Syntax and Semantics of Cedille

Aaron Stump, Chris Jenkins
Computer Science
The University of Iowa
aaron-stump@uiowa.edu, christopher-jenkins@uiowa.edu

1 Introduction

The type theory of Cedille is called the Calculus of Dependent Lambda Eliminations (CDLE). This document presents the version of CDLE as of April 13, 2021. We have made many changes from the first paper on CDLE [15], mostly in the form of dropping constructs we discovered (to our surprise) could be derived [16]. We have also omitted *lifting* – a technique for large eliminations with lambda encodings – in this document's version of CDLE. Some uses of lifting can be simulated other ways within the system, though the limits of this are still under investigation. We also include a construct δ, for deriving a contradiction from a proof that lambda-encoded true equals lambda-encoded false. This also compensates somewhat for the lack of lifting.

At a high level, CDLE is an extrinsic (i.e., Curry-style) type theory extending the Calculus of Constructions with three additional constructs, which allow deriving induction principles within the theory for lambda encodings of inductive datatypes. The goal is to support usual idioms of dependently typed programming and proving as in Agda or similar tools, but using pure lambda encodings for all data, and requiring a much smaller core theory suitable for formal verification.

The current Cedille implementation of CDLE extends with a number of features intended to make programming in the system more convenient and with less redundancy. These features all compile away to a slightly simplified version of the theory presented in this document, called Cedille Core, described here: `https://github.com/astump/cedille-core-spec`. At the time of writing, the Cedille implementation lags behind the formulation of CDLE in this document on one point: the treatment of the rewriting construct ρ. In the implementation, the fully-annotated form for this construct is $\rho\ t\ @x.T'$ - t', but in this document it is $\rho\ t\ @x\langle t_2\rangle.T'$ - t'. The implementation infers the additional subterm t_2.

2 Classification Rules

The classification rules are given in Figures 1, 2, and 3, with Figure 4 giving the context formation rules. For brevity, we take these figures as implicitly specifying the syntax of contexts Γ, kinds κ, types T, and annotated terms t; these may use term variables x and type variables X, which we assume come from distinct sets. So terms and types are syntactically distinguished. We follow the syntax of our implementation Cedille, which distinguishes application of a term or type e to a type ($e \cdot T$), from application to a term ($e\ t$), and application to an erased term argument (e -t, in which case e must be a term). Note that center dot ($\cdot$) is also used to denote the empty type context; since the usage for typing contexts always has the symbol occur to the left of the turnstile ($\vdash$), no confusion should arise from overloading notation.

The typing rules (Figure 3) are bidirectional [14], while the kinding rules (Figure 2) are unidirectional (synthesizing only) and the kind-formation rules (Figure 1) have no notion of directionality. We write $\Leftrightarrow$ to range over $\{\Leftarrow, \Rightarrow\}$, and when this symbol occurs multiple times in a rule, it is intended that such occurrences

$$\frac{}{\Gamma \vdash \star} \qquad \frac{\Gamma \vdash T \Rightarrow \star \quad \Gamma, x : T \vdash \kappa}{\Gamma \vdash \Pi\, x{:}T.\, \kappa} \qquad \frac{\Gamma \vdash \kappa' \quad \Gamma, X : \kappa' \vdash \kappa}{\Gamma \vdash \Pi\, X{:}\kappa'.\, \kappa}$$

Figure 1: Rules for checking that a kind is well-formed ($\Gamma \vdash \kappa$)

$$[t/x]^T \;=\; [\chi\ T\ \text{-}\ t/x]$$

$$\frac{(X : \kappa) \in \Gamma}{\Gamma \vdash X \Rightarrow \kappa} \qquad \frac{\Gamma \vdash \kappa \quad \Gamma, X : \kappa \vdash T \Rightarrow \star}{\Gamma \vdash \forall\, X{:}\kappa.\, T \Rightarrow \star}$$

$$\frac{\Gamma \vdash T \Rightarrow \star \quad \Gamma, x : T \vdash T' \Rightarrow \star}{\Gamma \vdash \forall\, x{:}T.\, T' \Rightarrow \star} \qquad \frac{\Gamma \vdash T \Rightarrow \star \quad \Gamma, x : T \vdash T' \Rightarrow \star}{\Gamma \vdash \Pi\, x{:}T.\, T' \Rightarrow \star}$$

$$\frac{\Gamma \vdash T \Rightarrow \star \quad \Gamma, x : T \vdash T' \Rightarrow \kappa}{\Gamma \vdash \lambda\, x{:}T.\, T' \Rightarrow \Pi\, x{:}T.\, \kappa} \qquad \frac{\Gamma \vdash \kappa \quad \Gamma, X : \kappa \vdash T' \Rightarrow \kappa'}{\Gamma \vdash \lambda\, X{:}\kappa.\, T' \Rightarrow \Pi\, X{:}\kappa.\, \kappa'}$$

$$\frac{\Gamma \vdash T \Rightarrow \Pi\, x{:}T'.\, \kappa \quad \Gamma \vdash t \Leftarrow T'}{\Gamma \vdash T\ t \Rightarrow [t/x]^{T'}\kappa} \qquad \frac{\Gamma \vdash T_1 \Rightarrow \Pi\, X{:}\kappa_2.\, \kappa_1 \quad \Gamma \vdash T_2 \Rightarrow \kappa_2' \quad \kappa_2 \cong \kappa_2'}{\Gamma \vdash T_1 \cdot T_2 \Rightarrow [T_2/X]\kappa_1}$$

$$\frac{\Gamma \vdash T \Rightarrow \star \quad \Gamma, x : T \vdash T' \Rightarrow \star}{\Gamma \vdash \iota\, x{:}T.\, T' \Rightarrow \star} \qquad \frac{FV(t\ t') \subseteq dom(\Gamma)}{\Gamma \vdash \{t \simeq t'\} \Rightarrow \star}$$

Figure 2: Rules for synthesizing a kind for a type ($\Gamma \vdash T \Rightarrow \kappa$)

be read the same way (i.e., read the occurrences as either all $\Leftarrow$ or all $\Rightarrow$). The rules are intended to be read bottom-up as an algorithm (in a standard way, c.f. [12, 13]) for synthesizing a classifier from a context and an expression (*type synthesis*, $\Rightarrow$) or checking an expression against a classifier in a context (*type checking*, $\Leftarrow$). Since variables have their type synthesized, and since we sometimes wish to substitute a variable with a term whose type can only be checked, we define a shorthand notation: $[t/x]^T$ means $[\chi\ T\ \text{-}\ t/x]$, where χ is the construct for explicit type annotations (see Section 2.1).

In typing rules, when the type of an introduction form is checked or the type of an elimination form is synthesized, we use call-by-name normalization, written $\rightsquigarrow_{\mathbf{n}}$ and $\rightsquigarrow_{\mathbf{n}}^*$ for the reflexive transitive closure, to put types in weak head normal form, revealing type constructors. We abbreviate the conjunction "term t synthesizes some type, and that type call-by-name reduces to another type" with the symbol $\overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow}$, defined formally at the top of Figure 3. When a redex (reducible expression) occurs such that the argument to a type is a term, such as $(\lambda\, x{:}T_1.\, T_2)\ t_1$, the reduction uses substitution with annotations: $[t_1/x]^{T_1}\ T_2$.

