Compiling Dependent Types Without Continuations (Technical Appendix)

ANONYMOUS AUTHOR(S)

TECHNICAL APPENDIX

This document includes extended figures, proofs, and discussion for the paper of the same title.

1 SOURCE: ECC WITH DEFINITIONS

Our source language, ECC, is Luo's Extended Calculus of Constructions (ECC) [Luo 1990] extended with dependent elimination of booleans and with definitions [Severi and Poll 1994]. We typeset ECC in a non-bold, blue, sans-serif font. We present the syntax of ECC in Figure 1. ECC extends the Calculus of Constructions (CC) [Coquand and Huet 1988] with Σ types (strong dependent pairs) and an infinite predicative hierarchy of universes. There is no explicit phase distinction, *i.e.*, there is no syntactic distinction between *terms*, which represent run-time expressions, and *types*, which classify terms. However, we usually use the meta-variable e to evoke a term, and the meta-variables A and B to evoke a type. The language includes one impredicative universe, Prop, and an infinite hierarchy of predicative universes Type_i. The syntax of expressions e includes names x, universes U, dependent function types $\Pi\,\mathsf{x} : \mathsf{A}.\,\mathsf{B}$, functions $\lambda\,\mathsf{x} : \mathsf{A}.\,\mathsf{e}$, application $\mathsf{e}_1\ \mathsf{e}_2$, dependent pair types $\Sigma\,\mathsf{x} : \mathsf{A}.\,\mathsf{B}$, dependent pairs $\langle \mathsf{e}_1, \mathsf{e}_2 \rangle\ \mathsf{as}\ \Sigma\,\mathsf{x} : \mathsf{A}.\,\mathsf{B}$, first $\mathsf{fst}\ \mathsf{e}$ and second $\mathsf{snd}\ \mathsf{e}$ projections of dependent pairs, dependent let $\mathsf{let}\ \mathsf{x} = \mathsf{e}\ \mathsf{in}\ \mathsf{e}'$, the boolean type bool, the boolean value true and false, and dependent if $\mathsf{if}\ \mathsf{e}\ \mathsf{then}\ \mathsf{e}_1\ \mathsf{else}\ \mathsf{e}_2$. For brevity, we omit the type annotation on dependent pairs, as in $\langle \mathsf{e}_1, \mathsf{e}_2 \rangle$. Note that let-bound definitions do not include type annotations; this is not standard, but type checking is still decidable [Severi and Poll 1994], and it simplifies our ANF translation[1].

For simplicity, we assume uniqueness of names and ignore capture-avoiding substitution. This is standard practice, but is worth pointing out explicitly anyway.

In Figure 2, we give the reductions $\Gamma \vdash \mathsf{e} \rhd \mathsf{e}'$ for ECC, which are entirely standard. As usual, we extend reduction to conversion by defining $\Gamma \vdash \mathsf{e} \rhd^* \mathsf{e}'$ to be the reflexive, transitive, compatible closure of reduction $\rhd$. The conversion relation, defined in Figure 3, is used to compute equivalence between types, but we can also view it as the operational semantics for the language. We define $\mathsf{eval}(\mathsf{e})$ as the evaluation function for whole-programs using conversion, which we use in our compiler correctness proof.

In Figure 4 we define *definitional equivalence* (or just *equivalence*) $\Gamma \vdash \mathsf{e} \equiv \mathsf{e}'$ as conversion up to η-equivalence. We usually we the notation $\mathsf{e}_1 \equiv \mathsf{e}_2$ for equivalence, eliding the environment when it is obvious or unnecessary. We also define *cumulativity* (subtyping) $\Gamma \vdash \mathsf{A} \preceq \mathsf{B}$, to allow types in lower universes to inhabit higher universes.

We define the type system for ECC in Figure 5, which is mutually defined with well-formedness of environments in Figure 6. The typing rules are entirely standard for a dependent type system. Note that types themselves, such as $\Pi\,\mathsf{x} : \mathsf{A}.\,\mathsf{B}$ have types (called universes), and universes also have types which are higher universes. In [Ax-Prop], the type of Prop is Type_0, and in [Ax-Type], the type of each universe Type_i is the next higher universe Type_{i+1}. Note that we have impredicative function types in Prop, given by [Prod-Prop]. For this work, we ignore the Set vs Prop distinction used in some type theories, such as Coq's, although adding it causes no difficulty. Note that the rules for application, [App], second projection, [Snd], let, [Let], and if [If] substitute sub-expressions into the type system. These are the key typing rules that introduce difficulty in type-preserving compilation for dependent types.

*We use a non-bold blue sans-serif font to typeset the source language, and a **bold red serif font** for the target language. The fonts are distinguishable in black-and-white, but the paper is easier to read when viewed in color.

[1] We describe in Section 3 how to extend the ANF translation to support annotated `let`.

2020. 2475-1421/2020/1-ART1 $15.00
https://doi.org/

$$
\begin{array}{llcl}
\textit{Universes} & \mathsf{U} & ::= & \mathsf{Prop} \mid \mathsf{Type}\,_i \\
\textit{Expressions} & \mathsf{e}, \mathsf{A}, \mathsf{B} & ::= & \mathsf{x} \mid \mathsf{U} \mid \Pi\, \mathsf{x} : \mathsf{A}.\, \mathsf{B} \mid \lambda\, \mathsf{x} : \mathsf{A}.\, \mathsf{e} \mid \mathsf{e}\ \mathsf{e} \mid \Sigma\, \mathsf{x} : \mathsf{A}.\, \mathsf{B} \mid \langle \mathsf{e}_1, \mathsf{e}_2 \rangle\ \mathsf{as}\ \Sigma\, \mathsf{x} : \mathsf{A}.\, \mathsf{B} \\
 & & \mid & \mathsf{fst}\ \mathsf{e} \mid \mathsf{snd}\ \mathsf{e} \mid \mathsf{let}\ \mathsf{x} = \mathsf{e}\ \mathsf{in}\ \mathsf{e} \mid \mathsf{bool} \mid \mathsf{true} \mid \mathsf{false} \mid \mathsf{if}\ \mathsf{e}\ \mathsf{then}\ \mathsf{e}_1\ \mathsf{else}\ \mathsf{e}_2 \\
\textit{Environments} & \Gamma & ::= & \cdot \mid \Gamma, \mathsf{x} : \mathsf{A} \mid \Gamma, \mathsf{x} = \mathsf{e}
\end{array}
$$

Fig. 1. ECC Syntax

$\boxed{\Gamma \vdash \mathsf{e} \rhd \mathsf{e}'}$

$$
\begin{array}{rcll}
\mathsf{x} & \rhd_\delta & \mathsf{e} & \text{where } \mathsf{x} = \mathsf{e} \in \Gamma \\
(\lambda\, \mathsf{x} : \mathsf{A}.\, \mathsf{e}_1)\ \mathsf{e}_2 & \rhd_\beta & \mathsf{e}_1[\mathsf{x} := \mathsf{e}_2] & \\
\mathsf{fst}\ \langle \mathsf{e}_1, \mathsf{e}_2 \rangle & \rhd_{\pi_1} & \mathsf{e}_1 & \\
\mathsf{snd}\ \langle \mathsf{e}_1, \mathsf{e}_2 \rangle & \rhd_{\pi_2} & \mathsf{e}_2 & \\
\mathsf{let}\ \mathsf{x} = \mathsf{e}\ \mathsf{in}\ \mathsf{e}' & \rhd_\zeta & \mathsf{e}'[\mathsf{x} := \mathsf{e}] & \\
\mathsf{if}\ \mathsf{true}\ \mathsf{then}\ \mathsf{e}_1\ \mathsf{else}\ \mathsf{e}_2 & \rhd_{\iota_1} & \mathsf{e}_1 & \\
\mathsf{if}\ \mathsf{false}\ \mathsf{then}\ \mathsf{e}_1\ \mathsf{else}\ \mathsf{e}_2 & \rhd_{\iota_2} & \mathsf{e}_2 &
\end{array}
$$

$\boxed{\Gamma \vdash \mathsf{e} \rhd^* \mathsf{e}'}$

$$
\dots \qquad \frac{\Gamma, \mathsf{x} = \mathsf{e} \vdash \mathsf{e}_1 \rhd^* \mathsf{e}_2}{\Gamma \vdash \mathsf{let}\ \mathsf{x} = \mathsf{e}\ \mathsf{in}\ \mathsf{e}_1 \rhd^* \mathsf{let}\ \mathsf{x} = \mathsf{e}\ \mathsf{in}\ \mathsf{e}_2}\ [\textsc{Red-Cong-Let}] \qquad \frac{}{\Gamma \vdash \mathsf{e} \rhd^* \mathsf{e}}\ [\textsc{Red-Refl}]
$$

$$
\frac{\Gamma \vdash \mathsf{e} \rhd \mathsf{e}_1 \qquad \Gamma \vdash \mathsf{e}_1 \rhd^* \mathsf{e}'}{\Gamma \vdash \mathsf{e} \rhd^* \mathsf{e}'}\ [\textsc{Red-Trans}]
$$

$\boxed{\mathsf{eval}(\mathsf{e}) = \mathsf{v}}$

$$
\mathsf{eval}(\mathsf{e}) \quad = \quad \mathsf{v} \quad \text{where } \mathsf{e} \rhd^* \mathsf{v} \text{ and } \mathsf{v} \not\rhd \mathsf{v}'
$$

Fig. 2. ECC Reduction, Conversion, and Evaluation (excerpts)

$$\frac{\Gamma \vdash A \rhd^* A' \qquad \Gamma, x : A \vdash e \rhd^* e'}{\Gamma \vdash \lambda\, x : A.\, e \rhd^* \lambda\, x : A'.\, e'} \text{ [Red-Cong-Lam1]} \qquad \frac{\Gamma \vdash A \rhd^* A' \qquad \Gamma, x : A \vdash B \rhd^* B'}{\Gamma \vdash \Pi\, x : A.\, B \rhd^* \Pi\, x : A'.\, B'} \text{ [Red-Cong-Pi]}$$

$$\frac{\Gamma \vdash A \rhd^* A' \qquad \Gamma, x : A \vdash B \rhd^* B'}{\Gamma \vdash \Sigma\, x : A.\, B \rhd^* \Sigma\, x : A'.\, B'} \text{ [Red-Cong-Sig]}$$

$$\frac{\Gamma \vdash e_1 \rhd^* e_1' \qquad \Gamma \vdash e_2 \rhd^* e_2' \qquad \Gamma \vdash A \rhd^* A'}{\Gamma \vdash \langle e_1, e_2 \rangle \text{ as } A \rhd^* \langle e_1', e_2' \rangle \text{ as } A'} \text{ [Red-Cong-Pair]} \qquad \frac{\Gamma \vdash e_1 \rhd^* e_1' \qquad \Gamma \vdash e_2 \rhd^* e_2'}{\Gamma \vdash e_1\; e_2 \rhd^* e_1'\; e_2'} \text{ [Red-Cong-App]}$$

$$\frac{\Gamma \vdash V \rhd^* V'}{\Gamma \vdash \text{fst } V \rhd^* \text{fst } V'} \text{ [Red-Cong-Fst]} \qquad \frac{\Gamma \vdash V \rhd^* V'}{\Gamma \vdash \text{snd } V \rhd^* \text{snd } V'} \text{ [Red-Cong-Snd]}$$

$$\frac{\Gamma, x = N \vdash M \rhd^* M'}{\Gamma \vdash \text{let } x = N \text{ in } M \rhd^* \text{let } x = N \text{ in } M'} \text{ [Red-Cong-Let]}$$

$$\frac{\Gamma \vdash e \rhd^* e' \qquad \Gamma \vdash e_1 \rhd^* e_1' \qquad \Gamma \vdash e_2 \rhd^* e_2'}{\Gamma \vdash \text{if } e \text{ then } e_1 \text{ else } e_2 \rhd^* \text{if } e' \text{ then } e_1' \text{ else } e_2'} \text{ [Red-Cong-If]}$$

Fig. 3. ECC Congruence Conversion Rules

$\boxed{\Gamma \vdash e \equiv e'}$

$$\frac{\Gamma \vdash e_1 \rhd^* e \qquad \Gamma \vdash e_2 \rhd^* e}{\Gamma \vdash e_1 \equiv e_2} \text{ [}\equiv\text{]} \qquad \frac{\Gamma \vdash e_1 \rhd^* \lambda\, x : A.\, e \qquad \Gamma \vdash e_2 \rhd^* e_2' \qquad \Gamma, x : A \vdash e \equiv e_2'\; x}{\Gamma \vdash e_1 \equiv e_2} \text{ [}\equiv\text{-}\eta_1\text{]}$$

$$\frac{\Gamma \vdash e_1 \rhd^* e_1' \qquad \Gamma \vdash e_2 \rhd^* \lambda\, x : A.\, e \qquad \Gamma, x : A \vdash e_1'\; x \equiv e}{\Gamma \vdash e_1 \equiv e_2} \text{ [}\equiv\text{-}\eta_2\text{]}$$

$\boxed{\Gamma \vdash A \preceq B}$

$$\frac{\Gamma \vdash A \equiv B}{\Gamma \vdash A \preceq B} \text{ [}\preceq\text{-}\equiv\text{]} \qquad \frac{\Gamma \vdash A \preceq A' \qquad \Gamma \vdash A' \preceq B}{\Gamma \vdash A \preceq B} \text{ [}\preceq\text{-Trans]} \qquad \frac{}{\Gamma \vdash \text{Prop} \preceq \text{Type}_{0}} \text{ [}\preceq\text{-Prop]}$$

$$\frac{}{\Gamma \vdash \text{Type}_{i} \preceq \text{Type}_{i+1}} \text{ [}\preceq\text{-Cum]} \qquad \frac{\Gamma \vdash A_1 \equiv A_2 \qquad \Gamma, x_1 : A_2 \vdash B_1 \preceq B_2[x_2 := x_1]}{\Gamma \vdash \Pi\, x_1 : A_1.\, B_1 \preceq \Pi\, x_2 : A_2.\, B_2} \text{ [}\preceq\text{-Pi]}$$

$$\frac{\Gamma \vdash A_1 \preceq A_2 \qquad \Gamma, x_1 : A_2 \vdash B_1 \preceq B_2[x_2 := x_1]}{\Gamma \vdash \Sigma\, x_1 : A_1.\, B_1 \preceq \Sigma\, x_2 : A_2.\, B_2} \text{ [}\preceq\text{-Sig]}$$

