equal in any context, they are in fact equivalent from the point of view of the particular dependency annotation for which we study non-interference, namely $x{:}\tau^0$. To observe the difference between those closures, we would need to apply the closure of type $[x{:}\tau^1](y : \sigma) \to \tau$, so would be in the different context $x{:}\tau^1$.

This insight leads us to our formulation of value equivalence in Figure 8. Instead of being as modular and general as a logical-relation definition, we fix a *global dependency* Φ_0 that restricts which terms can be used to differentiate values.

Our notion of value equivalence, $\Gamma \vdash v =_{\Phi_0} v' : \sigma$ is typed and includes structural equality. In the rule Equiv-Closure, we check that the two closures values are well-typed, and only compare captured values whose dependencies are included in those of the global context Φ_0, as we know that the others will not be used. This equality is tailored to the need of the non-interference result, which only compares values resulting from the evaluation of the same subterm – in distinct contexts.

Theorem 3 (Non-interference). *If $\Gamma^{\Phi_0} \vdash e : \sigma$ holds, then for any contexts V, V' such that $V =_{\Phi_0} V'$ and values v, v' such that $V \vdash e \implies v$ and $V' \vdash e \implies v'$, we have $\Gamma \vdash v =_{\Phi_0} v' : \sigma$. In particular, if σ is an atomic type, then $v = v'$ holds.*

Proof. We will proceed by simultaneous induction on the typing derivation $\Gamma \vdash e : \sigma$ and reduction derivation $V \vdash e \implies v$ and . Note that we use a different induction hypothesis: for any subderivations $\Gamma^\Phi \vdash e : \sigma$ and $V \vdash t \implies v$, we will prove that for any V' that agrees with V on Φ modulo Φ_0-equivalence ($\forall x, V(x) =_{\Phi_0} V'(x)$, which we still note $V =_\Phi V'$), and with $V' \vdash t \implies v'$, we have $v =_{\Phi_0} v'$.

We will omit the contexts and types Γ, σ of a value equivalence $\Gamma \vdash v =_{\Phi_0} v' : \sigma$ when they are clear from the context.

Case Red-Var: from $V =_{0,x:1,0} V'$ we have $V(x) =_{\Phi_0} V'(x)$.

Case Red-Lam, Red-Lam-Fix : the returned value does not depend on the environment.

Case Red-Pair, Red-Proj: direct by induction.

Case Red-Let: the involved derivations are the form

$$\frac{\Gamma^{\Phi_{\mathsf{def}}} \vdash e_1 : \sigma \qquad \Gamma^{\Phi_{\mathsf{body}}}, x{:}\sigma^{\phi} \vdash e_2 : \tau}{\Gamma^{\Phi_{\mathsf{body}}+\phi.\Phi_{\mathsf{def}}} \vdash \mathtt{let}\, x = e_1\, \mathtt{in}\, e_2 : \tau}$$

$$\frac{V \vdash e_1 \implies v_1 \qquad V, x \mapsto v_1 \vdash e_2 \implies v_2 \qquad v_2 \overset{x\backslash v_1}{\rightsquigarrow} v_3}{V \vdash \mathtt{let}\, x = e_1\, \mathtt{in}\, e_2 \implies v_3}$$

$$\frac{V' \vdash e_1 \implies v_1' \qquad V', x \mapsto v_1' \vdash e_2 \implies v_2' \qquad v_2' \overset{x\backslash v_1'}{\rightsquigarrow} v_3'}{V' \vdash \mathtt{let}\, x = e_1\, \mathtt{in}\, e_2 \implies v_3'}$$

The context equivalence $V =_{\Phi_{\mathsf{body}}+\phi.\Phi_{\mathsf{def}}} V'$ implies the weaker equivalence $V =_{\Phi_{\mathsf{body}}} V'$, from which we can deduce $V, x \mapsto v_1 =_{(\Phi_{\mathsf{body}},\phi)} V', x \mapsto v_1'$ regardless of the value of ϕ. Indeed, if ϕ is 0 this is direct, and if ϕ is 1 we get $v_1 =_{\Phi_0} v_1'$ by induction hypothesis. From this equality between contexts we get $v_2 =_{\Phi_0} v_2'$ by induction hypothesis.

We then reason by case distinction on the property $\Phi_{\mathsf{def}} \subseteq \Phi_0$. If it holds, then again $v_1 =_{\Phi_0} v_1'$ by induction, so substituting v_1, v_1' in the closures of v_2, v_2' will preserve Φ_0-equivalence. And if it does not, those values v_1, v_1' captured in the closures of v_2, v_2' will not be tested for Φ_0-equivalence. In any case, we have $v_3 =_{\Phi_0} v_3'$.