Call-by-name reduction is *not* what underpins the equivalence relation $\cong$ for types and kinds, which is full β-equivalence (for types) and $\beta\eta$-equivalence (for terms), both of which are modulo erasure of annotations in terms. The erasure operation is defined in Figure 5, and is essentially the *extraction* function for the Implicit Calculus of Constructions given by [1] adapted to CDLE. To understand the role of erasure, recall that the type theory is *extrinsic* (a.k.a. Curry-style), and hence we only consider erasures $|t|$ of terms when testing convertibility. This is lifted to the conversion relation on types $T \cong T'$ and kinds $\kappa \cong \kappa'$, whose rules are given in Figure 6.

$$\Gamma \vdash t \overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow} T \;=\; \exists T'.\ (\Gamma \vdash t \Rightarrow T') \wedge (T' \rightsquigarrow_{\mathbf{n}}^* T)$$

$$\frac{(x:T) \in \Gamma}{\Gamma \vdash x \Rightarrow T} \qquad \frac{\Gamma \vdash t \Rightarrow T' \quad T' \cong T}{\Gamma \vdash t \Leftarrow T}$$

$$\frac{T \rightsquigarrow_{\mathbf{n}}^* \Pi\, x{:}T_1.\, T_2 \quad \Gamma, x:T_1 \vdash t \Leftarrow T_2}{\Gamma \vdash \lambda\, x.\, t \Leftarrow T} \qquad \frac{\Gamma \vdash t \overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow} \Pi\, x{:}T'.\, T \quad \Gamma \vdash t' \Leftarrow T'}{\Gamma \vdash t\ t' \Rightarrow [t'/x]^{T'} T}$$

$$\frac{T' \rightsquigarrow_{\mathbf{n}}^* \forall\, X{:}\kappa.\, T \quad \Gamma, X:\kappa \vdash t \Leftarrow T}{\Gamma \vdash \Lambda\, X.\, t \Leftarrow T'} \qquad \frac{\Gamma \vdash t \overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow} \forall\, X{:}\kappa.\, T \quad \Gamma \vdash T' \Rightarrow \kappa' \quad \kappa' \cong \kappa}{\Gamma \vdash t \cdot T' \Rightarrow [T'/X]T}$$

$$\frac{T \rightsquigarrow_{\mathbf{n}}^* \forall\, x{:}T_1.\, T_2 \quad \Gamma, x:T_1 \vdash t \Leftarrow T_2 \quad x \notin FV(|t|)}{\Gamma \vdash \Lambda\, x.\, t \Leftarrow T} \qquad \frac{\Gamma \vdash t \overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow} \forall\, x{:}T'.\, T \quad \Gamma \vdash t' \Leftarrow T'}{\Gamma \vdash t\ \text{-}t' \Rightarrow [t'/x]^{T'} T}$$

$$\frac{\begin{array}{c} T \rightsquigarrow_{\mathbf{n}}^* \iota\, x{:}T_1.\, T_2 \qquad \Gamma \vdash t_1 \Leftarrow T_1 \\ \Gamma \vdash t_2 \Leftarrow [t_1/x]^{T_1}\ T_2 \quad |t_1| =_{\beta\eta} |t_2| \end{array}}{\Gamma \vdash [t_1, t_2] \Leftarrow T} \qquad \frac{\Gamma \vdash t \overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow} \iota\, x{:}T.\, T'}{\Gamma \vdash t.1 \Rightarrow T}$$

$$\frac{\Gamma \vdash t \overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow} \iota\, x{:}T.\, T'}{\Gamma \vdash t.2 \Rightarrow [t.1/x]T'} \qquad \frac{T \rightsquigarrow_{\mathbf{n}}^* \{t_1 \simeq t_2\} \quad FV(t') \subseteq dom(\Gamma) \quad |t_1| =_{\beta\eta} |t_2|}{\Gamma \vdash \beta\{t'\} \Leftarrow T}$$

$$\frac{\Gamma \vdash t \Rightarrow T' \quad T' \cong \{\lambda\, x.\, \lambda\, y.\, x \simeq \lambda\, x.\, \lambda\, y.\, y\}}{\Gamma \vdash \delta\ \text{-}\ t \Leftarrow T} \qquad \frac{\begin{array}{c} \Gamma \vdash t \overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow} \{t_1 \simeq t_2'\} \quad FV(t_2) \subseteq dom(\Gamma) \quad |t_2'| =_{\beta\eta} |t_2| \\ \Gamma \vdash [t_2/x]T' \Rightarrow \star \quad \Gamma \vdash t' \Leftarrow [t_2/x]T' \quad [t_1/x]T' \cong T \end{array}}{\Gamma \vdash \rho\ t\ @x\langle t_2\rangle.T'\ \text{-}\ t' \Leftarrow T}$$

$$\frac{\Gamma \vdash T \Rightarrow \star \quad \Gamma \vdash t \Leftarrow T}{\Gamma \vdash \chi\ T\ \text{-}\ t\ \Rightarrow T} \qquad \frac{\Gamma \vdash t \Leftarrow \{t' \simeq t''\} \quad \Gamma \vdash t' \Leftrightarrow T \quad FV(t'') \subseteq dom(\Gamma)}{\Gamma \vdash \varphi\ t\ \text{-}\ t'\ \{t''\} \Leftrightarrow T}$$

Figure 3: Rules for checking a term against a type ($\Gamma \vdash t \Leftarrow T$) and synthesizing a type for a term ($\Gamma \vdash t \Rightarrow T$)

$$\frac{}{\vdash \cdot} \qquad \frac{\vdash \Gamma \quad \Gamma \vdash T \Rightarrow \star}{\vdash \Gamma, x:T} \qquad \frac{\vdash \Gamma \quad \Gamma \vdash \kappa}{\vdash \Gamma, X:\kappa}$$

Figure 4: Rules for checking a context is well-formed

$$\begin{array}{lcllcl}
|x| & = & x & |\lambda\, x.\, t| & = & \lambda\, x.\, |t| \\
|t\ t'| & = & |t|\ |t'| & |t \cdot T| & = & |t| \\
|\Lambda\, x.\, t| & = & |t| & |t\ \text{-}t'| & = & |t| \\
|[t, t']| & = & |t| & |t.1| & = & |t| \\
|t.2| & = & |t| & |\beta\{t\}| & = & |t| \\
|\delta\ \text{-}\ t| & = & \lambda\, x.\, x & |\rho\ t\ @x\langle t_2\rangle.T'\ \text{-}\ t'| & = & |t'| \\
|\varphi\ t\ \text{-}\ t'\ \{t''\}| & = & |t''| & |\chi\ T\ \text{-}\ t| & = & |t|
\end{array}$$