Fig. 4. ECC Equivalence and Subtyping

$\boxed{\Gamma \vdash e : A}$

$$\frac{\vdash \Gamma}{\Gamma \vdash \mathsf{Prop} : \mathsf{Type}_0}\ [\textsc{Ax-Prop}] \qquad \frac{\vdash \Gamma}{\Gamma \vdash \mathsf{Type}_i : \mathsf{Type}_{i+1}}\ [\textsc{Ax-Type}] \qquad \frac{x : A \in \Gamma}{\Gamma \vdash x : A}\ [\textsc{Var}]$$

$$\frac{\Gamma \vdash e : A \qquad \Gamma, x : A, x = e \vdash e' : B}{\Gamma \vdash \mathsf{let}\ x = e\ \mathsf{in}\ e' : B[x := e]}\ [\textsc{Let}] \qquad \frac{\Gamma \vdash A : \mathsf{Type}_i \qquad \Gamma, x : A \vdash B : \mathsf{Prop}}{\Gamma \vdash \Pi\, x : A.\, B : \mathsf{Prop}}\ [\textsc{Prod-Prop}]$$

$$\frac{\Gamma \vdash A : \mathsf{Type}_i \qquad \Gamma, x : A \vdash B : \mathsf{Type}_i}{\Gamma \vdash \Pi\, x : A.\, B : \mathsf{Type}_i}\ [\textsc{Prod-Type}] \qquad \frac{\Gamma, x : A \vdash e : B}{\Gamma \vdash \lambda\, x : A.\, e : \Pi\, x : A.\, B}\ [\textsc{Lam}]$$

$$\frac{\Gamma \vdash e : \Pi\, x : A'.\, B \qquad \Gamma \vdash e' : A'}{\Gamma \vdash e\ e' : B[x := e']}\ [\textsc{App}] \qquad \frac{\Gamma \vdash A : \mathsf{Type}_i \qquad \Gamma, x : A \vdash B : \mathsf{Type}_i}{\Gamma \vdash \Sigma\, x : A.\, B : \mathsf{Type}_i}\ [\textsc{Sig}]$$

$$\frac{\Gamma \vdash e_1 : A \qquad \Gamma \vdash e_2 : B[x := e_1]}{\Gamma \vdash \langle e_1, e_2 \rangle\ \mathsf{as}\ \Sigma\, x : A.\, B : \Sigma\, x : A.\, B}\ [\textsc{Pair}] \qquad \frac{\Gamma \vdash e : \Sigma\, x : A.\, B}{\Gamma \vdash \mathsf{fst}\ e : A}\ [\textsc{Fst}] \qquad \frac{\Gamma \vdash e : \Sigma\, x : A.\, B}{\Gamma \vdash \mathsf{snd}\ e : B[x := \mathsf{fst}\ e]}\ [\textsc{Snd}]$$

$$\frac{\vdash \Gamma}{\Gamma \vdash \mathsf{bool} : \mathsf{Type}_0}\ [\textsc{Bool}] \qquad \frac{\vdash \Gamma}{\Gamma \vdash \mathsf{true} : \mathsf{bool}}\ [\textsc{True}] \qquad \frac{\vdash \Gamma}{\Gamma \vdash \mathsf{false} : \mathsf{bool}}\ [\textsc{False}]$$

$$\frac{\Gamma, x : \mathsf{bool} \vdash B : U \qquad \Gamma \vdash e : \mathsf{bool} \qquad \Gamma \vdash e_1 : B[x := \mathsf{true}] \qquad \Gamma \vdash e_2 : B[x := \mathsf{false}]}{\Gamma \vdash \mathsf{if}\ e\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 : B[x := e]}\ [\textsc{If}]$$

$$\frac{\Gamma \vdash e : A \qquad \Gamma \vdash B : U \qquad \Gamma \vdash A \preceq B}{\Gamma \vdash e : B}\ [\textsc{Conv}]$$

Fig. 5. ECC Typing

$\boxed{\vdash \Gamma}$

$$\frac{}{\vdash \cdot}\ [\textsc{W-Empty}] \qquad \frac{\vdash \Gamma \qquad \Gamma \vdash A : U}{\vdash \Gamma, x : A}\ [\textsc{W-Assum}] \qquad \frac{\vdash \Gamma \qquad \Gamma \vdash e : A}{\vdash \Gamma, x = e}\ [\textsc{W-Def}]$$

Fig. 6. ECC Well-Formed Environments

Universes	$\mathbf{U}$	::=	$\mathbf{Prop} \mid \mathbf{Type}_i$
Values	$\mathbf{V}$	::=	$\mathbf{x} \mid \mathbf{U} \mid \lambda\,\mathbf{x} : \mathbf{M}.\,\mathbf{M} \mid \Pi\,\mathbf{x} : \mathbf{M}.\,\mathbf{M} \mid \Sigma\,\mathbf{x} : \mathbf{M}.\,\mathbf{M} \mid \langle \mathbf{V}, \mathbf{V} \rangle \mid \mathbf{bool} \mid \mathbf{true} \mid \mathbf{false}$
Computations	$\mathbf{N}$	::=	$\mathbf{V} \mid \mathbf{V}\,\mathbf{V} \mid \mathbf{fst}\,\mathbf{V} \mid \mathbf{snd}\,\mathbf{V}$
Configurations	$\mathbf{M}$	::=	$\mathbf{N} \mid \mathbf{let}\,\mathbf{x} = \mathbf{N}\,\mathbf{in}\,\mathbf{M} \mid \mathbf{if}\,\mathbf{V}\,\mathbf{then}\,\mathbf{M}_1\,\mathbf{else}\,\mathbf{M}_2$
Continuations	$\mathbf{K}$	::=	$[\cdot] \mid \mathbf{let}\,\mathbf{x} = [\cdot]\,\mathbf{in}\,\mathbf{M}$
Environments	$\mathbf{\Gamma}$	::=	$\cdot \mid \mathbf{\Gamma}, \mathbf{x} : \mathbf{A} \mid \mathbf{\Gamma}, \mathbf{x} = \mathbf{V} \mid \mathbf{\Gamma}, \mathbf{V} = \mathbf{V}$

Fig. 7. ECC^A Syntax

...

$$\frac{\mathbf{\Gamma}, \mathbf{x} : \mathbf{bool} \vdash \mathbf{B} : \mathbf{U} \qquad \mathbf{\Gamma} \vdash \mathbf{e} : \mathbf{bool} \qquad \mathbf{\Gamma}, \mathbf{e} = \mathbf{true} \vdash \mathbf{e}_1 : \mathbf{B}[\mathbf{x} := \mathbf{true}] \qquad \mathbf{\Gamma}, \mathbf{e} = \mathbf{false} \vdash \mathbf{e}_2 : \mathbf{B}[\mathbf{x} := \mathbf{false}]}{\mathbf{\Gamma} \vdash \mathbf{if}\,\mathbf{e}\,\mathbf{then}\,\mathbf{e}_1\,\mathbf{else}\,\mathbf{e}_2 : \mathbf{B}[\mathbf{x} := \mathbf{e}]}\ [\textsc{If}]$$

Fig. 8. ECC^A Typing (excerpts)

2 TARGET: ECC WITH ANF SUPPORT

Our target language, ECC^A, is a variant of ECC with a modified typing rule for dependent **if** that introduces equalities between terms (akin to the identity type), and an elimination form for assumed equalities. These extensions are similar to the extensions used by Cong and Asai [2018] to support CPS translation with dependent pattern matching. While ECC^A supports ANF syntax, the full language is not ANF restricted; it has the same syntax as ECC, and uses the usual definitional equivalence and conversion relation for type checking. We do not restrict the full language because maintaining ANF while type checking adds needless complexity; instead, we show that our compiler generates only ANF restricted terms in ECC^A, and define a separate ANF-preserving machine-like semantics for evaluating programs in ANF.

We can imagine the compilation process as either: (1) generating ANF syntax in ECC^A from ECC, or (2) as first embedding ECC in ECC^A and then rewriting ECC^A terms into ANF. In Section 3 we present the compiler as process (1), a compiler from ECC to ANF ECC^A. In this section we develop most of the supporting meta-theory necessary for ANF as intra-language equivalences and process (2) may be a more helpful intuition. We typeset ECC^A in a **bold, red, serif font**; in later sections, we reserve this font exclusively for the ANF restricted ECC^A.

Note that because the whole language is not restricted to ANF, definitional equivalence is not suitable for equational reasoning about run-time terms (*e.g.*, reasoning about optimizations), unless we ANF translate any terms rewritten by definitional equivalence. This ability to break ANF locally to support reasoning is similar to the language F_J of Maurer et al. [2017], which does not enforce ANF syntactically, but supports ANF transformation and optimization with join points.

We give the ANF syntax for ECC^A in Figure 7. We impose a syntactic distinction between *values* $\mathbf{V}$ which do not reduce, *computations* $\mathbf{N}$ which eliminate values and can be composed using *continuations* $\mathbf{K}$, and *configurations* $\mathbf{M}$ which represent the machine configurations executed by the ANF machine semantics. A continuation $\mathbf{K}$ is a program with a hole, and is composed $\mathbf{K}[\mathbf{N}]$ with a computation $\mathbf{N}$ to form a configuration $\mathbf{M}$. For example, $(\mathbf{let}\,\mathbf{x} = [\cdot]\,\mathbf{in}\,\mathbf{snd}\,\mathbf{x})[\mathbf{N}] = (\mathbf{let}\,\mathbf{x} = \mathbf{N}\,\mathbf{in}\,\mathbf{snd}\,\mathbf{x})$. Since continuations are not first-class objects, we cannot express control effects—continuations are syntactically guaranteed to be used linearly. Note that despite the *syntactic* distinctions, we still do not enforce a *phase* distinction—configurations (programs) can appear in types.

We give a new typing rule in Figure 8. The key change in ECC^A is in the typing rule for dependent if. The typing rule for $\mathbf{if}\,\mathbf{e}\,\mathbf{then}\,\mathbf{e}_1\,\mathbf{else}\,\mathbf{e}_2$ introduces an unnamed equality in each branch. This records the information that in $\mathbf{e}_1$ the target $\mathbf{e}$ being eliminated will be equal to $\mathbf{true}$ ($\mathbf{e} = \mathbf{true}$), and in $\mathbf{e}_2$ we know statically that $\mathbf{e} = \mathbf{false}$. These record a machine step: the machine will have reduced $\mathbf{e}$ to $\mathbf{true}$ before jumping to the first branch, and reduced $\mathbf{e}$ to $\mathbf{false}$ before jumping to the second branch. This is necessary to support the ANF transformation of dependent if.

$\boxed{\Gamma \vdash e \equiv e}$

$$\cdots \qquad \frac{e_1 = e_2 \in \Gamma}{\Gamma \vdash e_1 \equiv e_2}\ [\equiv\text{-Reflect}]$$

Fig. 9. ECC^A Equivalence (excerpts)

$\boxed{K\langle\langle M\rangle\rangle = M}$

$$\begin{aligned}
K\langle\langle N\rangle\rangle &\stackrel{\text{def}}{=} K[N] \\
K\langle\langle \mathbf{let}\ x = N' \ \mathbf{in}\ M\rangle\rangle &\stackrel{\text{def}}{=} \mathbf{let}\ x = N' \ \mathbf{in}\ K\langle\langle M\rangle\rangle \\
K\langle\langle \mathbf{if}\ V\ \mathbf{then}\ M_1\ \mathbf{else}\ M_2\rangle\rangle &\stackrel{\text{def}}{=} \mathbf{if}\ V\ \mathbf{then}\ (K[x][M_1//x])\ \mathbf{else}\ (K[x][M_2//x])
\end{aligned}$$

$\boxed{K\langle\langle K\rangle\rangle = K}$

$$\begin{aligned}
K\langle\langle [\cdot]\rangle\rangle &\stackrel{\text{def}}{=} K \\
K\langle\langle \mathbf{let}\ x = [\cdot]\ \mathbf{in}\ M\rangle\rangle &\stackrel{\text{def}}{=} \mathbf{let}\ x = [\cdot]\ \mathbf{in}\ K\langle\langle M\rangle\rangle
\end{aligned}$$

$\boxed{M[M//x] = M}$

$$M[M'//x] \stackrel{\text{def}}{=} (\mathbf{let}\ x = [\cdot]\ \mathbf{in}\ M)\langle\langle M'\rangle\rangle$$

Fig. 10. Composition of Configurations

We require an additional equivalence rule shown in Figure 9. The rule [≡-Reflect] is necessary for proving ANF is type preserving in the presence of dependent if. This rule is required in exactly two places in the type-preservation proof, and allows us to conclude that two terms are equivalent if the equivalence is introduced earlier in our assumptions. The addition of this rule results in undecidable type checking of ECC^A, as shown in (cite Hofmann's thesis).

In ANF, all continuations are left associated, so substitution can break ANF. Note that β-reduction takes an ANF configuration $K[(\lambda\, x : A.\, M)\ V]$ but would naïvely produce $K[M[x := V]]$. Substituting the term $M[x := V]$, a *configuration*, into the continuation K could result in the non-ANF term $\mathbf{let}\ x = M\ \mathbf{in}\ M'$. In ANF, configurations cannot be nested.

To ensure reduction preserves ANF, we define composition of a continuation K and a configuration M, Figure 10, typically called *renormalization* in the literature [Kennedy 2007; Sabry and Wadler 1997]. When composing a continuation with a configuration, $K\langle\langle M\rangle\rangle$, we essentially unnest all continuations so they remain left associated. [2] When composing a continuation with an **if** statement, notice that the continuation is duplicated in the branches. This is the usual, naïve, presentation of ANF; we show later that the join-point optimization, which avoids this duplication, is admissible in ECC^A. Note that these definitions are simplified by our uniqueness-of-names assumption.

Digression on composition in ANF. In the literature, the composition operation $K\langle\langle M\rangle\rangle$ is usually introduced as *renormalization*, as if the only intuition for why it exists is "well, it happens that ANF is not preserved under β-reduction". It is not mere coincidence; the intuition for this operation is composition, and having a syntax for composing terms is not only useful for stating β-reduction, but useful for all reasoning about ANF! This should not come as a surprise—compositional reasoning is useful. The only surprise is that the composition operation is not the usual one used in programming language semantics, *i.e.*, substitution. In ANF, as in monadic normal form, substitution can be used to compose any expression with a *value*, since names are values and values can always be replaced by values. But substitution cannot just replace a name, which is a *value*, with a *computation* or *configuration*. That wouldn't be well-typed. So how do we compose computations with configurations? We can use **let**, as in $\mathbf{let}\ y = N\ \mathbf{in}\ M$, which we can imagine as an explicit substitution. In monadic form, there is no distinction between computations and configurations, so the same term works to compose configurations. But in ANF, we

[2]Some work uses an append notation, *e.g.*, $M :: K$ [Sabry and Wadler 1997], suggesting we are appending K onto the stack for M; we prefer notation that evokes composition.

$\boxed{M \mapsto M'}$

$$
\begin{array}{rcl}
K[(\lambda\, x : A.\, M)\ V] & \mapsto_\beta & K\langle\langle M[x := V]\rangle\rangle \\
K[\mathsf{fst}\ \langle V_1, V_2\rangle] & \mapsto_{\pi_1} & K[V_1] \\
K[\mathsf{snd}\ \langle V_1, V_2\rangle] & \mapsto_{\pi_2} & K[V_2] \\
\mathsf{let}\ x = V\ \mathsf{in}\ M & \mapsto_\zeta & M[x := V] \\
\mathsf{if\ true\ then}\ M_1\ \mathsf{else}\ M_2 & \mapsto_{\iota_1} & M_1 \\
\mathsf{if\ false\ then}\ M_1\ \mathsf{else}\ M_2 & \mapsto_{\iota_2} & M_2
\end{array}
$$

$\boxed{M \mapsto^* M'}$

$$
\frac{}{M \mapsto^* M}\ [\textsc{Red-Refl}]
\qquad\qquad
\frac{M \mapsto M_1 \qquad M_1 \mapsto^* M'}{M \mapsto^* M'}\ [\textsc{Red-Trans}]
$$

$\boxed{\mathsf{eval}(M) = V}$

$$
\mathsf{eval}(M) \quad = \quad V \quad \text{where } M \mapsto^* V \text{ and } V \not\mapsto V'
$$

Fig. 11. ECC^A Evaluation

$\boxed{\Gamma \vdash K : (M : A) \Rightarrow B}$

$$
\frac{}{\Gamma \vdash [\cdot] : (M : A) \Rightarrow A}\ [\textsc{K-Empty}]
\qquad\qquad
\frac{\Gamma \vdash M' : A \qquad \Gamma, y = M' \vdash M : B}{\Gamma \vdash \mathsf{let}\ y = [\cdot]\ \mathsf{in}\ M : (M' : A) \Rightarrow B}\ [\textsc{K-Bind}]
$$

Fig. 12. ECC^A Continuation Typing

have no object-level term to compose *configurations* or *continuations*. We cannot substitute a configuration M into a continuation $\mathsf{let}\ y = [\cdot]\ \mathsf{in}\ M'$, since this would result in the non-ANF (but valid monadic) expression $\mathsf{let}\ y = M\ \mathsf{in}\ M'$. Instead, ANF requires a new operation to compose configurations: $K\langle\langle M\rangle\rangle$. This operation is more generally known as *hereditary substitution* [Watkins et al. 2003], a form of substitution that maintains canonical forms. So we can think of it as a form of substitution, or, simply, as composition.

In Figure 11, we present the call-by-value (CBV) evaluation semantics for ANF ECC^A terms. It is essentially standard, but recall that β-reduction produces a configuration M which must be composed with the existing continuation K. This semantics is for the run-time evaluation of configurations; during type checking, we continue to use the type system and conversion relation defined in Section 1.