Case Red-App: the proof for the application case uses the same mechanisms as for the Red-Let case but is more tedious because of the repeated application and substitution of the closed-over values. To simplify notations, we will handle the case of a single captured value $x \mapsto v$. The involved derivations are the following:

$$\frac{\Gamma^{\Phi_{\mathsf{fun}}} \vdash t : [\Gamma^{\Phi_{\mathsf{clos}}}](y{:}\sigma^{\phi}) \to \tau \qquad \Gamma^{\Phi_{\mathsf{arg}}} \vdash u : \sigma \qquad \Gamma, y{:}\sigma \vdash \tau \overset{y\backslash \Phi_{\mathsf{arg}}}{\rightsquigarrow} \Gamma \vdash \tau'}{\Gamma^{\Phi_{\mathsf{fun}}+\Phi_{\mathsf{clos}}+\phi.\Phi_{\mathsf{arg}}} \vdash t\ u : \tau'}$$

$$\frac{\begin{array}{c} V \vdash t \implies (x \mapsto v, \lambda y.t') \qquad V \vdash u \implies v_{\mathsf{arg}} \\ V, y \mapsto v_{\mathsf{arg}}, x \mapsto v \vdash t' \implies w_1 \qquad w_1 \overset{x\backslash v}{\rightsquigarrow} w_2 \overset{y\backslash v_{\mathsf{arg}}}{\rightsquigarrow} w_3 \end{array}}{V \vdash t\ u \implies w_3}$$

$$\frac{\begin{array}{c} V' \vdash t \implies (x \mapsto v', \lambda y.t') \qquad V' \vdash u \implies v'_{\mathsf{arg}} \\ V, y \mapsto v'_{\mathsf{arg}}, x \mapsto v' \vdash t' \implies w_1' \qquad w_1' \overset{x\backslash v'}{\rightsquigarrow} w_2' \overset{y\backslash v'_{\mathsf{arg}}}{\rightsquigarrow} w_3' \end{array}}{V \vdash t\ u \implies w_3'}$$

From $\Phi_{\mathsf{fun}} \subseteq \Phi_{\mathsf{fun}} + \Phi_{\mathsf{clos}} + \phi.\Phi_{\mathsf{body}}$ we get by induction that $\Gamma \vdash (x \mapsto v, \lambda y.t') =_{\Phi_0} (x \mapsto v', \lambda y.t') : [\Gamma^{\Phi_{\mathsf{clos}}}](y{:}\sigma^{\phi}) \to \tau$. This equivalence gives us

the following premises:

$$\frac{\Gamma, x{:}\rho \vdash v : \tau_i \qquad \Gamma^{\Phi}, y{:}\sigma^{\phi}, x{:}\rho^{\psi} \vdash t : \tau \qquad \Gamma^{\Phi}, y{:}\sigma^{\phi}, x{:}\rho^{\psi} \vdash \tau \overset{x \setminus \Psi}{\rightsquigarrow} \Gamma^{\Phi'}, x{:}\sigma^{\phi} \vdash \tau' \qquad \Psi \subseteq \Phi_0 \implies \Gamma \vdash v =_{\Phi_0} v' : \rho}{\Gamma \vdash (x \mapsto v, \lambda y.t') =_{\Phi_0} (x \mapsto v', \lambda y.t') : [\Gamma^{\Phi_{\mathsf{clos}}}](y{:}\sigma^{\phi}) \to \tau}$$

If $\Psi \subseteq \Phi_0$ then $v =_{\Phi_0} v'$, and similarly we get $v_{\mathsf{arg}} = v'_{\mathsf{arg}}$ only in the case where $\Phi_{\mathsf{arg}} \subseteq \ldots$, that is ϕ (the argument dependency) is 1. In any case, w_1 and w'_1 are Φ_0-equivalent by induction, and by construction this is preserved by the substitutions $\overset{x \setminus v}{\rightsquigarrow}$ and $\overset{y \setminus v_{\mathsf{arg}}}{\rightsquigarrow}$.

□

5 Prototype implementation

To experiment with our type system, we implemented a software prototype in OCaml. At around one thousand lines, the implementation mainly contains two parts.

1. For each judgement in this paper, a definition of corresponding set of inference rules along with functions for building and checking derivations.
2. A (rudimentary) command-line interface that is based on a lexer, a parser, and a pretty-printer for the expressions, types, judgments and derivations of our system.

For the scope checking judgments for context and types, the implementation *checks* well-scoping of the given contexts and types. It ether builds a derivation using the well-scoping rules or fails to do so because of ill-scoped input.

For the typing judgment, the implementation performs some *inference*. Given Γ and e, it will return the Φ and σ for which a derivation (also returned) $\Gamma^{\Phi} \vdash e : \sigma$ exists, and fail otherwise. The substitution and reduction judgments are deterministic and computational in nature; our implementation takes their left-hand side of the judgement (with additional parameters) and *computes* the right-hand-side of the judgment along with a derivation.

