

1 Recovering Purity with Comonads and Capabilities

2 The marriage of purity and comonads
 3

4 **5 ANONYMOUS AUTHOR(S)**

6 In this paper, we take a pervasively effectful (in the style of ML) typed lambda calculus, and show how to
 7 extend it to permit capturing pure expressions with types. Our key observation is that, just as the pure simply-
 8 typed lambda calculus can be extended to support effects with a monadic type discipline, an impure typed
 9 lambda calculus can be extended to support purity with a *comonadic* type discipline.

10 We establish the correctness of our type system via a simple denotational model, which we call the *capability*-
 11 *space* model. Our model formalizes the intuition common to systems programmers that the ability to
 12 perform effects should be controlled via access to a permission or capability, and that a program is *capability-safe*
 13 if it performs no effects that it does not have a runtime capability for. We then identify the axiomatic
 14 categorical structure that the capability space model validates, and use these axioms to give a categorical
 15 semantics for our comonadic type system. We then give an equational theory (substitution and the call-by-value
 16 β and η laws) for the imperative lambda calculus, and show its soundness relative to this semantics.

17 Finally, we give a translation of the pure simply-typed lambda calculus into our comonadic imperative
 18 calculus, and show that any two terms which are $\beta\eta$ -equal in the STLC are equal in the equational theory of
 19 the comonadic calculus, establishing that pure programs can be mapped in an equation-preserving way into
 20 our imperative calculus.

21 **1 INTRODUCTION**

22 Consider the following definition of the familiar map functional.

```
23   map1 : ∀ a b. (a → b) → List a → List b
  24   map1 f []          = []
  25   map1 f (x :: xs) = let zs = map1 f xs in
  26           let z = f x in
  27           z :: zs
  28
```

29 This definition is the one that might be given in an introductory functional programming class –
 30 it recursively examines whether the list is nil or a cons and rebuilds the list, applying the function f
 31 each time. However, this definition is not ideally suited to be the implementation in a standard
 32 library, since it is *not tail-recursive*. As a result, one might be minded to replace it with the following
 33 “equivalent” definition:

```
34   map2 : ∀ a b. (a → b) → List a → List b
  35   map2 f ys =
  36       let rec loop xs acc =
  37           match xs with
  38           | []      → List.reverse acc
  39           | x :: xs → loop xs (f x :: acc)
  40       in
  41       loop xs []
  42
```

43 This version applies f in a tail-recursive loop, building up a reversed list of applications, and
 44 then reverses the list again before returning it to the client. This implementation allocates an in-
 45 termediate list, but will never blow the stack.

50 However, in an *impure* functional language, it is not possible to transparently replace the first
 51 definition with the second. The difference between these two implementations is *observable*.

```
52 let xs : List String = ["left "; "to "; "right "]  

  53  

  54 let f : String → String = fun s → stdout.print(s); s  

  55  

  56 let zs1 = map1 f xs  -- Prints "right to left " to stdout  

  57 let zs2 = map2 f xs  -- Prints "left to right " to stdout  

  58
```

59 So something as innocuous-seeming as a `print` function can radically change the equational theory
 60 of the language: no program transformation that changes the order in which sub-expressions
 61 are evaluated is in general sound. This greatly complicates reasoning about programs, as well as
 62 hindering many desirable program optimisations such as list fusion and deforestation [Wadler
 63 1990]. Transformations that are unconditionally valid in a pure language must, in an impure lan-
 64 guage, be gated by complex whole-program analyses tracking the purity of sub-expressions.
 65

66 *Contributions.* It is received wisdom that much as a drop of ink cannot be removed from a glass
 67 of water, once a language supports ambient effects, there is no way to regain the full equational
 68 theory of a pure programming language. In this paper, we show that this folk belief is *false*: we
 69 extend an ambiently effectful language to support purity. Entertainingly, it turns out that just as
 70 monads are a good tool to extend pure languages with effects, **comonads** are a good tool to extend
 71 impure languages with purity!

- 72 • We take a pervasively effectful lambda calculus in the style of ML and show how to *extend*
 73 it with a *comonadic* type discipline that permits capturing pure expressions with types.
- 74 • We give a simple and intuitive denotational model for our language, which we call the *ca-*
 75 *pability space* model. Our semantics is a formalisation of the intuition underpinning the
 76 *object-capability model* [Lauer and Needham 1979; Levy 1984; Miller 2006] familiar to sys-
 77 tems designers, which says that the ability to perform effects should be controlled via access
 78 to a permission or capability, and that a program is *capability-safe* precisely when it can only
 79 perform effects that it possesses a runtime capability for.

80 We do this by extending the most naive model of the lambda calculus – sets and functions –
 81 with just enough structure to model capability-safe programs. In our model, a type is just a
 82 set X (denoting a set of values), together with a function w saying which capabilities each
 83 value x owns. Then, a morphism $f : X \rightarrow Y$ is *capability-safe* if the capabilities of $f(x)$ are
 84 always bounded by the capabilities of x .

85 It is already known in the systems community that effectful lambda-calculi without ambient
 86 authority are capability-safe. Our model demonstrates that this observation is incomplete –
 87 having a comonad witnessing the *denial* of a capability is also very beneficial.

- 88 • We then identify the axiomatic categorical structure the capability space model validates,
 89 and use these axioms to give a categorical semantics for our comonadic type system. We
 90 then give an equational theory (substitution and the call-by-value β and η laws) for the
 91 imperative lambda calculus, and show its soundness relative to this semantics.
- 92 • Finally, we give a translation of the pure simply-typed lambda calculus into our comonadic
 93 imperative calculus, and show that any two terms which are $\beta\eta$ -equal in the STLC are equal
 94 in the equational theory of the comonadic calculus under the translation, establishing that
 95 pure programs can be mapped in an equation-preserving way into our imperative calculus.

96 Detailed proofs of the lemmas and theorems are given in the supplementary appendices.

99 **2 RECOVERING PURITY BY EXAMPLE**

100
 101 In order to reason about purity in an ambiently effectful language, it is necessary to identify
 102 whether a program may have effects or not. This is a relatively straightforward task in a first-
 103 order language: we can decide whether a procedure may have effects by examining each sub-
 104 phrase of an expression and seeing if it either performs an effect, or calls a procedure which may
 105 perform effects. In this way, programs can be partitioned into those which are definitely pure, or
 106 those which may have effects. However, this distinction breaks down in a higher-order functional
 107 language. Consider again the example of the `map` functional:

```
108
109   map : ∀ a b. (a → b) → List a → List b
110   map f []      = []
111   map f (x :: xs) = f x :: map f xs
```

112 The expression `map g` is effectful, depending on whether the body of the function `g` has an effect
 113 or not. So if we want to ensure that calls to `map` are always pure, we have to ensure that it is always
 114 passed a pure function. An alternative way of expressing the issue is that, within the definition
 115 of `map`, there is a function-valued variable `f`, and we are free to substitute *any* function (including
 116 effectful ones) for `f`.

117 Therefore, we introduce **two kinds of variables**: pure variables and arbitrary (or impure) vari-
 118 ables. This lets us define the notion of “pure term” in a simple and brutal fashion: we judge a
 119 pure term to be one which *both* performs no obvious effects, *and* all of whose free variables are
 120 themselves pure. Then, by restricting the substitution to only permit substituting pure terms for
 121 pure variables, the judgement of purity will be stable under substitution. Then, by internalising
 122 the purity judgement as a type, we can pass pure expressions around as first-class values.

123 To understand this, let us begin with a simple call-by-value higher-order functional language
 124 extended with types for string constants, channels (or output file handles), and a single effect:
 125 outputting a string onto a channel with `chan.print(s)`. There is no monadic or effect typing
 126 discipline here; the type of `print` is just as one might see in OCaml or Java.

```
127
128   print : Channel → String → Unit
```

129 For example, here is a simple function to print each element of a pair of strings to a given
 130 channel:

```
131
132   print_pair : String × String → Channel → Unit
133   print_pair = fun p chan →
134     chan.print(fst p);
135     chan.print(snd p)
```

136 Here, for clarity we use a semicolon for sequencing, and write `print` in method-invocation style
 137 *a la* Java (to make it easy to distinguish the file handle from the string argument).

138 To support purity, we extend the language with a new type constructor `Pure a`, denoting the
 139 set of expressions of type `a` which are *pure* – i.e., they own no file handles and so their execution
 140 cannot do any printing. So we add the introduction form `box(e)` to introduce a value whose type
 141 is `Pure a`; the type system accepts this if `e` has type `a` and is recognisably pure, but rejects it
 142 otherwise. Here, “recognisably pure” means that the term `e` has no syntactically obvious effects of
 143 its own, and all of its free variables are pure variables.

144 To eliminate a value of type `Pure a`, we will use *pattern matching*, writing the elimination
 145 form `let box(x) = e1 in e2` to bind the pure expression in `e1` to the variable `x`. The only differ-
 146 ence from ordinary pattern matching is that `x` is marked as a pure variable, permitting it to occur

148 inside of pure expressions. Intuitively, this makes sense – `e1` evaluates to a pure value, and so its
 149 result should be allowed to be used by other pure expressions.

150 We can see how these play out with the following examples, where we try to give a type for
 151 an apply function, which takes a function and an argument, applies the argument to the function,
 152 and returns the output, at varying levels of purity.

153 First, we consider a function that applies a pure argument to an unrestricted function:

```
154   apply : (String → Int) → Pure String → Int
155   apply f box(s) = f s  -- accepted
156
```

157 This example is accepted. The `box(s)` pattern tells us that `s` is a pure variable, but there are
 158 no restrictions on using pure variables as impure terms (since a pure term is an impure term that
 159 happens to not perform side-effects).

160 Next, we consider a variant of this function which applies an arbitrary function to a pure argument,
 161 and tries to return a pure result.

```
162   apply : (String → Int) → Pure String → Pure Int
163   apply f box(s) = box(f s)  -- REJECTED
164
```

165 This variant is rejected. Intuitively, the call to the function `f` could have side-effects. Syntactically,
 166 since `f` is an impure variable, it is simply not allowed to occur in the pure expression `box(f s)`. For
 167 similar reasons, it is not possible to write a polymorphic `fmap` : $\forall a b. (a \rightarrow b) \rightarrow \text{Pure } a$
 168 $\rightarrow \text{Pure } b$ function for the `Pure` type constructor. However, `Pure` is a functor in the semantic
 169 sense – the absence of a map action indicates that this functor lacks *tensorial strength*.

170 We can still make both the function and the argument to apply into boxed types.

```
171   apply : Pure (String → Int) → Pure String → Pure Int
172   apply box(f) box(s) = box(f s)  -- accepted
173
```

174 In this case, `box(f s)` is accepted, since both the variables `f` and `s` are known to be pure, and
 175 so are permitted to occur inside of a pure expression.

176 Our type discipline also permits typing functions whose behaviour is intermediate between pure
 177 and effectful. For example, suppose that we see the following type declaration:

```
178   maybe_print : Pure (Maybe Channel → String)
179   -- definition not visible
180
```

181 We do not know anything about the body of the definition, but due to the typing discipline, we
 182 know that `maybe_print` owns no capabilities of its own. As a result, we can make some inferences
 183 when we see the following two declarations:

```
184   x : String
185   x = let Box(f) = maybe_print in
186       f (Some stdout)
187
188   y : String
189   y = let Box(f) = maybe_print in
190       f None
191
```

192 The definition of `x` passes a channel to `maybe_print`, and so it may have an effect (it might use
 193 it to print). On the other hand, we *know* that the evaluation of `y` *will not* have an effect – we know
 194 that `maybe_print` owned no channels, and since we did not give it a channel, it can therefore
 195 perform no effects. Moreover, we know this without having to see the definition of `maybe_print`!

196

197	TYPES	$A, B ::= \text{unit} \mid A \times B \mid A \Rightarrow B \mid \text{str} \mid \text{cap} \mid \square A$
198	TERMS	$e ::= () \mid (e_1, e_2) \mid \text{fst } e \mid \text{snd } e \mid x \mid \lambda x : A. e \mid e_1 e_2$ $s \mid \text{box } \boxed{e} \mid \text{let box } \boxed{x} = e_1 \text{ in } e_2 \mid e_1 \cdot \text{print}(e_2)$
199	VALUES	$v ::= x \mid () \mid (v_1, v_2) \mid \lambda x : A. e \mid s \mid \text{box } \boxed{e}$
200	QUALIFIERS	$q, r ::= \textcolor{blue}{p} \mid \textcolor{red}{i}$
201	CONTEXTS	$\Gamma, \Delta, \Psi ::= \cdot \mid \Gamma, x : A^q$
202	SUBSTITUTIONS	$\theta, \phi ::= \langle \rangle \mid \langle \theta, e^q / x \rangle$

Fig. 1. Grammar

In the next two sections, we will see that this discipline of tracking whether a variable is pure or not is precisely a *comonadic* type discipline, corresponding to the \square modality in S4 modal logic, and that the model arises from a formalisation of object capabilities.

3 TYPING

We give the grammar of our language in figure 1.

We have the usual type constructors for unit, products, and functions from the simply-typed lambda calculus. In addition to this, we have the type str for strings, and the type cap representing output channels (used in the imperative $e_1 \cdot \text{print}(e_2)$ statement). Finally, we add the comonadic \square type constructor which corresponds to the **Pure** type constructor we introduced in section 2.

Despite the fact that there is a *type* cap of channels, and a print operation which uses them, there are no introduction forms for them. This is intentional! The absence of this facility corresponds to the principle of *capability safety* – the only capabilities a program should possess are those that are passed by its caller. So, a complete program will either be a function that receives a capability token as an argument, or have free variables that the system can bind capability tokens to.¹

The expressions in our language include the usual ones from the simply-typed lambda calculus, constants s for strings, and print. We also have an introduction form $\text{box } \boxed{e}$, and a let box elimination form for the $\square A$ type; we'll explain how these work later. Values are a subset of expressions, but box turns any expression into a value.²

We would like a modal type system where we can distinguish between expressions with and without side-effects. Following the style of [Pfenning and Davies 2001] for S4 modal logic, we could build a dual-context calculus. However, such a setup makes it difficult to define substitution; we can avoid dual contexts by tagging terms with qualifiers instead. We use two qualifiers that we can annotate terms with, in the appropriate places. We use **p** to tag *pure* terms, and **i** to tag *impure* terms.³

Next, we define contexts of variables. A well-formed context is either the empty context \cdot , or an extended context with a variable x of type A and qualifier q . Finally, we give a grammar for substitutions. A substitution is either the empty substitution $\langle \rangle$, or an extended substitution with an expression e substituted for variable x qualified by q .⁴

¹Of course, a full system should have the ability to create new private capabilities of its own. We omit this to keep the denotational semantics simple, but discuss how to add it in section 8.

²We sometimes use the expression form $e_1 ; e_2$, which is just syntactic sugar for $(\lambda x : \text{unit}. e_2) e_1$.

³We use different colours to distinguish *pure* and *impure* syntactic objects, and we'll follow this convention henceforth.

⁴When we have unknown qualifiers occurring on terms, we *highlight* them in a different colour, and the colour changes to the appropriate one when the qualifier is **p** or **i**.

246 $x : A^q \in \Gamma$ x is a variable of type A with qualifier q in context Γ
 247 $\Gamma \vdash e : A$ e is an expression of type A in context Γ
 248 $\Gamma \vdash^p e : A$ e is a *pure* expression of type A in context Γ
 249

Fig. 2. Typing Judgements

$$\begin{array}{c}
 \frac{}{\Gamma \vdash () : \text{unit}} \text{unitI} \quad \frac{}{\Gamma \vdash s : \text{str}} \text{strI} \\
 \frac{\Gamma \vdash e_1 : A \quad \Gamma \vdash e_2 : B}{\Gamma \vdash (e_1, e_2) : A \times B} \times\text{I} \quad \frac{\Gamma \vdash e : A \times B}{\Gamma \vdash \text{fst } e : A} \times\text{E}_1 \quad \frac{\Gamma \vdash e : A \times B}{\Gamma \vdash \text{snd } e : B} \times\text{E}_2 \\
 \frac{x : A^q \in \Gamma}{\Gamma \vdash x : A} \text{VAR} \quad \frac{\Gamma, x : A^i \vdash e : B}{\Gamma \vdash \lambda x : A. e : A \Rightarrow B} \Rightarrow\text{I} \quad \frac{\Gamma \vdash e_1 : A \Rightarrow B \quad \Gamma \vdash e_2 : A}{\Gamma \vdash e_1 e_2 : B} \Rightarrow\text{E} \\
 \frac{\Gamma \vdash^p e : A}{\Gamma \vdash e : A} \text{CTX-PURE} \quad \frac{\Gamma \vdash^p e : A}{\Gamma \vdash \text{box } e : \square A} \square\text{I} \quad \frac{\Gamma \vdash e_1 : \square A \quad \Gamma, x : A^p \vdash e_2 : B}{\Gamma \vdash \text{let box } x = e_1 \text{ in } e_2 : B} \square\text{E}
 \end{array}$$

Fig. 3. Typing Rules

$$\frac{}{x : A^q \in (\Gamma, x : A^q)} \in\text{-ID} \quad \frac{x : A^q \in \Gamma \quad (x \neq y)}{x : A^q \in (\Gamma, y : B^r)} \in\text{-EX}$$

Fig. 4. Context Membership Rules

3.1 Typing Judgements

We introduce three kinds of judgement forms, as explained in figure 2, and we state our typing rules in figure 3, which we explain below.

We give the standard rules for the context membership judgement in figure 4, following Barendregt's variable convention [Barendregt 1985]. The only difference is that variables now have an extra purity annotation.

We have the usual introduction and elimination rules for constants and products. If a variable is present in the context, we can introduce it, using the VAR rule. In the introduction rule for functions \Rightarrow I, we mark the hypothesis as *impure* when forming a λ -expression, because we do not want to restrict function arguments in general. The elimination rule \Rightarrow E, or function application works as usual. The print statement performs side-effects but has the type unit, as we've already seen. We need to do more work to add the comonadic type constructor.

$(\cdot)^p := \cdot$ $(\Gamma, x : A^p)^p := \Gamma^p, x : A^p$ $(\Gamma, x : A^i)^p := \Gamma^p$	$\langle \rangle^p := \langle \rangle$ $\langle \theta, e^p/x \rangle^p := \langle \theta^p, e^p/x \rangle$ $\langle \theta, e^i/x \rangle^p := \theta^p$
<p>(a) Purify Operation on Contexts</p>	<p>(b) Purify Operation on Substitutions</p>

Fig. 5. Purify Operations

- $\Gamma \supseteq \Delta$ Γ is a weakening of context Δ
- $\Gamma \vdash \theta : \Delta$ θ is a well-formed substitution from context Γ to Δ

Fig. 6. Weakening and Substitution Judgements

We know that we can mark a term as *pure* if it was well-typed in a *pure* context, where every variable has the *p* annotation. So we define a syntactic *purify* operation, which acts on contexts; applying it drops the terms with the *impure* annotation, as shown in figure 5a. This is expressed by the **CTX-PURE** rule, which introduces a *pure* expression using the *pure* judgement form. And then, we can put it in a box using the \Box I rule, to get a \Box -typed value.

We give an elimination rule $\Box E$ using the let box binding form. Given an expression in the \Box type, we let box-bind the underlying *pure* expression to the variable x . With an extended context that has a free variable x marked *pure*, if we can produce a well-typed expression in the motive, the elimination is complete.

3.2 Weakening and Substitution

We define two more judgement forms for weakening and substitution; these are meta-theoretic operations which are only used to state and prove meta-theoretic properties of the language. Note that we *do not* use explicit substitutions, i.e., substitutions do not appear as part of expressions.

3.2.1 Weakening. The context weakening relation follows the usual rules, as shown in figure 7a, with the extra purity annotation on free variables in contexts. The rule \sqsupseteq -WK allows us to drop a hypothesis to weaken the context, and we add the rules \sqsupseteq -ID and \sqsupseteq -CONG to get the smallest congruence closure.

We show that weakening is sound by proving a syntactic weakening lemma.

LEMMA 3.1 SYNTACTIC WEAKENING If $\Gamma \supset \Delta$ and $\Delta \vdash e : A$, then $\Gamma \vdash e : A$

3.2.2 Substitution. Substitution requires an extra bit of work, as we can see in figure 7b. Since our language is effectful, we have the usual rule **SUB-IMPURE** which allows substituting *values* for *impure* variables, as in the call-by-value lambda calculus. We also add another rule **SUB-PURE**, which allows one to substitute *pure expressions* for *pure* variables.

At this point, we can define the syntactic substitution function on raw terms.

Definition 3.2 (Syntactic substitution on variables)

$$\theta[x] := \begin{cases} \emptyset & \theta = \langle \rangle \\ e & \theta = \langle \phi, e^q/x \rangle \\ \phi[x] & \theta = \langle \phi, e^q/y \rangle, x \neq y \end{cases}$$

$$\begin{array}{c}
 \text{344} \quad \frac{}{\cdot \supseteq \cdot} \supseteq\text{-ID} \quad \text{345} \quad \frac{\Gamma \supseteq \Delta}{\Gamma, x : A^q \supseteq \Delta, x : A^q} \supseteq\text{-CONG} \quad \text{346} \quad \frac{\Gamma \supseteq \Delta}{\Gamma, x : A^q \supseteq \Delta} \supseteq\text{-WK} \\
 \text{347} \quad \text{(a) Weakening Rules} \\
 \text{348} \\
 \text{349} \\
 \text{350} \quad \frac{}{\Gamma \vdash \langle \rangle : \cdot} \text{SUB-ID} \\
 \text{351} \\
 \text{352} \\
 \text{353} \quad \frac{\Gamma \vdash \theta : \Delta \quad \Gamma \vdash p e : A}{\Gamma \vdash \langle \theta, e^p/x \rangle : \Delta, x : A^p} \text{SUB-PURE} \quad \text{354} \quad \frac{\Gamma \vdash \theta : \Delta \quad \Gamma \vdash v : A}{\Gamma \vdash \langle \theta, v^i/x \rangle : \Delta, x : A^i} \text{SUB-IMPURE} \\
 \text{355} \\
 \text{356} \quad \text{(b) Substitution Rules} \\
 \text{357} \\
 \text{358} \\
 \text{359} \quad \text{Fig. 7. Weakening and Substitution Rules} \\
 \text{360}
 \end{array}$$

361 *Definition 3.3 (Syntactic substitution on terms).*

$$\begin{aligned}
 \theta(x) &:= \theta[x] \\
 \theta(\langle \rangle) &:= \langle \rangle \\
 \theta(s) &:= s \\
 \theta((e_1, e_2)) &:= (\theta(e_1), \theta(e_2)) \\
 \theta(\text{fst } e) &:= \text{fst } \theta(e) \\
 \theta(\text{snd } e) &:= \text{snd } \theta(e) \\
 \theta(\lambda x. e) &:= \lambda y. \langle \theta, y^i/x \rangle(e) \\
 \theta(e_1 e_2) &:= \theta(e_1) \theta(e_2) \\
 \theta(\text{box } e) &:= \text{box } \boxed{\theta^p(e)} \\
 \theta(\text{let box } \boxed{x} = e_1 \text{ in } e_2) &:= \text{let box } \boxed{y} = \theta(e_1) \text{ in } \langle \theta, y^p/x \rangle(e_2) \\
 \theta(e_1 \cdot \text{print}(e_2)) &:= \theta(e_1) \cdot \text{print}(\theta(e_2))
 \end{aligned}$$

376 When substituting under a binder, we do a renaming of the bound variable by extending the
 377 substitution with an appropriately annotated variable. To substitute inside a box-ed expression,
 378 we have to *purify* the substitution when using it. We extend the *purify* operation to substitutions
 379 as well; it simply drops the *impure* substitutions, as shown in figure 5b.
 380

Finally, we show the soundness of substitution by proving a syntactic substitution theorem.

THEOREM 3.4 SYNTACTIC SUBSTITUTION. *If $\Gamma \vdash \theta : \Delta$ and $\Delta \vdash e : A$, then $\Gamma \vdash \theta(e) : A$.*

4 SEMANTICS

In this section, we sketch a categorical semantics for our language, motivated by an abstract model of capabilities.

4.1 The Object-Capability Model

The *object-capability* model is a methodology originating in the operating systems community for building secure operating systems and hardware. The idea behind this model is that systems must

393 be able to control permissions to perform potentially dangerous or insecure operations, and that
 394 a good way to control access is to tie the right to perform actions to values in a programming lan-
 395 guage, dubbed *capabilities*. Then, the usual variable-binding and parameter-passing mechanisms
 396 of the language can be used to grant rights to perform actions – access to a capability can be pro-
 397 hibited to a client by simply not passing it the capability as an argument. To quote Miller [2006]:

398 Our object-capability model is essentially the untyped call-by-value lambda calculus
 399 with applicative-order local side effects and a restricted form of **eval** – the model
 400 Actors and Scheme are based on. This correspondence of objects, lambda calculus, and
 401 capabilities was noticed several times by 1973.

402 In our kernel language from the previous section, the potentially dangerous operation that must
 403 be controlled is the right to print to a particular channel, and so we take channels as capabilities.
 404 The $c \cdot \text{print}(s)$ operation takes the channel c and prints the string s to it. We can see here how
 405 the print operation uses the channel value to select the channel to print on – in this case, the
 406 output channel is the capability. Of course, program values can possess multiple capabilities – for
 407 example, a list of channels naturally has a capability for each channel in the list, and a closure can
 408 capture channels to perform print actions on. Nevertheless, though, there is no way for a function
 409 to print on a channel that it did not either capture in its environment, or receive as an argument.
 410

411 This property is actually fundamental to the object-capability model, which says that the *only*
 412 way to access capabilities must be through capability values. If this is indeed the case, then the
 413 language is said to be *capability-safe*. However, if there are ways to conjure up capabilities out of
 414 nowhere (e.g., unrestricted filesystem operations in the standard library, or more alarmingly by
 415 casting integers to pointers in C), then reasoning about effects based on capability passing is not
 416 sound. In this case, the language is said to possess *ambient authority*.

418 4.2 Capability Spaces

419 Let \mathcal{C} be a fixed set of capability names, possibly countably infinite. We require that \mathcal{C} have de-
 420 cidable equality. The powerset $\wp(\mathcal{C})$ denotes the set of all subsets of \mathcal{C} , and is a complete lattice
 421 ordered by set inclusion $(\wp(\mathcal{C}); \emptyset, \mathcal{C}, \subseteq)$.

422 A capability space $X = (|X|, w_X)$ is a set $|X|$ with a weight function $w_X : |X| \rightarrow \wp(\mathcal{C})$ that
 423 assigns a set of capabilities to each member in X . Intuitively, we think of the set $|X|$ as the set of
 424 values of the type X , and we think of the weight function w_X as defining the set of capabilities
 425 that each value has access to.

426 We only allow those maps between capability spaces that preserve weights, i.e., a map between
 427 the underlying sets $|X|$ and $|Y|$ is a morphism of capability spaces iff for each x in $|X|$, all the weights
 428 in $|Y|$ for $f(x)$ are contained in the weights in $|X|$ for x . If we think of a function $f : X \rightarrow Y$ as a term
 429 of type Y with a free variable of type X , then this condition ensures that the capabilities of the
 430 term are limited to at most those of its free variables. In other words, weight-preserving functions
 431 are precisely those which are capability-safe; they do not have unauthorised access to arbitrary
 432 capabilities, and they do not have any ambient authority.

433 We now formally define the category of capability spaces \mathcal{C} , with objects as capability spaces
 434 and morphisms as weight-preserving functions.

436 *Definition 4.1 (Category \mathcal{C} of capability spaces).*

$$\begin{aligned} 438 \quad Obj_{\mathcal{C}} &:= X = (|X| : \text{Set}, w_X : |X| \rightarrow \wp(\mathcal{C})) \\ 439 \quad Hom_{\mathcal{C}}(X, Y) &:= \{f \in |X| \rightarrow |Y| \mid \forall x \in |X|, w_Y(f(x)) \subseteq w_X(x)\} \end{aligned}$$

We remark that the definition of this category is inspired by the category of length spaces defined in [Hofmann 2003], which again associates intensional information (in his work, memory usage, and in ours, capabilities) to a set-theoretic semantics.

4.3 Cartesian Closed Structure

We now explain the *cartesian closed* structure of \mathcal{C} .

Definition 4.2 (Terminal Object).

$$\begin{aligned} |1| &:= \{ * \} \\ w_1(*) &:= \emptyset \end{aligned}$$

The terminal object is the usual singleton set, and it has no capabilities. For any object A , the unique map $! : A \rightarrow 1$ is given by $!_A(a) = *$, which is evidently weight preserving.

Definition 4.3 (Product).

$$\begin{aligned} |A \times B| &:= |A| \times |B| \\ w_{A \times B}(a, b) &:= w_A(a) \cup w_B(b) \end{aligned}$$

Products are formed by pairing as usual, and the set of capabilities of a pair of values is the union of their capabilities. The projection maps $\pi_i : A_1 \times A_2 \rightarrow A_i$ are just the projections on the underlying sets, which are weight preserving as well.

Definition 4.4 (Exponential).

$$\begin{aligned} |A \rightarrow B| &:= |A| \rightarrow |B| \\ w_{A \rightarrow B}(f) &:= \left\{ c \in \mathcal{C} \mid \begin{array}{l} \exists a \in |A|, \\ c \in w_B(f(a)), \\ c \notin w_A(a) \end{array} \right\} \end{aligned}$$

Exponentials are given by functions on the underlying sets, but we have to assign capabilities to the closure. We only record those capabilities which are induced by the function, for some value in the domain. The intuition is that if we have a function closure $f : A \rightarrow B$, and for a given value $a \in A$, there is a capability c such that $c \notin w_B(f(a))$, then the closure f must have had access to c in its environment. So by taking the union of all such c over all inputs in the domain, we can bound all the capabilities that f must have access to.

We verify that our definition satisfies the currying isomorphism in lemma 4.5, and we name the currying/uncurrying and evaluation maps. The definitions are the same as in the case of sets, but we additionally have to verify that these maps are weight-preserving.

LEMMA 4.5.

$$\begin{aligned} \text{curry/uncurry} &: \mathcal{H}\text{om}_{\mathcal{C}}(\Gamma \times A, B) \xrightarrow{\sim} \mathcal{H}\text{om}_{\mathcal{C}}(\Gamma, A \rightarrow B) \\ \text{ev}_{A,B} &: \mathcal{H}\text{om}_{\mathcal{C}}(A \rightarrow B \times A, B) \end{aligned}$$

This shows that \mathcal{C} has finite products and exponentials, and is hence a cartesian closed category, which suffices to interpret the simply-typed lambda calculus.

4.4 Monad

Our language supports printing strings along a channel, and to model this effect we will structure our semantics monadically, in the style of Moggi [1991]. To model the print effect, we define a strong monad T on \mathcal{C} as follows, taking the monoid $(\Sigma^*; \varepsilon, \bullet)$ to be the set of strings Σ^* with the empty string ε and string concatenation \bullet .

491 *Definition 4.6 ($T : \mathcal{C} \rightarrow \mathcal{C}$).*

$$\begin{aligned} |T(A)| &:= |A| \times (\mathcal{C} \rightarrow \Sigma^*) \\ w_{T(A)}(a, o) &:= w_A(a) \cup \{ c \in \mathcal{C} \mid o(c) \neq \varepsilon \} \end{aligned}$$

495 This monad is essentially the writer monad: it adds an output function which records the output
496 produced in each channel. The weight of a monadic computation is taken to be the weight of the
497 returned value, unioned with all the channels that *anything* was written to. This corresponds to
498 the intuition that a computation which performs I/O on a channel must possess the capability to
499 do so.

500 *Definition 4.7 (T is a monad).* The unit and multiplication of the monad are defined below, and
501 we state and verify the monad laws in [lemma B.1](#).

$$\begin{aligned} \eta_A : A &\rightarrow TA \\ a &\mapsto (a, \lambda c. \varepsilon) \\ \mu_A : TTA &\rightarrow TA \\ ((a, o_1), o_2) &\mapsto (a, \lambda c. o_2(c) \bullet o_1(c)) \end{aligned}$$

509 *Definition 4.8 (T is a strong monad).* T is strong with respect to products, with a natural family
510 of left and right strengthening maps.

$$\begin{aligned} \tau_{A,B} : A \times TB &\rightarrow T(A \times B) \\ (a, (b, o)) &\mapsto ((a, b), o) \\ \sigma_{A,B} : TA \times B &\rightarrow T(A \times B) \\ ((a, o), b) &\mapsto ((a, b), o) \end{aligned}$$

517 We use this to define the natural map $\beta_{A,B}$, which evaluates a pair of effects, as follows. Notice
518 that it evaluates the effect on the right before the one on the left; we expand more on that
519 in [lemma B.2](#), and verify the appropriate coherences.

520 *Definition 4.9 ($\beta_{A,B} : TA \times TB \rightarrow T(A \times B)$).*

$$\beta_{A,B} := \tau_{TA,B} ; T\sigma_{A,B} ; \mu_{A \times B}$$

524 4.5 Comonad

525 To model the \square type constructor, we define an endofunctor \square on \mathcal{C} below; it filters out values
526 that *do not* possess any capabilities, i.e., values that are *pure*.

528 *Definition 4.10 ($\square : \mathcal{C} \rightarrow \mathcal{C}$).*

$$\begin{aligned} |\square A| &:= \{ a \in |A| \mid w_A(a) = \emptyset \} \\ w_{\square A}(a) &:= w_A(a) = \emptyset \\ \square : \mathcal{H}om_{\mathcal{C}}(A, B) &\rightarrow \mathcal{H}om_{\mathcal{C}}(\square A, \square B) \\ f &\mapsto f \upharpoonright_{|\square A|} \end{aligned}$$

535 On objects, we simply restrict the set to the subset of values that have the empty set \emptyset of capabilities.
536 \square acts on morphisms by restricting the domain of the functions to $|\square A|$. For any morphism f ,
537 since f is a weight-preserving function, we have that $\square(f)$ is a function between sets with empty
538 capabilities, hence it becomes trivially weight-preserving.

540 This type constructor is especially useful at function type $\square(A \rightarrow B)$, since in general the
 541 environment can hold capabilities, and the \square constructor lets us rule those out. We claim that \square
 542 is an idempotent strong monoidal comonad, as follows.

543 *Definition 4.11 (\square is an idempotent comonad).* The counit and comultiplication of the comonad
 544 are the natural families of maps given by the inclusion and the identity maps on the underlying
 545 set. δ is a natural isomorphism making it idempotent. We state and verify the comonad laws
 546 in lemma B.3.

$$\begin{array}{rcl} \varepsilon_A : \square A & \rightarrow & A \\ a & \mapsto & a \\ \delta_A : \square A & \xrightarrow{\sim} & \square \square A \\ a & \mapsto & a \end{array}$$

547 *Definition 4.12 (\square is a strong monoidal functor).* The functor is strong monoidal, in the sense that
 548 it preserves the monoidal structure of both products (and tensors, see the sequel in subsection 4.7).
 549 The identity element is preserved, and we have *natural isomorphisms* given by pairing on the
 550 underlying sets.

$$\begin{array}{rcl} m^I : 1 & \xrightarrow{\sim} & \square 1 \\ * & \mapsto & * \\ m_{A,B}^\times : (\square A \times \square B) & \xrightarrow{\sim} & \square(A \times B) \\ (a, b) & \mapsto & (a, b) \\ m_{A,B}^\otimes : (\square A \otimes \square B) & \xrightarrow{\sim} & \square(A \otimes B) \\ (a, b) & \mapsto & (a, b) \end{array}$$

561 We remark that \square is not a strong comonad, i.e., it does not possess a tensorial strength. This
 562 makes it impossible to evaluate an arbitrary function under the comonad, as seen in section 2.⁵

563 4.6 The Comonad cancels the Monad

564 Finally, we make the following observation. There is an isomorphism ϕ_A , natural in A , where the
 565 comonad cancels the monad. In programming terms, this says that *an effectful computation with*
 566 *no capabilities can perform no effects* – i.e., it is *pure*. Note that this definition works because of the
 567 particular definition of the monad T we chose, in which the weight of a computation includes all
 568 the channels it printed on. Consequently computation of weight zero cannot print on any channel,
 569 and so must be *pure!* As usual, we verify this fact in lemma B.4.

570 *Definition 4.13 ($\phi : \square T \Rightarrow \square$).*

$$\begin{array}{rcl} \phi_A : \square TA & \xrightarrow{\sim} & \square A \\ (a, o) & \mapsto & a \end{array}$$

581 This property is crucial and we will exploit this to manage our syntax: it will be how we justify
 582 treating terms in *pure* contexts as *pure*, without needing a second grammar for *pure* expressions.

583 ⁵For Haskellers, the \square functor is not a Functor, but it is an Applicative!

589 **4.7 Monoidal Closed Structure**

590
 591 While the monad and comonad, together with the cartesian closed structure, suffice to interpret
 592 our language, it is worth noting that the category \mathcal{C} also admits a *monoidal closed* structure.

593 *Definition 4.14 (Tensor product).*

$$594 \quad |A \otimes B| := \{ (a, b) \in |A| \times |B| \mid w_A(a) \cap w_B(b) = \emptyset \}$$

$$595 \quad w_{A \otimes B}(a, b) := w_A(a) \cup w_B(b)$$

596 The tensor product is given by pairing, with unit 1, but it only restricts to pairs whose sets of
 597 capabilities are disjoint. But, this tensor product also enjoys a right adjoint.

598 *Definition 4.15 (Linear exponential).*

$$601 \quad |A \multimap B| := \left\{ f \in |A| \rightarrow |B| \mid \begin{array}{l} \exists C \in \wp(\mathcal{C}), \forall a \in |A|, \\ C \cap w_A(a) = \emptyset \Rightarrow w_B(f(a)) \subseteq C \cup w_A(a) \end{array} \right\}$$

$$605 \quad w_{A \multimap B}(f) := \left\{ c \in \mathcal{C} \mid \begin{array}{l} \exists a \in |A|, \\ c \in w_B(f(a)), \\ c \notin w_A(a) \end{array} \right\}$$

606 The linear exponential works the same way as the exponential, except that we have to restrict it
 607 to satisfy the disjointness condition for the tensor product. We verify that this definition satisfies
 608 the tensor-hom adjunction in [lemma 4.16](#).

612 **LEMMA 4.16.**

$$613 \quad \mathcal{H}om_{\mathcal{C}}(\Gamma \otimes A, B) \cong \mathcal{H}om_{\mathcal{C}}(\Gamma, A \multimap B)$$

614 This supports an interpretation of a *linear* (actually, affine) type theory. The disjointness conditions in the interpretation of tensor product and linear implication are essentially the same as the disjointness conditions in the definition of the separating conjunction $A * B$ and magic wand $A \multimap B$ in separation logic [[Reynolds 2002](#)]. In separation logic, capabilities correspond to ownership of particular memory locations, and in our setting, capabilities correspond to the right to access a channel.

621 Our model reassuringly suggests that operating systems researchers and program verification
 622 researchers both identified the same notion of capability. However, it seems that the fact that these
 623 are *exactly* the same idea was overlooked because OS researchers focused on the cartesian closed
 624 structure, and semanticists focused on the monoidal closed structure!

625 **5 INTERPRETATION**

627 We now interpret the syntax of our language. An important point to note here is that, we only
 628 use the algebraic structure of the category, i.e., we use the *cartesian closed* structure, the *monoidal*
 629 *idempotent comonad*, the *strong monad*, and the *cancellation isomorphism* ϕ ; the proofs of our
 630 theorems use the universal property for each categorical construction. We only need to use the defi-
 631 nition of the monad in the interpretation of print.⁶

632 We adopt some standard notation to work with our categorical combinators.⁷ The sequential
 633 composition of two arrows, in the diagrammatic order, is $f ; g$. The product of morphisms f and g

635 ⁶Our results will still hold if we switched to another category with this structure, we say more about that in [section 8](#).

636 ⁷We sometimes drop the denotation symbol for brevity, i.e., we write $!_{\Gamma}$ instead of $!_{[\Gamma]}$, or δ_{Γ^P} instead of $\delta_{[\Gamma^P]}$.

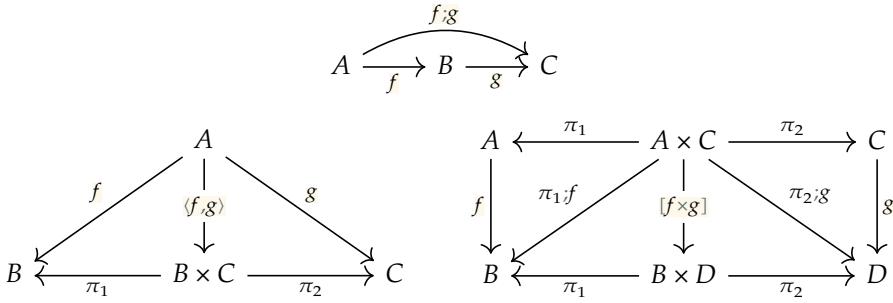


Fig. 8. Composition operations

is $\langle f, g \rangle$ (also called a fork operation in the algebra of programming community [Gibbons 2000]), and $[f \times g]$ is parallel composition with products. We define these using the universal property of products and composition, as shown in figure 8.

5.1 Types and Contexts

We interpret types as objects in \mathcal{C} . Note that we use the monad in the interpretation of functions, following the call-by-value computational lambda-calculus interpretation in [Moggi 1989]. We use the comonad to interpret the \square modality. We pick particular sets Σ^* and \mathcal{C} to interpret strings and capabilities respectively.

Definition 5.1 ($\llbracket A \rrbracket : Obj_{\mathcal{C}}$).

$$\begin{aligned}\llbracket \text{unit} \rrbracket &:= 1 \\ \llbracket \text{str} \rrbracket &:= \Sigma^* \\ \llbracket \text{cap} \rrbracket &:= \mathcal{C} \\ \llbracket A \times B \rrbracket &:= \llbracket A \rrbracket \times \llbracket B \rrbracket \\ \llbracket A \Rightarrow B \rrbracket &:= \llbracket A \rrbracket \rightarrow T[\llbracket B \rrbracket] \\ \llbracket \square A \rrbracket &:= \square[\llbracket A \rrbracket]\end{aligned}$$

We interpret contexts as finite products of objects. The comonad is used to interpret the *pure* variables in the context, while the *impure* variables are just arbitrary objects in \mathcal{C} .

Definition 5.2 ($\llbracket \Gamma \rrbracket : Obj_{\mathcal{C}}$).

$$\begin{aligned}\llbracket \cdot \rrbracket &:= 1 \\ \llbracket \Gamma, x : A^p \rrbracket &:= \llbracket \Gamma \rrbracket \times \square[\llbracket A \rrbracket] \\ \llbracket \Gamma, x : A^i \rrbracket &:= \llbracket \Gamma \rrbracket \times \llbracket A \rrbracket\end{aligned}$$

Now we give an interpretation for the context membership relation.⁸ The judgement $x : A^q \in \Gamma$ is interpreted as a morphism in $\mathcal{H}om_{\mathcal{C}}(\llbracket \Gamma \rrbracket, \llbracket A \rrbracket)$. It projects out the appropriately typed and annotated variable from the product in the context. For *pure* variables, we need to use the counit ε to get out of the comonad.

⁸When interpreting judgements and inference rules, we write $\llbracket \frac{\mathcal{J}_1 \dots \mathcal{J}_n}{\mathcal{J}} \rrbracket$ to mean the interpretation of \mathcal{J} , i.e., we recursively define $\llbracket \mathcal{J} \rrbracket$ under the assumption that we have an interpretation for \mathcal{J}_i , i.e., $\llbracket \mathcal{J}_1 \rrbracket, \dots, \llbracket \mathcal{J}_n \rrbracket$.

687 *Definition 5.3* ($\llbracket x : A^q \in \Gamma \rrbracket : \mathcal{H}om_{\mathcal{C}}(\llbracket \Gamma \rrbracket, \llbracket A \rrbracket)$).

688

$$689 \quad \llbracket \frac{}{x : A^i \in (\Gamma, x : A^i)} \rrbracket := \pi_2 \\ 690$$

691

$$692 \quad \llbracket \frac{}{x : A^p \in (\Gamma, x : A^p)} \rrbracket := \pi_2 ; \varepsilon_A \\ 693$$

$$694 \quad \llbracket \frac{x : A^q \in \Gamma \quad (x \neq y)}{x : A^q \in (\Gamma, y : B^r)} \rrbracket := \pi_1 ; \llbracket x : A^q \in \Gamma \rrbracket \\ 695$$

696

5.2 Expressions

697 We now give an interpretation for expressions $\Gamma \vdash e : A$, and *pure* expressions $\Gamma \vdash^p e : A$. We
698 interpret each typing rule as follows.

