# A Modal Language for the Safety of Mobile Values

**Sungwoo Park**

April 25, 2005
CMU-CS-05-124 3

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

**Abstract**

We present a modal language for distributed computation which addresses the safety of mobile values as well as mobile code. The safety of mobile code is achieved with the modality • which corresponds to necessity of modal logic. For the safety of mobile values, we introduce a new modality O which expresses that given code evaluates to a mobile value. We demonstrate the use of modal types with three communication constructs: remote evaluation, futures, and asynchronous channels.

**Keywords:** Modal language, Distributed computation, Type system

# 1 Introduction

A distributed computation is a cooperative process taking place in a network of nodes. Each node is capable of performing a stand-alone computation and also communicating with other nodes to distribute and collect code and data. Thus a distributed computation has the potential to make productive use of all the nodes in the network simultaneously.

Usually a distributed computation assumes a heterogeneous group of nodes with different *local resources.* A local resource can be either a permanent/physical object available at a particular node *(e.g.,* printer, database) or an ephemeral/semantic object created during a stand-alone computation *(e.g.,* heap cell, abstract data type). Local resources are accessed via their references *(e.g.,* handle for a database file, pointer to a heap cell).

Local resources, however, give rise to an issue not found in stand-alone computations: the safety of *mobile code,* or in our terminology, the safety of *mobile terms* where a term represents a piece of code. In essence, a node cannot access remote resources in the same way that it accesses its own local resources, but it may receive mobile terms in which references to remote resources are exposed. Therefore the safety of mobile terms is achieved either by supporting direct access to remote resources *(e.g.,* remote file access, remote memory access) or by preventing references to remote resources from being dereferenced. This paper focuses on the second case with the assumption that references to remote resources are allowed in mobile terms as long as they are never dereferenced.

One approach to the safety of mobile terms is to build a modal type system with the modality • [1, 12, 9, 13]. The basic idea is that a value of modal type *DA* contains a mobile term that can be evaluated at any node. An indexed modal type *O^A* is used for mobile terms that can be evaluated at node *UJ.* By requiring that a mobile term be from a value of type *DA* or *D^A,* we ensure its safety without recourse to runtime checks.

A type system augmented with the modality • is not, however, expressive enough for the safe communication of *values, i.e.,* the safety of *mobile values.* In other words, we cannot rely solely on modal types •^4 and *D^A* to verify that a value communicated from one node to another is mobile *(e.g.,* when a remote procedure call returns, or when a value is written to a channel). The reason is that in general, a value of type CM or *D^A* contains *not a mobile value but a mobile term.* The evaluation of such a mobile term (with the intention of obtaining a mobile value) may result in a value that is not necessarily mobile because of references to local resources created during the evaluation.

As an example, consider a term of type `int -> int` in an ML-like language:

```
let
  val new_reference = ref 0
  val f = fn x => x + !new.reference
in
  f
end
```

The above term may be used in building a mobile term of type •`(int -> int)`, since it can be evaluated at any node. The resultant value f, however, is not mobile because it accesses a local resource `new.reference`. In contrast, the following term, also of type `int -> int`, cannot be used in building a mobile term, but the resultant value is mobile because it does not access any local resource:

```
let
  val v =  !some_existing_reference
  val f = fn x => x + v
in
  f
end
```

Hence the modality • is irrelevant to the safety of mobile values, which should now be verified by programmers themselves.

This paper investigates a new modality O which expresses that a given term evaluates to a mobile value. The basic idea is that a term contained in a value of modal type *OA* evaluates to a value that is valid at any node. Similarly to $D_U,A_9$ an indexed modal type *O^A* is used if the resultant value is valid at node *w.* To obtain a value to be communicated to other nodes, we evaluate a term contained in a value of type O^4 or Ou,*A.* In this way, we achieve the safety of mobile values.

Since the mobility of a term is independent of the mobility of the value to which it evaluates, the two modalities • and O are developed in an orthogonal way:

*DA*

|

*O^A* - *A* - *OA*

|

$\Box_\omega A$

We use combinations of • and O to express various properties of mobile terms:

- *UOA:* evaluates at any node to a value valid at any node.
- $\Box\bigcirc$*CJA:* evaluates at any node to a value valid at node *u.*
- $\Box_\omega \bigcirc A$*:* evaluates at node *u* to a value valid at any node.
- $\Box_\omega \bigcirc_{\omega'} A$: evaluates at node u> to a value valid at node a/.

We first develop a modal language AQO by extending the A-calculus with the modalities • and O. We formulate its type system in the natural deduction style by giving introduction and elimination rules for each connective and modality. The modality O requires us to introduce a typing judgment differentiating values from terms. This typing judgment induces a substitution defined inductively on the structure of the term being substituted instead of the term being substituted into. We then develop another modal language Ano^ by extending AQO with the indexed modalities D^ and $O_w$.

We also present a network operational semantics for Ano^ which is capable of modeling distributed computations. We demonstrate the use of modal types in the network operational semantics with three communication constructs: *remote evaluation, futures,* and *asynchronous channels.* The safety of mobile terms and mobile values is shown by the type safety of the network operational semantics, *i.e.,* its type preservation and progress properties.

Depending on the degree of code mobility and data mobility, languages for distributed computation are classified into four paradigms: *client/server, remote evaluation, code on demand,* and *mobile agents* [4]. The client/server paradigm allows only data to be transmitted to remote nodes. The remote evaluation paradigm extends the client/server paradigm by allowing both code and data to be transmitted to remote nodes. The code on demand paradigm is similar to the remote evaluation paradigm, but both code and data are fetched from remote nodes. In the mobile agents paradigm, autonomous code migrates to remote nodes by itself and also carries its state. *XQCF* belongs to the remote evaluation paradigm as its primary capability is to transmit and evaluate mobile terms at remote nodes. The two modalities D and O deal with *name resolution* [5], a safety issue in languages for distributed computation.

This paper is organized as follows. In Section 2, we develop the modal language AQO- In Section 3, we develop the modal language Ano^w^- In Section 4, we present the network operational semantics and prove its type safety. Section 5 discusses how to handle local resources in distributed computations and compares AQCT with other modal languages for distributed computation. Section 6 concludes with future work. See Appendix for details of all proofs.

## 2 Modal Language $A_n$o

Since AQO is an extension of the A-calculus, we first review the type system of the A-calculus in the context of distributed computations.

The syntax of the A-calculus is standard; we use metavariables *A*, *B* for types and M, *N* for terms:

| | | | |
|---|---|---|---|
| type | *A* | ::= | *A* Z> *A* |
| term | *M* | ::= | *x\Xx:A.M \M M* |
| value | *V* | ::= | *Xx.A.M* |
| typing context | *T* | ::= | • \| F, x : *A* |

*A* variable *x* with binding *x* : *A* is assumed to hold a term and is not regarded as a value. We use a typing judgment **r** h *M : A* to mean that term *M* has type *A* under typing context *T:*

$$\frac{x.AeT}{T\backslash\text{-}x{:}A}\,{}^{yar}\quad\cdot\cdot\qquad \frac{T,x{:}A\backslash\text{-}M\ :B}{ThXx{:}A.M\ \ :ADB}\,{}_{3I}\ \cdot\qquad \frac{T\backslash\text{-}M{:}ADB\qquad T\ h\ N\ :\ A}{ThMN.B\ \cdot}\,{}_{DL}$$

The /3-reduction rule for the connective D uses a capture-avoiding substitution *[M/x]N* defined in a standard way:

$$(\backslash x{:}A.N)M \quad -\wedge \quad [M/x)N$$

It may be seen as the reduction of a typing derivation in which the introduction rule *D* is followed by the elimination rule DE. The following proposition shows that the reduction is indeed type-preserving:

**Proposition2.1.** *IfT* h *M* : *A andT,x : A* h *N* : *B, then T* h *[M/x]N : B.*

In the context of distributed computations, *x : A* in a typing context T means that variable *x* holds a term of type *A* that is valid at a hypothetical node where typechecking takes place, which we call the *current node* throughout the paper. Then a typing judgment *Th M : A* means that if typing context *T* is satisfied, the evaluation of term *M* at the current node returns a value *V* of type *A.* It does not, however, tell us if *M* is a mobile term that can be evaluated at other nodes. Nor does it tell us if *V* is a mobile value that is valid at other nodes. Therefore the above type system is not expressive enough for the safety of mobile terms and mobile values in distributed computations.

We first develop a modal language An which extends the A-calculus with the modality • to ensure the safety of mobile terms. AQ is based upon the type system for necessity of modal logic by Pfenning and Davies [14]. Next we develop another modal language Ao which extends the A-calculus with the modality O to ensure the safety of mobile values. *XQ* and Ao extend the A-calculus in an orthogonal way: the modality • is concerned with *where we can evaluate a given term* whereas the modality O is concerned with *where we can use the result ofevaluating a given term.* Thus we merge An and Ao to obtain the modal language Ano» which ensures the safety of both mobile terms and mobile values.

## 2.1 $\lambda_\Box$ for term mobility

The idea behind the modality $\Box$ is that if a term $M$ is well-typed under an empty typing context, *i.e.*, $\cdot \vdash M : A$, we can evaluate it at any node. Intuitively $M$ is valid at any node, or *globally valid*, because it does not depend on any local resource. Thus we use $M$ in building a value box $M$ of modal type $\Box A$.

The syntax of $\lambda_\Box$ is as follows:

$$\begin{array}{lll} \text{type} & A & ::= & \cdots \mid \Box A \\ \text{term} & M & ::= & \cdots \mid \mathsf{box}\ M \mid \mathsf{letbox}\ x = M \ \mathsf{in}\ M \\ \text{value} & V & ::= & \cdots \mid \mathsf{box}\ M \end{array}$$

If $M$ evaluates to box $M'$, then letbox $x = M$ in $N$ substitutes $M'$, *without evaluating it*, for $x$ in $N$.

Now a variable $x$ can hold a term that is globally valid (*e.g.*, letbox $x =$ box $M$ in $N$). Accordingly we introduce a *mobile typing context* $\Delta$. $\Gamma$ is now called a *local typing context*.

$$\begin{array}{llll} \text{mobile typing context} & \Delta & ::= & \cdot \mid \Delta, x :: A \\ \text{local typing context} & \Gamma & ::= & \cdot \mid \Gamma, x : A \end{array}$$

$x :: A$ in $\Delta$ means that variable $x$ holds a globally valid term of type $A$; hence a mobile typing context does not affect the mobility of a term being typechecked.

We use a typing judgment $\Delta; \Gamma \vdash M : A$ to mean that under mobile typing context $\Delta$ and local typing context $\Gamma$, term $M$ evaluates to a value of type $A$ valid at the current node.

$$\frac{x :: A \in \Delta \quad \text{or} \quad x : A \in \Gamma}{\Delta; \Gamma \vdash x : A}\ \mathsf{Cvar} \qquad \frac{\Delta; \cdot \vdash M : A}{\Delta; \Gamma \vdash \mathsf{box}\ M : \Box A}\ \Box\mathsf{I} \qquad \frac{\Delta; \Gamma \vdash M : \Box A \quad \Delta, x :: A; \Gamma \vdash N : B}{\Delta; \Gamma \vdash \mathsf{letbox}\ x = M \ \mathsf{in}\ N : B}\ \Box\mathsf{E}$$

The rule Cvar replaces the rule Var. The rule $\Box$I implies that $M$ is globally valid if it is well-typed under an empty local typing context and thus no assumption is made on the current node. Therefore the premise of the rule $\Box$I implicitly uses an arbitrary node as the current node in typechecking term $M$.

The $\beta$-reduction rule for the modality $\Box$ uses a capture-avoiding substitution $[M/x]N$ extended in a standard way:

$$\mathsf{letbox}\ x = \mathsf{box}\ M \ \mathsf{in}\ N \quad \rightarrow_{\beta\Box} \quad [M/x]N$$

As with the connective $\supset$, this $\beta$-reduction rule may be seen as the reduction of a typing derivation in which the introduction rule $\Box$I is followed by the elimination rule $\Box$E. The following proposition shows that the reduction is indeed type-preserving:

**Proposition 2.2.** *If* $\Delta; \cdot \vdash M : A$ *and* $\Delta, x :: A; \Gamma \vdash N : B$, *then* $\Delta; \Gamma \vdash [M/x]N : B$.

## 2.2 $\lambda_\bigcirc$ for value mobility

The typing judgment of the $\lambda$-calculus determines if a term is valid at a given node; if the term is well-typed, it evaluates to a value valid at that node. In contrast, the type system of $\lambda_\bigcirc$ should be able to check if the value to which a term evaluates is valid at a given node. This is a property that cannot be verified by the type system of the $\lambda$-calculus. Therefore we need an additional typing judgment for the type system of $\lambda_\bigcirc$.

As in the type system of $\lambda_\Box$, we split a typing context into two parts. We also introduce a new form of binding $v \sim A$:

$$\begin{array}{llll} \text{mobile typing context} & \Delta & ::= & \cdot \mid \Delta, v \sim A \\ \text{local typing context} & \Gamma & ::= & \cdot \mid \Gamma, x : A \end{array}$$

$v$ is called a *value variable* and holds a value; hence it itself is also regarded as a value. $v \sim A$ in $\Delta$ means that $v$ holds a globally valid value of type $A$.

We use a typing judgment A; *T* h *M* ~ *A* to mean that M evaluates to a globally valid value of type *A.* In order to express that the value is valid at the current node, we use an ordinary typing judgment A ; T h M : A For any language construct producing local resources, we can use only an ordinary typing judgment *(e.g.,* for a memory allocation construct which returns pointers to heap cells).

The following typing rules hold independently of the syntax of Ao:

$$\frac{v\sim AeA}{A ; r h , : i}\ \overset{w}{Vvar} \qquad \frac{A\text{-}_r\backslash\text{-}V{:}A}{A;ThV\sim A}\ Val$$

The rule Vvar says that a value variable in *v* ~ *A* is valid at the current node. The rule Val conforms to the definition of the new typing judgment: the premise of the rule Val checks if *V* is globally valid, in which case the conclusion holds because *V* is already a value.

The syntax of Ao is as follows:

| | | | |
|---|---|---|---|
| type | *A* | ::= | • • • \| *OA* |
| term | *M* | ::= | • • • \| *v* \| cir *M* \| letcir *v* = *M* in *M* |
| value | *V* | ::= | • • • \| *v* \| cir *M* |

cir *M* has a modal type *OA,* where *M* evaluates to a globally valid value, letcir *v* = *M* in *N* expects *M* to evaluate to cir M'; it conceptually finishes the evaluation of $M^1$ before substituting the resultant value for *v* in $N_9$ since *v* holds a value.

cir *M* corresponds to the introduction rule for the modality O. Note that in letcir *v* = *M* in *N,* the type of *M* does not determine the form of the typing judgment for the whole term. That is, regardless of the type of M, there are two possibilities for where the result of evaluating *N* is valid: at the current node and at any node. Therefore each instance of the modality O has one introduction rule and two elimination rules:

$$\frac{A;ThM\sim A}{A;T\ h\ cir\ M : OA}\ \overset{\frown}{wl}' \qquad \frac{A;rhM{:}Oi \quad A,v\sim A;T\backslash\text{-}N{:}B}{A;T\ h\ letcir\ v = M\ in\ N : B}\ \frown$$

$$\frac{\Delta;\Gamma \vdash M : OA \quad \Delta, v \sim A;\Gamma \vdash N \sim B}{A;T\ h\ letcir\ v = M\ in\ N \sim B}\ r\backslash c'_{ut}$$

The /^-reduction rule for the modality O reduces letcir *v* = cir *M* in *N.* In this case, we analyze *M* instead of *N.* The reason is that only a value can be substituted for v, but *M* may not be a value; therefore we analyze *M* to decide how to transform the whole term so that *v* is eventually replaced by a value. ConceptuaUy *N* should be replicated at those places within *M* where the evaluation of *M* is finished, so that *M* and *N* are evaluated exactly once and in that order. If *M* is already a value V, we reduce the whole term into *[V/v]N.* Thus we are led to define a new form of substitution *(M/v)N* which is defined inductively on the structure of *M* instead of $N_9$ and use it in the ^-reduction rule for the modality O:

$$\begin{aligned}(V/v)N &= [V/v]N \\ (\text{letcir } xf = M \text{ in } M^f/v)N &= \text{letcir } v' = M \text{ in } \{M'/v)N\end{aligned}$$

$$\text{letcir } v = \text{cir } M \text{ in } N \longrightarrow_{po} (M/v)N$$

Note that we do not define *(M M'/v)N* because cir *M* $M^f$ cannot be weU-typed: there is no derivation of A; F h *M* $M^f$ ~ *A,* which would require us to refine types of lambda abstractions. In practice, ordinary type *A* D *OB* for *M* suffices in conjunction with letcir *v* = *M M'* in *v* to simulate such a derivation.

As with the connective D, the /3-reduction rule may be seen as the reduction of a typing derivation in which the introduction rule Ol is foUowed by the elimination rule OE. The foUowing proposition shows that the reduction is indeed type-preserving:

**Proposition 23.**

*!fA;r\-M~AandA,v~A,rhN:C,thenA;r\-(M/v)N:C.*
*IfA;T h M ~ AandA,v ~ A;r \- N ~ C, then A;r h (M/v)N ~ C.*

*Proof.* By induction on the structure of M (not *N).* □

## 23 Ano **for term mobility and value mobility**

λ□○ is a modal language which incorporates both AQ and Ao. Since AQ and Ao are orthogonal extensions of the A-calculus, all their individual properties continue to hold in AQO.

We decide to allow letbox $x = M$ in $N$ in the typing judgment for value mobility. The decision is based upon the observation that a substitution of a mobile term for $x$ does not prevent $N$ from evaluating to a mobile value. For example, $x$ may not appear in $N$ at all. Therefore we introduce a new elimination rule for the modality • as follows:

$$\frac{A;T\backslash\text{-}M:\backslash 3A \qquad A,x::\ A;T\ h\ N \sim B}{A;\ r\ h\ \text{letbox}\ x = M\ \text{in}\ N \sim B}\ f$$

Since cir letbox $x = M$ in M' can now be well-typed, we define (letbox $x = M$ in *M'/v)N:*

$$(\backslash etboxx = M'mM'/v)N \quad = \quad \text{letbox}x = M \text{ in } (M'/v)N$$

An easy induction shows that Proposition 2.3 continues to hold. The following proposition shows that the /^-reduction rule for the modality • continues to be type-preserving:

**Proposition** 2.4. *If* A; - *h M : Aand A,x : A;T \- N ^ $B_f$ then A;T h [M/x]N ~ B.*

### 2.4 Primitive types

A primitive type is one for which value mobility is an inherent property. For example, a boolean value, of type bool, is atomic and does not contain references to local resources. Therefore boolean values are always globally valid and A; *T* h *M :* bool semantically implies A ; T h M ~ bool. Under the above type system, however, value mobility for primitive types should be expressed explicitly by programmers.

As an example, consider a primitive type nat for natural numbers:

| | | | |
|---|---|---|---|
| type | *A* | ::= | • • • \| nat |
| term | *M* | ::= | • • • \| zero \| succ *M* |
| value | *V* | ::= | • • • \| zero \| succ *V* |

We use the following construct for primitive recursion over nat:

$$\text{term} \quad M \quad ::= \quad \cdots \mid \text{rec } M \text{ of } /(\text{zero}) \Rightarrow M \,/\, /(\text{succ } x) \Rightarrow M$$

$$\frac{\begin{array}{l}A;ThM:nat\\ A;n\text{-}M_0:\wedge\\ A;T,x:\text{nat}, f(x):A\backslash\text{-}Mi:A\end{array}}{\begin{array}{l}A;\ r\ h\ \text{rec}\ M\ \text{of}\ /(\text{zero}) \Rightarrow M_o \quad :A\\ \qquad I\ /(\text{succ}\ x) \Rightarrow Mi\end{array}}\ \textbf{Rec} \qquad \frac{\begin{array}{l}A;ThM:nat\\ A;rhM_0\text{-}A\\ A, f(x) \sim A;T,x:\text{nat}\ h\ Mi \sim A\end{array}}{\begin{array}{l}A;\ T\ h\ \text{rec}\ M\ \text{of}\ /(\text{zero}) \Rightarrow M_o \quad \sim A\\ \qquad /\ /(\text{succ}\ x) \Rightarrow Mi\end{array}}\ \textbf{Rec}'$$

Now, for any term M such that A ; F h M : nat, we explictly express its value mobility with the following term M~, which evaluates to the same value as M and also satisfies A; *T* h *M~* ~ nat:

**M~ = rec M of /(zero) => zero / /(succ x) =^ letcir i; = cir *f(x)* in succ *v***

$$
\begin{array}{llll}
\text{type} & A & ::= & A \supset A \mid \Box A \mid \bigcirc A \\
\text{term} & M & ::= & x \mid \lambda x{:}A.\,M \mid M\;M \mid \mathsf{box}\;M \mid \mathsf{letbox}\;x = M\;\mathsf{in}\;M \mid \\
 & & & v \mid \mathsf{cir}\;M \mid \mathsf{letcir}\;v = M\;\mathsf{in}\;M \\
\text{value} & V & ::= & \lambda x{:}A.\,M \mid \mathsf{box}\;M \mid v \mid \mathsf{cir}\;M
\end{array}
$$

$$
\frac{x :: A \in \Delta \quad \text{or} \quad x : A \in \Gamma}{\Delta;\Gamma \vdash x : A}\;\mathsf{Cvar}
\qquad
\frac{v \sim A \in \Delta}{\Delta;\Gamma \vdash v : A}\;\mathsf{Vvar}
\qquad
\frac{\Delta;\cdot \vdash V : A}{\Delta;\Gamma \vdash V \sim A}\;\mathsf{Val}
$$

$$
\frac{\Delta;\Gamma, x : A \vdash M : B}{\Delta;\Gamma \vdash \lambda x{:}A.\,M : A \supset B}\;{\supset}\mathsf{I}
\qquad
\frac{\Delta;\Gamma \vdash M : A \supset B \quad \Delta;\Gamma \vdash N : A}{\Delta;\Gamma \vdash M\;N : B}\;{\supset}\mathsf{E}
$$

$$
\frac{\Delta;\cdot \vdash M : A}{\Delta;\Gamma \vdash \mathsf{box}\;M : \Box A}\;\Box\mathsf{I}
\qquad
\frac{\Delta;\Gamma \vdash M : \Box A \quad \Delta, x :: A;\Gamma \vdash N : B}{\Delta;\Gamma \vdash \mathsf{letbox}\;x = M\;\mathsf{in}\;N : B}\;\Box\mathsf{E}
$$

$$
\frac{\Delta;\Gamma \vdash M : \Box A \quad \Delta, x :: A;\Gamma \vdash N \sim B}{\Delta;\Gamma \vdash \mathsf{letbox}\;x = M\;\mathsf{in}\;N \sim B}\;\Box\mathsf{E}'
$$

$$
\frac{\Delta;\Gamma \vdash M \sim A}{\Delta;\Gamma \vdash \mathsf{cir}\;M : \bigcirc A}\;\bigcirc\mathsf{I}
\qquad
\frac{\Delta;\Gamma \vdash M : \bigcirc A \quad \Delta, v \sim A;\Gamma \vdash N : B}{\Delta;\Gamma \vdash \mathsf{letcir}\;v = M\;\mathsf{in}\;N : B}\;\bigcirc\mathsf{E}
$$

$$
\frac{\Delta;\Gamma \vdash M : \bigcirc A \quad \Delta, v \sim A;\Gamma \vdash N \sim B}{\Delta;\Gamma \vdash \mathsf{letcir}\;v = M\;\mathsf{in}\;N \sim B}\;\bigcirc\mathsf{E}'
$$

$$
\frac{\Delta;\Gamma \vdash M : A_{prim}}{\Delta;\Gamma \vdash M \sim A_{prim}}\;\mathsf{Prim}{\sim}
$$

**Figure 1:** Syntax and type system of $\lambda_{\Box\bigcirc}$.

We choose to take advantage of the fact that every term $M$ of a primitive type can be converted into an equivalent term $M^{\sim}$ with value mobility as illustrated above, and introduce the following typing rule in which value mobility for primitive types is built-in:

$$
\frac{\Delta;\Gamma \vdash M : A_{prim}}{\Delta;\Gamma \vdash M \sim A_{prim}}\;\mathsf{Prim}{\sim}
$$

Here $A_{prim}$ is a primitive type ($A \supset A$, $\Box A$, and $\bigcirc A$ cannot be a primitive type). With the rule Prim$\sim$ in the type system, we can easily express value mobility for primitive types.

The price we pay for the rule Prim$\sim$ is that $\beta$-reduction $\rightarrow_{\beta\bigcirc}$ is no longer valid: $\mathsf{letcir}\;v = \mathsf{cir}\;M\;\mathsf{in}\;N$ may typecheck while $\langle M/v\rangle N$ is not defined. For example, $M = M_1\;M_2$ of type nat satisfies $\Delta;\Gamma \vdash M \sim \mathsf{nat}$ by the rule Prim$\sim$, but $\langle M_1\;M_2/v\rangle N$ is not defined. Intuitively the rule Prim$\sim$ disguises an unanalyzable term of a primitive type as an analyzable term.

A quick fix is to reduce $\mathsf{letcir}\;v = \mathsf{cir}\;M\;\mathsf{in}\;N$ only if $M$ is already a value $V$:

$$
\mathsf{letcir}\;v = \mathsf{cir}\;V\;\mathsf{in}\;N \quad \rightarrow_{\beta\bigcirc} \quad [V/v]N \qquad\qquad (\rightarrow_{\beta\bigcirc}\text{ redefined})
$$

Note that we write $[V/v]N$ for $\langle V/v\rangle N$. Thus, in order to reduce $\mathsf{letcir}\;v = \mathsf{cir}\;M\;\mathsf{in}\;N$, we are forced to reduce $M$ into a value first, instead of analyzing $M$ to transform the whole term. Such a reduction strategy is reflected in the operational semantics, as we will see in Section 4.

Now we have introduced all typing rules of $\lambda_{\Box\bigcirc}$ (See Figure 1.) All the previous propositions, except Proposition 2.3, continue to hold for the type system of $\lambda_{\Box\bigcirc}$. The following proposition proves that $\Delta;\Gamma \vdash M \sim A$ is stronger than $\Delta;\Gamma \vdash M : A$:

**Proposition 2.5.** *The following typing rule is admissible:*

$$
\frac{\Delta;\Gamma \vdash M \sim A}{\Delta;\Gamma \vdash M : A}\;{\sim}{:}
$$

*Proof.* By induction on the structure of A; *V* \- *M* ~ A •

## 2.5 Example

To express term mobility and value mobility for each new construct M, we provide a rule for ordinary typing judgment *A;T h M : A* and optionally another rule for typing judgment A ; T h M ~ A As an example, consider constructs for memory allocation. We regard a heap cell as a local resource; hence its pointer is assumed to be valid only at the node where it is allocated. We use type ptr *A* for pointers to heap cells containing values of type *A*. For the sake of brevity, we do not consider typing rules for pointers.

| | | | |
|---|---|---|---|
| type | *A* | ::= | *ptr A* |
| term | *M* | ::= | new *M* \| read *M* \| write *M M* |

The three constructs work as follows:

- If *M* evaluates to a value *V*, then new *M* allocates a new heap cell containing *V* and returns its pointer ***L***
- If *M* evaluates to a pointer /, then read *M* returns the contents of the heap cell pointed to by Z.
- If *M* evaluates to a pointer *I* and *N* evaluates to a value *V*, then write *M N* writes *V* to the heap cell pointed to by *I* and returns *V*.