Figure 5: Erasure for annotated terms

$$\boxed{T_1 \cong T_2} \qquad \boxed{T_1 \cong^{\mathrm{t}} T_2}$$

$$\frac{T_1 \rightsquigarrow_{\mathbf{n}}^{*} T_1' \not\rightsquigarrow_{\mathbf{n}} \quad T_2 \rightsquigarrow_{\mathbf{n}}^{*} T_2' \not\rightsquigarrow_{\mathbf{n}} \quad T_1' \cong^{\mathrm{t}} T_2'}{T_1 \cong T_2}$$

$$\frac{}{X \cong^{\mathrm{t}} X} \qquad \frac{\kappa_1 \cong \kappa_2 \quad T_1 \cong T_2}{\forall\, X{:}\kappa_1.\, T_1 \cong^{\mathrm{t}} \forall\, X{:}\kappa_2.\, T_2}$$

$$\frac{T_1 \cong T_2 \quad T_1' \cong T_2'}{\forall\, x{:}T_1.\, T_1' \cong^{\mathrm{t}} \forall\, x{:}T_2.\, T_2'} \qquad \frac{T_1 \cong T_2 \quad T_1' \cong T_2'}{\Pi\, x{:}T_1.\, T_1' \cong^{\mathrm{t}} \Pi\, x{:}T_2.\, T_2'}$$

$$\frac{T_1 \cong T_2 \quad T_1' \cong T_2'}{\lambda\, x{:}T_1.\, T_1' \cong^{\mathrm{t}} \lambda\, x{:}T_2.\, T_2'} \qquad \frac{\kappa_1 \cong \kappa_2 \quad T_1 \cong T_2}{\lambda\, X{:}\kappa_1.\, T_1 \cong^{\mathrm{t}} \lambda\, X{:}\kappa_2.\, T_2}$$

$$\frac{T_1 \cong T_2 \quad T_1' \cong T_2'}{\iota\, x{:}T_1.\, T_1' \cong^{\mathrm{t}} \iota\, x{:}T_2.\, T_2'} \qquad \frac{T_1 \cong^{\mathrm{t}} T_2 \quad |t_1| =_{\beta\eta} |t_2|}{T_1\ t_1 \cong^{\mathrm{t}} T_2\ t_2}$$

$$\frac{T_1 \cong^{\mathrm{t}} T_2 \quad T_1' \cong T_2'}{T_1 \cdot T_1' \cong^{\mathrm{t}} T_2 \cdot T_2'} \qquad \frac{|t_1| =_{\beta\eta} |t_1'| \quad |t_2| =_{\beta\eta} |t_2'|}{\{t_1 \simeq t_2\} \cong^{\mathrm{t}} \{t_1' \simeq t_2'\}}$$

$$\boxed{\kappa_1 \cong \kappa_2}$$

$$\frac{}{\star \cong \star} \qquad \frac{T_1 \cong T_2 \quad \kappa_1 \cong \kappa_2}{\Pi\, x{:}T_1.\, \kappa_1 \cong \Pi\, x{:}T_2.\, \kappa_2}$$

$$\frac{\kappa_1 \cong \kappa_2 \quad \kappa_1' \cong \kappa_2'}{\Pi\, X{:}\kappa_1.\, \kappa_1' \cong \Pi\, X{:}\kappa_2.\, \kappa_2'}$$

Figure 6: Conversion rules for classifiers

2.1 Overview of the constructs

CDLE has as a subsystem the extrinsic Calculus of Constructions (CC). We have dependent function types $\Pi\, x : T.\, T'$ and kinds $\Pi\, x : T.\, \kappa$, as well as term- and type-level quantification over (possibly higher-kinded) types $\forall\, X : \kappa.\, T$ and $\Pi\, X : \kappa.\, \kappa'$. We use $\forall$ when the corresponding argument will be erased, and Π when it will be retained. Since we do not erase term or type arguments from type-level applications, we thus write $\Pi\, X : \kappa.\, \kappa'$ instead of $\forall\, X : \kappa.\, \kappa'$. For abstractions, we write λ to correspond to Π and Λ to correspond to $\forall$. As noted above, application to a type is denoted with center dot $(\cdot)$.

To Curry-style CC, CDLE adds: implicit products, introduced originally by Miquel [10]; a primitive equality type $\{t \simeq t'\}$; and dependent intersection types $\iota\, x : T.\, T'$, introduced by Kopylov [9]. Implicit products are used for erased arguments to functions, found also in systems like Agda (c.f. [11]). Dependent intersections are a rather exotic construct allowing us to assign type $\iota\, x : T_1.\, T_2$ to erased term t when we can assign T_1 to t, and also assign $[t/x]T$ to t. For an annotated introduction form, we write $[t_1, t_2]$, where t_1 checks against type T_1, t_2 checks against $[t_1/x]^{T_1} T_2$, and t_1 and t_2 have $\beta\eta$-equivalent erasures. Dependent intersections thus enable a controlled form of self-reference in the type. Previous work showed how to use this to derive induction for Church-encoded natural numbers [16].

The typing rules include conversion checks in a few places, e.g., as is standard when switching from checking to synthesizing mode. For the introduction forms for types, the checked type first is call-by-name reduced to weak head normal form, which must be formed from the appropriate connective for the term construct (e.g., a Π-type for a lambda abstraction). Similarly, for the elimination forms the major premise has its type synthesized and then call-by-name normalized to reveal the correct connective. As is standard for a bidirectional type system, we also include the construct $\chi\ T$ - t for type ascription (allowing a term whose type can be checked to be given a user-provided type so that the whole expression synthesizes its type) and a judgmental (or *subsumption*) rule stating that terms whose types can be synthesized may be checked against a convertible type.

We have modified the rules for equality types $\{t_1 \simeq t_2\}$ so that we require nothing of t_1 and t_2 except that the set $dom(\Gamma)$ of variables declared by Γ includes their free variables $FV(t_1\ t_2)$. Further modifications over the version of CDLE in [16] are:

- To prove $\{t_1 \simeq t_2\}$ for definitionally equal terms (that is, terms that are $\beta\eta$-equivalent modulo erasure), one now writes $\beta\{t'\}$, with the critical idea that $|\beta\{t'\}|$ erases to (the possibly unrelated) $|t'|$. We call this the **Kleene trick** because it goes back to Kleene's numeric realizability [8], which accepts any number n as a realizer of a true equation. Here, we accept any term t' as a realizer of $\{t_1 \simeq t_2\}$ when t_1 and t_2 are definitionally equal, provided the free variables of t' are declared in the context.

  The Kleene trick means that in Cedille, any such term — even otherwise untypable terms, non-normalizing terms, etc. — prove trivially true equations. Put another way, any trivially true equation type in CDLE is a suitable type to classify all untyped lambda calculus terms.

- The ρ construct allows one to rewrite occurrences of t_1 in the checked type T of the whole expression to t_2 before checking the type of the subexpression t'. The version presented here requires a type annotation ("guide") $@x\langle t_2 \rangle.T$.

  In $\rho\ t\ @x\langle t_2 \rangle.T$ - t', the first subexpression t must synthesize (possibly after some normalization) an equation type of the form $\{t_1 \simeq t_2'\}$, and the user provided term t_2 must be $\beta\eta$-convertible (modulo erasure) to t_2'. The user provided type T' is then checked to have kind $\star$ after replacing occurrences of x with t_2, and the subexpression t' is checked against this type. Since equality is untyped, it may be that $[t_2'/x]T$ is not a well-kinded type, so in this explicit form we require a definitionally equal term t_2 from the user, which may involve more typing annotations.

  Finally, $[t_1/x]T'$ (which need not be well-kinded) must be convertible with the expected type T. In Cedille, the guide is optional and the construct may be used to rewrite a contextually given type; a heuristic, whose details are beyond the scope of this document, is used to produce a resulting type

that is well-kinded. The current implementation of Cedille (as of April 13, 2021), does not support specifying t_2 in the guide $@x\langle t_2\rangle.T$. This additional specification of the term t_2 was required to prove Theorem 6, which did not appear in earlier versions of this document (and its absence in prior versions does not affect the semantic proofs).