2.1 Dependent Continuation Typing

The ANF translation manipulates continuations K as independent entities. To reason about them, and thus to reason about the translation, we introduce continuation typing, defined in Figure 12. The type $(M : A) \Rightarrow B$ of a continuation expresses that this continuation expects to be composed with a term equal to the configuration M of type A and returns a result of type B when completed. Normally, M is equivalent to some computation N, but it must be generalized to a configuration M to support dependent if expressions. This type formally expresses the idea that M is depended upon (in the sense introduced in **??**) in the rest of the computation. For the empty continuation $[\cdot]$, M is arbitrary since an empty continuation has no "rest of the program" that could depend on anything.

Intuitively, what we want from continuation typing is a compositionality property—that we can reason about the types of configurations $K[N]$ (generally, for configurations $K\langle\langle M\rangle\rangle$) by composing the typing derivations for K and N. To get this property, a continuation type must express not merely the *type* of its hole A, but *which term* N will be bound in the hole. We see this formally from the typing rule [Let] (the same for ECC^A as for ECC in Section 1), since showing that $\mathsf{let}\ y = N\ \mathsf{in}\ M$ is well-typed requires showing that $y = N \vdash M$, that is, requires knowing the definition $y = N$. If we omit the expression N from the type of a continuation, we know there are some configurations $K[N]$ that we cannot type check *compositionally*. Intuitively, if all we knew about y was its type, we would be in exactly

$$\boxed{[\![\mathbf{e}]\!]_M = e \text{ where } \Gamma \vdash \mathbf{e} : \mathbf{A}}$$

$$[\![\mathbf{subst}_{\mathbf{e_1}=\mathbf{e_2}}\ \mathbf{e}]\!]_M \stackrel{\text{def}}{=} \text{subst } p\ [\![\mathbf{e}]\!]_M \text{ where } p : [\![\mathbf{e_1}]\!]_M = [\![\mathbf{e_2}]\!]_M \in [\![\Gamma]\!]_M$$

$$[\![\mathbf{if\ e\ then\ e_1\ else\ e_2}]\!]_M \stackrel{\text{def}}{=} \begin{array}{l}(\text{if } [\![\mathbf{e}]\!]_M \text{ then } (\lambda\, p : \text{true} = [\![\mathbf{e}]\!]_M.\ \text{subst (if-eta1 } [\![\mathbf{e_1}]\!]_M\ [\![\mathbf{e_2}]\!]_M\ p)\ [\![\mathbf{e_1}]\!]_M) \\ \qquad\qquad \text{else } (\lambda\, p : \text{false} = [\![\mathbf{e}]\!]_M.\ \text{subst (if-eta2 } [\![\mathbf{e_1}]\!]_M\ [\![\mathbf{e_2}]\!]_M\ p)\ [\![\mathbf{e_2}]\!]_M)) \\ \text{refl } [\![\mathbf{e}]\!]_M\end{array}$$

$$\boxed{\text{Auxiliary CIC definitions}}$$

$$\ldots \qquad \frac{\Gamma \vdash p : e_1 = e_2 \qquad \Gamma \vdash e : B[x := e_1]}{\Gamma \vdash \text{subst } p\ e : B[x := e_2]}\ [\text{DEF-SUBST}]$$

$$\frac{\Gamma, x : \mathit{bool} \vdash B : U \qquad \Gamma \vdash e_1 : B[x := \text{true}] \qquad \Gamma \vdash e_2 : B[x := \text{false}] \qquad \Gamma \vdash p : \text{true} = e}{\Gamma \vdash \text{if-eta1 } e_1\ e_2\ p : \text{subst } p\ e_1 = \text{if } e \text{ then } e_1 \text{ else } e_2}\ [\text{DEF-IF-ETA1}]$$

$$\frac{\Gamma, x : \mathit{bool} \vdash B : U \qquad \Gamma \vdash e_1 : B[x := \text{true}] \qquad \Gamma \vdash e_2 : B[x := \text{false}] \qquad \Gamma \vdash p : \text{false} = e}{\Gamma \vdash \text{if-eta2 } e_1\ e_2\ p : \text{subst } p\ e_2 = \text{if } e \text{ then } e_1 \text{ else } e_2}\ [\text{DEF-IF-ETA2}]$$

Fig. 13. ECC^A Model in CIC (excerpts)

the situation of trying to type check a continuation that has abstracted some dependent type that depends on the *specific* $\mathbf{N}$ into one that depends on an *arbitrary* $\mathbf{y}$. We prove that our continuation typing is compositional in this way, Lemma 2.8 (Cut).

Note that the result of a continuation type cannot depend on the term that will be plugged in for the hole, *i.e.*, for a continuation $\mathbf{K} : (\mathbf{N} : \mathbf{A}) \Rightarrow \mathbf{B}$, $\mathbf{B}$ does not depend on $\mathbf{N}$. To see this, first note that the initial continuation must be empty and thus *cannot* have a result type that depends on its hole. The ANF translation will take this initial empty continuation and compose it with intermediate continuations $\mathbf{K'}$. Since composing any continuation $\mathbf{K} : (\mathbf{N} : \mathbf{A}) \Rightarrow \mathbf{B}$ with any continuation $\mathbf{K'}$ results in a new continuation with the final result type $\mathbf{B}$, then the composition of any two continuations cannot depend on the type of the hole. This is similar to how, in CPS, the answer type doesn't matter and might as well be $\perp$.

2.2 Meta-Theory

2.2.1 Consistency. To demonstrate that the new typing rule for dependent if is consistent, we give a syntactic model of ECC^A in CIC, and formalize the proofs of key properties of the model in Coq. The model essentially implements the new dependent if using the *convoy pattern* [Chlipala 2013], and implements assumed equalities as the identity type. The model in Coq uses propositional equivalence, so constructing a syntactic model relies on equivalence reflection to translate these into the required definitional equivalences. ECC^A itself does not explicitly rely on equivalence reflection, and it is not obvious whether a model exists that does not rely on equivalence reflection.

The essence of the model is given in Figure 13. There are only two interesting rules. The form $\mathbf{subst}_{\mathbf{e_1}=\mathbf{e_2}}\ \mathbf{e}$ is simply translated into a call to the function subst, implemented in CIC, applied to some variable p of the identity type that is in scope in the model. Each if expression $\mathbf{if\ e\ then\ e_1\ else\ e_2}$ is implemented using the convoy pattern, transforming each if expression into a new if expression that returns a function expecting a proof that $[\![\mathbf{e}]\!]_M$ is equal to true in the first branch and false in the second branch. The if expression is then immediately applied to refl. The model relies on auxiliary definitions in CIC, including subst, if-eta1 and if-eta2, whose types are given as inference rules in Figure 13. Note that the model for ECC^A's **if** is not valid ANF, so it does not suffice to merely *use* the convoy pattern if we want to take advantage of ANF for compilation.

We show this is a syntactic model using the usual recipe, which is explained well by Boulier et al. [2017]: we show the translation from ECC^A to CIC preserves equivalence, typing, and the definition of False (the empty type). This means that if ECC^A were inconsistent, then we could translate the proof of **False** into a proof of False in CIC, but no such proof exists in CIC, so ECC^A is consistent.

We use the usual definition of $\mathbf{False}$ as $\Pi\, \mathbf{x} : \mathbf{Prop} \,.\, \mathbf{x}$, and the same in CIC. It is trivial that the definition is preserved.

Lemma 2.1 (Model Preserves Falseness). $[\![\mathbf{False}]\!]_M \equiv \mathit{False}$

The essence of showing both that equivalence is preserved and that typing is preserved is in showing that the auxiliary definitions in Figure 13 exist and are well typed. We define these formally in the Coq model. Note, however, that Lemma 2.2 is stated in terms of definitional equivalence, while the Coq implementation uses propositional equivalence. This means interpreting our Coq implementation as a model requires equivalence reflection.

Lemma 2.2 (Model Preserves Equivalence). *If* $\mathbf{e_1} \equiv \mathbf{e_2}$ *then* $[\![\mathbf{e_1}]\!]_M \equiv [\![\mathbf{e_2}]\!]_M$.

Lemma 2.3 (Model Preserves Typing). *If* $\mathbf{\Gamma} \vdash \mathbf{e} : \mathbf{A}$ *then* $[\![\mathbf{\Gamma}]\!]_M \vdash [\![\mathbf{e}]\!]_M : [\![\mathbf{A}]\!]_M$.

Theorem 2.4 (Consistency). *There is no* $\mathbf{e}$ *such that* $\cdot \vdash \mathbf{e} : \mathbf{False}$

2.2.2 Correctness of ANF Evaluation. In ECC^A, we have an ANF evaluation semantics for run time and a separate definitional equivalence and reduction system for type checking. In this section, we prove that these two coincide: running in our ANF evaluation semantics produces a value definitionally equivalent to the original term.

When computing definitional equivalence, we end up with terms that are not in ANF, and can no longer be used in the ANF evaluation semantics. This is not a problem—we could always ANF translate the resulting term if needed—but can be confusing when reading equations. To make it clear which terms are in ANF and which are not, we leave terms and subterms that are in ANF in the **target language font**, and write terms or subterms that are not in ANF in the source language font. Meta-operations like substitution may be applied to ANF (**red**) terms, but result in non-ANF (blue) terms. Since substitution leaves no visual trace of its blueness, we wrap such terms in a distinctive language boundary such as $\mathcal{ST}(\mathbf{M}[\mathbf{x} := \mathbf{M'}])$ and $\mathcal{ST}(\mathbf{K}[\mathbf{M}])$. The boundary indicates the term is a target (ANF) ($\mathcal{T}$) term on the inside but a source (non-ANF) ($\mathcal{S}$) term on the outside. The boundary is only meant to communicate with the reader that a term is no longer in ANF; formally, $\mathcal{ST}(\mathbf{e}) = \mathbf{e}$.

The heart of the correctness proof is actually *naturality*, a property found in the literature on continuations and CPS that essentially expresses freedom from control effects (*e.g.*, Thielecke [2003] explain this well). This seems to be related to linearity and thunkability in the call-by-push-value literature; a recent draft by Pédrot and Tabareau [2017] explains how these properties relate to CPS translation in dependent type theory.

Lemma 2.5 is the formal statement of naturality in ANF: composing a term $\mathbf{M}$ with its continuation $\mathbf{K}$ in ANF is equivalent to running $\mathbf{M}$ to a value and substituting the result into the continuation $\mathbf{K}$. Formally, this states that composing continuations in ANF is sound with respect to standard substitution.

Lemma 2.5 (Naturality). $\mathbf{K}\langle\!\langle\mathbf{M}\rangle\!\rangle \equiv \mathcal{ST}(\mathbf{K}[\mathbf{M}])$

Proof. By induction on the structure of $\mathbf{M}$

Case: $\mathbf{M} = \mathbf{N}$ trivial

Case: $\mathbf{M} = \mathbf{let\,x = N' \,in\, M'}$

Must show that $\mathbf{let\,x = N'\,in\,K}\langle\!\langle\mathbf{M'}\rangle\!\rangle \equiv \mathcal{ST}(\mathbf{K}[\mathbf{let\,x = N'\,in\,M}])$. This requires breaking ANF while computing equivalence.

$$
\begin{aligned}
& \mathbf{let\,x = N'\,in\,K}\langle\!\langle\mathbf{M'}\rangle\!\rangle & & \\
\rhd_\zeta\ & \mathcal{ST}(\mathbf{K}\langle\!\langle\mathbf{M'}\rangle\!\rangle[\mathbf{x} := \mathbf{N'}]) & \text{note: this substitution is undefined in ANF} \quad & (1)\\
=\ & \mathbf{K}\langle\!\langle\mathcal{ST}(\mathbf{M'}[\mathbf{x} := \mathbf{N'}])\rangle\!\rangle & \text{by uniqueness of names} \quad & (2)\\
\lhd^*\ & \mathcal{ST}(\mathbf{K}[\mathbf{let\,x = N'\,in\,M}]) & \text{by } \zeta\text{-reduction and congruence} \quad & (3)
\end{aligned}
$$

□

Next we show that our ANF evaluation semantics are sound with respect to definitional equivalence. This is also central to our later proof of compiler correctness. To do that, we first show that the small-step semantics are sound. Then we show soundness of the evaluation function.

Lemma 2.6 (Small-step soundness). *If* $\mathbf{M} \mapsto \mathbf{M'}$ *then* $\mathbf{M} \equiv \mathbf{M'}$

Proof. By cases on $\mathbf{M} \mapsto \mathbf{M'}$. Most cases follow easily from the ECC reduction relation and congruence. We give representative cases.

Case: $K[(\lambda\, x : A.\, M_1)\ V] \mapsto_\beta K\langle\langle M_1[x := V]\rangle\rangle$
Must show that $K[(\lambda\, x : A.\, M_1)\ V] \equiv K\langle\langle M_1[x := V]\rangle\rangle$

$$\begin{aligned}
& K[(\lambda\, x : A.\, M_1)\ V] && \\
\rhd^* & \ \mathcal{ST}(K[M_1[x := V]]) && \text{by } \beta \text{ and congruence} \quad (4)\\
\equiv & \ K\langle\langle M_1[x := V]\rangle\rangle && \text{by Lemma 2.5} \quad (5)
\end{aligned}$$

Case: $K[\mathsf{fst}\ \langle V_1, V_2\rangle] \mapsto_{\pi_1} K[V_1]$
Must show that $K[\mathsf{fst}\ \langle V_1, V_2\rangle] \equiv K[V_1]$, which follows by $\rhd_{\pi_1}$ and congruence. □

Theorem 2.7 (Evaluation soundness). $\vdash \mathsf{eval}(M) \equiv M$

Proof. By induction on the length n of the reduction sequence given by $\mathsf{eval}(M)$. Note that, unlike conversion, the ANF evaluation semantics have no congruence rules.

Case: $n = 0$ By [Red-Refl] and [≡].
Case: $n = i + 1$ Follows by Lemma 2.6 and the induction hypothesis. □

2.2.3 Admissibility of Continuation Typing. To prove that continuation typing is not an extension to the type system—*i.e.*, is admissible—we prove Lemma 2.8 and Lemma 2.12, that plugging a well-typed computation or configuration into a well-typed continuation results in a well-typed term of the expected type.

We first show Lemma 2.8 (Cut), which is simple. This lemma corresponds to the [Cut] rule (*e.g.*, found in sequent calculi), and tells us that our continuation typing allows for compositional reasoning about configurations $K[N]$ whose result types do not depend on N. We generalize this lemma to configurations $K\langle\langle M\rangle\rangle$ shortly, but require more meta-theory to do so. The proof for this lemma is simple by definition.

Lemma 2.8 (Cut). *If* $\Gamma \vdash K : (N : A) \Rightarrow B$ *and* $\Gamma \vdash N : A$ *then* $\Gamma \vdash K[N] : B$.

Proof. By cases on $\Gamma \vdash K : (N : A) \Rightarrow B$

Case: $\Gamma \vdash [\cdot] : (N : A) \Rightarrow A$, trivial
Case: $\Gamma \vdash \mathsf{let}\, y = [\cdot]\ \mathsf{in}\, M : (N : A) \Rightarrow B$
We must show that $\Gamma \vdash \mathsf{let}\, y = N\, \mathsf{in}\, M : B$, which follows directly from [Let] since, by the continuation typing derivation, we have that $\Gamma, y = N \vdash M : B$ and $y \notin \mathrm{fv}(B)$. □

Continuation typing seems to require that we compose a continuation $K : (N : A) \Rightarrow B$ *syntactically* with N, but we will need to compose with some $N' \equiv N$. It's preferably to prove this as a lemma instead of building it into continuation typing to get a nicer induction property for continuation typing. The proof is essentially that substitution respects equivalence.

Lemma 2.9 (Cut Modulo Equivalence). *If* $\Gamma \vdash K : (N : A) \Rightarrow B$, $\Gamma \vdash N : A$, $\Gamma \vdash N' : A$, *and* $\Gamma \vdash N \equiv N'$, *then* $\Gamma \vdash K[N'] : B$.

Proof. By cases on the structure of K.