The rules for the ordinary typing judgment reflect how these three constructs work:

$$\frac{A;T\backslash\text{-}M:A}{A;r\,h\,new\,M:ptr\wedge}\ \text{New} \qquad \frac{A;rhM:ptr,4}{A;T\,h\,read\,M:A}\ \text{Read} \qquad \frac{A,T\backslash\text{-}M:ptrA \quad A;T\backslash\sim N:A}{A;T\,h\,write\,M\,N:A}\ \text{Write}$$

Thus any of these constructs is mobile if its argument is globally valid. For example, box new *M* (of type • ptr *A)* typechecks if *M* is globally valid, which means that allocating a new heap cell itself can be done at any node. Once we finish evaluating new M, however, the result is no longer mobile (because it is a pointer), which implies that the following rule is not allowed:

$$\frac{\cdots}{A;T\,h\,new\,M\sim ptr\,A}\ (wrong)$$

Since the value contained in a heap cell is not necessarily globally valid, we do not allow the following rule:

$$\frac{\cdots}{A;T\,h\,read\,M\sim A}\ (wrong)$$

The following rule is safe to use because write *M N* returns the value to which *N* evaluates:

$$\frac{A;ThM:ptrA \quad A;T\ h\ N - A}{A;\ T\ h\ write\ M\ N\ \sim\ A}\ \text{Write'}$$

As an example involving primitive types, let us build a mobile term adding two natural numbers. The following term does not typecheck because variables *x* and *y* are not added to the mobile typing context:

$$Xx{:}\text{nat}.Xy{:}\text{nat}.\text{box}(x+y)$$

We can make it typecheck by converting *x* and *y* into value variables $v_x$ and $v_y$ (using the rule Prim~):

$$\begin{aligned} Xx{:}\ \text{nat}.\ Xy{:}\ \text{nat}.\ \ & \text{letcir}\ v_x = \text{cir}\ x\ \text{in} \\ & \text{letcir}\ v_y = \text{cir}\ y\ \text{in} \\ & \text{box}\ (v_x + v_y) \end{aligned}$$

The foUowing term copies mobiles terms contained in variables $x$ and $y$, and the evaluation of the resultant mobile term may take longer than adding two natural numbers:

$$\text{Ax: Dnat. } Xy\text{: Dnat. letbox } x' = x \text{ in}$$
$$\text{letbox } y^f = y \text{ in}$$
$$\text{box } (x' + y')$$

The following term first finishes evaluating mobile terms contained in variables $x$ and $y$:

$$Xx\text{: Dnat. } Xy\text{: Dnat. letbox } x^1 = x \text{ in letcir } v_x = \text{cir } x^1 \text{ in}$$
$$\text{letbox } y^1 \text{ — } y \text{ in letcir } v_y = \text{cir } 2/ \text{ in}$$
$$\text{box } (v_x + v_y)$$

## 2.6 Logic for AQO

Modal types *DA* in A^o use the same type system for necessity of modal logic of Davies and Pfenning [6, 14]. A minor difference is that our interpretation of the modality • is spatial (CM means that *A* is true at every node), whereas their interpretation is temporal or proof-theoretic.

The type system for modal types *OA* is unusual in that it differentiates values *(i.e.,* terms in weak head normal form) from ordinary terms, as shown in the rule Val. This differentiation implies that the logic corresponding to the modality O requires a judgment that inspects not only hypotheses in a proof but also inferences rules in it. Thus the modality O sets itself apart from other modalities and is not found in any other logic.

A substitution *(M/v)N* for the modality O is similar to (and was inspired by) those substitutions for modal possibility and lax truth in [14] in that it is defined inductively on the structure of the term being substituted *(i.e., M)* instead of the term being substituted into *(i.e., N).* In fact, we may even think of *(M/v)N* as substituting *N* into *M* because conceptually *N* is replicated at those places within *M* where the evaluation of *M* is finished.

We close this section with a discussion of the properties of the modalities • and O. Note that the two modalities interact with each other, although they are developed in an orthogonal way.

- *DA D A* — *Xx:DA.* letbox $y = x$ in $y$
  *A* mobile term is a special case of an ordinary term.
- *DA* D DD^4 — *Xx: DA.* letbox $y = x$ in box box $y$
  *A* mobile term itself is mobile.
- *D(A DB)DDADDB* — *XX:D(A* D *B). Xy: DA.* letbox $x^f = x\backslash x\backslash$ letbox $y^1 = y\backslash n$ boxx'y'
- *OA D A* — *Xx:OA.* letcir $v = x$ in $v$
  *A* mobile value is a special case of an ordinary term.
- *OA* D OCL4 — Ax: *OA.* letcir $v = x$ in cir cir $v$
  *A* mobile value itself is mobile.
- *OADDA* — *XX:OA.* letcir $v = x$ in box $v$
  *A* mobile value is a special case of a mobile term.
- *DA* D *ODA* — *Xx: DA.* letbox $y = x$ in cir box $y$
  box *M* is a mobile value.

- *OA* D *DOA* \x:OA. letcir *v* = *x* in box cir *v*
  cir *V* is a mobile term.

- □O*A* D D i Ax: DOA letbox *y* = *x* in box letcir t> = x/ in *v*
  (derivable from *DOA* D *OA* D *DA)*

- CO.4 2 O*A*
  If OQA D *OA* held, DA and O-A would be equivalent because of *OA D DA* and *DA D ODA D OA*.

## 3 Modal language $A_D o^{u'}$ with indexed modalities

In the definition of Ano, "mobile" is synonymous with "globally valid": a mobile term or value is valid at any node in the network. Such a model for distributed computation is adequate if all participating nodes are assumed to be homogeneous and have the same permanent local resources. In a grid computing environment, for example, a mobile term valid at a particular remote node is also globally valid and can be evaluated at any other remote node. For a heterogenous group of nodes with different permanent local resources, however, AQO becomes inadequate because a mobile term or value is not always globally valid. For example, a client node may transmit to a printer server a "mobile" term for printing a document; such a mobile term can be evaluated only at printer servers and is not globally valid. Since this notion of restricted mobility is useful in practice, we extend AQO to allow terms and values valid only at specific nodes.

The main design issue is whether or not the type system specifies a node at which a mobile term or value is valid. As an example, consider a mobile term *M* that is valid only at printer servers *(e.g.,* for printing a document). There are two approaches to expressing its mobility with a type. In one approach, the type system does not specify the node at which *M* is to be evaluated; instead it only indicates that there exists a certain node at which *M* can be evaluated. In this case, it is the linker or the runtime system that decides where to evaluate such a mobile term. In the other approach, the type system specifies explicitly the node at which *M* is to be evaluated. In this case, it is the type system that decides where to evaluate such a mobile term.

The first approach is attractive because the type system abstracts from any particular network configuration. For example, new printer servers can be deployed into the network and old printer servers can be removed without changing the type system. The second approach is useful if the network configuration is static. For example, if the set of available printer servers is published and never changes, programmers can specify a printer server with an appropriate type involving its identifier. In this paper, we adopt the second approach to extend Ano and leave it as future work to apply the first approach.

We extend Ago with two indexed modalities D^ and O^ with the following interpretation:

- A value box^ *M* of indexed modal type *D^A* contains term *M* which is valid at node *u*>.

- A value cir^ *M* of indexed modal type *O^A* contains term *M* which evaluates to a value valid at node u/.

Since the type system of Ano is incapable of expressing properties of a term with respect to specific nodes, we replace the typing judgments of Ano by a new form of typing judgment A; *T* h^ *M* ~ *A* @ u/:

- A; T h^ *M* ~ *A* @ u/ means that under mobile typing context A and local typing context I\ term *M* at node *u*> evaluates to a value of type *A* valid at node u/.

- A; T K; *M : A* is a shorthand for A; *T* h^ *M* ~ *A* @ u;, where *u)* may be thought of as the current node for typechecking *M.* Note that it is *not* a separate judgment.

A mobile typing context A is defined as before, but a local typing context *T* now contains only those binding relativized to a specific node:

mobile typing context  A  ::=  • | A, *x* :: *A* | A, *v* ~ *A*
local typing context  *T*  *::=*  *-\T,x:A@u;\T,v^A@u;*

- *x* :: *A* in A means that *x* holds a globally valid term of type *A*.
- *v* ~ *A* in A means that v holds a globally valid value of type *A*.
- *x : A @ UJ* in *T* means that *x* holds a term valid at node a;.
- t; ~ A @ a; in F means that v holds a value valid at node *u*.

Note that the use of typing judgment A; *T* h^ *M* ~ A @ u/ implies that a term may evaluate to a value that is *not* valid at the node at which it is evaluated. For example, a term may scan a list of handles for remote files and select one; the evaluation is safe as long as the selected handle is not dereferenced. We refer to our new modal language with indexed modalities as AQO^.

The syntax of Ano^ is as follows:

type  *A*  ::=  *A* D *A \ DA \ $U_U$A \ OA \ O^A*
term  *M*  *::=*  *x\ XxiA.M \ M M * box *M* | box^ *M* | letbox *x* = *M* in *M* |
*v* | cir *M* | cir^ *M* | letcir *v* = *M* in *M*
value  *V*  *::=*  *XxiA.M* | box *M* | box^ *M \ v* | cir *M * cir^ *M*

For the sake of simplicity, we reuse letbox *x* = *M* in *N* and letcir *v* = *M* in iV to expose terms inside $box_\omega$ $M^f$ and cir^ $M^f$ (as well as box $M^f$ and cir M'). Thus both letbox *x* = box $M^f$ in JV and letbox *x* = $box_\omega$ M' in *N* substitute $M^1$ for *x* in AT; similarly both letcir v = cir M' in *N* and letcir v = cir^ $M^f$ in AT first reduce M' to a value, which is then substituted for *v* in *N*.

Figure 2 shows the typing rules of *XQCF'*• All these typing rules look similar to those of AQO, except that we explicitly annotate every typing judgment with a node at which the evaluation is to take place and another node at which its end result is valid. For each form *V* of value, we provide a typing rule for the judgment A; *T* h^ *V : A* only; in order to decide where else *V* is valid, we use the rule Val^. Note that in the rule Dlvr, the local typing context *T* of the conclusion is carried over to the premise (whereas in the rule Dl of Ano» it is replaced by an empty local typing context). This is safe because an arbitrary node a/ (instantiated by *fresh* u/) serves as the current node in the premise.

The rules Cvarvr and Vvar^ prevent references to local resources from being dereferenced at remote nodes. Suppose *x : A@ u;eT₉v^A@u;eT*, and u/ ^ *w*. In order to "evaluate" the term in *x* (which perhaps contains references to local resources belonging to *UJ)* at *u;* we should be able to derive A; T h^/ *x ~ A @ u"* for a certain node *u"*, which is impossible because of the rule Cvarvr; in order to "use" the value in *v* (which is perhaps a reference to a local resource belonging to a;) at u/, we should be able to derive A; *V* h^/ *v* : *A*, which is impossible because of the rule Vvar^y. Note, however, that we can derive *A-.Th^ v ^ A@ u;*, which implies that a reference to a local resource may be present at remote nodes as long as it is not dereferenced.

As value mobility for primitive types is built-in in the rule Prim~vr, we reduce letcir *v* = cir *M* in *N* and letcir *v* = cir^ *M* in *N* only if *M* is already a value, as in Ano. Thus all /3-reduction rules are defined in terms of an ordinary substitution *[M/x]N* or *[V/v]N:*

| | | |
|---|---|---|
| *(Xx :A.N)M* | —£3 | *[M/x]N* |
| letbox *x* = box *M* in *N* | *->pn* | *[M/x]N* |
| letbox *x* = box^ *M* in *N* | *-*pQr* | *[M/x]N* |
| letcir *v* = cir *V* in *N* | *->$p_o$* | *[V/v]N* |
| letcir *v* = cir^ *V* in *N* | *->$_{0O,}$* | *[V/v]N* |

$$\frac{xr.AeA \quad \text{or} \quad x:A@u>\epsilon.r}{A;T\vdash_u x:A} \; {}^r L_{\wedge}^{var}w \qquad \frac{v\sim Ae\_A \quad \text{or} \quad v \sim A@u>\epsilon F}{A'.Th\wedge viA} \; \text{Vvar}_W$$

$$\frac{\Delta;\Gamma\vdash_{\omega'} V : A}{\Delta;\Gamma\vdash_{\omega} V \sim A @ \omega'} \; \text{Valjy} \; (w \wedge \ast)$$

A; T, $x : A @ u$ h^ $M : B$ . A; $T$ h^ M : $A$ $D$ $B$ $A'.Th\wedge N :A$

$$\frac{fresh\ J \quad A;T \vdash_{u>} M : A}{\Delta;\Gamma\vdash_{\omega} \text{box}\ M : \Box A} \qquad \text{A j f ^ M } :UA \quad A,x :: \text{A;T h^, JV} \sim \text{J3 @ t«/}$$

$$\frac{\Delta;\Gamma\vdash_{\omega'} M : A}{\Delta;\Gamma\vdash_{\omega} \text{box}_{\omega'}\ M : \Box_{\omega'} A} \; \Box I_W \qquad \frac{A;ri\text{-}_M Af:EUA \quad A;T,x : >1 @ J'\ h_M\ JV \sim B @ \omega'}{\text{A; T h^ letbox } x = M \text{ in AT} \sim B @ a/} \; \Box E'_W$$

$$\frac{fresh\ \omega' \quad \Delta;\Gamma\vdash_{\omega} M \sim A @ \omega'}{A;n\text{-}_w drAf \ :O>1} \; \bigcirc I_W \qquad \frac{A;rh_w Af;Oi4 \quad A,t; \sim A;T \vdash_{»} N \sim B @ J}{\text{A; T h^ letcir v} = M \text{ in JV} \sim B @ w'} \; \bigcirc E_{\wedge}$$

$$\frac{\Delta;\Gamma\vdash_{\omega} M \sim A @ fa/ \; , \quad A;T h_w M\ O @_W A \quad A;T,v \sim A @ u'; \vdash_{»} N \approx B @ u'}{A;T\vdash_{\omega} dr_u>M:O_u>A^{\circ\wedge w}\circ\wedge w \qquad \text{A;T h letcir v} = M \text{ in JV} \sim B @ a/} \; \bigcirc E'_{\wedge}$$

$$\frac{\Delta;\Gamma\vdash_{\omega} M : A_{prim}}{\Delta;\Gamma\vdash_{\omega} M \sim A_{prim} @ \omega'} \; \text{Prim}\sim_W (\omega \neq \omega')$$

**Figure 2:** Typing rules of AQO$^{U'}$•

**The following propositions imply that all these /3-reductions are type-preserving:**

**Proposition3.1.** **//A;T h^** ***M : AandA;T$_y$x : A@u>"' h^ N - B @*** **c*/$_f$ f/^n A;T h^ [M/x]JV -** ***B @ J.***

**Proposition 3.2. 7/A;T K// Af :** ***Afar any node CJ" and A, x :: A^Thu N ~ B @ d, thenA.Th^ [M/x]N ~B@v'.***

**Proposition33. //A$_;$rh^ V : ,4a/w/A;I> -** ***A @ J'*** **h^ JV -** ***B @*** **u;[7], r/ien A;T h^ [V/v]iV - S Q a/.**

**Proposition 3.4.** ***IfA;T*** **h^ F :** ***Afar any node u" and A, v ~ A^rhu N ~ B @ u;', thenA^TY-^ [V/v]N ~B@v'.***

## 3.1 AQO^ as an extension of AQO

**Since all the /^-reduction rules of AQO arc included in Ano^, any reduction sequence in AQO is also valid in AQO^. All the typing rules of AQO can also be rewritten in terms of typing judgments in AQO^• Intuitively A;T h^** ***M ~ A @ J*** **is more expressive than A;*T* h *M* : *A* and *A;T\-* *M* ~ *A* because u> and *J* can be instantated into arbitrary nodes. Given a local typing context *T* in Ano, we write *[T]$^u$* for a local typing context in Ano^ that attaches @ *w* to every binding *x* : *A* in F:**

$$[T]'' \quad = \quad \{x:A@u>\backslash x:A\in T\}$$

**The following proposition shows how to interpret typing judgments in AQO in terms of those in $\lambda_{\Box\bigcirc}{}^{W}$:**

**Proposition 3.5.**

***IfA;*** **r h** ***M : A then*** **A; [T]" h^ M :** ***Afar any node w.***

***If*** **A; T h M ~ A f/ien A; [TJ^ h^ M ~ A @ u//^ any norfe5 c^ a/u/** ***J.***

## 3.2 Logic for $\lambda_{\Box\bigcirc}^{w}$

As every typing judgment in And*' is relative to a certain node, the logic for AQO^ requires judgments relativized to nodes. For example, *x : A @ w* in a local typing context corresponds to a judgment that *A* is true at node *v.* Since the indexed modalities D^ and Oa; directly internalize nodes within propositions, the logic for AncT is a restricted form of hybrid logic [2].

The notion of judgment relativized to nodes is also a suitable basis for the semantics of modal logic. For example, Simpson [15] provides a natural deduction system for intuitionistic modal logic based upon relative truth. The fragment of Ano$^{w>}$ without the indexed modalities can be explained in a similar way, with the assumption that all nodes are visible (or accessible) from each other. This assumption is justified because in a distribution computation, all nodes can communicate with each other.

The type system presented in this section is appropriate for understanding the roles of the modalities • and O and the indexed modalities *D^* and O^. It is not, however, expressive enough for distributed computations in which communication constructs may generate terms whose type is determined by *remote nodes.* For example, a synchronization variable produced by a future construct (to be explained in the next section) is essentially a pointer to a remote node, which determines its type. In the next section, we extend the type system of AQO^ SO that we can typecheck such terms, and also develop a network operational semantics which is capable of modeling distributed computations.

# 4 $A_D o^{u'}$ for distributed computation

In this section, we develop an extended type system and a network operational semantics for AQO$^{w}$. We demonstrate the use of modal types with three communication constructs: remote evaluation, futures, and asynchronous channels. We prove the type safety of the network operational semantics, *Le.*$_9$ its type preservation and progress properties, in the presence of these communication constructs. The type safety implies the safety of mobile terms and mobile values.

## 4.1 Physical nodes and logical nodes

So far, we have restricted ourselves to physical nodes by interpreting u; as an identifier of a physical node. For example, *u* may refer to a printer server or a database server. While appropriate for the type system, this interpretation poses a problem when we model distributed computations. For example, if a database server initiates a stand-alone computation for each query it receives, we cannot distinguish between these stand-alone computations with different node identifiers. Therefore there arises a need for *logical nodes*, each of which performs a single stand-alone computation. In order for a physical node to perform multiple stand-alone computations concurrently, it spawns the same number of logical nodes.

We distinguish between physical nodes and logical nodes as separate syntactic categories:

physical node *LJ*
logical node 7

A logical node on physical node *u;* inherits all permanent local resources belonging to *UJ.* Therefore a term valid at physical node *u;* is valid at every logical node on a;.

We assume two primitives, *new* 7 and *new* 7 @ a;, for creating logical nodes. *V(y)* stands for the physical node with which logical node 7 is associated, as defined below. Note that it is not defined as the actual physical node where logical node 7 resides:

- *new* 7 creates a new logical node 7 which may reside at an arbitrary physical node (including the physical node invoking *new* 7 itself). If 7 is created with *new* 7, then ^(7) is a fresh physical node

$\omega$ (which is different from any existing physical node).
Example: *new* $\gamma$ searches for an idle computer in the network and establishes a logical node $\gamma$ on it.

- *new* $\gamma$ @ $\omega$ creates a new logical node $\gamma$ at physical node $\omega$. If $\gamma$ is created with *new* $\gamma$ @ $\omega$, then $\mathcal{P}(\gamma) = \omega$.
Example: *new* $\gamma$ @ $\omega$ contacts a database server $\omega$ and requests a logical node $\gamma$ on it.

We assume that every physical node $\omega$ publishes a local typing context $\Gamma_\omega^{\mathsf{perm}}$ which records the type of its permanent local resources with bindings $v \sim A$ @ $\omega$, where $v$ may be thought of as a reference to a permanent local resource. We require that $A$ not be a primitive type (to ensure the progress property in Theorem 4.5). We write $\Gamma^{\mathsf{perm}}$ for the union of all known local typing contexts $\Gamma_\omega^{\mathsf{perm}}$.

## 4.2 Configuration

We represent the state of a network with a *configuration* $C$ which records the term being evaluated at each logical node. A *configuration type* $\Lambda$ records the type of the term and the mobility of the resultant value. We assume that no logical node appears more than once in $C$ and consider $C$ as an unordered set.

$$
\begin{array}{llcl}
\text{configuration} & C & ::= & \cdot \mid C, M \ \mathbf{at}\ \gamma \\
\text{configuration type} & \Lambda & ::= & \cdot \mid \Lambda, \gamma \sim A \ @\ \omega \mid \Lambda, \gamma \sim A \ @\ \star
\end{array}
$$

- $M$ **at** $\gamma$ in $C$ means that logical node $\gamma$ is currently evaluating term $M$.
- $\gamma \sim A$ @ $\omega$ in $\Lambda$ means that the term at logical node $\gamma$ evaluates to a value of type $A$ valid at physical node $\omega$.
- $\gamma \sim A$ @ $\star$ in $\Lambda$ means that the term at logical node $\gamma$ evaluates to a globally valid value of type $A$.

The extended type system is formulated with a *configuration typing judgment* $C :: \Lambda$, which means that configuration $C$ has configuration type $\Lambda$. The network operational semantics is formulated with a *configuration transition judgment* $C \Longrightarrow C'$, which means that configuration $C$ reduces or evolves to configuration $C'$. We first consider the extended type system and then the network operational semantics.

## 4.3 Extended type system

In order to be able to typecheck those terms whose type is determined by remote nodes, we introduce an *extended typing judgment* which includes a configuration type as part of its typing context:

- An extended typing judgment $\Lambda; \Delta; \Gamma \vdash_\omega M \sim A$ @ $\omega'$ means that under configuration type $\Lambda$, mobile typing context $\Delta$, and local typing context $\Gamma$, term $M$ at any logical node on physical node $\omega$ evaluates to a value of type $A$ valid at physical node $\omega'$. We assume $\Gamma^{\mathsf{perm}} \subset \Gamma$, which means that all references to permanent local resources are public.
- $\Lambda; \Delta; \Gamma \vdash_\omega M : A$ is a shorthand for $\Lambda; \Delta; \Gamma \vdash_\omega M \sim A$ @ $\omega$.

The rules for extended typing judgments are derived from (and given the same name as) those in Figure 2 by prepending a configuration type $\Lambda$ to every judgment $\Delta; \Gamma \vdash_\omega M \sim A$ @ $\omega'$.

The configuration typing judgment is defined in terms of extended typing judgments. It has only one inference rule, which may be regarded as its definition:

$$\frac{\begin{array}{l} \textit{for each } \text{M at 7 G C,} \\ \quad 7 \sim A\ @\ UJ \in \text{A} \textit{ and } \text{A; •; r**}^{1\text{TM}}\ \text{h}_{p(7)}\ M \sim A\ @\ \text{a;}, \textit{ or} \\ \quad 7 \sim A\ @ \bullet \text{G A and A; •; T}^{\wedge 1\text{TM}}\ \text{hp}_{(7)}\ \text{M} \sim A\ @\ u) \textit{ for a fresh node } u>. \end{array}}{C :: \Lambda}\ \textsf{Tcfg}$$

We assume \C\ = |A| to maintain a one-to-one correspondence between *C* and A; hence A contains exactly one element for each logical node in *C.*

## 4.4 Network operational semantics

The configuration transition judgment uses evaluation contexts in a call-by-name style; we could equally choose a call-by-value style with another case (Ax: *A. M) K* for evaluation contexts:

evaluation context *K* ::= \\ \ *K M* | letbox *x* = *K* in *M* \
letcir *v* = *K* in *M* \ letcir *v* = cir *K* in *M* \ letcir *v* = cir^ *K* in *M*

An evaluation context *K* is a term with a hole \\ in it, where the hole indicates the position where a reduction may occur. The following rule shows how to use the /^-reduction rules of Ano^ in the network operational semantics; —• refers to the one of the /3-reduction rules —>#> —•#> —*/O> ~>/?o> ~*&o$^f$ **of** $\lambda_{\Box\bigcirc}{}^{W}$**:**

$$\frac{M \longrightarrow N}{C, K[M] \text{ at } 7 \Rightarrow C, K[N] \text{ at } 7}\ \text{R}_{cfg}$$

Note that a configuration transition is nondeterministic, since the rule Rcfg can choose an arbitrary logical node 7 from a given configuration.

We also need another configuration transition rule to deal with value variables in r^"". Suppose that a value variable *v* is a reference to a permanent local resource *V* of a physical node *u*> (hence *v* ~ *A* @ *u** *e* $\Gamma^{\text{perm}}$^. p$_{\text{or exam}}$pi$_e$^ *y* $_{\text{CO}}$uld be a printing function at a printer server *u.* At a logical node 7 such that $\mathcal{P}(\gamma) \neq$ *u*>, *v* does not need to reduce to *V* because *V* is not valid at 7 anyway. If *V(y)* = *u*>, however, *v* reduces to *V* by accessing the local resource. Thus, for each binding *v* ~ *A* @ *u;* G r^$^{1\text{TM}}$, we define a reduction

$$v \rightarrow_{\text{perm}} V$$

such that *V* is not another value variable and •; •; r$^{\text{perm}}$ h^ *V : A* holds. The following rule specifies that a reference to a permanent local resource reduces to a value only at the node to which it belongs:

$$\frac{v \sim A\ @\ \omega \in \Gamma^{\text{perm}} \quad v \rightarrow_{\text{perm}} V \quad \mathcal{P}(\gamma) = \omega}{\text{C}, K[V] \text{ at } 7 \Rightarrow \text{C}, K[V] \text{ at } 7}\ \textsf{Rvalvar}$$

Thus the rule Rvalvar ensures that references to permanent local resources are never dereferenced at remote nodes.

## 4.5 Communication constructs

The network operational semantics becomes interesting only with communication constructs; without communication constructs, all logical nodes perform stand-alone computations independently of each other and the type safety holds trivially. Below we give three examples of communication constructs. Each construct is defined with extended typing rules and configuration transition rules.

type $A$ ::= ••• | unit
term $M$ ::= ••• | () | eval $M$
value $V$ ::= ... | ()
evaluation context $K$ ::= ••• | eval $K$

A; A; T h^ () : unit T() — A; A;T h^ M : DA / A; A; T h^ eval M : unit Teval — A; A;T h^ M : D^A / A; A; T h^ eval M : unit Teval®

nett; 7' / C, ^[eval box M] at 7 => C,«[()] at 7, M at $\gamma'$ Reval

new $7^7$ @ a;' / C, ^[eval box^/ M] at 7 ==• C,«[()] at 7, M at $\gamma'$ Reval®

**Figure** 3: Definition of the remote evaluation construct.

### 4.5.1 Remote evaluation

In order to be able to evaluate a mobile term at a remote node, we introduce a remote evaluation construct eval $M$. It expects $M$ to evaluate to box $N$ or boxa, $N$ and transmits $N$ to a remote node. Unlike a remote procedure call, it does not expect the result of evaluating $N$ and immediately returns a value () of type unit.

Figure 3 shows the definition of the remote evaluation construct. The rule Reval creates a new logical node $7^7$ with *new* 7' because $M$ may be evaluated at any node. In contrast, the rule Reval® creates a new logical node y with *new* y @ $J$ because $M$ may be evaluated only at node u/.[1]

### 4.5.2 Futures

A future construct [8] is similar to a remote procedure call in that it initiates a stand-alone computation at a remote node and also expects the result. The difference is that it does not wait for the result and immediately returns a *synchronization variable* which points to the remote node. When the result is needed, it is requested through a synchronization operation. If the remote node has finished the computation, the result is returned; otherwise the synchronization operation is suspended until the result becomes ready. We can simulate a remote procedure call by performing a synchronization operation immediately after evaluating a future construct.

Figure 4 shows the definition of the future construct future M. It expects $M$ to be of type DO$A$, $D$^$OA$, •O^/$A$, or CLOo/$A$. If $M$ evaluates to box $N$, it initiates a stand-alone computation of letcir $v = N$ in $v$ at a new logical node 7 created with *new* 7 and returns a synchronization variable syncvar 7 of type $A$ sync; if $M$ evaluates to box^ AT, it initiates the same stand-alone computation at a new logical node 7 created with *new* 7 @ $UJ$ and returns a synchronization variable syncvar 7 of type $A$ sync^. Since $N$ has type $OA$ or $0$^'$A$, letcir $v = N$ in $v$ evaluates to a mobile value of type $A$ that is valid either at any node or at node $d$. The result is requested through a synchronization operation syncwith syncvar 7.