- We adopt a strong form of Nuprl's **direct computation rules** [3]: If we have a term t' of type T and a proof t that $\{t' \simeq t''\}$, then we may conclude that t'' has type T by writing the annotated term $\varphi\ t$ - $t'\ \{t''\}$, which erases to t''.
- Where the previous version of CDLE uses β-equivalence for (erased) terms, we here adopt $\beta\eta$-equivalence. This allows us to observe in many cases that retyping functions are actually $\beta\eta$-equivalent to $\lambda\, x.\, x$. While $\beta\eta$-equivalence takes more work to incorporate into intrinsic type theory [6], it raises no difficulties for our extrinsic one.
- We add an explicit axiom δ saying that Church-encoded boolean *true* is different from *false*. In the implementation of Cedille, this is generalized to the rule where the proof t synthesizes an equation $\{t_1 \simeq t_2\}$ in which $|t_1|$ and $|t_2|$ are separable using the *Böhm-out algorithm* [2].

  In the first version of CDLE, such an axiom was derivable from *lifting*, a construct allowing terms with simple types to be lifted to the type level [15]. We omit lifting in this new version of CDLE, because while sound, lifting as defined in that previous work is complicated and appears to be incomplete. Developing a new form of lifting remains to future work.

The equality type remains **intensional**: we equate closed terms iff they are $\beta\eta$-equal.

2.2 Semantics and metatheory

Figure 7 gives a realizability semantics for types and kinds, following the semantics given in the previous papers on CDLE [16, 15]. Details of this semantics are presented further in Section 2.3 below. Using the semantics and the definition in Figure 8 of $[\![\Gamma]\!]$, we can prove the following theorem:

Theorem 1 (Soundness)**.** *Suppose* $(\sigma, \rho) \in [\![\Gamma]\!]$. *Then we have:*

1. *If* $\Gamma \vdash \kappa$, *then* $[\![\kappa]\!]_{\sigma,\rho}$ *is defined.*
2. *If* $\Gamma \vdash T \Rightarrow \kappa$, *then* $[\![T]\!]_{\sigma,\rho} \in [\![\kappa]\!]_{\sigma,\rho}$.
3. *If* $\Gamma \vdash t \Rightarrow T$ *then* $[\sigma|t|]_{c\beta\eta} \in [\![T]\!]_{\sigma,\rho} \in \mathcal{R}$.
4. *If* $\Gamma \vdash t \Leftarrow T$ *and* $[\![T]\!]_{\sigma,\rho} \in \mathcal{R}$, *then* $[\sigma|t|]_{c\beta\eta} \in [\![T]\!]_{\sigma,\rho}$.
5. *If* $T \cong T'$ *or* $T \cong^t T'$ *and* $[\![T]\!]_{\sigma,\rho}$ *and* $[\![T']\!]_{\sigma,\rho}$ *are both defined, then they are equal.*
6. *If* $\kappa \cong \kappa'$ *and* $[\![\kappa]\!]_{\sigma,\rho}$ *and* $[\![\kappa']\!]_{\sigma,\rho}$ *are both defined, then they are equal.*

An easy corollary, by the semantics of $\forall$-types, is then:

Theorem 2 (Logical consistency)**.** *There is no term* t *such that* $\cdot \vdash t \Rightarrow \forall\, X : \star.\, X$.

It may worry some readers that we have:

Observation 3. *There are typable terms* t *which fail to normalize.*

Defining `Top` to be $\{\lambda\, x.\, x \simeq \lambda\, x.\, x\}$, we may assign `Top` to any closed term `t`, including non-normalizing ones. In our annotated syntax, we write $\beta\{\mathtt{t}\}$. Even without this, the presence of φ allows us to type non-normalizing terms assuming an erased argument x of type $\{\lambda\, x.\, x \simeq \lambda\, x.\, x\ x\}$ by changing the type of the term `id · True id`, where `True` is $\forall\, X : \star.\, X \to X$. This would allow us to give the type `True` to $\Omega = (\lambda\, x.\, x\ x)\ \lambda\, x.\, x\ x$. In general, we can use any inconsistent assumption to do this, and in the presence of δ that includes all equations between two terms that are Böhm-separable. But, failure of normalization does not impinge on Theorem 2. Extensional Martin-Löf type theory (MLTT) is also non-normalizing, for a

very similar reason, but this fact does not contradict its logical soundness [5]. In CDLE, the guarantees one gets about the behavior of terms are expressed almost entirely in their types. If the types are weak, then not much is guaranteed; but stronger types can guarantee properties like normalization, as demonstrated by the following theorem:

Theorem 4 (Call-by-name normalization of functions)**.** *Suppose* $\cdot \vdash t \Rightarrow T$ *and* $\cdot \vdash t' \Rightarrow T \to \Pi\, x{:}T_1.\, T_2$*, and furthermore that* $|t'| = \lambda\, x.\, x$*. Then* $|t|$ *is call-by-name normalizing.*

Given the lack of normalization in general, several checks in the typing rules – for things like $|t| =_{\beta\eta} |t'|$ – are formally undecidable. We simply impose a bound on the number of steps of reduction, and thus restore formal decidability (we are checking "typable within a given budget"). In practice, the same is done for Coq and Agda, where type checking is decidable but, in general, infeasible (since one may write astronomically slow terminating functions).

Finally, in line with ideas recently advocated by Dreyer, we are less concerned with syntactic type preservation as we are with *semantic* type preservation [4]. Note that by construction, semantic types $[\![T]\!]_{\sigma,\rho}$ are preserved by $\beta\eta$-reduction:

Theorem 5 (Semantic type preservation)**.** *If* $t \rightsquigarrow_{\beta\eta} t'$ *and* $t \in [\![T]\!]_{\sigma,\rho}$*, then* $t' \in [\![T]\!]_{\sigma,\rho}$*.*

Confluence of $\beta\eta$-reduction for (erased) terms is nothing other than confluence of untyped lambda calculus. This is because, as easily verified by inspecting Figure 5, the erasure function maps annotated terms t to terms $|t|$ of pure untyped lambda calculus.

We make a concession to syntactic classifier preservation in the case of types and kinds. During type inference, types may be reduced using a call-by-name operational semantics to reveal type constructors. With the removal of lifting from CDLE, terms cannot compute types and so no terms need to be reduced during this process.

Theorem 6 (Syntactic kind preservation)**.** *If* $\Gamma \vdash T \Rightarrow \kappa$ *and* $T \rightsquigarrow_{\mathbf{n}} T'$ *then* $\Gamma \vdash T' \Rightarrow \kappa'$ *for some* κ' *such that* $\kappa \cong \kappa'$*.*

From this theorem and a few other lemmas (see Appendix C), we can show the *validity* (or *agreement*) of the judgments comprising CDLE.

Theorem 7 (Judgment validity)**.** *If* $\vdash \Gamma$ *then:*

1. *if* $\Gamma \vdash T \Rightarrow \kappa$ *then* $\Gamma \vdash \kappa$
2. *if* $\Gamma \vdash t \Rightarrow T$ *then* $\Gamma \vdash T \Rightarrow \star$

Type checking ($\Gamma \vdash t \Leftarrow T$) is not covered in Theorem 7, since the convention for a bidirectional system is that there T is already *assumed* to have type $\star$ under a typing context.