Case: $K = [\cdot]$. Trivial.
Case: $K = \mathsf{let}\, x = [\cdot]\ \mathsf{in}\, M'$
It suffices to show that: If $\Gamma, x = N \vdash M' : B$ then $\Gamma, x = N' \vdash M' : B$.
Note that anywhere in the derivation $\Gamma, x = N \vdash M' : B$ that $x = N$ is used, it must be used essentially as: $A \equiv_\zeta A[x := N]$. We can replace any such use by $A \equiv_\zeta A[x := N'] \equiv A[x := N]$ to construct a derivation for $\Gamma, x = N' \vdash M' : B$

□

Some presentations of evaluation context typing, in non-dependent settings, use a rule link the following.

$$\frac{\Gamma, x : A \vdash E[x] : B}{\Gamma \vdash E : A \Rightarrow B}$$

This suggests we could define continuation typing as follows.

$$\frac{\Gamma \vdash \mathrm{K}[\mathrm{N}] : \mathrm{B}}{\Gamma \vdash \mathrm{K} : (\mathrm{N} : \mathrm{A}) \Rightarrow \mathrm{B}} \text{ [K-Type]}$$

That is, instead of adding separate rules [K-Empty] and [K-Bind], we define a well-typed continuation to be one whose composition with the expect term in the whole is well-typed. Then, Lemma 2.8 (Cut) is definitional rather than admissible. This rule is somewhat surprising; it appears very much like the definition of [Cut], except the computation N being composed with the continuation comes from its type, and the continuation remains un-composed in what we would consider the output of the rule.

The presentations are equivalent, but it is less clear how [K-Type] is related to the definitions we wish to focus on. It is exactly the premises of [K-Bind] that we need to recover type-preservation for ANF, so we choose the presentation with [K-Bind].

However, the rule [K-Type] is more general in the sense that the continuation typing does not need and changes as the definition of continuations change.

The final lemma about continuation typing is also the key to why ANF is type preserving for dependent if. The heterogeneous composition operations necessarily performs the ANF translation on **if** expressions. The following lemma states that if a configuration M is well typed and equivalent to another configuration M' under an extended context Γ', and the continuation K is well-typed with respect to M' then the composition $\mathrm{K}\langle\!\langle \mathrm{M} \rangle\!\rangle$ is well typed. The proof is simple, except for the **if** case, which essentially must prove that ANF is type preserving for **if**. This requires us to prove additional equivalences for **if** statements. We must show that, if an **if** statement is equivalent to some configuration M', then the first branch is also equivalent to M' in a context where $\mathrm{V} \equiv \mathbf{true}$ (and equivalently, the second branch in a context where $\mathrm{V} \equiv \mathbf{false}$).

Lemma 2.10. *If* $\Gamma \vdash \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \equiv \mathrm{M}'$, *then* $\Gamma, \mathrm{V} \equiv \mathbf{true} \vdash \mathrm{M}_1 \equiv \mathrm{M}'$.

Proof. We have that $\Gamma \vdash \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \equiv \mathrm{M}'$. We also have that $\Gamma, \mathrm{V} \equiv \mathbf{true} \vdash \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \equiv \mathbf{if}\ \mathbf{true}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2$ by [Reflect] and substitution. By $\triangleright_{\iota_1}$, we have that $\Gamma \vdash \mathbf{if}\ \mathbf{true}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \equiv \mathrm{M}_1$. Then, by transitivity, we have $\Gamma, \mathrm{V} \equiv \mathbf{true} \vdash \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \equiv \mathrm{M}_1$. By Weakening, we change our initial assumption to $\Gamma, \mathrm{V} \equiv \mathbf{true} \vdash \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \equiv \mathrm{M}'$, and finally by symmetry and transitivity we achieve $\Gamma, \mathrm{V} \equiv \mathbf{true} \vdash \mathrm{M}_1 \equiv \mathrm{M}'$. ◻

Lemma 2.11. *If* $\Gamma \vdash \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \equiv \mathrm{M}'$ *then* $\Gamma, \mathrm{V} \equiv \mathbf{false} \vdash \mathrm{M}_2 \equiv \mathrm{M}'$.

Proof. Analogous to Lemma 2.10. ◻

With these equivalences, we can now prove admissability of heterogeneous composition.

Lemma 2.12 (Hetereogeneous Cut). *If* $\Gamma \vdash \mathrm{M} : \mathrm{A}$ *and* $\Gamma, \Gamma' \vdash \mathrm{K} : (\mathrm{M}' : \mathrm{A}) \Rightarrow \mathrm{B}$ *such that* $\Gamma, \Gamma' \vdash \mathrm{M} \equiv \mathrm{M}'$, *then* $\Gamma, \Gamma' \vdash \mathrm{K}\langle\!\langle \mathrm{M} \rangle\!\rangle : \mathrm{B}$.

Proof. By induction on $\Gamma \vdash \mathrm{M} : \mathrm{A}$.

Case: $\Gamma \vdash \mathrm{N} : \mathrm{A}$, by Lemma 2.9.

Case: $\Gamma \vdash \mathbf{let}\ \mathrm{x} = \mathrm{N}\ \mathbf{in}\ \mathrm{M} : \mathrm{B}'[\mathrm{x} := \mathrm{N}]$

We have that $\Gamma, \Gamma' \vdash \mathrm{K} : (\mathrm{M}' : \mathrm{B}'[\mathrm{x} := \mathrm{N}]) \Rightarrow \mathrm{B}$ such that $\Gamma, \Gamma' \vdash \mathbf{let}\ \mathrm{x} = \mathrm{N}\ \mathbf{in}\ \mathrm{M} \equiv \mathrm{M}'$. We must show $\Gamma, \Gamma' \vdash \mathrm{K}\langle\!\langle \mathbf{let}\ \mathrm{x} = \mathrm{N}\ \mathbf{in}\ \mathrm{M} \rangle\!\rangle : \mathrm{B}$, that is, $\Gamma, \Gamma' \vdash \mathbf{let}\ \mathrm{x} = \mathrm{N}\ \mathbf{in}\ \mathrm{K}\langle\!\langle \mathrm{M} \rangle\!\rangle : \mathrm{B}$. By [Let], we must show (1) $\Gamma, \Gamma' \vdash \mathrm{N} : \mathrm{A}$ and (2) $\Gamma, \Gamma', \mathrm{x} : \mathrm{A}, \mathrm{x} = \mathrm{N} \vdash \mathrm{K}\langle\!\langle \mathrm{M} \rangle\!\rangle : \mathrm{B}$.

(1) follows by inversion and Weakening on our initial assumption.

(2) follows by induction if we can show (2.1) $\Gamma, \Gamma', \mathrm{x} : \mathrm{A}, \mathrm{x} = \mathrm{N} \vdash \mathrm{K} : (\mathrm{M}' : \mathrm{B}') \Rightarrow \mathrm{B}$ and (2.2) $\Gamma, \Gamma', \mathrm{x} : \mathrm{A}, \mathrm{x} = \mathrm{N} \vdash \mathrm{M} \equiv \mathrm{M}'$.

(2.1) follows by [Conv].

(2.2) By $\triangleright_{\zeta}$, we have $\Gamma, \Gamma' \vdash \mathbf{let}\ \mathrm{x} = \mathrm{N}\ \mathbf{in}\ \mathrm{M} \equiv \mathrm{M}[\mathrm{x} := \mathrm{N}]$. By repeated applications of $\triangleright_{\delta}$, we have $\Gamma, \Gamma', \mathrm{x} : \mathrm{A}, \mathrm{x} = \mathrm{N} \vdash \mathbf{let}\ \mathrm{x} = \mathrm{N}\ \mathbf{in}\ \mathrm{M} \equiv \mathrm{M}$. Weakening on our initial assumption, we have $\Gamma, \Gamma', \mathrm{x} : \mathrm{A}, \mathrm{x} = \mathrm{N} \vdash \mathbf{let}\ \mathrm{x} = \mathrm{N}\ \mathbf{in}\ \mathrm{M} \equiv \mathrm{M}'$, and by symmetry and transitivity we finally conclude $\Gamma, \Gamma', \mathrm{x} : \mathrm{A}, \mathrm{x} = \mathrm{N} \vdash \mathrm{M} \equiv \mathrm{M}'$.

Case: $\Gamma \vdash \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 : \mathrm{B}'[\mathrm{x} := \mathrm{V}]$

We have that $\Gamma, \Gamma' \vdash \mathrm{K} : (\mathrm{M}' : \mathrm{B}'[\mathrm{x} := \mathrm{V}]) \Rightarrow \mathrm{B}$ such that $\Gamma, \Gamma' \vdash \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \equiv \mathrm{M}'$. We must show $\Gamma, \Gamma' \vdash \mathrm{K}\langle\!\langle \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \rangle\!\rangle : \mathrm{B}$, that is, $\Gamma, \Gamma' \vdash \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{K}\langle\!\langle \mathrm{M}_1 \rangle\!\rangle\ \mathbf{else}\ \mathrm{K}\langle\!\langle \mathrm{M}_2 \rangle\!\rangle : \mathrm{B}$. By [If], we must show (1) $\Gamma, \Gamma', x : \mathbf{bool} \vdash B' : U$, (2) $\Gamma, \Gamma' \vdash V : \mathbf{bool}$, (3) $\Gamma, \Gamma', V \equiv \mathbf{true} \vdash K\langle\langle M_1 \rangle\rangle : B$ and (4) $\Gamma, \Gamma', V \equiv \mathbf{false} \vdash K\langle\langle M_2 \rangle\rangle : B$.

(1) and (2) follow by inversion and Weakening on our initial assumption. (3) follows by induction if we can show (3.1) $\Gamma, \Gamma', V \equiv \mathbf{true} \vdash K : (M' : B'[x := \mathbf{true}]) \Rightarrow B$, and (3.2) $\Gamma, \Gamma', V \equiv \mathbf{true} \vdash M_1 \equiv M'$.

(3.1) follows by [Conv] if we can show $\Gamma, \Gamma', V \equiv \mathbf{true} \vdash B'[x := V] \equiv B'[x := \mathbf{true}]$. By [Reflect], we have that $\Gamma, \Gamma', V \equiv \mathbf{true} \vdash V \equiv \mathbf{true}$, thus by substitution we have $\Gamma, \Gamma', V \equiv \mathbf{true} \vdash B'[x := V] \equiv B'[x := \mathbf{true}]$.

(3.2) follows by Lemma 2.10.

(4) follows analogously.

□

$\boxed{[\![e]\!]\,K = M}$

$$
\begin{aligned}
[\![e]\!] &\stackrel{\text{def}}{=} [\![e]\!]\,[\cdot] \\
[\![x]\!]\,K &\stackrel{\text{def}}{=} K[x] \\
[\![\mathrm{Prop}]\!]\,K &\stackrel{\text{def}}{=} K[\mathbf{Prop}] \\
[\![\mathrm{Type}_i]\!]\,K &\stackrel{\text{def}}{=} K[\mathbf{Type}_i] \\
[\![\Pi\, x : A.\, B]\!]\,K &\stackrel{\text{def}}{=} K[\Pi\, x : [\![A]\!].\, [\![B]\!]] \\
[\![\lambda\, x : A.\, e]\!]\,K &\stackrel{\text{def}}{=} K[\lambda\, x : [\![A]\!].\, [\![e]\!]] \\
[\![e_1\ e_2]\!]\,K &\stackrel{\text{def}}{=} [\![e_1]\!]\ \mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ [\![e_2]\!]\ \mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ K[x_1\ x_2] \\
[\![\Sigma\, x : A.\, B]\!]\,K &\stackrel{\text{def}}{=} K[\Sigma\, x : [\![A]\!].\, [\![B]\!]] \\
[\![\langle e_1, e_2\rangle\ \mathrm{as}\ A]\!]\,K &\stackrel{\text{def}}{=} [\![e_1]\!]\ \mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ [\![e_2]\!]\ (\mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ K[(\langle x_1, x_2\rangle\ \mathbf{as}\ [\![A]\!])]) \\
[\![\mathrm{fst}\ e]\!]\,K &\stackrel{\text{def}}{=} [\![e]\!]\ \mathbf{let}\ x = [\cdot]\ \mathbf{in}\ K[\mathbf{fst}\ x] \\
[\![\mathrm{snd}\ e]\!]\,K &\stackrel{\text{def}}{=} [\![e]\!]\ \mathbf{let}\ x = [\cdot]\ \mathbf{in}\ K[\mathbf{snd}\ x] \\
[\![\mathrm{let}\ x = e\ \mathrm{in}\ e']\!]\,K &\stackrel{\text{def}}{=} [\![e]\!]\ \mathbf{let}\ x = [\cdot]\ \mathbf{in}\ [\![e']\!]\,K \\
[\![\mathrm{bool}]\!]\,K &\stackrel{\text{def}}{=} K[\mathbf{bool}] \\
[\![\mathrm{true}]\!]\,K &\stackrel{\text{def}}{=} K[\mathbf{true}] \\
[\![\mathrm{false}]\!]\,K &\stackrel{\text{def}}{=} K[\mathbf{false}] \\
[\![\mathrm{if}\ e\ \mathrm{then}\ e_1\ \mathrm{else}\ e_2]\!]\,K &\stackrel{\text{def}}{=} [\![e]\!]\ \mathbf{let}\ x = [\cdot]\ \mathbf{in}\ \mathbf{if}\ x\ \mathbf{then}\ [\![e_1]\!]\,K\ \mathbf{else}\ [\![e_2]\!]\,K
\end{aligned}
$$

Fig. 14. Naïve ANF Translation

3 ANF TRANSLATION

The ANF translation is presented in Figure 14. The naïve translation is defined inductively over syntax. The translation is indexed by a current continuation, which is used when translating a value and is is composed together "inside-out" the same continuation composition is defined in Section 2. The translation is essentially standard. When translating a value such as x, $\lambda\, x : A.\, e$, and Type_i, we essentially plug the value into the current continuation, recursively translating the sub-expressions of the value if applicable. For non-values such as application, we make sequencing explicit by recursively translating each sub-expression with a continuation that binds the result which will perform the computation.

Note that if the translation must produce type annotations then defining the translation and typing preservation proof are somewhat more complicated. For instance, if we generate join points directly, or require the **let**-bindings in the target language to have type annotations for bound expressions, then we would need to modify the translation to produce those annotations. This requires defining the translation over typing derivations, so the compiler has access to the type of the expression and not only its syntax.

Our goal is to prove type preservation: if e is well-typed in the source, then $[\![e]\!]$ is well-typed at a translated type in the target. But to prove type preservation, we must also preserve the rest of the judgmental and syntactic structure that dependent type systems rely on. To prove type-preservation, we follow a standard architecture for dependent type theory [Barthe et al. 1999; Barthe and Uustalu 2002; Boulier et al. 2017; Bowman and Ahmed 2018; Bowman et al. 2018]. Since type checking requires definitional equivalence, in the [Conv] rule, and substitution, in rules such as [App], we must preserve definitional equivalence and substitution. Since definitional equivalence is defined in terms of reduction, we must preserve reduction up to equivalence.

We stage the type-preservation proof as follows. First, we show *compositionality*, which states that the translation commutes with composition, *e.g.*, that substituting first and then translating is equivalent to translating first and then substituting. This proof is somewhat non-standard for ANF since the notion of composition in ANF is not the usual substitution. Next, we show that reduction and conversion are preserved up to equivalence. Note that for this theorem, we are interested in the conversion semantics used for definitional equivalence, not in the machine semantics used to evaluate ANF terms. Then, we show *equivalence preservation*: if two terms are definitionally equivalent in the source, then their translations are definitionally equivalent. Finally, we can show type preservation of the ANF translation, using continuation typing to express the inductive invariant required for ANF. The continuation typing allows us to formally state type preservation in terms of the intuitive reason that type preservation should hold: because the definitions expressed by the continuation typing suffice to prove equivalence between a computation variable and the original depended-upon expression.

After proving type preservation, we prove correctness of separate compilation for the ANF machine semantics. This requires a notion of linking, which we define later in this section. This proof is straightforward from the meta-theory about the machine semantics proved in Section 2, and from equivalence preservation.