700

701 *Definition 5.4* ($\llbracket \Gamma \vdash e : A \rrbracket : \mathcal{H}om_{\mathcal{C}}(\llbracket \Gamma \rrbracket, T \llbracket A \rrbracket)$, $\llbracket \Gamma \vdash^p e : A \rrbracket_p : \mathcal{H}om_{\mathcal{C}}(\llbracket \Gamma \rrbracket, \square \llbracket A \rrbracket)$).

702

$$703 \quad \llbracket \frac{}{\Gamma \vdash () : \text{unit}} \rrbracket := !_{\Gamma} ; \eta_1 \\ 704$$

705

706 To interpret unitI, we use the unique ! map to simply get to the terminal object 1, then lift it into
707 the monad using η , without performing any effects.

708

$$709 \quad \llbracket \frac{\Gamma \vdash e_1 : A \quad \Gamma \vdash e_2 : B}{\Gamma \vdash (e_1, e_2) : A \times B} \rrbracket := \text{let } \begin{cases} f := \llbracket \Gamma \vdash e_1 : A \rrbracket \\ g := \llbracket \Gamma \vdash e_2 : B \rrbracket \end{cases} \\ 710 \quad \text{in } \langle f, g \rangle ; \beta_{A,B} \\ 711$$

712

$$713 \quad \Gamma \xrightarrow{\langle f, g \rangle} TA \times TB \xrightarrow{\beta_{A,B}} T(A \times B) \\ 714$$

715

716 For pair introduction $\times I$, we evaluate both components of the pair, and compose, then use the
717 strength of the monad T with the β combinator to form the product.⁹

718

$$719 \quad \llbracket \frac{\Gamma \vdash e : A \times B}{\Gamma \vdash \text{fst } e : A} \rrbracket := \llbracket \Gamma \vdash e : A \times B \rrbracket ; T\pi_1 \\ 720 \\ 721 \quad \llbracket \frac{\Gamma \vdash e : A \times B}{\Gamma \vdash \text{snd } e : B} \rrbracket := \llbracket \Gamma \vdash e : A \times B \rrbracket ; T\pi_2 \\ 722$$

723

724 We eliminate products using the $\times E_1$ and $\times E_2$ rules. These are interpreted using the corresponding
725 product projection maps, under the functorial action of T .

726

$$727 \quad \llbracket \frac{x : A^q \in \Gamma}{\Gamma \vdash x : A} \rrbracket := \llbracket x : A^q \in \Gamma \rrbracket ; \eta_A \\ 728$$

729

730 Variables are introduced using the VAR rule, which is interpreted by looking up in the context,
731 for which we use the interpretation of our context membership judgement. This is followed by a
732 trivial lifting into the monad.

733

9The vigilant reader will have noticed that β evaluates the pair from right to left, so the action on the right will be performed first, like OCaml! This is also useful when interpreting function application, because we evaluate the argument first.

734

735

736

737

738

739

740

$$\llbracket \frac{\Gamma, x : A^i \vdash e : B}{\Gamma \vdash \lambda x : A. e : A \Rightarrow B} \rrbracket := \text{curry}(\llbracket \Gamma, x : A^i \vdash e : B \rrbracket) ; \eta_{A \rightarrow TB}$$

741

To interpret functions using the \Rightarrow I rule, we simply use the currying map, since our context extension is interpreted as a product. Then we lift it into the monad using η .

742

743

744

745

746

747

748

749

750

751

752

753

$$\llbracket \frac{\Gamma \vdash e_1 : A \Rightarrow B \quad \Gamma \vdash e_2 : A}{\Gamma \vdash e_1 e_2 : B} \rrbracket := \begin{array}{l} \text{let } \begin{cases} f := \llbracket \Gamma \vdash e_1 : A \Rightarrow B \rrbracket \\ g := \llbracket \Gamma \vdash e_2 : A \rrbracket \end{cases} \\ \text{in } \langle f, g \rangle ; \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B \end{array}$$

754

755

756

757

To eliminate functions using the \Rightarrow E rule, we evaluate the operator and operand in an application, followed by a use of the monad strength β to turn it into a pair. Then we use the evaluation map under the functor T to apply the argument. Since the function is effectful, we have to collapse the effects using a μ .

758

759

760

761

762

763

764

765

766

767

768

To interpret the \Box I rule, we need to interpret the pure judgement (defined later), which gives a value of type $\Box A$, and then we lift it into the monad.

769

770

771

772

773

774

775

776

777

778

779

$$\llbracket \frac{\Gamma \vdash p e : A}{\Gamma \vdash \text{box}[e] : \Box A} \rrbracket := \llbracket \Gamma \vdash p e : A \rrbracket_p ; \eta_{\Box A}$$

$$\Gamma \xrightarrow{\llbracket \Gamma \vdash p e : A \rrbracket_p} \Box A \xrightarrow{\eta_{\Box A}} T \Box A$$

$$\llbracket \frac{\Gamma \vdash e_1 : \Box A \quad \Gamma, x : A^p \vdash e_2 : B}{\Gamma \vdash \text{let box}[x] = e_1 \text{ in } e_2 : B} \rrbracket := \begin{array}{l} \text{let } \begin{cases} f := \llbracket \Gamma \vdash e_1 : \Box A \rrbracket \\ g := \llbracket \Gamma, x : A^p \vdash e_2 : B \rrbracket \end{cases} \\ \text{in } \langle id_\Gamma, f \rangle ; \tau_{\Gamma, \Box A} ; Tg ; \mu_B \end{array}$$

$$\Gamma \xrightarrow{\langle id_\Gamma, f \rangle} \Gamma \times T \Box A \xrightarrow{\tau_{\Gamma, \Box A}} T(\Gamma \times \Box A) \xrightarrow{Tg} T^2 B \xrightarrow{\mu_B} TB$$

780

781

782

783

To eliminate a box-ed value using the \Box E rule, we first evaluate f , which gives a value of type $\Box A$, but under the monad T . We can use it to introduce a *pure* variable in the context, but we use the strength of the monad to shift the product under the T and get an extended context. We evaluate g under this extended context, and then use a μ to collapse the effects.

784

$$\begin{array}{ll}
\rho(\cdot) := id_1 & \mathcal{M}(\cdot) := id_1 \\
\rho(\Gamma, x : A^p) := [\rho(\Gamma) \times id_{\square A}] & \mathcal{M}(\Gamma, x : A^p) := [\mathcal{M}(\Gamma) \times \delta_A] ; m_{\Gamma^p, \square A}^x \\
\rho(\Gamma, x : A^i) := \pi_1 ; \rho(\Gamma) & \mathcal{M}(\Gamma, x : A^i) := \mathcal{M}(\Gamma)
\end{array}$$

(a) $\rho(\Gamma) : \mathcal{H}\text{om}_{\mathcal{C}}([\Gamma], [\Gamma^p])$ (b) $\mathcal{M}(\Gamma) : \mathcal{H}\text{om}_{\mathcal{C}}([\Gamma^p], \square[\Gamma^p])$

Fig. 9. $\rho(\Gamma)$ and $\mathcal{M}(\Gamma)$

$$\frac{\Gamma \vdash e_1 : \text{cap} \quad \Gamma \vdash e_2 : \text{str}}{\Gamma \vdash e_1 \cdot \text{print}(e_2) : \text{unit}} = \text{let } \left\{ \begin{array}{l} f := [\Gamma \vdash e_1 : \text{cap}] \\ g := [\Gamma \vdash e_2 : \text{str}] \\ p : \mathcal{C} \times \Sigma^* \rightarrow T1 \\ (c, s) \mapsto (*, \lambda c'. \begin{cases} s & \text{if } c = c' \\ \varepsilon & \text{otherwise} \end{cases}) \end{array} \right. \text{in } \langle f, g \rangle ; \beta_{\mathcal{C}, \Sigma^*} ; Tp ; \mu_1$$

Finally, to interpret the PRINT rule, we need to perform a non-trivial effect. We define the function p which builds an output function that records the output on channels. Given any channel c and string s , it returns a value of type $T1$ containing the trivial value $*$; the output function instantiates a channel c' and tests equality with c – if it equals c , we record the string s , otherwise we just choose the empty string ε . We interpret the arguments of print and apply them to p to evaluate it.¹⁰ The rest of the interpretation is similar to the one for $\Rightarrow E$, with output type 1.

$$\Gamma \xrightarrow{\langle f, g \rangle} T\mathcal{C} \times T\Sigma^* \xrightarrow{\beta_{\mathcal{C}, \Sigma^*}} T(\mathcal{C} \times \Sigma^*) \xrightarrow{Tp} T^2 1 \xrightarrow{\mu_1} T1$$

We used a different interpretation function for *pure* expressions, which we define below. We need to interpret the *purify* operation p on contexts, for which we define the map $\rho(\Gamma)$ in figure 9a. We also need another combinator $\mathcal{M}(\Gamma)$, defined in figure 9b, which uses the monoidal action and the idempotence of the comonad \square to distribute the \square over the products in Γ . Note that $\mathcal{M}(\Gamma)$ is an isomorphism because m and δ are.

Now, the interpretation function for pure expressions $\Gamma \vdash^p e : A$ uses the CTX-PURE rule, and is defined as a morphism in $\mathcal{H}\text{om}_{\mathcal{C}}([\Gamma], \square[A])$.

$$\frac{\Gamma^p \vdash e : A}{\Gamma \vdash^p e : A} \xrightarrow{p} \rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square[\Gamma^p \vdash e : A] ; \phi_A$$

$$\Gamma \xrightarrow{\rho(\Gamma)} \Gamma^p \xrightarrow{\mathcal{M}(\Gamma)} \square \Gamma^p \xrightarrow{\square[\Gamma^p \vdash e : A]} \square TA \xrightarrow{\phi_A} \square A$$

We *purify* the context to a *pure* one, so that we can evaluate the expression. However, we need a value in $\square A$, but the expression interpretation would produce something in TA . Now, we can

¹⁰We have quietly elided the interpretation of the strI rule so far. It is simply given by $\square[\Gamma \vdash s : \text{str}] := !_{\Gamma} ; s ; \eta_{\Sigma^*}$, where $s : 1 \rightarrow \Sigma^*$ is the global element that picks out the string literal s in Σ^* .

834 only cancel the monad under the comonad, so we use the $\mathcal{M}(\Gamma)$ map which uses the idempotence
 835 of \square to do a readjustment. We can now evaluate the expression under the \square in the *pure* context,
 836 which gives a monadic value of type TA under the comonad \square . We can finally use ϕ to cancel the
 837 monad T under the \square .

838
 839 **5.3 Weakening and Substitution**
 840 We now give semantics for syntactic weakening and substitution.
 841

842 *5.3.1 Weakening.* For contexts Γ and Δ , we interpret the weakening judgement $\Gamma \supseteq \Delta$ as a mor-
 843 phism in $\mathcal{H}\text{om}_{\mathcal{C}}([\Gamma], [\Delta])$. We also refer to it as the weakening map $\text{Wk}(\Gamma \supseteq \Delta)$.
 844

845 *Definition 5.5* ($\text{Wk}(\Gamma \supseteq \Delta) := [[\Gamma \supseteq \Delta]] : \mathcal{H}\text{om}_{\mathcal{C}}([\Gamma], [\Delta])$).
 846

$$\begin{aligned} [[\frac{}{\cdot \supseteq \cdot}]] &:= id_1 \\ [[\frac{\Gamma \supseteq \Delta}{\Gamma, x : A^q \supseteq \Delta}]] &:= \pi_1 ; [[\Gamma \supseteq \Delta]] \\ [[\frac{\Gamma \supseteq \Delta}{\Gamma, \textcolor{blue}{x : A^p} \supseteq \Delta, \textcolor{blue}{x : A^p}}]] &:= [[[\Gamma \supseteq \Delta]] \times id_{\square A}] \\ [[\frac{\Gamma \supseteq \Delta}{\Gamma, \textcolor{violet}{x : A^i} \supseteq \Delta, \textcolor{violet}{x : A^i}}]] &:= [[[\Gamma \supseteq \Delta]] \times id_A] \end{aligned}$$

858 We prove a semantic weakening lemma, analogous to the [syntactic weakening lemma 3.1](#).
 859

860 **LEMMA 5.6 SEMANTIC WEAKENING.** *If $\Gamma \supseteq \Delta$ and $\Delta \vdash e : A$, then*

$$[[\Gamma \vdash e : A]] = \text{Wk}(\Gamma \supseteq \Delta) ; [[\Delta \vdash e : A]].$$

864
 865 *5.3.2 Substitution.* We now interpret a substitution $\Gamma \vdash \theta : \Delta$ as a morphism in $\mathcal{H}\text{om}_{\mathcal{C}}([\Gamma], [\Delta])$.
 866 However, this is not a trivial iteration of the expression interpretation. The reason is that the
 867 interpretation of contexts in [definition 5.2](#) interprets a variable $x : A^i$ in the context as an element
 868 of the type $[A]$, and a variable $x : A^p$ as an element of the type $\square [A]$. However, an expression
 869 $\Gamma \vdash e : A$ will be interpreted as a morphism in $\mathcal{H}\text{om}_{\mathcal{C}}([\Gamma], T[A])$. Operationally, we resolve
 870 this mismatch by only substituting *values* for variables in call-by-value languages, and indeed our
 871 definition of substitutions in [figure 7b](#) restricts the definition of substitution to range over values
 872 in the rule **SUB-IMPURE**.

873 Therefore, we mimic this syntactic restriction in the semantics, by giving a separate interpreta-
 874 tion only for values, interpreting the judgement $\Gamma \vdash v : A$ as a morphism in $\mathcal{H}\text{om}_{\mathcal{C}}([\Gamma], [A])$.
 875 Note in particular that the value interpretation yields an element of $[A]$, as the context interpreta-
 876 tion requires, rather than an element of $T[A]$. This value interpretation makes use of the ex-
 877 pression interpretation in the interpretation of λ -expressions, but the expression relation does not
 878 directly refer to the value interpretation. There are alternative presentations such as fine-grained
 879 call-by-value [[Levy et al. 2003](#)], which have a separate syntactic class of values and value judge-
 880 ments, and hence make the value and expression interpretations mutually recursive. However, we
 881 choose not to do that in order to remain close to the usual presentation.

883 *Definition 5.7* ($\llbracket \Gamma \vdash v : A \rrbracket_v : \mathcal{H}om_{\mathcal{C}}(\llbracket \Gamma \rrbracket, \llbracket A \rrbracket)$).

$$\begin{aligned} 885 \quad \llbracket \frac{}{\Gamma \vdash () : \text{unit}} \rrbracket_v &:= !_{\Gamma} \\ 886 \\ 887 \quad \llbracket \frac{\Gamma \vdash v_1 : A \quad \Gamma \vdash v_2 : B}{\Gamma \vdash (v_1, v_2) : A \times B} \rrbracket_v &:= \langle \llbracket \Gamma \vdash v_1 : A \rrbracket_v, \llbracket \Gamma \vdash v_2 : B \rrbracket_v \rangle \\ 888 \\ 889 \quad \llbracket \frac{x : A^q \in \Gamma}{\Gamma \vdash x : A} \rrbracket_v &:= \llbracket x : A^q \in \Gamma \rrbracket \\ 890 \\ 891 \quad \llbracket \frac{\Gamma, x : A^i \vdash e : B}{\Gamma \vdash \lambda x : A. e : A \Rightarrow B} \rrbracket_v &:= \text{curry}(\llbracket \Gamma, x : A^i \vdash e : B \rrbracket) \\ 892 \\ 893 \quad \llbracket \frac{\Gamma \vdash^p e : A}{\Gamma \vdash \text{box}[e] : \square A} \rrbracket_v &:= \llbracket \Gamma \vdash^p e : A \rrbracket_p \end{aligned}$$

897 Note that $\text{box } [e]$ expressions are also values, and our *pure* interpretation does the right thing
898 for box values, since the interpretation of $\square A$ uses the comonad, $\square[\llbracket A \rrbracket]$. With the interpretation
899 of values in hand, we can define the substitution interpretation as follows.

901 *Definition 5.8* ($\llbracket \Gamma \vdash \theta : \Delta \rrbracket : \mathcal{H}om_{\mathcal{C}}(\llbracket \Gamma \rrbracket, \llbracket \Delta \rrbracket)$).

$$\begin{aligned} 903 \quad \llbracket \frac{}{\Gamma \vdash \langle \rangle : \cdot} \rrbracket &:= !_{\Gamma} \\ 904 \\ 905 \quad \llbracket \frac{\Gamma \vdash \theta : \Delta \quad \Gamma \vdash^p e : A}{\Gamma \vdash \langle \theta, e^p / x \rangle : \Delta, x : A^p} \rrbracket &:= \langle \llbracket \Gamma \vdash \theta : \Delta \rrbracket, \llbracket \Gamma \vdash^p e : A \rrbracket_p \rangle \\ 906 \\ 907 \quad \llbracket \frac{\Gamma \vdash \theta : \Delta \quad \Gamma \vdash v : A}{\Gamma \vdash \langle \theta, v^i / x \rangle : \Delta, x : A^i} \rrbracket &:= \langle \llbracket \Gamma \vdash \theta : \Delta \rrbracket, \llbracket \Gamma \vdash v : A \rrbracket_v \rangle \end{aligned}$$

909 We use the *pure* expression interpretation to interpret **SUB-PURE**, and the *impure* value interpretation
910 for **SUB-IMPURE**.

912 Finally, we prove the semantic analogue of the [syntactic substitution theorem 3.4](#). We prove two
913 auxiliary lemmas 5.9 and 5.10, characterising the expression interpretation of *pure expressions* and
914 *impure values*. The lemmas show that the interpretation for each ends in a trivial lifting into the
915 monad T using η . This makes the proof of the [semantic substitution theorem 5.11](#) possible.

917 **LEMMA 5.9** **PURE INTERPRETATION.** *If $\Gamma \vdash^p e : A$, then*

$$\llbracket \Gamma \vdash e : A \rrbracket = \llbracket \Gamma \vdash^p e : A \rrbracket_p ; \varepsilon_A ; \eta_A.$$

920 **LEMMA 5.10** **VALUE INTERPRETATION.** *If $\Gamma \vdash v : A$, then*

$$\llbracket \Gamma \vdash v : A \rrbracket = \llbracket \Gamma \vdash v : A \rrbracket_v ; \eta_A.$$

923 **THEOREM 5.11** **SEMANTIC SUBSTITUTION.** *If $\Gamma \vdash \theta : \Delta$ and $\Delta \vdash e : A$, then*

$$\llbracket \Gamma \vdash \theta(e) : A \rrbracket = \llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash e : A \rrbracket$$

926 6 EQUATIONAL THEORY

928 Since we have an extension of the *pure* call-by-value simply-typed lambda calculus, we want
929 the usual $\beta\eta$ -equations to hold in our theory. However, we also have the new expression forms
930 for the \square type. We want computation and extensionality rules for the box form and the let box

```

932 EVALUATION CONTEXTS  $\mathcal{C} ::= [\cdot] \mid e \mathcal{C} \mid \mathcal{C} e \mid \lambda x : A. \mathcal{C}$ 
933 | fst  $\mathcal{C}$  | snd  $\mathcal{C}$  |  $(e, \mathcal{C})$  |  $(\mathcal{C}, e)$ 
934 | box  $\boxed{\mathcal{C}}$  | let box  $\boxed{x} = \mathcal{C}$  in  $e$  | let box  $\boxed{x} = e$  in  $\mathcal{C}$ 
935  $\mathcal{E} ::= [\cdot] \mid e \mathcal{E} \mid \mathcal{E} v$ 
936 | fst  $\mathcal{E}$  | snd  $\mathcal{E}$  |  $(e, \mathcal{E})$  |  $(\mathcal{E}, v)$ 
937 | let box  $\boxed{x} = \mathcal{E}$  in  $e$  | let box  $\boxed{x} = v$  in  $\mathcal{E}$ 
938

```

Fig. 10. Grammar extended with Evaluation Contexts

$\Gamma \vdash e_1 \approx e_2 : A$ e_1 and e_2 are equal expressions of type A in context Γ

Fig. 11. Equality Judgements

binding form, and to handle the commuting conversions [Girard et al. 1989], we use evaluation contexts.

We extend our grammar with two kinds of evaluation contexts — a *pure* evaluation context \mathcal{C} , and an *impure* evaluation context \mathcal{E} , as shown in figure 10. The intuition is that \mathcal{E} allows safe reductions for impure expressions, i.e., it picks out the contexts consistent with the evaluation order of the call-by-value simply-typed lambda calculus. The *pure* evaluation context \mathcal{C} allows redexes in every sub-expression; but it is restricted only to *pure* expressions. The hole $[\cdot]$ is the empty evaluation context. We use the notation $\mathcal{C}\langle e \rangle$ or $\mathcal{E}\langle e \rangle$ to indicate that we're replacing the hole in the respective evaluation context with e .

We define a judgement form for equality of terms, as shown in figure 11, and state the rules for the equational theory in figure 12. The usual `REFL`, `SYM`, and `TRANS` rules give the reflexive, symmetric, and transitive closure, so that the equality relation is an equivalence. We also give `CONG` rules for each term former, which makes the relation a congruence closure.

We have the computation rules $\times_1 \beta$ and $\times_2 \beta$ for pairs; we only allow values for these rules. The $\times \eta$ rule is the extensionality rule for pairs, but again, restricted to values.

The $\Rightarrow \beta$ rule is the usual call-by-value computation rule for an application of a λ -expression to an argument.¹¹ Since the calculus has effects, we only allow the operand to be a value. For example, consider the function $f := \lambda x : \text{unit}. x ; x$. We can safely β -reduce $f ()$ to $() ; ()$, but allowing a β -reduction for $f (c \cdot \text{print}(s))$ would duplicate the effect!

We add η rules for functions, but we need to be careful because we have effects. For example, consider the expression $f := c \cdot \text{print}(s) ; \lambda x. x$. On η -expansion, we get $g := \lambda y. f y$, but now the `print` operation is suspended in the closure, and doesn't evaluate when we apply g . Hence, we add two forms of η rules for functions — the $\Rightarrow \eta$ -**IMPURE** rule only allows η -expansion for values, and the $\Rightarrow \eta$ -**PURE** rule allows η -expansion also for expressions that are *pure*.

The computation rule $\boxed{\beta}$ for the $\boxed{\cdot}$ type allows computation under the `let box` binder. If we bind a box-ed expression under the `let box` binder, we can substitute the underlying expression in the motive. This is safe because e_1 is forced to be a *pure* expression.

Finally, we have the η expansion rules for the $\boxed{\cdot}$ type, which pushes an expression in an evaluation context under a `let box` binder. The $\boxed{\eta}$ -**PURE** rule uses the *pure* evaluation context \mathcal{C} , while the $\boxed{\eta}$ -**IMPURE** rule uses the *impure* evaluation context \mathcal{E} . The only difference in the rules is that the \mathcal{C} evaluation context can be plugged with *pure* expressions only.

¹¹The notation $[v/x]e$ is shorthand for $\langle \langle \Gamma \rangle, v^i/x \rangle(e)$ where $\langle \Gamma \rangle$ is the identity substitution $\Gamma \vdash \langle \Gamma \rangle : \Gamma$.

$$\begin{array}{c}
981 \quad \frac{\Gamma \vdash e : A}{\Gamma \vdash e \approx e : A} \text{ REFL} \quad \frac{\Gamma \vdash e_1 \approx e_2 : A}{\Gamma \vdash e_2 \approx e_1 : A} \text{ SYM} \quad \frac{\Gamma \vdash e_1 \approx e_2 : A \quad \Gamma \vdash e_2 \approx e_3 : A}{\Gamma \vdash e_1 \approx e_3 : A} \text{ TRANS} \\
982 \\
983 \\
984 \\
985 \quad \frac{\Gamma \vdash e_1 \approx e_2 : A \times B}{\Gamma \vdash \text{fst } e_1 \approx \text{fst } e_2 : A} \text{ fst -CONG} \quad \frac{\Gamma \vdash e_1 \approx e_2 : A \times B}{\Gamma \vdash \text{snd } e_1 \approx \text{snd } e_2 : B} \text{ snd -CONG} \\
986 \\
987 \\
988 \quad \frac{\Gamma \vdash e_1 \approx e_2 : A \quad \Gamma \vdash e_3 \approx e_4 : B}{\Gamma \vdash (e_1, e_3) \approx (e_2, e_4) : A \times B} \text{ PAIR-CONG} \quad \frac{\Gamma, x : A^i \vdash e_1 \approx e_2 : B}{\Gamma \vdash \lambda x : A. e_1 \approx \lambda x : A. e_2 : A \Rightarrow B} \text{ } \lambda\text{-CONG} \\
989 \\
990 \\
991 \quad \frac{\Gamma \vdash e_1 \approx e_2 : A \Rightarrow B \quad \Gamma \vdash e_3 \approx e_4 : A}{\Gamma \vdash e_1 e_3 \approx e_2 e_4 : B} \text{ APP-CONG} \quad \frac{\Gamma^p \vdash e_1 \approx e_2 : A}{\Gamma \vdash \text{box } \boxed{e_1} \approx \text{box } \boxed{e_2} : \Box A} \text{ box-CONG} \\
992 \\
993 \\
994 \\
995 \quad \frac{\Gamma \vdash e_1 \approx e_2 : \Box A \quad \Gamma, x : A^p \vdash e_3 \approx e_4 : B}{\Gamma \vdash (\text{let box } \boxed{x} = e_1 \text{ in } e_3) \approx (\text{let box } \boxed{x} = e_2 \text{ in } e_4) : B} \text{ let box-CONG} \\
996 \\
997 \\
998 \quad \frac{\Gamma \vdash e_1 \approx e_2 : \text{cap} \quad \Gamma \vdash e_3 \approx e_4 : \text{str}}{\Gamma \vdash e_1 \cdot \text{print}(e_3) \approx e_2 \cdot \text{print}(e_4) : \text{unit}} \text{ print-CONG} \\
999 \\
1000 \\
1001 \\
1002 \quad \text{Fig. 12. Equational Theory}
\end{array}$$

1003 We prove that our equality rules are sound with respect to our categorical semantics. If two
1004 expressions are equal in the equational theory, they have equal interpretations in the semantics.
1005

1006 **THEOREM 6.1** SOUNDNESS OF \approx . *If $\Gamma \vdash e_1 \approx e_2 : A$, then $\llbracket \Gamma \vdash e_1 : A \rrbracket = \llbracket \Gamma \vdash e_2 : A \rrbracket$.*

1007 7 EMBEDDING

1008 Our language is an extension of the *pure* call-by-value simply-typed lambda calculus. But how
1009 could we claim that it is really an *extension*? In this section, we show that we can *embed* the simply-
1010 typed lambda calculus into our calculus, while still preserving its nice properties.

1011 We give the grammar and judgements in figures 13a and 13b, typing rules in figure 13c, and the
1012 $\beta\eta$ -equational theory in figure 13d, for the *pure* call-by-value simply-typed lambda calculus. Note
1013 that we choose to use the base type unit, and we leave out products because their embedding is
1014 trivial and uninteresting for our purpose.

1015 Now, we define an embedding function from the simply-typed lambda calculus to our calculus.
1016 We use the notation \boxed{X} to denote the embedding of a raw syntactic object X from STLC into our
1017 calculus. We give the syntactic translation of types, contexts, and raw terms in figure 14.

1018 To embed the function type, we embed the domain and codomain, but we apply our comonadic
1019 type constructor \Box to restrict the domain to a *pure* type. This embedding is quite like the Gödel-
1020 McKinsey-Tarski embedding of the intuitionistic propositional calculus into classical S4 modal
1021 logic, as outlined in [McKinsey and Tarski 1948], but we do not need to apply the \Box type construc-
1022 tor on the codomain, because our functions are *capability-safe*. We remark that this is similar to
1023 the embedding of lax logic into S4 modal logic described in [Pfenning and Davies 2001], as well as
1024 the embedding of intuitionistic logic into linear logic [Girard 1987].

$$\begin{array}{c}
1030 \quad \frac{\Gamma \vdash v_1 : A \quad \Gamma \vdash v_2 : B}{\Gamma \vdash \text{fst}(v_1, v_2) \approx v_1 : A} \times_1 \beta \quad \frac{\Gamma \vdash v_1 : A \quad \Gamma \vdash v_2 : B}{\Gamma \vdash \text{snd}(v_1, v_2) \approx v_2 : B} \times_2 \beta \\
1031 \\
1032 \\
1033 \\
1034 \quad \frac{\Gamma \vdash v : A \times B}{\Gamma \vdash v \approx (\text{fst } v, \text{snd } v) : A \times B} \times \eta \\
1035 \\
1036 \\
1037 \quad \frac{\Gamma, x : A^i \vdash e : B \quad \Gamma \vdash v : A}{\Gamma \vdash (\lambda x : A. e) v \approx [v/x]e : B} \Rightarrow \beta \\
1038 \\
1039 \\
1040 \quad \frac{\Gamma \vdash v : A \Rightarrow B}{\Gamma \vdash v \approx \lambda x : A. v x : A \Rightarrow B} \Rightarrow \eta\text{-IMPURE} \quad \frac{\Gamma \vdash p e : A \Rightarrow B}{\Gamma \vdash e \approx \lambda x : A. e x : A \Rightarrow B} \Rightarrow \eta\text{-PURE} \\
1041 \\
1042 \\
1043 \\
1044 \quad \frac{\Gamma^p \vdash e_1 : A \quad \Gamma, x : A^p \vdash e_2 : B}{\Gamma \vdash \text{let box } \boxed{x} = \text{box } \boxed{e_1} \text{ in } e_2 \approx [e_1/x]e_2 : B} \square \beta \\
1045 \\
1046 \\
1047 \quad \frac{\Gamma \vdash p e : \square A \quad \Gamma \vdash C\langle\langle e \rangle\rangle : B \quad \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } C\langle\langle \text{box } \boxed{x} \rangle\rangle : B}{\Gamma \vdash C\langle\langle e \rangle\rangle \approx \text{let box } \boxed{x} = e \text{ in } C\langle\langle \text{box } \boxed{x} \rangle\rangle : B} \square \eta\text{-PURE} \\
1048 \\
1049 \\
1050 \quad \frac{\Gamma \vdash e : \square A \quad \Gamma \vdash E\langle\langle e \rangle\rangle : B \quad \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } E\langle\langle \text{box } \boxed{x} \rangle\rangle : B}{\Gamma \vdash E\langle\langle e \rangle\rangle \approx \text{let box } \boxed{x} = e \text{ in } E\langle\langle \text{box } \boxed{x} \rangle\rangle : B} \square \eta\text{-IMPURE} \\
1051 \\
1052 \\
1053 \\
1054 \quad \text{Fig. 12. Equational Theory}
\end{array}$$

1055
 1056
 1057 TYPES $A, B ::= \text{unit} \mid A \Rightarrow B$
 1058 TERMS $e ::= () \mid x \mid \lambda x : A. e \mid e_1 e_2$
 1059 VALUES $v ::= () \mid x \mid \lambda x : A. e$
 1060 CONTEXTS $\Gamma, \Delta, \Psi ::= \cdot \mid \Gamma, x : A$

(a) Grammar for STLC

1061
 1062
 1063 $x : A \in \Gamma$ x is a variable of type A in context Γ
 1064 $\Gamma \vdash_\lambda e : A$ e is an expression of type A in context Γ
 1065 $\Gamma \vdash_\lambda e_1 \approx e_2 : A$ e_1 and e_2 are equal expressions of type A in context Γ
 1066

(b) Judgements for STLC

1067
 1068
 1069
 1070 When embedding contexts, we mark the variables as *pure* using the p annotation. To embed
 1071 functions and applications, we need to use the introduction and elimination forms for \square . When
 1072 embedding a λ -expression, the bound variable is embedded as a term of \square type, so we eliminate
 1073 the underlying variable using the let box binding form before using it in the body. To embed an
 1074 application, we simply put the argument in a box.

1075 We show that this translation is type preserving, i.e., well-typed expressions embed to well-
 1076 typed expressions, and the type translation is preserved. Then, we show that the $\beta\eta$ -equational
 1077 theory of the *pure* call-by-value simply-typed lambda calculus is preserved under the translation. If
 1078

$$\begin{array}{c}
 \frac{}{\Gamma \vdash_{\lambda} () : \text{unit}} \text{unitI} \quad \frac{x : A \in \Gamma}{\Gamma \vdash_{\lambda} x : A} \text{VAR} \\
 \frac{\Gamma, x : A \vdash_{\lambda} e : B}{\Gamma \vdash_{\lambda} \lambda x : A. e : A \Rightarrow B} \Rightarrow_{\text{I}} \quad \frac{\Gamma \vdash_{\lambda} e_1 : A \Rightarrow B \quad \Gamma \vdash_{\lambda} e_2 : A}{\Gamma \vdash_{\lambda} e_1 e_2 : B} \Rightarrow_{\text{E}}
 \end{array}$$

(c) Typing rules for STLC

$$\begin{array}{c}
 \frac{\Gamma \vdash_{\lambda} e : A}{\Gamma \vdash_{\lambda} e \approx e : A} \text{REFL} \quad \frac{\Gamma \vdash_{\lambda} e_1 \approx e_2 : A}{\Gamma \vdash_{\lambda} e_2 \approx e_1 : A} \text{SYM} \\
 \frac{\Gamma \vdash_{\lambda} e_1 \approx e_2 : A \quad \Gamma \vdash_{\lambda} e_2 \approx e_3 : A}{\Gamma \vdash_{\lambda} e_1 \approx e_3 : A} \text{TRANS} \quad \frac{\Gamma, x : A \vdash_{\lambda} e_1 \approx e_2 : B}{\Gamma \vdash_{\lambda} \lambda x : A. e_1 \approx \lambda x : A. e_2 : A \Rightarrow B} \lambda\text{-CONG} \\
 \frac{\Gamma \vdash_{\lambda} e_1 \approx e_2 : A \Rightarrow B \quad \Gamma \vdash_{\lambda} e_3 \approx e_4 : A}{\Gamma \vdash_{\lambda} e_1 e_3 \approx e_2 e_4 : B} \text{APP-CONG}
 \end{array}$$

(d) Equational Theory for STLC

Fig. 13. The *pure* call-by-value simply-typed lambda calculus

$$\begin{array}{ll}
 \text{TYPES} & \text{unit} := \text{unit} \\
 & \boxed{A \Rightarrow B} := \boxed{A} \Rightarrow \boxed{B} \\
 \text{CONTEXTS} & \boxed{\cdot} := \cdot \\
 & \boxed{\Gamma, x : A} := \boxed{\Gamma, x : A}^p \\
 \text{TERMS} & \boxed{()} := () \\
 & \boxed{x} := x \\
 & \boxed{\lambda x : A. e} := \lambda z : \boxed{A}. \text{let box } \boxed{x} = z \text{ in } \boxed{e} \\
 & \boxed{e_1 e_2} := \boxed{e_1} \text{ box } \boxed{e_2}
 \end{array}$$

Fig. 14. Embedding STLC

two expressions are equal in the simply-typed lambda calculus, they *remain equal* after embedding into our imperative calculus.

THEOREM 7.1 TYPE PRESERVATION. *If $\Gamma \vdash_{\lambda} e : A$, then $\Gamma \vdash e : A$.*

THEOREM 7.2 EQUALITY PRESERVATION. *If $\Gamma \vdash_{\lambda} e_1 \approx e_2 : A$, then $\Gamma \vdash e_1 \approx e_2 : A$.*

Finally, we show that our imperative calculus is a conservative extension of the simply-typed lambda calculus. To do so, we claim that if two embedded terms are equal in the extended theory, then they must have been equal in the smaller theory. This shows that the equational theory of the imperative calculus does not introduce any extra equations that would destroy the computational properties of the *pure* simply-typed lambda calculus.

THEOREM 7.3 CONSERVATIVE EXTENSION. *If $\Gamma \vdash_{\lambda} e_1 : A$, $\Gamma \vdash_{\lambda} e_2 : A$, and $\Gamma \vdash e_1 \approx e_2 : A$, then $\Gamma \vdash_{\lambda} e_1 \approx e_2 : A$.*

8 DISCUSSION AND FUTURE WORK

There has been a vast amount of work on integrating effects into purely functional languages. Ironically though, even the very definition of what a purely functional language is has historically been a contested one. Sabry [1998] proposed that a functional language is pure when its behaviour under different evaluation strategies is “morally” the same, in the sense of Danielsson et al. [2006]. That is, if changing the evaluation strategy from call-by-value to (say) call-by-need could only change the divergence/error behaviour of programs in a language, then the language is pure. In contrast, the definition we use in this paper is less sophisticated: we take purity to be the preservation of the $\beta\eta$ equational theory of the simply-typed lambda calculus. However, it lets us prove the correctness of our embedding in an appealingly simple way, by translating derivations of equality.

The use of substructural type systems to control access to mutable data is a long-running theme in the development of programming languages. It is so long-running, in fact, that it actually predates linear logic [Girard 1987] by nearly a decade! Reynolds’ Syntactic Control of Interference [Reynolds 1978] proposed using a substructural type discipline to prevent aliased access to data structures. The intuition that substructural logic corresponds to ownership of capabilities is also a very old one – O’Hearn [1993] uses it to explain his model of SCI, and Crary et al. [1999] compare their static capabilities to the capabilities in the HYDRA system of Wulf et al. [1974].

However, these comparisons remained informal, due to the fact that semanticists tended to use capabilities in a substructural fashion (e.g., see [Crary et al. 1999; Terauchi and Aiken 2006]), but from the very outset ([Dennis and Horn 1966]) to modern day applications like capability-safe Javascript [Maffei et al. 2010], systems designers have tended to use capabilities *non-linearly*. In particular, they thought it was desirable for a principal to hand a capability to two different deputies, which is a design principle obviously incompatible with linearity.

The idea that the linear implication and intuitionistic implication could coexist, without one reducing to the other, first arose in the logic of bunched implications [O’Hearn and Pym 1999]. This led to separation logic [Reynolds 2002], which has been very successful at verifying programs with aliasable state. However, even though the semantics of separation logic supports BI, the bulk of the tooling infrastructure for separation logic (such as Smallfoot [Berdine et al. 2006]) have focused on the substructural fragment, often even omitting anything not in the linear fragment.

However, one observation very important to our work did arise from work on separation logic. Dodds et al. [2009] made the critical observation that in addition to being able to assert ownership, it is extremely useful to be able to *deny* the ownership of a capability. Basically, knowing that a client program *lacks* a capability can make it safe to invoke it in a secure context.

The idea that denial has comonadic structure was also known informally: it arises in the work of [Morrisett et al. 2005], where the exponential comonad in linear logic is modelled as the *lack* of any heap ownership; and in an intuitionistic context, the work on functional reactive programming [Krishnaswami 2013] used a capability to create temporal values, and a comonad denying

1177 ownership of it permitted writing space-leak-free reactive programs. However, both of these papers
 1178 used operational unary logical relations models, and so did not prove anything about the
 1179 equational theory.

1180 Equational theories are easier to get with denotational models, and our model derives from
 1181 the work of Hofmann [2003]. In his work, he developed a denotational model of space-bounded
 1182 computation, by taking a naive set-theoretic semantics, and then augmenting it with intensional
 1183 information. His sets were augmented with a *length function* saying how much memory each value
 1184 used, and in ours, we use a weight function saying how many capabilities each value holds. (In
 1185 fact, he even notes that his category also forms a model of bunched implications!) We think his
 1186 approach has a high power-to-weight ratio, and hope we have shown that it has broad applicability
 1187 as well.

1188 However, this semantics is certainly not the last word: e.g., the semantics in this paper does not
 1189 model the allocation of new capabilities as a program executes. In the categorical semantics of
 1190 bunched logics, it is common to use functor categories, such as functors from the *category of finite*
 1191 *sets and injections* \mathcal{I} , to Set, or presheaves over some other monoidal category. The functor category
 1192 forms a model of BI, inheriting the cartesian closed structure where the limits are computed Kripke-
 1193 style in Set, and also a monoidal closed structure using the tensor product from the monoidal
 1194 category and *Day convolution*. In addition, the ability to move to a bigger set permits modelling
 1195 allocation of new names and channels (e.g., as is done in models of the ν -calculus [Stark 1996]).

1196 Another natural question is how we might handle recursion, as our explicit description of the
 1197 category of capability spaces \mathcal{C} in section 4 seems quite tied to Set; our semantics handles copro-
 1198 ducts, natural numbers and iteration, but not general recursion. We have not done the work yet, but
 1199 we remark that our semantics can be viewed as an instance of a more general construction. Both
 1200 \mathcal{C} and $\wp(\mathcal{C})$ are objects in Set, so we can construct the *slice category* or the *over category* $\text{Set}/\wp(\mathcal{C})$.
 1201 The morphisms in this category are commuting triangles, with on-the-nose equality of capabili-
 1202 ties. But, we want the *lax* morphisms that we described in \mathcal{C} , which uses the lattice structure of
 1203 $\wp(\mathcal{C})$ to preserve capabilities. We can do this by considering $\wp(\mathcal{C})$ as a thin category (poset) and
 1204 constructing the *comma category* using Set as the domain for the functors. Since $\wp(\mathcal{C})$ is finitely
 1205 complete and co-complete, we get limits and co-limits in the comma category. By replaying this
 1206 in a category like CPO rather than Set, we may be able to derive a domain-theoretic analogue of
 1207 capability spaces.

1208 Another direction for future work lies in the observation that our \square comonad in subsection 4.5
 1209 takes away *all* capabilities, yielding a system with a syntax like that of Pfenning and Davies [2001]
 1210 with an interpretation close to the axiomatic categorical semantics proposed by Alechina et al.
 1211 [2001] and Kobayashi [1997]. However, we could consider a *graded* or *indexed* version of the same,
 1212 i.e., \square_C , which only takes away a set of capabilities $C \in \wp(\mathcal{C})$ from a value. Our hope would be
 1213 that this could form a model of systems like bounded linear logic [Dal Lago and Hofmann 2009;
 1214 Orchard et al. 2019], or other systems of coeffects [Petricek et al. 2014]. One issue we foresee is
 1215 that while this indexed comonad would still be a strong monoidal functor, it loses the idempotence
 1216 property, which we used in our interpretation and proofs.

1217 There has also been a great deal of work on using monads and effect systems [Gifford and
 1218 Lucassen 1986; Moggi 1989; Nielson and Nielson 1999; Wadler 1998] to control the usage of effects.
 1219 However, the general idea of using a static tag which broadcasts that an effect *may* occur seems
 1220 somewhat the reverse of the idea of object capabilities, where access to a dynamically-passed value
 1221 determines whether an effect can occur. The key feature of our system is that the comonad does
 1222 not say what effects are possible, but rather asserts that effects are *absent*. This manifests in the
 1223 cancellation law (in subsection 4.6) of the comonad and the monad. Still, the very phrases “*may*
 1224 *perform*” and “*does not possess*” hint that some sort of duality ought to exist.