2.3 Some details about the semantics and the proof of Theorem 1

Following the development in [15], we work with set-theoretic partial functions for the semantics of higher-kinded types. Types are interpreted as $\beta\eta$-closed sets of closed terms. Let $\mathcal{L}$ be the set of closed terms of pure lambda calculus (differently from [15], we include all terms at this point, even non-normalizing ones). We write $=_{c\beta\eta}$ for standard $\beta\eta$-equivalence of pure lambda calculus, restricted to closed terms; and $[t]_{c\beta\eta}$ for $\{t' \mid t =_{c\beta\eta} t'\}$. This is extended to sets S of terms by writing $[S]_{c\beta\eta}$ for $\{[t]_{c\beta\eta} \mid t \in S\}$. If (in our meta-language) we affirm a statement involving application of a partial function, then it is to be understood that that application is defined.

Definition 8 (Reducibility candidates)**.** $\mathcal{R} \coloneqq \{[S]_{c\beta\eta} \mid S \subseteq \mathcal{L}\}$.

Throughout the development we find it convenient to use a **choice function** ζ. Given any nonempty set E of terms, ζ returns some element of E. Note that if $a \in A \in \mathcal{R}$, then a is a nonempty set of terms of pure

$$
\begin{array}{lcl}
[\![X]\!]_{\sigma,\rho} & = & \rho(X) \\
[\![\Pi x : T_1.T_2]\!]_{\sigma,\rho} & = & [\{\lambda x.t \mid \forall E \in [\![T_1]\!]_{\sigma,\rho}. \\
 & & \quad [[\zeta(E)/x]t]_{c\beta\eta} \in [\![T_2]\!]_{\sigma[x\mapsto\zeta(E)],\rho} \ \wedge \ t = |t|\}]_{c\beta\eta} \\
[\![\forall X : \kappa.T]\!]_{\sigma,\rho} & = & \cap\{[\![T]\!]_{\sigma,\rho[X\mapsto S]} \mid S \in [\![\kappa]\!]_{\sigma,\rho}\} \\
[\![\forall x : T.T']\!]_{\sigma,\rho} & = & \cap_\star\{[\![T']\!]_{\sigma[x\mapsto\zeta(E)],\rho} \mid E \in [\![T]\!]_{\sigma,\rho}\} \\
[\![\iota x : T.T']\!]_{\sigma,\rho} & = & \{E \in [\![T]\!]_{\sigma,\rho} \mid E \in [\![T']\!]_{\sigma[x\mapsto\zeta(E)],\rho}\} \\
[\![\lambda X : \kappa.T]\!]_{\sigma,\rho} & = & (S \in [\![\kappa]\!]_{\sigma,\rho} \mapsto [\![T]\!]_{\sigma,\rho[X\mapsto S]}) \\
[\![\lambda x : T.T']\!]_{\sigma,\rho} & = & (E \in [\![T]\!]_{\sigma,\rho} \mapsto [\![T']\!]_{\sigma[x\mapsto\zeta(E)],\rho}) \\
[\![T\ T']\!]_{\sigma,\rho} & = & [\![T]\!]_{\sigma,\rho}([\![T']\!]_{\sigma,\rho}) \\
[\![T\ t]\!]_{\sigma,\rho} & = & [\![T]\!]_{\sigma,\rho}([\sigma|t|]_{c\beta\eta}) \\
[\![\{t \simeq t'\}]\!]_{\sigma,\rho} & = & [\{t'' \mid \sigma|t| =_{\beta\eta} \sigma|t'| \ \wedge \ t'' = |t''|\}]_{c\beta\eta} \\
 & & \quad \text{if } FV(t\ t') \subseteq dom(\sigma) \\
[\![\star]\!]_{\sigma,\rho} & = & \mathcal{R} \\
[\![\Pi x : T.\kappa]\!]_{\sigma,\rho} & = & (E \in [\![T]\!]_{\sigma,\rho} \to [\![\kappa]\!]_{\sigma[x\mapsto\zeta(E)],\rho}), \\
 & & \quad \text{if } [\![T]\!]_{\sigma,\rho} \in \mathcal{R} \\
[\![\Pi x : \kappa.\kappa']\!]_{\sigma,\rho} & = & (S \in [\![\kappa]\!]_{\sigma,\rho} \to [\![\kappa]\!]_{\sigma,\rho[X\mapsto S]}) \\
\cap_\star X & = & \begin{cases} \cap X, \text{ if } X \neq \varnothing \\ [\mathcal{L}]_{c\beta\eta}, \text{ otherwise} \end{cases}
\end{array}
$$

Figure 7: Semantics for types and kinds

$$
\begin{array}{lcl}
(\sigma \uplus [x \mapsto t], \rho) \in [\![\Gamma, x : T]\!] & \Leftrightarrow & (\sigma,\rho) \in [\![\Gamma]\!] \ \wedge \ [t]_{c\beta\eta} \in [\![T]\!]_{\sigma,\rho} \in \mathcal{R} \ \wedge \ t = |t| \\
(\sigma, \rho \uplus [X \mapsto S]) \in [\![\Gamma, X : \kappa]\!] & \Leftrightarrow & (\sigma,\rho) \in [\![\Gamma]\!] \ \wedge \ S \in [\![\kappa]\!]_{\sigma,\rho} \\
(\varnothing,\varnothing) \in [\![\cdot]\!] & &
\end{array}
$$

Figure 8: Semantics of typing contexts Γ

lambda calculus; it can also happen that $A \in \mathcal{R}$ is empty. The proof of Theorem 1 (see appendix) is then a straightforward adaptation of [15].

Acknowledgments. This work was partially supported by the US NSF support under award 1524519, and US DoD support under award FA9550-16-1-0082 (MURI program).

References

[1] Bruno Barras and Bruno Bernardo. The implicit calculus of constructions as a programming language with dependent types. In Roberto M. Amadio, editor, *Foundations of Software Science and Computational Structures, 11th International Conference, FOSSACS 2008, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2008, Budapest, Hungary, March 29 - April 6, 2008. Proceedings*, volume 4962 of *Lecture Notes in Computer Science*, pages 365–379. Springer, 2008.

[2] C. Böhm, M. Dezani-Ciancaglini, P. Peretti, and S.Ronchi Della Rocca. A discrimination algorithm inside lambda-beta-calculus. *Theoretical Computer Science*, 8(3):271 – 291, 1979.

[3] Robert L. Constable, Stuart F. Allen, Mark Bromley, Rance Cleaveland, J. F. Cremer, R. W. Harper, Douglas J. Howe, Todd B. Knoblock, N. P. Mendler, Prakash Panangaden, James T. Sasaki, and Scott F. Smith. *Implementing mathematics with the Nuprl proof development system*. Prentice Hall, 1986.

[4] Derek Dreyer. The Type Soundness Theorem That You Really Want to Prove (and Now You Can). Milner Award Lecture, delivered at Principles of Programming Languages (POPL), 2018.

[5] Peter Dybjer and Erik Palmgren. Intuitionistic Type Theory. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, winter 2016 edition, 2016.

[6] Herman Geuvers. The Church-Rosser Property for beta-eta-reduction in Typed lambda-Calculi. In *Proceedings of the Seventh Annual Symposium on Logic in Computer Science (LICS '92), Santa Cruz, California, USA, June 22-25, 1992*, pages 453–460. IEEE Computer Society, 1992.

[7] Ryo Kashima. A Proof of the Standardization Theorem in λ-Calculus. 2000. available from author's web page.

[8] S.C. Kleene. Classical Extensions of Intuitionistic Mathematics. In Y. Bar-Hillel, editor, *LMPS 2*, pages 31–44. North-Holland Publishing Company, 1965.

[9] Alexei Kopylov. Dependent intersection: A new way of defining records in type theory. In *18th IEEE Symposium on Logic in Computer Science (LICS)*, pages 86–95, 2003.