Recall from Section 2, we shift from the **target language font** to the source language font whenever we shift out of ANF, such as when we perform standard substitution or conversion. When the shift in font is not apparent, we use the language boundary term $\mathcal{ST}()$.

Before we proceed, we state a property about the syntactic form produced by the translation, in particular, that the ANF translation does produce syntax in ANF (Theorem 3.1). The proof is straightforward so we elide it.

Theorem 3.1 (ANF). *For all* e *and* K, $[\![e]\!]\ K = M$ *for some* M.

As discussed in Section 2, composition in ANF is somewhat non-standard. Normally, we compose via substitution, so the compositionality property we want is $[\![e[x := e']]\!] \equiv [\![e]\!][x := [\![e']\!]]$, which says we can either compose then translate or translate then compose. However, most composition in ANF goes through continuations, not through substitution, since only values can be substituted in ANF. Our primary compositionality lemma (Lemma 3.2) tells us that we can either first translate a program e under continuation K and then compose it with a continuation K', or we can first compose the continuations K and K' and then translate e under the composed continuation. Note that this proof is entirely within ECC^{A}; there are no language boundaries.

Lemma 3.2 (Compositionality). $K'\langle\!\langle\ [\![e]\!]\ K\rangle\!\rangle = [\![e]\!]\ K'\langle\!\langle K\rangle\!\rangle$

Proof. By induction on the structure of e. All value cases are trivial. The cases for non-values are all essentially similar, by definition of composition for continuations or configurations. We give some representative cases.

Case: $e = x$ Must show $K'\langle\!\langle K[x]\rangle\!\rangle = K'\langle\!\langle K[x]\rangle\!\rangle$, which is trivial.

Case: $e = \Pi\, x : A.\ B$ Must show that $K'\langle\!\langle K[\Pi\, x : [\![A]\!].\ [\![B]\!]]\rangle\!\rangle = K'\langle\!\langle K[\Pi\, x : [\![A]\!].\ [\![B]\!]]\rangle\!\rangle$, which is trivial. Note that we need not appeal to induction, since the recursive translation does not use the current continuation for values.

Case: $e = e_1\ e_2$ Must show that

$$K'\langle\!\langle([\![e_1]\!]\ (\mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ ([\![e_2]\!]\ \mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ K[x_1\ x_2])))\rangle\!\rangle$$
$$= ([\![e_1]\!]\ (\mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ ([\![e_2]\!]\ \mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ K'\langle\!\langle K\rangle\!\rangle[x_1\ x_2])))$$

The proof follows essentially from the definition of continuation composition.

$$\begin{aligned}
& K'\langle\!\langle([\![e_1]\!]\ (\mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ ([\![e_2]\!]\ \mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ K[x_1\ x_2])))\rangle\!\rangle \\
= \quad & ([\![e_1]\!]\ K'\langle\!\langle(\mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ ([\![e_2]\!]\ \mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ K[x_1\ x_2]))\rangle\!\rangle) && (6) \\
& \qquad \text{by the induction hypothesis applied to } e_1 \\
= \quad & ([\![e_1]\!]\ (\mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ K'\langle\!\langle([\![e_2]\!]\ \mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ K[x_1\ x_2])\rangle\!\rangle)) && (7) \\
& \qquad \text{by definition of continuation composition} \\
= \quad & ([\![e_1]\!]\ (\mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ ([\![e_2]\!]\ K'\langle\!\langle\mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ K[x_1\ x_2]\rangle\!\rangle))) && (8) \\
& \qquad \text{by the induction hypothesis applied to } e_2 \\
= \quad & ([\![e_1]\!]\ (\mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ ([\![e_2]\!]\ \mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ K'\langle\!\langle K\rangle\!\rangle[x_1\ x_2]))) && (9) \\
& \qquad \text{by definition of continuation composition}
\end{aligned}$$

□

Corollary 3.3. $K\langle\!\langle\ [\![e]\!]\ \rangle\!\rangle = [\![e]\!]\ K$

Next we show compositionality of the translation with respect to substitution (Lemma 3.4). While the proof relies on the previous lemma, this lemma is different in that substitution is the primary means of composition within the type system. We must essentially show that substitution is equivalent to composing via continuations. Since standard substitution does not preserve ANF, this lemma does not equate ECC^A terms, but ECC terms that have been transformed via ANF translation. We will again use language boundaries to indicate a shift from ANF to non-ANF terms. Note that this lemma relies on uniqueness of names.

Lemma 3.4 (Substitution). $\llbracket e[x := e'] \rrbracket\, K \equiv \mathcal{ST}((\llbracket e \rrbracket\, K)[x := \llbracket e' \rrbracket])$

Proof. By induction on the structure of e We give the key cases.

Case: $e = x$ Must show that $\llbracket e' \rrbracket\, K \equiv \mathcal{ST}((\llbracket x \rrbracket\, K)[x := \llbracket e' \rrbracket])$

$$\mathcal{ST}(\llbracket x \rrbracket\, K[x := \llbracket e' \rrbracket])$$
$$= \mathcal{ST}(K[x][x := \llbracket e' \rrbracket]) \tag{10}$$
$$= \mathcal{ST}(K[\llbracket e' \rrbracket]) \tag{11}$$
$$\equiv K\langle\!\langle \llbracket e' \rrbracket \rangle\!\rangle \quad \text{by Lemma 2.5} \tag{12}$$
$$\equiv \llbracket e' \rrbracket\, K \quad \text{by Lemma 3.2} \tag{13}$$
$$\tag{14}$$

Case: $e = \text{Prop}$ Trivial.

Case: $e = \Pi\, x' : A.\, B$

Must show that $\llbracket \Pi\, x' : A.\, B[x := e'] \rrbracket\, K \equiv \mathcal{ST}((\llbracket \Pi\, x' : A.\, B \rrbracket\, K)[x := \llbracket e' \rrbracket])$

$$\llbracket \Pi\, x' : A.\, B[x := e'] \rrbracket\, K$$
$$= \llbracket \Pi\, x' : A[x := e'].\, B[x := e'] \rrbracket\, K \tag{15}$$
$$= K[\Pi\, x' : \llbracket A[x := e'] \rrbracket.\, \llbracket B[x := e'] \rrbracket] \tag{16}$$
$$\equiv K[\Pi\, x' : \mathcal{ST}(\llbracket A \rrbracket[x := \llbracket e' \rrbracket]).\, \mathcal{ST}(\llbracket B \rrbracket[x := \llbracket e' \rrbracket])] \quad \text{by the induction hypothesis} \tag{17}$$
$$= \mathcal{ST}(K[\Pi\, x' : \llbracket A \rrbracket.\, \llbracket B \rrbracket][x := \llbracket e' \rrbracket]) \quad \text{by definition of substitution} \tag{18}$$
$$= \mathcal{ST}((\llbracket \Pi\, x' : A.\, B \rrbracket\, K)[x := \llbracket e' \rrbracket]) \quad \text{by definition} \tag{19}$$

Case: $e = e_1\ e_2$

Must show that $\llbracket (e_1\ e_2)[x := e'] \rrbracket\, K \equiv \mathcal{ST}((\llbracket e_1\ e_2 \rrbracket\, K)[x := \llbracket e' \rrbracket])$

$$\llbracket (e_1\ e_2)[x := e'] \rrbracket\, K$$
$$= \llbracket e_1[x := e']\ e_2[x := e'] \rrbracket\, K \quad \text{by substitution} \tag{20}$$
$$= \llbracket e_1[x := e'] \rrbracket\ \mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ \llbracket e_2[x := e'] \rrbracket\ \mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ K[x_1\ x_2] \quad \text{by translation} \tag{21}$$
$$\equiv \llbracket e_1[x := e'] \rrbracket\ \mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ \mathcal{ST}((\llbracket e_2 \rrbracket\ \mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ K[x_1\ x_2])[x := \llbracket e' \rrbracket]) \quad \text{by IH applied to } e_1 \tag{22}$$
$$\equiv \llbracket e_1 \rrbracket\ \mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ \llbracket e_2 \rrbracket\ \mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ K[x_1\ x_2][x := \llbracket e' \rrbracket][x := \llbracket e' \rrbracket] \quad \text{by IH applied to } e_2 \tag{23}$$
$$= \mathcal{ST}((\llbracket e_1 \rrbracket\ \mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ \llbracket e_2 \rrbracket\ \mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ K[x_1\ x_2])[x := \llbracket e' \rrbracket]) \quad \text{by substitution} \tag{24}$$
$$= \mathcal{ST}((\llbracket e_1\ e_2 \rrbracket\, K)[x := \llbracket e' \rrbracket]) \quad \text{by substitution} \tag{25}$$

□

Next we show equivalence is preserved, in two parts. First we show that reduction is preserved up to equivalence, and then show conversion is preserved up to equivalence. The proofs are straightforward; intuitively, ANF is just adding a bunch of ζ-reductions.

Lemma 3.5. *If* $\Gamma \vdash e \rhd e'$ *then* $\llbracket \Gamma \rrbracket \vdash \llbracket e \rrbracket \equiv \llbracket e' \rrbracket$.

Proof. By cases on $\Gamma \vdash e \rhd e'$. We give the key cases.

Case: $\Gamma \vdash x \rhd_\delta e'$

We must show that $\llbracket \Gamma \rrbracket \vdash \llbracket x \rrbracket \equiv \llbracket e' \rrbracket$

We know that $x = e' \in \Gamma$, and by definition $x = \llbracket e' \rrbracket \in \llbracket \Gamma \rrbracket$, so the goal follows by definition.

Case: $\Gamma \vdash \lambda\, x : A.\, e_1\ e_2 \rhd_\beta e_1[x := e_2]$

We must show $\llbracket \Gamma \rrbracket \vdash \llbracket (\lambda\, x : A.\, e_1)\ e_2 \rrbracket \equiv \llbracket e_1[x := e_2] \rrbracket$

$$\llbracket \lambda\, x : A.\, e_1\ e_2 \rrbracket$$

$$= [\![\lambda\, x : A.\, e_1]\!]\ \mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ [\![e_2]\!]\ \mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ x_1\ x_2 \tag{26}$$

$$= \mathbf{let}\ x_1 = (\boldsymbol{\lambda}\, x : [\![A]\!].\, [\![e_1]\!])\ \mathbf{in}\ [\![e_2]\!]\ \mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ x_1\ x_2 \tag{27}$$

$$\rhd^*\ [\![e_2]\!]\ \mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ \boldsymbol{\lambda}\, x : [\![A]\!].\, [\![e_1]\!]\ \ x_2 \tag{28}$$

$$= \mathbf{let}\ x_2 = [\cdot]\ \mathbf{in}\ (\boldsymbol{\lambda}\, x : [\![A]\!].\, [\![e_1]\!])\ x_2 \langle\!\langle\, [\![e_2]\!]\,\rangle\!\rangle \quad \text{by Lemma 3.2} \tag{29}$$

$$\equiv \mathrm{let}\ x_2 = [\![e_2]\!]\ \ \mathrm{in}\ (\boldsymbol{\lambda}\, x : [\![A]\!].\, [\![e_1]\!])\ x_2 \quad \text{by Lemma 2.5} \tag{30}$$

$$\rhd_\zeta\ (\boldsymbol{\lambda}\, x : [\![A]\!].\, [\![e_1]\!])\ \ [\![e_2]\!] \tag{31}$$

$$\rhd_\beta\ \mathcal{ST}([\![e_1]\!][x := [\![e_2]\!]]) \tag{32}$$

$$\equiv [\![e_1[x := e_2]]\!] \quad \text{by Lemma 3.4} \tag{33}$$

□

Next we show that conversion is preserved up to equivalence. Note that past work has a minor bug in the *proof* of the following lemma [Bowman and Ahmed 2018; Bowman et al. 2018], although it does not invalidate their *theorems*. The past proofs only account for transitivity of $\rhd^*$, but fail to account for the congruence rules. This is not a significant issue, since their translations are compositional and the congruence rules follow essentially from compositionality. We give the key cases of this proof to demonstrate the correct structure.

Lemma 3.6. *If* $\Gamma \vdash e \rhd^* e'$ *then* $[\![\Gamma]\!] \vdash [\![e]\!] \equiv [\![e']\!]$

Proof. By induction on the structure of $\Gamma \vdash e \rhd^* e'$.

Case: [Red-Refl], trivial.

Case: [Red-Trans], by Lemma 3.5 and the induction hypothesis.

Case: [Red-Cong-Let]

We have $\Gamma \vdash \mathrm{let}\ x = e_1\ \mathrm{in}\ e \rhd^* \mathrm{let}\ x = e_1\ \mathrm{in}\ e'$ and $\Gamma \vdash e \rhd^* e'$.

We must show that $[\![\Gamma]\!] \vdash [\![\mathrm{let}\ x = e_1\ \mathrm{in}\ e]\!] \equiv [\![\mathrm{let}\ x = e_1\ \mathrm{in}\ e']\!]$.

$$[\![\mathrm{let}\ x = e_1\ \mathrm{in}\ e]\!]$$

$$= [\![\mathrm{let}\ x = e_1\ \mathrm{in}\ y[y := e]]\!] \tag{34}$$

$$\equiv \mathcal{ST}([\![\mathrm{let}\ x = e_1\ \mathrm{in}\ y]\!][y := [\![e]\!]]) \quad \text{by Lemma 3.4 (Substitution)} \tag{35}$$

$$\equiv \mathcal{ST}([\![\mathrm{let}\ x = e_1\ \mathrm{in}\ y]\!][y := [\![e']\!]]) \quad \text{by the induction hypothesis} \tag{36}$$

$$\equiv [\![\mathrm{let}\ x = e_1\ \mathrm{in}\ y[y := e']]\!] \quad \text{by Lemma 3.4} \tag{37}$$

$$= [\![\mathrm{let}\ x = e_1\ \mathrm{in}\ e']\!] \tag{38}$$

□

The previous two lemmas imply equivalence preservation. Including η-equivalence makes this non-trivial, but not hard.

Lemma 3.7. *If* $\Gamma \vdash e \equiv e'$ *then* $[\![\Gamma]\!] \vdash [\![e]\!] \equiv [\![e']\!]$

Proof. By induction on the derivation of $\Gamma \vdash e \equiv e'$.

Case: [≡] Follows by Lemma 3.6.

Case: [≡-η_1]

By Lemma 3.6, we know $[\![e]\!] \equiv [\![\lambda\, x : A.\, e_1]\!]$. By transitivity, it suffices to show $[\![\lambda\, x : A.\, e_1]\!] \equiv [\![e']\!]$.

By [≡-η_1], since $[\![\lambda\, x : A.\, e_1]\!] = \boldsymbol{\lambda}\, x : [\![A]\!].\, [\![e_1]\!]$, it suffices to show that $[\![e_1]\!] \equiv [\![e']\!]\ \ x_2$

$$[\![e_1]\!]$$

$$\equiv [\![e'\ x_2]\!] \quad \text{by the induction hypothesis} \tag{39}$$

$$= [\![e']\!]\ \mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ x_1\ x_2 \tag{40}$$

$$= (\mathbf{let}\ x_1 = [\cdot]\ \mathbf{in}\ x_1\ x_2)\langle\!\langle\, [\![e']\!]\,\rangle\!\rangle \quad \text{by Lemma 3.2} \tag{41}$$

$$\equiv \mathrm{let}\ x_1 = [\![e']\!]\ \ \mathrm{in}\ x_1\ x_2 \quad \text{by Lemma 2.5} \tag{42}$$

$$\triangleright_\zeta \; [\![e']\!]\; x_2 \tag{43}$$

Case: [$\equiv$-η_2] Essentially similar to the previous case. □

Since we implement cumulative universes through subtyping, we must also show subtyping is preserved (Lemma 3.8). The proof is completely uninteresting, except insofar as it is simple, while it seems to be impossible for CPS translation [Bowman et al. 2018]. We discuss this further in **??**.

Lemma 3.8. *If* $\Gamma \vdash e \preceq e'$ *then* $[\![\Gamma]\!] \vdash [\![e]\!] \preceq [\![e']\!]$

Proof. By induction on the structure of $\Gamma \vdash e \preceq e'$.