Below is an example of interaction with the prototype interface:

```
% make
% ./closures.byte -str "let y = (y1, y2) in (y, \(x:\sigma) z)"
Parsed expression: let y = (y1, y2) in (y, λ(x:σ) z)

The variables (y1, y2, z) were unbound; we add them to the default environment
with dummy types (ty_y1, ty_y2, ty_z) and values (val_y1, val_y2, val_z).

Inferred typing:
  y1:ty_y1¹,y2:ty_y2¹,z:ty_z⁰ ⊢
    let y = (y1, y2) in (y, λ(x:σ) z)
    : ((ty_y1 * ty_y2) * [y1:ty_y1⁰,y2:ty_y2⁰,z:ty_z¹](x:σ⁰) → ty_z)

Result value: ((val_y1, val_y2), ([y1,y2,z], ((y↦(val_y1, val_y2))), λ(x) z))
```

In this example, adapted from the starting example of the article, $y{:}\sigma^1, z{:}\tau^0 \vdash (y, \lambda x.z)$, one can observe that the value z is marked as non-needed by the global value judgment, but needed in the type of the closure $\lambda x.z$. Besides, the computed value closure has captured the local variable y, but still references the variables $y1, y2, z$ of the outer context.

The prototype can also produce ASCII rendering of the typing and reduction derivations, when passed the `--typing-derivation` or `--reduction-derivation` option. This can be useful in particular in the case of typing or reduction errors, as a way to locate the erroneous sub-derivation.

The complete source code of the prototype is available at the following URL: http://gallium.inria.fr/~scherer/research/open_closure_types

6 Conclusion

We have introduced open closure types and their type theory. The technical novelty of the type system is the ability to track intensional properties of function application in function closures types. To maintain this information,we have to update function types when they escape to a smaller context. This update is performed by a novel non-trivial substitution operation. We have proved the soundness of this substitution and the type theory for a simply-typed lambda calculus with pairs, let bindings and fixpoints.

To demonstrate how our open closure types can be used in program verification we have applied this technique to track data-flow information and to ensure non-interference in the sense of information-flow theory. We envision open closure types to be applied in the context of type systems for strong intensional properties of higher-order programs, and this simple system to serve as a guideline for more advanced applications.

We already have preliminary results from an application of open closure types in amortized resource analysis [7,6]. Using them, we were for the first time able to express a linear resource bound for the curried append function (see Section 1).

References

1. Abel, A.: Semi-continuous Sized Types and Termination. Log. Methods Comput. Sci. 4(2) (2008)
2. Barthe, G., Grégoire, B., Riba, C.: Type-Based Termination with Sized Products. In: Computer Science Logic, 17th Ann. Conf. (CSL'08). pp. 493–507 (2008)
3. Chin, W.N., Khoo, S.C.: Calculating Sized Types. High.-Ord. and Symb. Comp. 14(2-3), 261–300 (2001)
4. Hannan, J., Hicks, P., Liben-Nowell, D.: A Lifetime Analysis for Higher-Order Languages. Tech. rep., The Pennsylvania State University (1997), http://www.cse.psu.edu/~hannan/papers/live.ps.gz
5. Heintze, N., Riecke, J.G.: The SLam Calculus: Programming with Secrecy and Integrity. In: 25th Symp. on Principles of Programming Languages (POPL'98). pp. 365–377 (1998)

6. Hoffmann, J., Aehlig, K., Hofmann, M.: Multivariate Amortized Resource Analysis. ACM Trans. Program. Lang. Syst. (2012)
7. Jost, S., Hammond, K., Loidl, H.W., Hofmann, M.: Static Determination of Quantitative Resource Usage for Higher-Order Programs. In: 37th Symp. on Principles of Programming Languages (POPL'10). pp. 223–236 (2010)
8. Lago, U.D., Petit, B.: The Geometry of Types. In: 40th Symp. on Principles of Programming Languages (POPL'13). pp. 167–178 (2013)
9. Leroy, X.: Polymorphic Typing of an Algorithmic Language. Research report 1778, INRIA (1992)
10. Minamide, Y., Morrisett, J.G., Harper, R.: Typed Closure Conversion. In: 23rd Symp. on Principles of Programming Languages (POPL'96). pp. 271–283 (1996)
11. Nanevski, A., Pfenning, F., Pientka, B.: Contextual Modal Type Theory. ACM Trans. Comput. Log. 9(3) (2008)
12. Petricek, T., Orchard, D., Mycroft, A.: Coeffects: The Essence of Context Dependence (2012), http://www.cl.cam.ac.uk/~tp322/drafts/coeffects.html
13. Pientka, B., Dunfield, J.: Programming with Proofs and Explicit Contexts. In: 10th International Conference on Principles and Practice of Declarative Programming (PPDP'08). pp. 163–173 (2008)
14. Sabelfeld, A., Myers, A.C.: Language-based information-flow security. IEEE Journal on Selected Areas in Communications 21(1), 5–19 (2003)
15. Stampoulis, A., Shao, Z.: Static and User-Extensible Proof Checking. In: 39th Symp. on Principles of Programming Languages (POPL'12). pp. 273–284 (2012)