1226 REFERENCES

- 1227 Natasha Alechina, Michael Mendler, Valeria de Paiva, and Eike Ritter. 2001. Categorical and Kripke Semantics for Con-
 1228 structive S4 Modal Logic. In *Computer Science Logic, 15th International Workshop, CSL 2001. 10th Annual Conference of*
 1229 *the EACSL, Paris, France, September 10–13, 2001, Proceedings (Lecture Notes in Computer Science)*, Laurent Fribourg (Ed.),
 1230 Vol. 2142. Springer, 292–307. https://doi.org/10.1007/3-540-44802-0_21
- 1231 Hendrik Pieter Barendregt. 1985. *The lambda calculus - its syntax and semantics*. Studies in logic and the foundations of
 1232 mathematics, Vol. 103. North-Holland. 132 pages. <https://doi.org/10.2307/2185110>
- 1233 Josh Berdine, Cristiano Calcagno, and Peter W. O’Hearn. 2006. Smallfoot: Modular Automatic Assertion Checking with
 1234 Separation Logic. In *Formal Methods for Components and Objects*, Frank S. de Boer, Marcello M. Bonsangue, Susanne
 1235 Graf, and Willem-Paul de Roever (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 115–137.
- 1236 Karl Crary, David Walker, and J. Gregory Morrisett. 1999. Typed Memory Management in a Calculus of Capabilities.
 1237 In *POPL ’99, Proceedings of the 26th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, San*
 1238 *Antonio, TX, USA, January 20–22, 1999*, Andrew W. Appel and Alex Aiken (Eds.). ACM, 262–275. <https://doi.org/10.1145/292540.292564>
- 1239 Ugo Dal Lago and Martin Hofmann. 2009. Bounded Linear Logic, Revisited. In *Typed Lambda Calculi and Applications*,
 1240 Pierre-Louis Curien (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 80–94.
- 1241 Nils Anders Danielsson, John Hughes, Patrik Jansson, and Jeremy Gibbons. 2006. Fast and Loose Reasoning is Morally
 1242 Correct. In *Conference Record of the 33rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*
 1243 (*POPL ’06*). ACM, 206–217. <https://doi.org/10.1145/1111037.1111056> Charleston, South Carolina, USA.
- 1244 Jack B. Dennis and Earl C. Van Horn. 1966. Programming semantics for multiprogrammed computations. *Commun. ACM*
 1245 9, 3 (1966), 143–155. <https://doi.org/10.1145/365230.365252>
- 1246 Mike Dodds, Xinyu Feng, Matthew Parkinson, and Viktor Vafeiadis. 2009. Deny-Guarantee Reasoning. In *Programming*
 1247 *Languages and Systems*, Giuseppe Castagna (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 363–377.
- 1248 Jeremy Gibbons. 2000. Calculating Functional Programs. In *Algebraic and Coalgebraic Methods in the Mathematics of Pro-*
 1249 *gram Construction, International Summer School and Workshop, Oxford, UK, April 10–14, 2000, Revised Lectures (Lecture*
 1250 *Notes in Computer Science)*, Roland Carl Backhouse, Roy L. Crole, and Jeremy Gibbons (Eds.), Vol. 2297. Springer, 149–
 1251 202. https://doi.org/10.1007/3-540-47797-7_5
- 1252 David K. Gifford and John M. Lucasen. 1986. Integrating Functional and Imperative Programming. In *Proceedings of*
 1253 *the 1986 ACM Conference on LISP and Functional Programming (LFP ’86)*. ACM, New York, NY, USA, 28–38. <https://doi.org/10.1145/319838.319848>
- 1254 Jean-Yves Girard. 1987. Linear logic. *Theoretical Computer Science* 50, 1 (Jan 1987), 1–101. [https://doi.org/10.1016/0304-3975\(87\)90045-4](https://doi.org/10.1016/0304-3975(87)90045-4)
- 1255 Jean-Yves Girard, Paul Taylor, and Yves Lafont. 1989. *Proofs and Types*. Cambridge University Press, New York, NY, USA.
 1256 217–241 pages. https://doi.org/10.1007/978-1-4612-2822-6_8
- 1257 Martin Hofmann. 2003. Linear types and non-size-increasing polynomial time computation. *Information and Computation*
 1258 183, 1 (may 2003), 57–85. [https://doi.org/10.1016/s0890-5401\(03\)00009-9](https://doi.org/10.1016/s0890-5401(03)00009-9)
- 1259 Satoshi Kobayashi. 1997. Monad as modality. *Theoretical Computer Science* 175, 1 (1997), 29 – 74. [https://doi.org/10.1016/S0304-3975\(96\)00169-7](https://doi.org/10.1016/S0304-3975(96)00169-7)
- 1260 Neelakantan R. Krishnaswami. 2013. Higher-Order Reactive Programming without Spacetime Leaks. In *International Con-*
 1261 *ference on Functional Programming (ICFP)*.
- 1262 Hugh C. Lauer and Roger M. Needham. 1979. On the Duality of Operating System Structures. *ACM SIGOPS Operating*
 1263 *Systems Review* 13, 2 (apr 1979), 3–19. <https://doi.org/10.1145/850657.850658>
- 1264 Henry M Levy. 1984. *Capability-based computer systems*. Digital Press.
- 1265 Paul Blain Levy, John Power, and Hayo Thielecke. 2003. Modelling environments in call-by-value programming languages.
 1266 *Information and Computation* 185, 2 (Sep 2003), 182–210. [https://doi.org/10.1016/S0890-5401\(03\)00088-9](https://doi.org/10.1016/S0890-5401(03)00088-9)
- 1267 S. Maffeis, J. C. Mitchell, and A. Taly. 2010. Object Capabilities and Isolation of Untrusted Web Applications. In *2010 IEEE*
 1268 *Symposium on Security and Privacy*. 125–140. <https://doi.org/10.1109/SP.2010.16>
- 1269 J. C. C. McKinsey and Alfred Tarski. 1948. Some Theorems About the Sentential Calculi of Lewis and Heyting. *J. Symb.*
 1270 *Log.* 13, 1 (1948), 1–15. <https://doi.org/10.2307/2268135>
- 1271 Mark Samuel Miller. 2006. *Robust Composition: Towards a Unified Approach to Access Control and Concurrency Control*. Ph.D.
 1272 Dissertation. USA. Advisor(s) Shapiro, Jonathan S. AAI3245526.
- 1273 Eugenio Moggi. 1989. Computational Lambda-Calculus and Monads. In *Proceedings of the Fourth Annual Symposium on*
 1274 *Logic in Computer Science (LICS ’89), Pacific Grove, California, USA, June 5–8, 1989*. IEEE Computer Society, 14–23. <https://doi.org/10.1109/LICS.1989.39155>
- 1275 Eugenio Moggi. 1991. Notions of Computation and Monads. *Inf. Comput.* 93, 1 (1991), 55–92. [https://doi.org/10.1016/0890-5401\(91\)90052-4](https://doi.org/10.1016/0890-5401(91)90052-4)

- 1275 Greg Morrisett, Amal Ahmed, and Matthew Fluet. 2005. L3: A Linear Language with Locations. In *Typed Lambda Calculi
1276 and Applications*, Paweł Urzyczyn (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 293–307.
- 1277 Flemming Nielson and Hanne Riis Nielson. 1999. *Type and Effect Systems*. Springer Berlin Heidelberg, Berlin, Heidelberg,
1278 114–136. https://doi.org/10.1007/3-540-48092-7_6
- 1279 Peter W. O'Hearn and David J. Pym. 1999. The Logic of Bunched Implications. *Bulletin Symbolic Logic* 5, 2 (06 1999),
1280 215–244. <https://projecteuclid.org:443/euclid.bsl/1182353620>
- 1281 Dominic A. Orchard, Vilem Liepelt, and Harley Eades. 2019. Quantitative program reasoning with graded modal types.
Proceedings of the ACM on Programming Languages (June 2019). <https://kar.kent.ac.uk/74450/>
- 1282 P. W. O'Hearn. 1993. A model for syntactic control of interference. *Mathematical Structures in Computer Science* 3, 4 (Dec
1283 1993), 435–465. <https://doi.org/10.1017/S096012950000311>
- 1284 Tomas Petricek, Dominic A. Orchard, and Alan Mycroft. 2014. Coeffects: a calculus of context-dependent computation.
In *Proceedings of the 19th ACM SIGPLAN international conference on Functional programming, Gothenburg, Sweden, September 1-3, 2014*, Johan Jeuring and Manuel M. T. Chakravarty (Eds.). ACM, 123–135. <https://doi.org/10.1145/2628136.2628160>
- 1285 Frank Pfenning and Rowan Davies. 2001. A judgmental reconstruction of modal logic. *Mathematical Structures in Computer
1286 Science* 11, 4 (2001), 511–540. <https://doi.org/10.1017/S0960129501003322>
- 1287 John C. Reynolds. 1978. Syntactic Control of Interference. In *Proceedings of the 5th ACM SIGACT-SIGPLAN Symposium
1288 on Principles of Programming Languages (POPL '78)*. ACM, 39–46. <https://doi.org/10.1145/512760.512766> event-place:
1289 Tucson, Arizona.
- 1290 J. C. Reynolds. 2002. Separation logic: a logic for shared mutable data structures. In *Proceedings 17th Annual IEEE Symposium
1291 on Logic in Computer Science*. 55–74. <https://doi.org/10.1109/LICS.2002.1029817>
- 1292 Amr Sabry. 1998. What is a purely functional language? *Journal of Functional Programming* 8, 1 (Jan 1998), 1–22. <https://doi.org/10.1017/S0956796897002943>
- 1293 Ian Stark. 1996. Categorical models for local names. *LISP and Symbolic Computation* 9, 1 (01 Feb 1996), 77–107. <https://doi.org/10.1007/BF01806033>
- 1294 Tachio Terauchi and Alex Aiken. 2006. A Capability Calculus for Concurrency and Determinism. In *CONCUR 2006 - Con-
1295 currency Theory, 17th International Conference, CONCUR 2006, Bonn, Germany, August 27-30, 2006, Proceedings (Lec-
1296 ture Notes in Computer Science)*, Christel Baier and Holger Hermanns (Eds.), Vol. 4137. Springer, 218–232. https://doi.org/10.1007/11817949_15
- 1297 Philip Wadler. 1990. Deforestation: transforming programs to eliminate trees. *Theoretical Computer Science* 73, 2 (jun 1990),
1298 231–248. [https://doi.org/10.1016/0304-3975\(90\)90147-a](https://doi.org/10.1016/0304-3975(90)90147-a)
- 1299 Philip Wadler. 1998. The Marriage of Effects and Monads. In *Proceedings of the Third ACM SIGPLAN International Conference
1300 on Functional Programming (ICFP '98)*. ACM, New York, NY, USA, 63–74. <https://doi.org/10.1145/289423.289429>
- 1301 W. Wulf, E. Cohen, W. Corwin, A. Jones, R. Levin, C. Pierson, and F. Pollack. 1974. HYDRA: The Kernel of a Multiprocessor
1302 Operating System. *Commun. ACM* 17, 6 (Jun 1974), 337–345. <https://doi.org/10.1145/355616.364017>
- 1303
- 1304
- 1305
- 1306
- 1307
- 1308
- 1309
- 1310
- 1311
- 1312
- 1313
- 1314
- 1315
- 1316
- 1317
- 1318
- 1319
- 1320
- 1321
- 1322
- 1323

1324 **A PROOFS FOR SECTION 3 (TYPING)**

1325 LEMMA A.1. *The weakening relation is reflexive.*
 1326 PROOF.

1327	(1)	$\boxed{\Gamma}$	
1328	(2)	$\boxed{\Gamma = \cdot}$	
1329	(3)	$\cdot \supseteq \cdot$	$\supseteq\text{-ID}$
1330	(4)	$\boxed{\Gamma = \Gamma', x : A^q}$	
1331	(5)	$\Gamma' \supseteq \Gamma'$	induction hypothesis
1332	(6)	$\Gamma', x : A^q \supseteq \Gamma', x : A^q$	$\supseteq\text{-CONG}$
1333	(7)	$\Gamma \supseteq \Gamma$	

1334
 1335
 1336
 1337
 1338
 1339
 1340
 1341

LEMMA A.2. *The weakening relation is transitive.*
 PROOF.

□

1342	(1)	$\boxed{\Gamma \supseteq \Delta, \Delta \supseteq \Psi}$	
1343	(2)	$\boxed{\Gamma = \cdot, \Delta = \cdot}$	case $\supseteq\text{-ID}$
1344	(3)	$\boxed{\Psi = \cdot}$	inversion
1345	(4)	$\cdot \supseteq \cdot$	$\supseteq\text{-ID}$
1346	(5)	$\boxed{\Gamma = \Gamma', x : A^q, \Delta = \Delta', x : A^q}$	case $\supseteq\text{-CONG}$
1347	(6)	$\boxed{\Psi = \Psi', x : A^q, \Delta' \supseteq \Psi'}$	case $\supseteq\text{-CONG}$
1348	(7)	$\boxed{\Gamma' \supseteq \Psi'}$	induction hypothesis
1349	(8)	$\Gamma', x : A^q \supseteq \Psi', x : A^q$	$\supseteq\text{-CONG}$
1350	(9)	$\boxed{\Delta' \supseteq \Psi}$	case $\supseteq\text{-WK}$
1351	(10)	$\Gamma' \supseteq \Psi$	induction hypothesis
1352	(11)	$\Gamma', x : A^q \supseteq \Psi$	induction hypothesis
1353	(12)	$\boxed{\Gamma' \supseteq \Delta}$	case $\supseteq\text{-WK}$
1354	(13)	$\Gamma' \supseteq \Psi$	induction hypothesis
1355	(14)	$\Gamma', x : A^q \supseteq \Psi$	
1356	(15)	$\Gamma \supseteq \Psi$	

□

1373
 1374 LEMMA A.3. If $x : A^q \in \Delta$ and $\Gamma \supseteq \Delta$, then $x : A^q \in \Gamma$.

1375 PROOF. Assuming $\Gamma \supseteq \Delta$, we do induction on $x : A^q \in \Delta$.

1376 $\diamond \in \text{-ID}$

1377

1378	(1)	$\boxed{x : A^q \in (\Delta', x : A^q)}$	$\in\text{-ID}$
1380		$\Gamma' \supseteq \Delta'$	
1381	(2)	$\boxed{\Gamma', x : A^q \supseteq \Delta', x : A^q}$	$\supseteq\text{-CONG}$
1382			
1383	(3)	$x : A^q \in (\Gamma', x : A^q)$	$\in\text{-ID}$
1384			
1385			

1386

1387 $\diamond \in \text{-EX}$

1388

1389	(1)	$\boxed{x : A^q \in \Delta' \quad (x \neq y)}$	$\in\text{-EX}$
1390		$\Gamma' \supseteq \Delta'$	
1391	(2)	$\boxed{\Gamma', y : B^r \supseteq \Delta', y : B^r}$	$\supseteq\text{-CONG}$
1392			
1393	(3)	$x : A^q \in \Delta'$	inversion
1394			
1395	(4)	$\Gamma' \supseteq \Delta'$	inversion
1396			
1397	(5)	$x : A^q \in \Gamma$	induction hypothesis
1398			
1399	(6)	$x : A^q \in (\Gamma', y : B^r)$	$\in\text{-EX}$
1400			

1401

1402 LEMMA A.4. If $\Gamma \supseteq \Delta$, then $\Gamma^p \supseteq \Delta^p$.

1403

1404 PROOF. We do induction on $\Gamma \supseteq \Delta$.

1405 $\diamond \supseteq \text{-ID}$

1406

1407

1408

1409

1410

1411

1412

1413

1414

1415

1416

1417

1418

1419

1420

1421

(1)	$\boxed{\cdot \supseteq \cdot}$	$\supseteq\text{-ID}$
(2)	$\cdot \supseteq \cdot$	$\supseteq\text{-ID}$

	$\Gamma' \supseteq \Delta'$	
1422 1423 1424 (1)	$\boxed{\Gamma', x : A^q \supseteq \Delta', x : A^q}$	\supseteq -CONG
1425 1426 (2)	$\Gamma' \supseteq \Delta'$	inversion
1427 1428 (3)	$\Gamma'^{\textcolor{blue}{p}} \supseteq \Delta'^{\textcolor{blue}{p}}$	induction hypothesis
1429 (4)	$\boxed{q = \textcolor{blue}{p}}$	
1430 1431 (5)	$\Gamma'^{\textcolor{blue}{p}}, x : A^{\textcolor{blue}{p}} \supseteq \Delta'^{\textcolor{blue}{p}}, x : A^{\textcolor{blue}{p}}$	\supseteq -CONG (3)
1432 1433 (6)	$\boxed{q = \textcolor{violet}{i}}$	
1434 (7)	$\Gamma'^{\textcolor{blue}{p}} \supseteq \Delta'^{\textcolor{blue}{p}}$	(3)
1435 1436 (8)	$(\Gamma', x : A^q)^{\textcolor{blue}{p}} \supseteq (\Delta', x : A^q)^{\textcolor{blue}{p}}$	

1437
1438
1439 $\diamond \supseteq$ -WK

1440

	$\Gamma' \supseteq \Delta$	
1441 1442 1443 (1)	$\boxed{\Gamma', x : A^q \supseteq \Delta}$	\supseteq -WK
1444 1445 (2)	$\Gamma' \supseteq \Delta$	inversion
1446 1447 (3)	$\Gamma'^{\textcolor{blue}{p}} \supseteq \Delta^{\textcolor{blue}{p}}$	induction hypothesis
1448 1449 (4)	$\boxed{q = \textcolor{blue}{p}}$	
1450 (5)	$\Gamma'^{\textcolor{blue}{p}}, x : A^{\textcolor{blue}{p}} \supseteq \Delta^{\textcolor{blue}{p}}$	\supseteq -WK (3)
1451 1452 (6)	$\boxed{q = \textcolor{violet}{i}}$	
1453 1454 (7)	$\Gamma'^{\textcolor{blue}{p}} \supseteq \Delta^{\textcolor{blue}{p}}$	(3)
1455 1456 (8)	$(\Gamma', x : A^q)^{\textcolor{blue}{p}} \supseteq \Delta^{\textcolor{blue}{p}}$	

1457

1458

1459

LEMMA 3.1 SYNTACTIC WEAKENING. If $\Gamma \supseteq \Delta$ and $\Delta \vdash e : A$, then $\Gamma \vdash e : A$. □

1460
1461 PROOF. Assuming $\Gamma \supseteq \Delta$, we do induction on $\Delta \vdash e : A$.

1462 \diamond VAR

1463

	$x : A^q \in \Delta$	
1464 1465 1466 (1)	$\boxed{\Delta \vdash x : A}$	VAR
1467 1468 (2)	$x : A^q \in \Delta$	inversion

1469

1471 (3) $x : A^q \in \Gamma$ lemma A.3
 1472

1473 (4) $\Gamma \vdash x : A$ VAR
 1474

1475
 1476 \diamond unitI
 1477

1478
 1479
 1480 (1)
$$\boxed{\Delta \vdash () : \text{unit}}$$
 unitI
 1481

1482 (2) $\Gamma \vdash () : \text{unit}$ unitI
 1483

1484
 1485 \diamond \times I
 1486

1487
 1488 (1)
$$\boxed{\Delta \vdash e_1 : A \quad \Delta \vdash e_2 : B} \quad \frac{}{\Delta \vdash (e_1, e_2) : A \times B}$$
 \times I
 1489
 1490

1491 (2) $\Delta \vdash e_1 : A$ inversion
 1492
 1493 (3) $\Delta \vdash e_2 : B$ inversion
 1494 (4) $\Gamma \vdash e_1 : A$ induction hypothesis
 1495
 1496 (5) $\Gamma \vdash e_2 : B$ induction hypothesis
 1497
 1498 (6) $\Gamma \vdash (e_1, e_2) : A \times B$ \times I
 1499

1500
 1501 \diamond \times E_i
 1502

1503
 1504 (1)
$$\boxed{\Delta \vdash e : A \times B} \quad \frac{}{\Delta \vdash \text{fst } e : A}$$
 \times E₁
 1505
 1506
 1507 (2) $\Delta \vdash e : A \times B$ inversion
 1508
 1509 (3) $\Gamma \vdash e : A \times B$ induction hypothesis
 1510 (4) $\Gamma \vdash \text{fst } e : A$ \times E₁
 1511

1512
 1513
 1514
 1515 (1)
$$\boxed{\Delta \vdash e : A \times B} \quad \frac{}{\Delta \vdash \text{snd } e : B}$$
 \times E₂
 1516
 1517

- 1520 (2) $\Delta \vdash e : A \times B$ inversion
 1521 (3) $\Gamma \vdash e : A \times B$ induction hypothesis
 1522 (4) $\Gamma \vdash \text{snd } e : B$ $\times E_2$
 1523
 1524
 1525

1526 $\diamond \Box I$

- 1527
 1528
 1529
 1530
 1531 (1)
$$\frac{\Delta \vdash p \ e : A}{\Delta \vdash \text{box}[e] : \Box A}$$
 $\Box I$
 1532
 1533 (2) $\Delta \vdash p \ e : A$ inversion
 1534 (3) $\Delta^p \vdash e : A$ inversion
 1535
 1536 (4) $\Gamma^p \supseteq \Delta^p$ lemma A.4
 1537
 1538 (5) $\Gamma^p \vdash e : A$ induction hypothesis
 1539
 1540 (6) $\Gamma \vdash p \ e : A$ CTX-PURE
 1541 (7) $\Gamma \vdash \text{box}[e] : \Box A$ $\Box I$
 1542
 1543

1544 $\diamond \Box E$

- 1545
 1546
 1547
 1548 (1)
$$\frac{\Delta \vdash e_1 : \Box A \quad \Delta, x : A^p \vdash e_2 : B}{\Delta \vdash \text{let box}[x] = e_1 \text{ in } e_2 : B}$$
 $\Box E$
 1549
 1550 (2) $\Delta \vdash e_1 : \Box A$ inversion
 1551
 1552 (3) $\Delta, x : A^p \vdash e_2 : B$ inversion
 1553
 1554 (4) $\Gamma \vdash e_1 : \Box A$ induction hypothesis (2)
 1555 (5) $\Gamma, x : A^p \supseteq \Delta, x : A^p$ \supseteq -CONG
 1556
 1557 (6) $\Gamma, x : A^p \vdash e_2 : B$ induction hypothesis (3) (5)
 1558
 1559 (7) $\Gamma \vdash \text{let box}[x] = e_1 \text{ in } e_2 : B$ $\Box E$
 1560

1561 $\diamond \Rightarrow I$

- 1562
 1563
 1564
 1565
 1566 (1)
$$\frac{\Delta, x : A^i \vdash e : B}{\Delta \vdash \lambda x : A. e : A \Rightarrow B}$$
 $\Rightarrow I$
 1567
 1568

1569	(2)	$\Delta, x : A^i \vdash e : B$	inversion
1570			
1571	(3)	$\Gamma, x : A^i \supseteq \Delta, x : A^i$	\supseteq -CONG
1572			
1573	(4)	$\Gamma, x : A^i \vdash e : B$	induction hypothesis (3)
1574			
1575	(5)	$\Gamma \vdash \lambda x. e : A \Rightarrow B$	\Rightarrow I
1576			
1577	$\diamond \Rightarrow E$		
1578			
1579			
1580	(1)	$\frac{\Delta \vdash e_1 : A \Rightarrow B \quad \Delta \vdash e_2 : A}{\Delta \vdash e_1 e_2 : B}$	\Rightarrow E
1581			
1582			
1583	(2)	$\Delta \vdash e_1 : A \Rightarrow B$	inversion
1584			
1585	(3)	$\Delta \vdash e_2 : A$	inversion
1586			
1587	(4)	$\Gamma \vdash e_1 : A \Rightarrow B$	induction hypothesis (2)
1588			
1589	(5)	$\Gamma \vdash e_2 : A$	induction hypothesis (3)
1590			
1591	(6)	$\Gamma \vdash e_1 e_2 : B$	\Rightarrow E
1592			
1593	$\diamond \text{strI}$		
1594			
1595			
1596	(1)	$\boxed{\quad}$	strI
1597			
1598			
1599	(2)	$\Gamma \vdash s : \text{str}$	strI
1600			
1601			
1602	$\diamond \text{PRINT}$		
1603			
1604			
1605	(1)	$\frac{\Delta \vdash e_1 : \text{cap} \quad \Delta \vdash e_2 : \text{str}}{\Delta \vdash e_1 \cdot \text{print}(e_2) : \text{unit}}$	PRINT
1606			
1607			
1608	(2)	$\Delta \vdash e_1 : \text{cap}$	inversion
1609			
1610	(3)	$\Delta \vdash e_2 : \text{str}$	inversion
1611			
1612	(4)	$\Gamma \vdash e_1 : \text{cap}$	induction hypothesis (2)
1613			
1614	(5)	$\Gamma \vdash e_2 : \text{str}$	induction hypothesis (3)
1615			
1616	(6)	$\Gamma \vdash e_1 \cdot \text{print}(e_2) : \text{unit}$	PRINT
1617			

1618

1619

1620 LEMMA A.5. If $\Gamma \supseteq \Delta$ and $\Delta \vdash \theta : \Psi$, then $\Gamma \vdash \theta : \Psi$.

1621

1622 PROOF. Assuming $\Gamma \supseteq \Delta$, we do induction on $\Delta \vdash \theta : \Psi$.1623 \diamond SUB-ID

1624

1625
$$\boxed{(1) \quad \frac{}{\Delta \vdash \langle \rangle : \cdot}}$$

1626 SUB-ID

1627

1628
$$(2) \quad \Gamma \vdash \langle \rangle : \cdot \quad \text{SUB-ID}$$

1629

1630 \diamond SUB-PURE

1631

1632 \diamond SUB-PURE

1633

1634

1635
$$\boxed{(1) \quad \frac{\Delta \vdash \theta : \Psi' \quad \Delta \vdash \textcolor{blue}{e} : A}{\Delta \vdash \langle \theta, \textcolor{blue}{e}^p/x \rangle : \Psi', \textcolor{teal}{x} : A^p}}$$

1636 SUB-PURE

1637

1638
$$(2) \quad \Delta \vdash \theta' : \Psi' \quad \text{inversion}$$

1639

1640
$$\Delta^p \vdash e : A$$

1641

1642
$$(3) \quad \Delta^p \vdash e : A \quad \text{CTX-PURE}$$

1643

1644
$$(4) \quad \Delta^p \vdash e : A \quad \text{inversion}$$

1645

1646
$$(5) \quad \Gamma \vdash \theta' : \Psi' \quad \text{induction hypothesis (2)}$$

1647

1648
$$(6) \quad \Gamma^p \supseteq \Delta^p \quad \text{lemma A.4}$$

1649

1650
$$(7) \quad \Gamma^p \vdash e : A \quad \text{syntactic weakening lemma 3.1 (3)}$$

1651

1652
$$(8) \quad \Gamma \vdash \textcolor{blue}{e} : A \quad \text{CTX-PURE}$$

1653

1654
$$(9) \quad \Gamma \vdash \langle \theta', \textcolor{blue}{e}^p/x \rangle : \Psi', \textcolor{teal}{x} : A^p \quad \text{SUB-PURE}$$

1655

1656

1657 \diamond SUB-IMPURE

1658

1659
$$\boxed{(1) \quad \frac{\Delta \vdash \theta : \Psi' \quad \Delta \vdash v : A}{\Delta \vdash \langle \theta, v^i/x \rangle : \Psi', \textcolor{teal}{x} : A^i}}$$

1660 SUB-IMPURE

1661

1662
$$(2) \quad \Delta \vdash \theta' : \Psi' \quad \text{inversion}$$

1663

1664
$$(3) \quad \Delta \vdash v : A \quad \text{inversion}$$

1665

1666
$$(4) \quad \Gamma \vdash \theta' : \Psi' \quad \text{induction hypothesis (2)}$$

1667

1668
$$(5) \quad \Gamma \vdash v : A \quad \text{syntactic weakening lemma 3.1 (3)}$$

1669

1667 (6) $\Gamma \vdash \langle \theta', v^i/x \rangle : \Psi', x : A^i$ SUB-IMPURE

1671 LEMMA A.6. If $\Gamma \vdash \theta : \Delta$ then $\Gamma^p \vdash \theta^p : \Delta^p$. □

1673 PROOF. We do induction on $\Gamma \vdash \theta : \Delta$.

1675 (1)	$\boxed{\Gamma \vdash \theta : \Delta}$	
1676 (2)	$\boxed{\Gamma \vdash \langle \rangle : \cdot}$	SUB-ID
1678 (3)	$\Gamma^p \vdash \langle \rangle : \cdot$	SUB-ID
1680 (4)	$\frac{\Gamma \vdash \theta : \Delta \quad \Gamma \vdash^p e : A}{\Gamma \vdash \langle \theta, e^p/x \rangle : \Delta, x : A^p}$	SUB-PURE
1685 (5)	$\frac{\Gamma \vdash \theta : \Delta \quad \Gamma^p \vdash e : A}{\Gamma \vdash^p e : A}$	inversion
1688 (6)	$\Gamma^p \vdash e : A$	CTX-PURE
1689 (7)	$\Gamma^p \vdash e : A$	inversion
1690 (8)	$\Gamma^p \vdash \theta^p : \Delta^p$	induction hypothesis
1692 (9)	$(\Gamma^p)^p \vdash e : A$	$(\Gamma^p)^p = \Gamma^p$
1694 (10)	$\Gamma^p \vdash^p e : A$	CTX-PURE
1695 (11)	$\Gamma^p \vdash \langle \theta^p, e^p/x \rangle : \Delta^p, x : A^p$	SUB-PURE
1697 (12)	$\frac{\Gamma \vdash \theta : \Delta \quad \Gamma \vdash v : A}{\Gamma \vdash \langle \theta, v^i/x \rangle : \Delta, x : A^i}$	SUB-IMPURE
1700 (13)	$\Gamma \vdash \theta : \Delta$	inversion
1702 (14)	$\Gamma^p \vdash \theta^p : \Delta^p$	induction hypothesis
1703 (15)	$\Gamma^p \vdash \theta^p : \Delta^p$	

1707 LEMMA A.7. For any context Γ , we have $\Gamma \supseteq \Gamma^p$. □

1708 PROOF. We do induction on Γ .

1710 (1)	$\boxed{\Gamma}$	
1712 (2)	$\boxed{\Gamma = \cdot}$	

1716	(3)	$\cdot \supseteq \cdot$	$\supseteq\text{-ID}$
1717	(4)	$\boxed{\Gamma = \Delta, \textcolor{blue}{x : A^p}}$	
1718	(5)	$\Delta \supseteq \Delta^p$	induction hypothesis
1719	(6)	$\Delta, \textcolor{blue}{x : A^p} \supseteq \Delta^p, \textcolor{blue}{x : A^p}$	$\supseteq\text{-CONG}$
1720	(7)	$\boxed{\Gamma = \Delta, \textcolor{violet}{x : A^i}}$	
1721	(8)	$\Delta \supseteq \Delta^p$	induction hypothesis
1722	(9)	$\Delta, \textcolor{violet}{x : A^i} \supseteq \Delta^p$	$\supseteq\text{-WK}$
1723	(10)	$\Gamma \supseteq \Gamma^p$	
1724			
1725			
1726			
1727			
1728			
1729			
1730			
1731			
1732			□
1733			
1734		LEMMA A.8. If $\Gamma \vdash \theta : \Delta$ and $x : A^q \in \Delta$, then $\Gamma \vdash \theta[x] : A$.	
1735		PROOF. Assuming $\Gamma \vdash \theta : \Delta$, we do induction on $x : A^q \in \Delta$.	
1736		$\diamond \in \text{-ID}$	
1737			
1738	(1)	$\boxed{x : A^q \in (\Delta', x : A^q)}$	$\in\text{-ID}$
1739	(2)	$\boxed{q = p}$	
1740		$\Gamma \vdash \phi : \Delta' \quad \Gamma \vdash p e : A$	
1741	(3)	$\frac{\Gamma \vdash \langle \phi, e^p/x \rangle : \Delta', \textcolor{blue}{x : A^p}}{\Gamma^p \vdash e : A}$	SUB-PURE
1742	(4)	$\Gamma^p \vdash e : A$	CTX-PURE
1743	(5)	$\Gamma^p \vdash e : A$	inversion
1744	(6)	$\Gamma \supseteq \Gamma^p$	lemma A.7
1745	(7)	$\Gamma \vdash e : A$	syntactic weakening lemma 3.1
1746	(8)	$\Gamma \vdash \langle \phi, e^p/x \rangle[x] : A$	definition
1747	(9)	$\boxed{q = i}$	
1748		$\Gamma \vdash \phi : \Delta' \quad \Gamma \vdash v : A$	
1749	(10)	$\frac{\Gamma \vdash \langle \phi, v^i/x \rangle : \Delta', \textcolor{violet}{x : A^i}}{\Gamma \vdash v : A}$	SUB-IMPURE
1750	(11)	$\Gamma \vdash v : A$	inversion
1751	(12)	$\Gamma \vdash \langle \phi, v^i/x \rangle[x] : A$	definition
1752	(13)	$\Gamma \vdash \theta[x] : A$	
1753			
1754			
1755			
1756			
1757			
1758			
1759			
1760			
1761			
1762			
1763			
1764			

1765

1766 $\diamond \in \text{-EX}$

1767

1768

1769

$$(1) \quad \frac{x : A^q \in \Delta' \quad (x \neq y)}{x : A^q \in (\Delta', y : B^r)} \quad \in\text{-EX}$$

1770

1771

$$(2) \quad x : A^q \in \Delta' \quad \text{inversion}$$

1772

1773

$$(3) \quad q = p \quad \frac{\Gamma \vdash \phi : \Delta' \quad \Gamma \vdash e : B}{\Gamma \vdash \langle \phi, e^p / y \rangle : \Delta', y : B^p} \quad \text{SUB-PURE}$$

1775

1776

$$(4) \quad \Gamma \vdash \phi : \Delta' \quad \text{inversion}$$

1777

1778

$$(5) \quad \Gamma \vdash \phi[x] : A \quad \text{induction hypothesis}$$

1779

1780

$$(6) \quad \Gamma \vdash \langle \phi, e^p / y \rangle [x] : A \quad \text{definition}$$

1781

1782

$$(7) \quad q = i \quad \frac{\Gamma \vdash \phi : \Delta' \quad \Gamma \vdash v : B}{\Gamma \vdash \langle \phi, v^i / y \rangle : \Delta', y : B^i} \quad \text{SUB-IMPURE}$$

1783

1784

$$(8) \quad \Gamma \vdash \phi : \Delta' \quad \text{inversion}$$

1785

1786

$$(9) \quad \Gamma \vdash \phi[x] : A \quad \text{induction hypothesis}$$

1787

1788

$$(10) \quad \Gamma \vdash \langle \phi, v^i / y \rangle [x] : A \quad \text{definition}$$

1789

1790

$$(11) \quad \Gamma \vdash \theta[x] : A \quad \text{definition}$$

1791

$$(12) \quad \Gamma \vdash \theta(x) : A \quad \text{definition}$$

1792

1793

$$(13) \quad \Gamma \vdash \theta[x] : A$$

1794

1795

□

1796

1797

THEOREM 3.4 SYNTACTIC SUBSTITUTION. *If $\Gamma \vdash \theta : \Delta$ and $\Delta \vdash e : A$, then $\Gamma \vdash \theta(e) : A$.*

1798

PROOF. Assuming $\Gamma \vdash \theta : \Delta$, we do induction on $\Delta \vdash e : A$.

1799 $\diamond \text{VAR}$

1800

$$(1) \quad \frac{x : A^q \in \Delta}{\Delta \vdash x : A} \quad \text{VAR}$$

1801

1802

$$(2) \quad x : A^q \in \Delta \quad \text{inversion}$$

1803

1804

$$(3) \quad \Gamma \vdash \theta[x] : A \quad \text{lemma A.8}$$

1805

1806

$$(4) \quad \Gamma \vdash \theta(x) : A \quad \text{definition}$$

1807

1808

1809

1810

1811

1812

1813

1814 $\diamond \text{unitI}$

1815

1816

1817

1818 (1) $\boxed{\Delta \vdash () : \text{unit}}$ unitI

1819

1820 (2) $\Gamma \vdash () : \text{unit}$ unitI

1821

1822 (3) $\Gamma \vdash \theta(() : \text{unit})$ definition

1823

1824

 $\diamond \times\text{I}$

1826

1827

$$(1) \quad \frac{\Delta \vdash e_1 : A \quad \Delta \vdash e_2 : B}{\Delta \vdash (e_1, e_2) : A \times B} \quad \times\text{I}$$

1829

1830 (2) $\Delta \vdash e_1 : A$ inversion

1831

1832 (3) $\Delta \vdash e_2 : B$ inversion

1833

1834 (4) $\Gamma \vdash \theta(e_1) : A$ induction hypothesis

1835

1836 (5) $\Gamma \vdash \theta(e_2) : B$ induction hypothesis

1837

1838 (6) $\Gamma \vdash (\theta(e_1), \theta(e_2)) : A \times B$ $\times\text{I}$

1839

1840 (7) $\Gamma \vdash \theta((e_1, e_2)) : A \times B$ definition

1841

1842 $\diamond \times\text{E}_i$

1843

1844

$$(1) \quad \frac{\Delta \vdash e : A \times B}{\Delta \vdash \text{fst } e : A} \quad \times\text{E}_1$$

1845

1846 (2) $\Delta \vdash e : A \times B$ inversion

1847

1848 (3) $\Gamma \vdash \theta(e) : A \times B$ induction hypothesis

1849

1850 (4) $\Gamma \vdash \text{fst } \theta(e) : B$ $\times\text{E}_1$

1851

1852 (5) $\Gamma \vdash \theta(\text{fst } e) : B$ definition

1853

1854

1855

1856

$$(1) \quad \frac{\Delta \vdash e : A \times B}{\Delta \vdash \text{snd } e : B} \quad \times\text{E}_2$$

1857

1858 (2) $\Delta \vdash e : A \times B$ inversion

1859

1860

1861

1862

1863 (3) $\Gamma \vdash \theta(e) : A \times B$ induction hypothesis

1864 (4) $\Gamma \vdash \text{snd } \theta(e) : B$ $\times E_2$

1865 (5) $\Gamma \vdash \theta(\text{snd } e) : B$ definition

1866

1867 $\diamond \Rightarrow I$

1868

1869

1870

1871

1872

1873

$$\boxed{\Delta, x : A^i \vdash e : B}$$

1874 (1) $\Delta \vdash \lambda x : A. e : A \Rightarrow B$ $\Rightarrow I$

1875

1876 (2) $\Delta, x : A^i \vdash e : B$ inversion

1877 (3) $\Gamma, y : A^i \supseteq \Gamma$ $\supseteq\text{-WK}$

1878 (4) $\Gamma, y : A^i \vdash \theta : \Delta$ lemma A.5

1879

1880 (5) $\Gamma, y : A^i \vdash y : A$ VAR

1881

1882 (6) $\Gamma, y : A^i \vdash \langle \theta, y^i/x \rangle : \Delta, x : A^i$ SUB-IMPURE (4) (5)

1883

1884 (7) $\Gamma, y : A^i \vdash \langle \theta, y^i/x \rangle(e) : B$ induction hypothesis (6) (2)

1885

1886 (8) $\Gamma \vdash \lambda y. \langle \theta, y^i/x \rangle(e) : A \Rightarrow B$ $\Rightarrow I$

1887

1888 (9) $\Gamma \vdash \theta(\lambda y. e) : A \Rightarrow B$ definition

1889

1890

1891 $\diamond \Rightarrow E$

1892

$$\boxed{\frac{\Delta \vdash e_1 : A \Rightarrow B \quad \Delta \vdash e_2 : A}{\Delta \vdash e_1 e_2 : B}}$$

1893

1894

1895 (1) $\Rightarrow E$

1896

1897 (2) $\Delta \vdash e_1 : A \Rightarrow B$ inversion

1898 (3) $\Delta \vdash e_2 : A$ inversion

1899

1900 (4) $\Gamma \vdash \theta(e_1) : A \Rightarrow B$ induction hypothesis (2)

1901

1902 (5) $\Gamma \vdash \theta(e_2) : A$ induction hypothesis (3)

1903

1904 (6) $\Gamma \vdash \theta(e_1) \theta(e_2) : B$ $\Rightarrow E$

1905

1906

1907

1908 (7) $\Gamma \vdash \theta(e_1 e_2) : B$ definition

1909

1910

1911

$\diamond \text{strI}$

1912			
1913	(1)	$\frac{}{\Delta \vdash s : \text{str}}$	strI
1914			
1915	(2)	$\Gamma \vdash s : \text{str}$	strI
1916			
1917	(3)	$\Gamma \vdash \theta(s) : \text{str}$	definition
1918			
1919			
1920	◊ PRINT		
1921			
1922			
1923			
1924	(1)	$\frac{\Delta \vdash e_1 : \text{cap} \quad \Delta \vdash e_2 : \text{str}}{\Delta \vdash e_1 \cdot \text{print}(e_2) : \text{unit}}$	PRINT
1925			
1926	(2)	$\Delta \vdash e_1 : \text{cap}$	inversion
1927			
1928	(3)	$\Delta \vdash e_2 : \text{str}$	inversion
1929			
1930	(4)	$\Gamma \vdash \theta(e_1) : \text{cap}$	induction hypothesis (2)
1931	(5)	$\Gamma \vdash \theta(e_2) : \text{str}$	induction hypothesis (3)
1932			
1933	(6)	$\Gamma \vdash \theta(e_1) \cdot \text{print}(\theta(e_2)) : \text{unit}$	PRINT
1934			
1935	(7)	$\Gamma \vdash \theta(e_1 \cdot \text{print}(e_2)) : \text{unit}$	definition
1936			
1937	◊ □ I		
1938			
1939			
1940			
1941	(1)	$\frac{\Delta \vdash \textcolor{blue}{p} e : A}{\Delta \vdash \text{box}[\textcolor{teal}{e}] : \square A}$	□ I
1942			
1943			
1944	(2)	$\frac{\Delta \textcolor{blue}{p} \vdash e : A}{\Delta \vdash \textcolor{blue}{p} e : A}$	CTX-PURE
1945			
1946	(3)	$\Delta \textcolor{blue}{p} \vdash e : A$	inversion
1947			
1948	(4)	$\Gamma \textcolor{blue}{p} \vdash \theta \textcolor{blue}{p} : \Delta \textcolor{blue}{p}$	lemma A.6
1949			
1950	(5)	$\Gamma \textcolor{blue}{p} \vdash \theta \textcolor{blue}{p}(e) : A$	induction hypothesis (3) (4)
1951			
1952	(6)	$\Gamma \vdash \textcolor{blue}{p} \theta \textcolor{blue}{p}(e) : A$	CTX-PURE
1953			
1954	(7)	$\Gamma \vdash \text{box}[\theta \textcolor{blue}{p}(e)] : \square A$	□ I
1955			
1956			
1957	◊ □ E		
1958			
1959			
1960			

1961	$\Delta \vdash e_1 : \square A$	$\Delta, x : A^p \vdash e_2 : B$	
1962	(1) $\Delta \vdash \text{let box } [x] = e_1 \text{ in } e_2 : B$		$\square E$
1963			
1964	(2) $\Delta \vdash e_1 : \square A$		inversion
1965			
1966	(3) $\Delta, x : A^p \vdash e_2 : B$		inversion
1967			
1968	(4) $\Gamma, y : A^p \supseteq \Gamma$		$\supseteq\text{-WK}$
1969			
1970	(5) $\Gamma, y : A^p \vdash \theta : \Delta$		lemma A.5 (4)
1971			
1972	(6) $y : A^p \in \Gamma^p, y : A^p$		$\supseteq\text{-ID}$
1973			
1974	(7) $\Gamma^p, y : A^p \vdash y : A$		VAR
1975			
1976	(8) $\Gamma, y : A^p \vdash \langle \theta, y^p/x \rangle : \Delta, x : A^p$		SUB-PURE
1977			
1978	(9) $\Gamma, y : A^p \vdash \langle \theta, y^p/x \rangle(e_2) : B$		induction hypothesis (8) (3)
1979			
1980	(10) $\Gamma \vdash \theta(e_1) : \square A$		induction hypothesis (2)
1981			
1982	(11) $\Gamma \vdash \text{let box } [y] = \theta(e_1) \text{ in } \langle \theta, y^p/x \rangle(e_2) : B$		$\square E$ (9) (10)
1983			
1984	(12) $\Gamma \vdash \theta(\text{let box } [x] = e_1 \text{ in } e_2) : B$		definition
1985			
1986			□

B PROOFS FOR SECTION 4 (SEMANTICS)

LEMMA 4.5.

$$\begin{aligned} \text{curry/uncurry} &: \mathcal{H}om_{\mathcal{C}}(\Gamma \times A, B) \xrightarrow{\sim} \mathcal{H}om_{\mathcal{C}}(\Gamma, A \rightarrow B) \\ \text{ev}_{A,B} &: \mathcal{H}om_{\mathcal{C}}(A \rightarrow B \times A, B) \end{aligned}$$

PROOF. Let $f \in \mathcal{H}om_{\mathcal{C}}(\Gamma \times A, B)$. So $f \in (|\Gamma \times A|) \rightarrow |B| = (|\Gamma| \times |A|) \rightarrow |B|$, and

$$\forall \gamma, \forall a, w_B(f(\gamma, a)) \subseteq w_{\Gamma \times A}(\gamma, a) = w_{\Gamma}(\gamma) \cup w_A(a)$$

Now, $\hat{f} \in |\gamma| \rightarrow (|A| \rightarrow |B|)$, and we claim, $\hat{f} \in \mathcal{H}om_{\mathcal{C}}(\Gamma, A \rightarrow B)$.

For any γ , we want to show that, $\hat{f}(\gamma) \in |A \rightarrow B|$. Let $C = w_{A \rightarrow B}(\hat{f}(\gamma))$, and for any a , let $c \in w_B(\hat{f}(\gamma)(a))$. Either $c \in w_A(a)$, or $c \notin w_A(a)$. If $c \in w_A(a)$, then $c \in C \cup w_A(a)$ and we're done. If $c \notin w_A(a)$, then we've found an a such that $c \in w_B(f(a))$ and $c \notin w_A(a)$, hence $c \in C$, and $c \in C \cup w_A(a)$. Thus, $w_B(f(a)) \subseteq C \cup w_A(a)$.

Next, for any γ , we want to show that $w_{A \rightarrow B}(\hat{f}(\gamma)) \subseteq w_{\Gamma}(\gamma)$. Let $c \in w_{A \rightarrow B}(\hat{f}(\gamma))$, then there exists an a , such that $c \in w_B(\hat{f}(\gamma)(a))$ and $c \notin w_A(a)$. But, $w_B(\hat{f}(\gamma)(a)) = w_B(f(\gamma, a)) \subseteq w_{\Gamma}(\gamma) \cup w_A(a)$. Since $c \notin w_A(a)$, it must be the case that $c \in w_{\Gamma}(\gamma)$. Hence, $w_{A \rightarrow B}(\hat{f}(\gamma)) \subseteq w_{\Gamma}(\gamma)$.