Note that a synchronization variable itself is inherently mobile and we can synchronize with it *at any node*. Intuitively it is just a pointer to a certain logical node and hence is globally valid. The result of a synchronization operation may not be valid at the node where it takes place, but the typing system correctly

**[1] A remote evaluation construct can be simulated by a future construct; we present the remote evaluation construct only as a simple example of using modal types D^4 and D^A As we will see below, eval $M$ is simulated as let. = future (letbox $x = M$ in box let. = $x$ in cir ()) in () where let $x = M$ in $N$ is standard let-binding and _ is a wildcard pattern.**

indicates the mobility of the result. For example, in the rule Tswith[7], the result of evaluating syncwith *M* is valid only at node u/, which is correctly indicated by @ u/ in the typing judgment of the conclusion.

The rules Tsvar and Tsvar[7] show that a configuration type A is necessary in extended typing judgments in order to typecheck synchronization variables. Since synchronization variables are created only by the future construct and do not appear in a source program, we need these rules only for proving the type safety.

| | | | |
|---|---|---|---|
| type | *A* | ::= | ··· I *A* **sync** \| *A* **sync^** |
| term | *M* | ::= | ··· **I future** *M* **\| syncvar 7 \| syncwith** *M* |
| value | *V* | ::= | ··· **Isyncvar 7** |
| evaluation context | K | ::= | ··· **I future K I syncwith** *K* |

A; A; F h^ *M : DOA*
A; A; F h^ future *M* ~ ^ sync @ *cv** Tfuture

A ; A ; F K ; M : □∧ω○A
A; A; F h^ future M ~ ^ sync @ *u** Tfuture®

Λ; Δ; Γ ⊢ω *M* : □○ω″ *A*
A; A; F K, future *M* ~ *A* sync^ @ a;* Tfuture/

Λ; Δ; Γ ⊢ω *M* : □ω′○ω″ *A*
A; A; F !-,, future *M* ~ A sync^,, @ u;* Tfuture@/

$\gamma \sim A$ @ ⋆ ∈ Λ
A; A; F h^ syncvar 7 : A sync **Tsvar**

$\gamma \sim A$ @ ω′ ∈ Λ
A; A; F h^ syncvar 7 : *A* **sync**$_{\omega'}$ **Tsvar[7]**

*A'.A'.Th^MiAsync*
A; A; F h^ syncwith *M~A@LJ** Tswith

A; A;F h^ M: ^ ^syncA,
A; A; F h^ syncwith M ~ *A* @ a;[7] Tswith′

*new* γ′
C, ^[future box *M]* at 7 => C, /^[syncvar 7[7]] at 7, letcir v = M in *v* at Y **Rfuture**

*new*'T[7] @u/
C, K[future box^/ M] at 7 => C, ^[syncvar 7[7]] at 7, letcir v = *M* in t> at 7[7] **Rfuture®**

C, K[syncwith syncvar T[7]] at 7, V^ at 7[7] => C, **K[F]** at 7, *V* at T[7] **Rswith**

**Figure** 4: Definition of the future construct. u>* may be read as "any node."

### 4.53 Asynchronous channels

An asynchronous channel is a first-in-first-out buffer containing values communicated among nodes. A write operation adds a value to the buffer and always succeeds. A read operation removes the oldest value from the buffer, if the buffer is empty, it waits until a new value is written. We assume that an asynchronous channel is accessible to every node. This means that a value written to it must be globally valid, which in turn means that a value read from it is also globally valid. A similar idea can be used to implement *shared variables,* for which a write operation overwrites a single-entry buffer and a read operation leaves the buffer intact.

We implement an asynchronous channel for type *A* as a special node holding a list of values of type *A.* The node updates the list when a read or write operation is performed on the channel. It maintains the invariant that every value in the list is globally valid.

Figure 5 shows the definition of asynchronous channels, nil and *Vh* :: $V_u$ both of type *A* vlist, are constructs for lists, newchan^ creates a new logical node 7 to implement an asynchronous channel for type A, and returns a *channel variable* chanvar 7 of type *A* chan. A channel variable points to an asynchronous channel and is globally valid. The rules Rreadc and Rwritec show how read and write operations manipulate the node associated with an asynchronous channel.

Like synchronization variables for future constructs, channel variables are created only by newchan 4 and do not appear in a source program. Therefore we need the rule Tchanv only for proving the type safety.

| | | |
|---|---|---|
| type | A | ::= • • • \| A chan \| A vlist |
| **term** | ***M*** | **::= • • • \| nil \| *V* :: *V* \| chanvar 7 \| newchan^ \| readchan *M* \| writechan *M M*** |
| **value** | ***V*** | **::= • • • \| nil \| *V* :: *V* \| chanvar 7** |
| **evaluation context** | ***n*** | **::= • • • \| readchan *n* \| writechan *K M* \| writechan (chanvar 7) *n*** |

A; A; *T* h^ nil : *A* vlist **Tvnil**

A-&-T^$V_h$:A A; A; T K, ^: ,4 vlist / A; A; V h^ $V_h$ :: $V_t$:A vlist **Tvcon**

**7 ~ *A* vlist @ • *e* A**

**A ; A ; r K , chanvar 7 :^chan** Tchanv **A; A; *T* \-$_u$ newchan^ ~ *A* chan @ u;*** TnewC

**A; A; *T* h^ *M* : *A* chan**

**A; A; *T* h^ readchan M ~ A @ a;*** Treadc

**AjAsrhq; Af : Achan /T^/I^ A; A;T h^ AT ^ ^ @ ^**

**A; A; T h^ writechan M AT ~ *A* @ c/*** **Twritec**

**next; 7'**

**C, ^[newchan^] at 7 ==> C, K[chanvar T$^7$] at 7, nil at V** **Rnewc**

**C, ^[readchan chanvar $_7$'] at 7, $V_h$ :: $F_t$ at y => C, K ^ ] at 7, $V_t$ at γ'** **Rread$_0$**

**C, «:[writechan (chanvar y) V] at 7, Vi':: • ·• :: V^ :: nil at 7$^7$ =>** **Rwritec**

**C,«[^ at 7, Vi :: • • • :: $F_n$.'' V :: nil at y**

Figure 5: Definition of asynchronous channels, *u;** may be read as "any node."

## 4.6 Type safety

The type safety of the network operational semantics consists of two properties: configuration type preservation (Theorem 4.1) and configuration progress (Theorem 4.5). Configxiration type preservation states that a configuration transition does not alter the type and mobility of the term being evaluated at each node. Configuration progress states that we can apply a configuration transition rule until every node has finished its stand-alone computation or waits for a result from another node (by the rules Rswith, Rreadc, and Rwritec).

**Theorem 4.1 (configuration type preservation).**
*IfC ::AandC=> C, thenC :: A'suchthat Ac* A'.

*Proof.* By case analysis on *C* => C''. There are three cases:

1) Co, *K[M]* **at** 7 = > Co, *K[N]* **at** 7
2) Co, *K[M]* at 7 = » $C_o$, *K[N]* **at** 7, AT$^7$ **at** V
3) Co, K[M] **at** 7, M$^7$ **at** y = > $C_o$, K[JV] **at** 7, TV' **at**$_7$ ;

In each case, we show that *N* preserves the type and mobility of M. In case 3), we also show that $N^f$ preserves the type and mobility of *M'*. d

**Lemma 4.2 (Canonical forms).** *If* A; · ; r$^{perm}$ h^ *V* - *A* @ u/, ***then***

*V* = *v*,

*A is a primitive type,*
*A = Ai D A2andV = \x:A\.M,*
*A = UBandV =* boxM,
*A = Uu'tB and V =* box^// M,
*A = OBandV = drM,*
*A = Ou'fB and V =* cir^// *M,*
*A =* unit *andV =* (),
*A = B* sync *and V* = syncvar 7,
*A = B* synqy/ *and V* = syncvar 7,
*A = B* chan and *V* = chanvar 7,
,4 = S vlist *and V =* nil,
*or A = B* vlist *and V =* $V_h$ :: 14.

***Proc/*** Suppose that V ^ *v* and >1 is not a primitive type.

If *A = Ai* D $A_2$, then A; •; $r^{perm}$ h^ *V ~ A @ J* is derived by the rule *D\\v,* optionally followed by the rule *\ZB\W-* Hence *V* = Ax: *A\. M.*

All the other cases are analogous. •

**Lemma *43.*** *IfA; -; r*>$^{erm}$ \-uM~AQw', then*

*M = V ^v,* *M = vandv~A@u;'e T**™™,
*M = K[V] andv~ B@ue* T^$^1$™, *M = K[N] where N* —• *N',*
*M =* Ac[eval box *N],* *M =* «[eval box^// *N],*
*M =* ^[future box **AT],** *M =* /c[future box^// *N],*
***M* = ^[syncwith syncvar 7],** ***M = l*^[newchans],**
***M* = K[readchan chanvar 7],** ***or M = l*c[writechan (chanvar 7) *V],***

*Proof.* By induction on the structure of A; •; $r^{perm}$ h^ M ~ *A @ w'.* We present one case.

CaSe --*A^T^^M-A©prim* P n m ∧ ( '' ∧ '' } :

If M = *V* ^ i; by induction hypothesis, we are done.

*M = v* and *v ~ A^$i_m$ @ u;* G r**$^1$™ cannot happen by induction hypothesis, since the assumption on **$\Gamma^{perm}$ re**quires that permanent local resources not be of a primitive type.

If *M = K[M']* by induction hypothesis where

*M' = vandv ~ B @u e* r^"$^1$,

*M'* —> ***N*** or

***M$^f$* is eval box *N* eval box^," AT', future box *M* future *box^f N'$_9$* syncwith syncvar 7, newchan#, readchan chanvar 7, or writechan (chanvar 7) *V,***

then we are done. •

Lemma 4.4. *If* A; A; *T* h^ K[M] ~ *A @ d, then there exist B and J' such that* A; A; *T V-$_u$ M ~ B @ J'.*

*Proof* By induction on the structure of *K.* D

**Theorem 4.5 (configuration progress).**
*IfC* :: A, *then either there exists C$^f$ such that C* => C$^7$, *or C consists only of the following:*

Vat 7,
**^[syncwith syncvar T$^7$] at 7,**
**K[readchan chanvar *Y* $^a$* 7>**
**K[writechan (chanvar 7') *V]* at 7.**

*Proof.* Suppose $C = C_0, M$ **at** $\gamma$. By the rule Tcfg, we have $\Lambda; \cdot; \Gamma^{\mathsf{perm}} \vdash_\omega M \sim A \mathbin{@} \omega'$ for $\mathcal{P}(\gamma) = \omega$ and a certain node $\omega'$. We do case analysis according to Lemma 4.3. We present one case.
Case $M = \kappa[\mathsf{writechan}\ (\mathsf{chanvar}\ \gamma')\ V]$:

By Lemma 4.4, we have $\Lambda; \cdot; \Gamma^{\mathsf{perm}} \vdash_\omega \mathsf{writechan}\ (\mathsf{chanvar}\ \gamma')\ V \sim B \mathbin{@} \omega''$.

By the rule Twritec (optionally preceded by the rule Prim $\sim_W$ if $B$ is a primitive type), we have $\Lambda; \cdot; \Gamma^{\mathsf{perm}} \vdash_\omega \mathsf{chanvar}\ \gamma' : B\ \mathsf{chan}$.

By the rule Tchanv, we have $\gamma' \sim B\ \mathsf{vlist} \mathbin{@} \star \in \Lambda$.

Since $C :: \Lambda$, we have $C = C_0', M$ **at** $\gamma, N$ **at** $\gamma'$ and $\Lambda; \cdot; \Gamma^{\mathsf{perm}} \vdash_{\mathcal{P}(\gamma')} N \sim B\ \mathsf{vlist} \mathbin{@} \omega^*$ for a fresh node $\omega^*$.

If $N = V_1 :: \cdots :: V_n :: \mathsf{nil}$ (where $0 \leq n$), then

$$\frac{}{\begin{array}{r} C_0', \kappa[\mathsf{writechan}\ (\mathsf{chanvar}\ \gamma')\ V]\ \textbf{at}\ \gamma, V_1 :: \cdots :: V_n :: \mathsf{nil}\ \textbf{at}\ \gamma' \Longrightarrow \\ C_0', \kappa[V]\ \textbf{at}\ \gamma, V_1 :: \cdots :: V_n :: V :: \mathsf{nil}\ \textbf{at}\ \gamma' \end{array}}\ \mathsf{Rwritec}$$

Otherwise $N \neq V_1 :: \cdots :: V_n :: \mathsf{nil}$ and $M$ is not further reduced. ☐

The two cases $\kappa[\mathsf{syncwith\ syncvar}\ \gamma']$ **at** $\gamma$ and $\kappa[\mathsf{readchan\ chanvar}\ \gamma']$ **at** $\gamma$ in Theorem 4.5 can occur during a distributed computation. Here is an example of a configuration whose transition gives rise to the two cases:

$$\begin{array}{ll} & \mathsf{syncwith\ future\ box\ cir}\ (\mathsf{readchan\ newchan}_A)\ \textbf{at}\ \gamma \\ \Longrightarrow & \mathsf{syncwith\ syncvar}\ \gamma'\ \textbf{at}\ \gamma, \mathsf{letcir}\ v = \mathsf{cir}\ (\mathsf{readchan\ newchan}_A)\ \mathsf{in}\ v\ \textbf{at}\ \gamma' \\ \Longrightarrow & \mathsf{syncwith\ syncvar}\ \gamma'\ \textbf{at}\ \gamma, \mathsf{letcir}\ v = \mathsf{cir}\ (\mathsf{readchan\ chanvar}\ \gamma'')\ \mathsf{in}\ v\ \textbf{at}\ \gamma', \mathsf{nil}\ \textbf{at}\ \gamma'' \end{array}$$

Here node $\gamma$ waits for a result from node $\gamma'$, which in turns waits for a value to be written to node $\gamma''$. Since no value can be written to node $\gamma''$, the last configuration is stuck. The case $\kappa[\mathsf{writechan}\ (\mathsf{chanvar}\ \gamma')\ V]$ **at** $\gamma$ in Theorem 4.5 occurs only when the term being evaluated at node $\gamma'$ cannot be reduced to a list of values (whether empty or not), as clarified in the proof above. This case, however, does not actually occur because an asynchronous channel is always initialized as nil by the rule Rnewc and never holds a term that is not a list.

The type safety of the network operational semantics implies that mobile terms and mobile values are both safe to use: well-typed terms never go wrong even in the presence of mobile terms and mobile values.

## 4.7 Example

Consider a network of two nodes **S** (server) and **C** (client). Node **S** has a printer attached to it, and provides a function *print* for printing pdf files of type pdf. The printer accepts pdf files written only with local fonts, and provides a function $convert_{\mathbf{S}}$ for converting ordinary pdf files into a suitable format. Node **C** has its own conversion function $convert_{\mathbf{C}}$.

$$\begin{array}{lcl} \Gamma^{\mathsf{perm}}_{\mathbf{S}} & = & \mathit{file}_{\mathbf{S}} \sim \mathsf{pdf} \mathbin{@} \mathbf{S}, \mathit{convert}_{\mathbf{S}} \sim \bigcirc(\mathsf{pdf} \supset \bigcirc_{\mathbf{S}}\mathsf{pdf}) \mathbin{@} \mathbf{S}, \mathit{print} \sim \mathsf{pdf} \supset \mathsf{unit} \mathbin{@} \mathbf{S} \\ \Gamma^{\mathsf{perm}}_{\mathbf{C}} & = & \mathit{file}_{\mathbf{C}} \sim \mathsf{pdf} \mathbin{@} \mathbf{C}, \mathit{convert}_{\mathbf{C}} \sim \mathsf{pdf} \supset \bigcirc_{\mathbf{S}}\mathsf{pdf} \mathbin{@} \mathbf{C} \end{array}$$

We give three examples (similar to those in [9]) to illustrate how to describe tasks in $\lambda_{\Box\bigcirc}{}^{W}$. All terms below have type $\Box_{\mathbf{S}}\mathsf{unit}$ and typecheck at any node. We use syntactic sugar rpc $M$ for syncwith future $M$.

Printing a pdf file $\mathit{file}_{\mathbf{S}}$ of node **S**:

$$\mathsf{box}_{\mathbf{S}}\ (\mathit{print}\ \mathit{file}_{\mathbf{S}})$$

Printing a pdf file $\mathit{file}_{\mathbf{C}}$ of node **C** after converting it with $\mathit{convert}_{\mathbf{C}}$:

$$\begin{array}{l} \mathsf{letcir}\ v = \mathsf{cir}_{\mathbf{S}}\ \mathsf{rpc}\ \mathsf{box}_{\mathbf{C}}\ (\mathit{convert}_{\mathbf{C}}\ \mathit{file}_{\mathbf{C}})\ \mathsf{in} \\ \mathsf{box}_{\mathbf{S}}\ (\mathit{print}\ v) \end{array}$$

Printing a pdf file $file_c$ of node C after converting it with *converts:*

boxs letcir $v$ = *converts* in
letcir $v'$ = cirs rpc boxc $(v\ file_c)$ in
*print* $v^1$

# 5 Related work

## 5.1 Local resources in distributed computations

In designing a distributed system, there are several ways to handle references to local resources when they are transmitted (as part of a mobile term) to a remote node. If the underlying system supports direct access to remote resources, such a reference can be replaced in the remote node by a proxy which automatically redirects all requests for the resource to the originating node. Obliq [3] adopts such a computation model, in which *local references* are replaced by *network references* in a remote node.

*\u&* allows references to remote resources in mobile terms, but it also ensures that they are never dereferenced. In essence, references to local resources become invalid when they are transmitted to remote nodes, but their validity is restored when they are brought back to the original node. For example, if a term *M* accesses local resources of node *u>* and returns a globally valid value of type *A,* then

syncwith future box^ cir *M*

can be evaluated *at any node:* wherever the above term is evaluated, it calls back with the same term *M* to node a?, where all references in *M* again point to their corresponding local resources. The same computation model is used by Mascolo *et al.* [11] in their treatment of references.

References to remote resources, as used in the above two computation models, are suitable for persistent resources such as printers and databases, but they can be problematic for ephemeral resources which are eventually destroyed. For example, die presence of references to remote heap cells incurs the problem of distributed garbage collection [7]. An alternative computation model is one that permits no references to remote resources either by rejecting mobile terms containing such references or by transmitting copies of local resources along with mobile terms. Facile [10] supports such a computation model, in which local resources are copied whenever their references (called *singular values)* are transmitted to a remote node. Thus the problem with ephemeral resources is resolved at an increased cost of transmitting mobile terms.

## 5.2 Modal languages for distributed computation

Borghuis and Feijs [1] present a typed A-calculus *MTSN* (Modal Type System for Networks). It assumes stationary services *(Le.,* stationary code) and mobile data, and belongs to the client/server paradigm. An indexed modal type *Of(A —• B)* represents services transforming data of type *A* into data of type *B* at node *u>* (similarly to D^ *(A* D *B)* in $AQO^H$ ). MTSN is a task description language rather than a programming language, since services are all "black boxes" whose inner workings are unknown. For example, terms of type *tex —> dvi* all describe procedures to convert tex files to dvi files. Thus reduction on terms is tantamount to simplifying procedures to achieve a certain task.

Jia and Walker [9] present a modal language $A_{rpc}$ which belongs to the remote evaluation paradigm. It is based upon hybrid logic [2], and every typing judgment explicitly specifies the current node where typechecking takes place. The modalities • and 0 are used for mobile terms that can be evaluated at any node and at a certain node, respectively.

Murphy *et al* [13] present a modal language *Lambda 5* which addresses both code mobility and resource locality. It also belongs to the remote evaluation paradigm, and is based upon modal logic S5 where all judgments are relativized to nodes. A value of type *DA* contains a mobile term that can be evaluated at any node, and a value of type *()A* contains a *label,* a reference to a local resource. A label may appear at remote nodes, but the type system guarantees that it is dereferenced only at the node where it is valid.

Although the intuition behind the modality • is the same, $A_{rpc}$ and Lambda 5 are fundamentally different from $Ano^{w'}$ in their use of modal types *DA* in remote procedure calls. In both languages, a remote procedure call, by the pull construct in $A_{rpc}$ and by the fetch construct in Lambda 5, is given a specific node where the evaluation is to occur, and therefore *does not expect a term contained in a value of type DA.* Instead it expects just a term of type *DA,* which itself may not be mobile but eventually produces a mobile term valid at any node including the caller node. The resultant mobile term is delivered to *(i.e.,* pulled or fetched by) the caller node, which needs to further evaluate it to obtain a value. As such, neither language needs to address the issue of value mobility. In contrast, a remote procedure call in *XQC^* (by the eval or future construct) transmits a term *contained in a value of type DA* and relies on the modality O for return values. Such use of the modality • is natural in Ano^, since it supports remote procedure calls to unknown nodes.

Moody [12] presents a system which is based upon modal logic S4 and belongs to the remote evaluation paradigm. The modality • is used for mobile terms that can be evaluated at any node, and the modality 0 is used for terms located at some node. As in $Ano^{w}$\ remote procedure calls use modal types *DA* to transmit mobile terms to unknown remote nodes. Moody's system uses the elimination rules for the modalities • and 0 to send mobile terms to remote nodes, and does not provide a separate construct for remote procedure calls.

# 6 Conclusion and future work

We present a modal language AQO^ which ensures the safety of both mobile terms and mobile values. It provides a flexible programming environment for various kinds of distributed computations. For example, if the network evolves dynamically and no permanent local resources are known in advance, only modal types *DA* and *OA* are necessary; if the network is static and every node publishes its permanent local resources, we can program exclusively with indexed modal types *D^A* and Oo,A

The modality O is useful in Ano^ only because the unit of communication includes a value. That is, if the unit of communication was just a term and did not include a value, the modality O would be unnecessary. Then, however, the future construct would have to be redefined in a similar way to the pull construct of Arpc and the fetch construct of Lambda 5, and asynchronous channels would be difficult to implement.

The three communication constructs of AQO^ are all defined separately. A better approach would be to introduce a few primitive operations and then implement various communication constructs using these primitive operations. For example, we could introduce a send operation for the modality • and a receive operation for the modality O, and then implement the future construct using these operations. Because of technical difficulties arising from asynchronous channels, however, we do not adopt this approach and define all communication constructs separately.

A drawback of Ano^ is that in general, references to ephemeral local resources cannot be transmitted to remote nodes. As an example, consider a pointer *v* of type ptr *A* at a logical node 7 created with *new* 7. Node 7 wishes to use *v* as a shared pointer among all its child nodes, *i.e.,* those nodes created with the eval and future constructs. No child node, however, even knows the existence of *v* because the physical node *u* in a binding *v ~ A @ u;* is not known statically. (If node 7 was created with *new* 7 @ $u>_9$ then *v* could be transmitted to remote nodes.)

To overcome this drawback, we are currently investigating how to augment Ano (not Ano^) with a modality 0 similar to that of Jia and Walker [9]. The idea is that a term *M* in dia *M* of type *OA* can be evaluated at a certain node, which is unknown to the type system but known to the runtime system. The use of the modality 0 will allow us to dispense with indexed modalies *D^* and Ou;.

## Acknowledgment

I am grateful to Tom Murphy and Jonathan Moody for their helpful comments on an earlier draft of this paper, and Karl Crary for his helpful comments on the type system.

## References

[1] T. Borghuis and L. Feijs. A constructive logic for services and information flow in computer networks. *The Computer Journal*, 43(4):275–289, 2000.

[2] T. Braüner. Natural deduction for hybrid logic. *Journal of Logic and Computation*, 14(3):329–353, 2004.

[3] L. Cardelli. A language with distributed scope. In *Proceedings of the 22nd ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 286–297. ACM Press, 1995.

[4] A. Carzaniga, G. P. Picco, and G. Vigna. Designing distributed applications with mobile code paradigms. In *Proceedings of the 19th international conference on Software engineering*, pages 22–32. ACM Press, 1997.

[5] G. Cugola, C. Ghezzi, G. P. Picco, and G. Vigna. Analyzing mobile code languages. In *Selected Presentations and Invited Papers Second International Workshop on Mobile Object Systems - Towards the Programmable Internet*, pages 93–110. Springer-Verlag, 1997.

[6] R. Davies and F. Pfenning. A modal analysis of staged computation. *Journal of the ACM*, 48(3):555–604, 2001.

[7] F. L. Fessant, I. Piumarta, and M. Shapiro. An implementation of complete, asynchronous, distributed garbage collection. In *Proceedings of the ACM SIGPLAN 1998 conference on Programming language design and implementation*, pages 152–161. ACM Press, 1998.

[8] R. H. Halstead, Jr. Multilisp: a language for concurrent symbolic computation. *ACM Transactions on Programming Languages and Systems*, 7(4):501–538, 1985.

[9] L. Jia and D. Walker. Modal proofs as distributed programs (extended abstract). In D. Schmidt, editor, *Proceedings of the European Symposium on Programming, LNCS 2986*, pages 219–233. Springer, Apr. 2004.

[10] F. C. Knabe. *Language Support for Mobile Agents*. PhD thesis, Department of Computer Science, Carnegie Mellon University, 1995.

[11] C. Mascolo, G. P. Picco, and G.-C. Roman. A fine-grained model for code mobility. In *Proceedings of the 7th European software engineering conference held jointly with the 7th ACM SIGSOFT international symposium on Foundations of software engineering*, pages 39–56. Springer-Verlag, 1999.

[12] J. Moody. Modal logic as a basis for distributed computation. Technical Report CMU-CS-03-194, Carnegie Mellon University, Oct. 2003.

[13] T. Murphy, VII, K. Crary, R. Harper, and F. Pfenning. A symmetric modal lambda calculus for distributed computing. In *Proceedings of the 19th IEEE Symposium on Logic in Computer Science (LICS 2004)*. IEEE Press, July 2004.

[14] F. Pfenning and R. Davies. A judgmental reconstruction of modal logic. *Mathematical Structures in Computer Science,* 11(4):511-540, 2001.

[15] A. K. Simpson. *The Proof Theory and Semantics of Intuitionistic Modal Logic.* PhD thesis, Department of Philosophy, University of Edinburgh, 1994.

# A Proofs of the properties of AQO

**Proposition A.I.**

*//A;T h M : Aand A;I\x : A h N : B, then A;T h [M/x]N : B.*

*If A]Th M : Aand A,r,x: Ah N ~B, then A;F\- [M/x]N ~ B.*

*Proof* By simultaneous induction on the structure of of the derivation of A; r, *x : A h N : B* and A; T, *x : A h N* ~ *B*.

Proof of the first clause:

Case *N = x: [M/x]N = M*

By the rule Cvar, A; T, *x : A h N : B* implies *A = B.*

A;T h *M* : ^implies A;T h *[M/x]N : A.*

Therefore A; *T h* [M/x]*N* : B.

Case *N = y,y ^ x: [M/x]N = y*

By the rule Cvar, A; T, x : *A h* iV : *B* implies y :: 5 e A or 2/: *B* G I\x : *A.*

Since *y ^ x,v/c* have y :: 2? G A or *y : B* G F.

By the rule Cvar, A; *T* h *y* : B.

Therefore A; T h [Af/o;]JV : S.

Case *N = v: [M/x]N = v*

By the rule Vvar, *A;T,x : A\- N : B* implies *v ~ B e A.*

By the rule Vvar, A; *T* h *v* : *B.*

Therefore A; *V* h [M/x] AT: £.

Case *N = Xy:* $B^f$. *N\ y ^* x, y not a free variable of M: [M/x]iV = Ay: $B^1$. *[M/x]N'*

By the rule Dl, A; I\x : A h AT: *B* impUes A; T,x : *A,y : B' h N' : B"* and *B =* $B^1$ D $B^{/;}$.

By weakening, *A;Th M :A* implies A;r,j/:B'hM:A

By induction hypothesis, A; I\y : $B^1$ h [M/x] $AT^7$ : £".

By the rule Dl, A; *T* h Ay: $S^r$. [M/x] $JV^;$ : S' *D B".*

Therefore A; *V* h [M/x]iV : B.