[10] Alexandre Miquel. The Implicit Calculus of Constructions Extending Pure Type Systems with an Intersection Type Binder and Subtyping. In Samson Abramsky, editor, *Typed Lambda Calculi and Applications*, volume 2044 of *Lecture Notes in Computer Science*, pages 344–359. Springer, 2001.

[11] Nathan Mishra-Linger and Tim Sheard. Erasure and Polymorphism in Pure Type Systems. In Roberto M. Amadio, editor, *Foundations of Software Science and Computational Structures, 11th International Conference, FOSSACS 2008, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2008, Budapest, Hungary, March 29 - April 6, 2008. Proceedings*, volume 4962 of *Lecture Notes in Computer Science*, pages 350–364. Springer, 2008.

[12] Simon Peyton Jones, Dimitrios Vytiniotis, Stephanie Weirich, and Mark Shields. Practical Type Inference for Arbitrary-rank Types. *J. Funct. Program.*, 17(1):1–82, January 2007.

[13] Frank Pfenning. Lecture notes on bidirectional typing. https://www.cs.cmu.edu/ fp/courses/15312-f04/handouts/15-bidirectional.pdf, October 2001.

[14] Benjamin C. Pierce and David N. Turner. Local type inference. *ACM Trans. Program. Lang. Syst.*, 22(1):1–44, 2000.

[15] Aaron Stump. The Calculus of Dependent Lambda Eliminations. *J. Funct. Program.*, 27:e14, 2017.

[16] Aaron Stump. From Realizability to Induction via Dependent Intersection, 2018. in press.

A Proof of Theorem 1

First a few lemmas (easy proofs omitted):

Lemma 9. *$[\![\kappa]\!]_{\sigma,\rho}$ is nonempty if defined.*

Lemma 10. *If E is nonempty, then $[\zeta(E)]_{c\beta\eta} = E$*

Lemma 11. *The set $\mathcal{R}$ ordered by subset forms a complete lattice, with greatest element $[\mathcal{L}]_{c\beta\eta}$ and greatest lower bound of a nonempty set of elements given by intersection. Also, $\varnothing$ is the least element.*

Lemma 12 (Term substitution and interpretation)**.** *If $t' =_{c\beta\eta} \sigma|t|$, then:*

- $[\![T]\!]_{\sigma[x\mapsto t'],\rho} = [\![[t/x]T]\!]_{\sigma,\rho}$
- $[\![\kappa]\!]_{\sigma[x\mapsto t'],\rho} = [\![[t/x]\kappa]\!]_{\sigma,\rho}$

Note that Lemma 12 also applies to typed substitution: if $t' =_{c\beta\eta} \sigma|t|$ then by erasure it is equal to $\sigma|\chi\ T\ \text{-}\ t'|$.

Lemma 13 (Type substitution and interpretation)**.**

- $[\![T]\!]_{\sigma,\rho[X\mapsto[\![T']\!]_{\sigma,\rho}]} = [\![[T'/X]T]\!]_{\sigma,\rho}$
- $[\![\kappa]\!]_{\sigma,\rho[X\mapsto[\![T']\!]_{\sigma,\rho}]} = [\![[T'/X]\kappa]\!]_{\sigma,\rho}$

x

Lemma 14. *If $T \rightsquigarrow^*_{\mathbf{n}} T'$ and $[\![T]\!]_{\sigma,\rho}$ is defined, then $[\![T']\!]_{\sigma,\rho}$ is also defined and equals $[\![T]\!]_{\sigma,\rho}$.*

Proof. This follows by induction on the reduction derivation, making use of the previous substitution lemmas. □

Soundness (Theorem 1). The following proof is adapted from [15]. It proceeds by mutual induction on the assumed typing, kinding, or kind formation derivation, for each part of the lemma. We prove the parts successively.

A.1 Proof of part (1)

Case:

$$\frac{}{\Gamma \vdash \star}$$

$[\![\star]\!]_{\sigma,\rho}$ is just $\mathcal{R}$, which is defined.

Case:

$$\frac{\Gamma \vdash T \Rightarrow \star \quad \Gamma, x : T \vdash \kappa}{\Gamma \vdash \Pi\, x{:}T.\, \kappa}$$

By the IH, $[\![T]\!]_{\sigma,\rho} \in \mathcal{R}$, and so $[\![\Pi x : T.\, \kappa]\!]_{\sigma,\rho}$ is $(E \in [\![T]\!]_{\sigma,\rho} \to [\![\kappa]\!]_{\sigma[x\mapsto\zeta(E)],\rho})$. The latter quantity is defined if for all $E \in [\![T]\!]_{\sigma,\rho}$, $[\![\kappa]\!]_{\sigma[x\mapsto\zeta(E)],\rho})$ is, too. Since $[\![T]\!]_{\sigma,\rho} \in \mathcal{R}$, every element E of $[\![T]\!]_{\sigma,\rho}$ is nonempty, as noted above, so $\zeta(E)$ is defined. We may apply the IH to the second premise, since $(\sigma[x \mapsto \zeta(E)], \rho) \in [\![\Gamma, x : T]\!]$, because $E \in [\![T]\!]_{\sigma,\rho}$ (by assumption) and $[\zeta(E)]_{c\beta\eta} = E$. This gives definedness of the semantics of the Π-kind.

Case:

$$\frac{\Gamma \vdash \kappa' \quad \Gamma, X : \kappa' \vdash \kappa}{\Gamma \vdash \Pi\, X{:}\kappa'.\, \kappa}$$

We must show $(S \in [\![\kappa]\!]_{\sigma,\rho} \to [\![\kappa]\!]_{\sigma,\rho[X \mapsto S]})$ is defined. This is true if $[\![\kappa]\!]_{\sigma,\rho}$ is defined, which is the case by the IH applied to the first premise; and if for all $S \in [\![\kappa]\!]_{\sigma,\rho}$, $[\![\kappa]\!]_{\sigma,\rho[X \mapsto S]}$ is defined. The latter is true by the IH applied to the second premise.

A.2 Proof of part (2)

Case:

$$\frac{(X : \kappa) \in \Gamma}{\Gamma \vdash X \Rightarrow \kappa}$$

From the definition of $[\![\Gamma]\!]$, we obtain $\rho(X) \in [\![\kappa]\!]_{\sigma,\rho}$.

Case:

$$\frac{\Gamma \vdash T \Rightarrow \star \quad \Gamma, x : T \vdash T' \Rightarrow \star}{\Gamma \vdash \Pi\, x{:}T.\, T' \Rightarrow \star}$$

We must show $[\![\Pi x : T.T']\!]_{\sigma,\rho} \in \mathcal{R}$. The semantics defines $[\![\Pi x : T.T']\!]_{\sigma,\rho}$ to be $[A]_{c\beta\eta}$ for a certain A, where if A is defined, then $A \subseteq \mathcal{L}$. So it suffices to shown definedness. By the IH for the first premise, $[\![T]\!]_{\sigma,\rho} \in \mathcal{R}$. This means that if $E \in [\![T]\!]_{\sigma,\rho}$, $\zeta(E)$ is defined. We can then apply the IH to the second premise, since $\sigma[x \mapsto \zeta(E)] \in [\![\Gamma, x : T]\!]$, to obtain definedness of $[\![T']\!]_{\sigma[x \mapsto \zeta(E),\rho}$.