For the other direction, let $\hat{g} \in \mathcal{H}om_{\mathcal{C}}(\Gamma, A \rightarrow B)$. So $\hat{g} \in |\Gamma| \rightarrow (|A \rightarrow B|)$ such that,

$$\forall \gamma, w_{A \rightarrow B}(\hat{g}(\gamma)) \subseteq w_{\Gamma}(\gamma)$$

Also, $\hat{g} \in |\Gamma| \rightarrow (|A| \rightarrow |B|)$, so $g \in |\Gamma \times A| \rightarrow |B|$, and we claim $g \in \mathcal{H}om_{\mathcal{C}}(\Gamma \times A, B)$.

2010 Now, for any γ, a , we want to show that $w_B(g(\gamma, a)) \subseteq w_{\Gamma \times A}(\gamma, a)$. Let $c \in w_B(g(\gamma, a))$.
 2011 For any $a \in |A|$, either $c \in w_A(a)$, or $c \notin w_A(a)$. If $c \in w_A(a)$, then $c \in w_\Gamma(\gamma) \cup w_A(a) =$
 2012 $w_{\Gamma \times A}(\gamma, a)$. If $c \notin w_A(a)$, then $c \in w_C(g(\gamma, a))$ and $c \notin w_A(a)$, so $c \in w_{A \rightarrow B}(\hat{g}(\gamma))$. Therefore,
 2013 $c \in w_\Gamma(\gamma)$, and $c \in w_\Gamma(\gamma) \cup w_A(a) = w_{\Gamma \times A}(\gamma, a)$. Hence, $w_B(\hat{g}(\gamma)(a)) \subseteq w_{\Gamma \times A}(\gamma, a)$. \square

2014 LEMMA B.1. The following diagrams commute.

2015

2016

The left diagram shows a commutative square with vertices T , TT , T , and T . The top horizontal arrow is ηT , the right vertical arrow is $T\eta$, and the bottom vertical arrow is μ . The right diagram shows a commutative square with vertices TTT , TT , TT , and T . The top horizontal arrow is μT , the right vertical arrow is μ , and the bottom horizontal arrow is μ .

2017

2018

2019

2020

2021

2022

2023

2024

2025

2026 PROOF.

2027

$$\begin{aligned} & \mu(\eta T(a, o)) & \mu(T\eta(a, o)) \\ = & \mu((a, \lambda c. e), o) & = \mu((a, o), \lambda c. e) \\ = & (a, \lambda c. o(c) \bullet e) & = (a, \lambda c. e \bullet o(c)) \\ = & (a, \lambda c. o(c)) & = (a, \lambda c. o(c)) \\ = & (a, o) & = (a, o) \end{aligned}$$

2028

2029

2030

2031

2032

2033

2034

2035

2036

2037

2038

2039

2040 LEMMA B.2. Strengthening with 1 is irrelevant.

2041

2042

2043

2044

2045

2046

2047

2048

2049 Consecutive applications of strength commute.

2050

2051

2052

2053

2054

2055

2056

2057

2058

$$\begin{array}{ccc} 1 \times TA & \xrightarrow{\quad} & TA \\ & \searrow \tau_{1,A} & \downarrow \\ & & T(1 \times A) \end{array}$$

$$\begin{array}{ccc} (A \times B) \times TC & \xrightarrow{\tau_{A \times B, C}} & T((A \times B) \times C) \\ \cong \downarrow & & \downarrow \cong \\ A \times (B \times TC) & \xrightarrow{\quad} & T(A \times (B \times C)) \\ \searrow A \times \tau_{B, C} & & \nearrow \tau_{A, B \times C} \\ & A \times T(B \times C) & \end{array}$$

2059 Strength commutes with monad unit and multiplication.

$$\begin{array}{ccccc}
 & & A \times B & & \\
 & \swarrow A \times \eta_B & & \searrow \eta_{A \times B} & \\
 A \times TB & \xrightarrow{\tau_{A,B}} & T(A \times B) & & \\
 \swarrow A \times \mu_B & & & & \nwarrow \mu_{A \times B} \\
 A \times T^2B & \xrightarrow{\tau_{A,TB}} & T(A \times TB) & \xrightarrow{T\tau_{A,B}} & T^2(A \times B)
 \end{array}$$

2067 Left are right strengths are compatible.

$$\begin{array}{ccc}
 A \times TB & \xrightarrow{\tau_{A,B}} & T(A \times B) \\
 \downarrow \beta_{A,TB} & & \downarrow T\beta_{A,B} \\
 TB \times A & \xrightarrow{\sigma_{B,A}} & T(B \times A)
 \end{array}$$

2075 PROOF. All monads on Set are strong, and Set is symmetric monoidal for products. Note that, T is not a commutative monad, because the following natural transformations are not equal.

$$\alpha : TA \times TB \xrightarrow{\sigma_{A,TB}} T(A \times TB) \xrightarrow{T\tau_{A,B}} T^2(A \times B) \xrightarrow{\mu_{A \times B}} T(A \times B)$$

$$\begin{aligned}
 \beta : TA \times TB &\xrightarrow{\tau_{TA,B}} T(TA \times B) \xrightarrow{T\sigma_{A,B}} T^2(A \times B) \xrightarrow{\mu_{A \times B}} T(A \times B) \\
 &= \sigma_{A,TB}((a, o_1), (b, o_2)) && \tau_{TA,B}((a, o_1), (b, o_2)) \\
 &= T\tau_{A,B}((a, (b, o_2)), o_1) && = T\sigma_{A,B}(((a, o_1), b), o_2) \\
 &= \mu_{A \times B}((a, b), o_2) && = \mu_{A \times B}((a, b), o_1) \\
 &= ((a, b), \lambda c. o_1(c) \bullet o_2(c)) && = ((a, b), \lambda c. o_2(c) \bullet o_1(c))
 \end{aligned}$$

2087 This means that the order of evaluation matters depending on whether we choose α or β for evaluating products. \square

2089 LEMMA B.3. The following diagrams commute.

$$\begin{array}{ccc}
 \square & \xleftarrow{\varepsilon \square} & \square \square \\
 & \nwarrow & \uparrow \delta \\
 & \square & \nearrow \square \varepsilon \\
 & \uparrow & \\
 \square \square \square & \xleftarrow{\delta \square} & \square \square
 \end{array}$$

2090

2091

2092

2093

2094

2095

2096

2097

2098

2099

2100

PROOF. Since δ and ε are identities, it follows trivially. Each arrow is weight-preserving because the weight is not altered by \square , δ , or ε . \square

LEMMA B.4.

$$\square TA \simeq \square A$$

2101

2102

2103

2104

2105

2106

2107

PROOF. Let $a \in |A|$ such that $(a, o) \in |\square TA|$. Since, $w_{TA}(a, o) = w_A(a) \cup \{c \in \mathcal{C} \mid o(c) \neq \varepsilon\} = \emptyset$, we have $w_A(a) = \emptyset$ and $o(c) = \varepsilon$ for all $c \in \mathcal{C}$. Hence, $a \in |\square A|$, and $o = \lambda c. \varepsilon$. This gives the map $\phi_A : \square TA \rightarrow \square A$, which is natural in A . We also have $\square \eta_A : \square A \rightarrow \square TA$ sending $a \in |A|$ to $(a, \lambda c. \varepsilon)$. This gives a bijection, which is weight-preserving. \square

2108 LEMMA 4.16.

$$\mathcal{H}om_{\mathcal{C}}(\Gamma \otimes A, B) \cong \mathcal{H}om_{\mathcal{C}}(\Gamma, A \multimap B)$$

2109 PROOF. Let $f \in \mathcal{H}om_{\mathcal{C}}(\Gamma \otimes A, B)$. So $f \in (|\Gamma \otimes A|) \rightarrow |B|$, and

$$\forall \gamma, \forall a, w_{\Gamma}(\gamma) \cap w_A(a) = \emptyset \Rightarrow w_B(f(\gamma, a)) \subseteq w_{\Gamma \otimes A}(\gamma, a) = w_{\Gamma}(\gamma) \cup w_A(a)$$

2110 Now, $\hat{f} \in |\gamma| \rightarrow (|A| \rightarrow |B|)$, and we claim, $\hat{f} \in \mathcal{H}om_{\mathcal{C}}(\Gamma, A \multimap B)$.

2111 For any γ , we want to show that $\hat{f}(\gamma) \in |A \multimap B|$. Let $C = w_{A \multimap B}(\hat{f}(\gamma))$, and for any a such
2112 that $C \cap w_A(a) = \emptyset$, let $c \in w_B(\hat{f}(\gamma)(a))$. Either $c \in w_A(a)$, or $c \notin w_A(a)$. If $c \in w_A(a)$, then
2113 $c \in C \cup w_A(a)$ and we're done. If $c \notin w_A(a)$, then we've found an a such that $c \in w_B(f(a))$ and
2114 $c \notin w_A(a)$, hence $c \in C$, and $c \in C \cup w_A(a)$. Thus, $w_B(f(a)) \subseteq C \cup w_A(a)$.

2115 Next, for any γ , we want to show that $w_{A \multimap B}(\hat{f}(\gamma)) \subseteq w_{\Gamma}(\gamma)$. Let $c \in w_{A \multimap B}(\hat{f}(\gamma))$, then
2116 there exists an a , such that $c \in w_B(\hat{f}(\gamma)(a))$ and $c \notin w_A(a)$. But, $w_B(\hat{f}(\gamma)(a)) = w_B(f(\gamma, a)) \subseteq$
2117 $w_{\Gamma}(\gamma) \cup w_A(a)$. Since $c \notin w_A(a)$, it must be the case that $c \in w_{\Gamma}(\gamma)$. Hence, $w_{A \multimap B}(\hat{f}(\gamma)) \subseteq$
2118 $w_{\Gamma}(\gamma)$.

2119 For the other direction, let $\hat{g} \in \mathcal{H}om_{\mathcal{C}}(\Gamma, A \multimap B)$. So $\hat{g} \in |\Gamma| \rightarrow (|A \multimap B|)$ such that,

$$\forall \gamma, w_{A \multimap B}(\hat{g}(\gamma)) \subseteq w_{\Gamma}(\gamma)$$

2120 Also, $\hat{g} \in |\Gamma| \rightarrow (|A| \rightarrow |B|)$, so $g \in |\Gamma \times A| \rightarrow |B| \subseteq |\Gamma \otimes A| \rightarrow |B|$, and we claim $g \in$
2121 $\mathcal{H}om_{\mathcal{C}}(\Gamma \otimes A, B)$.

2122 Now, for any γ, a , such that $w_{\Gamma}(\gamma) \cap w_A(a) = \emptyset$, we want to show that $w_B(g(\gamma, a)) \subseteq$
2123 $w_{\Gamma \otimes A}(\gamma, a)$. Let $c \in w_B(g(\gamma, a))$. For any $a \in |A|$, either $c \in w_A(a)$, or $c \notin w_A(a)$. If $c \in w_A(a)$,
2124 then $c \in w_{\Gamma}(\gamma) \cup w_A(a) = w_{\Gamma \otimes A}(\gamma, a)$. If $c \notin w_A(a)$, then $c \in w_C(g(\gamma, a))$ and $c \notin w_A(a)$,
2125 so $c \in w_{A \multimap B}(\hat{g}(\gamma))$. Therefore, $c \in w_{\Gamma}(\gamma)$, and $c \in w_{\Gamma}(\gamma) \cup w_A(a) = w_{\Gamma \otimes A}(\gamma, a)$. Hence,
2126 $w_B(g(\gamma, a)) \subseteq w_{\Gamma \otimes A}(\gamma, a)$. \square

C PROOFS FOR SECTION 5 (INTERPRETATION)

2134 LEMMA C.1. If $\Gamma \supseteq \Delta$, then

$$\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \Box \text{Wk}(\Gamma^{\textcolor{blue}{p}} \supseteq \Delta^{\textcolor{blue}{p}}) = \text{Wk}(\Gamma \supseteq \Delta) ; \rho(\Delta) ; \mathcal{M}(\Delta)$$

2137 PROOF. We do induction on $\Gamma \supseteq \Delta$.

$$\diamond \frac{}{\cdot \supseteq \cdot} \supseteq\text{-ID}$$

$$\boxed{\rho(\cdot) ; \mathcal{M}(\cdot) ; \Box \text{Wk}(\cdot^{\textcolor{blue}{p}} \supseteq \cdot^{\textcolor{blue}{p}})}$$

$$\asymp \text{definition } \rangle$$

$$\boxed{id_1 ; id_1 ; \Box id_1}$$

$$\asymp \Box \text{preserves } id \rangle$$

$$\boxed{id_1 ; id_1 ; id_1}$$

$$\asymp \text{definition } \rangle$$

$$\boxed{\text{Wk}(\cdot \supseteq \cdot) ; \rho(\cdot) ; \mathcal{M}(\cdot)}$$

$$\Gamma \supseteq \Delta$$

$$\diamond \frac{\Gamma \supseteq \Delta}{\Gamma, x : A^q \supseteq \Delta, x : A^q} \supseteq\text{-CONG}$$

2155 When $q = \textcolor{blue}{p}$,

2157 $\rho(\Gamma, \textcolor{teal}{x : A^p}) ; \mathcal{M}(\Gamma, \textcolor{teal}{x : A^p}) ; \square \text{Wk}(\Gamma^p, \textcolor{teal}{x : A^p} \supseteq \Delta^p, \textcolor{teal}{x : A^p})$

2158 $\asymp \text{definition } \rightarrow$

2159 $[\rho(\Gamma) \times id_{\square A}] ; [\mathcal{M}(\Gamma) \times \delta_A] ; m_{\Gamma^p, \square A}^x ; \square [\text{Wk}(\Gamma^p \supseteq \Delta^p) \times id_{\square A}]$

2160 $\asymp \text{monoidal action of } \square \rightarrow$

2161 $[\rho(\Gamma) \times id_{\square A}] ; [\mathcal{M}(\Gamma) \times \delta_A] ; [\square \text{Wk}(\Gamma^p \supseteq \Delta^p) \times \square id_{\square A}] ; m_{\Delta^p, \square A}^x$

2162 $\asymp \text{exchange law } \rightarrow$

2163 $[\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square \text{Wk}(\Gamma^p \supseteq \Delta^p) \times id_{\square A} ; \delta_A ; \square id_{\square A}] ; m_{\Delta^p, \square A}^x$

2164 $\asymp \text{identity law } \rightarrow$

2165 $[\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square \text{Wk}(\Gamma^p \supseteq \Delta^p) \times \delta_A] ; m_{\Delta^p, \square A}^x$

2166 $\asymp \text{induction hypothesis } \rightarrow$

2167 $[\text{Wk}(\Gamma \supseteq \Delta) ; \rho(\Delta) ; \mathcal{M}(\Delta) \times \delta_A] ; m_{\Delta^p, \square A}^x$

2168 $\asymp \text{identity law } \rightarrow$

2169 $[\text{Wk}(\Gamma \supseteq \Delta) ; \rho(\Delta) ; \mathcal{M}(\Delta) \times id_{\square A} ; id_{\square A} ; \delta_A] ; m_{\Delta^p, \square A}^x$

2170 $\asymp \text{exchange law } \rightarrow$

2171 $[\text{Wk}(\Gamma \supseteq \Delta) \times id_{\square A}] ; [\rho(\Delta) \times id_{\square A}] ; [\mathcal{M}(\Delta) \times \delta_A] ; m_{\Delta^p, \square A}^x$

2172 $\asymp \text{definition } \rightarrow$

2173 $\text{Wk}(\Gamma, \textcolor{teal}{x : A^p} \supseteq \Delta, \textcolor{teal}{x : A^p}) ; \rho(\Delta, \textcolor{teal}{x : A^p}) ; \mathcal{M}(\Delta, \textcolor{teal}{x : A^p})$

2181

When $q = i$,

2182 $\rho(\Gamma, \textcolor{teal}{x : A^i}) ; \mathcal{M}(\Gamma, \textcolor{teal}{x : A^i}) ; \square \text{Wk}((\Gamma, \textcolor{teal}{x : A^i})^p \supseteq (\Delta, \textcolor{teal}{x : A^i})^p)$

2183 $\asymp \text{definition } \rightarrow$

2184 $\rho(\Gamma, \textcolor{teal}{x : A^i}) ; \mathcal{M}(\Gamma, \textcolor{teal}{x : A^i}) ; \square \text{Wk}(\Gamma^p \supseteq \Delta^p)$

2185 $\asymp \text{definition } \rightarrow$

2186 $\pi_1 ; \rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square \text{Wk}(\Gamma^p \supseteq \Delta^p)$

2187 $\asymp \text{induction hypothesis } \rightarrow$

2188 $\pi_1 ; \text{Wk}(\Gamma \supseteq \Delta) ; \rho(\Delta) ; \mathcal{M}(\Delta)$

2189 $\asymp \text{definition of } \pi_1 \rightarrow$

2190 $\langle \pi_1 ; \text{Wk}(\Gamma \supseteq \Delta), \pi_2 ; id_A \rangle ; \pi_1 ; \rho(\Delta) ; \mathcal{M}(\Delta)$

2191 $\asymp \text{universal property of product } \rightarrow$

2192 $[\text{Wk}(\Gamma \supseteq \Delta) \times id_A] ; \pi_1 ; \rho(\Delta) ; \mathcal{M}(\Delta)$

2193 $\asymp \text{definition } \rightarrow$

2194 $\text{Wk}(\Gamma, \textcolor{teal}{x : A^i} \supseteq \Delta, \textcolor{teal}{x : A^i}) ; \rho(\Delta, \textcolor{teal}{x : A^i}) ; \mathcal{M}(\Delta, \textcolor{teal}{x : A^i})$

2202

2203

2204

2205

2206 $\diamond \frac{\Gamma \supseteq \Delta}{\Gamma, x : A^q \supseteq \Delta}$ \supseteq -wk
 2207 When $q = p$,
 2209

2210 $\boxed{\rho(\Gamma, x : A^p) ; \mathcal{M}(\Gamma, x : A^p) ; \square \text{Wk}(\Gamma^p, x : A^p \supseteq \Delta^p)}$
 2211 \equiv definition \rightarrow
 2212 $\boxed{[\rho(\Gamma) \times id_{\square A}] ; [\mathcal{M}(\Gamma) \times \delta_A] ; m_{\Gamma^p, \square A}^x ; \square (\pi_1 ; \text{Wk}(\Gamma^p \supseteq \Delta^p))}$
 2213 \equiv \square preserves composition \rightarrow
 2214 $\boxed{[\rho(\Gamma) \times id_{\square A}] ; [\mathcal{M}(\Gamma) \times \delta_A] ; m_{\Gamma^p, \square A}^x ; \square \pi_1 ; \square \text{Wk}(\Gamma^p \supseteq \Delta^p)}$
 2215 \equiv exchange law \rightarrow
 2216 $\boxed{[\rho(\Gamma) ; \mathcal{M}(\Gamma) \times id_{\square A} ; \delta_A] ; m_{\Gamma^p, \square A}^x ; \square \pi_1 ; \square \text{Wk}(\Gamma^p \supseteq \Delta^p)}$
 2217 \equiv identity law \rightarrow
 2218 $\boxed{[\rho(\Gamma) ; \mathcal{M}(\Gamma) \times \delta_A] ; m_{\Gamma^p, \square A}^x ; \square \pi_1 ; \square \text{Wk}(\Gamma^p \supseteq \Delta^p)}$
 2219 \equiv definition of m^x \rightarrow
 2220 $\boxed{[\rho(\Gamma) ; \mathcal{M}(\Gamma) \times \delta_A] ; \pi_1 ; \square \text{Wk}(\Gamma^p \supseteq \Delta^p)}$
 2221 \equiv universal property of product \rightarrow
 2222 $\boxed{\langle \pi_1 ; \rho(\Gamma) ; \mathcal{M}(\Gamma), \pi_2 ; \delta_A \rangle ; \pi_1 ; \square \text{Wk}(\Gamma^p \supseteq \Delta^p)}$
 2223 \equiv definition of π_1 \rightarrow
 2224 $\boxed{\pi_1 ; \rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square \text{Wk}(\Gamma^p \supseteq \Delta^p)}$
 2225 \equiv induction hypothesis \rightarrow
 2226 $\boxed{\pi_1 ; \text{Wk}(\Gamma \supseteq \Delta) ; \rho(\Delta) ; \mathcal{M}(\Delta)}$
 2227 \equiv definition \rightarrow
 2228 $\boxed{\text{Wk}(\Gamma, x : A^p \supseteq \Delta) ; \rho(\Delta) ; \mathcal{M}(\Delta)}$

2229 When $q = i$,
 2230
 2231 \equiv definition \rightarrow
 2232 $\boxed{\pi_1 ; \rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square \text{Wk}(\Gamma^p \supseteq \Delta^p)}$
 2233 \equiv induction hypothesis \rightarrow
 2234 $\boxed{\pi_1 ; \text{Wk}(\Gamma \supseteq \Delta) ; \rho(\Delta) ; \mathcal{M}(\Delta)}$
 2235 \equiv definition \rightarrow
 2236 $\boxed{\text{Wk}(\Gamma, x : A^i \supseteq \Delta) ; \rho(\Delta) ; \mathcal{M}(\Delta)}$

2237
 2238
 2239
 2240
 2241
 2242
 2243
 2244
 2245
 2246
 2247
 2248
 2249
 2250
 2251 LEMMA C.2. If $x : A^q \in \Delta$ and $\Gamma \supseteq \Delta$, then
 2252 $\llbracket x : A^q \in \Gamma \rrbracket = \text{Wk}(\Gamma \supseteq \Delta) ; \llbracket x : A^q \in \Delta \rrbracket$
 2253
 2254

□

PROOF. Assume $\Gamma \supseteq \Delta$. We do induction on $x : A^q \in \Delta$ followed by inversion on $\Gamma \supseteq \Delta$.

$$\diamond \frac{x : A^q \in (\Gamma, x : A^q)}{x : A^q \in (\Gamma, x : A^q)} \in\text{-ID}$$

When $q = i$,

$$\begin{aligned} & \boxed{\llbracket x : A^i \in (\Gamma, x : A^i) \rrbracket} \\ \asymp & \text{ definition } \rightarrow \\ & \boxed{\pi_2} \\ \asymp & \text{ identity law } \rightarrow \\ & \boxed{\pi_2 ; id_A} \\ \asymp & \text{ definition of } \pi_2 \rightarrow \\ & \boxed{\langle \pi_1 ; \text{Wk}(\Gamma \supseteq \Delta), \pi_2 ; id_A \rangle ; \pi_2} \\ \asymp & \text{ universal property of products } \rightarrow \\ & \boxed{[\text{Wk}(\Gamma \supseteq \Delta) \times id_A] ; \pi_2} \\ \asymp & \text{ definition } \rightarrow \\ & \boxed{\text{Wk}(\Gamma, x : A^i \supseteq \Delta, x : A^i) ; \llbracket x : A^i \in (\Delta, x : A^i) \rrbracket} \end{aligned}$$

When $q = p$,

$$\begin{aligned} & \boxed{\llbracket x : A^p \in (\Gamma, x : A^p) \rrbracket} \\ \asymp & \text{ definition } \rightarrow \\ & \boxed{\pi_2 ; \varepsilon_A} \\ \asymp & \text{ identity law } \rightarrow \\ & \boxed{\pi_2 ; id_{\square A} ; \varepsilon_A} \\ \asymp & \text{ definition of } \pi_2 \rightarrow \\ & \boxed{\langle \pi_1 ; \text{Wk}(\Gamma \supseteq \Delta), \pi_2 ; id_{\square A} \rangle ; \pi_2 ; \varepsilon_A} \\ \asymp & \text{ universal property of products } \rightarrow \\ & \boxed{[\text{Wk}(\Gamma \supseteq \Delta) \times id_{\square A}] ; \pi_2 ; \varepsilon_A} \\ \asymp & \text{ definition } \rightarrow \\ & \boxed{\text{Wk}(\Gamma, x : A^p \supseteq \Delta, x : A^p) ; \llbracket x : A^p \in (\Delta, x : A^p) \rrbracket} \end{aligned}$$

$$\diamond \frac{x : A^q \in \Gamma \quad (x \neq y)}{x : A^q \in (\Gamma, y : B^r)} \in\text{-EX}$$

When $r = i$,

$$\begin{aligned} & \boxed{\llbracket x : A^q \in (\Gamma, y : B^r) \rrbracket} \\ \asymp & \text{ definition } \rightarrow \\ & \boxed{\pi_1 ; \llbracket x : A^q \in \Gamma \rrbracket} \end{aligned}$$

2304 \models induction hypothesis \rangle
 2305 $\boxed{\pi_1 : \text{Wk}(\Gamma \supseteq \Delta) ; \llbracket x : A^q \in \Delta \rrbracket}$
 2306
 2307 \models definition of π_2 \rangle
 2308 $\boxed{\langle \pi_1 : \text{Wk}(\Gamma \supseteq \Delta), \pi_2 : id_B \rangle ; \pi_1 ; \llbracket x : A^q \in \Delta \rrbracket}$
 2309
 2310 \models universal property of products \rangle
 2311 $\boxed{[\text{Wk}(\Gamma \supseteq \Delta) \times id_B] ; \pi_1 ; \llbracket x : A^q \in \Delta \rrbracket}$
 2312
 2313 \models definition \rangle
 2314 $\boxed{\text{Wk}(\Gamma, y : B^r \supseteq \Delta, y : B^r) ; \llbracket x : A^q \in (\Delta, y : B^r) \rrbracket}$
 2315
 2316

When $r = p$,

2317
 2318 $\boxed{\llbracket x : A^q \in (\Gamma, y : B^r) \rrbracket}$
 2319
 2320 \models definition \rangle
 2321 $\boxed{\pi_1 ; \llbracket x : A^q \in \Gamma \rrbracket}$
 2322
 2323 \models induction hypothesis \rangle
 2324 $\boxed{\pi_1 : \text{Wk}(\Gamma \supseteq \Delta) ; \llbracket x : A^q \in \Delta \rrbracket}$
 2325
 2326 \models definition of π_2 \rangle
 2327 $\boxed{\langle \pi_1 : \text{Wk}(\Gamma \supseteq \Delta), \pi_2 : id_{\Box}B \rangle ; \pi_1 ; \llbracket x : A^q \in \Delta \rrbracket}$
 2328
 2329 \models universal property of products \rangle
 2330 $\boxed{[\text{Wk}(\Gamma \supseteq \Delta) \times id_{\Box}B] ; \pi_1 ; \llbracket x : A^q \in \Delta \rrbracket}$
 2331
 2332 \models definition \rangle
 2333 $\boxed{\text{Wk}(\Gamma, y : B^r \supseteq \Delta, y : B^r) ; \llbracket x : A^q \in (\Delta, y : B^r) \rrbracket}$
 2334
 2335
 2336

□

LEMMA 5.6 SEMANTIC WEAKENING. If $\Gamma \supseteq \Delta$ and $\Delta \vdash e : A$, then

$$\llbracket \Gamma \vdash e : A \rrbracket = \text{Wk}(\Gamma \supseteq \Delta) ; \llbracket \Delta \vdash e : A \rrbracket.$$

PROOF. We proceed by induction on $\Delta \vdash e : A$.

2340 \diamond
$$\frac{x : A^q \in \Gamma}{\Gamma \vdash x : A} \text{ VAR}$$

 2341
 2342
 2343
 2344 $\boxed{\llbracket \Gamma \vdash x : A \rrbracket}$
 2345
 2346 \models definition \rangle
 2347 $\boxed{\llbracket x : A^i \in \Gamma \rrbracket}$
 2348
 2349 \models lemma C.2 \rangle
 2350 $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; \llbracket x : A^i \in \Delta \rrbracket}$
 2351
 2352

- 2353 $\equiv \text{definition } \rightarrow$
 2354 $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash x : A]}$
- 2355
- 2356
- 2357
- 2358 $\diamond \frac{}{\Gamma \vdash () : \text{unit}} \text{unitI}$
 2359
- 2360
- 2361 $\boxed{[\Gamma \vdash () : \text{unit}]}$
- 2362 $\equiv \text{definition } \rightarrow$
 2363 $\boxed{!_\Gamma ; \eta_1}$
- 2364 $\equiv \text{universal property of } ! \rightarrow$
 2365 $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; !_\Delta ; \eta_1}$
- 2366 $\equiv \text{definition } \rightarrow$
 2367 $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash () : \text{unit}]}$
- 2368
- 2369
- 2370
- 2371 $\diamond \frac{\Gamma \vdash e_1 : A \quad \Gamma \vdash e_2 : B}{\Gamma \vdash (e_1, e_2) : A \times B} \times\text{I}$
 2372
- 2373
- 2374 $\boxed{[\Gamma \vdash (e_1, e_2) : A \times B]}$
- 2375 $\equiv \text{definition } \rightarrow$
 2376 $\boxed{\langle [\Gamma \vdash e_1 : A], [\Gamma \vdash e_2 : B] \rangle ; \beta_{A,B}}$
- 2377
- 2378 $\equiv \text{induction hypothesis } \rightarrow$
 2379 $\boxed{\langle \text{Wk}(\Gamma \supseteq \Delta) ; [\Gamma \vdash e_1 : A], \text{Wk}(\Gamma \supseteq \Delta) ; [\Gamma \vdash e_2 : B] \rangle ; \beta_{A,B}}$
- 2380
- 2381 $\equiv \text{universal property of products } \rightarrow$
 2382 $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; \langle [\Delta \vdash e_1 : A], [\Delta \vdash e_2 : B] \rangle ; \beta_{A,B}}$
- 2383
- 2384 $\equiv \text{definition } \rightarrow$
 2385 $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash (e_1, e_2) : A \times B]}$
- 2386
- 2387
- 2388
- 2389 $\diamond \frac{\Gamma \vdash e : A \times B}{\Gamma \vdash \text{fst } e : A} \times\text{E}_1$
 2390
- 2391
- 2392 $\boxed{[\Gamma \vdash \text{fst } e : A \times B]}$
- 2393 $\equiv \text{definition } \rightarrow$
 2394 $\boxed{[\Gamma \vdash e : A \times B] ; T\pi_1}$
- 2395 $\equiv \text{induction hypothesis } \rightarrow$
 2396 $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash e : A \times B] ; T\pi_1}$
- 2397
- 2398 $\equiv \text{definition } \rightarrow$
 2399
- 2400
- 2401

2402 $\text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash \text{fst } e : A]$

2403

2404

2405 $\diamond \frac{\Gamma \vdash e : A \times B}{\Gamma \vdash \text{snd } e : B} \times E_2$

2407

2408 $[\Gamma \vdash \text{snd } e : A \times B]$

2409

2410 $\equiv \text{definition } \rightarrow$

2411 $[\Gamma \vdash e : A \times B] ; T\pi_2$

2412

2413 $\equiv \text{induction hypothesis } \rightarrow$

2414 $\text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash e : A \times B] ; T\pi_2$

2415

2416 $\equiv \text{definition } \rightarrow$

2417 $\text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash \text{snd } e : B]$

2418

2419

2420 $\diamond \frac{\Gamma, x : A^i \vdash e : B}{\Gamma \vdash \lambda x : A. e : A \Rightarrow B} \Rightarrow I$

2421

2422

2423 $[\Gamma \vdash \lambda x. e : A \Rightarrow B]$

2424

2425 $\equiv \text{definition } \rightarrow$

2426 $\text{curry}([\Gamma, x : A^i \vdash e : B]) ; \eta_{A \rightarrow TB}$

2427

2428 $\equiv \text{induction hypothesis } \rightarrow$

2429 $\text{curry}(\text{Wk}(\Gamma, x : A^i \supseteq \Delta, x : A^i) ; [\Delta, x : A^i \vdash e : B]) ; \eta_{A \rightarrow TB}$

2430

2431 $\equiv \text{definition } \rightarrow$

2432 $\text{curry}([\text{Wk}(\Gamma \supseteq \Delta) \times id_A] ; [\Delta, x : A^i \vdash e : B]) ; \eta_{A \rightarrow TB}$

2433

2434 $\equiv \text{universal property of exponential } \rightarrow$

2435 $\text{Wk}(\Gamma \supseteq \Delta) ; \text{curry}([\Delta, x : A^i \vdash e : B]) ; \eta_{A \rightarrow TB}$

2436

2437 $\equiv \text{definition } \rightarrow$

2438 $\text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash \lambda x. e : A \Rightarrow B]$

2439

2440

2441 $\diamond \frac{\Gamma \vdash e_1 : A \Rightarrow B \quad \Gamma \vdash e_2 : A}{\Gamma \vdash e_1 e_2 : B} \Rightarrow E$

2442

2443 $[\Gamma \vdash e_1 e_2 : B]$

2444

2445 $\equiv \text{definition } \rightarrow$

2446 $\langle [\Gamma \vdash e_1 : A \Rightarrow B], [\Gamma \vdash e_2 : A] \rangle$

2447

2448 $; \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$

2449

2450

- 2451 \models induction hypothesis \rangle
 2452 $\langle \text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash e_1 : A \Rightarrow B] , \text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash e_2 : A] \rangle$
 2453 $; \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
- 2455 \models universal property of products \rangle
 2456 $\text{Wk}(\Gamma \supseteq \Delta) ; \langle [\Delta \vdash e_1 : A \Rightarrow B] , [\Delta \vdash e_2 : A] \rangle$
 2457 $; \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
- 2459 \models definition \rangle
 2460 $\text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash e_1 e_2 : B]$
- 2462
- 2463 $\diamond \frac{\Gamma \vdash e_1 : \text{cap} \quad \Gamma \vdash e_2 : \text{str}}{\Gamma \vdash e_1 \cdot \text{print}(e_2) : \text{unit}} \text{ PRINT}$
- 2465
- 2466
- 2467 $[\Gamma \vdash e_1 \cdot \text{print}(e_2) : \text{unit}]$
- 2468 \models definition \rangle
 2469 $\langle [\Gamma \vdash e_1 : \text{cap}] , [\Gamma \vdash e_2 : \text{str}] \rangle ; \beta_{C, \Sigma^*} ; Tp ; \mu_1$
- 2470
- 2471 \models induction hypothesis \rangle
 2472 $\langle \text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash e_1 : \text{cap}] , \text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash e_2 : \text{str}] \rangle ; \beta_{C, \Sigma^*} ; Tp ; \mu_1$
- 2473
- 2474 \models universal property of products \rangle
 2475 $\text{Wk}(\Gamma \supseteq \Delta) ; \langle [\Delta \vdash e_1 : \text{cap}] , [\Delta \vdash e_2 : \text{str}] \rangle ; \beta_{C, \Sigma^*} ; Tp ; \mu_1$
- 2476
- 2477 \models definition \rangle
 2478 $\text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash e_1 \cdot \text{print}(e_2) : \text{unit}]$
- 2479
- 2480
- 2481 $\diamond \frac{\Gamma \vdash \textcolor{blue}{p} e : A}{\Gamma \vdash \text{box}[\textcolor{blue}{e}] : \Box A} \Box I$
- 2482
- 2483
- 2484 $[\Gamma \vdash \text{box}[\textcolor{blue}{e}] : \Box A]$
- 2485
- 2486 \models definition \rangle
 2487 $[\Gamma \vdash \textcolor{blue}{p} e : A]_p ; \eta_{\Box A}$
- 2488
- 2489 \models definition \rangle
 2490 $\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \Box [\Gamma \textcolor{blue}{p} \vdash e : A] ; \phi_A ; \eta_{\Box A}$
- 2491
- 2492 \models induction hypothesis \rangle
 2493 $\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \Box (\text{Wk}(\Gamma \textcolor{blue}{p} \supseteq \Delta \textcolor{blue}{p}) ; [\Delta \textcolor{blue}{p} \vdash e : A]) ; \phi_A ; \eta_{\Box A}$
- 2494
- 2495 \models \Box preserves composition \rangle
 2496 $\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \Box \text{Wk}(\Gamma \textcolor{blue}{p} \supseteq \Delta \textcolor{blue}{p}) ; \Box [\Delta \textcolor{blue}{p} \vdash e : A] ; \phi_A ; \eta_{\Box A}$
- 2497 \models lemma C.1 \rangle
- 2498
- 2499

2500	$\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; \rho(\Delta) ; \mathcal{M}(\Delta) ; \square[\Delta^p \vdash e : A] ; \phi_A ; \eta_{\square A}}$
2501	$\preceq \text{definition } \rightarrow$
2502	$\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash^p e : A]_p ; \eta_{\square A}}$
2503	$\preceq \text{definition } \rightarrow$
2504	$\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash \text{box}[e] : \square A]}$
2505	
2506	
2507	
2508	
2509	$\diamond \frac{\Gamma \vdash e_1 : \square A \quad \Gamma, x : A^p \vdash e_2 : B}{\Gamma \vdash \text{let box}[x] = e_1 \text{ in } e_2 : B} \square E$
2510	
2511	
2512	$\boxed{[\Gamma \vdash \text{let box}[x] = e_1 \text{ in } e_2 : B]}$
2513	
2514	$\preceq \text{definition } \rightarrow$
2515	$\langle id_\Gamma, [\Gamma \vdash e_1 : \square A] \rangle ; \tau_{\Gamma, \square A} ; T[\Gamma, x : A^p \vdash e_2 : B] ; \mu_B$
2516	
2517	$\preceq \text{induction hypothesis } \rightarrow$
2518	$\langle id_\Gamma, \text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash e_1 : \square A] \rangle ; \tau_{\Gamma, \square A}$
2519	$; T(\text{Wk}(\Gamma, x : A^p \supseteq \Delta, x : A^p) ; [\Delta, x : A^p \vdash e_2 : B]) ; \mu_B$
2520	
2521	$\preceq \text{definition } \rightarrow$
2522	$\langle id_\Gamma, \text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash e_1 : \square A] \rangle ; \tau_{\Gamma, \square A}$
2523	$; T([\text{Wk}(\Gamma \supseteq \Delta) \times id_{\square A}] ; [\Delta, x : A^p \vdash e_2 : B]) ; \mu_B$
2524	
2525	$\preceq T \text{ preserves composition } \rightarrow$
2526	$\langle id_\Gamma, \text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash e_1 : \square A] \rangle ; \tau_{\Gamma, \square A}$
2527	$; T[\text{Wk}(\Gamma \supseteq \Delta) \times id_{\square A}] ; T[\Delta, x : A^p \vdash e_2 : B] ; \mu_B$
2528	
2529	$\preceq \text{tensorial strength of } T \rightarrow$
2530	$\langle id_\Gamma, \text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash e_1 : \square A] \rangle ; [\text{Wk}(\Gamma \supseteq \Delta) \times id_{T\square A}] ; \tau_{\Delta, \square A}$
2531	$; T[\Delta, x : A^p \vdash e_2 : B] ; \mu_B$
2532	
2533	$\preceq \text{composition of products } \rightarrow$
2534	$\langle id_\Gamma ; \text{Wk}(\Gamma \supseteq \Delta), \text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash e_1 : \square A] ; id_{T\square A} \rangle ; \tau_{\Delta, \square A}$
2535	$; T[\Delta, x : A^p \vdash e_2 : B] ; \mu_B$
2536	
2537	
2538	$\preceq \text{identity law } \rightarrow$
2539	$\langle \text{Wk}(\Gamma \supseteq \Delta) ; id_\Delta, \text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash e_1 : \square A] \rangle ; \tau_{\Delta, \square A}$
2540	$; T[\Delta, x : A^p \vdash e_2 : B] ; \mu_B$
2541	
2542	$\preceq \text{universal property of products } \rightarrow$
2543	$\text{Wk}(\Gamma \supseteq \Delta) ; \langle id_\Delta, [\Delta \vdash e_1 : \square A] \rangle ; \tau_{\Delta, \square A} ; T[\Delta, x : A^p \vdash e_2 : B] ; \mu_B$
2544	
2545	$\preceq \text{definition } \rightarrow$
2546	$\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash \text{let box}[x] = e_1 \text{ in } e_2 : B]}$
2547	
2548	

2549

2550

2551 LEMMA C.3. If $\Gamma \supseteq \Delta$ and $\Delta \vdash^p e : A$, then

2552

2553

$$\llbracket \Gamma \vdash^p e : A \rrbracket_p = \text{Wk}(\Gamma \supseteq \Delta) ; \llbracket \Delta \vdash^p e : A \rrbracket_p.$$

2554 PROOF.

2555

$$\llbracket \Gamma \vdash^p e : A \rrbracket_p$$

2557 \Leftarrow definition \rightarrow

$$\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square \llbracket \Gamma^p \vdash e : A \rrbracket ; \phi_A$$

2558 \Leftarrow semantic weakening lemma 5.6 \rightarrow

$$\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square (\text{Wk}(\Gamma^p \supseteq \Delta^p) ; \llbracket \Delta^p \vdash e : A \rrbracket) ; \phi_A$$

2559 \Leftarrow \square preserves composition \rightarrow

$$\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square \text{Wk}(\Gamma^p \supseteq \Delta^p) ; \square \llbracket \Delta^p \vdash e : A \rrbracket ; \phi_A$$

2560 \Leftarrow lemma C.1 \rightarrow

$$\text{Wk}(\Gamma \supseteq \Delta) ; \rho(\Delta) ; \mathcal{M}(\Delta) ; \llbracket \Delta^p \vdash e : A \rrbracket ; \phi_A$$

2561 \Leftarrow definition \rightarrow

$$\text{Wk}(\Gamma \supseteq \Delta) ; \llbracket \Delta \vdash^p e : A \rrbracket_p$$

2562

2563

2564

2565

2566

2567

2568

2569

2570

2571

2572

2573

2574 LEMMA C.4. If $\Gamma \supseteq \Delta$ and $\Delta \vdash v : A$, then

2575

2576

$$\llbracket \Gamma \vdash v : A \rrbracket_v = \text{Wk}(\Gamma \supseteq \Delta) ; \llbracket \Delta \vdash v : A \rrbracket_v.$$

2577 PROOF. Assuming $\Gamma \supseteq \Delta$, we do induction on $\Delta \vdash v : A$.

2578

2579

2580

$$\diamond \frac{x : A^q \in \Gamma}{\Gamma \vdash x : A} \text{ VAR}$$

2581

2582

$$\llbracket \Gamma \vdash v : A \rrbracket_v$$

2583 \Leftarrow definition \rightarrow

$$\llbracket x : A^q \in \Gamma \rrbracket$$

2584 \Leftarrow lemma C.2 \rightarrow

$$\text{Wk}(\Gamma \supseteq \Delta) ; \llbracket x : A^q \in \Delta \rrbracket$$

2585 \Leftarrow definition \rightarrow

$$\text{Wk}(\Gamma \supseteq \Delta) ; \llbracket \Delta \vdash x : A \rrbracket_v$$

2586

2587

2588

2589

2590

2591

2592

2593

2594

2595

2596

2597

```

2598    $\llbracket \Gamma \vdash () : \text{unit} \rrbracket_v$ 
2599    $\equiv$  definition  $\rangle$ 
2600    $\boxed{!_\Gamma}$ 
2601    $\equiv$  universal property of 1  $\rangle$ 
2602    $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; !_\Delta}$ 
2603    $\equiv$  definition  $\rangle$ 
2604    $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; \llbracket \Gamma \vdash () : \text{unit} \rrbracket_v}$ 
2605
2606
2607
2608
2609    $\diamond \frac{\Gamma \vdash e_1 : A \quad \Gamma \vdash e_2 : B}{\Gamma \vdash (e_1, e_2) : A \times B} \times_I$ 
2610
2611
2612    $\llbracket \Gamma \vdash (v_1, v_2) : A \times B \rrbracket_v$ 
2613
2614    $\equiv$  definition  $\rangle$ 
2615    $\langle \llbracket \Gamma \vdash v_1 : A \rrbracket_v, \llbracket \Gamma \vdash v_2 : B \rrbracket_v \rangle$ 
2616
2617    $\equiv$  induction hypothesis  $\rangle$ 
2618    $\langle \text{Wk}(\Gamma \supseteq \Delta) ; \llbracket \Delta \vdash v_1 : A \rrbracket_v, \text{Wk}(\Gamma \supseteq \Delta) ; \llbracket \Delta \vdash v_2 : B \rrbracket_v \rangle$ 
2619
2620    $\equiv$  universal property of products  $\rangle$ 
2621    $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; \langle \llbracket \Delta \vdash v_1 : A \rrbracket_v, \llbracket \Delta \vdash v_2 : B \rrbracket_v \rangle}$ 
2622
2623    $\equiv$  definition  $\rangle$ 
2624    $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; \llbracket \Delta \vdash (v_1, v_2) : A \times B \rrbracket_v}$ 
2625
2626
2627    $\diamond \frac{\Gamma, \boxed{x : A^i \vdash e : B}}{\Gamma \vdash \lambda x : A. e : A \Rightarrow B} \Rightarrow_I$ 
2628
2629
2630    $\llbracket \Gamma \vdash \lambda x. e : A \Rightarrow B \rrbracket_v$ 
2631
2632    $\equiv$  definition  $\rangle$ 
2633    $\boxed{\text{curry} (\llbracket \Gamma, x : A^i \vdash e : B \rrbracket)}$ 
2634
2635    $\equiv$  semantic weakening lemma 5.6  $\rangle$ 
2636    $\boxed{\text{curry} (\text{Wk}(\Gamma, \boxed{x : A^i \supseteq \Delta, x : A^i}) ; \llbracket \Delta, x : A^i \vdash e : B \rrbracket)}$ 
2637
2638    $\equiv$  definition  $\rangle$ 
2639    $\boxed{\text{curry} ([\text{Wk}(\Gamma \supseteq \Delta) \times id_A] ; \llbracket \Delta, x : A^i \vdash e : B \rrbracket)}$ 
2640
2641    $\equiv$  universal property of exponential  $\rangle$ 
2642    $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; \text{curry} (\llbracket \Delta, x : A^i \vdash e : B \rrbracket)}$ 
2643
2644    $\equiv$  definition  $\rangle$ 
2645    $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; \llbracket \Delta \vdash \lambda x. e : A \Rightarrow B \rrbracket_v}$ 
2646

```

2647
 2648 $\diamond \frac{\Gamma \vdash^p e : A}{\Gamma \vdash \text{box}[e] : \Box A} \Box I$
 2649
 2650
 2651 $\boxed{\llbracket \Gamma \vdash \text{box}[e] : \Box A \rrbracket_v}$
 2652 \equiv definition \rangle
 2653 $\boxed{\llbracket \Gamma \vdash^p e : A \rrbracket_p}$
 2654 \equiv lemma C.3 \rangle
 2655 $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; \llbracket \Delta \vdash^p e : A \rrbracket_p}$
 2656 \equiv definition \rangle
 2657 $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; \llbracket \Delta \vdash \text{box}[e] : \Box A \rrbracket_v}$
 2658
 2659
 2660
 2661
 2662
 2663

□

2664 LEMMA C.5. If $\Gamma \supseteq \Delta$ and $\Delta \vdash \theta : \Psi$, then

$$\llbracket \Gamma \vdash \theta : \Psi \rrbracket = \text{Wk}(\Gamma \supseteq \Delta) ; \llbracket \Delta \vdash \theta : \Psi \rrbracket$$

2665 PROOF. Assume $\Gamma \supseteq \Delta$. We proceed by induction on $\Delta \vdash \theta : \Psi$.

2666
 2667 $\diamond \frac{}{\Gamma \vdash \langle \rangle : \cdot} \text{SUB-ID}$
 2668
 2669
 2670
 2671 $\boxed{\llbracket \Gamma \vdash \langle \rangle : \cdot \rrbracket}$
 2672 \equiv definition \rangle
 2673 $\boxed{!_\Gamma}$
 2674 \equiv universal property of 1 \rangle
 2675 $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; !_\Delta}$
 2676 \equiv definition \rangle
 2677 $\boxed{\text{Wk}(\Gamma \supseteq \Delta) ; \llbracket \Delta \vdash \langle \rangle : \cdot \rrbracket}$
 2678
 2679
 2680
 2681

2682
 2683 $\diamond \frac{\Gamma \vdash \theta : \Delta \quad \Gamma \vdash^p e : A}{\Gamma \vdash \langle \theta, e^p/x \rangle : \Delta, x : A^p} \text{SUB-PURE}$
 2684
 2685
 2686 $\boxed{\llbracket \Gamma \vdash \langle \theta, e^p/x \rangle : \Psi, x : A^p \rrbracket}$
 2687 \equiv definition \rangle
 2688 $\boxed{\langle \llbracket \Gamma \vdash \theta : \psi \rrbracket, \llbracket \Gamma \vdash^p e : A \rrbracket_p \rangle}$
 2689 \equiv induction hypothesis \rangle
 2690 $\boxed{\langle \text{Wk}(\Gamma \supseteq \Delta) ; \llbracket \Delta \vdash \theta : \psi \rrbracket, \llbracket \Gamma \vdash^p e : A \rrbracket_p \rangle}$
 2691 \equiv lemma C.3 \rangle
 2692
 2693
 2694
 2695

2696 $\langle \text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash \theta : \psi], \text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash^p e : A]_p \rangle$
 2697
 2698 \equiv universal property of products \rightarrow
 2699 $\text{Wk}(\Gamma \supseteq \Delta) ; \langle [\Delta \vdash \theta : \psi], [\Delta \vdash^p e : A]_p \rangle$
 2700
 2701 \equiv definition \rightarrow
 2702 $\text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash \langle \theta, e^p/x \rangle : \Psi, x : A^p]$
 2703

2704

2705 $\diamond \frac{\Gamma \vdash \theta : \Delta \quad \Gamma \vdash v : A}{\Gamma \vdash \langle \theta, v^i/x \rangle : \Delta, x : A^i}$ SUB-IMPURE
 2706
 2707

2708 $[\Gamma \vdash \langle \theta, v^i/x \rangle : \Psi, x : A^i]$
 2709
 2710 \equiv definition \rightarrow
 2711 $\langle [\Gamma \vdash \theta : \Psi], [\Gamma \vdash v : A]_v \rangle$
 2712
 2713 \equiv induction hypothesis \rightarrow
 2714 $\langle \text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash \theta : \Psi], [\Gamma \vdash v : A]_v \rangle$
 2715
 2716 \equiv lemma C.4 \rightarrow
 2717 $\langle \text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash \theta : \Psi], \text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash v : A]_v \rangle$
 2718
 2719 \equiv universal property of products \rightarrow
 2720 $\text{Wk}(\Gamma \supseteq \Delta) ; \langle [\Delta \vdash \theta : \Psi], [\Delta \vdash v : A]_v \rangle$
 2721
 2722 \equiv definition \rightarrow
 2723 $\text{Wk}(\Gamma \supseteq \Delta) ; [\Delta \vdash \langle \theta, v^i/x \rangle : \Psi, x : A^i]$

□

LEMMA C.6. If $\Gamma^p \vdash e : A^p$, then

$$\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square [\Gamma^p \vdash^p e : A]_p = [\Gamma \vdash^p e : A]_p ; \delta_A$$

PROOF.