Case AT = iVi $AT_2$: [M/x]AT = [M/x]^ [M/x]$AT_2$

By the rule DE, A; I\x : A h AT: S implies A; T, x : A h JVi : $B^;$ D *B* and A; T, x : *A* h $AT_2$ : *B'.*

By induction hypothesis, A; *V* h [M/x]JVi : $B^f$ D B and A; *V* h [M/x]$AT_2$ : $S^;$.

By the rule DE, A; *V* h [M/x]iVi [M/x] $AT_2$ : S.

Therefore A; T h [M/x]iV : *B.*

Case AT = box *N': [M/x]N* = box [M/x]AT

By the rule Dl, A;I\x : *A* h *N : B* implies A; • h *N':* $B^f$ and *B = OB'.*

Since x is not a free variable of *N* we have [M/x]*N'* = AT.

By the rule Dl, A; *T* h box [M/x] $AT^7$ : •£'.

Therefore A; *T* h [M/x] AT: £.

Case AT = letbox y = $AT_X$ in $AT_2$, y 7^ x, y not a free variable of M:

[M/x]AT = letbox y = *[M/x]Ni* in [M/x]$AT_2$

BytheruleDE,A;r,x: A h AT: .Bimplies A;T,x : *Ah* $N_x$ : $DB_X$ and A,y :: £i;I\x : A h $AT_2$ : B.

By weakening, A; *T h M* : A implies A, y :: Si; *T h M : A.*

By induction hypothesis, A; *T h [M/x]$N_x$* : QBi and A, *y* :: *By T h* [M/x]$AT_2$ : £.

By the rule DE, A; *T h* letbox y = [M/x] $AT_X$ in [M/x]$AT_2$ : £.

Therefore A; *T h* [M/x] AT : B.

Case AT = cir *N':* *[M/x]N* = cir [M/x]AT'

By the rule Ol, A; I\ *x : A h N* : £ implies A; I\ x : A h *N'* ~ J5' and B = *OB'.*

By induction hypothesis, A; *T h* [M/x]AT' ~ £'.

By the rule Ol, A; *T h* cir [M/x]TV' : $OS^7$.

Therefore A; T h [M/x] AT: £.

Case *N* = letcir t; = *Ni* in $AT_2$, i; not a free variable of *M:* *[M/x]N* = letcir v = *[M/x]N* in [M/x] $AT_2$

ByTheraleOE,A;r,x:^hAr:£impliesA;r,x:,4hAri : OBi and A,v ~ £i;I\x : >1 h $iV_2$ : B.

By weakening, A; *T* h M : A implies A , v ~ B i ; r h M : A

By induction hypothesis, A; *T* h [M/x]iVi : OBi and A, r; ~ *$B_x$\ T* h [Af/x]$JV_2$ : £.

By the rule OE, A; *T* h letcir t; = [M/x]^ in [M/x]iV2 : *B.*

Therefore A; *T* h [M/x] AT: B.

Proof of the second clause:

If the rule Prim~ is used to deduce A; T,x : *A* h N ~ *B:*

*A;T,x : Ah N : B* and *B* is a primitive type.

By induction hypothesis, A; T h [M/x]AT: *B.*

By the rule Prim~, A; *T* h [M/x] AT ~ B.

Now AT cannot be an application iVi $AT_2$ or a variable *y.*

Case AT = *V:*

By the rule Val, A; I\ x : *A* h AT ~ *B* implies A; • h *N : B.*

Since x is not a free variable of *$N_9$* we have *[M/x]N = N.*

By the rule Val, A; *T* h [M/x]*N* ~ S.

Case AT = letbox y = iVi in $AT_2$, *y* ^ x, *y* not a free variable of M:

[M/x]AT = letbox *y = [M/x]^* in [M/x]$AT_2$

By the rule DE', A; I\ x : *A* h AT ~ S implies A; T,x : ,4 h $AT_X$ : DBi and A, *y :: B^T^x : Ah $N_2$ ~ B.*

By weakening, A; F h M : *A* implies A, *y :: B\\ T h M : A.*

By induction hypothesis, A; *T h [M/x]Ni : UB* and A, *y* :: *Bi; T h [M/x]$N_2$ ~ B.*

By the rule DE', A; *T h* letbox *y* = [M/x]ATi in [M/x]$AT_2$ - *B.*

Therefore A; *T h* [M/x]AT ~ *B.*

Case *N* = letcir *v* = *N* in $AT_2$, v not a free variable of M: [M/x]*N* = letcir t; = *[M/x]N* in [M/x] $AT_2$

By theruleO^A^x : *A h N* ~ Bimplies A;I\x : A h JVi : O#i and A, v ~ Bi;r,x : >1 h $AT_2$ ~ *B.*

By weakening, A; *V h M* : *A* implies A, *v ~ B\\ T h M : A.*

By induction hypothesis, A; T *h [M/x]Ni : OBi* and A, *v ~ By, T h [M/x]$N_2$ ~ B.*

By the rule $OE^7$, A; *T h* letcir *v = [M/x]Ni* in *[M/x]$N_2$ ~ B.*

Therefore A; *T h [M/x] N ~ B.* D

Proof of Proposition 2.2 and Proposition2.4:

*Proof.* By simulataneous induction on the structure of the derivation of A, x :: *A', T h N : B* and A, x :: *A; T h N ~ B.*

Proof of Proposition 2.2:

Case *N = x:* *[M/x]N = M*

*A;-hM:A* implies A; • h [M/x] *N : A.*

By weakening, A; • h [M/x]AT : *A* implies A; T *h [M/x]N : A.*

A, x :: *A; T h N* : *B* implies *A = B.*

Therefore A; *T h [M/x]N : B.*

Case *N = y,y^x:* *[M/x]N = y*

By the rule Cvar, A, *x* :: A *F* h *N* : *B* implies *y* :: *B e* A, *x* :: *A* or *y* : *B* € *T*.
Since *y* ^ x, we have *y* :: *B* G A or *y* : *B* G F.
By the rule Cvar, A; *V* h y : £.
Therefore A; *V* h [M/x] AT : £.

Case AT = *v*: *[M/x]N = v*
By the rule Vvar, *A,x :: A;T \- N : B* implies *v* ~ f? € A, *x* :: A which means V ^ B G A .
By the rule Vvar, A; T h i;: *B*.
Therefore A; *V* h [M/x] AT: B.

Case *N* = *\y: B'. N\ y* ^ x, *y* not a free variable of Af: [M/x] AT = Ay: *B'*. *[M/x]N*$^f$
By the rule Dl, A, x :: *A; T* h AT: *B* implies A, x :: *A*; T, y : .$B^7$ h 7V' : .$B^{77}$ and B = $S^7$ D $B^{7/}$.
By induction hypothesis, A; I\ y : $S^7$ h *[M/x]N'* : $S^{77}$.
By the rule Dl, A; *T* h Ay: $B^7$. [M/x]*N' : B'* D $B^{77}$.
Therefore A; *T* h [M/x] AT: £.

Case AT = $N_x$ $N_2$: *[M/x]N = [M/x]*$N_x$ *[M/x]*$N_2$
By the rule DE, A, x *::A;ThN : B* implies A, x :: *A;T* h $AT_X$ : $B^7$ D S and A, x :: *A;T* h $AT_2$ : $B^7$.
By induction hypothesis, A; T h [M/x] $AT_X$ : $B^1$ *D B* and A; *T* h [M/x]$AT_2$ : $5^7$.
By the rule DE, A; T h [M/x]JVi [M/x]$AT_2$ : *B*.
Therefore A; *T* h [M/x] AT: 5.

Case *N* = box $AT^7$: [M/x]AT = box [M/x]$AT^7$
By the rule *D\9A,x::A;T\-N:B* impUes *A,x :: A;- h N' : B' and B = DB'.*
By induction hypothesis, A; • h [M/x] $AT^7$: *B'*.
By the rule Dl, A; *T* h box [M/x]$AT^7$: $DS^7$.
Therefore A; T h [M/x] AT: 5.

Case AT = letbox y = ATi in JVjj, y-7^ x, y not a free variable of M:
[M/x]AT = letbox y = *[M/x]Nx* in [M/x]$AT_2$
By the rule DE, A, x :: *A-Th N* : 5impUesA,x :: *A;Th* $N_x$ : DJ5i and A, x :: *A,y i.B^Th* $N_2$ *: B*.
By weakening, A; • h M : *A* implies A, y :: 2?i; • h M : A
By induction hypothesis, A; *T* h [M/x]ATx : DSi and A, y :: £1; *T* h [M/x]$AT_2$ : B.
By the rule DE, A; *T* h letbox y = *[M/x]*$N_x$ in [M/x]$AT_2$ : B.
Therefore A; *T* h [M/x] AT: B.

Case AT = cir $A^{\wedge 7}$: [M/x]AT = cir [M/x]$AT^7$
By the rule Ol, A, x :: *A,T* h *N* : *B* implies A, x :: A;T h $AT^7$ ~ $B^7$ and B = *OB*$^f$.
By induction hypothesis, A; *T* h [M/x] $AT^7$ ~ $B^7$.
By the rule Ol, A; T h cir [M/x] $AT^7$ : $OS^7$.
Therefore A; T h [M/x]*N : B*.

Case AT = letcir *v* = *Ni* in $AT_2$, i; not a free variable of M: [M/x]*N* = letcir v = *[M/x]N* in [M/x]$AT_2$
By the rule OE, A, x :: *A;T\- N :* ^implies A, x :: *A;T* h A^i : O£i and A, x :: A *v* ~ *B^T* h $AT_2$ : *B*.
By weakening, A; « h M : A implies A, *v* ~ Si; • h M : A
By induction hypothesis, A; T h [M/x]A^i : OJBI and A, t; ~ Bi; T h [M/x]$AT_2$ : S.
By the rule OE, A; *T* h letcir v = [M/x]*Ni* in [M/x] $AT_2$ : B.
Therefore A; *T* h [M/x]AT: B.

**Proof of Proposition 2.4:**

If the rule Prim~ is used to deduce $A_y$*x :: A;Th N ~ B:*
A, x :: A; T h AT: *B* and B is a primitive type.
By induction hypothesis, A; *T* h [M/x] AT: *B*.

By the rule Prim~, A; $T$ h $[M/x]N$ ~ £.

Now $N$ cannot be an application $Ni$ $N_2$ or a variable $y$.

Case AT = $V$:

By the rule Val, A, $x$ :: $A$; $T$ h $N$ ~ $B$ implies A, x :: -4; • h $N$ : $B$.

By induction hypothesis, A; • h [Af/x] AT : B.

By the rule Val, A; $V$ h [M/x] AT - S.

Case AT = letbox y = iVi in $AT_2$, $y$ ^ $x,y$ not a free variable of $M$:

$[M/x]N$ = letbox ≤/ = $[M/x]N_x$ in $[M/x]AT_2$

By the rule $DE^7$, A, x:: $A;T$ h $N$ ~ $Bimphes$ $A$, $x$· :: $A,T$ h $Nx$ $:DB_1andA,x::A,y::B_1,rhN_2$~$B$.

By weakening, A ; « h M : 4 implies A, $y$ :: Bi; • h M : A

By induction hypothesis, A; T h [M/x]ATi : DBi and A, y :: $B_\pm$; $T$ h $[M/x]AT_2$ ~ £.

By the rule $DE^7$, A; $T$ h letbox y = [M/ar]JVi in $[M/ar]AT_2$ - B.

Therefore A; T h $[M/x]N$ - B.

Case $N$ = letcir v = JVi in $iV_2$, $v$ not a free variable of $M$: $[M/x]N$ = letcir $v$ = [M/x] JVi in $[M/x]JV_2$

By the rule $OE^7$, A, x:: A;ThAr~ BimpUes A,x :: ^;T h $AT_X$ : OBi and A,x :: A,v ~ Bi;T h $AT_2$ - $B$.

By weakening, A; • h M : A implies A, $v$ ~ $B$\; • h M : A

By induction hypothesis, A; T h [M/x]ATi : OJ5i and A, $v$ - Bi; T h $[Af/x]AT_2$ ~ JB.

By the rule $OE^7$, A; T h letcir v = [M/x] JVi in $[Af/x]AT_2$ ~ 5.

Therefore A; $T$ h [M/x] AT - 5. •

**Lemma A.2.**

//A; • h F : ^lanrf A, $v$ ~ $A;T$ h AT : B, lAm A;T h [V/v]i\T : B.

*If* $\Delta; \cdot \vdash V : A$ *and* $\Delta, v \sim A; \Gamma \vdash N \sim B$, *then* $\Delta$; r h [V/vJJV ~ S.

***Proof.*** By simulataneous induction on the structure of the derivation of A, $v$ ~ $A$; $F$ \- $N$ : $B$ and A, $v$ ~ $A$; $T$ h $N$ ~ $B$.

Proof of the first clause:

Case $N$ = $x$: $[V/v]N = x$

BytheruleCvar, A,v ~ $A\Y\-$ $N$ : $B$ implies x :: $B$ G A,v ~ Aorx : B E T, which means x :: 5 G A or x : B G T.

By the rule Cvar, A; T h x : B.

Therefore A; $T$ h [V/v]AT: B.

Case $N$ = $v$: $[V/v]N = V$

$A;-hV$ $:A$ implies A; • h $[V/v]N$ : $A$.

By weakening, A; • h [V/v]^ : A implies A; $T$ h [V/v]Ar: A.

$A,v$ ~ $A;Th$ $N$ : $B$ implies $A = B$.

Therefore A; $T$ h [V/v]AT: B.

Case $N$ = $w,w$ ^$v$: $[V/v]N = w$

By the rule Vvar, A, $v$ ~ A; F h $N$ : $B$ implies $w$ ~ $B$ $e$ $A,v$ ~ $A$, which means $w$ ~ $B$ G A.

By the rule Vvar, A ; T h w : B .

Therefore A; T h [V/v]AT: $B$.

Case AT = Ax: $B^f$. $N\backslash$ $x$ not a free variable of $V$: $[V/v]N$ = Ax: $B'$. $[V/v\backslash N^f$

By the rule Dl, A,v - $A;T$ h AT: £ implies A, v ~ A;T,x : $B^f$ h AT : B^andB = $B^7$ D $B^{77}$.

By induction hypothesis, A; T, x : $B^7$ h $[V/v]N'$ : B".

By the rule Dl, A; $T$ h Ax: $B^1$. $[V/v]N^f$ : $B^1$ $D$ $B''$.

Therefore A; $T$ h [V/v] AT: B.

Case $N$ = $N_x$ $N_2$: $[V/v]N$ = $[V/v]$^ $[V/v]N_2$

By the rule DE, A, $v$ ~ $A$; $T$ h AT: $B$ implies A, $v$ ~ $A$; $T$ h ATi : $B^7$ D $B$ and A, $v$ ~ A; T h $AT_2$ : $B^7$.

By induction hypothesis, A; T h [V/v]ATi : $B^7$ D B and A; T h $[V/v]N_2$ : $B^7$.

By the rule DE, A; *T* h *[V/v]Ni* *[V/v]$N_2$* : B.

Therefore A; T h [V/v] AT : B.

Case AT = box *N':* *[V/v]N* = box *[V/v\$N^f$*

By the rule Dl, A, *v* ~ *A; T* h AT: B implies A, v ~ A; • h AT': B' and B = DB'.

By induction hypothesis, A; • h *[V/v]$N^f$*: B'.

By the rule Dl, A; *T* h box [V/v] AT : DB'.

Therefore A; T h [V/v] AT : B.

Case AT = letbox *x* = *Ni* in $iV_2$, x not a free variable of *V:* *[V/v]N* = letbox *x* = *[V/v]Ni* in *[V/v]$N_2$*

BytheruleDE,A,v~ *A;T\-N:* B implies A,v~ A;ThiVi : □$B_1$ and A,v - *A,x ::* Bi;T h $iV_2$ : B.

By weakening, A ; - h F : i implies A, *x* :: Bi; • h V : A

By induction hypothesis, A; T h [V/v]ATi : □$B_1$ and A, x :: J5i; T h *[V/v]$N_2$* : *B*.

By the rule DE, A; *T* h letbox x = [V/v]$N_1$ in *[V/v]$N_2$ : B.*

Therefore A; *T* h [V/v]iV : *B.*

Case AT = cir *N':* *[V/v]N* = cir *[V/v]$N^f$*

By the rule Ol, A, *v* ~ *A; T* h *N* : B implies A, *v* ~ *A; T* h *N'* ~ $B^f$ and *B* = *OB*

By induction hypothesis, A; *T* h [V/v] JV' ~ $JB^7$.

By the rule Ol, A; *T* h cir [V/vJA/$^7$ : $O5^7$.

Therefore A; T h [V/v]A^: B.

Case *N* = letcir w = *Ni* in $AT_2$, w; ^ v, it; not a free variable of V: [V/v] AT = letcir *w* = *[V/v]Ni* in *[V/v]$N_2$*

BytheruleOE,A,v~ *A;T\- N : B*implies A, v - A; T h $iV_1$ : O$B_1$ and Δ,v ~ ^l,it; ~ BijTh $AT_2$ : J5.

By weakening, A; • h V : A implies A, i/; ~ Si; • h V : A

By induction hypothesis, A; *T* h [V/vJA^i : OBi. and A, it; ~ $B_1$; T h [V/v]$AT_2$ : B.

By the rule OE, A; *T* h letcir w; = [V/v] $AT_X$ in [V/v]$AT_2$ : B.

Therefore A; *T* h [V/v]AT: B.

Proof of the second clause:

If the rule Prim~ is used to deduce A , v ~ i ; r h i V ~ B :

A, v ~ ^4; T h AT: B and B is a primitive type.

By induction hypothesis, A; *T* h [V/v] AT: B.

By the rule Prim-, A; *T* h [V/v] AT - B.

Now AT cannot be an application JVi *$N_2$* or a variable *x.*

Case AT = $V^7$:

By the rule Val, A , v ~ ^ 4 ; n - A T ~ B implies A, v ~ A; • h AT: B.

By induction hypothesis, A; • h [V/v]JV : B.

By the rule Val, A; *V* h [V/v] AT ~ B.

Case Af = letbox a: = *N* in $AT_2$, x not a free variable of V:

[V/v]AT = letbox x = *[V/v]$N_x$* in [V/v]$AT_2$

BytheruleDE^A^-^ri- AT ~ Bimplies A,v ~ ^4; Γ h $N_1$ : □$B_1$ and A, v ~ Λ,x :: Bi;TI-$AT_2$ ~ B.

By weakening, A; • h V : A implies A, x :: Bi; • h V : A

By induction hypothesis, A; *T* h [V/v]ATi : DBi and A, *x ::* $B_x$; T h [V/v]$AT_2$ ~ B.

By the rule DE', A; *T* h letbox x = [V/v]ATi in [V/v]$AT_2$ ~ B.

Therefore A; T h [V/v]JV - B.

Case AT = letcir *w* = *N* in $AT_2$, *w* ^ *v,w* not a free variable of V: [V/v] AT = letcir *w* = [V/v]ATx in [V/v]$AT_2$

By the rule OE', A, v~ *A; Th N* ~ B implies A,v ~ *A;T* \- *Ni* : OBi andA,v ~ A,tt; ~ Bi;T h $AT_2$ ~ *B.*

By weakening, A; • h V : *A* implies A, *w* ~ *B* • h V : A

By induction hypothesis, A; T h [V/v]iVi : OBi and A, *w* ~ Bi; *T* h [V/v]$AT_2$ ~ *B.*

By the rule OE', A; *T* h letcir tt; = [V/v]JVi in [V/v]$AT_2$ ~ B.

Therefore A; T h [V/v]AT ~ B. □

**Proof of Proposition 2.3:**

*Proof.* By induction on the structure of M.

Proof of the first clause:

Case *M = V:* *(M/v)N = [M/v]N*

By the rule Val, A; F h *M ~ A* implies A; • h M : A

By Lemma A.2, we have A; F h *[M/v]N : B.*

Therefore A; F h *(M/v)N : B.*

Case *M* = letbox *x* = *Mi* in *M^* *(M/v)N* = letbox x = Mi in *{M2/v)N*

By the rule DE[7], A; T h M - A implies A; T h Mi : HL4iandA,x ::Ai;rhM$_2$ ~ A

By weakening, *A,v ~ A;T \- N : B* implies *A,v ~ A,x :: Ai;F h N : B.*

By induction hypothesis on M2, A, *x :: A\;* F h *(M2/v)N* : *B.*

By the rule DE[7], A; F h letbox *x = $M_x$* in *($M_2$/v)N : B.*

Therefore A; *T* h *(M/v)N : B.*

Case M = letcir it; = Mi in M2: *(M/v)N* = letcir w = Mi in *{M2/v)N*

By the rule OE', *A^Th M ~ A* implies A; T h $M_x$ : O^4i and A ^ ~ i i ; n - M$_2$ ~ A

By weakening, *A,v ~ A;T\- N : B* implies *A,v ~ A,w ~ Ai;T \- N : B.*

By induction hypothesis on M2, A, *w* ~ J4I; F h *(M2/v)N* : B.

By the rule OE', A; T h letcir w = $M_x$ in *($M_2$/v)N : B.*

Therefore A; T h *(M/v)N : B.*

Proof of the second clause:

Case M = *V:* *(M/v)N = [M/v]N*

By the rule Val, *A;T h M ~ A* implies A; • h M : A

By Lemma A.2, we have A; *T* h [Af/v]JV ~ B.

Therefore A; *T* h *(M/v)N ~* J5.

Case M = letbox x = Mi in M2: *(M/v)N* = letbox x = Mi in *(M2/v)N*

By the rule DE[7], A; T h M ~ ^4 implies A; T h Mi : QAi and A, x :: Ai; T h M$_2$ ~ A.

By weakening, *A,v ~ A;T \- N ~ B* in^lies A,*v ~ A,x :: Ai;T* h *N ~ B.*

By induction hypothesis on M2, A, *x* :: *A\;* F h *(M2/v)N ~ B.*

By the rule DE', A; F h letbox x = $M_x$ in *($M_2$/v)N ~ B.*

Therefore A; F h *(M/v)N ~* S.

Case M = letcir it; = Mi in $M_2$: *(M/v)N* = letcir it; = Mi in ($M_2$/v)AT

By the rule OE[7], A; F h M ~ A implies A; F h Mi : O^4i and A, w ~ ^1; F h M$_2$ ~ A

By weakening, A,v~A;FI-iV~5 implies *A,v ~ A,w ~ Ai;F\- N ~ B.*

By induction hypothesis on M2, A, *w ~ A±; T* h *(M2/v)N* ~ B.

By the rule OE[7], A; F h letcir it; = $M_x$ in *($M_2$/v)N* ~ S.

Therefore A; F h *(M/v)N ~* 5.

□

**Proof of Proposition 2.5:**

*Proof.* By induction on the structure of the derivation of A; F h M ~ A

Case $\dfrac{\Delta; \cdot \vdash \quad A}{\Delta; \Gamma \vdash \quad A}$ Val and $M = V$:

By weakening, *A;-\-V : A* implies *A;F h V : A.*

Therefore A; F h M : A

Case $\dfrac{\text{A;F h Mi : } HAi \quad \text{A,x :: } A_1;T\text{\-}M_2\text{^}A}{\text{A;Fhletboxx = MiinM}_2\text{^^}}$ DE ' and M = letbox x = Mi in $M_2$:

By induction hypothesis on A, x :: *Ai;* F h $M_2$ ~ A, we have A, x :: J4X; F h $M_2$ : A

By the rule $\Box$E, $\Delta; \Gamma \vdash \text{letbox } x = M_1 \text{ in } M_2 : A$

Therefore $\Delta; \Gamma \vdash M : A$.

Case $\dfrac{\Delta; \Gamma \vdash M_1 : \bigcirc A_1 \quad \Delta, v \sim A_1; \Gamma \vdash M_2 \sim A}{\Delta; \Gamma \vdash \text{letcir } v = M_1 \text{ in } M_2 \sim A} \bigcirc\text{E}'$ and $M = \text{letcir } v = M_1 \text{ in } M_2$:

By induction hypothesis on $\Delta, v \sim A_1; \Gamma \vdash M_2 \sim A$, we have $\Delta, v \sim A_1; \Gamma \vdash M_2 : A$.

By the rule $\bigcirc$E, $\Delta; \Gamma \vdash \text{letcir } v = M_1 \text{ in } M_2 : A$.

Therefore $\Delta; \Gamma \vdash M : A$.

Case $\dfrac{\Delta; \Gamma \vdash M : A}{\Delta; \Gamma \vdash M \sim A}$ Prim$\sim$

The premise gives $\Delta; \Gamma \vdash M : A$. □

# B Proofs of the properties of $\lambda_{\Box\bigcirc}^{W}$

Proof of Proposition 3.1:

**Lemma B.1.** *$[M/x]V$ is a value.*

*Proof.* By case analysis of $V$. □

*Proof.* By induction on the structure of the derivation of $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$.

If $N = V$ and the rule Val$_W$ is used to deduce $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$:

$\Delta; \Gamma, x : A @ \omega'' \vdash_{\omega'} N : B$.

By induction hypothesis, $\Delta; \Gamma \vdash_{\omega'} [M/x]N : B$.

By the rule Cvar$_W$, $\Delta; \Gamma \vdash_\omega [M/x]N \sim B @ \omega'$ because $[M/x]N$ is a value by Lemma B.1.

If the rule Prim$\sim_W$ is used to deduce $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$:

$\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N : B$ and $B$ is a primitive type.

By induction hypothesis, $\Delta; \Gamma \vdash_\omega [M/x]N : B$.

By the rule Prim$\sim_W$, $\Delta; \Gamma \vdash_\omega [M/x]N \sim B @ \omega'$.

Now we assume that the rules Cvar$_W$ and Cvar$_W$ are not used to deduce $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$.

Case $N = x$: $\quad [M/x]N = M$

By the rule Cvar$_W$, $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$ implies $A = B$ and $\omega = \omega' = \omega''$.

$\Delta; \Gamma \vdash_{\omega''} M : A$ implies $\Delta; \Gamma \vdash_{\omega''} [M/x]N : A$.

Therefore $\Delta; \Gamma \vdash_\omega [M/x]N \sim B @ \omega'$.

Case $N = y, y \neq x$: $\quad [M/x]N = y$

By the rule Cvar$_W$, $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$ implies $y :: B \in \Delta$ or $y : B @ \omega \in \Gamma, x : A @ \omega''$, and $\omega = \omega'$.

Since $y \neq x$, we have $y :: B \in \Delta$ or $y : B @ \omega \in \Gamma$.

By the rule Cvar$_W$, $\Delta; \Gamma \vdash_\omega y : B$.

Therefore $\Delta; \Gamma \vdash_\omega [M/x]N \sim B @ \omega'$.

Case $N = v$: $\quad [M/x]N = v$

By the rule Vvar$_W$, $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$ implies $v \sim B \in \Delta$ or $v \sim B @ \omega \in \Gamma, x : A @ \omega''$, and $\omega = \omega'$.

Since $v \neq x$, we have $v \sim B \in \Delta$ or $v \sim B @ \omega \in \Gamma$.

By the rule Vvar$_W$, $\Delta; \Gamma \vdash_\omega v : B$.

Therefore $\Delta; \Gamma \vdash_\omega [M/x]N \sim B @ \omega'$.

Case $N = \lambda y{:}B'.\, N'$, $y \neq x$, $y$ not a free variable of $M$: $\quad [M/x]N = \lambda y{:}B'.\, [M/x]N'$

By the rule $\supset$I$_W$, $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$ implies $\Delta; \Gamma, x : A @ \omega'', y : B' @ \omega \vdash_\omega N' : B''$, $B = B' \supset B''$, and $\omega = \omega'$.

By weakening, $\Delta; \Gamma \vdash_{\omega''} M : A$ implies $\Delta; \Gamma, y : B' @ \omega \vdash_{\omega''} M : A$.
By induction hypothesis, $\Delta; \Gamma, y : B' @ \omega \vdash_\omega [M/x]N' : B''$.
By the rule $\supset\mathsf{I}_W$, $\Delta; \Gamma \vdash_\omega \lambda y{:}B'. [M/x]N' : B' \supset B''$.
Therefore $\Delta; \Gamma \vdash_\omega [M/x]N \sim B @ \omega'$.