Case: [$\preceq$-$\equiv$]. Follows by Lemma 3.7.
Case: [$\preceq$-Trans]. Follows the induction hypothesis.
Case: [$\preceq$-Prop]. Trivial, since $[\![\mathsf{Prop}]\!] = \mathbf{Prop}$ and $[\![\mathsf{Type}_0]\!] = \mathbf{Type}_0$.
Case: [$\preceq$-Cum]. Trivial, since $[\![\mathsf{Type}_i]\!] = \mathbf{Type}_i$ and $[\![\mathsf{Type}_{i+1}]\!] = \mathbf{Type}_{i+1}$.
Case: [$\preceq$-Pi].

We must show that $[\![\Gamma]\!] \vdash [\![\Pi\, x_1 : A_1.\, B_1]\!] \preceq [\![\Pi\, x_2 : A_2.\, B_2]\!]$

By definition of the translation, we must show $[\![\Gamma]\!] \vdash \mathbf{\Pi}\, \mathbf{x_1} : [\![A_1]\!].\, [\![B_1]\!] \preceq \mathbf{\Pi}\, \mathbf{x_2} : [\![A_2]\!].\, [\![B_2]\!]$.

Note that if we lifted the continuations in type annotations A_1 and A_2 outside the Π, as CBPV suggests we should, we would need a new subtyping rule that allows subtyping **let** expressions. As it is, we proceed by [$\preceq$-Pi].

It suffices to show that

(a) $[\![\Gamma]\!] \vdash [\![A_1]\!] \equiv [\![A_2]\!]$, which follows by the induction hypothesis.
(b) $[\![\Gamma]\!], \mathbf{x_1} : [\![A_2]\!] \vdash [\![B_1]\!] \preceq [\![B_2]\!][\mathbf{x_2} := \mathbf{x_1}]$, which follows by the induction hypothesis.

Case: [$\preceq$-Sig]. Similar to previous case.

□

The structure of the theorem for type preservation and its proof are a little surprising. Intuitively, we would expect to show something like "if $e : A$ then $[\![e]\!] : [\![A]\!]$". We will ultimately prove this, but we need a stronger lemma first.

As an example of the of the ANF translation, consider the $\mathsf{snd}\; e$ case: $[\![\mathsf{snd}\; e]\!]\; \mathbf{K} \overset{\text{def}}{=} [\![e]\!]\; \mathbf{let}\; \mathbf{x} = [\cdot]\; \mathbf{in}\; \mathbf{K}[\mathbf{snd}\; \mathbf{x}]$. Notice that the ANF translation is pushing the computation inside-out by translating the sub-expression e of the term $\mathsf{snd}\; e$ and constructing a new continuation that expects the translated sub-expression $[\![e]\!]$. Furthermore, the translation ensures that the original continuation $\mathbf{K}$ is applied to a target computation $\mathbf{snd}\; \mathbf{x}$, which, after some machine steps, is equivalent to the translation of the source expression $[\![\mathsf{snd}\; e]\!]$.

These observations lead us to state the following lemma, which includes reasoning about the type of the continuation $\mathbf{K}$: If $\Gamma \vdash e : A$, and $[\![\Gamma]\!], \mathbf{\Gamma'} \vdash \mathbf{K} : (\mathbf{N} : [\![A]\!]) \Rightarrow \mathbf{B}$ such that $[\![\Gamma]\!], \mathbf{\Gamma'} \vdash [\![e]\!] \equiv \mathbf{N}$, then $[\![\Gamma]\!], \mathbf{\Gamma'} \vdash [\![e]\!]\; \mathbf{K} : \mathbf{B}$. We require the continuation $\mathbf{K}$ and its type are not arbitrary, but have a particular relationship to the translation of the source term e. It expects a term that is *not* the translation of the source expression directly, but rather some target computation $\mathbf{N}$ that is equivalent to the translated source expression e under an extended context $\mathbf{\Gamma'}$.

Intuitively, this extended context $\mathbf{\Gamma'}$ contains information about new variables introduced through the ANF translation. In the case of dependent if, this extended context contains equivalences about the expression being eliminated. We then use [Reflect] to prove that the continuation is applied to an expression equivalent to the translation of the dependent if.

We first prove this stronger lemma (Lemma 3.9), towards our goal of proving type preservation (Theorem 3.11). Wielding our propositions-as-types hat, we can view this lemma as in accumulator-passing style. The ANF translation takes a procedural accumulator (the continuation $\mathbf{K}$) and builds up the translation in an accumulator as a procedure from values to ANF terms. Our type preservation proof builds up a proof of correctness as an accumulator as well. The accumulator is a *proposition* that if the computation it receives is well-typed, then composing the continuation with the computation is well-typed.

Lemma 3.9.

(1) If $\vdash \Gamma$ *then* $\vdash [\![\Gamma]\!]$
(2) If $\Gamma \vdash e : A$*, and* $[\![\Gamma]\!], \mathbf{\Gamma'} \vdash \mathbf{K} : (\mathbf{N} : [\![A]\!]) \Rightarrow \mathbf{B}$ *such that* $[\![\Gamma]\!], \mathbf{\Gamma'} \vdash [\![e]\!] \equiv \mathbf{N}$*, then* $[\![\Gamma]\!], \mathbf{\Gamma'} \vdash [\![e]\!]\; \mathbf{K} : \mathbf{B}$.

Proof. The proof is by induction on the mutually defined judgments $\vdash \Gamma$ and $\Gamma \vdash e : A$. Cases [Ax-Prop], [Lam], [App], [Snd], and [If] are given.

Case: [Ax-Prop]

We have that $\vdash \Gamma$, $\Gamma \vdash \mathsf{Prop} : \mathsf{Type}_0$, and $[\![\Gamma]\!], \Gamma' \vdash K : (N : [\![\mathsf{Type}_0]\!]) \Rightarrow B$ such that $[\![\Gamma]\!], \Gamma' \vdash [\![\mathsf{Prop}]\!] \equiv N$. We must show that $[\![\Gamma]\!], \Gamma' \vdash [\![\mathsf{Prop}]\!]\, K : B$, that is, $[\![\Gamma]\!], \Gamma' \vdash K[\mathbf{Prop}] : B$. This follows from Lemma 2.8 if we can show $[\![\mathsf{Prop}]\!]$ is equivalent to $\mathbf{Prop}$ and that $[\![\Gamma]\!], \Gamma' \vdash \mathbf{Prop} : [\![\mathsf{Type}_0]\!]$. $[\![\mathsf{Prop}]\!]$ is equivalent to $\mathbf{Prop}$ by the ANF translation. Finally, since $[\![\mathsf{Type}_0]\!]$ is equivalent to $\mathbf{Type}_0$ by the ANF translation, we are trying to show $[\![\Gamma]\!], \Gamma' \vdash \mathbf{Prop} : \mathbf{Type}_0$, which follows by [Ax-Prop].

Case: [Lam]

We have that $\vdash \Gamma$, $\Gamma \vdash [\![\lambda x : A'.\, e']\!] : \Pi x : A'.\, B'$, and $[\![\Gamma]\!], \Gamma' \vdash K : (N : [\![\Pi x : A'.\, B']\!]) \Rightarrow B$ such that $[\![\Gamma]\!], \Gamma' \vdash [\![\lambda x : A'.\, e']\!] \equiv N$. We must show that $[\![\Gamma]\!] \vdash [\![\lambda x : A'.\, e']\!]\, K : B$, that is, $[\![\Gamma]\!] \vdash K[\boldsymbol{\lambda}\, x : [\![A']\!].\, [\![e']\!]] : B$. This follows from Lemma 2.8 if we can show $[\![\lambda x : A'.\, e']\!]$ is equivalent to $\boldsymbol{\lambda}\, x : [\![A']\!].\, [\![e']\!]$ and that $[\![\Gamma]\!], \Gamma \vdash \boldsymbol{\lambda}\, x : [\![A']\!].\, [\![e']\!] : [\![\Pi x : A'.\, B']\!]$. $[\![\lambda x : A'.\, e']\!]$ is equivalent to $\boldsymbol{\lambda}\, x : [\![A']\!].\, [\![e']\!]$ by the ANF translation.

Since $[\![\Pi x : A'.\, B']\!]$ is equivalent to $\boldsymbol{\Pi}\, x : [\![A']\!].\, [\![B']\!]$ by the ANF translation, we are trying to show $[\![\Gamma]\!], \Gamma' \vdash \boldsymbol{\lambda}\, x : [\![A']\!].\, [\![e']\!] : \boldsymbol{\Pi}\, x : [\![A']\!].\, [\![B']\!]$. This follows from [Lam] if we can show $[\![\Gamma]\!], \Gamma', x : [\![A']\!] \vdash [\![e']\!] : [\![B']\!]$. By induction on the judgment $\Gamma, x : A' \vdash e' : B'$ with the empty continuation $[\![\Gamma]\!], \Gamma'_1 \vdash [\cdot] : ([\![e']\!] : [\![B']\!]) \Rightarrow [\![B']\!]$, where $\Gamma'_1 = \Gamma', [\![x : A']\!] = \Gamma', x : [\![A']\!]$, we obtain $[\![\Gamma]\!], \Gamma', x : [\![A']\!] \vdash [\![e']\!] : [\![B']\!]$ as desired.

Case: [App]

We have that $\vdash \Gamma$, $\Gamma \vdash e_1\, e_2 : B'[x := e_2]$, and $[\![\Gamma]\!], \Gamma' \vdash K : (N : [\![B'[x := e_2]]\!]) \Rightarrow B$ such that $[\![\Gamma]\!], \Gamma' \vdash [\![e_1\, e_2]\!] \equiv N$. We must show that $[\![\Gamma]\!], \Gamma' \vdash [\![e_1\, e_2]\!]\, K : B$, that is, $[\![\Gamma]\!], \Gamma' \vdash [\![e_1]\!]\, (\mathbf{let}\, x_1 = [\cdot]\, \mathbf{in}\, [\![e_2]\!]\, (\mathbf{let}\, x_2 = [\cdot]\, \mathbf{in}\, K[x_1\, x_2])) : B$. Let $K_1 = (\mathbf{let}\, x_1 = [\cdot]\, \mathbf{in}\, [\![e_2]\!]\, (\mathbf{let}\, x_2 = [\cdot]\, \mathbf{in}\, K[x_1\, x_2]))$. Our conclusion follows by induction on $\Gamma \vdash e_1 : \Pi x : A'.\, B'$, if we show $[\![\Gamma]\!], \Gamma' \vdash K_1 : ([\![e_1]\!] : [\![\Pi x : A'.\, B']\!]) \Rightarrow B$. By [K-Bind], we must show (1) $[\![\Gamma]\!], \Gamma' \vdash [\![e_1]\!] : [\![\Pi x : A'.\, B']\!]$ and (2) $[\![\Gamma]\!], \Gamma', x_1 = [\![e_1]\!] \vdash [\![e_2]\!]\, (\mathbf{let}\, x_2 = [\cdot]\, \mathbf{in}\, K[x_1\, x_2]) : B$.

(1) follows from induction on $\Gamma \vdash e_1 : \Pi x : A'.\, B'$ with the empty continuation $[\![\Gamma]\!], \Gamma' \vdash [\cdot] : ([\![e_1]\!] : [\![\Pi x : A'.\, B']\!]) \Rightarrow [\![\Pi x : A'.\, B']\!]$.

(2) follows by induction on $\Gamma \vdash e_2 : A'$, if we can show $[\![\Gamma]\!], \Gamma', x_1 = [\![e_1]\!] \vdash \mathbf{let}\, x_2 = [\cdot]\, \mathbf{in}\, K[x_1\, x_2] : ([\![e_2]\!] : [\![A']\!]) \Rightarrow B$. By [K-Bind], we must show (2.1) $[\![\Gamma]\!], \Gamma', x_1 = [\![e_1]\!] \vdash [\![e_2]\!] : [\![A']\!]$ and (2.2) $[\![\Gamma]\!], \Gamma', x_1 = [\![e_1]\!], x_2 = [\![e_2]\!] \vdash K[x_1\, x_2] : B$.

(2.1) follows from induction on $\Gamma \vdash e_2 : A'$ with the empty continuation $[\![\Gamma]\!], \Gamma', x_1 = [\![e_1]\!] \vdash [\cdot] : ([\![e_2]\!] : [\![A']\!]) \Rightarrow [\![A']\!]$.

(2.2) follows from Lemma 2.9 if we can show (2.2.1) $[\![\Gamma]\!], \Gamma', x_1 = [\![e_1]\!], x_2 = [\![e_2]\!] \vdash x_1\, x_2 : [\![B'[x := e_2]]\!]$ and (2.2.2) $[\![\Gamma]\!], \Gamma', x_1 = [\![e_1]\!], x_2 = [\![e_2]\!] \vdash [\![e_1\, e_2]\!] \equiv x_1\, x_2$.

(2.2.1) By $\triangleright_\delta$, we are trying to show $[\![\Gamma]\!], \Gamma', x_1 = [\![e_1]\!], x_2 = [\![e_2]\!] \vdash [\![e_1]\!]\ [\![e_2]\!] : [\![B'[x := e_2]]\!]$. We have previously shown in (1) and (2.1) that $[\![\Gamma]\!], \Gamma' \vdash [\![e_1]\!] : \boldsymbol{\Pi}\, x : [\![A']\!].\, [\![B']\!]$ and $[\![\Gamma]\!], \Gamma', x_1 = [\![e_1]\!] \vdash [\![e_2]\!] : [\![A']\!]$. Using these facts with [App] and Weakening, we derive $[\![\Gamma]\!], \Gamma', x_1 = [\![e_1]\!], x_2 = [\![e_2]\!] \vdash x_1\, x_2 : [\![B']\!][x := [\![e_2]\!]]$. We have that $[\![B']\!][x := [\![e_2]\!]]$ is equivalent to $[\![B'[x := e_2]]\!]$ by Lemma 3.4, and we finally derive our conclusion by [Conv].