2731 $\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square [\Gamma^p \vdash^p e : A]_p$
 2732
 2733 \equiv definition \rightarrow
 2734 $\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square (\rho(\Gamma^p) ; \mathcal{M}(\Gamma^p) ; \square [\Gamma^p \vdash e : A] ; \phi_A)$
 2735
 2736 \equiv \square preserves composition \rightarrow
 2737 $\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square \rho(\Gamma^p) ; \square \mathcal{M}(\Gamma^p) ; \square \square [\Gamma^p \vdash e : A] ; \square \phi_A$
 2738
 2739 \equiv definition \rightarrow
 2740 $\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square id_{\Gamma^p} ; \delta_{\Gamma^p} ; \delta_{\Gamma^p}^{-1} ; \square [\Gamma^p \vdash e : A] ; \phi_A ; \delta_A$
 2741
 2742 \equiv simplification \rightarrow
 2743 $\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square [\Gamma^p \vdash e : A] ; \phi_A ; \delta_A$

2745 \Rightarrow definition \rangle

$$\boxed{[\Gamma \vdash^p e : A]_p ; \delta_A}$$

2750 LEMMA C.7. If $\Gamma \vdash \theta : \Delta$, then \square

$$\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square [\Gamma^p \vdash \theta^p : \Delta^p] = [\Gamma \vdash \theta : \Delta] ; \rho(\Delta) ; \mathcal{M}(\Delta)$$

2754 PROOF. We do induction on $\Gamma \vdash \theta : \Delta$.

$$\diamond \frac{}{\Gamma \vdash \langle \rangle : \cdot} \text{SUB-ID}$$

$$\boxed{\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square [\Gamma^p \vdash \langle \rangle : \cdot]}$$

2759 \Rightarrow definition \rangle

$$\boxed{\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square !_{\Gamma^p}}$$

2762 \Rightarrow definition \rangle

$$\boxed{\rho(\Gamma) ; \mathcal{M}(\Gamma) ; !_{\square \Gamma^p}}$$

2765 \Rightarrow universal property of $1 \rangle$

$$\boxed{!_\Gamma}$$

2767 \Rightarrow identity law \rangle

$$\boxed{!_\Gamma ; id_1 ; id_1}$$

2770 \Rightarrow definition \rangle

$$\boxed{[\Gamma \vdash \langle \rangle : \cdot] ; \rho(\cdot) ; \mathcal{M}(\cdot)}$$

$$\diamond \frac{\Gamma \vdash \theta : \Delta \quad \Gamma \vdash^p e : A}{\Gamma \vdash \langle \theta, e^p/x \rangle : \Delta, x : A^p} \text{SUB-PURE}$$

$$\boxed{\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square [\Gamma^p \vdash \langle \theta^p, e^p/x \rangle : \Delta^p, x : A^p]}$$

2779 \Rightarrow definition \rangle

$$\boxed{\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square \langle [\Gamma^p \vdash \theta^p : \Delta^p], [\Gamma^p \vdash^p e : A]_p \rangle}$$

2782 \Rightarrow monoidal action of $\square \rangle$

$$\boxed{\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \langle \square [\Gamma^p \vdash \theta^p : \Delta^p], \square [\Gamma^p \vdash^p e : A]_p \rangle ; m_{\Delta^p, \square A}^\times}$$

2785 \Rightarrow universal property of products \rangle

$$\boxed{\langle \rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square [\Gamma^p \vdash \theta^p : \Delta^p], \rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square [\Gamma^p \vdash^p e : A]_p \rangle ; m_{\Delta^p, \square A}^\times}$$

2788 \Rightarrow induction hypothesis \rangle

$$\boxed{\langle [\Gamma \vdash \theta : \Delta] ; \rho(\Delta) ; \mathcal{M}(\Delta), \rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square [\Gamma^p \vdash^p e : A]_p \rangle ; m_{\Delta^p, \square A}^\times}$$

2791 \Rightarrow lemma C.6 \rangle

2794	$\langle \llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \rho(\Delta) ; \mathcal{M}(\Delta), \llbracket \Gamma \vdash^p e : A \rrbracket_p ; \delta_A \rangle ; m_{\Delta^p, \square A}^x$
2795	\equiv identity law \rangle
2796	$\langle \llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \rho(\Delta) ; \mathcal{M}(\Delta), \llbracket \Gamma \vdash^p e : A \rrbracket_p ; id_{\square A} ; \delta_A \rangle ; m_{\Delta^p, \square A}^x$
2797	\equiv universal property of products \rangle
2798	$\langle \llbracket \Gamma \vdash \theta : \Delta \rrbracket, \llbracket \Gamma \vdash^p e : A \rrbracket_p \rangle ; [\rho(\Delta) ; \mathcal{M}(\Delta) \times id_{\square A} ; \delta_A] ; m_{\Delta^p, \square A}^x$
2799	\equiv exchange law \rangle
2800	$\langle \llbracket \Gamma \vdash \theta : \Delta \rrbracket, \llbracket \Gamma \vdash^p e : A \rrbracket_p \rangle ; [\rho(\Delta) \times id_{\square A}] ; [\mathcal{M}(\Delta) \times \delta_A] ; m_{\Delta^p, \square A}^x$
2801	\equiv definition \rangle
2802	$\llbracket \Gamma \vdash \langle \theta, e^p/x \rangle : \Delta, x : A^p \rrbracket ; \rho(\Delta, x : A^p) ; \mathcal{M}(\Delta, x : A^p)$
2803	
2804	
2805	
2806	
2807	
2808	
2809	$\diamond \frac{\Gamma \vdash \theta : \Delta \quad \Gamma \vdash v : A}{\Gamma \vdash \langle \theta, v^i/x \rangle : \Delta, x : A^i}$ SUB-IMPURE
2810	
2811	
2812	$\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square \llbracket \Gamma^p \vdash \langle \theta, v^i/x \rangle^p : (\Delta, x : A^i)^p \rrbracket$
2813	
2814	\equiv definition \rangle
2815	$\llbracket \rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square \llbracket \Gamma^p \vdash \theta^p : \Delta^p \rrbracket \rrbracket$
2816	
2817	\equiv induction hypothesis \rangle
2818	$\llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \rho(\Delta) ; \mathcal{M}(\Delta)$
2819	
2820	\equiv definition of π_1 \rangle
2821	$\langle \llbracket \Gamma \vdash \theta : \Delta \rrbracket, \llbracket \Gamma \vdash v : A \rrbracket_v \rangle ; \pi_1 ; \rho(\Delta) ; \mathcal{M}(\Delta)$
2822	
2823	\equiv definition \rangle
2824	$\llbracket \Gamma \vdash \langle \theta, v^i/x \rangle : \Delta, x : A^i \rrbracket ; \rho(\Delta, x : A^i) ; \mathcal{M}(\Delta, x : A^i)$
2825	
2826	
2827	
2828	LEMMA C.8. For any context Γ ,
2829	$\text{Wk}(\Gamma \supseteq \Gamma^p) = \rho(\Gamma)$
2830	
2831	PROOF. We do induction on Γ .
2832	$\diamond \Gamma = \cdot$
2833	
2834	$\text{Wk}(\cdot \supseteq \cdot^p)$
2835	
2836	\equiv definition \rangle
2837	$\text{Wk}(\cdot \supseteq \cdot)$
2838	
2839	\equiv definition \rangle
2840	id_1
2841	
2842	

□

2843 \Rightarrow definition \rangle

2844 $\boxed{\rho(\cdot)}$

2845

2846

2847 $\diamond \Gamma = \Delta, x : A^q$

2848 When $q = p$,

2849

2850 $\boxed{\text{Wk}(\Delta, \boxed{x : A^p} \supseteq \Delta^p, x : A^p)}$

2851

2852 \Rightarrow definition \rangle

2853 $\boxed{[\text{Wk}(\Delta \supseteq \Delta^p) \times id_{\square A}]}$

2854

2855 \Rightarrow induction hypothesis \rangle

2856 $\boxed{[\rho(\Delta) \times id_{\square A}]}$

2857

2858 \Rightarrow definition \rangle

2859 $\boxed{\rho(\Delta, \boxed{x : A^p})}$

2860

2861 When $q = i$,

2862

2863 $\boxed{\text{Wk}(\Delta, \boxed{x : A^i} \supseteq \Delta^p)}$

2864

2865 \Rightarrow definition \rangle

2866 $\boxed{\pi_1 ; \text{Wk}(\Delta \supseteq \Delta^p)}$

2867

2868 \Rightarrow induction hypothesis \rangle

2869 $\boxed{\pi_1 ; \rho(\Delta)}$

2870

2871 \Rightarrow definition \rangle

2872 $\boxed{\rho(\Delta, \boxed{x : A^i})}$

2873

2874

□

2875 LEMMA 5.9 PURE INTERPRETATION. If $\Gamma \vdash^p e : A$, then

2876

2877

$$\llbracket \Gamma \vdash e : A \rrbracket = \llbracket \Gamma \vdash^p e : A \rrbracket_p ; \varepsilon_A ; \eta_A.$$

2878

2879 PROOF. Assume $\Gamma \vdash^p e : A$. By inversion, we have $\Gamma^p \vdash e : A$.

2880

2881 $\boxed{\llbracket \Gamma \vdash e : A \rrbracket}$

2882

2883 \Rightarrow semantic weakening lemma 5.6 \rangle

2884 $\boxed{\text{Wk}(\Gamma \supseteq \Gamma^p) ; \llbracket \Gamma^p \vdash e : A \rrbracket}$

2885

2886 \Rightarrow lemma C.8 \rangle

2887 $\boxed{\rho(\Gamma) ; \llbracket \Gamma^p \vdash e : A \rrbracket}$

2888

2889 \Rightarrow definition \rangle

2890 $\boxed{\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square \llbracket \Gamma^p \vdash e : A \rrbracket ; \varepsilon_{TA}}$

2891

$$\begin{aligned}
 & 2892 \boxed{\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square [\Gamma^p \vdash e : A] ; \phi_A ; \varepsilon_A ; \eta_A} \\
 & 2893 \quad \asymp \text{definition } \rightarrow \\
 & 2894 \quad \boxed{[\Gamma \vdash^p e : A]_p ; \varepsilon_A ; \eta_A} \\
 & 2895 \\
 & 2896 \\
 & 2897 \\
 & 2898 \quad \square
 \end{aligned}$$

LEMMA 5.10 VALUE INTERPRETATION. If $\Gamma \vdash v : A$, then

$$[\Gamma \vdash v : A] = [\Gamma \vdash v : A]_v ; \eta_A.$$

PROOF. We proceed by induction on $\Gamma \vdash v : A$.

$$\begin{aligned}
 & 2903 \diamond \frac{}{\Gamma \vdash () : \text{unit}} \text{unitI} \\
 & 2904 \quad \boxed{[\Gamma \vdash () : \text{unit}]} \\
 & 2905 \quad \asymp \text{definition } \rightarrow \\
 & 2906 \quad \boxed{!_\Gamma ; \eta_1} \\
 & 2907 \quad \asymp \text{definition } \rightarrow \\
 & 2908 \quad \boxed{[\Gamma \vdash () : \text{unit}]_v ; \eta_1} \\
 & 2909 \\
 & 2910 \\
 & 2911 \\
 & 2912 \\
 & 2913 \\
 & 2914 \diamond \frac{\Gamma \vdash v_1 : A \quad \Gamma \vdash v_2 : B}{\Gamma \vdash (v_1, v_2) : A \times B} \times I \\
 & 2915 \quad \boxed{[\Gamma \vdash (v_1, v_2) : A \times B]} \\
 & 2916 \quad \asymp \text{definition } \rightarrow \\
 & 2917 \quad \boxed{\langle [\Gamma \vdash v_1 : A], [\Gamma \vdash v_2 : B] \rangle ; \beta_{A,B}} \\
 & 2918 \quad \asymp \text{induction hypothesis } \rightarrow \\
 & 2919 \quad \boxed{\langle [\Gamma \vdash v_1 : A]_v, [\Gamma \vdash v_2 : B]_v \rangle ; \beta_{A,B}} \\
 & 2920 \quad \asymp \text{tensorial strength of } T \rightarrow \\
 & 2921 \quad \boxed{\langle [\Gamma \vdash v_1 : A]_v, [\Gamma \vdash v_2 : B]_v ; \eta_B \rangle ; \sigma_{A,B}} \\
 & 2922 \quad \asymp \text{tensorial strength of } T \rightarrow \\
 & 2923 \quad \boxed{\langle [\Gamma \vdash v_1 : A]_v, [\Gamma \vdash v_2 : B]_v ; \eta_{A \times B} \rangle ; \eta_{A \times B}} \\
 & 2924 \quad \asymp \text{definition } \rightarrow \\
 & 2925 \quad \boxed{[\Gamma \vdash (v_1, v_2) : A \times B]_v ; \eta_{A \times B}}
 \end{aligned}$$

$$\begin{aligned}
 & 2934 \diamond \frac{x : A^q \in \Gamma}{\Gamma \vdash x : A} \text{VAR} \\
 & 2935 \quad \boxed{[\Gamma \vdash x : A]}
 \end{aligned}$$

2941 \equiv definition \rangle
 2942 $\boxed{[\![x : A^q \in \Gamma]\!] ; \eta_A}$
 2943
 2944 \equiv definition \rangle
 2945 $\boxed{[\![\Gamma \vdash x : A]\!]_v ; \eta_A}$
 2946
 2947
 2948 $\diamond \frac{\Gamma, x : A^i \vdash e : B}{\Gamma \vdash \lambda x : A. e : A \Rightarrow B} \Rightarrow I$
 2949
 2950
 2951 $\boxed{[\![\Gamma \vdash \lambda x. e : A \Rightarrow B]\!]}$
 2952
 2953 \equiv definition \rangle
 2954 $\boxed{[\![\text{curry } (\Gamma, x : A^i \vdash e : B)]\!] ; \eta_{A \rightarrow TB}}$
 2955
 2956 \equiv definition \rangle
 2957 $\boxed{[\![\Gamma \vdash \lambda x. e : A \Rightarrow B]\!]_v ; \eta_{A \rightarrow TB}}$
 2958
 2959
 2960 $\diamond \frac{\Gamma \vdash p e : A}{\Gamma \vdash \text{box}[e] : \Box A} \Box I$
 2961
 2962
 2963 $\boxed{[\![\Gamma \vdash \text{box}[e] : \Box A]\!]}$
 2964
 2965 \equiv definition \rangle
 2966 $\boxed{[\![\Gamma \vdash p e : A]\!]_p ; \eta_{\Box A}}$
 2967
 2968 \equiv definition \rangle
 2969 $\boxed{[\![\Gamma \vdash \text{box}[e] : \Box A]\!]_v ; \eta_{\Box A}}$
 2970
 2971
 2972
 2973 \square
 2974 LEMMA C.9. If $\Gamma \vdash \theta : \Delta$ and $x : A^q \in \Delta$, then
 2975 $[\![\Gamma \vdash \theta[x] : A]\!] = [\![\Gamma \vdash \theta : \Delta]\!] ; [\![x : A^q \in \Delta]\!] ; \eta_A$
 2976
 2977 PROOF. We proceed by induction on $x : A^q \in \Delta$.
 2978 $\diamond \frac{x : A^q \in (\Gamma, x : A^q)}{\Gamma \vdash \langle \phi, e^p / x \rangle [x] : A} \in-ID$
 2979
 2980 When $q = p$,
 2981
 2982 $\boxed{[\![\Gamma \vdash \langle \phi, e^p / x \rangle [x] : A]\!]}$
 2983
 2984 \equiv definition \rangle
 2985 $\boxed{[\![\Gamma \vdash e : A]\!]}$
 2986
 2987 \equiv pure interpretation lemma 5.9 \rangle
 2988 $\boxed{[\![\Gamma \vdash p e : A]\!]_p ; \varepsilon_A ; \eta_A}$
 2989

2990 \equiv definition of $\pi_2 \rightarrow$
 2991 $\langle \llbracket \Gamma \vdash \phi : \Delta \rrbracket, \llbracket \Gamma \vdash^{\textcolor{teal}{p}} e : A \rrbracket_p ; \pi_2 ; \varepsilon_A ; \eta_A \rangle$
 2992
 2993 \equiv definition \rightarrow
 2994 $\llbracket \Gamma \vdash \langle \phi, \textcolor{teal}{e}^{\textcolor{teal}{p}} / x \rangle : \Delta, x : A^p \rrbracket ; \llbracket x : A^p \in (\Delta, x : A^p) \rrbracket ; \eta_A$
 2995
 2996

2997 When $q = \textcolor{violet}{i}$,
 2998

2999 $\llbracket \Gamma \vdash \langle \phi, v^i / x \rangle [x] : A \rrbracket$
 3000
 3001 \equiv definition \rightarrow
 3002 $\llbracket \Gamma \vdash v : A \rrbracket$
 3003
 3004 \equiv value interpretation lemma 5.10 \rightarrow
 3005 $\llbracket \Gamma \vdash v : A \rrbracket_v ; \eta_A$
 3006
 3007 \equiv definition of $\pi_2 \rightarrow$
 3008 $\langle \llbracket \Gamma \vdash \phi : \Delta \rrbracket, \llbracket \Gamma \vdash v : A \rrbracket_v ; \pi_2 ; \eta_A \rangle$
 3009
 3010 \equiv definition \rightarrow
 3011 $\llbracket \Gamma \vdash \langle \phi, v^i / x \rangle : \Delta, x : A^i \rrbracket ; \llbracket x : A^i \in (\Delta, x : A^i) \rrbracket ; \eta_A$
 3012

$$\diamond \frac{x : A^q \in \Gamma \quad (x \neq y)}{x : A^q \in (\Gamma, y : B^r)} \in\text{-ex}$$

3015 When $r = \textcolor{teal}{p}$

3016
 3017 $\llbracket \Gamma \vdash \langle \phi, \textcolor{teal}{e}^{\textcolor{teal}{p}} / y \rangle [x] : A \rrbracket$
 3018
 3019 \equiv definition \rightarrow
 3020 $\llbracket \Gamma \vdash \phi[x] : A \rrbracket$
 3021
 3022 \equiv induction hypothesis \rightarrow
 3023 $\llbracket \Gamma \vdash \phi : \Delta \rrbracket ; \llbracket x : A^q \in \Delta \rrbracket ; \eta_A$
 3024
 3025 \equiv definition of $\pi_1 \rightarrow$
 3026 $\langle \llbracket \Gamma \vdash \phi : \Delta \rrbracket, \llbracket \Gamma \vdash^{\textcolor{teal}{p}} e : B \rrbracket ; \pi_1 ; \llbracket x : A^q \in \Delta \rrbracket ; \eta_A \rangle$
 3027
 3028 \equiv definition \rightarrow
 3029 $\llbracket \Gamma \vdash \langle \phi, \textcolor{teal}{e}^{\textcolor{teal}{p}} / y \rangle : \Delta, y : B^p \rrbracket ; \pi_1 ; \llbracket x : A^q \in \Delta \rrbracket ; \eta_A$
 3030
 3031 \equiv definition \rightarrow
 3032 $\llbracket \Gamma \vdash \langle \phi, \textcolor{teal}{e}^{\textcolor{teal}{p}} / y \rangle : \Delta, y : B^p \rrbracket ; \llbracket x : A^q \in (\Delta, y : B^p) \rrbracket ; \eta_A$
 3033

3034
 3035 When $r = \textcolor{violet}{i}$,
 3036

3039 $\llbracket \Gamma \vdash \langle \phi, v^i/y \rangle[x] : A \rrbracket$
 3040
 3041 \equiv definition \rightarrow
 3042 $\llbracket \Gamma \vdash \phi[x] : A \rrbracket$
 3043
 3044 \equiv induction hypothesis \rightarrow
 3045 $\llbracket \Gamma \vdash \phi : \Delta \rrbracket ; \llbracket x : A^q \in \Delta \rrbracket ; \eta_A$
 3046
 3047 \equiv definition of π_1 \rightarrow
 3048 $\langle \llbracket \Gamma \vdash \phi : \Delta \rrbracket, \llbracket \Gamma \vdash v : B \rrbracket ; \pi_1 ; \llbracket x : A^q \in \Delta \rrbracket ; \eta_A$
 3049
 3050 \equiv definition \rightarrow
 3051 $\llbracket \Gamma \vdash \langle \phi, v^i/y \rangle : \Delta, y : B^i \rrbracket ; \pi_1 ; \llbracket x : A^q \in \Delta \rrbracket ; \eta_A$
 3052
 3053 \equiv definition \rightarrow
 3054 $\llbracket \Gamma \vdash \langle \phi, v^i/y \rangle : \Delta, y : B^i \rrbracket ; \llbracket x : A^q \in (\Delta, y : B^i) \rrbracket ; \eta_A$
 3055
 3056
 3057

□

THEOREM 5.11 SEMANTIC SUBSTITUTION. If $\Gamma \vdash \theta : \Delta$ and $\Delta \vdash e : A$, then

$$\llbracket \Gamma \vdash \theta(e) : A \rrbracket = \llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash e : A \rrbracket$$

PROOF. Assume $\Gamma \vdash \theta : \Delta$. We proceed by induction on $\Delta \vdash e : A$.

$$\diamond \frac{x : A^q \in \Gamma}{\Gamma \vdash x : A} \text{ VAR}$$

3065 $\llbracket \Gamma \vdash \theta(x) : A \rrbracket$
 3066
 3067 \equiv definition \rightarrow
 3068 $\llbracket \Gamma \vdash \theta[x] : A \rrbracket$
 3069
 3070 \equiv lemma C.9 \rightarrow
 3071 $\llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket x : A^q \in \Delta \rrbracket ; \eta_A$
 3072
 3073 \equiv definition \rightarrow
 3074 $\llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash x : A \rrbracket$
 3075
 3076

$$\diamond \frac{}{\Gamma \vdash () : \text{unit}} \text{ unitI}$$

3080 $\llbracket \Gamma \vdash \theta(()) : \text{unit} \rrbracket$
 3081
 3082 \equiv definition \rightarrow
 3083 $\llbracket \Gamma \vdash () : \text{unit} \rrbracket$
 3084
 3085 \equiv definition \rightarrow
 3086 $!_\Gamma ; \eta_1$
 3087

3088 \equiv universal property of 1 \rangle
 3089 $\boxed{[\Gamma \vdash \theta : \Delta] ; !_\Delta : \eta_1}$
 3090
 3091 \equiv definition \rangle
 3092 $\boxed{[\Gamma \vdash \theta : \Delta] ; [\Delta \vdash () : \text{unit}]}$
 3093
 3094
 3095 $\diamond \frac{\Gamma \vdash e_1 : A \quad \Gamma \vdash e_2 : B}{\Gamma \vdash (e_1, e_2) : A \times B} \times_I$
 3096
 3097
 3098 $\boxed{[\Gamma \vdash \theta((e_1, e_2)) : A \times B]}$
 3099
 3100 \equiv definition \rangle
 3101 $\boxed{[\Gamma \vdash (\theta(e_1), \theta(e_2)) : A \times B]}$
 3102
 3103 \equiv definition \rangle
 3104 $\boxed{\langle [\Gamma \vdash \theta(e_1) : A], [\Gamma \vdash \theta(e_2) : B] \rangle ; \beta_{A,B}}$
 3105
 3106 \equiv induction hypothesis \rangle
 3107 $\boxed{\langle [\Gamma \vdash \theta : \Delta] ; [\Delta \vdash e_1 : A], [\Gamma \vdash \theta : \Delta] ; [\Delta \vdash e_2 : B] \rangle ; \beta_{A,B}}$
 3108 \equiv universal property of products \rangle
 3109 $\boxed{[\Gamma \vdash \theta : \Delta] ; \langle [\Delta \vdash e_1 : A], [\Delta \vdash e_2 : B] \rangle ; \beta_{A,B}}$
 3110
 3111 \equiv definition \rangle
 3112 $\boxed{[\Gamma \vdash \theta : \Delta] ; [\Delta \vdash (e_1, e_2) : A \times B]}$
 3113
 3114
 3115 $\diamond \frac{\Gamma \vdash e : A \times B}{\Gamma \vdash \text{fst } e : A} \times_E 1$
 3116
 3117
 3118 $\boxed{[\Gamma \vdash \theta(\text{fst } e) : A]}$
 3119
 3120 \equiv definition \rangle
 3121 $\boxed{[\Gamma \vdash \text{fst } \theta(e) : A]}$
 3122
 3123 \equiv definition \rangle
 3124 $\boxed{[\Gamma \vdash \theta(e) : A \times B] ; T\pi_1}$
 3125
 3126 \equiv induction hypothesis \rangle
 3127 $\boxed{[\Gamma \vdash \theta : \Delta] ; [\Delta \vdash e : A \times B] ; T\pi_1}$
 3128
 3129 \equiv definition \rangle
 3130 $\boxed{[\Gamma \vdash \theta : \Delta] ; [\Delta \vdash \text{fst } e : A]}$
 3131
 3132
 3133 $\diamond \frac{\Gamma \vdash e : A \times B}{\Gamma \vdash \text{snd } e : B} \times_E 2$
 3134
 3135
 3136

3137	$\boxed{[\Gamma \vdash \theta(\text{snd } e) : B]}$
3138	$\asymp \text{definition } \rightarrow$
3139	$\boxed{[\Gamma \vdash \text{snd } \theta(e) : B]}$
3140	$\asymp \text{definition } \rightarrow$
3141	$\boxed{[\Gamma \vdash \theta(e) : A \times B] ; T\pi_2}$
3142	$\asymp \text{induction hypothesis } \rightarrow$
3143	$\boxed{[\Gamma \vdash \theta : \Delta] ; [\Delta \vdash e : A \times B] ; T\pi_2}$
3144	$\asymp \text{definition } \rightarrow$
3145	$\boxed{[\Gamma \vdash \theta : \Delta] ; [\Delta \vdash \text{snd } e : B]}$
3146	
3147	
3148	
3149	
3150	
3151	$\diamond \frac{\Gamma \vdash^p e : A}{\Gamma \vdash \text{box}[e] : \square A} \square I$
3152	
3153	
3154	$\boxed{[\Gamma \vdash \theta(\text{box } e) : \square A]}$
3155	$\asymp \text{definition } \rightarrow$
3156	$\boxed{[\Gamma \vdash \text{box } [\theta^p(e)] : \square A]}$
3157	$\asymp \text{definition } \rightarrow$
3158	$\boxed{[\Gamma \vdash^p \theta^p(e) : A]_p ; \eta_{\square A}}$
3159	$\asymp \text{definition } \rightarrow$
3160	$\boxed{\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square [\Gamma^p \vdash \theta^p(e) : A] ; \phi_A ; \eta_{\square A}}$
3161	$\asymp \text{definition } \rightarrow$
3162	$\boxed{\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square [\Gamma^p \vdash \theta^p(e) : A] ; \phi_A ; \eta_{\square A}}$
3163	$\asymp \text{induction hypothesis } \rightarrow$
3164	$\boxed{\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square [\Gamma^p \vdash \theta^p(e) : A] ; \phi_A ; \eta_{\square A}}$
3165	$\asymp \square \text{ preserves composition } \rightarrow$
3166	$\boxed{\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square [\Gamma^p \vdash \theta^p(e) : A] ; \phi_A ; \eta_{\square A}}$
3167	$\asymp \square \text{ preserves composition } \rightarrow$
3168	$\boxed{\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \square [\Gamma^p \vdash \theta^p(e) : A] ; \phi_A ; \eta_{\square A}}$
3169	$\asymp \text{lemma C.7 } \rightarrow$
3170	$\boxed{\Gamma \vdash \theta : \Delta ; \rho(\Delta) ; \mathcal{M}(\Delta) ; \square [\Delta^p \vdash e : A] ; \phi_A ; \eta_{\square A}}$
3171	$\asymp \text{definition } \rightarrow$
3172	$\boxed{\Gamma \vdash \theta : \Delta ; \rho(\Delta) ; \mathcal{M}(\Delta) ; \square [\Delta^p \vdash e : A] ; \phi_A ; \eta_{\square A}}$
3173	$\asymp \text{definition } \rightarrow$
3174	$\boxed{[\Gamma \vdash \theta : \Delta] ; [\Delta \vdash^p e : A]_p ; \eta_{\square A}}$
3175	$\asymp \text{definition } \rightarrow$
3176	$\boxed{[\Gamma \vdash \theta : \Delta] ; [\Delta \vdash \text{box } [e] : \square A]}$
3177	
3178	
3179	
3180	$\diamond \frac{\Gamma \vdash e_1 : \square A \quad \Gamma, x : A^p \vdash e_2 : B}{\Gamma \vdash \text{let box } [x] = e_1 \text{ in } e_2 : B} \square E$
3181	
3182	
3183	
3184	
3185	

3186 $\llbracket \Gamma \vdash \theta(\text{let box } \boxed{x} = e_1 \text{ in } e_2) : B \rrbracket$

3187 $\models \text{definition } \rightarrow$

3188 $\llbracket \Gamma \vdash \text{let box } \boxed{y} = \theta(e_1) \text{ in } \langle \theta, \boxed{y^p/x} \rangle(e_2) : B \rrbracket$

3189 $\models \text{definition } \rightarrow$

3190 $\langle id_\Gamma, \llbracket \Gamma \vdash \theta(e_1) : A \rrbracket ; \tau_{\Gamma, \square A} ; T[\Gamma, \boxed{y : A^p} \vdash \langle \theta, \boxed{y^p/x} \rangle(e_2) : B] ; \mu_B$

3191 $\models \text{induction hypothesis } \rightarrow$

3192 $\langle id_\Gamma, \llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash e_1 : A \rrbracket ; \tau_{\Gamma, \square A}$

3193 $; T(\llbracket \Gamma, \boxed{y : A^p} \vdash \langle \theta, \boxed{y^p/x} \rangle : \Delta, \boxed{x : A^p} \rrbracket ; \llbracket \Delta, \boxed{x : A^p} \vdash e_2 : B \rrbracket) ; \mu_B$

3194 $\models T \text{ preserves composition } \rightarrow$

3195 $\langle id_\Gamma, \llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash e_1 : A \rrbracket ; \tau_{\Gamma, \square A}$

3196 $; T[\Gamma, \boxed{y : A^p} \vdash \langle \theta, \boxed{y^p/x} \rangle : \Delta, \boxed{x : A^p}] ; T[\Delta, \boxed{x : A^p} \vdash e_2 : B] ; \mu_B$

3197 $\models \text{definition } \rightarrow$

3198 $\langle id_\Gamma, \llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash e_1 : A \rrbracket ; \tau_{\Gamma, \square A}$

3199 $; T(\llbracket \Gamma, \boxed{y : A^p} \vdash \theta : \Delta \rrbracket, \llbracket \Gamma, \boxed{y : A^p} \vdash^p y : A \rrbracket_p)$

3200 $; T[\Delta, \boxed{x : A^p} \vdash e_2 : B] ; \mu_B$

3201 $\models \text{lemma C.5 } \rightarrow$

3202 $\langle id_\Gamma, \llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash e_1 : A \rrbracket ; \tau_{\Gamma, \square A}$

3203 $; T(\text{Wk}(\Gamma, \boxed{y : A^p} \supseteq \Gamma) ; \llbracket \Gamma \vdash \theta : \Delta \rrbracket, \llbracket \Gamma, \boxed{y : A^p} \vdash^p y : A \rrbracket_p)$

3204 $; T[\Delta, \boxed{x : A^p} \vdash e_2 : B] ; \mu_B$

3205 $\models \text{definition } \rightarrow$

3206 $\langle id_\Gamma, \llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash e_1 : A \rrbracket ; \tau_{\Gamma, \square A}$

3207 $; T(\pi_1 : \llbracket \Gamma \vdash \theta : \Delta \rrbracket, \pi_2) ; T[\Delta, \boxed{x : A^p} \vdash e_2 : B] ; \mu_B$

3208 $\models \text{universal property of products } \rightarrow$

3209 $\langle id_\Gamma, \llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash e_1 : A \rrbracket ; \tau_{\Gamma, \square A}$

3210 $; T[\llbracket \Gamma \vdash \theta : \Delta \rrbracket \times id_{\square A}] ; T[\Delta, \boxed{x : A^p} \vdash e_2 : B] ; \mu_B$

3211 $\models \text{tensorial strength of } T \rightarrow$

3212 $\langle \llbracket \Gamma \vdash \theta : \Delta \rrbracket, id_\Delta, \llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash e_1 : A \rrbracket ; \tau_{\Delta, \square A}$

3213 $; T[\Delta, \boxed{x : A^p} \vdash e_2 : B] ; \mu_B$

3214 $\models \text{universal property of products } \rightarrow$

3215 $\llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \langle id_\Delta, \llbracket \Delta \vdash e_1 : A \rrbracket ; \tau_{\Delta, \square A} ; T[\Delta, \boxed{x : A^p} \vdash e_2 : B] ; \mu_B$

3216 $\models \text{definition } \rightarrow$

3217 $\llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash \text{let box } \boxed{x} = e_1 \text{ in } e_2 : B \rrbracket$

3235	$\diamond \frac{\Gamma, x : A^i \vdash e : B}{\Gamma \vdash \lambda x : A. e : A \Rightarrow B} \Rightarrow I$	
3236		$\llbracket \Gamma \vdash \theta(\lambda x. e) : A \Rightarrow B \rrbracket$
3237	\asymp definition \rightarrow	
3238		$\llbracket \Gamma \vdash \lambda y. (\theta, y^i/x)(e) : A \Rightarrow B \rrbracket$
3239	\asymp definition \rightarrow	
3240		$\text{curry}(\llbracket \Gamma, y : A^i \vdash (\theta, y^i/x)(e) : B \rrbracket ; \eta_{A \rightarrow TB})$
3241	\asymp induction hypothesis \rightarrow	
3242		$\text{curry}(\langle \llbracket \Gamma, y : A^i \vdash (\theta, y^i/x) : \Delta, x : A^i \rrbracket ; \llbracket \Delta, x : A^i \vdash e : B \rrbracket \rangle$
3243		$; \eta_{A \rightarrow TB}$
3244	\asymp definition \rightarrow	
3245		$\text{curry}(\langle \llbracket \Gamma, y : A^i \vdash \theta : \Delta \rrbracket, \llbracket \Gamma, y : A^i \vdash y : A \rrbracket_v ; \llbracket \Delta, x : A^i \vdash e : B \rrbracket \rangle$
3246		$; \eta_{A \rightarrow TB}$
3247	\asymp lemma C.5 \rightarrow	
3248		$\text{curry}(\langle \text{Wk}(\Gamma, y : A^i \supseteq \Gamma) ; \llbracket \Gamma \vdash \theta : \Delta \rrbracket, \pi_2 \rangle ; \llbracket \Delta, x : A^i \vdash e : B \rrbracket)$
3249		$; \eta_{A \rightarrow TB}$
3250	\asymp definition \rightarrow	
3251		$\text{curry}(\langle \pi_1 : \llbracket \Gamma \vdash \theta : \Delta \rrbracket, \pi_2 \rangle ; \llbracket \Delta, x : A^i \vdash e : B \rrbracket) ; \eta_{A \rightarrow TB}$
3252	\asymp universal property of products \rightarrow	
3253		$\text{curry}(\llbracket \llbracket \Gamma \vdash \theta : \Delta \rrbracket \times id_A \rrbracket ; \llbracket \Delta, x : A^i \vdash e : B \rrbracket) ; \eta_{A \rightarrow TB}$
3254	\asymp universal property of exponential \rightarrow	
3255		$\llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \text{curry}(\llbracket \Delta, x : A^i \vdash e : B \rrbracket) ; \eta_{A \rightarrow TB}$
3256	\asymp definition \rightarrow	
3257		$\llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash \lambda x. e : A \Rightarrow B \rrbracket$
3258		
3259		
3260		
3261		
3262		
3263		
3264		
3265		
3266		
3267		
3268		
3269		
3270		
3271		
3272	$\diamond \frac{\Gamma \vdash e_1 : A \Rightarrow B \quad \Gamma \vdash e_2 : A}{\Gamma \vdash e_1 e_2 : B} \Rightarrow E$	
3273		$\llbracket \Gamma \vdash \theta(e_1 e_2) : B \rrbracket$
3274	\asymp definition \rightarrow	
3275		$\llbracket \Gamma \vdash \theta(e_1) \theta(e_2) : B \rrbracket$
3276	\asymp definition \rightarrow	
3277		$\langle \llbracket \Gamma \vdash \theta(e_1) : A \Rightarrow B \rrbracket, \llbracket \Gamma \vdash \theta(e_2) : A \rrbracket \rangle ; \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
3278		
3279		
3280		
3281		
3282		
3283		

3284	\equiv	induction hypothesis \rightarrow
3285		$\langle \llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash e_1 : A \Rightarrow B \rrbracket , \llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash e_2 : A \rrbracket \rangle$
3286		$; \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
3287		
3288	\equiv	universal property of products \rightarrow
3289		$\llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \langle \llbracket \Delta \vdash e_1 : A \Rightarrow B \rrbracket , \llbracket \Delta \vdash e_2 : A \rrbracket \rangle ; \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
3290		
3291	\equiv	definition \rightarrow
3292		$\llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash e_1 e_2 : B \rrbracket$
3293		
3294		
3295		
3296	\diamond	$\frac{}{\Gamma \vdash s : \text{str}}$ strI
3297		
3298		$\llbracket \Gamma \vdash \theta(s) : \text{str} \rrbracket$
3299		
3300	\equiv	definition \rightarrow
3301		$\llbracket \Gamma \vdash s : \text{str} \rrbracket$
3302		
3303	\equiv	definition \rightarrow
3304		$\llbracket \Gamma \vdash \langle \cdot \rangle : \cdot \rrbracket ; \llbracket \cdot \vdash s : \text{str} \rrbracket$
3305		
3306	\equiv	universal property of 1 \rightarrow
3307		$\llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash \langle \cdot \rangle : \cdot \rrbracket ; \llbracket \cdot \vdash s : \text{str} \rrbracket$
3308	\equiv	definition \rightarrow
3309		$\llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash s : \text{str} \rrbracket$
3310		
3311		
3312	\diamond	$\frac{\Gamma \vdash e_1 : \text{cap} \quad \Gamma \vdash e_2 : \text{str}}{\Gamma \vdash e_1 \cdot \text{print}(e_2) : \text{unit}}$ PRINT
3313		
3314		
3315		
3316		$\llbracket \Gamma \vdash \theta(e_1 \cdot \text{print}(e_2)) : \text{unit} \rrbracket$
3317	\equiv	definition \rightarrow
3318		$\llbracket \Gamma \vdash \theta(e_1) \cdot \text{print}(\theta(e_2)) : \text{unit} \rrbracket$
3319		
3320	\equiv	definition \rightarrow
3321		$\langle \llbracket \Gamma \vdash \theta(e_1) : \text{cap} \rrbracket , \llbracket \Gamma \vdash \theta(e_2) : \text{str} \rrbracket \rangle ; \beta_{C, \Sigma^*} ; Tp ; \mu_1$
3322		
3323	\equiv	induction hypothesis \rightarrow
3324		$\langle \llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash e_1 : \text{cap} \rrbracket , \llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash e_2 : \text{str} \rrbracket \rangle ; \beta_{C, \Sigma^*} ; Tp ; \mu_1$
3325		
3326	\equiv	universal property of products \rightarrow
3327		$\llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \langle \llbracket \Delta \vdash e_1 : \text{cap} \rrbracket , \llbracket \Delta \vdash e_2 : \text{str} \rrbracket \rangle ; \beta_{C, \Sigma^*} ; Tp ; \mu_1$
3328	\equiv	definition \rightarrow
3329		$\llbracket \Gamma \vdash \theta : \Delta \rrbracket ; \llbracket \Delta \vdash e_1 \cdot \text{print}(e_2) : \text{unit} \rrbracket$
3330		
3331		
3332		

3333
3334
3335

□

D PROOFS FOR SECTION 6 (EQUATIONAL THEORY)3337 THEOREM 6.1 SOUNDNESS OF \approx . If $\Gamma \vdash e_1 \approx e_2 : A$, then $\llbracket \Gamma \vdash e_1 : A \rrbracket = \llbracket \Gamma \vdash e_2 : A \rrbracket$.3338 PROOF. We proceed by induction on $\Gamma \vdash e_1 \approx e_2 : A$.