Case $N = N_1\ N_2$: $[M/x]N = [M/x]N_1\ [M/x]N_2$
By the rule $\supset\mathsf{E}_W$, $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$ implies $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N_1 : B' \supset B$, $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N_2 : B'$, and $\omega = \omega'$.
By induction hypothesis, $\Delta; \Gamma \vdash_\omega [M/x]N_1 : B' \supset B$ and $\Delta; \Gamma \vdash_\omega [M/x]N_2 : B'$.
By the rule $\supset\mathsf{E}_W$, $\Delta; \Gamma \vdash_\omega [M/x]N_1\ [M/x]N_2 : B$.
Therefore $\Delta; \Gamma \vdash_\omega [M/x]N \sim B @ \omega'$.

Case $N = \mathsf{box}\ N'$: $[M/x]N = \mathsf{box}\ [M/x]N'$
By the rule $\Box\mathsf{I}_W$, $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$ implies $\Delta; \Gamma, x : A @ \omega'' \vdash_{\omega^*} N' : B'$, $B = \Box B'$, and $\omega = \omega'$ where $\omega^*$ is a fresh node.
By induction hypothesis, $\Delta; \Gamma \vdash_{\omega^*} [M/x]N' : B'$.
By the rule $\Box\mathsf{I}_W$, $\Delta; \Gamma \vdash_\omega \mathsf{box}\ [M/x]N' : \Box B'$.
Therefore $\Delta; \Gamma \vdash_\omega [M/x]N \sim B @ \omega'$.

Case $N = \mathsf{box}_{\omega^*}\ N'$: $[M/x]N = \mathsf{box}_{\omega^*}\ [M/x]N'$
By the rule $\Box\mathsf{I}'_W$, $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$ implies $\Delta; \Gamma, x : A @ \omega'' \vdash_{\omega^*} N' : B'$, $B = \Box_{\omega^*} B'$, and $\omega = \omega'$.
By induction hypothesis, $\Delta; \Gamma \vdash_{\omega^*} [M/x]N' : B'$.
By the rule $\Box\mathsf{I}'_W$, $\Delta; \Gamma \vdash_\omega \mathsf{box}_{\omega^*}\ [M/x]N' : \Box_{\omega^*} B'$.
Therefore $\Delta; \Gamma \vdash_\omega [M/x]N \sim B @ \omega'$.

Case $N = \mathsf{letbox}\ y = N_1\ \mathsf{in}\ N_2$, $y \neq x$, $y$ not a free variable of $M$:
$[M/x]N = \mathsf{letbox}\ y = [M/x]N_1\ \mathsf{in}\ [M/x]N_2$
If the rule $\Box\mathsf{E}_W$ is used to deduce $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$,
$\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$ implies $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N_1 : \Box B_1$ and $\Delta, y :: B_1; \Gamma, x : A @ \omega'' \vdash_\omega N_2 \sim B @ \omega'$.
By weakening, $\Delta; \Gamma \vdash_{\omega''} M : A$ implies $\Delta, y :: B_1; \Gamma \vdash_{\omega''} M : A$.
By induction hypothesis, $\Delta; \Gamma \vdash_\omega [M/x]N_1 : \Box B_1$ and $\Delta, y :: B_1; \Gamma \vdash_\omega [M/x]N_2 \sim B @ \omega'$.
By the rule $\Box\mathsf{E}_W$, $\Delta; \Gamma \vdash_\omega \mathsf{letbox}\ y = [M/x]N_1\ \mathsf{in}\ [M/x]N_2 \sim B @ \omega'$.
Therefore $\Delta; \Gamma \vdash_\omega [M/x]N \sim B @ \omega'$.
If the rule $\Box\mathsf{E}'_W$ is used to deduce $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$,
$\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$ implies $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N_1 : \Box_{\omega^*} B_1$ and $\Delta; \Gamma, x : A @ \omega'', y : B_1 @ \omega^* \vdash_\omega N_2 \sim B @ \omega'$.
By weakening, $\Delta; \Gamma \vdash_{\omega''} M : A$ implies $\Delta; \Gamma, y : B_1 @ \omega^* \vdash_{\omega''} M : A$.
By induction hypothesis, $\Delta; \Gamma \vdash_\omega [M/x]N_1 : \Box_{\omega^*} B_1$ and $\Delta; \Gamma, y : B_1 @ \omega^* \vdash_\omega [M/x]N_2 \sim B @ \omega'$.
By the rule $\Box\mathsf{E}'_W$, $\Delta; \Gamma \vdash_\omega \mathsf{letbox}\ y = [M/x]N_1\ \mathsf{in}\ [M/x]N_2 \sim B @ \omega'$.
Therefore $\Delta; \Gamma \vdash_\omega [M/x]N \sim B @ \omega'$.

Case $N = \mathsf{cir}\ N'$: $[M/x]N = \mathsf{cir}\ [M/x]N'$
By the rule $\bigcirc\mathsf{I}_W$, $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$ implies $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N' \sim B' @ \omega^*$, $B = \bigcirc B'$, and $\omega = \omega'$ where $\omega^*$ is a fresh node.
By induction hypothesis, $\Delta; \Gamma \vdash_\omega [M/x]N' \sim B' @ \omega^*$.
By the rule $\bigcirc\mathsf{I}_W$, $\Delta; \Gamma \vdash_\omega \mathsf{cir}\ [M/x]N' : \bigcirc B'$.
Therefore $\Delta; \Gamma \vdash_\omega [M/x]N \sim B @ \omega'$.

Case $N = \mathsf{cir}_{\omega^*}\ N'$: $[M/x]N = \mathsf{cir}_{\omega^*}\ [M/x]N'$
By the rule $\bigcirc\mathsf{I}'_W$, $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'$ implies $\Delta; \Gamma, x : A @ \omega'' \vdash_\omega N' \sim B' @ \omega^*$, $B = \bigcirc_{\omega^*} B'$, and $\omega = \omega'$.

By induction hypothesis, A; F h^ $[M/x]N^f$ ~ $B'$ © $u$*.
By the rule $Ol^7$^, A; F K, cir $\backslash M/x]N'$: $O$^$B^f$.
Therefore A; F h^ $[M/x]N$ ~$B$@$d$.

Case $N$ = letcir $v$ = $N$± in AT₂, v not a free variable of M: $[M/x]N$ = letcir $v$ = [M/x]ATi in $[M/x]N_2$

If the rule OEjy is used to deduce A; F, $x$ : $A$ © $d^1$ $h_w$ $N$ ~ $B$ © $d$,
$A\backslash T,x:A@d^f\backslash$-$_{UJ}N$^$B@d$ implies A;F,x : $A$ © $d^f$ h^ $N_x$ : OSi and A,t; - Si;T,x : $A$ © $d'$ \-$_u$ $N_2$ ~ $B$ © $d$.
By weakening, A; F h^/ M : A implies A, $v$ ~ $B$\\ F h^// $M$ : $A$.
By induction hypothesis, A; F h^ [M/x]ATi : $OBi$ and A, i; ~ J5i; T h^ [Af/xJiV^ ~ $B@u^f$.
By the rule OEvr, A; $T$ h^ letcir v = $[M/x]N$± in [M/x]A^₂ ~ $B$ @ $d$.
Therefore A; $T$ h^ $[M/x]N$ - B @ $u'$.

If the rule OE^ is used to deduce A; T, $x$ : ^4 @ $d'$ h^ iV ~ 5 @ a;',
A;T,x : ^ @ $a;^{7'}$ h^ AT ~ $B$ @ $a;^7$ impUes A;T,x : $A$ @ $d'$ \-$_u$ $N_x$ : $O_w$*Bi and A;T,a: :$A@d',v$~$B_1@u$;*\-$_{UJ}N2$~$B@$ $d$.
By weakening, A; F h^// M : ^4 implies A; F, v ~ $B$\ @ a;* h^// M : A.
By induction hypothesis, A; F h^ [Af/x]JVi : Oa;*^! and A; F, $v$ ~ $B$\ @ a;* h^ [M/x]AT₂ ~ S @ $a;^7$.
By the rule $OE^7$^, A; F h^ letcir v = [M/x]$N_x$ in [M/x]AT₂ ~ S @ $d$.
Therefore A; F h^ $[M/x]N$ ~ $B@d$. D

Proof of Proposition 3.2:

*Proo/* By induction on the structure of the derivation of A, $x$ :: A; F h^ AT ~ $B$ @ $d$.
If AT = $V$ and the rale $Va\backslash_w$ is used to deduce A, $x$ :: A; F h^ AT ~ J5 © $d$:
$\Delta, x :: A; \Gamma \vdash_{\omega'} N : B$.
By induction hypothesis, A; F h^/ [M/x]$N$ : $B$.
By the rule Cvarws A; F h^ $[M/x]N$ ~ $B$ @ $d$ because $[M/x]N$ is a value by Lemma B.I.
If the rale Prim~vr is used to deduce A, x :: A; F h^ AT ~ $B$ © $d$:
A, x :: ^4; F h^ AT: $B$ and S is a primitive type.
By induction hypothesis, A; F h^ $[M/x]N$ : $B$.
By the rale Prim~vr, A; F h^ [M/x]AT ~ $B@d$.
Now we assume that the rales Cvarvr and Cvarvr are not used to deduce A, x :: $A$; $T$ h^ AT ~ $B$ @ $d$.
Case AT = x: $[M/x]N = M$
By the rale Cvarvr, $A$,$x$ :: $A]T$ $h$^ $N$ ~ $B$ @ $d$ implies $A$ = $B$ and $u$) =— $d$.
A; F \-$_u$$n$ $M$ : $A$ implies A; F h^ M : $A$.
Therefore A; F h^ $[M/x]N$ ~$B$@$d$.
Case $N$ = $y$,$y$ ^ $x$: $[M/x]N$ = $y$
By the rale Cvarvr, $A$,$x$ :: $A$;$F$ $h$^ $N$ ~ $B$ © $u$/ implies $y$ :: $B$ G A,x :: $A$ or y : B © $w$ G F, and $LJ$ = $d$.
Since y ^ x, we have y::BG Aorj/:jB@a;Gr.
By the rale Cvarns A; F \-$_u$ $y$ : $B$.
Therefore A; F h^ $[M/x]$ $N$ ~$B$@$d$.
Case $N$ = $v$: $[M/x]N$ = $v$
By the rule Vvarvr, A, x :: $A$; $T$ h^ AT ~ B @ $u;^7$ implies $v$ ~ $B$ G A, x :: A or v ~ B @ a; G F, and $u$)=$d$.
Since $v$ ^ x, we have v ~ B G $\Delta$ or $v \sim B$ @ $\omega \in \Gamma$.
By the rule Vvarvr, A; F h^ i;: $B$.
Therefore A; F h^ $[M/x]$ $N$ ~$B$@$d$.
Case $N$ = $Xy$: $B^f$. $N$\ $y$ ^ x, y not a free variable of M: [M/x]AT = Ay: $B^f$. $[M/x]$ $N'$

By the rule Dl^, A, x :: A;T h^ AT - B @ u;7 implies A, x :: A;T,y : B' @ u> K, AT7: B\B = B' D B", and u = d,

By weakening, A; F h^/ M : A implies A; I\ y : B' @ a; h^// M : A

By induction hypothesis, A;T,y : B' @ Luh^ [M/x]N' : B".

By the rule D\w, A; F h^ A</:B7. [M/x]AT7 : B' D B".

Therefore A; F h^ [M/x]N ~ B@d.

Case N = NX N2: [M/x]N = [M/x]Nx [M/x]N2

By the rule DEW, A, x :: A; F h^ N ~ 5 @ d implies A, x :: A; F h^ Ni : B' D B9 A,x :: A;T h^ AT2 : B7, and u> = d.

By induction hypothesis, A; F h^ [M/x]N± : B' D B and A; F h^ [M/x]N2 : B'.

By the rule DEW, A; F hu [M/x]Ni [M/x]N2 : B.

Therefore A; V hw [M/x]N - B & d.

Case AT = box N': [M/x]N = box [M/x] AT7

BytheruleDlvr, A,x :: A;T h^ N ~ B@ d implies A, x :: A\Y\-^ N' : B\B = QB7,andu; = d where OJ* is a fresh node.

By induction hypothesis, A; T h^* [M/x] AT7: B'.

By the rule U\w> A; T h^ box [M/x]AT7 : DB'.

Therefore A; T h^ [M/x]AT ~ B @ d.

Case AT = box^* N': [M/x]N = box^* [M/x]AT7

By the rule Dl7^, A,x :: A;T h^ N ~ B @ d implies A,x :: A;T h^ AT7 : B\ B = D^B7, and $\omega = \omega'$.

By induction hypothesis, A; T h^* [M/x] AT7: B7.

By the rule Dl7^, A; T h^ box^* [M/x]AT7 : U^B'.

Therefore A; T h^ [M/x] AT ~ B@d.

Case N = letbox y = Ni in AT2, y ^ x,y not a free variable of M:

[M/x]AT = letbox y = [M/x]Nx in [M/x]N2

If the rule DEvr is used to deduce A, x :: A; T h^ N ~ i? @ a;7,

A, x :: A; F h^ AT ~ B @ d implies A, x :: A; T h^ ATX : QBi and A., 2/ B\.,x '.'. A\ F h^ N2 rsj B @ UJ'.

By weakening, A; F Y^" M : A implies A, y :: B\\ F h^// M : A.

By induction hypothesis, A; F h^ [M/x]N\ : OBi and A, y :: £?i; F h^ [M/x]AT2 ~ B @ d.

By the rule DE^, A; F h^ letbox y = [M/x]Ni in [M/x]AT2 ~ B @ d.

Therefore A; F h^ [M/x]AT - B @ d.

If the rule DE7^ is used to deduce A, x :: A\ F h^ N ~ B @ a;7,

A, x :: A; F h^ AT ~ B @ d implies A, x :: A; F h^ A^i : Q^*J3i and A, x :: A; F, y : Bx @ v* h^ AT2 ~ B @ c;7.

By weakening, A; F h^// M : A implies A; F, y : B\ @ w* h^/ M : A.

By induction hypothesis, A;F h^ [M/x]Ni : D^Bi and A; F, y : Bx @ LJ* h^ [M/x]AT2 ~ J5 @ a;7.

By the rule DE7^, A; F h^ letbox y = [M/x]Nx in [M/x] AT2 ~ J5 @ d.

Therefore A; F h^ [M/x]N ~ B @d.

Case AT = cir AT7: [M/x] AT = cir [M/x] AT7

By the rule Ol^, A, x :: A; F h^ AT ~ B @ d implies A, x :: A; T h^ N' ~ B' @ u>*9 B = OB\ and u) = d where a;* is a fresh node.

By induction hypothesis, A; F h^ [M/x]N' ~ B' @ a;*.

By the rule Olw, A; F h^ cir [M/x]AT7 : OB7.

Therefore A; F h^ [M/x] AT ~ B @ a;7.

Case N = cir^* AT7: [M/x]N = cir^* [M/x]AT7

By the rule Ol'^, A,x :: *A;T* h^ *N* ~ *B* @ u/ implies A,x :: *A;T h^ N'* ~ $B^1$ @ a;*, 5 = O^B', and a; = a;[7].

By induction hypothesis, A; F h^ [M/x]$AT^7$ ~ $B^7$ @ a;*.

By the rule Ol'^, A; F $\backslash\text{-}_u$ cir *[M/x)*$N^r$: $O_w$.*B'*.

Therefore A; F h^ *[M/x]N ~B@u'.*

Case AT = letcir *v* = *N*± in $AT_2$, t; not a free variable of *M:* *[M/x]N* = letcir *v* = *\M/x]N* in [M/x]$AT_2$

If the rule OEvr is used to deduce A, x :: A;F h^ *N* ~ j? @ a;[7],

A,x::^4;FK; *N* ~ *B* @ *w'* implies A,x :: ^4;T h^ ATi : OJ5i and *A,v~Bi,x* :: AjTho, $AT_2$ ~ *B* @ *J.*

By weakening, A; F Ky/ M : *A* implies A, *v* ~ *B*\\ *T* $h_w$// M : ^4.

By induction hypothesis, A; *T* $h_u$ *[M/x]N* : *OBi* and A, v ~ $B_x$; T h^ [M/x]$AT_2$ ~ B @ a;[7].

By the rule OE^r, A; *V* $h_u$ letcir *v* = *[M/x]Ni* in *[M/x]*$N_2$ ~ *B@v'.*

Therefore A; *T* h^ *[M/x]N* ~ *B* @ *J.*

If the rule $OE^7$^ is used to deduce A, *x :: A; T* h^ *N* ~ *B* @ *J,*

A,*x*::A;*V*h^AT~J5@*J* implies A, x :: *A\ T* h^ $AT_X$ : $O_{(JJ}{}^*B_1$ and A, x :: *A; T*%*v* ~ $B_x$ @ a;* h^ $AT_2$ ~ *B* @ a;[7].

By weakening, A; F h^// M : *A* implies A; F, t; ~ Bi @ a;* h^/ M : A.

By induction hypothesis, A; F h^ [M/x] JVi : O^* $B_x$ and A; F, *v* ~ Si @ a;* h^ [M/x]$AT_2$ ~ *B* @ a;[7].

By the rule $OE^7$^, A; F h^ letcir *v* = *[M/x]Nx* in *[M/x]*$N_2$ ~ *B* @ a;[7].

Therefore A; F h^ [M/x]iV - S @ *J.* *U*

**Proof of Proposition 3.3:**

***Proof.*** By induction on the structure of the derivation of A; F, *v* ~ *A* @ u;[77] h^ JV ~ *B* @ a;[7].

If *N* is a value and the rule Val^ is used to deduce A; F, *v* ~ *A* @ *J'* h^ AT ~ *B* @ a;[7]:

*A;T,v~A@u;"*$\backslash\text{-}_{u;}$*<N:B.*

By induction hypothesis, A; F h<y [V/v] JV : B.

By the rule Cvarvr, A; F h^ *[V/v]N* ~ S @ *J* because *[V/v]N* is a value by Lemma B.I.

If the rule Prim~vr is used to deduce A; F, *v* ~ *A* @ $J^1$ $\backslash\text{-}_u$ *N* ~ *B* @ u;[7]:

A; F, *v* ~ A @ a?[77] $\backslash\text{-}_u$ *N : B* and *B* is a primitive type.

By induction hypothesis, A; F h^ *[V/v]N* : *B.*

By the rule Prim~vr, A; F h^ [V/v]iV ~ *B* @ *J.*

Now we assume that the rules Cvar^ and Cvarvr are not used to deduce A; F, *v* ~ *A* @ a;[77] h^ *N* ~ B @ a?[7].

Case AT = x: [V/v]JV = x

BytheruleCvarvr, A;F,v ~ A @ a;[77] h^ AT ~ *B* @ a;[7]impliesx ::BG Aorx : *B* @ *u e T,v* ~ *A* @ *u/* and *u)* = a;[7].

Since x ^ v, we have x::BGAorx:B@a;Gr.

By the rule Cvarvr, A; F h^ x : B.

Therefore A; F h^ [F/v]A^ - *B* @ *J.*

Case AT = *v:* *[V/v]N* = *V*

By the rule Vvarvr, A; F, *v* ~ *A* @ $J^1$ h^ AT ~ *B* @ *J* implies *A* = *B* and *u;* = a;[7] = a/[7].

A;F h^/ F : A implies A;F h^ *V : B.*

Therefore A; F h^ *[V/v]N* ~ S @ a;[7].

Case *N* = *w,w* ^ *v:* *[V/v]N* = *w*

BytheruleVvarty,A;F,i; ~ A @ a;[77] h^ AT ~ *B* @ a;[7] implies K; ~ B G Aorit; ~ B @ a; €F,v~^4@a;″, and a; = u;[7].

Since *w* ^ v, we have ti;~BG Aor^~B@o;Gr.

By the rule Vvar^, A; F h^ it; : *B.*

Therefore A; $T$ \-$_w$ *[V/v]N ~B@J.*

Case $N$ = *Xx:B'*. AT, *x* not a free variable of V: *[V/v]N* = Ax: *B'*. *[V/v]N'*

By the rule Dlw, *A;T,v ~ A* Qu/'h, *N ~* 5 @ u>' implies A; I\ *v* ~ 4 @ u/',x : *B' @u*\-$_w$ *N' : B"*, *B = B' D B"*, and *u = u'*.

By weakening, A; *T* hy *V : A* implies A; *T, x : B' @ u* \-$_w$*" V : A*.

By induction hypothesis, A; *T, x : B' @ u* \-$_u$ *[V/v}N' : B"*.

By the rule *D*\$_w$, A; T \-$_u$ Ax :£'. *[V/v)N$^f$: B'* D *B"*.

Therefore A; *T* h$_w$ *[V/v]N ~ B @ J*.

Case *N = Ni N$_2$:* *[V/v]N = \V/v]Ni [V/v)N$_2$*

By the rule *DE$_W$*, A;T,V ~ *A @ J$^1$* \-$_w$ *N ~ B @ J* impUes A;T,u ~ *A* @ w" h^ *Ni : B' D B*, A;T,*v* ~ ^4 @ *u"* h$_w$ iV$_2$ : B', and w = a;'.

By induction hypothesis, A; *T* \-$_u$ *[V/v]Ni : B' D B* and A; T *h$_u$* *[V/v]N$_2$* : £'.

By the rule DE^, A; *T* h^ [V7t;]JVi [F/v]AT$_2$ : *B*.

Therefore A; *T* h$_w$ *[V/v]N ~* 5 @ u/.

Case AT = box AT: [V/t;]JV = box [V/v]^'

By the rule *D*\$_w$, A;T,t; ~ *A @ u" h$_u$ N ~ B* @ u/ implies A; T, v ~ *A* @ w" h^ JV' *:B',B* = OB', and u; = *u/* where w* is a fresh node.

By induction hypothesis, A; *T* \-^* *[V/v)N$^f$ : B'*.

By the rule *U*\$_w$, A; *V h$_u$* box *[V/v)N' : DB'*.

Therefore A; *T* h^ *[V/v]N ~B@u>'*.

Case AT = box^ *N':* *[V/v]N* = box^ *[V/v]N'*

By the rule Dl'^, *A;T,v ~ A @ J'* h^ iV ~ *B* @ a/ impUes A; T, v ~ y4 @u/' !-,,,. *N' :B',B = D^B'*, and *u>* = o»'.

By induction hypothesis, A; *T* !-,,,. [V/u] A$^{77}$ : B'.

By the rule Dl^, A; *T* h^ box^ *[V/v]N'* : D^.B'.

Therefore A;*T*\-$_u$ *[V/v]N ~B@u;'*.

Case *N* — letbox x = *Ni* in A^, x not a free variable of *V:*

*[V/v]N* = letbox x = *[V/v]^* in *[V/v]N$_2$*

If the rule DEvr is used to deduce A; *T, v ~ A* @ w" h$_w$ AT ~ B @ a;',

A; T, v ~ *A* @ a/' h^ AT ~ B @ a;' implies A; T, v ~ *A* @ a;" h^ ATi : DBi and A,x :: *Bi;T,v~ A@ J'* t-$_w$ AT$_2$ ~ *B @ J*.

By weakening, A; F h^" V : *A* implies A, x :: *B*\\ *T* \-^*t V : A*.

By induction hypothesis, A; T \-$_w$ *[V/v]Ni : DBi* and A,x :: *B*\; *T h$_u$ [V/v]N$_2$ ~ B @ J*.

By the rale DE$_W$, A; *T* h^ letbox x = *\V/v]Ni* in [V/wjA^ ~ *B @ J*.

Therefore A; *T h$_w$ [V/v)N* ~ B @ *J*.

If the rale DE^ is used to deduce A; I\ *v* ~ ^4 @ *J'* h^ AT ~ B @ *J*,

*A;T,v~A@u;"*\-$_u$*,N~B@u;'* impUes A;T,v ~ *A* @ *u>"* h$_w$ JVi : DwBi and $\Delta;\Gamma, v \sim A \,@\, \omega'', x : B_1 \,@\, \omega^* \vdash_\omega N_2 \sim B$ @ u/.

By weakening, A; *T* \-$_w$» *V : A* implies A; T, x : *Bi* @ u;* h^// V : A.

By induction hypothesis, A; *T* h$_w$ [F/v]ATx : D^Bi and A; T, x : *Bi* @ *u** h$_w$ [F/v]AT$_2$ ~ *B* @ <*;'.

By the rale DE'^, A; T h$_w$ letbox x = *[V/v]Ni* in [V/u] AT$_2$ ~ *B @ J*.

Therefore A; *T* h$_w$ [V/w]JV ~ B @ u/.

Case AT = cir AT: *[V/v]N* = cir *[V/v]N$^f$*

By the rule Olw, A; *T,v* ~ A @ *u"* \-$_u$ *N* ~ B @ <*J* implies A;T,u ~ *A @ J'* \-$_w$ *N' ~ B' @ u**, *B = OB'*, and *OJ* = <*J* where a;* is a fresh node.

By induction hypothesis, A; *T* \-$_w$ *[V/v]N' ~ B'* @ w*.

By the rule *O*\$_w$, A; T h$_w$ cir *[V/v]N$^f$* : OB'.

Therefore A;T $h_w$ *[V/v]N ~B@u'.*

Case *N* = cir^ *N':* *[V/v]N* = cir^* *[V/v)N*$^f$

By the rule *O\'*$_w$, A;T,i; ~ ,4 @ u/$^7$ K, *N ~ B © J* implies *A;T,v~ A@ d' \-» N' ~ B' @* a% B = *Ou*B'*$_9$ and u; = a/.

By induction hypothesis, A; *T* h^ [V/vjAT$^7$ ~ £' © a;*.

By the rule Ol$^7$^, A; T \-$_u$ cir [V/v]^ : CV#$^7$.

Therefore A; *T* h^ [V/v]*N ~B@d.*

Case AT = letcir *w* = *Ni* in iV$_2$, *w^v,w* not a free variable of *V:* *[V/v]N* = letcir it; = *[V/v]Ni* in [V/v]*N*$_2$

If the rule OEvr is used to deduce A; I\ v ~ *A* © u/$^7$ K, AT ~ 5 © a;$^7$,

A; T, i; ~ ^4 © *u"* h^ iV ~ 5 © *J* implies A; T, *v ~ A* © a;$^{:/}$ h^ iVi : OBi and A, *w* - Si; T, *v ~ A* © u;$^{77}$ K, iV$_2$ ~ S © u/.

By weakening, A; T h^// V : ^4 implies A, it; ~ Si; T h^/ V : A.

By induction hypothesis, A; *T* h^ *[V/v]Ni :* O^i and A, *w* ~ .Bi; T h^ *[V/v]N*$_2$ *~ B@v'.*

By the rule OE^, A; *T* h^ letcir *w = [V/v]Ni* in [V/v]*N*$_2$ ~ *B* © a;$^7$.

Therefore A; T h^, [V/v]AT - 5 @ ^$^7$.

If the rule OE$^7$^ is used to deduce A; I\ *v ~ A* © a;$^{77}$ h^ iV ~ S © a/,

A;T,v~ ^©a;$^{77}$!-^ *N ~ B @ u'* implies A;I\v ~ A © *u"* \-$_u$ *N*$_\pm$ *: O^Bx* and A; T, *v* ~ A © a;$^{77}$, it; ~ 5i © a;* h^ AT$_2$ ~ B © a;$^7$.

By weakening, A; *T* h^/ V": A implies A; T, it; ~ Bi © a;* h^/ F : A.

By induction hypothesis, A; T h^ *[V/v]Ni* : Oa;* Si and A; T, it; ~ 5i © *u** h^ [V/v]A^$_2$ ~ *B* © a;$^7$.

By the rule OE$^7$^, A; T h^ letcir n; = [V7v]iVi in *[V/v]N*$_2$ *~B@CJ'.*

Therefore A; *T* h^ *[V/v]N ~B@v'.* *D*

**Proof of Proposition 3.4:**

*Proof* By induction on the structure of the derivation of A, *v ~ A; T* h^ *N ~ B @ ω'*.

If *N* is a value and the rule Valjy is used to deduce A, *v ~ A; T* \-$_u$ *N ~ B* © a/:

$\Delta, v \sim A; \Gamma \vdash_{\omega'} N : B$.