Case:

$$\frac{\Gamma \vdash T \Rightarrow \star \quad \Gamma, x : T \vdash T' \Rightarrow \star}{\Gamma \vdash \forall\, x{:}T.\, T' \Rightarrow \star}$$

By the IH for the second premise, $[\![T_2]\!]_{\sigma[x \mapsto \zeta(E)],\rho} \in \mathcal{R}$, for every $E \in [\![T_1]\!]_{\sigma,\rho}$ where $[\![T_1]\!]_{\sigma,\rho} \in \mathcal{R}$. By the IH for the first premise, we indeed have $[\![T_1]\!]_{\sigma,\rho} \in \mathcal{R}$. So if $[\![T_1]\!]_{\sigma,\rho}$ is non-empty, then the intersection of all the sets $[\![T_2]\!]_{\sigma[x \mapsto \zeta(E)],\rho}$ where $E \in [\![T_1]\!]_{\sigma,\rho}$ is a reducibility candidate, since each of those sets is. By the semantics of $\forall$-types quantifying over terms, this is sufficient. If $[\![T_1]\!]_{\sigma,\rho}$ is empty, then the interpretation of the $\forall$-type is $[\mathcal{L}]_{c\beta\eta}$ by the definition of $\cap_\star$, and this is in $\mathcal{R}$.

Case:

$$\frac{\Gamma \vdash \kappa \quad \Gamma, X : \kappa \vdash T \Rightarrow \star}{\Gamma \vdash \forall\, X{:}\kappa.\, T \Rightarrow \star}$$

Similarly to the previous case: by the IH for the second premise, $[\![T_2]\!]_{\sigma,\rho[X \mapsto S} \in \mathcal{R}$, for every $S \in [\![\kappa]\!]_{\sigma,\rho}$. By the IH part for the first premise, $[\![\kappa]\!]_{\sigma,\rho}$ is defined. So the intersection of all the sets $[\![T_2]\!]_{\sigma,\rho[X \mapsto S]}$ where $S \in [\![\kappa]\!]_{\sigma,\rho}$ is a reducibility candidate, since each of those sets is. The intersection is nonempty, since $[\![\kappa]\!]_{\sigma,\rho}$ is (as stated in a lemma above). By the semantics of $\forall$-types quantifying over types, this is sufficient.

Case:

$$\frac{\Gamma \vdash T \Rightarrow \star \quad \Gamma, x : T \vdash T' \Rightarrow \star}{\Gamma \vdash \iota\, x{:}T.\, T' \Rightarrow \star}$$

The set $[\![\iota x : T.T']\!]_{\sigma,\rho}$ is explicitly defined to be a subset of $[\![T]\!]_{\sigma,\rho}$, which is in $\mathcal{R}$, by the IH applied to the first premise. Since for any $A \subseteq \mathcal{L}$, $[A]_{c\beta\eta}$ is in $\mathcal{R}$, to show that $[\![\iota x : T.T']\!]_{\sigma,\rho}$ is also in $\mathcal{R}$ it suffices to show definedness of $[\![T']\!]_{\sigma[x \mapsto \zeta(E)],\rho}\}$ (which is used in the predicate picking out the particular subset of $[\![T]\!]_{\sigma,\rho}$), for $E \in [\![T]\!]_{\sigma,\rho}$. For such E, $\zeta(E)$ is defined (since $[\![T]\!]_{\sigma,\rho} \in \mathcal{R}$ and hence $E \in [\![T]\!]_{\sigma,\rho}$ is nonempty) and in E, so $\sigma[x \mapsto \zeta(E)] \in [\![\Gamma, x : T]\!]$. So by the IH for the second premise, $[\![T']\!]_{\sigma[x \mapsto \zeta(E),\rho]}$ is defined.

Case:

$$\frac{\Gamma \vdash T \Rightarrow \star \quad \Gamma, x : T \vdash T' \Rightarrow \kappa}{\Gamma \vdash \lambda\, x{:}T.\, T' \Rightarrow \Pi\, x{:}T.\, \kappa}$$

By the semantics, $[\![\lambda x : T.T']\!]_{\sigma,\rho}$ is $(E \in [\![T]\!]_{\sigma,\rho} \mapsto [\![T']\!]_{\sigma[x\mapsto\zeta(E)],\rho})$. We must show that this (meta-level) function is in $[\![\Pi x : T.\kappa]\!]_{\sigma,\rho}$. By the semantics of kinds, the latter quantity, if defined, is $(E \in [\![T]\!]_{\sigma,\rho} \to_{c\beta\eta} [\![\kappa]\!]_{\sigma[x\mapsto\zeta(E)],\rho})$. By the IH for the first premise, $[\![T]\!]_{\sigma,\rho} \in \mathcal{R}$. So we must just show that for any $E \in [\![T]\!]_{\sigma,\rho}$, $[\![T']\!]_{\sigma[x\mapsto\zeta(E)],\rho} \in [\![\kappa]\!]_{\sigma[x\mapsto\zeta(E)],\rho}$. But this follows by the IH for the second premise.

Case:

$$\frac{\Gamma \vdash \kappa \quad \Gamma, X : \kappa \vdash T' \Rightarrow \kappa'}{\Gamma \vdash \lambda\, X{:}\kappa.\, T' \Rightarrow \Pi\, X{:}\kappa.\, \kappa'}$$

This case is an easier version of the previous one. It suffices to assume an arbitrary $S \in [\![\kappa]\!]_{\sigma,\rho}$ and show $[\![T']\!]_{\sigma,\rho[X\mapsto S]} \in [\![\kappa']\!]_{\sigma,\rho[X\mapsto S]}$. But this follows by the IH applied to the second premise. And we have definedness of $[\![\kappa]\!]_{\sigma,\rho}$ by the IH for the first premise.

Case:

$$\frac{\Gamma \vdash T \Rightarrow \Pi\, x{:}T'.\, \kappa \quad \Gamma \vdash t \Leftarrow T'}{\Gamma \vdash T\ t \Rightarrow [t/x]^{T'}\ \kappa}$$

By the IH for the first premise, $[\![T]\!]_{\sigma,\rho} \in [\![\Pi x : T'.\kappa]\!]_{\sigma,\rho}$. By the semantics of Π-kinds, this means that $[\![T]\!]_{\sigma,\rho}$ is a function which given any $E \in [\![T']\!]_{\sigma,\rho}$, will produce a result in $[\![\kappa]\!]_{\sigma[x\mapsto\zeta(E)],\rho}$. By the semantics of type applications, $[\![T\ t]\!]_{\sigma,\rho}$ is equal to $[\![T]\!]_{\sigma,\rho}([\sigma|t|]_{c\beta\eta})$. This is defined, since $[\sigma|t|]_{c\beta\eta} \in [\![T']\!]_{\sigma,\rho}$, by the IH for the second premise; note that $[\![T']\!]_{\sigma,\rho}$ is defined since otherwise $[\![\Pi x : T'.\kappa]\!]_{\sigma,\rho}$ would not be defined. The result of applying the function is thus indeed in $[\![[t/x]^{T'}\ \kappa]\!]_{\sigma,\rho}$, since $|\chi\ T'\ \text{-}\ t| = |t|$ (recall the shorthand $[t/x]^{T'} = [\chi\ T'\ \text{-}\ t/x]$), and with Lemma 12 we have that the interpretation equals $[\![\kappa]\!]_{\sigma[x\mapsto\zeta([\sigma|t|]_{c\beta\eta})],\rho}$ (the codomain of the function being applied).