3339
$$\diamond \frac{\Gamma \vdash e : A}{\Gamma \vdash e \approx e : A} \text{ REFL}$$

3340
$$\begin{array}{c} \boxed{\llbracket \Gamma \vdash e : A \rrbracket} \\ \Leftarrow \text{ reflexivity } \Rightarrow \\ \boxed{\llbracket \Gamma \vdash e : A \rrbracket} \end{array}$$

3341
$$\diamond \frac{\Gamma \vdash e_1 \approx e_2 : A}{\Gamma \vdash e_2 \approx e_1 : A} \text{ SYM}$$

3342
$$\begin{array}{c} \boxed{\llbracket \Gamma \vdash e_2 : A \rrbracket} \\ \Leftarrow \text{ induction hypothesis } \Rightarrow \\ \boxed{\llbracket \Gamma \vdash e_1 : A \rrbracket} \end{array}$$

3343
$$\diamond \frac{\Gamma \vdash e_1 \approx e_2 : A \quad \Gamma \vdash e_2 \approx e_3 : A}{\Gamma \vdash e_1 \approx e_3 : A} \text{ TRANS}$$

3344
$$\begin{array}{c} \boxed{\llbracket \Gamma \vdash e_1 : A \rrbracket} \\ \Leftarrow \text{ induction hypothesis } \Rightarrow \\ \boxed{\llbracket \Gamma \vdash e_2 : A \rrbracket} \\ \Leftarrow \text{ induction hypothesis } \Rightarrow \\ \boxed{\llbracket \Gamma \vdash e_3 : A \rrbracket} \end{array}$$

3345
$$\diamond \frac{\Gamma \vdash e_1 \approx e_2 : A \times B}{\Gamma \vdash \text{fst } e_1 \approx \text{fst } e_2 : A} \text{ fst -CONG}$$

3346
$$\begin{array}{c} \boxed{\llbracket \Gamma \vdash \text{fst } e_1 : A \rrbracket} \\ \Leftarrow \text{ definition } \Rightarrow \\ \boxed{\llbracket \Gamma \vdash e_1 : A \times B \rrbracket ; T\pi_1} \\ \Leftarrow \text{ induction hypothesis } \Rightarrow \\ \boxed{\llbracket \Gamma \vdash e_2 : A \times B \rrbracket ; T\pi_1} \\ \Leftarrow \text{ definition } \Rightarrow \end{array}$$

3382	$\llbracket \Gamma \vdash \text{fst } e_2 : A \rrbracket$
3383	
3384	
3385	$\diamond \frac{\Gamma \vdash e_1 \approx e_2 : A \times B}{\Gamma \vdash \text{snd } e_1 \approx \text{snd } e_2 : B}$ snd -CONG
3386	
3387	
3388	$\llbracket \Gamma \vdash \text{snd } e_1 : B \rrbracket$
3389	
3390	\equiv definition \rightarrow
3391	$\llbracket \Gamma \vdash e_1 : A \times B \rrbracket ; T\pi_2$
3392	
3393	\equiv induction hypothesis \rightarrow
3394	$\llbracket \Gamma \vdash e_2 : A \times B \rrbracket ; T\pi_2$
3395	
3396	\equiv definition \rightarrow
3397	$\llbracket \Gamma \vdash \text{snd } e_2 : B \rrbracket$
3398	
3399	
3400	$\diamond \frac{\Gamma \vdash e_1 \approx e_2 : A \quad \Gamma \vdash e_3 \approx e_4 : B}{\Gamma \vdash (e_1, e_3) \approx (e_2, e_4) : A \times B}$ PAIR-CONG
3401	
3402	
3403	$\llbracket \Gamma \vdash (e_1, e_3) : A \times B \rrbracket$
3404	
3405	\equiv definition \rightarrow
3406	$\langle \llbracket \Gamma \vdash e_1 : A \rrbracket, \llbracket \Gamma \vdash e_3 : B \rrbracket \rangle ; \beta_{A,B}$
3407	
3408	\equiv induction hypothesis \rightarrow
3409	$\langle \llbracket \Gamma \vdash e_2 : A \rrbracket, \llbracket \Gamma \vdash e_4 : B \rrbracket \rangle ; \beta_{A,B}$
3410	
3411	\equiv definition \rightarrow
3412	$\llbracket \Gamma \vdash (e_2, e_4) : A \times B \rrbracket$
3413	
3414	
3415	$\diamond \frac{\Gamma, x : A^i \vdash e_1 \approx e_2 : B}{\Gamma \vdash \lambda x : A. e_1 \approx \lambda x : A. e_2 : A \Rightarrow B}$ λ -CONG
3416	
3417	$\llbracket \Gamma \vdash \lambda x. e_1 : A \Rightarrow B \rrbracket$
3418	
3419	\equiv definition \rightarrow
3420	$\text{curry}(\llbracket \Gamma, x : A^i \vdash e_1 : B \rrbracket) ; \eta_{A \rightarrow TB}$
3421	
3422	\equiv induction hypothesis \rightarrow
3423	$\text{curry}(\llbracket \Gamma, x : A^i \vdash e_2 : B \rrbracket) ; \eta_{A \rightarrow TB}$
3424	
3425	\equiv definition \rightarrow
3426	$\llbracket \Gamma \vdash \lambda x. e_2 : A \Rightarrow B \rrbracket$
3427	
3428	
3429	
3430	

3431	$\diamond \frac{\Gamma \vdash e_1 \approx e_2 : A \Rightarrow B \quad \Gamma \vdash e_3 \approx e_4 : A}{\Gamma \vdash e_1 e_3 \approx e_2 e_4 : B}$	APP-CONG
3432		
3433		
3434	$\llbracket \Gamma \vdash e_1 e_3 : B \rrbracket$	
3435	\equiv definition \rangle	
3436	$\langle \llbracket \Gamma \vdash e_1 : A \Rightarrow B \rrbracket, \llbracket \Gamma \vdash e_3 : A \rrbracket ; \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$	
3437		
3438	\equiv induction hypothesis \rangle	
3439	$\langle \llbracket \Gamma \vdash e_2 : A \Rightarrow B \rrbracket, \llbracket \Gamma \vdash e_4 : A \rrbracket ; \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$	
3440		
3441	\equiv definition \rangle	
3442	$\llbracket \Gamma \vdash e_2 e_4 : B \rrbracket$	
3443		
3444		
3445		
3446	$\diamond \frac{\Gamma^p \vdash e_1 \approx e_2 : A}{\Gamma \vdash \text{box } \boxed{e_1} \approx \text{box } \boxed{e_2} : \Box A}$	box-CONG
3447		
3448		
3449	$\llbracket \Gamma \vdash \text{box } \boxed{e_1} : \Box A \rrbracket$	
3450		
3451	\equiv definition \rangle	
3452	$\llbracket \Gamma \vdash^p e_1 : A \rrbracket_p : \eta_{\Box A}$	
3453		
3454	\equiv definition \rangle	
3455	$\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \Box \llbracket \Gamma^p \vdash e_1 : A \rrbracket ; \phi_A ; \eta_{\Box A}$	
3456		
3457	\equiv induction hypothesis \rangle	
3458	$\rho(\Gamma) ; \mathcal{M}(\Gamma) ; \Box \llbracket \Gamma^p \vdash e_2 : A \rrbracket ; \phi_A ; \eta_{\Box A}$	
3459		
3460	\equiv definition \rangle	
3461	$\llbracket \Gamma \vdash^p e_2 : A \rrbracket_p : \eta_{\Box A}$	
3462		
3463	\equiv definition \rangle	
3464	$\llbracket \Gamma \vdash \text{box } \boxed{e_2} : \Box A \rrbracket$	
3465		
3466		
3467	$\diamond \frac{\Gamma \vdash e_1 \approx e_2 : \Box A \quad \Gamma, x : A^p \vdash e_3 \approx e_4 : B}{\Gamma \vdash (\text{let box } \boxed{x} = e_1 \text{ in } e_3) \approx (\text{let box } \boxed{x} = e_2 \text{ in } e_4) : B}$	let box-CONG
3468		
3469		
3470	$\llbracket \Gamma \vdash \text{let box } \boxed{x} = e_1 \text{ in } e_3 : B \rrbracket$	
3471		
3472	\equiv definition \rangle	
3473	$\langle id_\Gamma, \llbracket \Gamma \vdash e_1 : \Box A \rrbracket ; \tau_{\Gamma, \Box A} ; T \llbracket \Gamma, x : A^p \vdash e_3 : B \rrbracket ; \mu_B$	
3474		
3475	\equiv induction hypothesis \rangle	
3476	$\langle id_\Gamma, \llbracket \Gamma \vdash e_2 : \Box A \rrbracket ; \tau_{\Gamma, \Box A} ; T \llbracket \Gamma, x : A^p \vdash e_4 : B \rrbracket ; \mu_B$	
3477		
3478	\equiv definition \rangle	
3479		

3480	$\boxed{\llbracket \Gamma \vdash \text{let box } \boxed{x} = e_2 \text{ in } e_4 : B \rrbracket}$
3481	
3482	
3483	$\diamond \frac{\Gamma \vdash e_1 \approx e_2 : \text{cap} \quad \Gamma \vdash e_3 \approx e_4 : \text{str}}{\Gamma \vdash e_1 \cdot \text{print}(e_3) \approx e_2 \cdot \text{print}(e_4) : \text{unit}}$ print-CONG
3484	
3485	
3486	$\boxed{\llbracket \Gamma \vdash e_1 \cdot \text{print}(e_3) : \text{unit} \rrbracket}$
3487	
3488	$\equiv \text{definition } \rightarrow$
3489	$\boxed{\langle \llbracket \Gamma \vdash e_1 : \text{cap} \rrbracket, \llbracket \Gamma \vdash e_3 : \text{str} \rrbracket \rangle ; \beta_{C,\Sigma^*} ; Tp ; \mu_1}$
3490	
3491	$\equiv \text{induction hypothesis } \rightarrow$
3492	$\boxed{\langle \llbracket \Gamma \vdash e_2 : \text{cap} \rrbracket, \llbracket \Gamma \vdash e_4 : \text{str} \rrbracket \rangle ; \beta_{C,\Sigma^*} ; Tp ; \mu_1}$
3493	
3494	$\equiv \text{definition } \rightarrow$
3495	$\boxed{\llbracket \Gamma \vdash e_2 \cdot \text{print}(e_4) : \text{unit} \rrbracket}$
3496	
3497	
3498	$\diamond \frac{\Gamma \vdash v_1 : A \quad \Gamma \vdash v_2 : B}{\Gamma \vdash \text{fst } (v_1, v_2) \approx v_1 : A} \times_1 \beta$
3499	
3500	
3501	$\boxed{\llbracket \Gamma \vdash \text{fst } (v_1, v_2) : A \rrbracket}$
3502	
3503	$\equiv \text{definition } \rightarrow$
3504	$\boxed{\llbracket \Gamma \vdash (v_1, v_2) : A \times B \rrbracket ; T\pi_1}$
3505	
3506	$\equiv \text{value interpretation lemma 5.10 } \rightarrow$
3507	$\boxed{\llbracket \Gamma \vdash (v_1, v_2) : A \times B \rrbracket_v ; \eta_{A \times B} ; T\pi_1}$
3508	
3509	$\equiv \text{monad laws } \rightarrow$
3510	$\boxed{\llbracket \Gamma \vdash (v_1, v_2) : A \times B \rrbracket_v ; \pi_1 ; \eta_A}$
3511	
3512	$\equiv \text{definition } \rightarrow$
3513	$\boxed{\langle \llbracket \Gamma \vdash v_1 : A \rrbracket_v, \llbracket \Gamma \vdash v_2 : B \rrbracket_v \rangle ; \pi_1 ; \eta_A}$
3514	
3515	$\equiv \text{definition of } \pi_1 \rightarrow$
3516	$\boxed{\llbracket \Gamma \vdash v_1 : A \rrbracket_v ; \eta_A}$
3517	
3518	$\equiv \text{value interpretation lemma 5.10 } \rightarrow$
3519	$\boxed{\llbracket \Gamma \vdash v_1 : A \rrbracket}$
3520	
3521	$\diamond \frac{\Gamma \vdash v_1 : A \quad \Gamma \vdash v_2 : B}{\Gamma \vdash \text{snd } (v_1, v_2) \approx v_2 : B} \times_2 \beta$
3522	
3523	
3524	$\boxed{\llbracket \Gamma \vdash \text{snd } (v_1, v_2) : B \rrbracket}$
3525	
3526	$\equiv \text{definition } \rightarrow$
3527	$\boxed{\llbracket \Gamma \vdash (v_1, v_2) : A \times B \rrbracket ; T\pi_2}$
3528	

3529	\equiv	value interpretation lemma 5.10	\rangle
3530		$\boxed{[\Gamma \vdash (v_1, v_2) : A \times B]_v ; \eta_{A \times B} ; T\pi_2}$	
3531	\equiv	monad laws	\rangle
3532		$\boxed{[\Gamma \vdash (v_1, v_2) : A \times B]_v ; \pi_2 ; \eta_B}$	
3533	\equiv	definition	\rangle
3534		$\langle [\Gamma \vdash v_1 : A]_v , [\Gamma \vdash v_2 : B]_v \rangle ; \pi_2 ; \eta_B$	
3535	\equiv	definition of π_2	\rangle
3536		$\boxed{[\Gamma \vdash v_2 : B]_v ; \eta_B}$	
3537	\equiv	value interpretation lemma 5.10	\rangle
3538		$\boxed{[\Gamma \vdash v_2 : B]}$	
3539			
3540	\diamond	$\frac{\Gamma \vdash v : A \times B}{\Gamma \vdash v \approx (\text{fst } v, \text{snd } v) : A \times B} \times_\eta$	
3541		$\boxed{[\Gamma \vdash (\text{fst } v, \text{snd } v) : A \times B]}$	
3542	\equiv	definition	\rangle
3543		$\langle [\Gamma \vdash \text{fst } v : A] , [\Gamma \vdash \text{snd } v : B] \rangle ; \beta_{A,B}$	
3544	\equiv	definition	\rangle
3545		$\langle [\Gamma \vdash v : A \times B] ; T\pi_1 , [\Gamma \vdash v : A \times B] ; T\pi_2 \rangle ; \beta_{A,B}$	
3546	\equiv	value interpretation lemma 5.10	\rangle
3547		$\langle [\Gamma \vdash v : A \times B]_v ; \eta_{A \times B} ; T\pi_1 , [\Gamma \vdash v : A \times B]_v ; \eta_{A \times B} ; T\pi_2 \rangle ; \beta_{A,B}$	
3548	\equiv	monad laws	\rangle
3549		$\langle [\Gamma \vdash v : A \times B]_v ; \pi_1 ; \eta_A , [\Gamma \vdash v : A \times B]_v ; \pi_2 ; \eta_B \rangle ; \beta_{A,B}$	
3550	\equiv	universal property of products	\rangle
3551		$\boxed{[\Gamma \vdash v : A \times B]_v ; \langle \pi_1 ; \eta_A , \pi_2 ; \eta_B \rangle ; \beta_{A,B}}$	
3552	\equiv	universal property of products	\rangle
3553		$\boxed{[\Gamma \vdash v : A \times B]_v ; [\eta_A \times \eta_B] ; \beta_{A,B}}$	
3554	\equiv	diagram	\rangle
3555		$\boxed{[\Gamma \vdash v : A \times B]_v ; \eta_{A \times B}}$	
3556	\equiv	value interpretation lemma 5.10	\rangle
3557		$\boxed{[\Gamma \vdash v : A \times B]}$	
3558			
3559			
3560			
3561	\diamond	$\frac{\Gamma, x : A^i \vdash e : B \quad \Gamma \vdash v : A}{\Gamma \vdash (\lambda x : A. e) v \approx [v/x]e : B} \Rightarrow \beta$	
3562			
3563			
3564			
3565			
3566			
3567			
3568			
3569			
3570			
3571			
3572			
3573			
3574			
3575			
3576			
3577			

3578 $\llbracket \Gamma \vdash (\lambda x. e) v : B \rrbracket$
 3579 \asymp definition \rangle
 3580 $\quad \langle \llbracket \Gamma \vdash \lambda x. e : A \Rightarrow B \rrbracket, \llbracket \Gamma \vdash v : A \rrbracket \rangle ; \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
 3582 \asymp definition \rangle
 3583 $\quad \langle \text{curry}(\llbracket \Gamma, x : A^i \vdash e : B \rrbracket) ; \eta_{A \rightarrow TB}, \llbracket \Gamma \vdash v : A \rrbracket \rangle$
 3584 $\quad ; \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
 3586 \asymp value interpretation lemma 5.10 \rangle
 3587 $\quad \langle \text{curry}(\llbracket \Gamma, x : A^i \vdash e : B \rrbracket) ; \eta_{A \rightarrow TB}, \llbracket \Gamma \vdash v : A \rrbracket_v ; \eta_A \rangle$
 3588 $\quad ; \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
 3590 \asymp universal property of products \rangle
 3591 $\quad \langle \text{curry}(\llbracket \Gamma, x : A^i \vdash e : B \rrbracket), \llbracket \Gamma \vdash v : A \rrbracket_v \rangle$
 3592 $\quad ; [\eta_{A \rightarrow TB} \times \eta_A] ; \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
 3594 \asymp diagram \rangle
 3595 $\quad \langle \text{curry}(\llbracket \Gamma, x : A^i \vdash e : B \rrbracket), \llbracket \Gamma \vdash v : A \rrbracket_v \rangle$
 3596 $\quad ; \eta_{(A \rightarrow TB) \times A} ; T \text{ ev}_{A, TB} ; \mu_B$
 3598 \asymp monad laws \rangle
 3599 $\quad \langle \text{curry}(\llbracket \Gamma, x : A^i \vdash e : B \rrbracket), \llbracket \Gamma \vdash v : A \rrbracket_v \rangle ; \text{ev}_{A, TB}$
 3601 \asymp universal property of exponential \rangle
 3602 $\quad \langle id_\Gamma, \llbracket \Gamma \vdash v : A \rrbracket_v \rangle ; \llbracket \Gamma, x : A^i \vdash e : B \rrbracket$
 3604 \asymp definition \rangle
 3605 $\quad \langle \llbracket \Gamma \vdash \langle r \rangle : \Gamma \rrbracket, \llbracket \Gamma \vdash v : A \rrbracket_v \rangle ; \llbracket \Gamma, x : A^i \vdash e : B \rrbracket$
 3607 \asymp definition \rangle
 3608 $\quad \llbracket \Gamma \vdash \langle \langle r \rangle, v^i/x \rangle : \Gamma, x : A^i \rrbracket ; \llbracket \Gamma, x : A^i \vdash e : B \rrbracket$
 3610 \asymp semantic substitution theorem 5.11 \rangle
 3611 $\quad \llbracket \Gamma \vdash \langle \langle r \rangle, v^i/x \rangle(e) : B \rrbracket$
 3613 \asymp definition \rangle
 3614 $\quad \llbracket \Gamma \vdash [v/x]e : B \rrbracket$
 3616
 3617
 3618 $\diamond \frac{\Gamma \vdash v : A \Rightarrow B}{\Gamma \vdash v \approx \lambda x : A. vx : A \Rightarrow B} \Rightarrow^\eta \text{IMPURE}$
 3619
 3620
 3621 $\quad \llbracket \Gamma \vdash \lambda x. vx : A \Rightarrow B \rrbracket$
 3622 \asymp definition \rangle
 3624 $\quad \text{curry}(\llbracket \Gamma, x : A^i \vdash vx : B \rrbracket) ; \eta_{A \rightarrow TB}$
 3625
 3626

3627 \equiv definition \rangle
 3628 let $h = \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
 3629 in $\text{curry}(\langle \llbracket \Gamma, x : A^i \vdash v : A \Rightarrow B \rrbracket, \llbracket \Gamma, x : A^i \vdash x : A \rrbracket \rangle; h) ; \eta_{A \rightarrow TB}$
 3630
 3631 \equiv semantic weakening lemma 5.6 \rangle
 3632 let $f = \text{Wk}(\Gamma, x : A^i \supseteq \Gamma)$
 3633 let $g = \llbracket x : A^i \in \Gamma, x : A^i \rrbracket$
 3634 let $h = \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
 3635 in $\text{curry}(\langle f ; \llbracket \Gamma \vdash v : A \Rightarrow B \rrbracket, g ; \eta_A \rangle; h) ; \eta_{A \rightarrow TB}$
 3636
 3637 \equiv definition \rangle
 3638 let $h = \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
 3639 in $\text{curry}(\langle \pi_1 ; \llbracket \Gamma \vdash v : A \Rightarrow B \rrbracket, \pi_2 ; \eta_A \rangle; h) ; \eta_{A \rightarrow TB}$
 3640
 3641
 3642 \equiv value interpretation lemma 5.10 \rangle
 3643 let $h = \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
 3644 in $\text{curry}(\langle \pi_1 ; \llbracket \Gamma \vdash v : A \Rightarrow B \rrbracket_v ; \eta_{A \rightarrow TB}, \pi_2 ; \eta_A \rangle; h) ; \eta_{A \rightarrow TB}$
 3645
 3646 \equiv strength diagram and monad laws \rangle
 3647 $\text{curry}(\langle \pi_1 ; \llbracket \Gamma \vdash v : A \Rightarrow B \rrbracket_v, \pi_2 \rangle ; \text{ev}_{A, TB}) ; \eta_{A \rightarrow TB}$
 3648
 3649 \equiv universal property of products \rangle
 3650 $\text{curry}(\llbracket \Gamma \vdash v : A \Rightarrow B \rrbracket_v \times id_A) ; \text{ev}_{A, TB}) ; \eta_{A \rightarrow TB}$
 3651
 3652 \equiv universal property of exponential \rangle
 3653 $\llbracket \Gamma \vdash v : A \Rightarrow B \rrbracket_v ; \eta_{A \rightarrow TB}$
 3654
 3655 \equiv value interpretation lemma 5.10 \rangle
 3656 $\llbracket \Gamma \vdash v : A \Rightarrow B \rrbracket$
 3657
 3658
 3659 $\diamond \frac{\Gamma \vdash^p e : A \Rightarrow B}{\Gamma \vdash e \approx \lambda x : A. ex : A \Rightarrow B} \Rightarrow^\eta \text{-PURE}$
 3660
 3661
 3662 $\llbracket \Gamma \vdash \lambda x. ex : A \Rightarrow B \rrbracket$
 3663
 3664 \equiv definition \rangle
 3665 $\text{curry}(\llbracket \Gamma, x : A^i \vdash ex : B \rrbracket) ; \eta_{A \rightarrow TB}$
 3666
 3667 \equiv definition \rangle
 3668 let $h = \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
 3669 in $\text{curry}(\langle \llbracket \Gamma, x : A^i \vdash e : A \Rightarrow B \rrbracket, \llbracket \Gamma, x : A^i \vdash x : A \rrbracket \rangle; h) ; \eta_{A \rightarrow TB}$
 3670
 3671 \equiv semantic weakening lemma 5.6 \rangle
 3672
 3673
 3674
 3675

3676 $f = \text{Wk}(\Gamma, \boxed{x : A^i} \supseteq \Gamma)$
 3677 $\text{let } g = \llbracket \boxed{x : A^i} \in \Gamma, \boxed{x : A^i} \rrbracket$
 3678 $h = \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
 3680 $\text{in } \text{curry}(\langle f ; \llbracket \Gamma \vdash e : A \Rightarrow B \rrbracket, g ; \eta_A \rangle ; h) ; \eta_{A \rightarrow TB}$

3681 \equiv definition \rangle
 3682 $\text{let } h = \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
 3683 $\text{in } \text{curry}(\langle \pi_1 ; \llbracket \Gamma \vdash e : A \Rightarrow B \rrbracket, \pi_2 ; \eta_A \rangle ; h) ; \eta_{A \rightarrow TB}$

3685 \equiv pure interpretation lemma 5.9 \rangle
 3686 $\text{let } h = \beta_{A \rightarrow TB, A} ; T \text{ ev}_{A, TB} ; \mu_B$
 3688 $\text{in } \text{curry}(\langle \pi_1 ; \llbracket \Gamma \vdash p e : A \Rightarrow B \rrbracket_p ; \varepsilon_{A \rightarrow TB} ; \eta_{A \rightarrow TB}, \pi_2 ; \eta_A \rangle ; h) ; \eta_{A \rightarrow TB}$

3690 \equiv diagram and monad laws \rangle
 3691 $\text{curry}(\langle \pi_1 ; \llbracket \Gamma \vdash p e : A \Rightarrow B \rrbracket_p ; \varepsilon_{A \rightarrow TB}, \pi_2 \rangle ; \text{ev}_{A, TB}) ; \eta_{A \rightarrow TB}$

3693 \equiv universal property of products \rangle
 3694 $\text{curry}(\llbracket \Gamma \vdash p e : A \Rightarrow B \rrbracket_p ; \varepsilon_{A \rightarrow TB} \times id_A) ; \text{ev}_{A, TB} ; \eta_{A \rightarrow TB}$

3696 \equiv universal property of exponential \rangle
 3697 $\llbracket \Gamma \vdash p e : A \Rightarrow B \rrbracket_p ; \varepsilon_{A \rightarrow TB} ; \eta_{A \rightarrow TB}$

3699 \equiv pure interpretation lemma 5.9 \rangle
 3700 $\llbracket \Gamma \vdash e : A \Rightarrow B \rrbracket$

3701
 3702

3703 $\diamond \frac{\Gamma^p \vdash e_1 : A \quad \Gamma, \boxed{x : A^p} \vdash e_2 : B}{\Gamma \vdash \text{let box } \boxed{x} = \text{box } \boxed{e_1} \text{ in } e_2 \approx [e_1/x]e_2 : B} \blacksquare \beta$
 3704 $\llbracket \Gamma \vdash \text{let box } \boxed{x} = \text{box } \boxed{e_1} \text{ in } e_2 : B \rrbracket$

3705
 3706
 3707 \equiv definition \rangle
 3708 $\langle id_\Gamma, \llbracket \Gamma \vdash \text{box } \boxed{e_1} : \square A \rrbracket ; \tau_{\Gamma, \square A} ; T \llbracket \Gamma, \boxed{x : A^p} \vdash e_2 : B \rrbracket ; \mu_B \rangle$

3711 \equiv definition \rangle
 3712 $\langle id_\Gamma, \llbracket \Gamma \vdash p e_1 : A \rrbracket_p ; \eta_{\square A} \rangle ; \tau_{\Gamma, \square A} ; T \llbracket \Gamma, \boxed{x : A^p} \vdash e_2 : B \rrbracket ; \mu_B \rangle$

3714 \equiv strength commutes with unit \rangle
 3715 $\langle id_\Gamma, \llbracket \Gamma \vdash p e_1 : A \rrbracket_p \rangle ; \eta_{\Gamma \times \square A} ; T \llbracket \Gamma, \boxed{x : A^p} \vdash e_2 : B \rrbracket ; \mu_B \rangle$

3717 \equiv monad laws \rangle
 3718 $\langle id_\Gamma, \llbracket \Gamma \vdash p e_1 : A \rrbracket_p \rangle ; \llbracket \Gamma, \boxed{x : A^p} \vdash e_2 : B \rrbracket ; \eta_{TB} ; \mu_B \rangle$

3720 \equiv monad laws \rangle
 3721 $\langle id_\Gamma, \llbracket \Gamma \vdash p e_1 : A \rrbracket_p \rangle ; \llbracket \Gamma, \boxed{x : A^p} \vdash e_2 : B \rrbracket$

3723 \equiv definition \rangle

3725 $\langle \llbracket \Gamma \vdash \langle r \rangle : \Gamma \rrbracket, \llbracket \Gamma \vdash^p e_1 : A \rrbracket_p ; \llbracket \Gamma, x : A^p \vdash e_2 : B \rrbracket \rangle$
 3726
 3727 \equiv definition \rangle
 3728 $\llbracket \Gamma \vdash \langle \langle r \rangle, e_1^p/x \rangle : \Gamma, x : A^p \rrbracket ; \llbracket \Gamma, x : A^p \vdash e_2 : B \rrbracket \rangle$
 3729
 3730 \equiv semantic substitution theorem 5.11 \rangle
 3731 $\llbracket \Gamma \vdash \langle \langle r \rangle, e_1^p/x \rangle (e_2) : B \rrbracket \rangle$
 3732
 3733 \equiv definition \rangle
 3734 $\Gamma \vdash [e_1/x] e_2 : B$
 3735

$$\diamond \frac{\Gamma \vdash^p e : \square A \quad \Gamma \vdash C\langle\langle e \rangle\rangle : B \quad \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } C\langle\langle \text{box } \boxed{x} \rangle\rangle : B}{\Gamma \vdash C\langle\langle e \rangle\rangle \approx \text{let box } \boxed{x} = e \text{ in } C\langle\langle \text{box } \boxed{x} \rangle\rangle : B} \blacksquare \eta\text{-PURE}$$

We first make the following observation.

Observation.

3742 $\llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } C\langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket \rangle$
 3743
 3744 \equiv definition \rangle
 3745 $\begin{array}{l} \text{let } f = \llbracket \Gamma \vdash e : \square A \rrbracket \\ \quad g = \llbracket \Gamma, x : A^p \vdash C\langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket \\ \quad \text{in } \langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg ; \mu_B \end{array}$
 3746
 3747
 3748
 3749 \equiv pure interpretation lemma 5.9 \rangle
 3750 $\begin{array}{l} \text{let } f = \llbracket \Gamma \vdash^p e : \square A \rrbracket_p ; \varepsilon_{\square A} ; \eta_{\square A} \\ \quad g = \llbracket \Gamma, x : A^p \vdash C\langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket \\ \quad \text{in } \langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg ; \mu_B \end{array}$
 3751
 3752
 3753
 3754 \equiv simplification \rangle
 3755 $\begin{array}{l} \text{let } f = \llbracket \Gamma \vdash^p e : \square A \rrbracket_p ; \varepsilon_{\square A} \\ \quad g = \llbracket \Gamma, x : A^p \vdash C\langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket \\ \quad \text{in } \langle id_\Gamma, f \rangle ; \eta_{\square A} ; \tau_{\Gamma, \square A} ; Tg ; \mu_B \end{array}$
 3756
 3757
 3758
 3759
 3760 \equiv strength commutes with unit \rangle
 3761 $\begin{array}{l} \text{let } f = \llbracket \Gamma \vdash^p e : \square A \rrbracket_p ; \varepsilon_{\square A} \\ \quad g = \llbracket \Gamma, x : A^p \vdash C\langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket \\ \quad \text{in } \langle id_\Gamma, f \rangle ; \eta_{\Gamma \times \square A} ; Tg ; \mu_B \end{array}$
 3762
 3763
 3764
 3765 \equiv monad laws \rangle
 3766 $\begin{array}{l} \text{let } f = \llbracket \Gamma \vdash^p e : \square A \rrbracket_p ; \varepsilon_{\square A} \\ \quad g = \llbracket \Gamma, x : A^p \vdash C\langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket \\ \quad \text{in } \langle id_\Gamma, f \rangle ; g ; T\eta_B ; \mu_B \end{array}$
 3767
 3768
 3769
 3770
 3771 \equiv monad laws \rangle
 3772
 3773

3774 let $f = \llbracket \Gamma \vdash^p e : \square A \rrbracket_p ; \varepsilon_{\square A}$
 3775 g = $\llbracket \Gamma, x : A^p \vdash C \langle\!\langle \text{box } x \rangle\!\rangle : B \rrbracket$
 3776 in $\langle id_\Gamma, f \rangle ; g$

3778

3779

3780 Fixing f , we proceed by cases on C .3781 $\diamond C = [\cdot]$

3783

3784 $\llbracket \Gamma \vdash \text{let box } x = e \text{ in box } x : \square A \rrbracket$
 3785
 3786 \preceq observation \rangle
 3787 $\langle id_\Gamma, f \rangle ; \llbracket \Gamma, x : A^p \vdash \text{box } x : \square A \rrbracket$
 3788
 3789 \preceq definition \rangle
 3790 $\langle id_\Gamma, f \rangle ; \llbracket \Gamma, x : A^p \vdash^p x : A \rrbracket_p ; \eta_{\square A}$
 3791
 3792 \preceq definition \rangle
 3793 $\langle id_\Gamma, f \rangle ; \pi_2 ; \eta_{\square A}$
 3794
 3795 \preceq applying π_2 \rangle
 3796 $f ; \eta_{\square A}$
 3797
 3798 \preceq definition \rangle
 3799 $\llbracket \Gamma \vdash e : \square A \rrbracket$

3800

3801 $\diamond C = e_1 C_1$

3802

3803

3804

3805

3806

3807

3808

3809

3810

3811

3812

3813

3814

3815

3816

3817

3818

3819

3820

3821

3822

let $h_1 = \llbracket \Gamma, x : A^p \vdash e_1 : C \Rightarrow B \rrbracket$

let $h_2 = \llbracket \Gamma, x : A^p \vdash C_1 \langle\!\langle \text{box } x \rangle\!\rangle : C \rrbracket$

in $\langle id_\Gamma, f \rangle ; \langle h_1, h_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ ev}_{C, TB} ; \mu_B$

let $h_1 = \llbracket \Gamma \vdash e_1 : C \Rightarrow B \rrbracket$

let $h_2 = \llbracket \Gamma, x : A^p \vdash C_1 \langle\!\langle \text{box } x \rangle\!\rangle : C \rrbracket$

in $\langle id_\Gamma, f \rangle ; \langle \pi_1 ; h_1, h_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ ev}_{C, TB} ; \mu_B$

3823 let $h_1 = \llbracket \Gamma \vdash e_1 : C \Rightarrow B \rrbracket$
 3824 $h_2 = \llbracket \Gamma, x : A^p \vdash C_1 \langle\!\langle \text{box}[x] \rangle\!\rangle : C \rrbracket$
 3825 in $\langle\langle id_\Gamma, f \rangle ; \pi_1 ; h_1, \langle id_\Gamma, f \rangle ; h_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ ev}_{C, TB} ; \mu_B$
 3826
 3827 \preceq simplification \rangle
 3828
 3829 let $h_1 = \llbracket \Gamma \vdash e_1 : C \Rightarrow B \rrbracket$
 3830 $h_2 = \llbracket \Gamma, x : A^p \vdash C_1 \langle\!\langle \text{box}[x] \rangle\!\rangle : C \rrbracket$
 3831 in $\langle h_1, \langle id_\Gamma, f \rangle ; h_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ ev}_{C, TB} ; \mu_B$
 3832
 3833 \preceq observation \rangle
 3834 let $h_1 = \llbracket \Gamma \vdash e_1 : C \Rightarrow B \rrbracket$
 3835 $h_2 = \llbracket \Gamma \vdash \text{let box}[x] = e \text{ in } C_1 \langle\!\langle \text{box}[x] \rangle\!\rangle : C \rrbracket$
 3836 in $\langle h_1, h_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ ev}_{C, TB} ; \mu_B$
 3837
 3838 \preceq induction hypothesis \rangle
 3839 let $h_1 = \llbracket \Gamma \vdash e_1 : C \Rightarrow B \rrbracket$
 3840 $h_2 = \llbracket \Gamma \vdash C_1 \langle\!\langle e \rangle\!\rangle : C \rrbracket$
 3841 in $\langle h_1, h_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ ev}_{C, TB} ; \mu_B$
 3842
 3843 \preceq definition \rangle
 3844 $\llbracket \Gamma \vdash e_1 C_1 \langle\!\langle e \rangle\!\rangle : B \rrbracket$
 3845
 3846
 3847
 3848 $\diamond C = C_1 e_1$
 3849
 3850
 3851 $\llbracket \Gamma \vdash \text{let box}[x] = e \text{ in } C_1 \langle\!\langle \text{box}[x] \rangle\!\rangle e_1 : B \rrbracket$
 3852 \preceq observation \rangle
 3853 $\langle id_\Gamma, f \rangle ; \llbracket \Gamma, x : A^p \vdash C_1 \langle\!\langle \text{box}[x] \rangle\!\rangle e_1 : B \rrbracket$
 3854
 3855 \preceq definition \rangle
 3856 let $h_1 = \llbracket \Gamma, x : A^p \vdash C_1 \langle\!\langle \text{box}[x] \rangle\!\rangle : C \Rightarrow B \rrbracket$
 3857 $h_2 = \llbracket \Gamma, x : A^p \vdash e_1 : C \rrbracket$
 3858 in $\langle id_\Gamma, f \rangle ; \langle h_1, h_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ ev}_{C, TB} ; \mu_B$
 3859
 3860 \preceq semantic weakening lemma 5.6 \rangle
 3861 let $h_1 = \llbracket \Gamma, x : A^p \vdash C_1 \langle\!\langle \text{box}[x] \rangle\!\rangle : C \Rightarrow B \rrbracket$
 3862 $h_2 = \llbracket \Gamma \vdash e_1 : C \rrbracket$
 3863 in $\langle id_\Gamma, f \rangle ; \langle h_1, \pi_1 ; h_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ ev}_{C, TB} ; \mu_B$
 3864
 3865 \preceq simplification \rangle
 3866 let $h_1 = \llbracket \Gamma, x : A^p \vdash C_1 \langle\!\langle \text{box}[x] \rangle\!\rangle : C \Rightarrow B \rrbracket$
 3867 $h_2 = \llbracket \Gamma \vdash e_1 : C \rrbracket$
 3868 in $\langle\langle id_\Gamma, f \rangle ; h_1, \langle id_\Gamma, f \rangle ; \pi_1 ; h_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ ev}_{C, TB} ; \mu_B$
 3869
 3870
 3871

3872 $\models \text{simplification } \rangle$

3873 let $h_1 = \llbracket \Gamma, x : A^p \vdash C_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C \Rightarrow B \rrbracket$
3874 $h_2 = \llbracket \Gamma \vdash e_1 : C \rrbracket$
3875 in $\langle \langle id_\Gamma, f \rangle ; h_1, h_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ ev}_{C, TB} ; \mu_B$

3877 $\models \text{observation } \rangle$

3879 let $h_1 = \llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } C_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C \Rightarrow B \rrbracket$
3880 $h_2 = \llbracket \Gamma \vdash e_1 : C \rrbracket$
3881 in $\langle h_1, h_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ ev}_{C, TB} ; \mu_B$

3883 $\models \text{induction hypothesis } \rangle$

3884 let $h_1 = \llbracket \Gamma \vdash C_1 \langle\!\langle e \rangle\!\rangle : C \Rightarrow B \rrbracket$
3885 $h_2 = \llbracket \Gamma \vdash e_1 : C \rrbracket$
3886 in $\langle h_1, h_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ ev}_{C, TB} ; \mu_B$

3888 $\models \text{definition } \rangle$

3889 $\llbracket \Gamma \vdash C_1 \langle\!\langle e \rangle\!\rangle e_1 : B \rrbracket$

3891

3892

3893 $\diamond C = \lambda z : C. C_1$

3894

3895 $\llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } \lambda z : C. C_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C \Rightarrow B \rrbracket$

3896

3897 $\models \text{observation } \rangle$

3898 $\langle id_\Gamma, f \rangle ; \llbracket \Gamma, x : A^p \vdash \lambda z : C. C_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C \Rightarrow B \rrbracket$

3899

3900 $\models \text{definition } \rangle$

3901 let $h = \llbracket \Gamma, x : A^p, z : C^i \vdash C_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : B \rrbracket$
3902 in $\langle id_\Gamma, f \rangle ; \text{curry}(h) ; \eta_{C \rightarrow TB}$

3904 $\models \text{semantic substitution theorem 5.11 and semantic weakening lemma 5.6 } \rangle$

3905 let $s = \llbracket \Gamma, x : A^p, z : C^i \vdash \theta : \Gamma, z : C^i, x : A^p \rrbracket$
3906 $h = s ; \llbracket \Gamma, z : C^i, x : A^p \vdash C_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : B \rrbracket$
3908 in $\langle id_\Gamma, f \rangle ; \text{curry}(h) ; \eta_{C \rightarrow TB}$

3909 $\models \text{simplification } \rangle$

3911 let $h = \llbracket \Gamma, z : C^i, x : A^p \vdash C_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : B \rrbracket$
3912 in $\langle id_\Gamma, f \rangle ; \text{curry}(\langle \pi_1 ; \pi_1, \pi_2, \pi_1 ; \pi_2 \rangle ; h) ; \eta_{C \rightarrow TB}$

3913

3914 $\models \text{universal property of exponential } \rangle$

3915 let $h = \llbracket \Gamma, z : C^i, x : A^p \vdash C_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : B \rrbracket$
3916 in $\text{curry}(\langle id_{\Gamma \times C}, \pi_1 ; f \rangle ; h) ; \eta_{C \rightarrow TB}$

3917

3918 $\models \text{observation } \rangle$

3919

3920

3921 let $h = \llbracket \Gamma, z : C^i \vdash \text{let box } [x] = e \text{ in } \mathcal{C}_1 \langle\langle \text{box } [x] \rangle\rangle : B \rrbracket$
 3922 in $\text{curry}(h) ; \eta_{C \rightarrow TB}$

3924 \asymp induction hypothesis \rangle

3925 let $h = \llbracket \Gamma, z : C^i \vdash \mathcal{C}_1 \langle\langle e \rangle\rangle : B \rrbracket$
 3926 in $\text{curry}(h) ; \eta_{C \rightarrow TB}$

3928 \asymp definition \rangle

3929 $\llbracket \Gamma \vdash \lambda z. \mathcal{C}_1 \langle\langle e \rangle\rangle : C \Rightarrow B \rrbracket$

3931 $\diamond \mathcal{C} = \text{fst } \mathcal{C}_1$

3934

3935 $\llbracket \Gamma \vdash \text{let box } [x] = e \text{ in } \text{fst } \mathcal{C}_1 \langle\langle \text{box } [x] \rangle\rangle : B \rrbracket$

3936 \asymp observation \rangle

3937 $\langle id_\Gamma, f \rangle ; \llbracket \Gamma, x : A^p \vdash \text{fst } \mathcal{C}_1 \langle\langle \text{box } [x] \rangle\rangle : B \rrbracket$

3938 \asymp definition \rangle

3939 $\langle id_\Gamma, f \rangle ; \llbracket \Gamma, x : A^p \vdash \mathcal{C}_1 \langle\langle \text{box } [x] \rangle\rangle : B \times C \rrbracket ; T\pi_1$

3940 \asymp observation \rangle

3941 $\llbracket \Gamma \vdash \text{let box } [x] = e \text{ in } \mathcal{C}_1 \langle\langle \text{box } [x] \rangle\rangle : B \times C \rrbracket ; T\pi_1$

3942 \asymp induction hypothesis \rangle

3943 $\llbracket \Gamma \vdash \mathcal{C}_1 \langle\langle e \rangle\rangle : B \times C \rrbracket ; T\pi_1$

3944 \asymp definition \rangle

3945 $\llbracket \Gamma \vdash \text{fst } \mathcal{C}_1 \langle\langle e \rangle\rangle : B \rrbracket$

3946

3953 $\diamond \mathcal{C} = \text{snd } \mathcal{C}_1$

3954

3955 $\llbracket \Gamma \vdash \text{let box } [x] = e \text{ in } \text{snd } \mathcal{C}_1 \langle\langle \text{box } [x] \rangle\rangle : B \rrbracket$

3956 \asymp observation \rangle

3957 $\langle id_\Gamma, f \rangle ; \llbracket \Gamma, x : A^p \vdash \text{snd } \mathcal{C}_1 \langle\langle \text{box } [x] \rangle\rangle : B \rrbracket$