By induction hypothesis, A; T *h^ [V/v]N : B.*

By the rule Cvarjy, A; *T* h^ *[V/v]N ~ B @* a/ because [F/v]JV is a value by Lemma B.I.

If the rule Prim^vr is used to deduce A, *v ~ A; T* h^ AT ~ *B* © a;$^7$:

A, v ~ ^4; F h^ AT: i? and B is a primitive type.

By induction hypothesis, A; *T* h^ *[V/v]N : B.*

By the rule Prim~w, A; T h^ [V/v]AT ~ *B* © u/.

Now we assume that the rules Cvarvr and Cvar^ are not used to deduce A, *v ~ A; T* h^ *N ~ B @* u;$^7$.

Case AT = x: [V/v]iV = ar

By the rule Cvar^, A, v ~ *A; T* h^ AT ~ *B* © a/ implies x::i? G A,v~Aorx:B@o? G T, and *UJ* = CJ$^7$.

Since x ^ *v,* we have x::J5G Aorx:B@(jGr.

By the rule Cvarvr, AjTh^xiB.

Therefore A; T h^ [V/v]JV - *B* @ a;$^7$.

Case *N = v:* *\V/v]N = V*

By the rule Vvarvr, A, v ~ *A; T* h^ AT ~ *B* © a;$^7$ implies A = 5 and a; = a;$^7$.

A; T *\~u» V* : A implies A; *T* h^ V : *B.*

Therefore A; *T* h^ *[V/v]N ~ B* © a/.

Case *N = w,w ^v:* *[V/v]N = w*

By the rule Vvarw, A, t; ~ A; T h^ AT ~ S @ *d* implies it;~5GA,v~^4orit;^-B@a;Gr, and *U)* == *(JU'*.

Since *w* ^ *v,* we have *w~B(z̄* Δ or *w* ~ *B* @ *ω* ∈ Γ.

By the rule Vvarvr, A; *T h^ w* : B.

Therefore A; *T* h^ *[V/v]N ~B@UJ'.*

Case *N* = *\x: B'*. AT[7], *x* not a free variable of *V:* *[V/v]N = Xx:B'. [V/v]N'*

BytheruleDlvr, A,v - A;T h^ AT ~ B Q *UJ'*implies A, v ~ A;I\x : B[7] @ u; K; A/[7] : *B",B* = $B^f$ *D* B", and a; = a;'.

By weakening, A; T Ky/ *V* : A implies A; *T,* x : B[7] @ *UJ* h^// V : A.

By induction hypothesis, A; I\ *x : B'* © *UJ* h^ *[V/v]N'* : B".

By the rule $D\_w$, A; r K, Ax: B[7]. [V>]iV[7] : *B'* D B".

Therefore A; *T* h^ [F/v] AT - *B @ J.*

Case AT = $N_x$ $N_2$: *[V/v]N = \Vfv\Nx [V/v]$N_2$*

By the rule $DE_W$, A, *v* ~ A; T h^ *N ~ B @ J* implies A, *v ~ A; T t-^* $N_x$ *: B' D B, A,v ~ A;T* h^ $N_2$ *: B* and *UJ=OJ'.*

By induction hypothesis, A; *T* h^ *\V/v]Ni* : B[7] D S and A; T h^ [V/i;]i$V_2$ : S[7].

By the rule $DE_W$, A; *T* h^ [F/v]iVi [V/v] J$V_2$ : *B.*

Therefore A; *V* h^ *[V/v]N* - J5 Q o;[r].

Case AT = box AT[7]: *[V/v]N* = box [V>]Ar[7]

BytheruleDlvr, A,t>~ Ajrh^ AT ~ B @ a;[7] implies A, v ~ A^h^* AT[7]: *B\B = OB\andu; = J* where *UJ**isafreshnode.

By induction hypothesis, A; *T* K,* [F/fjAT[7] : *B'.*

By the rule $Dl_w$, A; T h^ box [V/v]AT[7] : DJB[7].

Therefore A; *T* h^ *[V/v]N* ~ B @ *UJ'.*

Case AT = box^* AT[7]: *[V/v]N* = box^* *[V/v]*$N^f$

By the rule Dl[7]^, A, *v ~ A; T* h^ AT ~ *B @ UJ'* implies A, *v ~ A; T* h^* AT[7]*: B\ B* = D^B[7], and *UJ = Uj'.*

By induction hypothesis, A; *T* h^* *[V/v]N' : B'.*

By the rule Dl[7]^, A; *T* h^ box^* *[V/v]N'*: D^*B'.*

Therefore A; *T* h^ *[V/v]N ~B@UJ'.*

Case AT = letbox *x* = *Ni* in A^, x not a free variable of *V:*

*[V/v]N* = letbox x = [V/v]JVi in *[V/v]*$N_2$

If the rule DE^ is used to deduce A, *v* ~ A; T h^ AT ~ B @ a;[7],

A, i; ~ A; T h^ AT ~ S @ u;[7] implies A, v ~ A; *T* h^ $AT_X$ : DBi and A, x :: Si, *v* ~ A; T h^ $AT_2$ ~ B @ a;[7].

By weakening, A; T h^// *V* : A implies A, x :: Bi; T h^// *V* : A.

By induction hypothesis, A; *T* h^ [V/v]JVi : DBi and A, x :: $B_x$; T h^ [V/v]J$V_2$ ~ B @ u;[7].

By the rule DE^, A; *T* $\-_u$ letbox x = [V/v]iVi in [V/v]$N_2$ ~ *B @ UJ'.*

Therefore A; *T* h^ *[V/v]N ~B@UJ'.*

If the rule DE[7]^ is used to deduce A, *v* ~ A; T h^ AT ~ B @ a;[7],

A, v ~ A; T h^ AT ~ *B @ UJ'* implies A, *v* ~ A; *T* h^ $AT_X$ : D^^Bi and A,i;~ A;T,x:Bi @ a;* h^ $AT_2$ ~ B © a;[7].

By weakening, A; *T* h^/ V : A implies A; I\ x : Bi © a;* h^// *V* : A.

By induction hypothesis, A; *T* h^ [V/v]*Ni : D^* $B_x$* and A; r, x : $B_x$ © *UJ* \-$_U$ [V/V]$N_2$ ~ B@UJ'.*

By the rule DE[7]^, A; *T* h^ letbox x = *[V/v)Ni* in [V/v] $AT_2$ ~ B © a;[7].

Therefore A; *T* h^ [V/v]AT - B @ c^[7].

Case AT = cir AT[7]: *[V/v]N* = cir *[V/v]N'*

By the rule Olvr, A, *v* ~ A; T h^ A^ ~ B © a;[7] implies A, t; ~ A; *T* h^ AT[7] ~ B[7] © a;*, B = OB[7], and *UJ* = *UJ'* where a;* is a fresh node.

By induction hypothesis, A; *T* K, *[V/v]N'* ~ $B^7$ @ u/*.

By the rule *O\w*, A; *T* $h_w$ cir [V/v]$AT^7$ : $OB^7$.

Therefore A; *T* h^ *[V/v]N ~ B@u;'.*

Case *N* = cir^* $AT^7$: *[V/v]N* = cir^* [V/v]$iV^7$

By the rule *O\'w*, A, v ~ *A; T* h^ AT ~ B @ $a;^7$ implies A, v ~ A; T h^ *N'* ~ *B'* @ ω*, B = $O_{a;}$*$B^7$,andu; = u/.

By induction hypothesis, A; *T* h^ [V/v] $AT^7$ ~ $B^7$ @ *u**.

By the rule $Ol^7$^, A; *T* h^ cir [V/v] $AT^7$: O ^ $B^7$.

Therefore A; *T* $h_w$ [V/v] AT ~ B @ $u>^7$.

Case *N* = letcir w = iVi in $AT_2$, *w^v,w* not a free variable of V: [V/v] AT = letcir *w = [V/v]Ni* in $[V/v]N_2$

If the rule OE ^ is used to deduce A, v ~ *A; T* h^ AT ~ B @ $a;^7$,

A, v ~ ^4;T h^ AT ~ B @ $a;^7$ implies *A,v ~ A;T h^ Ni :* OBi and A, *w* ~ Bi, v ~ A; T h^ $AT_2$ ~ B @ $tc;^7$.

By weakening, A; T h^/ V : *A* implies A, *w* ~ *B\\ T* h^/ V : *A*.

By induction hypothesis, A; *V* h^ [V/vjA^ : OBi and A, *w* ~ $B_x$; *T* h^ [V/v]$A^_2$ ~ B @ $a;^7$.

By the rule OEvr, A; *T* h^ letcir ^ = *[V/v]Ni* in [V/v]$AT_2$ ~ B @ $a;^7$.

Therefore A; T h^ [V/v]AT ~ B @ *J.*

If the rule $OE^7$^ is used to deduce A, v ~ A; T h^ AT ~ B @ $a;^7$,

A, v ~ ^4; F h^ *N ~ B @* $u^f$ implies A, v ~ *A; T* h^ *N\ : O^Bi* and A, v ~ ^4; F, *w* ~ Bi @ a?* h^ $A^_2$ ~ B @ $a;^7$.

By weakening, A; *T* h^// V : ^4 implies A; T, ti; ~ *B* @ a;* $h_w$// V : *A*.

By induction hypothesis, A; *T* h^ [V/v]$Ar_x$ : O^^Bi and A; I\ w; ~ $B_x$ @ a;* h^ [V/v]$AT_2$ ~ B @ $a;^7$.

By the rule $OE^7$^, A; T h^ letcir ^ = [V/v]$N_x$ in [V/v]$AT_2$ ~ B @ *J.*

Therefore A; *T* h^ *[V/v]N ~ B @ J.* D

**Proof of Proposition 3.5:**

***Proof.*** By simultaneous induction on the structure of the derivation of A; *T* h *M : A* and A ; T I - M ~ A (Below we reuse metavarible *M* and type A)

Case $\dfrac{x ::Ae\ A \quad \text{or} \quad X:\hat{}4GT}{A; T h x * A}$ Cvar :

*x :: A e Aorx : AeT* implies *x :: A e Aor x : A@ u> e [T]".*

Then,

$$\dfrac{x::A\ G\ A \ \text{or}\ x : A @ u)\ G\ [r]^{a'}}{A; \backslash \pounds f \vdash_\omega x : A}\ \mathsf{Cvar}_W$$

Case $\dfrac{v \sim Ae\ A}{A; T h v : A}$ $\mathsf{Vvar}^w$ :

v ~ ^4 G A implies *v~A€Aorv~A@uje \Tf.*

Then,

$$\dfrac{v \sim A\ G\ A \quad \text{or} \quad v \sim \hat{}4 @ \omega \in [\Gamma]^\omega}{A;\ [IT\ \backslash\text{-}» v : A}\ \mathsf{Vvar}_W$$

Case $\dfrac{\Delta; \cdot \vdash V : A}{A;T\backslash\text{-}V\sim A}$ Val :

By induction hypothesis on A; • h V : *A*, we have A; • h^/ V : *A*.

By weakening, A; • h^ V : ^4 implies A; [r]^ h^ V : *A*.

Then,

A; [IT l-y V : A
A; [r]^w H_w V ~ A 0 a;" Val_W

Case $\dfrac{\Delta;\Gamma,x:A\vdash M:B}{\text{A } \vdash \text{ H A a}' \text{: A M : A D £}}$ ⊃I :

By induction hypothesis on A; T, x : A h M : B, we have A; [F]^u', x :A®u\-_w M:B.
Then,

$$\dfrac{\Delta;[\Gamma]^{\omega},x:A\,@\,\omega\vdash_{\omega}M:B}{\text{A;[rf K,AX:AM: } A\supset B}\ \supset\! I_w$$

Case $\dfrac{A;T\backslash\text{-}M:ApB \quad A;T\backslash\sim N:A}{A;T\backslash\text{-}MN:B}$ DE :

By induction hypothesis on A; T \- M : A D B, we have A; [T]"' h^ Af : A D B.
By induction hypothesis on A; F h A^ : A we have A; [F]^w h^ jV : A.
Then,

$$\dfrac{\text{A; [r]" \textbackslash-uM :ADB} \quad \text{A; [T]}^{w}\ \text{h}_{M}\ \text{JV : A}}{A;\backslash Tf\backslash\text{-}_{u}MN:B}\ \supset\! E_W$$

Case $\dfrac{A;\text{-}\backslash\text{-}M:A}{\text{A; F h box } M : DA}$ Dl :

By induction hypothesis on A; • I- M : A, we have A; • h^/ M : J4.
By weakening, A; • Ky M : A implies A; [T]^w h_w/ M : A.
Then,

$$\dfrac{A;\cdot\vdash_{\omega} M:A}{\text{A; [r]}^{w}\ \text{h}^\wedge\ \text{box } M : \text{DA}}\ \Box I$$

Case $\dfrac{\text{A;rhM:Di} \quad A,x::A;T\,h\,N:B}{\text{A; r h )etboxa• = M in iV : S}}$ DE :

By induction hypothesis on A; T \- M : OA, we have A; [T]" h_w M : DA.
By induction hypothesis on A, x :: A;T\- N : B, we have A, x :: A; [T]" h^ N : B.
A,x::A; [T]^u h_u N : B is equivalent to A, x :: A; [Tf \-_u N ~ B @ w.
Then,

$$\dfrac{\text{A; [r]" h\^{} M : DA} \quad \text{A, a::: A; [T]" h}_{w}\ N \sim \text{g Q o>}}{\text{A; [T]}^{w}\ \text{h\^{} letbox x = M in } N \sim B\ @\ u}\ \Box E_w$$

A; [r]^u) K, letbox x = MiniV~_J B@a; is equivalent to A; \Tf \-_w letbox ar = M in JV : B.

Case $\dfrac{\text{A;nM:DA} \quad A,x::A;T\backslash\text{-}N\sim B}{\Delta;\Gamma\vdash \text{letbox } x = \text{MiniV}\sim\text{B}}$ Ut * 

By induction hypothesis on A; T h M : OA, we have A; [T]" \-_u M : OA.
By induction hypothesis on A, x :: A; T h N ~ B, we have A, x :: A; [r]^1" h^ AT ~ S @ u'.
Then,

$$\dfrac{\text{A; [T]}^{W}\ \text{h}_{w}\ \text{M : CL1} \quad \text{A, x :: A; [ I f H\^{} AT} \sim B\ @u>'}{\text{A; [r]\^{} K, letbox x = MinAT\textasciitilde B@o;}'}\ \Box E_W$$

CaSe $\dfrac{\text{A;T I M}\sim\text{A}}{\text{A;rhcirM:OA}}$ Ol :

By induction hypotheis on A; T \- M ~ A, we have A; [r]"* h^ M ~ A @ u/.

Then,

$$\frac{\Delta; [\Gamma]^{\omega} \vdash_{\omega} M \sim A \mathbin{@} \omega'}{\Delta; [\Gamma]^{\omega} \vdash_{\omega} \mathsf{cir}\ M : \bigcirc A}\ \bigcirc\mathsf{I}_W$$

Case $\dfrac{\Delta; \Gamma \vdash M : \bigcirc A \quad \Delta, v \sim A; \Gamma \vdash N : B}{\Delta; \Gamma \vdash \mathsf{letcir}\ v = M\ \mathsf{in}\ N : B}\ \bigcirc\mathsf{E}$ :

By induction hypothesis on $\Delta; \Gamma \vdash M : \bigcirc A$, we have $\Delta; [\Gamma]^{\omega} \vdash_{\omega} M : \bigcirc A$.
By induction hypothesis on $\Delta, v \sim A; \Gamma \vdash N : B$, we have $\Delta, v \sim A; [\Gamma]^{\omega} \vdash_{\omega} N : B$.
$\Delta, v \sim A; [\Gamma]^{\omega} \vdash_{\omega} N : B$ is equivalent to $\Delta, v \sim A; [\Gamma]^{\omega} \vdash_{\omega} N \sim B \mathbin{@} \omega$.
Then,

$$\frac{\Delta; [\Gamma]^{\omega} \vdash_{\omega} M : \bigcirc A \quad \Delta, v \sim A; [\Gamma]^{\omega} \vdash_{\omega} N \sim B \mathbin{@} \omega}{\Delta; [\Gamma]^{\omega} \vdash_{\omega} \mathsf{letcir}\ v = M\ \mathsf{in}\ N \sim B \mathbin{@} \omega}\ \bigcirc\mathsf{E}_W$$

$\Delta; [\Gamma]^{\omega} \vdash_{\omega} \mathsf{letcir}\ v = M\ \mathsf{in}\ N \sim B \mathbin{@} \omega$ is equivalent to $\Delta; [\Gamma]^{\omega} \vdash_{\omega} \mathsf{letcir}\ v = M\ \mathsf{in}\ N : B$.

Case $\dfrac{\Delta; \Gamma \vdash M : \bigcirc A \quad \Delta, v \sim A; \Gamma \vdash N \sim B}{\Delta; \Gamma \vdash \mathsf{letcir}\ v = M\ \mathsf{in}\ N \sim B}\ \bigcirc\mathsf{E}'$ :

By induction hypothesis on $\Delta; \Gamma \vdash M : \bigcirc A$, we have $\Delta; [\Gamma]^{\omega} \vdash_{\omega} M : \bigcirc A$.
By induction hypothesis on $\Delta, v \sim A; \Gamma \vdash N \sim B$, we have $\Delta, v \sim A; [\Gamma]^{\omega} \vdash_{\omega} N \sim B \mathbin{@} \omega'$.
Then,

$$\frac{\Delta; [\Gamma]^{\omega} \vdash_{\omega} M : \bigcirc A \quad \Delta, v \sim A; [\Gamma]^{\omega} \vdash_{\omega} N \sim B \mathbin{@} \omega'}{\Delta; [\Gamma]^{\omega} \vdash_{\omega} \mathsf{letcir}\ v = M\ \mathsf{in}\ N \sim B \mathbin{@} \omega'}\ \bigcirc\mathsf{E}_W$$

Case $\dfrac{\Delta; \Gamma \vdash M : A_{prim}}{\Delta; \Gamma \vdash M \sim A_{prim}}\ \mathsf{Prim}{\sim}$ :

By induction hypothesis on $\Delta; \Gamma \vdash M : A_{prim}$, we have $\Delta; [\Gamma]^{\omega} \vdash_{\omega} M : A_{prim}$.
Then,

$$\frac{\Delta; [\Gamma]^{\omega} \vdash_{\omega} M : A_{prim}}{\Delta; [\Gamma]^{\omega} \vdash_{\omega} M \sim A_{prim} \mathbin{@} \omega'}\ \mathsf{Prim}{\sim}_W$$

□

## C Proofs of the type safety of $\lambda_{\Box\bigcirc}{}^{W}$

**Proposition C.1.**
*If* $\Lambda; \Delta; \Gamma \vdash_{\omega''} M : A$ *and* $\Lambda; \Delta; \Gamma, x : A \mathbin{@} \omega'' \vdash_{\omega} N \sim B \mathbin{@} \omega'$, *then* $\Lambda; \Delta; \Gamma \vdash_{\omega} [M/x]N \sim B \mathbin{@} \omega'$.

*Proof.* By induction on the structure of the derivation of $\Lambda; \Delta; \Gamma, x : A \mathbin{@} \omega'' \vdash_{\omega} N \sim B \mathbin{@} \omega'$. □

**Proposition C.2.**
*If* $\Lambda; \Delta; \Gamma \vdash_{\omega''} M : A$ *for any node* $\omega''$ *and* $\Lambda; \Delta, x :: A; \Gamma \vdash_{\omega} N \sim B \mathbin{@} \omega'$, *then* $\Lambda; \Delta; \Gamma \vdash_{\omega} [M/x]N \sim B \mathbin{@} \omega'$.

*Proof.* By induction on the structure of the derivation of $\Lambda; \Delta, x :: A; \Gamma \vdash_{\omega} N \sim B \mathbin{@} \omega'$. □

**Proposition C.3.**
*If* $\Lambda; \Delta; \Gamma \vdash_{\omega''} V : A$ *and* $\Lambda; \Delta; \Gamma, v \sim A \mathbin{@} \omega'' \vdash_{\omega} N \sim B \mathbin{@} \omega'$, *then* $\Lambda; \Delta; \Gamma \vdash_{\omega} [V/v]N \sim B \mathbin{@} \omega'$.

*Proof.* By induction on the structure of the derivation of $\Lambda; \Delta; \Gamma, v \sim A \mathbin{@} \omega'' \vdash_{\omega} N \sim B \mathbin{@} \omega'$. □

**Proposition C.4.**
*If* $\Lambda; \Delta; \Gamma \vdash_{\omega''} V : A$ *for any node* $\omega''$ *and* $\Lambda; \Delta, v \sim A; \Gamma \vdash_{\omega} N \sim B \mathbin{@} \omega'$, *then* $\Lambda; \Delta; \Gamma \vdash_{\omega} [V/v]N \sim B \mathbin{@} \omega'$.

*Proof.* By induction on the structure of the derivation of $\Lambda; \Delta, v \sim A; \Gamma \vdash_\omega N \sim B @ \omega'$. □

Proofs of Propositions C.1 to C.4 are similar to those of Propositions 3.1 to 3.4. Cases for communication constructs are also straightforward, as substitutions on communication constructs are all structural:

$$\begin{array}{rcl}
[M/x]() & = & () \\
[M/x]\mathsf{eval}\ N & = & \mathsf{eval}\ [M/x]N \\
[M/x]\mathsf{future}\ N & = & \mathsf{future}\ [M/x]N \\
[M/x]\mathsf{syncvar}\ \gamma & = & \mathsf{syncvar}\ \gamma \\
[M/x]\mathsf{syncwith}\ N & = & \mathsf{syncwith}\ [M/x]N \\
[M/x]\mathsf{nil} & = & \mathsf{nil} \\
[M/x]V_1 :: V_2 & = & [M/x]V_1 :: [M/x]V_2 \\
[M/x]\mathsf{chanvar}\ \gamma & = & \mathsf{chanvar}\ \gamma \\
[M/x]\mathsf{newchan}_A & = & \mathsf{newchan}_A \\
[M/x]\mathsf{readchan}\ N & = & \mathsf{readchan}\ [M/x]N \\
[M/x]\mathsf{writechan}\ N_1\ N_2 & = & \mathsf{writechan}\ [M/x]N_1\ [M/x]N_2
\end{array}$$

**Lemma C.5.** *If* $\Lambda; \Delta; \Gamma \vdash_\omega M \sim A @ \omega'$ *and* $M \longrightarrow N$, *then* $\Lambda; \Delta; \Gamma \vdash_\omega N \sim A @ \omega'$.

*Proof.* By induction on the structure of the derivation of $\Lambda; \Delta; \Gamma \vdash_\omega M \sim A @ \omega'$. (Below we reuse metavariable $M$ and type $A$.)

Case $\dfrac{\Lambda; \Delta; \Gamma \vdash_\omega M : A_{prim}}{\Lambda; \Delta; \Gamma \vdash_\omega M \sim A_{prim} @ \omega'}\ \mathsf{Prim}{\sim}_W\ (\omega \neq \omega')$ :

By induction hypothesis, $\Lambda; \Delta; \Gamma \vdash_\omega N : A_{prim}$.

By the rule $\mathsf{Prim}{\sim}_W$, $\Lambda; \Delta; \Gamma \vdash_\omega N \sim A_{prim} @ \omega'$.

Now we now assume that the rule $\mathsf{Prim}{\sim}_W$ is not used to derive $\Lambda; \Delta; \Gamma \vdash_\omega M \sim A @ \omega'$.

Case $(\lambda x{:}A.\, N)\ M \to_{\beta\supset} [M/x]N$:

The only possible derivation is:

$$\dfrac{\dfrac{\Lambda; \Delta; \Gamma, x : A @ \omega \vdash_\omega N : B}{\Lambda; \Delta; \Gamma \vdash_\omega \lambda x{:}A.\, N : A \supset B}\ \supset\mathsf{I}_W \quad \Lambda; \Delta; \Gamma \vdash_\omega M : A}{\Lambda; \Delta; \Gamma \vdash_\omega (\lambda x{:}A.\, N)\ M : B}\ \supset\mathsf{E}_W$$

By Proposition C.1, $\Lambda; \Delta; \Gamma \vdash_\omega [M/x]N : B$.

Case $\mathsf{letbox}\ x = \mathsf{box}\ M\ \mathsf{in}\ N \to_{\beta\Box} [M/x]N$:

The only possible derivation is:

$$\dfrac{\dfrac{\textit{fresh}\ \omega'' \quad \Lambda; \Delta; \Gamma \vdash_{\omega''} M : A}{\Lambda; \Delta; \Gamma \vdash_\omega \mathsf{box}\ M : \Box A}\ \Box\mathsf{I}_W \quad \Lambda; \Delta, x :: A; \Gamma \vdash_\omega N \sim B @ \omega'}{\Lambda; \Delta; \Gamma \vdash_\omega \mathsf{letbox}\ x = \mathsf{box}\ M\ \mathsf{in}\ N \sim B @ \omega'}\ \Box\mathsf{E}_W$$

By Proposition C.2, $\Lambda; \Delta; \Gamma \vdash_\omega [M/x]N \sim B @ \omega'$.

Case $\mathsf{letbox}\ x = \mathsf{box}_{\omega''}\ M\ \mathsf{in}\ N \to_{\beta\Box'} [M/x]N$:

The only possible derivation is:

$$\dfrac{\dfrac{\Lambda; \Delta; \Gamma \vdash_{\omega''} M : A}{\Lambda; \Delta; \Gamma \vdash_\omega \mathsf{box}_{\omega''}\ M : \Box_{\omega''} A}\ \Box\mathsf{I}'_W \quad \Lambda; \Delta; \Gamma, x : A @ \omega'' \vdash_\omega N \sim B @ \omega'}{\Lambda; \Delta; \Gamma \vdash_\omega \mathsf{letbox}\ x = \mathsf{box}_{\omega''}\ M\ \mathsf{in}\ N \sim B @ \omega'}\ \Box\mathsf{E}'_W$$

By Proposition C.1, $\Lambda; \Delta; \Gamma \vdash_\omega [M/x]N \sim B @ \omega'$.

Case $\mathsf{letcir}\ v = \mathsf{cir}\ V\ \mathsf{in}\ N \to_{\beta\bigcirc} [V/v]N$:

The only possible derivation is:

$$\dfrac{fresh\ u>" \quad \dfrac{\Lambda;\Delta;\Gamma \vdash_{\omega''} V : A}{A; A; T \backslash\text{-}_u V \sim A\ @\ J'}\ \text{Val}^{\text{TM}} \quad \text{OI}_w}{\Lambda;\Delta;\Gamma \vdash_\omega \textsf{cir}\ V\ :OA} \quad \dfrac{}{A;A,v \sim A;T\backslash\text{-}_U N \sim B\ Qu/}\ \text{OE}_W$$

$$\Lambda;\Delta;\Gamma \vdash_\omega \textsf{letcir}\ v = c\backslash rVmN \sim B@u'.$$

By Proposition C.4, A; A; *T* h^ *[V/v]N* ~ B @ a;'.

Case letcir v = cir^,// F in *N-+p₀i [V/v]N:*

The only possible derivation is:

$$\dfrac{\dfrac{\Lambda;\Delta;\Gamma \vdash_\omega V \sim A\ @\ \omega''}{A; A;T\ h\wedge\ \textbf{cir}\wedge/\ F : Q\wedge/A}\ \text{OI}'_W \qquad A;A;T,v\sim A@'u;\backslash_{u;}N\sim B@u'}{A; A;T\ h\wedge\ \text{letcir}\ v = \text{cir}\wedge\ F\ \text{in}\ iV \sim £\ @\ u/}\ \text{OE}'_w$$

From A; A; *T* h^ *V* ~ *A* @ u/\ we have A; A; *V* h^// *V : A,* whether *u>* = *J*[1] or a; ^ a?[r/].

By Proposition C.3, A; A; T h^ *[V/v]N ~B@u;*[f]. D

**Lemma** C.6.

*Consider two terms Mo and NQ such that* A; A; *T* h^ *MQ ~ AQ @* **LJO** *implies* A; A; *T* h^ *No* ~ A) @ o;o /<?r any Ao *and* a;o.