(2.2.2) By $\triangleright_\delta$, we are trying to show $[\![\Gamma]\!], \Gamma', x_1 = [\![e_1]\!], x_2 = [\![e_2]\!] \vdash [\![e_1\, e_2]\!] \equiv [\![e_1]\!]\ [\![e_2]\!]$. We find that the left-hand side of the equivalence can be converted as well:

$$
\begin{aligned}
& [\![e_1\, e_2]\!] \\
& \stackrel{\text{def}}{=} [\![e_1]\!]\, \mathbf{let}\, x_1 = [\cdot]\, \mathbf{in}\ [\![e_2]\!]\, \mathbf{let}\, x_2 = [\cdot]\, \mathbf{in}\, x_1\ x_2 && && (44)\\
& = \mathbf{let}\, x_1 = [\cdot]\, \mathbf{in}\ [\![e_2]\!]\, \mathbf{let}\, x_2 = [\cdot]\, \mathbf{in}\, x_1\ x_2 \langle\!\langle\, [\![e_1]\!]\, \rangle\!\rangle && \text{by Lemma 3.2} && (45)\\
& \equiv \mathsf{let}\, x_1 = [\![e_1]\!]\ \mathsf{in}\ [\![e_2]\!]\, \mathbf{let}\, x_2 = [\cdot]\, \mathbf{in}\, x_1\ x_2 && \text{by Lemma 2.5} && (46)\\
& \triangleright^*\ [\![e_2]\!]\, \mathbf{let}\, x_2 = [\cdot]\, \mathbf{in}\ [\![e_1]\!]\ x_2 && && (47)\\
& = \mathbf{let}\, x_2 = [\cdot]\, \mathbf{in}\ [\![e_1]\!]\ x_2 \langle\!\langle\, [\![e_2]\!]\, \rangle\!\rangle && \text{by Lemma 3.2} && (48)\\
& \equiv \mathsf{let}\, x_2 = [\![e_2]\!]\ \mathsf{in}\ [\![e_1]\!]\ x_2 && \text{by Lemma 2.5} && (49)\\
& \triangleright_\zeta\ [\![e_1]\!]\ [\![e_2]\!] && && (50)
\end{aligned}
$$

Case: [Snd]

We have that $\vdash \Gamma, \Gamma \vdash \mathsf{snd}\, e : B'[x := \mathsf{fst}\, e]$, and $[\![\Gamma]\!], \Gamma' \vdash K : (N : [\![B'[x := \mathsf{fst}\, e]]\!]) \Rightarrow B$ such that $[\![\Gamma]\!], \Gamma' \vdash [\![\mathsf{snd}\, e]\!] \equiv N$. We must show that $[\![\Gamma]\!], \Gamma' \vdash [\![\mathsf{snd}\, e]\!]\, K : B$, that is, $[\![\Gamma]\!], \Gamma' \vdash [\![e]\!]\, (\mathbf{let}\, x_1 = [\cdot]\, \mathbf{in}\, K[\mathbf{snd}\, x_1]) : B$. Our conclusion follows by induction on $\Gamma \vdash e : \Sigma\, x : A'.\, B'$, if we show $[\![\Gamma]\!], \Gamma' \vdash \mathbf{let}\, x_1 = [\cdot]\, \mathbf{in}\, K[\mathbf{snd}\, x_1] : ([\![e]\!] : [\![\Sigma\, x : A'.\, B']\!]) \Rightarrow B$. By [K-Bind], we must show (1) $[\![\Gamma]\!], \Gamma' \vdash [\![e]\!] : [\![\Sigma\, x : A'.\, B']\!]$ and (2) $[\![\Gamma]\!], \Gamma', x_1 = [\![e]\!] \vdash K[\mathbf{snd}\, x_1] : B$.
(1) follows from induction on $\Gamma \vdash e : \Sigma\, x : A'.\, B'$ with the empty continuation $[\![\Gamma]\!], \Gamma' \vdash [\cdot] : ([\![e]\!] : [\![\Sigma\, x : A'.\, B']\!]) \Rightarrow [\![\Sigma\, x : A'.\, B']\!]$.
(2) follows by Lemma 2.9 if we can show (2.1) $[\![\Gamma]\!], \Gamma', x_1 = [\![e]\!] \vdash \mathbf{snd}\, x_1 : [\![B'[x := \mathsf{fst}\, e]]\!]$ and (2.2) $[\![\Gamma]\!], \Gamma', x_1 = [\![e]\!] \vdash [\![\mathsf{snd}\, e]\!] \equiv \mathbf{snd}\, x_1$.
(2.1) By $\triangleright_\delta$, we are trying to show $[\![\Gamma]\!], \Gamma', x_1 = [\![e]\!] \vdash \mathbf{snd}\, [\![e]\!] : [\![B'[x := \mathsf{fst}\, e]]\!]$. We have previously shown in (1) that $[\![\Gamma]\!], \Gamma' \vdash [\![e]\!] : \Sigma\, x : [\![A']\!].\, [\![B']\!]$. Using this fact with [Snd] and weakening, we derive that $[\![\Gamma]\!], \Gamma', x_1 = [\![e]\!] \vdash \mathbf{snd}\, [\![e]\!] : [\![B']\!][x := \mathbf{fst}\, [\![e]\!]]$. We can derive our conclusion by [Conv] if we can show that $[\![B'[x := \mathsf{fst}\, e]]\!]$ is equivalent to $[\![B']\!][x := \mathbf{fst}\, [\![e]\!]]$.
By Lemma 3.4, we have that $[\![B'[x := \mathsf{fst}\, e]]\!]$ is equivalent to $[\![B']\!][x := [\![\mathsf{fst}\, e]\!]]$. Focusing on $[\![\mathsf{fst}\, e]\!]$, we have:

$$
\begin{aligned}
& [\![\mathsf{fst}\, e]\!] \\
& \overset{\text{def}}{=} [\![e]\!]\, (\mathbf{let}\, x_1 = [\cdot]\, \mathbf{in}\, \mathbf{fst}\, x_1) && && (51)\\
& = \mathbf{let}\, x_1 = [\cdot]\, \mathbf{in}\, \mathbf{fst}\, x_1 \langle\!\langle\, [\![e]\!]\, \rangle\!\rangle && \text{by Lemma 3.2} && (52)\\
& \equiv \mathbf{let}\, x_1 = [\![e]\!]\, \mathbf{in}\, \mathbf{fst}\, x_1 && \text{by Lemma 2.5} && (53)\\
& \triangleright_\zeta\, \mathbf{fst}\, [\![e]\!] && && (54)
\end{aligned}
$$

Thus we derive that $[\![B'[x := \mathsf{fst}\, e]]\!]$ is equivalent to $[\![B']\!][x := \mathbf{fst}\, [\![e]\!]]$.
(2.2) By $\triangleright_\delta$, we are trying to show $[\![\Gamma]\!], \Gamma', x_1 = [\![e]\!] \vdash [\![\mathsf{snd}\, e]\!] \equiv \mathbf{snd}\, [\![e]\!]$. Focusing on $[\![\mathsf{snd}\, e]\!]$, we have:

$$
\begin{aligned}
& [\![\mathsf{snd}\, e]\!] \\
& \overset{\text{def}}{=} [\![e]\!]\, (\mathbf{let}\, x_1 = [\cdot]\, \mathbf{in}\, \mathbf{snd}\, x_1) && && (55)\\
& = \mathbf{let}\, x_1 = [\cdot]\, \mathbf{in}\, \mathbf{snd}\, x_1 \langle\!\langle\, [\![e]\!]\, \rangle\!\rangle && \text{by Lemma 3.2} && (56)\\
& \equiv \mathbf{let}\, x_1 = [\![e]\!]\, \mathbf{in}\, \mathbf{snd}\, x_1 && \text{by Lemma 2.5} && (57)\\
& \triangleright_\zeta\, \mathbf{snd}\, [\![e]\!] && && (58)
\end{aligned}
$$

Case: [If]
We have that $\vdash \Gamma, \Gamma \vdash \mathsf{if}\, e\, \mathsf{then}\, e_1\, \mathsf{else}\, e_2 : B'[x' := e]$, and $[\![\Gamma]\!], \Gamma' \vdash K : (N : [\![B'[x' := e]]\!]) \Rightarrow B$ such that $[\![\Gamma]\!], \Gamma' \vdash [\![\mathsf{if}\, e\, \mathsf{then}\, e_1\, \mathsf{else}\, e_2]\!] \equiv N$. We must show that $[\![\Gamma]\!], \Gamma' \vdash [\![\mathsf{if}\, e\, \mathsf{then}\, e_1\, \mathsf{else}\, e_2]\!]\, K : B$, that is, $[\![\Gamma]\!], \Gamma' \vdash [\![e]\!]\, (\mathbf{let}\, x = [\cdot]\, \mathbf{in}\, \mathbf{if}\, x\, \mathbf{then}\, [\![e_1]\!]\, K\, \mathbf{else}\, [\![e_2]\!]\, K) : B$. Let $K_1 = \mathbf{let}\, x = [\cdot]\, \mathbf{in}\, \mathbf{if}\, x\, \mathbf{then}\, [\![e_1]\!]\, K\, \mathbf{else}\, [\![e_2]\!]\, K$. Our conclusion follows by induction on $\Gamma \vdash e : \mathsf{bool}$, if we show $[\![\Gamma]\!], \Gamma' \vdash K_1 : ([\![e]\!] : [\![\mathsf{bool}]\!]) \Rightarrow B$. By [K-Bind], we must show (1) $[\![\Gamma]\!], \Gamma' \vdash [\![e]\!] : [\![\mathsf{bool}]\!]$ and (2) $[\![\Gamma]\!], \Gamma', x = [\![e]\!] \vdash \mathbf{if}\, x\, \mathbf{then}\, [\![e_1]\!]\, K\, \mathbf{else}\, [\![e_2]\!]\, K : B$.
(1) follows from induction on $\Gamma \vdash e : \mathsf{bool}$ with the empty continuation $[\![\Gamma]\!], \Gamma' \vdash [\cdot] : ([\![e]\!] : [\![\mathsf{bool}]\!]) \Rightarrow [\![\mathsf{bool}]\!]$.
(2) By [If], we now must show (2.1) $[\![\Gamma]\!], \Gamma', x = [\![e]\!] \vdash B : U$, (2.2) $[\![\Gamma]\!], \Gamma', x = [\![e]\!] \vdash x : \mathbf{bool}$ (2.3) $[\![\Gamma]\!], \Gamma', x = [\![e]\!], x \equiv \mathbf{true} \vdash [\![e_1]\!]\, K : B$ (2.4) $[\![\Gamma]\!], \Gamma', x = [\![e]\!], x \equiv \mathbf{false} \vdash [\![e_2]\!]\, K : B$
(2.1) should follow from induction on $\Gamma \vdash B : U$ and the empty continuation.
(2.2) By $\triangleright_\delta$ and the fact that $[\![\mathsf{true}]\!] = \mathbf{true}$, we can show that $[\![\Gamma]\!], \Gamma', x = [\![e]\!] \vdash [\![e]\!] : \mathbf{true}$ following the same method done above in (1).
(2.3) This follows by induction on $\Gamma \vdash e_1 : B'[x' := \mathsf{true}]$ if we can show (2.3.1) $[\![\Gamma]\!], \Gamma', x = [\![e]\!], x \equiv \mathbf{true} \vdash K : ([\![e_1]\!] : [\![B'[x' := \mathsf{true}]]\!]) \Rightarrow B$ and (2.3.2) $[\![\Gamma]\!], \Gamma', x = [\![e]\!], x \equiv \mathbf{true} \vdash [\![\mathsf{if}\, e\, \mathsf{then}\, e_1\, \mathsf{else}\, e_2]\!] \equiv [\![e_1]\!]$.
(2.3.1) follows from our earlier assumption and [Conv] if we can show that $[\![\Gamma]\!], \Gamma', x = [\![e]\!], x \equiv \mathbf{true} \vdash [\![B'[x' := e]]\!] \equiv [\![B'[x' := \mathsf{true}]]\!]$. By Lemma 3.4, we are trying to show $[\![\Gamma]\!], \Gamma', x = [\![e]\!], x \equiv \mathbf{true} \vdash [\![B']\!][x' := [\![e]\!]] \equiv [\![B']\!][x' := \mathbf{true}]$. By [Reflect] and Lemma 3.10, symmetry and transitivity, we can derive that under this extended context $[\![\Gamma]\!], \Gamma', x = [\![e]\!], x \equiv \mathbf{true} \vdash [\![e]\!] \equiv \mathbf{true}$, and thus we can conclude $[\![\Gamma]\!], \Gamma', x = [\![e]\!], x \equiv \mathbf{true} \vdash [\![B']\!][x' := [\![e]\!]] \equiv [\![B']\!][x' := \mathbf{true}]$.
(2.3.2) follows by reducing the left-hand side of the expression, and the fact that we derived $[\![e]\!] \equiv \mathbf{true}$ in (2.3.1.):

$\boxed{\mathsf{v} \approx \mathbf{V}}$

$$\mathsf{true} \approx \mathbf{true} \qquad\qquad \mathsf{false} \approx \mathbf{false}$$

$\boxed{\Gamma \vdash \gamma}$

$$\frac{}{\cdot \vdash \emptyset} \qquad \frac{\cdot \vdash \mathsf{e} : \mathsf{A} \qquad \Gamma \vdash \gamma}{\Gamma, \mathsf{x} = \mathsf{e} \vdash \gamma[\mathsf{x} \mapsto \gamma(\mathsf{e})]} \qquad \frac{\cdot \vdash \mathsf{e} : \mathsf{A} \qquad \Gamma \vdash \gamma}{\Gamma, \mathsf{x} : \mathsf{A} \vdash \gamma[\mathsf{x} \mapsto \mathsf{e}]}$$

Fig. 15. Separate Compilation Definitions

$$
\begin{aligned}
&[\![\mathsf{if\ e\ then\ e_1\ else\ e_2}]\!] \\
&\stackrel{\text{def}}{=} [\![\mathsf{e}]\!]\,(\mathbf{let\ x} = [\cdot]\ \mathbf{in\ if\ x\ then}\ [\![\mathsf{e_1}]\!]\ \mathbf{else}\ [\![\mathsf{e_2}]\!]) && && (59)\\
&= \mathbf{let\ x} = [\cdot]\ \mathbf{in\ if\ x\ then}\ [\![\mathsf{e_1}]\!]\ \mathbf{else}\ [\![\mathsf{e_2}]\!]\ \langle\!\langle\, [\![\mathsf{e}]\!]\, \rangle\!\rangle && \text{by Lemma 3.2} && (60)\\
&\equiv \mathsf{let\ x} = [\![\mathsf{e}]\!]\ \mathsf{in}\ \mathbf{if}\ \mathsf{x}\ \mathbf{then}\ [\![\mathsf{e_1}]\!]\ \mathbf{else}\ [\![\mathsf{e_2}]\!] && \text{by Lemma 2.5} && (61)\\
&\rhd_\zeta\ \mathbf{if}\ [\![\mathsf{e}]\!]\ \mathbf{then}\ [\![\mathsf{e_1}]\!]\ \mathbf{else}\ [\![\mathsf{e_2}]\!] && && (62)\\
&\rhd^*\ [\![\mathsf{e_1}]\!] && \text{by } [\![\mathsf{e}]\!] \equiv \mathbf{true} && (63)
\end{aligned}
$$

Thus we obtain our goal of $[\![\Gamma]\!], \mathbf{\Gamma'}, \mathbf{x} = [\![\mathsf{e}]\!], \mathbf{x} \equiv \mathbf{true} \vdash [\![\mathsf{if\ e\ then\ e_1\ else\ e_2}]\!] \equiv [\![\mathsf{e_1}]\!]$.
(2.4) follows analogously (but we derive that $[\![\mathsf{e}]\!] \equiv \mathbf{false}$).

□

Lemma 3.10. *If* $\mathbf{\Gamma} \vdash \mathbf{x} : \mathbf{A}$, $\mathbf{\Gamma} \vdash \mathbf{e} : \mathbf{A}$, *and* $\mathbf{x} = \mathbf{e} \in \mathbf{\Gamma}$, *then* $\mathbf{\Gamma} \vdash \mathbf{x} \equiv \mathbf{e}$.

Proof. We have that $\mathbf{\Gamma} \vdash \mathbf{x} \rhd^* \mathbf{e}$ by $\rhd_\delta$, and $\mathbf{\Gamma} \vdash \mathbf{e} \rhd^* \mathbf{e}$ by [Refl]. Then, by [≡], $\mathbf{\Gamma} \vdash \mathbf{x} \equiv \mathbf{e}$. □

Theorem 3.11 (Type Preservation). *If* $\Gamma \vdash \mathsf{e} : \mathsf{A}$ *then* $[\![\Gamma]\!] \vdash [\![\mathsf{e}]\!] : [\![\mathsf{A}]\!]$

Proof. By Lemma 3.9, it suffices to show that $[\![\Gamma]\!] \vdash [\cdot] : (\_ : [\![\mathsf{A}]\!]) \Rightarrow [\![\mathsf{A}]\!]$, which is trivial. □

We also prove correctness of separate compilation with respect to the ANF evaluation semantics. To do this we must define linking and define a specification, independent of the compiler, of when outputs are related across languages.

We first define observations, and when observations are related across languages. Without such a relation, the best we can prove is that the *translation* of the value v produced in the source is *definitionally equivalent* to the value we get by running the translated term, *i.e.*, we would get $[\![\mathsf{v}]\!] \equiv \mathbf{eval}([\![\mathsf{e}]\!])$. This fails to tell us how $[\![\mathsf{v}]\!]$ is related to v, unless we inspect the compiler. Instead, we define an independent specification relating observation across languages, which allows us to understand the correctness theorem without reading the compiler. We define the relation $\mathsf{v} \approx \mathbf{V}$ to compare ground values in Figure 15.

We define linking as substitution with well-typed closed terms, and define a closing substitution γ with respect to the environment Γ (also in Figure 15). Linking is defined by closing a term e such that $\Gamma \vdash \mathsf{e} : \mathsf{A}$ with a substitution $\Gamma \vdash \gamma$, written $\gamma(\mathsf{e})$. Any γ is valid for Γ if it maps each $\mathsf{x} : \mathsf{A} \in \Gamma$ to a closed term e of type A. For definitions in Γ, we require that if $\mathsf{x} = \mathsf{e} \in \Gamma$, then $\gamma[\mathsf{x} \mapsto \gamma(\mathsf{e})]$, that is, the substitution must map x to a closed version of its definition e. We lift the ANF translation to substitutions.