3958 \asymp definition \rangle

3959 $\langle id_\Gamma, f \rangle ; \llbracket \Gamma, x : A^p \vdash \mathcal{C}_1 \langle\langle \text{box } [x] \rangle\rangle : C \times B \rrbracket ; T\pi_2$

3960 \asymp observation \rangle

3961 $\llbracket \Gamma \vdash \text{let box } [x] = e \text{ in } \mathcal{C}_1 \langle\langle \text{box } [x] \rangle\rangle : C \times B \rrbracket ; T\pi_2$

3962 \asymp induction hypothesis \rangle

3963 $\llbracket \Gamma \vdash \mathcal{C}_1 \langle\langle e \rangle\rangle : C \times B \rrbracket ; T\pi_2$

3964

3970 $\equiv \text{definition } \rangle$
 3971 $\boxed{\llbracket \Gamma \vdash \text{snd } \mathcal{C}_1 \langle\langle e \rangle\rangle : B \rrbracket}$
 3972

3973

3974 $\diamond \mathcal{C} = (e_1, \mathcal{C}_1)$
 3975

3976

3977 $\boxed{\llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } (e_1, \mathcal{C}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle) : B \times C \rrbracket}$
 3978

3979 $\equiv \text{observation } \rangle$
 3980 $\boxed{\langle id_\Gamma, f \rangle ; \llbracket \Gamma, x : A^p \vdash (e_1, \mathcal{C}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle) : B \times C \rrbracket}$
 3981

3982 $\equiv \text{definition } \rangle$
 3983 $\boxed{\langle id_\Gamma, f \rangle ; \langle \llbracket \Gamma, x : A^p \vdash e_1 : B \rrbracket, \llbracket \Gamma, x : A^p \vdash \mathcal{C}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : C \rrbracket \rangle ; \beta_{B,C}}$
 3984

3985 $\equiv \text{semantic weakening lemma 5.6 } \rangle$
 3986 $\boxed{\langle id_\Gamma, f \rangle ; \langle \pi_1 ; \llbracket \Gamma \vdash e_1 : B \rrbracket, \langle id_\Gamma, f \rangle ; \llbracket \Gamma, x : A^p \vdash \mathcal{C}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : C \rrbracket \rangle ; \beta_{B,C}}$
 3987

3988 $\equiv \text{universal property of products } \rangle$
 3989 $\boxed{\langle \langle id_\Gamma, f \rangle ; \pi_1 ; \llbracket \Gamma \vdash e_1 : B \rrbracket, \langle id_\Gamma, f \rangle ; \llbracket \Gamma, x : A^p \vdash \mathcal{C}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : C \rrbracket \rangle ; \beta_{B,C}}$
 3990

3991 $\equiv \text{definition of } \pi_1 \rangle$
 3992 $\boxed{\langle \llbracket \Gamma \vdash e_1 : B \rrbracket, \langle id_\Gamma, f \rangle ; \llbracket \Gamma, x : A^p \vdash \mathcal{C}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : C \rrbracket \rangle ; \beta_{B,C}}$
 3993

3994 $\equiv \text{observation } \rangle$
 3995 $\boxed{\langle \llbracket \Gamma \vdash e_1 : B \rrbracket, \llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } \mathcal{C}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : C \rrbracket \rangle ; \beta_{B,C}}$
 3996

3997 $\equiv \text{induction hypothesis } \rangle$
 3998 $\boxed{\langle \llbracket \Gamma \vdash e_1 : B \rrbracket, \llbracket \Gamma \vdash \mathcal{C}_1 \langle\langle e \rangle\rangle : C \rrbracket \rangle ; \beta_{B,C}}$
 3999

4000 $\equiv \text{definition } \rangle$
 4001 $\boxed{\llbracket \Gamma \vdash (e_1, \mathcal{C}_1 \langle\langle e \rangle\rangle) : B \times C \rrbracket}$
 4002

4003 $\diamond \mathcal{C} = (\mathcal{C}_1, e_1)$
 4004

4005

4006 $\boxed{\llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } (\mathcal{C}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle, e_1) : C \times B \rrbracket}$
 4007

4008 $\equiv \text{observation } \rangle$
 4009 $\boxed{\langle id_\Gamma, f \rangle ; \llbracket \Gamma, x : A^p \vdash (\mathcal{C}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle, e_1) : C \times B \rrbracket}$
 4010

4011 $\equiv \text{definition } \rangle$
 4012 $\boxed{\langle id_\Gamma, f \rangle ; \langle \llbracket \Gamma, x : A^p \vdash \mathcal{C}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : C \rrbracket, \llbracket \Gamma, x : A^p \vdash e_1 : B \rrbracket \rangle ; \beta_{C,B}}$
 4013

4014 $\equiv \text{semantic weakening lemma 5.6 } \rangle$
 4015 $\boxed{\langle id_\Gamma, f \rangle ; \langle \llbracket \Gamma, x : A^p \vdash \mathcal{C}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : C \rrbracket, \pi_1 ; \llbracket \Gamma \vdash e_1 : B \rrbracket \rangle ; \beta_{C,B}}$
 4016

4017 $\equiv \text{universal property of products } \rangle$

```

4019   ⟨⟨ $\text{id}_\Gamma, f\rangle; [\Gamma, \mathbf{x} : A^p \vdash \mathcal{C}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C], \langle id_\Gamma, f \rangle; \pi_1 : [\Gamma \vdash e_1 : B] \rangle; \beta_{C,B}
4020
4021   \models \text{definition of } \pi_1 \rangle
4022   \langle \langle id_\Gamma, f \rangle; [\Gamma, \mathbf{x} : A^p \vdash \mathcal{C}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C], [\Gamma \vdash e_1 : B] \rangle; \beta_{C,B}
4023
4024   \models \text{observation } \rangle
4025   \langle [\Gamma \vdash \text{let box } \boxed{x} = e \text{ in } \mathcal{C}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C], [\Gamma \vdash e_1 : B] \rangle; \beta_{C,B}
4026
4027   \models \text{induction hypothesis } \rangle
4028   \langle [\Gamma \vdash \mathcal{C}_1 \langle\!\langle e \rangle\!\rangle : C], [\Gamma \vdash e_1 : B] \rangle; \beta_{C,B}
4029
4030   \models \text{definition } \rangle
4031   \langle [\Gamma \vdash (\mathcal{C}_1 \langle\!\langle e \rangle\!\rangle, e_1) : C \times B] \rangle
4032
4033   \diamond \mathcal{C} = \text{box } \boxed{\mathcal{C}_1}
4034
4035
4036
4037   \langle [\Gamma \vdash \text{let box } \boxed{x} = e \text{ in box } \mathcal{C}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : \Box B] \rangle
4038
4039   \models \text{observation } \rangle
4040   \langle id_\Gamma, f \rangle; [\Gamma, \mathbf{x} : A^p \vdash \text{box } \mathcal{C}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : \Box B]
4041
4042   \models \text{definition } \rangle
4043   \langle id_\Gamma, f \rangle; [\Gamma, \mathbf{x} : A^p \vdash^p \mathcal{C}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : B]_p; \eta_{\Box Y}
4044
4045   \models \text{observation } \rangle
4046   \langle [\Gamma \vdash^p \text{let box } \boxed{x} = e \text{ in } \mathcal{C}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : B]_p; \eta_{\Box Y} \rangle
4047
4048   \models \text{induction hypothesis } \rangle
4049   \langle [\Gamma \vdash^p \mathcal{C}_1 \langle\!\langle e \rangle\!\rangle : B]_p; \eta_{\Box Y} \rangle
4050
4051   \models \text{definition } \rangle
4052   \langle [\Gamma \vdash \text{box } \boxed{\mathcal{C}_1 \langle\!\langle e \rangle\!\rangle} : \Box B] \rangle
4053
4054
4055   \diamond \mathcal{C} = \text{let box } \boxed{z} = \boxed{\mathcal{C}_1} \text{ in } e_1
4056
4057
4058   \langle [\Gamma \vdash \text{let box } \boxed{x} = e \text{ in } (\text{let box } \boxed{z} = \mathcal{C}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle \text{ in } e_1) : B] \rangle
4059
4060   \models \text{observation } \rangle
4061   \langle id_\Gamma, f \rangle; [\Gamma, \mathbf{x} : A^p \vdash \text{let box } \boxed{z} = \mathcal{C}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle \text{ in } e_1 : B]
4062
4063   \models \text{definition } \rangle
4064
4065
4066
4067$ 
```

```

4068   let g =  $\llbracket \Gamma, x : A^p \vdash C_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : \Box C \rrbracket$ 
4069   h =  $\llbracket \Gamma, x : A^p, z : C^p \vdash e_1 : B \rrbracket$ 
4070   in  $\langle id_\Gamma, f \rangle ; \langle id_{\Gamma \times \Box A}, g \rangle ; \tau_{\Gamma \times \Box A, \Box C} ; Th ; \mu_B$ 
4071
4072  $\models$  semantic substitution theorem 5.11 and semantic weakening lemma 5.6  $\rightarrow$ 
4073
4074   let g =  $\llbracket \Gamma, x : A^p \vdash C_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : \Box C \rrbracket$ 
4075   h =  $\langle \pi_1 ; \pi_1, \pi_2 \rangle ; \llbracket \Gamma, z : C^p \vdash e_1 : B \rrbracket$ 
4076   in  $\langle id_\Gamma, f \rangle ; \langle id_{\Gamma \times \Box A}, g \rangle ; \tau_{\Gamma \times \Box A, \Box C} ; Th ; \mu_B$ 
4077
4078  $\models$  simplification  $\rightarrow$ 
4079   let g =  $\llbracket \Gamma, x : A^p \vdash C_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : \Box C \rrbracket$ 
4080   h =  $\llbracket \Gamma, z : C^p \vdash e_1 : B \rrbracket$ 
4081   in  $\langle \langle id_\Gamma, f \rangle, \langle id_\Gamma, f \rangle ; g \rangle ; \tau_{\Gamma \times \Box A, \Box C} ; T \langle \pi_1 ; \pi_1, \pi_2 \rangle ; Th ; \mu_B$ 
4082
4083  $\models$  simplification  $\rightarrow$ 
4084   let g =  $\llbracket \Gamma, x : A^p \vdash C_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : \Box C \rrbracket$ 
4085   h =  $\llbracket \Gamma, z : C^p \vdash e_1 : B \rrbracket$ 
4086   in  $\langle id_\Gamma, \langle id_\Gamma, f \rangle ; g \rangle ; \tau_{\Gamma, \Box C} ; Th ; \mu_B$ 
4087
4088  $\models$  observation  $\rightarrow$ 
4089
4090   let g =  $\llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } C_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : \Box C \rrbracket$ 
4091   h =  $\llbracket \Gamma, z : C^p \vdash e_1 : B \rrbracket$ 
4092   in  $\langle id_\Gamma, g \rangle ; \tau_{\Gamma, \Box C} ; Th ; \mu_B$ 
4093
4094  $\models$  induction hypothesis  $\rightarrow$ 
4095
4096   let g =  $\llbracket \Gamma \vdash C_1 \langle\langle e \rangle\rangle : \Box C \rrbracket$ 
4097   h =  $\llbracket \Gamma, z : C^p \vdash e_1 : B \rrbracket$ 
4098   in  $\langle id_\Gamma, g \rangle ; \tau_{\Gamma, \Box C} ; Th ; \mu_B$ 
4099
4100  $\models$  definition  $\rightarrow$ 
4101    $\llbracket \Gamma \vdash \text{let box } \boxed{z} = C_1 \langle\langle e \rangle\rangle \text{ in } e_1 : B \rrbracket$ 
4102
4103  $\diamond C = \text{let box } \boxed{z} = e_1 \text{ in } C_1$ 
4104
4105
4106
4107    $\llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } (\text{let box } \boxed{z} = e_1 \text{ in } C_1 \langle\langle \text{box } \boxed{x} \rangle\rangle) : B \rrbracket$ 
4108  $\models$  observation  $\rightarrow$ 
4109    $\langle id_\Gamma, f \rangle ; \llbracket \Gamma, x : A^p \vdash \text{let box } \boxed{z} = e_1 \text{ in } C_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket$ 
4110
4111  $\models$  definition  $\rightarrow$ 
4112   let h1 =  $\llbracket \Gamma, x : A^p \vdash e_1 : \Box C \rrbracket$ 
4113   h2 =  $\llbracket \Gamma, x : A^p, z : C^p \vdash C_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket$ 
4114   in  $\langle id_\Gamma, f \rangle ; \langle id_{\Gamma \times \Box A}, h_1 \rangle ; \tau_{\Gamma \times \Box A, \Box C} ; Th_2 ; \mu_B$ 
4115

```

- 4117 \Leftarrow semantic weakening lemma 5.6)
- 4118 let $h_1 = \llbracket \Gamma \vdash e_1 : \Box C \rrbracket$
4119 $h_2 = \llbracket \Gamma, x : A^p, z : C^p \vdash C_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket$
4120 in $\langle id_\Gamma, f \rangle ; \langle id_{\Gamma \times \Box A}, \pi_1 ; h_1 \rangle ; \tau_{\Gamma \times \Box A, \Box C} ; Th_2 ; \mu_B$
- 4122 \Leftarrow simplification)
- 4124 let $h_1 = \llbracket \Gamma \vdash e_1 : \Box C \rrbracket$
4125 $h_2 = \llbracket \Gamma, x : A^p, z : C^p \vdash C_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket$
4126 in $\langle \langle id_\Gamma, f \rangle, h_1 \rangle ; \tau_{\Gamma \times \Box A, \Box C} ; Th_2 ; \mu_B$
- 4128 \Leftarrow semantic substitution theorem 5.11 and semantic weakening lemma 5.6)
- 4129 let $h_1 = \llbracket \Gamma \vdash e_1 : \Box C \rrbracket$
4130 $h_2 = \llbracket \Gamma, z : C^p, x : A^p \vdash C_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket$
4131 in $\langle \langle id_\Gamma, f \rangle, h_1 \rangle ; \tau_{\Gamma \times \Box A, \Box C} ; T \langle \pi_1, \pi_1, \pi_2, \pi_1 ; \pi_2 \rangle ; Th_2 ; \mu_B$
- 4133 \Leftarrow simplification)
- 4134 let $h_1 = \llbracket \Gamma \vdash e_1 : \Box C \rrbracket$
4135 $h_2 = \llbracket \Gamma, z : C^p, x : A^p \vdash C_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket$
4136 in $\langle id_\Gamma, h_1 \rangle ; \tau_{\Gamma, \Box C} ; T \langle id_{\Gamma \times \Box C}, \pi_1 ; f \rangle ; Th_2 ; \mu_B$
- 4138 \Leftarrow observation)
- 4139 let $h_1 = \llbracket \Gamma \vdash e_1 : \Box C \rrbracket$
4140 $h_2 = \llbracket \Gamma, z : C^p \vdash \text{let box } \boxed{x} = e \text{ in } C_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket$
4141 in $\langle id_\Gamma, h_1 \rangle ; \tau_{\Gamma, \Box C} ; Th_2 ; \mu_B$
- 4144 \Leftarrow induction hypothesis)
- 4145 let $h_1 = \llbracket \Gamma \vdash e_1 : \Box C \rrbracket$
4146 $h_2 = \llbracket \Gamma, z : C^p \vdash C_1 \langle\langle e \rangle\rangle : B \rrbracket$
4147 in $\langle id_\Gamma, h_1 \rangle ; \tau_{\Gamma, \Box C} ; Th_2 ; \mu_B$
- 4149 \Leftarrow definition)
- 4150 $\llbracket \Gamma \vdash \text{let box } \boxed{z} = e_1 \text{ in } C_1 \langle\langle e \rangle\rangle : B \rrbracket$
- 4152
- 4153 $\diamond \frac{\Gamma \vdash e : \Box A \quad \Gamma \vdash \mathcal{E} \langle\langle e \rangle\rangle : B \quad \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } \mathcal{E} \langle\langle \text{box } \boxed{x} \rangle\rangle : B}{\Gamma \vdash \mathcal{E} \langle\langle e \rangle\rangle \approx \text{let box } \boxed{x} = e \text{ in } \mathcal{E} \langle\langle \text{box } \boxed{x} \rangle\rangle : B}$ $\Box \eta\text{-IMPURE}$
- 4155 We proceed by cases on \mathcal{E} .
- 4156 $\diamond \mathcal{E} = [\cdot]$
- 4159 $\llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in box } \boxed{x} : \Box A \rrbracket$
- 4161 \Leftarrow definition)
- 4162 $\langle id_\Gamma, \llbracket \Gamma \vdash e : \Box A \rrbracket \rangle ; \tau_{\Gamma, \Box A} ; T \llbracket \Gamma, x : A^p \vdash \text{box } \boxed{x} : \Box A \rrbracket ; \mu_{\Box A}$

```

4166 ≌ definition   )
4167   ⟨idΓ, [Γ ⊢ e : □A] ; τΓ,□A; T[Γ, x : Ap ⊢p x : A] ; Tη□A; μ□A
4168
4169 ≌ definition   )
4170   ⟨idΓ, [Γ ⊢ e : □A] ; τΓ,□A; Tπ2; Tη□A; μ□A
4171
4172 ≌ monad laws   )
4173   ⟨idΓ, [Γ ⊢ e : □A] ; τΓ,□A; Tπ2; idT□A
4174
4175 ≌ tensorial action of T   )
4176   ⟨idΓ, [Γ ⊢ e : □A] ; π2
4177
4178 ≌ applying π2   )
4179   [Γ ⊢ e : □A]
4180
4181
4182 ◊ E = e1 E1
4183
4184
4185   [Γ ⊢ let box[x] = e in e1 E1⟨⟨box[x]⟩⟩ : B]
4186
4187 ≌ definition   )
4188   let f = [Γ ⊢ e : □A]
4189   g = [Γ, x : Ap ⊢ e1 E1⟨⟨box[x]⟩⟩ : B]
4190   in ⟨idΓ, f⟩ ; τΓ,□A; Tg ; μB
4191
4192 ≌ definition   )
4193   f = [Γ ⊢ e : □A]
4194   let g1 = [Γ, x : Ap ⊢ e1 : C ⇒ B]
4195   g2 = [Γ, x : Ap ⊢ E1⟨⟨box[x]⟩⟩ : C]
4196   g = ⟨g1, g2⟩ ; βC→TB,C; T evC,TY; μB
4197   in ⟨idΓ, f⟩ ; τΓ,□A; Tg ; μB
4198
4199 ≌ functoriality of T   )
4200   f = [Γ ⊢ e : □A]
4201   let g1 = [Γ, x : Ap ⊢ e1 : C ⇒ B]
4202   g2 = [Γ, x : Ap ⊢ E1⟨⟨box[x]⟩⟩ : C]
4203   in ⟨idΓ, f⟩ ; τΓ,□A; T⟨g1, g2⟩ ; TβC→TB,C; T2 evC,TY; TμB; μB
4204
4205
4206 ≌ semantic weakening lemma 5.6   )
4207   f = [Γ ⊢ e : □A]
4208   let g1 = π1 ; [Γ ⊢ e1 : C ⇒ B]
4209   g2 = [Γ, x : Ap ⊢ E1⟨⟨box[x]⟩⟩ : C]
4210   in ⟨idΓ, f⟩ ; τΓ,□A; T⟨g1, g2⟩ ; TβC→TB,C; T2 evC,TY; TμB; μB
4211
4212 ≌ simplification   )
4213
4214

```

4215 $f = \llbracket \Gamma \vdash e : \Box A \rrbracket$
 4216 $\text{let } g_1 = \llbracket \Gamma \vdash e_1 : C \Rightarrow B \rrbracket$
 4217 $g_2 = \llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\langle \text{box}[x] \rangle\rangle : C \rrbracket$
 4218 $\text{in } \langle id_\Gamma, f \rangle ; \tau_{\Gamma, \Box A} ; T \langle \pi_1 ; g_1 , g_2 \rangle ; T \beta_{C \rightarrow TB, C} ; T^2 \text{ ev}_{C, TY} ; T \mu_B ; \mu_B$

4220 \equiv simplification \rangle

4222 $f = \llbracket \Gamma \vdash e : \Box A \rrbracket$
 4223 $\text{let } g_1 = \llbracket \Gamma \vdash e_1 : C \Rightarrow B \rrbracket$
 4224 $g_2 = \llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\langle \text{box}[x] \rangle\rangle : C \rrbracket$
 4225 $\text{in } \langle g_1, \langle id_\Gamma, f \rangle ; \tau_{\Gamma, \Box A} ; T g_2 ; \mu_Z \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ ev}_{C, TY} ; \mu_B$

4227 \equiv definition \rangle

4228 $\text{let } g_1 = \llbracket \Gamma \vdash e_1 : C \Rightarrow B \rrbracket$
 4229 $g_2 = \llbracket \Gamma \vdash \text{let box}[x] = e \text{ in } \mathcal{E}_1 \langle\langle \text{box}[x] \rangle\rangle : C \rrbracket$
 4230 $\text{in } \langle g_1, g_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ ev}_{C, TY} ; \mu_B$

4232 \equiv induction hypothesis \rangle

4234 $\text{let } g_1 = \llbracket \Gamma \vdash e_1 : C \Rightarrow B \rrbracket$
 4235 $g_2 = \llbracket \Gamma \vdash \mathcal{E}_1 \langle\langle e \rangle\rangle : C \rrbracket$
 4236 $\text{in } \langle g_1, g_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ ev}_{C, TY} ; \mu_B$

4238 \equiv definition \rangle

4239 $\llbracket \Gamma \vdash e_1 \mathcal{E}_1 \langle\langle e \rangle\rangle : B \rrbracket$

4242 $\diamond \mathcal{E} = \mathcal{E}_1 v$

4245 $\llbracket \Gamma \vdash \text{let box}[x] = e \text{ in } \mathcal{E}_1 \langle\langle \text{box}[x] \rangle\rangle v : B \rrbracket$

4247 \equiv definition \rangle

4248 $\text{let } f = \llbracket \Gamma \vdash e : \Box A \rrbracket$
 4249 $g = \llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\langle \text{box}[x] \rangle\rangle v : B \rrbracket$
 4250 $\text{in } \langle id_\Gamma, f \rangle ; \tau_{\Gamma, \Box A} ; T g ; \mu_B$

4252 \equiv definition \rangle

4253 $f = \llbracket \Gamma \vdash e : \Box A \rrbracket$
 4254 $\text{let } g_1 = \llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\langle \text{box}[x] \rangle\rangle : C \Rightarrow B \rrbracket$
 4255 $g_2 = \llbracket \Gamma, x : A^p \vdash v : C \rrbracket$
 4256 $g = \langle g_1, g_2 \rangle ; \beta_{(C \rightarrow TB), C} ; T \text{ ev}_{C, TY} ; \mu_B$
 4257 $\text{in } \langle id_\Gamma, f \rangle ; \tau_{\Gamma, \Box A} ; T g ; \mu_B$

4260 \equiv functoriality of T \rangle

4264 $f = \llbracket \Gamma \vdash e : \square A \rrbracket$
 4265 let $g_1 = \llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C \Rightarrow B \rrbracket$
 4266 $g_2 = \llbracket \Gamma, x : A^p \vdash v : C \rrbracket$
 4268 in $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; T\langle g_1, g_2 \rangle ; T\beta_{C \rightarrow TB, C} ; T^2 \text{ev}_{C, TY} ; T\mu_B ; \mu_B$

4269 \equiv semantic weakening lemma 5.6 \rangle

4271 $f = \llbracket \Gamma \vdash e : \square A \rrbracket$
 4272 let $g_1 = \llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C \Rightarrow B \rrbracket$
 4273 $g_2 = \pi_1 ; \llbracket \Gamma \vdash v : C \rrbracket$
 4274 in $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; T\langle g_1, g_2 \rangle ; T\beta_{C \rightarrow TB, C} ; T^2 \text{ev}_{C, TY} ; T\mu_B ; \mu_B$

4276 \equiv simplification \rangle

4277 $f = \llbracket \Gamma \vdash e : \square A \rrbracket$
 4278 let $g_1 = \llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C \Rightarrow B \rrbracket$
 4279 $g_2 = \llbracket \Gamma \vdash v : C \rrbracket$
 4281 in $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; T\langle g_1, \pi_1 ; g_2 \rangle ; T\beta_{C \rightarrow TB, C} ; T^2 \text{ev}_{C, TY} ; T\mu_B ; \mu_B$

4283 \equiv simplification \rangle

4284 $f = \llbracket \Gamma \vdash e : \square A \rrbracket$
 4285 let $g_1 = \llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C \Rightarrow B \rrbracket$
 4286 $g_2 = \llbracket \Gamma \vdash v : C \rrbracket$
 4288 in $\langle \langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg_1 ; \mu_{C \rightarrow TB} , g_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ev}_{C, TY} ; \mu_B$

4289 \equiv definition \rangle

4290 let $g_1 = \llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C \Rightarrow B \rrbracket$
 4292 $g_2 = \llbracket \Gamma \vdash v : C \rrbracket$
 4293 in $\langle g_1, g_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ev}_{C, TY} ; \mu_B$

4295 \equiv induction hypothesis \rangle

4296 let $g_1 = \llbracket \Gamma \vdash \mathcal{E}_1 \langle\!\langle e \rangle\!\rangle : C \Rightarrow B \rrbracket$
 4297 $g_2 = \llbracket \Gamma \vdash v : C \rrbracket$
 4299 in $\langle g_1, g_2 \rangle ; \beta_{C \rightarrow TB, C} ; T \text{ev}_{C, TY} ; \mu_B$

4300 \equiv definition \rangle

4301 $\llbracket \Gamma \vdash \mathcal{E}_1 \langle\!\langle e \rangle\!\rangle v : B \rrbracket$

4303

4304 $\diamond \mathcal{E} = \text{fst } \mathcal{E}_1$

4305

4307 $\llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in fst } \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : B \rrbracket$

4309 \equiv definition \rangle

4310

4311

4312

4313 let $f = \llbracket \Gamma \vdash e : \square A \rrbracket$
 4314 g = $\llbracket \Gamma, x : A^p \vdash \text{fst } \mathcal{E}_1 \langle\!\langle \text{box } [x] \rangle\!\rangle : B \rrbracket$
 4315 in $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg ; \mu_B$

4317 \equiv definition \rangle

4318 let $f = \llbracket \Gamma \vdash e : \square A \rrbracket$
 4319 g = $\llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } [x] \rangle\!\rangle : B \times C \rrbracket$
 4320 in $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg ; T^2\pi_1 ; \mu_B$

4322 \equiv monad laws \rangle

4324 let $f = \llbracket \Gamma \vdash e : \square A \rrbracket$
 4325 g = $\llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } [x] \rangle\!\rangle : B \times C \rrbracket$
 4326 in $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg ; \mu_B ; T\pi_1$

4328 \equiv definition \rangle

4329 $\llbracket \Gamma \vdash \text{let box } [x] = e \text{ in } \mathcal{E}_1 \langle\!\langle \text{box } [x] \rangle\!\rangle : B \times C \rrbracket ; T\pi_1$

4331 \equiv induction hypothesis \rangle

4332 $\llbracket \Gamma \vdash \mathcal{E}_1 \langle\!\langle e \rangle\!\rangle : B \times C \rrbracket ; T\pi_1$

4334 \equiv definition \rangle

4335 $\llbracket \Gamma \vdash \text{fst } \mathcal{E}_1 \langle\!\langle e \rangle\!\rangle : B \rrbracket$

4338 $\diamond \mathcal{E} = \text{snd } \mathcal{E}_1$

4339

4340

4341 $\llbracket \Gamma \vdash \text{let box } [x] = e \text{ in } \text{snd } \mathcal{E}_1 \langle\!\langle \text{box } [x] \rangle\!\rangle : B \rrbracket$

4342 \equiv definition \rangle

4344 let $f = \llbracket \Gamma \vdash e : \square A \rrbracket$
 4345 g = $\llbracket \Gamma, x : A^p \vdash \text{snd } \mathcal{E}_1 \langle\!\langle \text{box } [x] \rangle\!\rangle : B \rrbracket$
 4346 in $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg ; \mu_B$

4348 \equiv definition \rangle

4349 let $f = \llbracket \Gamma \vdash e : \square A \rrbracket$
 4350 g = $\llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } [x] \rangle\!\rangle : C \times B \rrbracket$
 4351 in $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg ; T^2\pi_2 ; \mu_B$

4353 \equiv monad laws \rangle

4354 let $f = \llbracket \Gamma \vdash e : \square A \rrbracket$
 4355 g = $\llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } [x] \rangle\!\rangle : C \times B \rrbracket$
 4356 in $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg ; \mu_B ; T\pi_2$

4358 \equiv definition \rangle

4359

4360

4361

4362	$\llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C \times B \rrbracket ; T\pi_2$
4363	$\asymp \text{induction hypothesis } \rightarrow$
4364	$\llbracket \Gamma \vdash \mathcal{E}_1 \langle\!\langle e \rangle\!\rangle : C \times B \rrbracket ; T\pi_2$
4365	$\asymp \text{definition } \rightarrow$
4366	$\llbracket \Gamma \vdash \text{snd } \mathcal{E}_1 \langle\!\langle e \rangle\!\rangle : B \rrbracket$
4367	
4368	
4369	
4370	
4371	$\diamond \mathcal{E} = (e_1, \mathcal{E}_1)$
4372	
4373	$\llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } (e_1, \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle) : B \times C \rrbracket$
4374	
4375	$\asymp \text{definition } \rightarrow$
4376	
4377	$\text{let } f = \llbracket \Gamma \vdash e : \square A \rrbracket$
4378	$\text{let } g = \llbracket \Gamma, x : A^p \vdash (e_1, \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle) : B \times C \rrbracket$
4379	$\text{in } \langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg ; \mu_{B \times C}$
4380	
4381	$\asymp \text{definition } \rightarrow$
4382	
4383	$f = \llbracket \Gamma \vdash e : \square A \rrbracket$
4384	$\text{let } g_1 = \llbracket \Gamma, x : A^p \vdash e_1 : B \rrbracket$
4385	$\text{let } g_2 = \llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C \rrbracket$
4386	$g = \langle g_1, g_2 \rangle ; \beta_{B,C}$
4387	$\text{in } \langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg ; \mu_{B \times C}$
4388	
4389	$\asymp \text{semantic weakening lemma 5.6 } \rightarrow$
4390	
4391	$f = \llbracket \Gamma \vdash e : \square A \rrbracket$
4392	$\text{let } g_1 = \pi_1 ; \llbracket \Gamma \vdash e_1 : B \rrbracket$
4393	$\text{let } g_2 = \llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C \rrbracket$
4394	$g = \langle g_1, g_2 \rangle ; \beta_{B,C}$
4395	$\text{in } \langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg ; \mu_{B \times C}$
4396	
4397	$\asymp \text{simplification } \rightarrow$
4398	
4399	$f = \llbracket \Gamma \vdash e : \square A \rrbracket$
4400	$\text{let } g_1 = \llbracket \Gamma \vdash e_1 : B \rrbracket$
4401	$\text{let } g_2 = \llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C \rrbracket$
4402	$\text{in } \langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; T(\pi_1 ; g_1, g_2) ; T\beta_{B,C} ; \mu_{B \times C}$
4403	
4404	$\asymp \text{simplification } \rightarrow$
4405	
4406	$f = \llbracket \Gamma \vdash e : \square A \rrbracket$
4407	$\text{let } g_1 = \llbracket \Gamma \vdash e_1 : B \rrbracket$
4408	$\text{let } g_2 = \llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : C \rrbracket$
4409	$\text{in } \langle g_1, \langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg_2 ; \mu_C \rangle ; \beta_{B,C}$
4410	

```

4411  ≒ definition   )
4412    let g1 =  $\llbracket \Gamma \vdash e_1 : B \rrbracket$ 
4413      g2 =  $\llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } \mathcal{E}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : C \rrbracket$ 
4414      in  $\langle g_1, g_2 \rangle ; \beta_{B,C}$ 
4415
4416  ≒ induction hypothesis   )
4417    let g1 =  $\llbracket \Gamma \vdash e_1 : B \rrbracket$ 
4418      g2 =  $\llbracket \Gamma \vdash \mathcal{E}_1 \langle\langle e \rangle\rangle : C \rrbracket$ 
4419      in  $\langle g_1, g_2 \rangle ; \beta_{B,C}$ 
4420
4421  ≒ definition   )
4422     $\llbracket \Gamma \vdash (e_1, \mathcal{E}_1 \langle\langle e \rangle\rangle) : B \times C \rrbracket$ 
4423
4424
4425
4426  ◊  $\mathcal{E} = (\mathcal{E}_1, v)$ 
4427
4428
4429     $\llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } (\mathcal{E}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle, v) : C \times B \rrbracket$ 
4430
4431  ≒ definition   )
4432    let f =  $\llbracket \Gamma \vdash e : \Box A \rrbracket$ 
4433      g =  $\llbracket \Gamma, \boxed{x} : A^p \vdash (\mathcal{E}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle, v) : C \times B \rrbracket$ 
4434      in  $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \Box A} ; Tg ; \mu_{C \times B}$ 
4435
4436  ≒ definition   )
4437    f =  $\llbracket \Gamma \vdash e : \Box A \rrbracket$ 
4438    let g1 =  $\llbracket \Gamma, \boxed{x} : A^p \vdash \mathcal{E}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : C \rrbracket$ 
4439      g2 =  $\llbracket \Gamma, \boxed{x} : A^p \vdash v : B \rrbracket$ 
4440      g =  $\langle g_1, g_2 \rangle ; \beta_{C,B}$ 
4441      in  $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \Box A} ; Tg ; \mu_{C \times B}$ 
4442
4443
4444  ≒ semantic weakening lemma 5.6   )
4445    f =  $\llbracket \Gamma \vdash e : \Box A \rrbracket$ 
4446    let g1 =  $\llbracket \Gamma \vdash \mathcal{E}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : C \rrbracket$ 
4447      g2 =  $\pi_1 ; \llbracket \Gamma, \boxed{x} : A^p \vdash v : B \rrbracket$ 
4448      g =  $\langle g_1, g_2 \rangle ; \beta_{C,B}$ 
4449      in  $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \Box A} ; Tg ; \mu_{C \times B}$ 
4450
4451
4452  ≒ simplification   )
4453    f =  $\llbracket \Gamma \vdash e : \Box A \rrbracket$ 
4454    let g1 =  $\llbracket \Gamma, \boxed{x} : A^p \vdash \mathcal{E}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : C \rrbracket$ 
4455      g2 =  $\llbracket \Gamma \vdash v : B \rrbracket$ 
4456      in  $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \Box A} ; T\langle g_1, \pi_1 ; g_2 \rangle ; T\beta_{C,B} ; \mu_{C \times B}$ 
4457
4458
4459

```

```

4460    ≒ simplification   )
4461      f   =   $\llbracket \Gamma \vdash e : \square A \rrbracket$ 
4462      let g1 =   $\llbracket \Gamma, x : Ap \vdash \mathcal{E}_1 \langle\!\langle \text{box } x \rangle\!\rangle : C \rrbracket$ 
4463          g2 =   $\llbracket \Gamma \vdash v : B \rrbracket$ 
4464      in   $\langle \langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg_1 ; \mu_C, g_2 \rangle ; \beta_{C,B}$ 
4465
4466    ≒ definition   )
4467      let g1 =   $\llbracket \Gamma \vdash \text{let box } x = e \text{ in } \mathcal{E}_1 \langle\!\langle \text{box } x \rangle\!\rangle : C \rrbracket$ 
4468          g2 =   $\llbracket \Gamma \vdash v : B \rrbracket$ 
4469          in   $\langle g_1, g_2 \rangle ; \beta_{C,B}$ 
4470
4471    ≒ induction hypothesis   )
4472      let g1 =   $\llbracket \Gamma \vdash \mathcal{E}_1 \langle\!\langle e \rangle\!\rangle : C \rrbracket$ 
4473          g2 =   $\llbracket \Gamma \vdash v : B \rrbracket$ 
4474          in   $\langle g_1, g_2 \rangle ; \beta_{C,B}$ 
4475
4476    ≒ definition   )
4477       $\llbracket \Gamma \vdash (\mathcal{E}_1 \langle\!\langle e \rangle\!\rangle, v) : C \times B \rrbracket$ 
4478
4479
4480
4481
4482    ◊  $\mathcal{E} = \text{let box } z = \mathcal{E}_1 \text{ in } e_1$ 
4483
4484
4485       $\llbracket \Gamma \vdash \text{let box } x = e \text{ in } (\text{let box } z = \mathcal{E}_1 \langle\!\langle \text{box } x \rangle\!\rangle \text{ in } e_1) : B \rrbracket$ 
4486
4487    ≒ definition   )
4488      let f =   $\llbracket \Gamma \vdash e : \square A \rrbracket$ 
4489          g =   $\llbracket \Gamma, x : Ap \vdash \text{let box } z = \mathcal{E}_1 \langle\!\langle \text{box } x \rangle\!\rangle \text{ in } e_1 : B \rrbracket$ 
4490          in   $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg ; \mu_B$ 
4491
4492    ≒ definition   )
4493      f   =   $\llbracket \Gamma \vdash e : \square A \rrbracket$ 
4494      let g1 =   $\llbracket \Gamma, x : Ap \vdash \mathcal{E}_1 \langle\!\langle \text{box } x \rangle\!\rangle : \square C \rrbracket$ 
4495          g2 =   $\llbracket \Gamma, x : Ap, z : Cp \vdash e_1 : B \rrbracket$ 
4496          g   =   $\langle id_{\Gamma \times \square A}, g_1 \rangle ; \tau_{\Gamma \times \square A, \square C} ; Tg_2 ; \mu_B$ 
4497          in   $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; Tg ; \mu_B$ 
4498
4499    ≒ functoriality of  $T$    )
4500      f   =   $\llbracket \Gamma \vdash e : \square A \rrbracket$ 
4501      let g1 =   $\llbracket \Gamma, x : Ap \vdash \mathcal{E}_1 \langle\!\langle \text{box } x \rangle\!\rangle : \square C \rrbracket$ 
4502          g2 =   $\llbracket \Gamma, x : Ap, z : Cp \vdash e_1 : B \rrbracket$ 
4503          in   $\langle id_\Gamma, f \rangle ; \tau_{\Gamma, \square A} ; T \langle id_{\Gamma \times \square A}, g_1 \rangle ; T \tau_{\Gamma \times \square A, \square C} ; T^2 g_2 ; T \mu_B ; \mu_B$ 
4504
4505
4506    ≒ semantic substitution theorem 5.11 and semantic weakening lemma 5.6   )
4507
4508

```

```

4509      f   =   $\llbracket \Gamma \vdash e : \square A \rrbracket$ 
4510    let  g1  =   $\llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : \square C \rrbracket$ 
4511        g2  =   $\langle \pi_1 ; \pi_1 , \pi_2 \rangle ; \llbracket \Gamma, z : C^p \vdash e_1 : B \rrbracket$ 
4512    in    $\langle id_{\Gamma}, f \rangle ; \tau_{\Gamma, \square A} ; T \langle id_{\Gamma \times \square A}, g_1 \rangle ; T \tau_{\Gamma \times \square A, \square C} ; T^2 g_2 ; T \mu_B ; \mu_B$ 
4513
4514 ≡ simplification  }
4515
4516      f   =   $\llbracket \Gamma \vdash e : \square A \rrbracket$ 
4517    let  g1  =   $\llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : \square C \rrbracket$ 
4518        g2  =   $\llbracket \Gamma, z : C^p \vdash e_1 : B \rrbracket$ 
4519    in    $\langle id_{\Gamma}, f \rangle ; \tau_{\Gamma, \square A} ; T \langle id_{\Gamma \times \square A}, g_1 \rangle ; T \tau_{\Gamma \times \square A, \square C}$ 
4520        ;  $T^2 \langle \pi_1 ; \pi_1 , \pi_2 \rangle ; T^2 g_2 ; T \mu_B ; \mu_B$ 
4521
4522 ≡ simplification  }
4523
4524      f   =   $\llbracket \Gamma \vdash e : \square A \rrbracket$ 
4525    let  g1  =   $\llbracket \Gamma, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : \square C \rrbracket$ 
4526        g2  =   $\llbracket \Gamma, z : C^p \vdash e_1 : B \rrbracket$ 
4527    in    $\langle id_{\Gamma}, f \rangle ; \tau_{\Gamma, \square A} ; T g_1 ; \mu_{\square C} ; \tau_{\Gamma, \square C} ; T g_2 ; \mu_B$ 
4528
4529 ≡ definition  }
4530
4531      let  g1  =   $\llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : \square C \rrbracket$ 
4532        g2  =   $\llbracket \Gamma, z : C^p \vdash e_1 : B \rrbracket$ 
4533    in    $\langle id_{\Gamma}, g_1 \rangle ; \tau_{\Gamma, \square C} ; T g_2 ; \mu_B$ 
4534
4535 ≡ induction hypothesis  }
4536
4537      let  g1  =   $\llbracket \Gamma \vdash \mathcal{E}_1 \langle\!\langle e \rangle\!\rangle : \square C \rrbracket$ 
4538        g2  =   $\llbracket \Gamma, z : C^p \vdash e_1 : B \rrbracket$ 
4539    in    $\langle id_{\Gamma}, g_1 \rangle ; \tau_{\Gamma, \square C} ; T g_2 ; \mu_B$ 
4540
4541 ≡ definition  }
4542
4543
4544 ◊  $\mathcal{E} = \text{let box } \boxed{z} = v \text{ in } \mathcal{E}_1$ 
4545
4546
4547       $\llbracket \Gamma \vdash \text{let box } \boxed{x} = e \text{ in } (\text{let box } \boxed{z} = v \text{ in } \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle) : B \rrbracket$ 
4548
4549      let  f   =   $\llbracket \Gamma \vdash e : \square A \rrbracket$ 
4550        g   =   $\llbracket \Gamma, x : A^p \vdash \text{let box } \boxed{z} = v \text{ in } \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \rangle\!\rangle : B \rrbracket$ 
4551    in    $\langle id_{\Gamma}, f \rangle ; \tau_{\Gamma, \square A} ; T g ; \mu_B$ 
4552
4553 ≡ definition  }
4554
4555
4556
4557

```

```

4558      f   =   $\llbracket \Gamma \vdash e : \square A \rrbracket$ 
4559
4560  let  g1  =   $\llbracket \Gamma, x : A^p \vdash v : \square C \rrbracket$ 
4561      g2  =   $\llbracket \Gamma, x : A^p, z : C^p \vdash \mathcal{E}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket$ 
4562      g   =   $\langle id_{\Gamma \times \square A}, g_1 \rangle ; \tau_{\Gamma \times \square A, \square C} ; Tg_2 ; \mu_B$ 
4563  in    $\langle id_{\Gamma}, f \rangle ; \tau_{\Gamma, \square A} ; Tg ; \mu_B$ 
4564

```

\Leftarrow functoriality of $T \rightarrow$

```

4566      f   =   $\llbracket \Gamma \vdash e : \square A \rrbracket$ 
4567  let  g1  =   $\llbracket \Gamma, x : A^p \vdash v : \square C \rrbracket$ 
4568      g2  =   $\llbracket \Gamma, x : A^p, z : C^p \vdash \mathcal{E}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket$ 
4569  in    $\langle id_{\Gamma}, f \rangle ; \tau_{\Gamma, \square A} ; T \langle id_{\Gamma \times \square A}, g_1 \rangle ; T \tau_{\Gamma \times \square A, \square C} ; T^2 g_2 ; T \mu_B ; \mu_B$ 
4570

```

\Leftarrow semantic weakening lemma 5.6 \rightarrow

```

4572      f   =   $\llbracket \Gamma \vdash e : \square A \rrbracket$ 
4573  let  g1  =   $\pi_1 ; \llbracket \Gamma \vdash v : \square C \rrbracket$ 
4574      g2  =   $\llbracket \Gamma, x : A^p, z : C^p \vdash \mathcal{E}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket$ 
4575  in    $\langle id_{\Gamma}, f \rangle ; \tau_{\Gamma, \square A} ; T \langle id_{\Gamma \times \square A}, g_1 \rangle ; T \tau_{\Gamma \times \square A, \square C} ; T^2 g_2 ; T \mu_B ; \mu_B$ 
4576

```

\Leftarrow simplification \rightarrow

```

4579      f   =   $\llbracket \Gamma \vdash e : \square A \rrbracket$ 
4580  let  g1  =   $\llbracket \Gamma \vdash v : \square C \rrbracket$ 
4581      g2  =   $\llbracket \Gamma, x : A^p, z : C^p \vdash \mathcal{E}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket$ 
4582  in    $\langle id_{\Gamma}, f \rangle ; \tau_{\Gamma, \square A} ; T \langle id_{\Gamma \times \square A}, \pi_1 ; g_1 \rangle ; T \tau_{\Gamma \times \square A, \square C} ; T^2 g_2 ; T \mu_B ; \mu_B$ 
4583

```

\Leftarrow semantic substitution theorem 5.11 and semantic weakening lemma 5.6 \rightarrow

```

4586      f   =   $\llbracket \Gamma \vdash e : \square A \rrbracket$ 
4587  let  g1  =   $\llbracket \Gamma \vdash v : \square C \rrbracket$ 
4588      g2  =   $\langle \pi_1 ; \pi_1, \pi_2, \pi_1 ; \pi_2 \rangle ; \llbracket \Gamma, z : C^p, x : A^p \vdash \mathcal{E}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket$ 
4589  in    $\langle id_{\Gamma}, f \rangle ; \tau_{\Gamma, \square A} ; T \langle id_{\Gamma \times \square A}, \pi_1 ; g_1 \rangle ; T \tau_{\Gamma \times \square A, \square C} ; T^2 g_2 ; T \mu_B ; \mu_B$ 
4590

```

\Leftarrow functoriality of $T \rightarrow$

```

4592      f   =   $\llbracket \Gamma \vdash e : \square A \rrbracket$ 
4593  let  g1  =   $\llbracket \Gamma \vdash v : \square C \rrbracket$ 
4594      g2  =   $\llbracket \Gamma, z : C^p, x : A^p \vdash \mathcal{E}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket$ 
4595  in    $\langle id_{\Gamma}, f \rangle ; \tau_{\Gamma, \square A} ; T \langle id_{\Gamma \times \square A}, \pi_1 ; g_1 \rangle ; T \tau_{\Gamma \times \square A, \square C}$ 
4596          ;  $T^2 \langle \pi_1 ; \pi_1, \pi_2, \pi_1 ; \pi_2 \rangle ; T^2 g_2 ; T \mu_B ; \mu_B$ 
4597

```

\Leftarrow semantic weakening lemma 5.6 \rightarrow

```

4600      f   =   $\llbracket \Gamma, z : C^p \vdash e : \square A \rrbracket$ 
4601  let  g1  =   $\llbracket \Gamma \vdash v : \square C \rrbracket$ 
4602      g2  =   $\llbracket \Gamma, z : C^p, x : A^p \vdash \mathcal{E}_1 \langle\langle \text{box } \boxed{x} \rangle\rangle : B \rrbracket$ 
4603  in    $\langle id_{\Gamma}, f \rangle ; \tau_{\Gamma, \square A} ; T \langle id_{\Gamma \times \square A}, \pi_1 ; g_1 \rangle ; T \tau_{\Gamma \times \square A, \square C}$ 
4604          ;  $T^2 \langle \pi_1 ; \pi_1, \pi_2, \pi_1 ; \pi_2 \rangle ; T^2 g_2 ; T \mu_B ; \mu_B$ 
4605

```

4607 \Leftarrow simplification \rangle

$$\begin{array}{l} f = \llbracket \Gamma, z : C^p \vdash e : \square A \rrbracket \\ \text{let } g_1 = \llbracket \Gamma \vdash v : \square C \rrbracket \\ g_2 = \llbracket \Gamma, z : C^p, x : A^p \vdash \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \!\rangle\!\rangle : B \rrbracket \\ \text{in } \langle id_\Gamma, g_1 \rangle ; \tau_{\Gamma, \square C} ; T \langle id_{\Gamma \times \square C}, f \rangle ; T \tau_{\Gamma \times \square C, \square A} ; T^2 g_2 ; T \mu_B ; \mu_B \end{array}$$

4613 \Leftarrow definition \rangle

$$\begin{array}{l} \text{let } g_1 = \llbracket \Gamma \vdash v : \square C \rrbracket \\ g_2 = \llbracket \Gamma, z : C^p \vdash \text{let box } \boxed{x} = e \text{ in } \mathcal{E}_1 \langle\!\langle \text{box } \boxed{x} \!\rangle\!\rangle : B \rrbracket \\ \text{in } \langle id_\Gamma, g_1 \rangle ; \tau_{\Gamma, \square C} ; T g_2 ; \mu_B \end{array}$$

4619 \Leftarrow induction hypothesis \rangle

$$\begin{array}{l} \text{let } g_1 = \llbracket \Gamma \vdash v : \square C \rrbracket \\ g_2 = \llbracket \Gamma, z : C^p \vdash \mathcal{E}_1 \langle\!\langle e \!\rangle\!\rangle : B \rrbracket \\ \text{in } \langle id_\Gamma, g_1 \rangle ; \tau_{\Gamma, \square C} ; T g_2 ; \mu_B \end{array}$$

4624 \Leftarrow definition \rangle

$$\llbracket \Gamma \vdash \text{let box } \boxed{z} = v \text{ in } \mathcal{E}_1 \langle\!\langle e \!\rangle\!\rangle : B \rrbracket$$

□

E PROOFS FOR SECTION 7 (EMBEDDING)

LEMMA E.1. For any context Γ , we have $\underline{\Gamma}^p = \underline{\Gamma}$.