//* A; A; T $h_u$ *M* - A @ u/, *then for any* K *such that* *M* = *K[M₀], it holds* A; A; *T* h^ *K[N₀]* ~ *A* @ *J.*

*Proof.* If *K* = 0, then M = M₀ and K[AT₀] = AT₀. Hence A; A; *T* h^ *K[N₀]* ~ *A* @ a;[7] holds by the assumption on Mo and iV₀.

Suppose *n* ^ [], which means that *M* ^ *x> M* ^*v,* and *M* ^ V.

Now we apply induction on the structure of A; A; *T* h^ *M* ~ A @ u/. (Below we reuse metavarible M and type A.)

CaSe $\dfrac{AjAjrh\wedge M{:}A_{prim}}{W \wedge M - A_{prim}\ @\ \omega'}$ Prim~$_W$ $(\omega \neq \omega')$ , $M = \kappa[M_0]$:

By induction hypothesis, A; A; *T* K, *K[N₀] :* $A_{prim}$.

By the rule Prim~vr, A; A; T h^ K[iV₀] ~ >l$_{prim}$ @ $\omega'$.

Case $\dfrac{\wedge \quad A\ A}{AiAirh_\omega MATig}$ DEU„ , M ^ = K[M₀^ = *K* [M₀]iV:

By induction hypothesis on A; A; *T* K, M : >1 D S, we have A; A; T h^ «'[iVo] : *A D B.*

**By the rule** *DE_W,* A; **A; T** \-*w K'[N₀] N:B,* **and** *K'[N₀] N = K[N₀].*

**Case** $\dfrac{\Lambda;\Delta;\Gamma \vdash_\omega M : \Box A \quad A;A,x\ ::\ A;T\backslash\text{-}_U N\ \sim B@u;^f}{\Lambda;\Delta;\Gamma \vdash_\omega \textsf{letbox}\ x = \text{MiniV}\sim_J B@u;'}$ □E$_W$,

letbox a: = *M* in JV = K[M₀] = letbox *x* = K'[M₀] in *N:*

By induction hypothesis on A; A; T H$_w$ *M : DA,* we have A; A; T h^ «'[iVo] : DA.

By the rule DE^, A; A; *T* \-*w* letbox *x* = *K'[N₀]* in JV ~ *B* @ *LS,* and letbox *x* = *K'[N₀]* in JV = K[JV₀].

Case *OE'_W* is similar to Case DE^.

**Case** $\dfrac{A;\ A;T\ \backslash\text{-}_u\ M\ :\ OA \quad A\text{-},A,v\ \sim\ A;T\backslash\text{-}_U N\ \sim\ BQu/}{A;A;rh_a,\text{letcirv} = \text{MiniV}\sim i?@a;'}$ OE$_W$

If letcir t; = *M* in JV = K[M₀] = letcir *v* = *K'[M₀]* in JV and *M* = *K'[M₀),*

By induction hypothesis on A; A; *T* K, M : OA, we have A; A; *T* \-*u K'[NQ\ : OA.*

By the rule OE^, A; A; T H^ letcir *v* = *K'[N₀]* in JV ~ *B* @ u/, and letcir v = K'[JV₀] in JV = K[JV₀].

If letcir *v* = *M* in JV = K[MQ] = letcir v = cir *K'[MQ]* in JV and *M* = cir K'[JV/₀],

w u ft^W7 A; A;F h, K7[M0] ~ A @ ^ OIw .
We have ——————:— n 1
A; A; F h^ cir /c'[Afo] : O-4 @ ω''.
By induction hypothesis on A; A; F h^ K![MQ] ~ A @ J1, we have A; A; F \-u K'[N0] ~ A
Then,
fresh J' A; A; F h^ K'[NQ] ~ A @ a/7 OI
A; A;F !-„ cir K'[NQ] : OA W A; A,v ~ ^;T !-„ AT ~ g @ u/ OE
and letcir v = cir K'[NO] in JV = letcir v = cir K'[N0) in AT - B @ J W
If letcir v = M in N = K[MQ] = letcir v = cir^// K'[MO] in N and M = cir^// K7[MO],
There is no rule for deriving A; A; F h^ M : OA.
Case OE^y is similar to Case OEw.
Case Λ; Δ·Γ ⊢ A / A i A i r ' H ^ v a ^ u n i t Teval , eval M = «^ = eval κ'[M0]:
By induction hypothesis on A; A; T h^ M : DA, we have A; A; F h^ K'[NO] : DA
By the rule Teval, A; A; F h^ eval K'[N0] : unit, and eval K'[N0] = K[N0].
Case Teval® is similar to Case Teval.
Case Λ·Δ·Γ ⊢ M : □OA / A A FL A ^JJ A ^ 5r Tfuture , future M = K[MO] = future K'[MQ\: L J l J
A; A; F h^ future M ~ A sync @ a;
By induction hypothesis on A; A; F h^ M : DOA, we have A; A; F h^ K'[N0] : DOA.
By the rule Tfuture, A; A; F h^ future K'[N0] ~ A sync @ u*9 and future K'[NO] = K[N0].
Cases Tfuture®, Tfuture7, Tfuture®7 are similar to Case Tfuture.
Case A'Δ;Γ ⊢ω M : A sync / A A , ... %jr T-S; 5r Tswith , syncwith M = K[MQ] = syncwith K!\MQ}: J L UJ 7 L UJ
A; A; F h^ syncwith M ~ A @ v
By induction hypothesis on A; A; F h^ M : A sync, we have A; A; F h^ K'[N0] : ^4 sync.
By the rule Tswith, A; A; F h^ syncwith K7[AT0] ~ A @ a;*, and syncwith K'[N0] = /c[iV0].
Case Tswith7 is similar to Case Tswith.
Case A; A; F h^ newchan^ ~ A chan @ a;* TnewC :
There is no K such that newchan^ = K[MQ] and K 7^ \\.
Case A' Δ' Γ ⊢ω M : A / A; A; r ' h j readdian M " I "Ω a;* Treadc • readchan M = *lM<>] = readchan K'[M0}:
By induction hypothesis on A; A; F h^ M : A chan, we have A; A; F h^ K7[AT0] : A chan.
By the rule Treadc, A; A; F h^ readchan K7[iVo] ~ A @ a;*, and readchan K7[iV0] = K[iV0].
**Case** A; A; F h^ M : A chan ,/res/i a;7 A; A; F h^ iV ~ A @ u;7 / A; A; F h^ writechan M N - ^ @ a;* Twritec :
If writechan M N = K[M0] = writechan n'[M0] NandM = K7[M0],
By induction hypothesis on A; A; F h^ M : A chan, we have A; A; F \-u K'[N0] : A chan.
By the rule Twritec, A; A; F h^ writechan K'[N0] N ~ A @ a;*, and writechan K'[N0] N = /c[iVb].
If writechan M N = K[M0] = writechan M K/[M0] and iV = K7[M0] where M = chanvar 7,
By induction hypothesis on A; A; F h^ JV ~ A @ u;7, we have A; A; F h^ K'[N0] ~ A@U;'.
By the rule Twritec, A; A; F h^ writechan M K![N0] ~ A @ u;*, and writechan M K7[iVo] = K[iV0].

D

**Lemma C.7.**
*IfC, M* at 7 :: A, 7 ~ A @ *u and* A, 7 ~ ^4 @ a;; •; FPerm hP(7) AT ~ A @ u9
*then C, N* at 7 :: A, 7 ~ >1 @ a;.

***Proof.*** C, M at 7 :: A, 7 ~ ^4 @ *UJ* implies that for each M7 at y G C,
77 - A7 @ a;7 G A, 7 - A @ *UJ* and A, 7 ~ ^ @ *u;* ,-F^"11 hp(y) M7 ~ A7 O a;7, or
y ~7A @, ⋆ ∈7Λ, γ~ A\@ ω@and A ; ; .;FPerrn h^y) M7 ~ A @ a;77 for a fiesh node a;77.

By the rule Tcfg and A, 7 ~ *A* @ *u;* •; T$^{perm}$ h$_{P(7)}$ AT ~ A @ a;, we have C, JV **at** 7 :: A, 7 ~ ^ @ *u.*

*D*

**Lemma C.8.**

*IfC,M* **at** 7 :: A, 7 ~ ^ @ •a/w/ A, 7 ~ ,4 @ •; .;rP$^{erm}$ hp$_{(7)}$ *N ~A@ w for afresh node u>,*
*then* C, *N* **at** 7 :: A, 7 ~ *A* @ *.

***Proc/*** C, M **at** 7 :: A, 7 ~ ^4 @ • implies that for each M$^7$ at V G C,
7' ~ ,4$^7$ @ *<j' e* A, 7 ~ A @ • and A, 7 ~ A @ •; •; r^$^1$™ l"p(y) M$^7$ ~ A$^7$ @ *J,* or
7$^7$ ~ ^l$^7$ @ • *e* A, 7 ~ >1 @ • and A, 7 ~ A @ •; •; r$^{perfT1}$ h$_{p(7,)}$ M$^7$ ~ A$^7$ @ a;$^{77}$ for a fresh node u;$^{77}$.

By the rule Tcfg and A, 7 ~ *A* @ •; •; r$^{perm}$ h$_{P(7)}$ AT ~ ^1 @ a;, we have C, AT **at** 7 :: A, 7 ~ ^ @ •.

**D**

Proof of Lemma 4.4:

***Proc/*** By induction on the structure of *n.*

Case *K* = *\\:*

*B* = *A* and a/$^7$ = a/.

If K ·7^ [], it suffices to consider those cases in which the rule Prinv^vr is not used to deduce A; A;F h^ *K[M] ~ A@ U;';* if the rule Prim~vr is used, we repeat the same case analysis on the premise of the rule.

Case *K* = *no Mo:*

By the rule *DEw* and induction hypothesis on *KQ.*

Case *K* = letbox *x* = *KQ* in Mo:

By the rule • E ^ or *DE$^f_w$* and induction hypothesis on KO-

Case *K* = letcir i; = ACO in Mo:

By the rule O E ^ or OE$^7$^ and induction hypothesis on KO-

Case *K* = letcir v = cir *KO* in Mo:

By the rules OEvr and Olvr and induction hypothesis on *KQ.*

Case *K* =— letcir v = cir^ KO in Mo:

By the rules *OEl$_w$* and O1^ and induction hypothesis on «o.

Case eval *K§*

By the rule Teval or Teval® and induction hypothesis on KO.

Case future /q>:

By the rule Tfuture, Tfuture®, Tfuture$^7$, or Tfuture®$^7$, and induction hypothesis on *K§.*

Case syncwith *K§*

By the rule Tswith or Tswith$^7$ and induction hypothesis on «o.

Case readchan «o:

By the rule Treadc and induction hypothesis on «o.

Case writechan *KQ MQ:*

By the rule Twritec and induction hypothesis on *KO.*

Case writechan (chanvar 7) /q>:

By the rule Twritec and induction hypothesis on «o-

E

**Proposition C.9 (Weakening).**

*Suppose*

*C::X*

A;.;rP$^{erm}$h$_{u;}$M: *A*

*u; = V{^)$_9$ where* 7 *is notfound in* A.

*Then* C, M **at** 7 :: A, 7 ~ *A* @ a;.

*Proof.*
If M7 at V G *C* and V ~ *A*1 © *J* G A,

By the rule Tcfg, A; •; rperm \-v{y) *M'* ~ *A'@ J*

By weakening on A, we have A, 7 ~ >1 @ *u*\ •; rperm Hj>(7/) M7 ~ A @ u;7

If M7 at *i* G *C* and V ~ *A!* © • G A,

By the rule Tcfg, A; •; P*"" hp(y) M7 ~ A' Q u/ for a fresh node u/.

By weakening on A, we have A, 7 ~ ^4 @ u;; •; rperm ^*v(Y)* M' ~ A' @ ω'

For M at 7,

By weakening A; •; *T***m* *h^ M : A,* we have A, 7 ~ A @ a;; •; Γperm ⊢ω M : A

That is, A, 7 ~ A @ a;; •; rperm hp(7) M ~ *A* @ *u.*

Therefore C, *M* at 7 :: A, 7 ~ A @ a; by the rule Tcfg. □

**Lemma CIO.**
***If***

C, M at 7 :: A, 7 ~ $A_\gamma$ @ a;,

**A, γ ~ $A_\gamma$ @ ω, γ' ~ $A_{\gamma'}$ @ *; •; Γperm ⊢P(γ) *N* ~ $A_\gamma$ @ a;,**

**A, 7 ~ $A_\gamma$ @ a;, *i* ~ Ay/ @ *; •; Γperm ⊢P(γ') iV7 ~ Ay/ @ ¿^*/<?r an *arbitrary node u*9***

*then*

***C,N* at 7, AT7 at y :: A, 7 ~ $A_\gamma$ @ u;,77 ~ Ay/ @ •.**

***Proc/*** From C, M at 7 :: A, 7 ~ $A_\gamma$ @ a;,
for each Mo at 70 G C,

70 ~ Ao @ o;0 G A and A, 7 ~ Ay @ u;; •; Γperm ~ $A_0$ @ o;0, or

70 ~ *AQ* @ • G A and A, 7 ~ A7 @ a;; •; Γperm l-p(7o) Mo ~ $A_0$ @ ^0 for an arbitrary node $\omega_0$.

By weakening on A, 7 ~ Ay @ it>,

A, 7 ~ A7 @ *u, i* ~ *Ay* @ •; •; r^"1 Hp(7o) Mo ~ *Ao* @ o;0, or

A, 7 ~ A7 @ a;, T7 ~ Ay/ @ •; •; rperm Hp(7o) Mo ~ *Ao @ u>o* for an arbitrary node o;o.

By the rule Tcfg, we have C, *N* at 7, *N'* at T7 :: A, 7 ~ A7 @ a;, 77 ~ Ay/ @ •. ●

**Lemma C.ll.**
//

**C, M at 7 :: A, 7 ~ Ay @ a;,**

**A,7 ~ Ay @ ^ T 7 - Ay/ @ u;7; .;rperfT1 \-*v{ri)* *N* ~ Ay @ ω,**

**A,7 ~ $A_\gamma$ @ω, *i* ~ Ay/ © a;77; •; rperm hp(y) iV7 ~ $A_{\gamma'}$ @ a;7,**

*then*

***C, N* at 7, AT7 at γ' :: A, 7 ~ A7 © a;, 77 ~ Ay/ © u;7.**

**Lemma C.12.**
***If***

**C,M at 7 :: A, 7 ^ Ay © •,**

**A, 7 ~ Ay © •, T7 ~ Ay/ © •; •; rperm hp(7) AT ~ A7 © u;* /or a/i *arbitrary node UJ*9***

**A, 7 ~ Ay © •, 77 ~ Ay/ © *; •; rperm hp(y) *N'* ~ Ay/ © a;* /or a/i *arbitrary node* a;*,**

***then***

C, AT at 7, AT7 at Y :: A, 7 ~ $A_\gamma$ © •, 77 ~ Ay/ © •.

**Lemma C.13.**
***If***

**C, M at 7 :: A, 7 ~ Ay @ •,**

**A, 7 ~ Ay © •, *i* ~ Ay/ © u;7; •; *T***rm* hP(7) iV ~ Ay © u;* /or an *arbitrary node* a;*,**

A, 7 ~ Ay @ •, *i* ~ ^ @ a/; •; 1^™ h p(y) AT ~ Ay/ @ ω',

*then*

*C, N* at 7, AT⁷ at Y :: A, 7 ~ Ay @ *, 7' ~ Ay/ @ a/.

***Proof.*** Similar to the proof of Lemma C.I0. •

**Proof of Theorem 4.1:**

*Proof* By case analysis of *C* => C". (Below we reuse all metavariables.)

Case $\dfrac{M \longrightarrow N}{C, K[M] \text{ at } 7 \Rightarrow C, K[JV] \text{ at } 7}$ R6 :

If C, K[M] at 7 :: A, 7 - Ay @ *w₉* then A, 7 - Ay @ a;; •; rP^erm h p(7) «[M] ~ Ay @ a;.

Since M —• *N₉* Lemmas C.5 and C.6 imply A, 7 ~ ^4₇ @ u>; •; r**^1™ h P(7) «[j\T] ~ Ay @ u;.

By Lemma C.7, we have C, K[JV] at 7 :: A, 7 ~ Ay @ *v*.

If C, AC[M] at 7 :: A, 7 - Ay @ •, then A, 7 ~ Ay @ •; •; r^perm h p(7) K[M] ~ Ay @ a; for a fresh node

Since M —> AT, Lemmas C.5 and C.6 imply A, 7 ~ ^4₇ @ •; •; r^perm h P(7) «[JV] ~ Ay @ *w*.

By Lemma C.8, we have C, «[iV] at 7 :: A, 7 ~ Ay @ •.

Case $\dfrac{\text{nett; V}}{C, «[\text{eval box } M] \text{ at } 7 \Rightarrow C, «[()] \text{ at } 7, M \text{ at } </}$ Reval :

If C, ^[eval box M] at 7 :: A, 7 ~ A₇ @ a;, then A, 7 ~ A₇ @ a;; •; T^^1™ h P(7) K[eval box *M]* ~ A₇ @ 4*;.

By Lemma 4.4, eval box *M* typechecks:

$$\dfrac{\dfrac{\textit{freshw'} \quad A, 7 \sim A_y @ a;;-;!^{1™} h^ M : A}{A, 7 \sim Ay @ w; •; r"*"" h_{P(7)} \text{ box } M : OA}\Box I_W}{A, 7 \sim A_7 @ w; •; T^"" h_{W7)} \text{ eval box } M : \text{unit}} \text{Teval}$$

Since A, 7 ~ A₇ @ a;; •; T^^1711 h p(7) () : unit,

. A, 7 ~ A₇ @ a;; •; TP^6"" h P(7) «[()] ~ Ay @ a; by Lemma C.6.

By Lemma C.7,

C,«[()] at 7 :: A, 7 ~ *A₁* @ a;.

From

C,«[()] at 7 :: A, 7 ~ A₇ @ a;,

A, 7 ~ Ay @ a;; •; r^17" *h^ M : A* where we let a/ = *V(^)₉*

we have C, K[()] at 7, M at V :: A, 7 ~ Ay @ a;, T⁷ ~ *A* @ *u>^f* by Proposition C.9.

The case for C, «[eval box M] at 7 :: A, 7 ~ A₇ @ • is similar, except that we use Lemma C.8 instead of Lemma C.7.

Case $\dfrac{new\ Y @ J}{C, /qeval\ box^/ M] \text{ at } 7 \Rightarrow C, K[()J \text{ at } 7, M \text{ at } y}$ Reval® :

The proof is similar to Case Reval, except that we use u/ without creating a fresh node.

Case $\dfrac{new\ y}{C, /c[future\ box\ M] \text{ at } 7 \Rightarrow C, /c[syncvar\ y] \text{ at } 7, \text{letcir } v = M \text{ in } i; \text{ at } Y}$ Rfuture :

If C, ^[future box Af] at 7 :: A, 7 ~ ^4₇ @ a;, then A, 7 ~ Ay @ a;; •; T^1™ h P(7) K[future box M] ~ A₇ @ a;.

By Lemma 4.4, future box M typechecks:

$$\dfrac{\dfrac{\textit{freshu'} \quad A, 7 - A y O ^ \cdot; \Gamma^{perm} \vdash_{\omega'} M : \bigcirc A}{A, 7 \sim Ay @ a;; •; rP^{erm} h_{p(7)} \text{ box } M : DO.4}\Box I_W}{A, 7 \sim A_7 @ ex;; •; T^{**™} \vdash_{\nu<a)} \text{ future box } M \sim A \text{ sync } @ u;} \text{Tfuture}$$

or

$$\dfrac{\dfrac{fresh\ J \quad \text{A, 7} \sim \text{Ay @ a;; •; } r^{perm}\ h\wedge\ M : O\wedge A}{\text{A, 7 - Ay @ } LJ; \text{ •; T } \wedge\ h_{p(7)}\ \text{box M : DCVA}}\ \Box I_w}{\text{A, 7 - } Ay \text{ Q a;; •;} \Gamma^{perm}\ h_{P(7)}\ \text{future box M} \sim \text{A synq,,, @ a;*}}\ \text{Tfuture}$$

In the first case,

A, 7 ~ $A_7$ @ a;; ·; $\Gamma^{perm} \vdash_{\mathcal{P}(\gamma)}$ Ac[future box M] ~ $A_7$ @ a;,

A, 7 ~ $A_7$ @ u>; •; $r^{perm}$ I~p(7) future box $M \sim A$ sync @ a;* for an arbitrary node u;*,

A, 7 ~ $A_7$ @ a;; •; $\Gamma^{perm} \vdash$^/ M : OA for a fresh node $J$,

A, 7 ~ Ay @ a;; •; $\Gamma^{perm}$ $h_w$/ letcir v = M in $v \sim A$ @ a;* for an arbitrary node a;*,

and we let $J = \mathcal{P}(\gamma')$.

By weakening on A, 7 $\sim A_1$ @ a;,

A, 7 ~ $A_7$ @ a;, $7^7 \sim$ A @ •; ·; $\Gamma^{perm} \vdash_{\mathcal{P}(\gamma)}$ K[future box M] ~ $A_7$ @ a;,

A, 7 *rsj* $A_1$ @ a;, $7^7 \sim$ A @ •; ·; $\Gamma^{perm} \vdash_{\mathcal{P}(\gamma)}$ future box $M \sim A$ sync @ a?* for an arbitrary node $v*_9$

A, 7 ~ $A_1$ @ a;, $7^7 \sim$ A @ •; ·; $\Gamma^{perm} \vdash_{\omega'}$ letcir t; = $M$ in v ~ A @ $u$* for an arbitrary node u;*.

By the rules Tsvar and Valvr»

A, 7 ~ $A_1$ @ a;, $7^r$ ~ A @ •; ·; $\Gamma^{perm} \vdash_{\mathcal{P}(\gamma)}$ syncvar y ~ $A$ sync @ a;* for an arbitrary node a;*,

By Lemma C.6,

A, 7 ~ $A_7$ @ a;, $7^7$ ~ $A$ @ •; ·; $\Gamma^{perm} \vdash_{\mathcal{P}(\gamma)}$ «[syncvar V] ~ $A_7$ @ a;,

By applying Lemma CIO to

C, K[future box $M$] at 7 :: A, 7 ~ $A_7$ @ a;,

A, 7 ~ ^$4_7$ @ a;, $7^7$ ~ A @ •; •; $r^{perm} \vdash_{\mathcal{P}(\gamma)}$ ^[syncvar V] ~ $A_\gamma$ @ a;,

A, 7 ~ ^$4_7$ @ a;, $7^7$ ~ $A$ @ •; ·; $\Gamma^{perm} \vdash_{\omega'}$ letcir v = $M$ in x; ~ $A$ @ a;* for an arbitrary node a;*,

we have C, /s[syncvar $7^7$] at 7, letcir $v = M$ in v at 7' :: A, 7 ~ $A$^ @ a;, $T^7$ ~ ^4 @ •.

In the second case, we prove C, Ac[syncvar $T^7$] at 7, letcir $v = M$ in $v$ at V :: A, 7 ~ Ay @ a;, $7^7 \sim A$ @ $\omega''$; the proof is similar to the first case, except that we use Lemma C. 11.

The case for C, ^[future box M] at 7 :: A, 7 ~ $A_1$ @ * is similar, except that we use Lemmas C.12 and C.13.

Case $\dfrac{new\ V\ @\ a/}{\text{C, K[future box^/ M] at 7 => C, ^[syncvar YJ at 7, letcir v = M in v at } \gamma'}$ Rfuture® :

The proof is similar to Case Rfuture, except that we use $u^1$ without creating a fresh node.

Case $\dfrac{}{\text{C, K[syncwlth syncvar V] at 7, } V \text{ at } {}_7{}^7 \text{ => } C, K[V] \text{ at 7, V at V}}$ RsWith :

If C, K[syncwith syncvar $7^7$] at 7, F at $7^7$:: A, 7 ~ Ay @ u;, $T^7$ ~ Ay/ @ $u;^7$, then

A, 7 ~ $A_7$ @ u>, $7^7$ ~ Ay/ @ $J$\ •; $r^{perm}$ hp(7) /c[syncwith syncvar Y] $\sim A_\gamma$ @ $\omega$,

A, 7 ~ ^$_7$ @ a;, $7^7$ ~ Ay/ @ $ic;^7$; •; $T^{perm}$ $h_{p(7/)}$ V ~ Ay @ $a;^7$.

By Lemma 4.4 and the rules $Tsvar^7$ and $Tswith^7$,

A, 7 ~ $A$~$y$ @ a?, $7^7$ ~ Ay/ @ $a;^7$; ·; $r^{perm}$ h^(7) syncwith syncvar V ~ $A_{\gamma'}$ @ $a;^7$.

If $\mathcal{P}(\gamma')$ = $a;^7$ (whether *Viri)* = $\mathcal{P}$(^) or not),

A, 7 ~ $A_7$ Q a;, ${}_7{}^7$ ~ Ay/ @ $a;^7$; •; $T^{perm}$ $h_{p(7)}$ V - Ay/ @ $a;^7$ by the rule $Val_W$.

If $\mathcal{P}(\gamma') \neq \omega$/

A, 7 ~ $A_7$ @ a;, $7^7$ ~ Ay/ @ $a;^7$; •; $r^{perm} \vdash_{\omega'}$ V : Ay/ by the rule Val^, and

A, 7 ~ $A_7$ @ w, $7^7$ ~ Ay/ @ $u;^7$; •; $r^{perm} \vdash_{\mathcal{P}(\gamma)}$ $V$ ~ Ay/ @ $\wedge^7$ by the rule $Val_W$.

By Lemma C.6,

A, 7 ~ $A_7$ @ a;, $T^7$ ~ Ay/ @ a/; •; $T^{perm} \vdash_{\mathcal{P}(\gamma)} \kappa[V]$ ~ Ay @ a;,

By Lemma C.7,

C, K[V] at 7, V at $\gamma'$ :: A, 7 ~ $A_\gamma$ @ a;, $\gamma'$ ~ Ay/ @ $a;^7$.

The case for C, K [syncwith syncvar y] at 7, V at $T^7$ :: A, 7 ~ $A_\gamma$ @ $u$>, V ~ Ay/ @ • is similar.

The cases for

C, /c[syncwith syncvar Y\ at 7, V at y :: A, 7 ~ Ay @ •, y ~ Ay/ @ a?' and

C, ^[syncwith syncvar Y\ at 7, V at y :: A, 7 ~ Ay @ *, y ~ Ay/ @ •

are also similar, except that we use Lemma C.8 instead of Lemma C.7.

Case $\dfrac{new\ 7'}{\text{C, /sfnewchan^] at 7 =>• C, «[chanvar 7'] at 7, nil at y}}$ Rnewc :

If C, ^[newchan^] at 7 :: A, 7 ~ Ay @ a;, then

A, 7 ~ $A_7$ @ a;; •; F^1™ l"p(7) ^[newchan^] ~ Ay @ *UJ*.

By weakening on A, 7 ~ Ay @ a;,

A, 7 ~ Ay @ a;, 7' ~ *A* vlist @ *; •; *T**xm* l"p(7) ^[newchan^] ~ Ay @ *u)*.

By Lemma 4.4, newchan^ typechecks:

$$\dfrac{}{\text{A, 7 ~ Ay @ a;, y ~ A vlist @ •; •; r^"1 l~p(7) newchan^ ~ A chan @ a;*}}\ \text{Tnewc}$$

By the rules Tchanv and Val^,

A, 7 ~ Ay @ a;, 7' ~ *A* vlist @ •; •; $r^{perm}$ $h_{P(7)}$ chanvar y ~ *A* chan @ a;*

By Lemma C.6,

A, 7 ~ Ay @ a;, $7^7$ ~ *A* vlist @ •; •; $r^{perm}$ $h_{p(7)}$ K[chanvar y] ~ Ay @ *u*.

By the rule Tvnil and Val^,

A, 7 ~ $A_7$ @ a;, y ~ A vlist @ •; •; $T^{perm}$ ^p(7/) nil ~ ^4 vlist @ CJ* for an arbitrary node a;*.