Correctness of separate compilation says that we can either link then run a program in the source language semantics, *i.e.*, using the conversion semantics, or separately compile the term and its closing substitution then run in the ANF evaluation semantics. Either way, we get equivalent terms.

Theorem 3.12 (Correctness of Separate Compilation). *If* $\Gamma \vdash \mathsf{e} : \mathsf{A}$, *(and* A *ground) and* $\Gamma \vdash \gamma$ *then* $\mathbf{eval}([\![\gamma]\!]\,([\![\mathsf{e}]\!])) \approx \mathsf{eval}(\gamma(\mathsf{e}))$.

Proof. The following diagram commutes, because ≡ corresponds to ≈ on ground types, the translation commutes with substitution, preserves equivalence, reduction implies equivalence, and equivalence is transitive.

$$\begin{tikzcd}
\mathrm{eval}(\gamma(\mathrm{e})) \arrow[r, "\equiv"] \arrow[d, "\equiv"] & [\![\gamma(\mathrm{e})]\!] \arrow[d, "\equiv"] \\
\mathbf{eval}([\![\gamma([\![\mathrm{e}]\!])]\!]) \arrow[r, "\equiv"] & [\![\gamma([\![\mathrm{e}]\!])]\!]
\end{tikzcd}$$

□

4 JOIN-POINT OPTIMIZATION

Recall from Figure 10 that the composition of a continuation K with a configuration $\mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2$, $\mathrm{K}\langle\langle \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \rangle\rangle$, duplicates K in the branches: intuitively, $\mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{K}\langle\langle \mathrm{M}_1 \rangle\rangle\ \mathbf{else}\ \mathrm{K}\langle\langle \mathrm{M}_2 \rangle\rangle$, although for type checking we need the ANF version of $\mathrm{K}\langle\langle \mathbf{subst}_{\mathrm{V}=\mathbf{true}}\ \mathrm{M}_1 \rangle\rangle$ for the branches. Similarly, the ANF translation in Figure 14 performs the same duplication when translating $\mathbf{if}$ expressions. This can cause exponential code duplication, which is no problem in theory but is a problem in practice.

ECC^A supports implementing the join-point optimization, which avoids this code duplication. We can see the optimization as either a modification to the ANF translation itself, or as an intra-language optimization over ECC^A programs. We present join-point optimization as the latter, as it is strictly more general (applies to all ECC^A terms, instead of only terms generated by one compiler) and easier to prove correct.

Formally, in ECC^A, the join-point optimization requires the following equivalence.

$$\begin{aligned}\mathrm{K}\langle\langle \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \rangle\rangle \equiv\ & \mathbf{let}\ \mathrm{f} = (\lambda\, \mathrm{x} : \mathrm{B}[\mathrm{x} := \mathrm{V}].\ \mathrm{K}[\mathrm{x}])\ \mathbf{in} \\ & \quad \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ (\mathbf{let}\ \mathrm{x} = [\cdot], \mathrm{z} = \mathbf{subst}_{\mathrm{V}=\mathbf{true}}\ \mathrm{x}\ \mathbf{in}\ \mathrm{f}\ \mathrm{z})\langle\langle \mathrm{M}_1 \rangle\rangle \\ & \quad\quad \mathbf{else}\ (\mathbf{let}\ \mathrm{x} = [\cdot], \mathrm{z} = \mathbf{subst}_{\mathrm{V}=\mathbf{false}}\ \mathrm{x}\ \mathbf{in}\ \mathrm{f}\ \mathrm{z})\langle\langle \mathrm{M}_2 \rangle\rangle\end{aligned}$$

Note that instead of duplicating K in the branches as before, we introduce a function f that abstracts over K and call it in the branches. In essence, this introduces a local first-class continuation f that abstracts the non-first-class continuation K. We also prove a more general statement of this equivalence in our Coq model.

From β and ζ reduction, it is simple to conclude the desired equivalence, formally stated below as Lemma 4.1.

Lemma 4.1 (Join Point Equivalence).

$$\begin{aligned}\mathrm{K}\langle\langle \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \rangle\rangle \equiv\ & \mathbf{let}\ \mathrm{f} = (\lambda\, \mathrm{x} : \mathrm{B}[\mathrm{x} := \mathrm{V}].\ \mathrm{K}[\mathrm{x}])\ \mathbf{in} \\ & \quad \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ (\mathbf{let}\ \mathrm{x} = [\cdot], \mathrm{z} = \mathbf{subst}_{\mathrm{V}=\mathbf{true}}\ \mathrm{x}\ \mathbf{in}\ \mathrm{f}\ \mathrm{z})\langle\langle \mathrm{M}_1 \rangle\rangle \\ & \quad\quad \mathbf{else}\ (\mathbf{let}\ \mathrm{x} = [\cdot], \mathrm{z} = \mathbf{subst}_{\mathrm{V}=\mathbf{false}}\ \mathrm{x}\ \mathbf{in}\ \mathrm{f}\ \mathrm{z})\langle\langle \mathrm{M}_2 \rangle\rangle\end{aligned}$$

Proof. By β and ζ reduction, it suffices to show that
$\mathrm{K}\langle\langle \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \rangle\rangle \equiv \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ (\mathrm{K}[\mathbf{subst}_{\mathrm{V}=\mathbf{true}}\ \mathrm{x}][\mathrm{M}_1//\mathrm{x}])\ \mathbf{else}\ (\mathrm{K}[\mathbf{subst}_{\mathrm{V}=\mathbf{false}}\ \mathrm{x}][\mathrm{M}_2//\mathrm{x}])$
which holds by definition.
Note that since equivalence is defined over untyped syntax, the annotation $\mathrm{B}[\mathrm{x} := \mathrm{V}]$ is irrelevant. □

The more difficult part is showing that the join point optimization is well typed. To do this, we need continuation typing. Assuming that the unoptimized term $\mathrm{K}\langle\langle \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \rangle\rangle$ is well typed and K itself has the expected type, then the join-point optimization is well typed.

Lemma 4.2 (Join Point Well Typed). *If* $\Gamma \vdash \mathrm{K}\langle\langle \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \rangle\rangle : \mathrm{C}$, $\Gamma \vdash \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 : \mathrm{B}[\mathrm{x} := \mathrm{V}]$, *and* $\Gamma \vdash \mathrm{K} : \mathtt{hole}(\mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2) : \mathrm{B}' \Rightarrow \mathrm{C}$ *then*

$$\begin{aligned}\Gamma \vdash\ & \mathbf{let}\ \mathrm{f} = (\lambda\, \mathrm{x} : \mathrm{B}[\mathrm{x} := \mathrm{V}].\ \mathrm{K}[\mathrm{x}])\ \mathbf{in} \\ & \quad \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ (\mathbf{let}\ \mathrm{x} = [\cdot], \mathrm{z} = \mathbf{subst}_{\mathrm{V}=\mathbf{true}}\ \mathrm{x}\ \mathbf{in}\ \mathrm{f}\ \mathrm{z})\langle\langle \mathrm{M}_1 \rangle\rangle \\ & \quad\quad \mathbf{else}\ (\mathbf{let}\ \mathrm{x} = [\cdot], \mathrm{z} = \mathbf{subst}_{\mathrm{V}=\mathbf{false}}\ \mathrm{x}\ \mathbf{in}\ \mathrm{f}\ \mathrm{z})\langle\langle \mathrm{M}_2 \rangle\rangle : \mathrm{C}\end{aligned}$$

Proof. By definition, $\Gamma \vdash \mathrm{K}\langle\langle \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{M}_1\ \mathbf{else}\ \mathrm{M}_2 \rangle\rangle : \mathrm{C}$ implies
$\Gamma \vdash \mathbf{if}\ \mathrm{V}\ \mathbf{then}\ \mathrm{K}[\mathbf{subst}_{\mathrm{V}=\mathbf{true}}\ \mathrm{x}][\mathrm{M}_1//\mathrm{x}]\ \mathbf{else}\ \mathrm{K}[\mathbf{subst}_{\mathrm{V}=\mathbf{false}}\ \mathrm{x}][\mathrm{M}_2//\mathrm{x}] : \mathrm{C}$
Let $\Gamma' = (\Gamma, \mathrm{f} = \lambda\, \mathrm{x} : (\mathrm{B}[\mathrm{x} := \mathrm{V}]).\ \mathrm{K}[\mathrm{x}])$, and note that $\mathrm{f} : (\mathrm{B}[\mathrm{x} := \mathrm{V}]) \rightarrow \mathrm{C}$.
By [If] and Lemma 2.12 (Hetereogeneous Cut), it suffices to show that

(1) $\Gamma', \mathrm{V} = \mathbf{true}, \mathtt{defs}(\mathrm{M}_1) \vdash (\mathbf{let}\ \mathrm{x} = [\cdot], \mathrm{z} = \mathbf{subst}_{\mathrm{V}=\mathbf{true}}\ \mathrm{x}\ \mathbf{in}\ \mathrm{f}\ \mathrm{z}) : (\mathtt{hole}(\mathrm{M}_1) : \mathrm{B}[\mathbf{true} := \mathrm{x}]) \Rightarrow \mathrm{C}$
 By [K-Bind] and [Let], it suffices to show
 $\Gamma', \mathrm{V} = \mathbf{true}, \mathtt{defs}(\mathrm{M}_1), \mathrm{x} = \mathtt{hole}(\mathrm{M}_1), \mathrm{z} = \mathbf{subst}_{\mathrm{V}=\mathbf{true}}\ \mathrm{x} \vdash \mathrm{f}\ \mathrm{z} : \mathrm{C}$
 By [App], it suffices to show that
 $\Gamma', \mathrm{V} = \mathbf{true}, \mathtt{defs}(\mathrm{M}_1), \mathrm{x} = \mathtt{hole}(\mathrm{M}_1) \vdash \mathbf{subst}_{\mathrm{V}=\mathbf{true}}\ \mathrm{x} : (\mathrm{B}[\mathrm{x} := \mathrm{V}])$,
 which follows by [Subst] since $(\mathtt{hole}(\mathrm{M}_1) : \mathrm{B}'[\mathrm{x} := \mathbf{true}])$ and we have $\mathrm{V} = \mathbf{true}$.
(2) $\Gamma', \mathrm{V} = \mathbf{false}, \mathtt{defs}(\mathrm{M}_2) \vdash (\mathbf{let}\ \mathrm{x} = [\cdot], \mathrm{z} = \mathbf{subst}_{\mathrm{V}=\mathbf{false}}\ \mathrm{x}\ \mathbf{in}\ \mathrm{f}\ \mathrm{z}) : (\mathtt{hole}(\mathrm{M}_2) : \mathrm{B}[\mathbf{false} := \mathrm{x}]) \Rightarrow \mathrm{C}$, which follows symmetrically. □

It's a simple corollary to show we can now modify the ANF translation from Section 3 to use the definition in Figure 16, and it is still correct and type preserving. However, note that the new translation requires access to the

$\boxed{[\![e]\!]\,K = M}$

$$\vdots$$

$$
\begin{aligned}
[\![\mathsf{if}\ e\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2]\!]\,K \stackrel{\text{def}}{=}\ & [\![e]\!]\ \mathbf{let}\ x' = [\cdot]\ \mathbf{in}\ \mathbf{let}\ f = (\lambda\, x : [\![B]\!][x := [\![e]\!]].\,K[x])\ \mathbf{in} \\
& \qquad\qquad\qquad\qquad \mathbf{if}\ x'\ \mathbf{then}\ [\![e_1]\!]\ (\mathbf{let}\ x = [\cdot], z = \mathbf{subst}_{\,x'=\mathbf{true}}\ x\ \mathbf{in}\ f\ z) \\
& \qquad\qquad\qquad\qquad\quad \mathbf{else}\ [\![e_2]\!]\ (\mathbf{let}\ x = [\cdot], z = \mathbf{subst}_{\,x'=\mathbf{false}}\ x\ \mathbf{in}\ f\ z) \\
& \text{where } \Gamma \vdash \mathsf{if}\ e\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 : B[x := e]
\end{aligned}
$$

Fig. 16. Join-Point Optimized ANF Translation

type B from the derivation. We can do this either by defining the translation by induction over typing derivations, or (preferably) modifying the syntax of if to include B as a type annotation, similar to dependent pairs.

REFERENCES

Gilles Barthe, John Hatcliff, and Morten Heine B. Sørensen. 1999. CPS Translations and Applications: The Cube and Beyond. *Higher-Order and Symbolic Computation* 12, 2 (Sept. 1999). https://doi.org/10.1023/a:1010000206149

Gilles Barthe and Tarmo Uustalu. 2002. CPS Translating Inductive and Coinductive Types. In *Workshop on Partial Evaluation and Semantics-based Program Manipulation (PEPM)*. https://doi.org/10.1145/509799.503043

Simon Boulier, Pierre-Marie Pédrot, and Nicolas Tabareau. 2017. The Next 700 Syntactical Models of Type Theory. In *Conference on Certified Programs and Proofs (CPP)*. https://doi.org/10.1145/3018610.3018620

William J. Bowman and Amal Ahmed. 2018. Typed Closure Conversion for the Calculus of Constructions. In *International Conference on Programming Language Design and Implementation (PLDI)*. https://doi.org/10.1145/3192366.3192372

William J. Bowman, Youyou Cong, Nick Rioux, and Amal Ahmed. 2018. Type-preserving CPS Translation of Σ and Π Types Is Not Not Possible. *Proceedings of the ACM on Programming Languages (PACMPL)* 2, POPL (Jan. 2018). https://doi.org/10.1145/3158110

Adam Chlipala. 2013. *Certified Programming with Dependent Types - A Pragmatic Introduction to the Coq Proof Assistant.* MIT Press. http://adam.chlipala.net/cpdt/

Youyou Cong and Kenichi Asai. 2018. Handling Delimited Continuations with Dependent Types. *Proceedings of the ACM on Programming Languages (PACMPL)* 2, ICFP (Sept. 2018). https://doi.org/10.1145/3236764

Thierry Coquand and Gérard Huet. 1988. The Calculus of Constructions. *Information and Computation* 76, 2-3 (Feb. 1988). https://doi.org/10.1016/0890-5401(88)90005-3

Andrew Kennedy. 2007. Compiling with Continuations, Continued. In *International Conference on Functional Programming (ICFP)*. https://doi.org/10.1145/1291220.1291179

Zhaohui Luo. 1990. *An Extended Calculus of Constructions*. Ph.D. Dissertation. University of Edinburgh. http://www.lfcs.inf.ed.ac.uk/reports/90/ECS-LFCS-90-118/

Luke Maurer, Paul Downen, Zena M. Ariola, and Simon Peyton Jones. 2017. Compiling without Continuations. In *International Conference on Programming Language Design and Implementation (PLDI)*. https://doi.org/10.1145/3062341.3062380

Pierre-Marie Pédrot and Nicolas Tabareau. 2017. The Fire Triangle: How To Mix Substitution, Dependent Elimination and Effects. (2017). https://www.pe%CC%81drot.fr/articles/dcbpv.pdf

Amr Sabry and Philip Wadler. 1997. A Reflection on Call-by-Value. *ACM Transactions on Programming Languages and Systems (TOPLAS)* 19, 6 (Nov. 1997). https://doi.org/10.1145/267959.269968

Paula Severi and Erik Poll. 1994. Pure Type Systems with Definitions. In *International Symposium Logical Foundations of Computer Science (LFCS)*. https://doi.org/10.1007/3-540-58140-5_30

Hayo Thielecke. 2003. From Control Effects to Typed Continuation Passing. In *Symposium on Principles of Programming Languages (POPL)*. https://doi.org/10.1145/640128.604144

Kevin Watkins, Iliano Cervesato, Frank Pfenning, and David Walker. 2003. A Concurrent Logical Framework: The Propositional Fragment. In *International Workshop on Types for Proofs and Programs (TYPES)*. https://doi.org/10.1007/978-3-540-24849-1_23