PROOF. We do induction on the context Γ .

(1) $\underline{\Gamma}$

(2) $\underline{\Gamma} = \cdot$

(3) $\cdot^p = \cdot^p = \cdot = \cdot$ by definition

(4) $\underline{\Gamma} = \Delta, x : A$

(5) $\underline{\Delta, x : A}^p = (\underline{\Delta}, \underline{x : A})^p$ by definition

(6) $(\underline{\Delta}, \underline{x : A})^p = \underline{\Delta}^p, \underline{x : A}^p$ by definition

(7) $\underline{\Delta}^p, \underline{x : A}^p = \underline{\Delta}, \underline{x : A}^p$ induction hypothesis

(8) $\underline{\Delta, x : A}^p = \underline{\Delta}, \underline{x : A}^p$

(9) $\underline{\Gamma}^p = \underline{\Gamma}$

□

LEMMA E.2. $\underline{[e'/x] e} = [e'/x] \underline{e}$.

4656 PROOF. We proceed by cases on e .

4657	(1)	$[e'/x] e$	
4658	(2)	$e = ()$	
4659	(3)	$[e'/x] ()$	by definition
4660	(4)	$()$	by definition
4661	(5)	$[e'/x] ()$	by definition
4662	(6)	$[e'/x] ()$	by definition
4663	(7)	$e = x$	
4664	(8)	$[e'/x] x$	by definition
4665	(9)	e'	by definition
4666	(10)	$[e'/x] x$	by definition
4667	(11)	$[e'/x] x$	by definition
4668	(12)	$e = y, (y \neq x)$	
4669	(13)	$[e'/y] x$	by definition
4670	(14)	x	by definition
4671	(15)	x	by definition
4672	(16)	$[e'/y] x$	by definition
4673	(17)	$[e'/y] x$	by definition
4674	(18)	$e = \lambda y. e_1, (y \neq x)$	
4675	(19)	$[e'/x] \lambda y. e_1$	by definition
4676	(20)	$\lambda y. [e'/x] e_1$	by definition
4677	(21)	$\lambda z. \text{let box } \boxed{y} = z \text{ in } [e'/x] e_1$	by definition
4678	(22)	$\lambda z. \text{let box } \boxed{y} = [e'/x] z \text{ in } [e'/x] e_1$	by definition
4679	(23)	$[e'/x] \lambda z. \text{let box } \boxed{x} = z \text{ in } e_1$	by definition
4680	(24)	$[e'/x] \lambda x. e_1$	by definition
4681	(25)	$e = e_1 e_2$	

4705	(26)	$[e'/x] e_1 e_2$	by definition
4706	(27)	$[e'/x] e_1 [e'/x] e_2$	by definition
4707	(28)	$[e'/x] e_1 (\text{box } [e'/x] e_2)$	by definition
4708	(29)	$[e'/x] e_1 ([e'/x] \text{ box } e_2)$	by definition
4709	(30)	$[e'/x] e_1 (\text{box } e_2)$	by definition
4710	(31)	$[e'/x] e_1 e_2$	by definition
4711	(32)	$[e'/x] e$	by definition
4712			
4713			□
4714			
4715			
4716			
4717			
4718			
4719			
4720			
4721	LEMMA E.3.	If $x : A \in \Gamma$, then $\underline{x : A^p} \in \Gamma$.	
4722			
4723	PROOF.	We do induction on $x : A \in \Gamma$.	
4724			
4725	(1)	$x : A \in \Gamma$	
4726			
4727	(2)	$x : A \in (\Gamma, x : A)$	$\in\text{-ID}$
4728			
4729	(3)	$\underline{x : A^p} \in \Gamma, \underline{x : A^p}$	$\in\text{-ID}$
4730			
4731	(4)	$\underline{x : A^p} \in \Gamma, \underline{x : A}$	by definition
4732			
4733	(5)	$x : A \in \Gamma \quad (x \neq y)$	
4734			
4735		$x : A \in (\Gamma, y : B)$	$\in\text{-EX}$
4736			
4737	(6)	$x : A \in \Gamma$	inversion
4738			
4739	(7)	$\underline{x : A^p} \in \Gamma$	induction hypothesis
4740			
4741	(8)	$\underline{x : A^p} \in \Gamma, \underline{y : B^p}$	$\in\text{-EX}$
4742			
4743	(9)	$\underline{x : A^p} \in \Gamma, \underline{y : B}$	by definition
4744			
4745	(10)	$\underline{x : A^p} \in \Gamma$	
4746			
4747			□
4748	THEOREM 7.1 TYPE PRESERVATION.	If $\Gamma \vdash_\lambda e : A$, then $\underline{\Gamma} \vdash \underline{e} : \underline{A}$.	
4749	PROOF.	We do induction on $\Gamma \vdash_\lambda e : A$.	
4750			
4751	(1)	$\boxed{\Gamma \vdash_\lambda e : A}$	
4752			
4753			

4754		$\boxed{\Gamma \vdash_{\lambda} () : \text{unit}}$	
4755	(2)	$\boxed{\Gamma \vdash_{\lambda} () : \text{unit}}$	unitI
4756			
4757	(3)	$\boxed{\Gamma \vdash () : \text{unit}}$	unitI
4758			
4759	(4)	$\boxed{\Gamma \vdash () : \text{unit}}$	by definition
4760			
4761		$\boxed{x : A \in \Gamma}$	
4762	(5)	$\boxed{\Gamma \vdash_{\lambda} x : A}$	VAR
4763			
4764	(6)	$x : A \in \Gamma$	inversion
4765			
4766	(7)	$\boxed{x : A^p \in \Gamma}$	lemma E.3
4767			
4768	(8)	$\boxed{\Gamma \vdash x : A}$	VAR
4769			
4770	(9)	$\boxed{\Gamma \vdash x : A}$	by definition
4771			
4772	(10)	$\boxed{\Gamma, x : A \vdash_{\lambda} e : B}$	$\Rightarrow I$
4773			
4774	(11)	$\Gamma, x : A \vdash_{\lambda} e : B$	inversion
4775			
4776	(12)	$\boxed{\Gamma, x : A \vdash e : B}$	induction hypothesis
4777			
4778	(13)	$\boxed{\Gamma, x : A^p \vdash e : B}$	by definition
4779			
4780	(14)	$\boxed{\Gamma, z : \Box A \vdash z : \Box A}$	VAR
4781			
4782	(15)	$(\Gamma, z : \Box A) \supseteq \Gamma$	\supseteq -WK
4783			
4784	(16)	$(\Gamma, z : \Box A, x : A^p) \supseteq (\Gamma, x : A^p)$	\supseteq -CONG
4785			
4786	(17)	$\boxed{\Gamma, z : \Box A, x : A^p \vdash e : B}$	lemma 3.1 (16) (13)
4787			
4788	(18)	$\Gamma, z : \Box A \vdash \text{let box } [x] = z \text{ in } e : B$	$\Box E$ (14) (17)
4789			
4790	(19)	$\boxed{\Gamma \vdash \lambda z : \Box A. \text{ let box } [x] = z \text{ in } e : \Box A \Rightarrow B}$	$\Rightarrow I$
4791			
4792	(20)	$\boxed{\Gamma \vdash \lambda x : A. e : A \Rightarrow B}$	by definition
4793			
4794	(21)	$\boxed{\Gamma \vdash_{\lambda} e_1 : A \Rightarrow B \quad \Gamma \vdash_{\lambda} e_2 : A}$	$\Rightarrow E$
4795			
4796	(22)	$\Gamma \vdash_{\lambda} e_1 : A \Rightarrow B$	inversion
4797			
4798	(23)	$\Gamma \vdash_{\lambda} e_2 : A$	inversion
4799			
4800	(24)	$\boxed{\Gamma \vdash e_1 : A \Rightarrow B}$	induction hypothesis
4801			
4802	(25)	$\boxed{\Gamma \vdash e_1 : \Box A \Rightarrow B}$	by definition

4803	(26)	$\Gamma \vdash e_2 : A$	induction hypothesis
4804	(27)	$\Gamma^P \vdash e_2 : A$	lemma E.1
4805	(28)	$\Gamma \vdash^P e_2 : A$	CTX-PURE
4806	(29)	$\Gamma \vdash \text{box } e_2 : \square A$	$\square I$
4807	(30)	$\Gamma \vdash e_1 (\text{box } e_2) : B$	$\Rightarrow E (25) (29)$
4808	(31)	$\Gamma \vdash e_1 e_2 : B$	by definition
4809	(32)	$\Gamma \vdash e : A$	

□

THEOREM 7.2 EQUALITY PRESERVATION. If $\Gamma \vdash_\lambda e_1 \approx e_2 : A$, then $\Gamma \vdash e_1 \approx e_2 : A$.

PROOF. We do induction on $\Gamma \vdash_\lambda e_1 \approx e_2 : A$.

4823	(1)	$\Gamma \vdash_\lambda e_1 \approx e_2 : A$	
4824	(2)	$\frac{\Gamma, x : A \vdash_\lambda e_1 : B \quad \Gamma \vdash_\lambda e_2 : A}{\Gamma \vdash_\lambda (\lambda x : A. e_1) e_2 \approx [e_2/x]e_1 : B}$	$\Rightarrow \beta$
4825	(3)	$\Gamma, x : A \vdash_\lambda e_1 : B$	inversion
4826	(4)	$\Gamma, x : A \vdash e_1 : B$	theorem 7.1
4827	(5)	$\Gamma, x : A^P \vdash e_1 : B$	by definition
4828	(6)	$\Gamma \vdash_\lambda e_2 : A$	inversion
4829	(7)	$\Gamma \vdash e_2 : A$	theorem 7.1
4830	(8)	$\Gamma^P \vdash e_2 : A$	lemma E.1
4831	(9)	$\Gamma \vdash \text{let box } x = \text{box } e_2 \text{ in } e \approx [e_2/x]e : B$	$\square \beta$
4832	(10)	$\frac{\Gamma \vdash (\lambda z : \square A. \text{let box } x = z \text{ in } e_1) (\text{box } e_2) \approx \text{let box } x = \text{box } e_2 \text{ in } e_1 : B}{(\lambda z : \square A. \text{let box } x = z \text{ in } e_1) (\text{box } e_2) : B} \Rightarrow \beta$	
4833	(11)	$\frac{\Gamma \vdash (\lambda z : \square A. \text{let box } x = z \text{ in } e_1) (\text{box } e_2) \approx [e_1/x]e_2 : B}{(\lambda z : \square A. \text{let box } x = z \text{ in } e_1) (\text{box } e_2) : B} \text{ TRANS}$	

4852	(12)	$\Gamma \vdash (\lambda x : A. e_1) e_2 \approx [e_2/x]e_1 : B$	by definition
4853		$\boxed{\Gamma \vdash_{\lambda} e : A \Rightarrow B}$	
4854	(13)	$\Gamma \vdash_{\lambda} e \approx \lambda x : A. e x : A \Rightarrow B$	$\Rightarrow\eta$
4855	(14)	$\Gamma \vdash_{\lambda} e : A \Rightarrow B$	inversion
4856	(15)	$\Gamma \vdash e : A \Rightarrow B$	theorem 7.1
4857	(16)	$\Gamma \vdash e : \Box A \Rightarrow B$	by definition
4858	(17)	$\Gamma^p \vdash e : \Box A \Rightarrow B$	lemma E.1
4859	(18)	$\Gamma \vdash^p e : \Box A \Rightarrow B$	CTX-PURE
4860	(19)	$\Gamma \vdash e \approx \lambda z. e z : \Box A \Rightarrow B$	$\Rightarrow\eta$ -PURE
4861	(20)	$\Gamma, z : \Box A \vdash z : \Box A$	VAR
4862	(21)	$\Gamma, z : \Box A \vdash e : \Box A \Rightarrow B$	lemma 3.1 (16)
4863	(22)	$\Gamma, z : \Box A \vdash e z : B$	$\Rightarrow E$
4864	(23)	$\Gamma, z : \Box A, x : A^p \vdash x : A$	VAR
4865	(24)	$\Gamma, z : \Box A, x : A^p \vdash \text{box}[x] : \Box A$	$\Box I$
4866	(25)	$\Gamma, z : \Box A, x : A^p \vdash e(\text{box}[x]) : B$	$\Rightarrow E$
4867	(26)	$\Gamma, z : \Box A \vdash \text{let box}[x] = z \text{ in } e(\text{box}[x]) : B$	$\Box E$
4868	(27)	$\Gamma, z : \Box A \vdash \begin{array}{c} e z \\ \approx \\ \text{let box}[x] = z \text{ in } e(\text{box}[x]) \end{array} : B$	$\Box \eta$ -IMPURE on e \mathcal{E}
4869	(28)	$\Gamma \vdash \begin{array}{c} \lambda z. e z \\ \approx \\ \lambda z. \text{let box}[x] = z \text{ in } e(\text{box}[x]) \end{array} : \Box A \Rightarrow B$	λ -CONG
4870	(29)	$\Gamma \vdash \begin{array}{c} e \\ \approx \\ \lambda z. \text{let box}[x] = z \text{ in } e(\text{box}[x]) \end{array} : \Box A \Rightarrow B$	TRANS
4871	(30)	$\Gamma \vdash \begin{array}{c} e \\ \approx \\ \lambda z. \text{let box}[x] = z \text{ in } e(\text{box}[x]) \end{array} : \Box A \Rightarrow B$	by definition
4872	(31)	$\Gamma \vdash e \approx \lambda x. e x : A \Rightarrow B$	by definition
4873	(32)	$\boxed{\Gamma \vdash_{\lambda} e : A}$	REFL

4901	(33)	$\Gamma \vdash_{\lambda} e : A$	inversion
4902	(34)	$\boxed{\Gamma \vdash \underline{e} : \underline{A}}$	theorem 7.1
4903	(35)	$\boxed{\Gamma \vdash \underline{e} \approx \underline{e} : \underline{A}}$	REFL
4904		$\frac{\Gamma \vdash_{\lambda} e_1 \approx e_2 : A}{\Gamma \vdash_{\lambda} e_2 \approx e_1 : A}$	
4905	(36)	$\Gamma \vdash_{\lambda} e_2 \approx e_1 : A$	SYM
4906	(37)	$\Gamma \vdash_{\lambda} e_1 \approx e_2 : A$	inversion
4907	(38)	$\boxed{\Gamma \vdash \underline{e}_1 \approx \underline{e}_2 : \underline{A}}$	induction hypothesis
4908	(39)	$\Gamma \vdash \underline{e}_2 \approx \underline{e}_1 : \underline{A}$	SYM
4909		$\frac{\Gamma \vdash_{\lambda} e_1 \approx e_2 : A \quad \Gamma \vdash_{\lambda} e_2 \approx e_3 : A}{\Gamma \vdash_{\lambda} e_1 \approx e_3 : A}$	
4910	(40)	$\Gamma \vdash_{\lambda} e_1 \approx e_3 : A$	TRANS
4911	(41)	$\Gamma \vdash_{\lambda} e_1 \approx e_2 : A$	inversion
4912	(42)	$\Gamma \vdash_{\lambda} e_2 \approx e_3 : A$	inversion
4913	(43)	$\boxed{\Gamma \vdash \underline{e}_1 \approx \underline{e}_2 : \underline{A}}$	induction hypothesis
4914		$\frac{\Gamma \vdash_{\lambda} e_2 \approx e_3 : A}{\Gamma \vdash \underline{e}_2 \approx \underline{e}_3 : \underline{A}}$	
4915	(44)	$\Gamma \vdash \underline{e}_2 \approx \underline{e}_3 : \underline{A}$	induction hypothesis
4916	(45)	$\Gamma \vdash \underline{e}_1 \approx \underline{e}_3 : \underline{A}$	TRANS
4917		$\frac{\Gamma, x : A \vdash_{\lambda} e_1 \approx e_2 : B}{\Gamma \vdash_{\lambda} \lambda x : A. e_1 \approx \lambda x : A. e_2 : A \Rightarrow B}$	
4918	(46)	$\Gamma \vdash_{\lambda} \lambda x : A. e_1 \approx \lambda x : A. e_2 : A \Rightarrow B$	λ -CONG
4919	(47)	$\Gamma, x : A \vdash_{\lambda} e_1 \approx e_2 : B$	inversion
4920	(48)	$\boxed{\Gamma, x : A \vdash \underline{e}_1 \approx \underline{e}_2 : \underline{B}}$	induction hypothesis
4921	(49)	$\boxed{\Gamma, \textcolor{blue}{x} : A^P \vdash \underline{e}_1 \approx \underline{e}_2 : \underline{B}}$	by definition
4922	(50)	$\boxed{\Gamma, z : \square A, \textcolor{blue}{x} : A^P \vdash \underline{e}_1 \approx \underline{e}_2 : \underline{B}}$	lemma 3.1
4923	(51)	$\Gamma, z : \square A \vdash z : \square A$	VAR
4924	(52)	$\boxed{\Gamma, z : \square A \vdash z \approx z : \square A}$	REFL
4925	(53)	$\boxed{\Gamma, z : \square A \vdash \begin{array}{c} (\text{let box } \boxed{x} = z \text{ in } \underline{e}_1) \\ \approx \\ (\text{let box } \boxed{x} = z \text{ in } \underline{e}_2) \end{array} : B}$	let box-CONG
4926		$\boxed{\Gamma \vdash \begin{array}{c} (\lambda z. \text{let box } \boxed{x} = z \text{ in } \underline{e}_1) \\ \approx \\ (\lambda z. \text{let box } \boxed{x} = z \text{ in } \underline{e}_2) \end{array} : \square A \Rightarrow B}$	
4927	(54)	$\Gamma \vdash \boxed{\begin{array}{c} (\lambda z. \text{let box } \boxed{x} = z \text{ in } \underline{e}_1) \\ \approx \\ (\lambda z. \text{let box } \boxed{x} = z \text{ in } \underline{e}_2) \end{array} : \square A \Rightarrow B}$	λ -CONG

4950	(55)	$\Gamma \vdash \lambda x. e_1 \approx \lambda x. e_2 : A \Rightarrow B$	by definition
4951			
4952	(56)	$\frac{\Gamma \vdash_\lambda e_1 \approx e_2 : A \Rightarrow B \quad \Gamma \vdash_\lambda e_3 \approx e_4 : A}{\Gamma \vdash_\lambda e_1 e_3 \approx e_2 e_4 : B}$	APP-CONG
4953			
4954	(57)	$\Gamma \vdash_\lambda e_1 \approx e_2 : A \Rightarrow B$	inversion
4955			
4956	(58)	$\Gamma \vdash e_1 \approx e_2 : A \Rightarrow B$	induction hypothesis
4957			
4958	(59)	$\Gamma \vdash e_1 \approx e_2 : \square A \Rightarrow B$	by definition
4959			
4960	(60)	$\Gamma \vdash e_3 \approx e_4 : A$	induction hypothesis
4961			
4962	(61)	$\Gamma^p \vdash e_3 \approx e_4 : A$	lemma E.1
4963			
4964	(62)	$\Gamma \vdash \text{box } \boxed{e_3} \approx \text{box } \boxed{e_4} : \square A$	box-CONG
4965			
4966	(63)	$\Gamma \vdash e_1 (\text{box } \boxed{e_2}) \approx e_3 (\text{box } \boxed{e_4}) : B$	APP-CONG
4967			
4968	(64)	$\Gamma \vdash e_1 e_2 \approx e_3 e_4 : B$	by definition
4969			
4970	(65)	$\Gamma \vdash e_1 \approx e_2 : A$	
4971			
4972			
4973			
4974			□

We can define a reverse translation which forgets the purity annotations, in figure 17.

4975 4976 4977 4978 4979 4980 4981 4982 4983 4984 4985 4986 4987 4988 4989 4990 4991 4992 4993 4994 4995 4996 4997 4998	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; text-align: right; padding-right: 10px;">TYPES</td> <td style="width: 70%;">$\widehat{b} := \text{unit}$ $\widehat{A \Rightarrow B} := \widehat{A} \Rightarrow \widehat{B}$ $\widehat{\square A} := \widehat{A}$</td> </tr> <tr> <td style="text-align: right; padding-right: 10px;">CONTEXTS</td> <td>$\widehat{\cdot} := \cdot$ $\widehat{\Gamma, x : A^q} := \widehat{\Gamma}, x : \widehat{A}$</td> </tr> <tr> <td style="text-align: right; padding-right: 10px;">TERMS</td> <td>$\widehat{()} := ()$ $\widehat{s} := ()$ $\widehat{x} := x$ $\widehat{\lambda x : A. e} := \lambda x : \widehat{A}. \widehat{e}$ $\widehat{e_1 e_2} := \widehat{e_1} \widehat{e_2}$ $\widehat{\text{box } \boxed{e}} := \widehat{e}$ $\widehat{\text{let box } \boxed{x} = e_1 \text{ in } e_2} := (\lambda x. \widehat{e_2}) \widehat{e_1}$ $\widehat{e_1 \cdot \text{print}(e_2)} := ()$</td> </tr> </table>	TYPES	$\widehat{b} := \text{unit}$ $\widehat{A \Rightarrow B} := \widehat{A} \Rightarrow \widehat{B}$ $\widehat{\square A} := \widehat{A}$	CONTEXTS	$\widehat{\cdot} := \cdot$ $\widehat{\Gamma, x : A^q} := \widehat{\Gamma}, x : \widehat{A}$	TERMS	$\widehat{()} := ()$ $\widehat{s} := ()$ $\widehat{x} := x$ $\widehat{\lambda x : A. e} := \lambda x : \widehat{A}. \widehat{e}$ $\widehat{e_1 e_2} := \widehat{e_1} \widehat{e_2}$ $\widehat{\text{box } \boxed{e}} := \widehat{e}$ $\widehat{\text{let box } \boxed{x} = e_1 \text{ in } e_2} := (\lambda x. \widehat{e_2}) \widehat{e_1}$ $\widehat{e_1 \cdot \text{print}(e_2)} := ()$
TYPES	$\widehat{b} := \text{unit}$ $\widehat{A \Rightarrow B} := \widehat{A} \Rightarrow \widehat{B}$ $\widehat{\square A} := \widehat{A}$						
CONTEXTS	$\widehat{\cdot} := \cdot$ $\widehat{\Gamma, x : A^q} := \widehat{\Gamma}, x : \widehat{A}$						
TERMS	$\widehat{()} := ()$ $\widehat{s} := ()$ $\widehat{x} := x$ $\widehat{\lambda x : A. e} := \lambda x : \widehat{A}. \widehat{e}$ $\widehat{e_1 e_2} := \widehat{e_1} \widehat{e_2}$ $\widehat{\text{box } \boxed{e}} := \widehat{e}$ $\widehat{\text{let box } \boxed{x} = e_1 \text{ in } e_2} := (\lambda x. \widehat{e_2}) \widehat{e_1}$ $\widehat{e_1 \cdot \text{print}(e_2)} := ()$						

Fig. 17. Reverse Translation to STLC

4999 We use the notation \widehat{X} to denote the *unembedding* of a syntactic object X from our calculus to
 5000 STLC. We use b to mean base types, i.e., unit, str and cap.

5001 We prove some properties of the unembedding of an embedded term.

5002 LEMMA E.4. For any STLC type A , $\widehat{\widehat{A}} = A$.

5003 PROOF. We do induction on A .

5005	(1)	A	
5006	(2)	\widehat{b}	
5007	(3)	\widehat{b}	definition
5008	(4)	b	definition
5009	(5)	$A \Rightarrow B$	
5010	(6)	$\widehat{A \Rightarrow B}$	definition
5011	(7)	$\widehat{\widehat{A \Rightarrow B}}$	definition
5012	(8)	$\widehat{\widehat{A \Rightarrow B}}$	definition
5013	(9)	$A \Rightarrow B$	induction hypothesis
5014	(10)	$\widehat{\widehat{A}} = A$	

□

5026 LEMMA E.5. For any STLC context Γ , $\widehat{\widehat{\Gamma}} = \Gamma$.

5027 PROOF. We do induction on Γ .

5028	(1)	Γ	
5029	(2)	$\widehat{\Gamma}$	
5030	(3)	$\widehat{\widehat{\Gamma}}$	definition
5031	(4)	.	definition
5032	(5)	$\widehat{\widehat{\Gamma}}, x : A$	
5033	(6)	$\widehat{\widehat{\widehat{\Gamma}}}, x : A^p$	definition
5034	(7)	$\widehat{\widehat{\widehat{\Gamma}}}, x : \widehat{A}$	definition
5035	(8)	$\widehat{\widehat{\widehat{\Gamma}}}, x : A$	lemma E.4
5036	(9)	$\widehat{\widehat{\Gamma}}, x : A$	induction hypothesis
5037	(10)	$\widehat{\widehat{\widehat{\Gamma}}} = \Gamma$	

5048

5049

LEMMA E.6. If $\Gamma \vdash_{\lambda} e : A$, then $\Gamma \vdash_{\lambda} \widehat{e} : A$. □

5051

PROOF. We do induction on $\Gamma \vdash_{\lambda} e : A$.

5053

(1)	$\boxed{\Gamma \vdash_{\lambda} e : A}$	
(2)	$\boxed{\Gamma \vdash_{\lambda} () : \text{unit}}$	unitI
(3)	$\boxed{\Gamma \vdash_{\lambda} () : \text{unit}}$	unitI
(4)	$\boxed{\frac{x : A \in \Gamma}{\Gamma \vdash_{\lambda} x : A}}$	VAR
(5)	$x : A \in \Gamma$	inversion
(6)	$\boxed{\Gamma \vdash_{\lambda} x : A}$	VAR
(7)	$\boxed{\frac{\Gamma, x : A \vdash_{\lambda} e : B}{\Gamma \vdash_{\lambda} \lambda x : A. e : A \Rightarrow B}}$	$\Rightarrow I$
(8)	$\Gamma, x : A \vdash_{\lambda} e : B$	inversion
(9)	$\Gamma \vdash_{\lambda} \boxed{\lambda x : A. e} : A \Rightarrow B$	
(10)	$\boxed{\frac{\Gamma \vdash_{\lambda} e_1 : A \Rightarrow B \quad \Gamma \vdash_{\lambda} e_2 : A}{\Gamma \vdash_{\lambda} e_1 e_2 : B}}$	$\Rightarrow E$
(11)	$\Gamma \vdash_{\lambda} e_1 : A \Rightarrow B$	inversion
(12)	$\Gamma \vdash_{\lambda} e_2 : A$	inversion
(13)	$\Gamma \vdash_{\lambda} \boxed{e_1 e_2} : B$	
(14)	$\Gamma \vdash_{\lambda} \widehat{e} : A$	

5083

5084

□

We observe that an embedding followed by an unembedding gives a $\beta\eta$ -equal term.

5085

LEMMA E.7. If $\Gamma \vdash_{\lambda} e : A$, then $\Gamma \vdash_{\lambda} e \approx \widehat{e} : A$.

5088

PROOF. We do induction on $\Gamma \vdash_{\lambda} e : A$.

5089

(1)	$\boxed{\Gamma \vdash_{\lambda} e : A}$	
(2)	$\boxed{\frac{x : A \in \Gamma}{\Gamma \vdash_{\lambda} x : A}}$	VAR

5097	(3)	$\widehat{\widehat{x}} = \widehat{x} = x$	definition
5098	(4)	$\Gamma \vdash_{\lambda} \widehat{\widehat{x}} : A$	
5099	(5)	$\Gamma \vdash_{\lambda} x \approx \widehat{\widehat{x}} : A$	REFL
5100	(6)	$\frac{\Gamma, x : A \vdash_{\lambda} e : B}{\Gamma \vdash_{\lambda} \lambda x : A. e : A \Rightarrow B}$	$\Rightarrow I$
5101	(7)	$\Gamma \vdash_{\lambda} \lambda x : A. e \approx \lambda z : A. (\lambda x : A. e) z : B$	$\Rightarrow \eta$
5102	(8)	$\lambda z : A. (\lambda x : A. e) z = \lambda z : \widehat{A}. (\lambda x : A. e) z$	lemma E.4
5103	(9)	$\lambda z : \widehat{A}. (\lambda x : A. e) z = \lambda z : \widehat{\square A}. \text{let box } \widehat{x} = z \text{ in } e$	definition
5104	(10)	$\lambda z : \widehat{\square A}. \text{let box } \widehat{x} = z \text{ in } e = \lambda z : \widehat{\square A}. \text{let box } \widehat{x} = z \text{ in } e$	definition
5105	(11)	$\lambda z : \widehat{\square A}. \text{let box } \widehat{x} = z \text{ in } e = \lambda x : A. e$	definition
5106	(12)	$\Gamma \vdash_{\lambda} \lambda x : A. e \approx \lambda x : A. e : A \Rightarrow B$	
5107	(13)	$\frac{\Gamma \vdash_{\lambda} e_1 : A \Rightarrow B \quad \Gamma \vdash_{\lambda} e_2 : A}{\Gamma \vdash_{\lambda} e_1 e_2 : B}$	$\Rightarrow E$
5108	(14)	$\Gamma \vdash_{\lambda} e_1 : A \Rightarrow B$	inversion
5109	(15)	$\Gamma \vdash_{\lambda} e_2 : A$	inversion
5110	(16)	$\Gamma \vdash_{\lambda} e_1 \approx \widehat{e_1} : A \Rightarrow B$	induction hypothesis
5111	(17)	$\Gamma \vdash_{\lambda} e_2 \approx \widehat{e_2} : A$	induction hypothesis
5112	(18)	$\Gamma \vdash_{\lambda} e_1 e_2 \approx \widehat{e_1} \widehat{e_2} : B$	APP-CONG
5113	(19)	$\widehat{e_1} \widehat{e_2} = \widehat{e_1} \text{ box } \widehat{e_2} = \widehat{e_1} \text{ box } \widehat{\square e_2} = \widehat{e_1 e_2}$	definition
5114	(20)	$\Gamma \vdash_{\lambda} e_1 e_2 \approx \widehat{e_1 e_2} : B$	
5115	(21)	$\Gamma \vdash_{\lambda} e \approx \widehat{e} : A$	

□

At this point, we could setup a syntactic logical relation to show a conservative extension result. Instead, we will use an abstract trick.

Note that there is a forgetful functor from \mathcal{C} to Set, which forgets the weight assignments. It is easy to see from our definition of \mathcal{C} in section 4 that this functor preserves the cartesian closed structure, and is hence a cartesian closed functor. Forgetting the extra structure of Set, we could instead choose CCC[1], the free cartesian closed category on one generator 1. We consider the forgetful functor \mathcal{F} from \mathcal{C} to CCC[1], which forgets the capability annotations.

$$\begin{aligned}
 5146 \quad \mathcal{F}(\text{unit}) &:= 1 \\
 5147 \quad \mathcal{F}(\Sigma^*) &:= 1 \\
 5148 \quad \mathcal{F}(A \times B) &:= \mathcal{F}(A) \times \mathcal{F}(B) \\
 5149 \quad \mathcal{F}(A \Rightarrow B) &:= \mathcal{F}(A) \Rightarrow \mathcal{F}(B)
 \end{aligned}$$

5152 We note that it maps the monad and comonad to identity.

$$\begin{aligned}
 5153 \quad \mathcal{F}(\square A) &= \mathcal{F}(A) \\
 5154 \quad \mathcal{F}(TA) &= \mathcal{F}(A)
 \end{aligned}$$

5155 We observe that the action of this functor \mathcal{F} on embedded terms gives back the original term.

5156 LEMMA E.8. If $\Gamma \vdash_\lambda e : A$, then $\mathcal{F}(\llbracket \Gamma \vdash e : A \rrbracket) = \llbracket \Gamma \vdash_\lambda e : A \rrbracket$.

5157 PROOF. We proceed by induction on $\Gamma \vdash_\lambda e : A$.

$$\diamond \frac{x : A \in \Gamma}{\Gamma \vdash_\lambda x : A} \text{ VAR}$$

$$\begin{aligned}
 5160 \quad &\mathcal{F}(\llbracket \Gamma \vdash x : A \rrbracket) \\
 5161 \quad &\equiv \text{definition } \rightarrow \\
 5162 \quad &\boxed{\mathcal{F}(\llbracket x : A \in \Gamma \rrbracket ; \eta_A)} \\
 5163 \quad &\equiv \text{functoriality of } \mathcal{F} \rightarrow \\
 5164 \quad &\boxed{\mathcal{F}(\llbracket x : A \in \Gamma \rrbracket) ; \mathcal{F}(\eta_A)} \\
 5165 \quad &\equiv \text{definition } \rightarrow \\
 5166 \quad &\boxed{\llbracket x : A \in \Gamma \rrbracket} \\
 5167 \quad &\equiv \text{definition } \rightarrow \\
 5168 \quad &\boxed{\llbracket \Gamma \vdash_\lambda e : A \rrbracket}
 \end{aligned}$$

$$\diamond \frac{\Gamma, x : A \vdash_\lambda e : B}{\Gamma \vdash_\lambda \lambda x : A. e : A \Rightarrow B} \Rightarrow I$$

$$\begin{aligned}
 5169 \quad &\mathcal{F}(\llbracket \Gamma \vdash \lambda x : A. e : A \Rightarrow B \rrbracket) \\
 5170 \quad &\equiv \text{definition } \rightarrow \\
 5171 \quad &\boxed{\mathcal{F}(\llbracket \Gamma \vdash \lambda z : \square A. \text{let box } \boxed{x} = z \text{ in } e : \square A \Rightarrow B \rrbracket)} \\
 5172 \quad &\equiv \text{definition } \rightarrow \\
 5173 \quad &\boxed{\mathcal{F}(\text{curry}(\llbracket \Gamma, z : \square A \rrbracket \vdash \text{let box } \boxed{x} = z \text{ in } e : B) ; \eta_{A \rightarrow TB})} \\
 5174 \quad &\equiv \text{functoriality of } \mathcal{F} \rightarrow \\
 5175 \quad &\boxed{\mathcal{F}(\text{curry}(\llbracket \Gamma, z : \square A \rrbracket \vdash \text{let box } \boxed{x} = z \text{ in } e : B)) ; \mathcal{F}(\eta_{A \rightarrow TB})}
 \end{aligned}$$

- 5195 \Leftarrow definition)
- 5196 let $f = \llbracket \Gamma, z : \square A^i \vdash z : \square A \rrbracket$
 5197 let $g = \llbracket \Gamma, z : \square A^i, x : A^p \vdash e : B \rrbracket$
 5198 in $\mathcal{F}(\text{curry}(\langle id_{\Gamma \times \square A}, f \rangle; \tau_{\Gamma \times \square A, \square A}; Tg; \mu_B))$
- 5200
- 5201 \Leftarrow simplification)
- 5202 let $g = \llbracket \Gamma, z : \square A^i, x : A^p \vdash e : B \rrbracket$
 5203 in $\mathcal{F}(\text{curry}(\langle id_{\Gamma \times \square A}, \pi_2; \eta_{\square A} \rangle; \tau_{\Gamma \times \square A, \square A}; Tg; \mu_B))$
- 5204
- 5205 \Leftarrow strength law and monad laws)
- 5206 let $g = \llbracket \Gamma, z : \square A^i, x : A^p \vdash e : B \rrbracket$
 5207 in $\mathcal{F}(\text{curry}(\langle id_{\Gamma \times \square A}, \pi_2 \rangle; g))$
- 5208
- 5209 \Leftarrow \mathcal{F} preserves exponentials)
- 5210 $\text{curry}(\mathcal{F}(\llbracket \Gamma, x : A^p \vdash e : B \rrbracket))$
- 5211
- 5212 \Leftarrow definition)
- 5213 $\text{curry}(\mathcal{F}(\llbracket \Gamma, x : A \vdash e : B \rrbracket))$
- 5214
- 5215 \Leftarrow induction hypothesis)
- 5216 $\text{curry}(\llbracket \Gamma, x : A \vdash_{\lambda} e : B \rrbracket)$
- 5217
- 5218 \Leftarrow definition)
- 5219 $\llbracket \Gamma \vdash_{\lambda} \lambda x : A. e : A \Rightarrow B \rrbracket$
- 5220
- 5221
- 5222
- 5223
- 5224 $\diamond \frac{\Gamma \vdash_{\lambda} e_1 : A \Rightarrow B \quad \Gamma \vdash_{\lambda} e_2 : A}{\Gamma \vdash_{\lambda} e_1 e_2 : B} \Rightarrow_E$
- 5225
- 5226
- 5227 $\mathcal{F}(\llbracket \Gamma \vdash e_1 e_2 : B \rrbracket)$
- 5228
- 5229 \Leftarrow definition)
- 5230 $\mathcal{F}(\llbracket \Gamma \vdash e_1 \text{ box } e_2 : B \rrbracket)$
- 5231
- 5232 \Leftarrow definition)
- 5233 let $f = \llbracket \Gamma \vdash e_1 : \square A \Rightarrow B \rrbracket$
 5234 let $g = \llbracket \Gamma \vdash \text{box } e_2 : \square A \rrbracket$
 5235 in $\mathcal{F}(f, g) ; \beta_{\square A \rightarrow TB, \square A} ; T \text{ ev}_{\square A, TB} ; \mu_B$
- 5236
- 5237
- 5238 \Leftarrow functoriality of \mathcal{F})
- 5239
- 5240
- 5241
- 5242
- 5243

5244 $f = \llbracket \Gamma \vdash e_1 : \square A \Rightarrow B \rrbracket$
 5245 let
 5246 $g = \llbracket \Gamma \vdash \text{box } e_2 : \square A \rrbracket$
 5247 in $\mathcal{F}(\langle f, g \rangle) ; \mathcal{F}(\beta_{\square A \rightarrow TB, \square A}) ; \mathcal{F}(T \text{ ev}_{\square A, TB}) ; \mathcal{F}(\mu_B)$
 5248
 5249 \equiv action of \mathcal{F} \rangle
 5250 let $f = \mathcal{F}(\llbracket \Gamma \vdash e_1 : A \Rightarrow B \rrbracket)$
 5251 $g = \mathcal{F}(\llbracket \Gamma \vdash e_2 : A \rrbracket)$
 5252 in $\langle f, g \rangle ; \text{ev}_{A,B}$
 5253
 5254 \equiv induction hypothesis \rangle
 5255 let $f = \llbracket \Gamma \vdash_\lambda e_1 : A \Rightarrow B \rrbracket$
 5256 $g = \llbracket \Gamma \vdash_\lambda e_2 : A \rrbracket$
 5257 in $\langle f, g \rangle ; \text{ev}_{A,B}$
 5258
 5259 \equiv definition \rangle
 5260 $\llbracket \Gamma \vdash_\lambda e_1 e_2 : B \rrbracket$
 5261
 5262
 5263
 5264
 5265

THEOREM 7.3 CONSERVATIVE EXTENSION. If $\Gamma \vdash_\lambda e_1 : A$, $\Gamma \vdash_\lambda e_2 : A$, and $\llbracket \Gamma \vdash e_1 \approx e_2 : A \rrbracket$,
 then $\Gamma \vdash_\lambda e_1 \approx e_2 : A$.
 PROOF.

□

5269
 5270 (1) $\llbracket \Gamma \vdash_\lambda e_1 : A, \Gamma \vdash_\lambda e_2 : A \rrbracket$
 5271
 5272 (2) $\llbracket \Gamma \vdash e_1 \approx e_2 : A \rrbracket$
 5273
 5274 (3) $\llbracket \Gamma \vdash e_1 : A \rrbracket = \llbracket \Gamma \vdash e_2 : A \rrbracket$ soundness of \approx theorem 6.1
 5275
 5276 (4) $\mathcal{F}(\llbracket \Gamma \vdash e_1 : A \rrbracket) = \mathcal{F}(\llbracket \Gamma \vdash e_2 : A \rrbracket)$ congruence
 5277
 5278 (5) $\llbracket \Gamma \vdash_\lambda e_1 : A \rrbracket = \llbracket \Gamma \vdash_\lambda e_2 : A \rrbracket$ lemma E.8
 5279
 5280 (6) $\Gamma \vdash_\lambda e_1 \approx e_2 : A$ completeness of STLC

□

5281
 5282
 5283
 5284
 5285
 5286
 5287
 5288
 5289
 5290
 5291
 5292