By applying Lemma CIO to

C, K[newchan^] at 7 :: A, 7 ~ $^4_7$ @ $u_9$

A, 7 ~ Ay @ a;, y ~ A vlist @ •; •; r P ^ $h_{p(7)}$ /^[chanvar y] - Ay @ a;,

A, 7 ~ $A_7$ @ a;, $7^r$ ~ ^4 vlist @ *; •; r^1™ ^~*v(Y)* m' ~ ^ vlist @ a;* for an arbitrary node a;*,

we have

C, ^[chanvar y] at 7, nil at y :: A, 7 ~ $A_7$ @ a;, y ~ ^4 vlist @ •.

The case for C, Ktnewchan^] at 7 :: A, 7 ~ $A_7$ @ • is similar, except that we use Lemma C.12.

Case $\dfrac{}{\text{c, ^[readchan chanvar y] at 7, } V_h \text{ :: } y_t \text{ at y => C, K ^ ] at 7,14 at 7'}}$ Rreadc :

If C, ^[readchan chanvar 7'] at 7, V& :: Vt at y :: A, 7 ~ $A_7$ @ a;, $7^r$ ~ Ay/ @ *, then

A, 7 ~ Ay @ a;, $7^7$ ~ Ay/ @ •; •; T^"11 l"^>(7) «[readchan chanvar y] ~ Ay @ $u)_9$

A, 7 ~ $A_7$ @ u;, 7/ ~ Ay/ @ *; ; $r^{perm}$ $h_{p(7/)}$ V^ :: Vt ~ Ay/ @ a;* for an arbitrary node a;*.

By the rules Valvr and Tvcon,

Ay/ = A vlist,

A, 7 ~ $A_7$ @ u>, 7' ~ Ay/ @ •; •;T^1™ $h_{p(7)}$ V^ ~ *A* @ u;*,

A, 7 - Ay @ u;, $7^7$ - Ay/ @ •; -; $rP^{erm}$ \~*ny)* $V_t$ - Ay/ @ a;*.

By Lemma 4.4 and the rules Tchanv and Treadc,

A, 7 ~ $A_7$ @ a;, 7' ~ Ay/ @ •; •; r1^"11 f~p(7) readchan chanvar y ~ ^4 @ a;*,

By Lemma C.6,

$\Lambda, \gamma \sim A_\gamma \ @\ \omega, \gamma' \sim A_{\gamma'} \ @\ \star; \cdot; \Gamma^{perm} \vdash_{\mathcal{P}(\gamma)} \kappa[V_h] \sim A_\gamma \ @\ \omega.$

By Lemma C.7,

C,«[Vy at *iM* :: $F_t$ at y :: A, 7 ~ $A_7$ @ a;, y ^ Ay/ @ •.

By Lemma C.8,

C, /c[Vh] at 7, $y_t$ at *i* :: A, 7 ~ $^4_7$ @ a;, y ~ Ay/ @ •.

The case for C, ^[readchan chanvar Y\ at 7, V^ :: Vt at *i ::* A, 7 ~ $^4_7$ @ •, y ~ Ay/ @ • is similar, except that we use Lemma C.8 instead of Lemma C.7.

The two cases with Y ~ *Ay* @ *u/* for some node u/ are impossible because of the rule Tchanv.

Case C, «[writechan (chanvar Y) V] at 7, *V* :: • • • :: $V_n$ :: nil at Y => C,/c[V] at 7, Vi :: • • • :: $V_n$ :: *V* :: nil at Y

If C, «;[writechan (chanvar y) V] at 7, Vi :: ··· :: V^ :: nil at y :: A, 7 ~ Ay @ a;, y ~ Ay @ •, then

A, 7 ~ $A_\gamma$ @ a;, 7' ~ $A_{\gamma'}$ @ •; •; $\Gamma^{perm}$ $\vdash_{\mathcal{P}(\gamma)}$ «[writechan (chanvar Y) V] ~ Ay @ a;,

A, 7 ~ Ay @ a;, 7' ~ Ay/ @ •; •; $\Gamma^{perm}$ $\vdash_{\mathcal{P}(\gamma')}$ Vi :: • • • :: $V_n$ :: nil ~ Ay @ a;* for an arbitrary node $\omega^*$.

By the rules Valvr and Tvcon,

Ay/ = ^4 vlist,

A, 7 ~ ^i₇ @ a;, 7ˣ ~ Ay/ @ •; ·; $\Gamma^{perm}$ $\vdash_{\mathcal{P}(\gamma')}$ $V_1 \sim A$ @ $\omega^*$,

· · ·,

A,7 ~ $A_7$ Q u;^⁷ ~ Ay/ @ •; ·; $\Gamma^{perm}$ $\vdash_{\mathcal{P}(\gamma')}$ $V_n \sim A$ @ a;*.

By Lemma 4.4 and the rules Tchanv, Twritec, and $Val_W$,

A, 7 ~ Ay @ a;, 7⁷ ~ Ay/ @ •; •; T^¹™ hp₍₇₎ writechan (chanvar y) *V ~ A* @ *LJ*₉*

A, 7 ~ $A_7$ @ a;, 7⁷ ~ Ay/ @ •; •; $T^{perm}$ $h_{p(7)}$ *V ~ A* @ a;*,

A, 7 ~ $A_7$ @ a;, 7⁷ - Ay/@•;•;T^¹™ $h_{P(7/)}$ *V* ~ *A* @a;*.

By Lemma C.6,

A, 7 ~ $A_7$ @ o;, $\gamma'$ ~ Ay/ @ •; , $\Gamma^{perm}$ $\vdash_{\mathcal{P}(\gamma)}$ $\kappa[V] \sim A_\gamma$ @ a;.

By Lemma C.7,

C, «[V] at 7, VL :: • • • :: $F_n$ :: nil at y :: A, 7 ~ $A_\gamma$ @ $\omega$, 7' ~ Ay/ @ •.

By the rules Valvr, Tvcon, Tvnil,

A,7 - Ay @o;,y~ Ay/ @•; , TP⁶'l¹¹ $\vdash_{v(y)}$ $V_1$ :: ··· :: $F_n$ :: V :: nil ~ Ay/ @ *v**.

By Lemma C.8,

C, «[F] at 7, $V_1$ :: ··· :: $V_n$ :: V :: nil at y :: A, 7 ~ $A_\gamma$ @ a;, y ~ Ay/ @ *.

The case for C, ^[writechan (chanvar y) V] at 7, $V_1$ :: ··· :: V^ :: V :: nil at Y :: A, 7 ~ $A_7$ @ •, y ~ Ay/ @ • is similar, except that we use Lemma C.8 instead of Lemma C.7.

The two cases with Y ~ Ay/ @ a/ for some node a/ are impossible because of the rule Tchanv.

Case <; ~ *A @ u)* € TP⁶"" *V* -•pe™ V Pfr) = *U)* — Rvalvar :

C, /c[v] at 7 = ^ C, K[VJ at 7

If C, K[V] at 7 :: A, 7 ~ Ay @ *J,* then

A, 7 - Ay @ a/; •; $T^{perm}$ $h_{p(7)}$ K[V] ~ $A_7$ @ *v'*.

Since v ~ *A* @ *u e* T^¹⁷" and ^(7) = a;,

A, 7 - Ay @ a;'; •; *T*>^{erm} $\vdash_{v(y)}$ *v : A.*

By the assumption on *V* and weakening,

A,7 - Ay @ a/; .;$TP^{erm}$ h^ *V : A.*

Since ^(7) = u>,

A, 7 - Ay @ *J* •; $r^{perm}$ hf>₍₇₎ K[V] ~ $A_\gamma$ @ u;ʳ by Lemma C.6.

By Lemma C.7,

*C,K[V)* at 7 :: A, 7 ~ ^₇ @ ^.

The case for C, *K[V]* at 7 :: A, 7 ~ ^4^γ @ • is similar, except that we use Lemma C.8 instead of Lemma C.7.

●

**Proof of Lemma 4.3:**

*Proof.* By induction on the structure of A; •; $\Gamma^{perm}$ ⊢^ *M* ~ *A* @ u/. (Below we reuse all metavariables.)

Case $Cvar_W$:

impossible.

Case $\mathsf{Vvar}_W$:

$M = v$, $\omega = \omega'$, and $v \sim A @ \omega' \in \Gamma^{\mathsf{perm}}$.

Cases $\supset\mathsf{I}_W$, $\Box\mathsf{I}_W$, $\Box\mathsf{I}'_W$, $\bigcirc\mathsf{I}_W$, $\bigcirc\mathsf{I}'_W$, T(), Tsvar, Tsvar', Tvnil, Tvcon, Tchanv:

$M = V \neq v$.

Case $\dfrac{\Lambda; \cdot; \Gamma^{\mathsf{perm}} \vdash_{\omega'} V : A}{\Lambda; \cdot; \Gamma^{\mathsf{perm}} \vdash_{\omega} V \sim A @ \omega'}\ \mathsf{Val}_W\ (\omega \neq \omega')$ :

If $V = v$, then $v \sim A @ \omega' \in \Gamma^{\mathsf{perm}}$ by the rule $\mathsf{Vvar}_W$.

Case $\dfrac{\Lambda; \cdot; \Gamma^{\mathsf{perm}} \vdash_{\omega} M : A \supset B \quad \Lambda; \cdot; \Gamma^{\mathsf{perm}} \vdash_{\omega} N : A}{\Lambda; \cdot; \Gamma^{\mathsf{perm}} \vdash_{\omega} M\ N : B}\ \supset\mathsf{E}_W$ :

If $M = V \neq v$,

$M = \lambda x\!:\!A.\, M'$ by Lemma 4.2.

$M\ N = ([])[(\lambda x\!:\!A.\, M')\ N]$ and $(\lambda x\!:\!A.\, M')\ N \longrightarrow [N/x]M'$.

If $M = v$,

$v \sim A \supset B @ \omega \in \Gamma^{\mathsf{perm}}$ by the rule $\mathsf{Vvar}_W$.

$M\ N = ([]\ N)[v]$ and $v \sim A \supset B @ \omega \in \Gamma^{\mathsf{perm}}$.

If $M \neq V$,

$M = \kappa[M']$ by induction hypothesis where

$M' = v$ and $v \sim A' @ \omega \in \Gamma^{\mathsf{perm}}$,

$M' \longrightarrow N'$, or

$M'$ is eval box $N'$, eval box$_{\omega''}$ $N'$, future box $N'$, future box$_{\omega''}$ $N'$, syncwith syncvar $\gamma$, newchan$_{B'}$, readchan chanvar $\gamma$, or writechan (chanvar $\gamma$) $V'$.

Then we let $M\ N = (\kappa\ N)[M']$.

Case $\dfrac{\Lambda; \cdot; \Gamma^{\mathsf{perm}} \vdash_{\omega} M : \Box A \quad \Lambda; \cdot, x :: A; \Gamma^{\mathsf{perm}} \vdash_{\omega} N \sim B @ \omega'}{\Lambda; \cdot; \Gamma^{\mathsf{perm}} \vdash_{\omega} \mathsf{letbox}\ x = M\ \mathsf{in}\ N \sim B @ \omega'}\ \Box\mathsf{E}_W$ :

If $M = V \neq v$,

$M = \mathsf{box}\ M'$ by Lemma 4.2.

letbox $x = M$ in $N = ([])[\mathsf{letbox}\ x = \mathsf{box}\ M'\ \mathsf{in}\ N]$ and letbox $x =$ box $M'$ in $N \longrightarrow [M'/x]N$.

If $M = v$,

$v \sim \Box A @ \omega \in \Gamma^{\mathsf{perm}}$ by the rule $\mathsf{Vvar}_W$.

letbox $x = M$ in $N = (\mathsf{letbox}\ x = []\ \mathsf{in}\ N)[v]$ and $v \sim \Box A @ \omega \in \Gamma^{\mathsf{perm}}$.

If $M \neq V$,

$M = \kappa[M']$ by induction hypothesis where

$M' = v$ and $v \sim A' @ \omega \in \Gamma^{\mathsf{perm}}$,

$M' \longrightarrow N'$, or

$M'$ is eval box $N'$, eval box$_{\omega''}$ $N'$, future box $N'$, future box$_{\omega''}$ $N'$, syncwith syncvar $\gamma$, newchan$_{B'}$, readchan chanvar $\gamma$, or writechan (chanvar $\gamma$) $V'$.

Then we let letbox $x = M$ in $N = (\mathsf{letbox}\ x = \kappa\ \mathsf{in}\ N)[M']$.

Case $\Box\mathsf{E}'_W$ is similar to Case $\Box\mathsf{E}_W$.

Case $\dfrac{\Lambda; \cdot; \Gamma^{\mathsf{perm}} \vdash_{\omega} M : \bigcirc A \quad \Lambda; \cdot, v \sim A; \Gamma^{\mathsf{perm}} \vdash_{\omega} N \sim B @ \omega'}{\Lambda; \cdot; \Gamma^{\mathsf{perm}} \vdash_{\omega} \mathsf{letcir}\ v = M\ \mathsf{in}\ N \sim B @ \omega'}\ \bigcirc\mathsf{E}_W$ :

If $M = V \neq v'$,

$M = \mathsf{cir}\ M'$ by Lemma 4.2 and

$$\frac{\textit{fresh}\ \omega^* \quad \Lambda; \cdot; \Gamma^{\mathsf{perm}} \vdash_{\omega} M' \sim A @ \omega^*}{\Lambda; \cdot; \Gamma^{\mathsf{perm}} \vdash_{\omega} \mathsf{cir}\ M' : \bigcirc A}\ \bigcirc\mathsf{I}_W.$$

1) If $M' = V' \neq v''$,

letcir $v = M$ in $N$ = (Q)[letcir $v$ = cir $V'$ in $N$] and letcir $v$ = cir $V$ in $N$ —• $[V'/v]N$.

2) $M^r = v''$ is impossible.

$M^f = K[M'']$ by induction hypothesis where

$M'' = v''$ and $v''$~$A'$@$u$>€ $T$**™,

$M''$ —> $N$\ or

$M''$ is eval box $N$\ eval box^" $N$\ future box $N$\ future box^// TV', syncwith syncvar 7, newchan^/, readchan chanvar 7, or writechan (chanvar 7) $V''$.

Then we let letcir $v = M$ in $N$ = (letcir t> = cir $K$ in AT)[$M^{7/}$].

If M = i/,

v ^ O i @ a ; G $T^{perm}$ by the rule Vvar^.

letcir $v = M$ jn $N$ = (letcir t; = Q in JV)[t/] and v' ~ Oi4 @ a; G $T^{perm}$.

If $M \neq V$,

M = K[$M^X$] by induction hypothesis where

$M' = v'$ and $v^7$ - $A!$ @ $u$> € $T$*™,

$M^f$ —> $N'$, or

$M^f$ is eval box $N$\ eval box^// $AT^7$, future box $iV^7$, future box^// $A$^$^7$, syncwith syncvar 7, newchan^, readchan chanvar 7, or writechan (chanvar 7) $V$.

Then we let letcir $v = M$ \n $N$ = (letcir t> = AC in $N)[M']$.

Case $OE^7$^ is similar to Case $OEw$, except that Subcases 1) and 2) are now combined as follows:

If $M'$ = $V$\

letcir $v = M$ in $N$ = (Q)[letcir v = cir^* $V$ in iV] and letcir $v$ = cir^* $V^1$ in JV —• $[V'/v]N$.

Case $\dfrac{\quad prim}{\Lambda; \cdot; \Gamma^{perm} \vdash_\omega M \sim A_{prim} @ \omega'}$ Prim~$_W$ $(\omega \neq \omega')$ :

If $M$ = V 7^ v by induction hypothesis, we are done.

$M = v$ and $v$ ~ $Apri_m$ @ $u$ G $r^{perm}$ cannot happen by the assumption on $\Gamma^{perm}$.

If $M$ = AC[$M^7$] by induction hypothesis where

$M^f = v$ and $v$ ~ $A'$ @ $w$ G $r^{perm}$,

$M^7$ —• $iV^7$, or

$M^1$ is eval box $N$\ eval box^// $A$/^$^7$, future box $N$\ future box^// $AT^7$, syncwith syncvar 7, newchan^/, readchan chanvar 7, or writechan (chanvar 7) $V$\

then we are done.

CaSC $\dfrac{}{\text{A; •; TP}^{erm} \text{ H}_W \text{ eval M : unit}}$ Teval :

If $M = V \neq v$,

$M$ = box $M'$ by Lemma 4.2.

eval M = (Q)[eval box M'].

If Af = «,

t; ~ $DA$ @ $UJ$ € $TP^{6}$"" by the rule Vvar^.

eval $M$ = (eval D)[v] and $v$ ~ D^4 @ w 6 $\Gamma^{perm}$.

If $M \neq V$,

M = K[M'] by induction hypothesis where

$M'$ = u and v ~ $A'$ @ $u$> € $r^{perm}$,

M' —» AT, or

$M'$ is eval box $N'$, eval box^," AT', future box AT', future box^w $N'$, syncwith syncvar 7, newchan^s readchan chanvar 7, or writechan (chanvar 7) $V$.

Then we let eval $M = (\text{eval } \kappa)[M']$.

Case Teval@ is similar to Case Teval.

Case $\dfrac{\Lambda; \cdot; \Gamma^{\text{perm}} \vdash_\omega M : \Box\bigcirc A}{\Lambda; \cdot; \Gamma^{\text{perm}} \vdash_\omega \text{future } M \sim A \text{ sync} @ \omega^*}$ Tfuture :

If $M = V \neq v$,

$M = \text{box } M'$ by Lemma 4.2.

future $M = ([])[\text{future box } M']$.

If $M = v$,

$v \sim \Box\bigcirc A @ \omega \in \Gamma^{\text{perm}}$ by the rule $\text{Vvar}_W$.

future $M = (\text{future } [])[v]$ and $v \sim \Box\bigcirc A @ \omega \in \Gamma^{\text{perm}}$.

If $M \neq V$,

$M = \kappa[M']$ by induction hypothesis where

$M' = v$ and $v \sim A' @ \omega \in \Gamma^{\text{perm}}$,

$M' \longrightarrow N'$, or

$M'$ is eval box $N'$, eval $\text{box}_{\omega''}$ $N'$, future box $N'$, future $\text{box}_{\omega''}$ $N'$, syncwith syncvar $\gamma$, $\text{newchan}_{B'}$, readchan chanvar $\gamma$, or writechan (chanvar $\gamma$) $V'$.

Then we let future $M = (\text{future } \kappa)[M']$.

Cases Tfuture@, Tfuture′, and Tfuture@′ are similar to Case Tfuture.

Case $\dfrac{\Lambda; \cdot; \Gamma^{\text{perm}} \vdash_\omega M : A \text{ sync}}{\Lambda; \cdot; \Gamma^{\text{perm}} \vdash_\omega \text{syncwith } M \sim A @ \omega^*}$ Tswith :

If $M = V \neq v$,

$M = \text{syncvar } \gamma$ by Lemma 4.2.

syncwith $M = ([])[\text{syncwith syncvar } \gamma]$.

If $M = v$,

$v \sim A \text{ sync} @ \omega \in \Gamma^{\text{perm}}$ by the rule $\text{Vvar}_W$.

syncwith $M = (\text{syncwith } [])[v]$ and $v \sim A \text{ sync} @ \omega \in \Gamma^{\text{perm}}$.

If $M \neq V$,

$M = \kappa[M']$ by induction hypothesis where

$M' = v$ and $v \sim A' @ \omega \in \Gamma^{\text{perm}}$,

$M' \longrightarrow N'$, or

$M'$ is eval box $N'$, eval $\text{box}_{\omega''}$ $N'$, future box $N'$, future $\text{box}_{\omega''}$ $N'$, syncwith syncvar $\gamma$, $\text{newchan}_{B'}$, readchan chanvar $\gamma$, or writechan (chanvar $\gamma$) $V'$.

Then we let syncwith $M = (\text{syncwith } \kappa)[M']$.

Case Tswith′ is similar to Case Tswith.

Case $\dfrac{}{\Lambda; \cdot; \Gamma^{\text{perm}} \vdash_\omega \text{newchan}_A \sim A \text{ chan} @ \omega^*}$ Tnewc :

$\text{newchan}_A = ([])[\text{newchan}_A]$.

Case $\dfrac{\Lambda; \cdot; \Gamma^{\text{perm}} \vdash_\omega M : A \text{ chan}}{\Lambda; \cdot; \Gamma^{\text{perm}} \vdash_\omega \text{readchan } M \sim A @ \omega^*}$ Treadc :

If $M = V \neq v$,

$M = \text{chanvar } \gamma$ by Lemma 4.2.

readchan $M = ([])[\text{readchan chanvar } \gamma]$.

If $M = v$,

$v \sim A \text{ chan} @ \omega \in \Gamma^{\text{perm}}$ by the rule $\text{Vvar}_W$.

readchan $M = (\text{chanvar } [])[v]$ and $v \sim A \text{ chan} @ \omega \in \Gamma^{\text{perm}}$.

If $M \neq V$,

$M = \kappa[M']$ by induction hypothesis where

$M' = v$ and $v \sim A' @ \omega \in \Gamma^{\text{perm}}$,

$M' \longrightarrow N'$, or

*M'* is eval box *M* eval box^" *M* future box *M* future box^// AT⁷, syncwith syncvar 7, newchan^s readchan chanvar 7, or writechan (chanvar 7) *V.*

Then we let readchan *M* = (readchan /^[M⁷].

$$\text{CaSe}\ \frac{A;\bullet;r\ \text{perm}\ h\ \wedge\ M:\wedge\ \text{chan}\quad \textit{fresh J}\quad A;\bullet;r^{perm}\ h,\ N \sim A@\_\wedge}{A;\bullet;F^{*""}\ h\wedge\ \text{writechan}\ M\ AT \sim A @ u;*}\ \text{Twritec}:$$

If $M =$

*M* = chanvar 7 by Lemma 4.2.

1) If $N = V' \neq v'$,

writechan *M N* = ([]) [writechan (chanvar 7) V⁷].

2) If *N* = *v'* is impossible.

3) If $N \neq V'$,

$N = \kappa[N']$ by induction hypothesis where

*N'* = *v^f* and *v^r* - *A'* @ a; G rP^perm,

JV'—•JV^,or

*N^f* is eval box *N^f* eval box^// JV⁷', future box *N^f* future box$_{\omega''}$ $N''$, syncwith syncvar V, newchan^/, readchan chanvar Y, or writechan (chanvar y) *V".*

Then we let writechan *M N* = (writechan (chanvar 7) *K)[N'].*

If $M = v$,

*v* ~ *A* chan @ *u* G r^perm by the rule Vvar$_W$.

writechan *M N* = (writechan \\ *N)[v]* and *v* ~ *A* chan @ $\omega$ G r^perm.

If $M \neq V$,

M = K[M⁷] by induction hypothesis where

*M'* = *vandv~A'@u;e* r^perm,

M⁷—>iV⁷,or

M⁷ is eval box A/^⁷, eval box^" AT⁷, future box TV⁷, future box^// iV⁷, syncwith syncvar 7, newchan^', readchan chanvar 7, or writechan (chanvar 7) *V.*

Then we let writechan *M N* = (writechan *K N)[M'].* •

**Proof of Theorem 4.5:**

***Proof.***

**Suppose *C* = Co, *M* at 7. By the rule Tcfg, we have A; •; T^^1TM h^ M - *A* @ a;⁷ for ^(7) = a; and a certain node a/. By Lemma 4.3, we consider the following cases:**

- $M = V \neq v$.
- *M* = *v* (where *v* ~ *A@u;^f e* r^perm)
- *M* = *k[v], v* ~ *B* *@u> e* r**^1TM, and

$$\frac{v \sim B\ @(j\ G\ r^{perm}\quad V \to_{perm} V \quad \mathcal{P}(\gamma) = \omega}{C_o, K[V]\ at\ 7 \Rightarrow Co, K[F]\ at\ 7}\ \text{Rvalvar}.$$

- *M* = *K[N]* where AT —• *N* and

$$\frac{N \longrightarrow N'}{Co, K[N]\ at\ 7 \Rightarrow Co, \kappa[iV]\ at\ 7}\ \text{Rcfg}.$$

• *M* = «[eval box *N]* and

$$\frac{new\ 7'}{\text{Co, tf[eval box } N] \text{ at } 7 \Rightarrow C_o, *[()] \text{ at } 7, AT \text{ at } \gamma'} \text{ Reval}.$$

• *M* = *c[eval box^" *N]* and

$$\frac{\text{new } 7' @ u/'}{C_o, /c[\text{eval box}^\wedge/ AT] \text{ at } 7 \Rightarrow Co, «[()] \text{ at } 7, AT \text{ at } V} \text{ Reval®}.$$

• *M* = /c[future box iV] and

$$\frac{new\ 7'}{\text{Co, /^[future box AT] at 7 => Co, «:[syncvar 7^ at 7, letcir i; = AT in } v \text{ at V}} \text{ Rfuture}.$$

• *M* = *K*[future box^// *N]* and

$$\frac{\text{new V} @ UJ''}{\text{Co, /c[future box^// } N] \text{ at 7 ==> Co, ^[syncvar } T^7] \text{ at 7, letcir } v = N\ mv\ at\ \gamma'} \text{ Rfuture@}.$$

• *M* = /^[syncwith syncvar y] and *V* at $T^7$ ^ Co- (£.g., M at Y € Co and M is not a value.)

• *M* = *;[syncwith syncvar 7'], *V* at V € Co, and

$$\frac{}{\text{Co, /c[syncwith syncvar 7'] at 7 =£> Co, } K[V] \text{ at 7}} \text{ Rswith}.$$

• *M* = ^[newchan^] and

$$\frac{new\ V}{\text{Co, K[newchan£] at 7 => Co, ^[chanvar 7'] at 7, nil at Y}} \text{ Rnewc}.$$

• *M* = KJreadchan chanvar Y].

By Lemma 4.4,

A; •; $T^{\wedge 1}$™ ho; readchan chanvar Y ~ ^ @ a;".

By the rule Treadc (optionally preceded by the rule Prim~^ if *B* is a primitive type),

A; •; $T^{\wedge rpn}$ h^ chanvar Y : *B* chan.

By the rule Tchanv,

*i* ~ B vlist @ • € A.

Since C :: A,

C = $C'_0$,*M* at 7, AT at $7^7$ and A; •; $T^{\wedge 1}$™ $h_{p(7}$/) AT ~ JB vlist @ a;* for a fresh node a;*.

- $N = V_h :: V_t$ and

$$\frac{}{\text{CQ, ^[readchan chanvar Y] at 7, V^ :: } V_t \text{ at Y => Co'}^{K}i^v h] \text{ at } 7> \wedge* \text{ at Y}} \text{ Rreadc}.$$

- AT ^ 14 :: $V_t$.

• $M$ = ^[writechan (chanvar Y) $V$).

By Lemma 4.4,

A; •; r^rm $h_w$ writechan (chanvar 7') $V$ ~ $B$ Q a;77.

By the rule Twritec (optionally preceded by the rule *Pr\xr\~w* if -B is a primitive type),

A; •; $T^{perm}$ ho, chanvar 7' : £ chan.

By the rule Tchanv,

$7^7$ ~ 5 vlist @ • G A.

Since C :: A,

*C* = *C^M* at 7, AT at y and A; •; T^1TM $hp_{(y)}$ A^ ~ *B* vlist @ a;* for a fresh node uA

- *N* = *Vi* :: • ··:: $V_n$ :: nil and

$$\frac{C\dot{Q}, /c[\text{writechan (chanvar y) F] at 7, Vi} :: \cdots :: V_n :: \text{nil at y} =\hat{}}{\text{CJ,K[V] at 7,Fi} :: \cdots :: F_n :: F :: \text{nil at } i} \text{ Rwritec}$$

- -Y^Vi ::-.-:: $V_n$:: nil.

Therefore, if there exists no C" such that C ==> C", C consists only of the following:

F at 7,
/c[syncwith syncvar y] at 7 (where V at y 0 C),
K[readchan chanvar y] at 7 (where *Vh* :: T4 at y 0 C),
/c[writechan (chanvar y) F] at 7 (where Fi ::•••:: $V_n$ :: nil at y ^ C). D