Case:

$$\frac{\Gamma \vdash T_1 \Rightarrow \Pi\, X{:}\kappa_2.\, \kappa_1 \quad \Gamma \vdash T_2 \Rightarrow \kappa_2' \quad \kappa_2 \cong \kappa_2'}{\Gamma \vdash T_1 \cdot T_2 \Rightarrow [T_2/X]\kappa_1}$$

By the IH applied to the first premise, $[\![T_1]\!]_{\sigma,\rho} \in [\![\Pi\, X{:}\kappa_2.\, \kappa_1]\!]_{\sigma,\rho}$. By the semantics of Π-kinds, this means that for any $S \in [\![\kappa_2]\!]_{\sigma,\rho}$, $[\![T_1]\!]_{\sigma,\rho}\ S$ is in $[\![\kappa_1]\!]_{\sigma,\rho[X\mapsto S]}$. By the IH for the second premise, we have $[\![T_2]\!] \in [\![\kappa_2']\!]_{\sigma,\rho}$, and by the IH for the third premise, we have $[\![\kappa_2]\!]_{\sigma,\rho} = [\![\kappa_2']\!]_{\sigma,\rho}$. So we get $[\![T_1]\!]_{\sigma,\rho}([\![T_2]\!]_{\sigma,\rho}) \in [\![\kappa_1]\!]_{\sigma,\rho[X\mapsto[\![T']\!]_{\sigma,\rho}]}$, which suffices by Lemma 13.

Case:

$$\frac{FV(t\ t') \subseteq dom(\Gamma)}{\Gamma \vdash \{t \simeq t'\} : \star}$$

Either $\sigma|t| =_{c\beta\eta} \sigma|t'|$ or not. Either way, the interpretation is defined and in $\mathcal{R}$, since $FV(t\ t') \subseteq dom(\sigma)$ (as an easy consequence of $(\sigma, \rho) \in [\![\Gamma]\!]$).

A.3 Proof of parts (3) and (4)

Case:

$$\frac{(x : T) \in \Gamma}{\Gamma \vdash x \Rightarrow T}$$

This follows from the definition of $[\![\Gamma]\!]$.

Case:

$$\frac{\Gamma \vdash t \Rightarrow T' \quad T' \cong T}{\Gamma \vdash t \Leftarrow T}$$

By the IH applied to the first premise, we have $[\sigma|t|]_{c\beta\eta} \in [\![T']\!]_{\sigma,\rho} \in \mathcal{R}$. By assumption, $[\![T]\!]_{\sigma,\rho} \in \mathcal{R}$, and so by the IH applied to the second premise, we have $[\sigma|t|]_{c\beta\eta} \in [\![T']\!]_{\sigma,\rho} = [\![T]\!]_{\sigma,\rho}$.

Case:

$$\frac{T \rightsquigarrow^*_{\mathbf{n}} \Pi\, x{:}T_1.\, T_2 \quad \Gamma, x : T_1 \vdash t \Leftarrow T_2}{\Gamma \vdash \lambda\, x.\, t \Leftarrow T}$$

To show $[\sigma\lambda x.|t|]_{c\beta\eta} \in [\![\Pi\, x{:}T_1.\, T_2]\!]_{\sigma,\rho}$ (noting that the latter is defined and in $\mathcal{R}$ by assumption), it suffices to assume an arbitrary $E \in [\![T_1]\!]_{\sigma,\rho}$, and show $[[\zeta(E)/x]\sigma|t|]_{c\beta\eta} \in [\![T_2]\!]_{\sigma[x\mapsto\zeta(E)],\rho}$. By the IH, we have $[\sigma[x \mapsto \zeta(E)]|t|]_{c\beta\eta} \in [\![T_2]\!]_{\sigma[x\mapsto\zeta(E)],\rho}$. But $[\sigma[x \mapsto \zeta(E)]t]_{c\beta\eta} = [[\zeta(E)/x]\sigma|t|]_{c\beta\eta}$, so this is sufficient.

Case:

$$\frac{\Gamma \vdash t \overset{\rightsquigarrow^*_{\mathbf{n}}}{\Rightarrow} \Pi\, x{:}T'.\, T \quad \Gamma \vdash t' \Leftarrow T'}{\Gamma \vdash t\ t' \Rightarrow [t'/x]^{T'}T}$$

By the IH applied to the first premise, $[\sigma|t|]_{c\beta\eta} \in [\![\Pi x : T'.T]\!]_{\sigma,\rho} \in \mathcal{R}$. This means that there exists a λ-abstraction $\lambda x.\hat{t}$ such that $\lambda x.\hat{t} =_{c\beta\eta} \sigma|t|$, by the semantics of Π-types. Furthermore, for any $E \in [\![T']\!]_{\sigma,\rho}$, $[[\zeta(E)/x]\hat{t}]_{c\beta\eta} \in [\![T]\!]_{\sigma[x\mapsto\zeta(E)],\rho}$. By the IH applied to the second premise, $[\sigma|t'|]_{c\beta\eta} \in [\![T']\!]_{\sigma,\rho}$, so we can instantiate the quantifier in the previous formula to obtain

$$[[\zeta([\sigma|t'|]_{c\beta\eta})/x]\hat{t}]_{c\beta\eta} \in [\![T]\!]_{\sigma[x\mapsto\zeta([\sigma|t'|]_{c\beta\eta})],\rho}$$

By Lemma 12, this is equivalent to

$$[[\zeta([\sigma|t'|]_{c\beta\eta})/x]\hat{t}]_{c\beta\eta} \in [\![[t'/x]T_2]\!]_{\sigma,\rho}$$

Since $\sigma|t\ t'| =_{c\beta\eta} (\lambda x.\hat{t})\ \sigma|t'| =_{c\beta\eta} [[\zeta([\sigma|t'|]_{c\beta\eta})/x]\hat{t}$, this is sufficient.

Case:

$$\frac{T' \rightsquigarrow^*_{\mathbf{n}} \forall\, X{:}\kappa.\, T \quad \Gamma, X : \kappa \vdash t \Leftarrow T}{\Gamma \vdash \Lambda\, X.\, t \Leftarrow T'}$$

By the IH, $[\sigma|t|]_{c\beta\eta} \in [\![T]\!]_{\sigma,\rho[X\mapsto S]}$, for all $S \in [\![\kappa]\!]_{\sigma,\rho}$. This is sufficient to prove $[\sigma|\Lambda\, X.\, t|]_{c\beta\eta} \in [\![\forall X : \kappa.T]\!]_{\sigma,\rho}$, by the semantics of $\forall$-types and definition of erasure.

Case:

$$\frac{\Gamma \vdash t \overset{\rightsquigarrow^*_{\mathbf{n}}}{\Rightarrow} \forall\, X{:}\kappa.\, T \quad \Gamma \vdash T' \Rightarrow \kappa' \quad \kappa' \cong \kappa}{\Gamma \vdash t \cdot T' \Rightarrow [T'/X]T}$$

By the semantics of $\forall$-types and the IH applied to the first premise, we have $[\sigma|t|]_{c\beta\eta} \in [\![T]\!]_{\sigma,\rho[X\mapsto S]}$, for all $S \in [\![\kappa]\!]_{\sigma,\rho}$. By applying the IH twice, once to the second premise and once to the third, we have, we have $[\![T']\!]_{\sigma,\rho} \in [\![\kappa]\!]_{\sigma,\rho}$. So, can derive $[\sigma|t|]_{c\beta\eta} \in [\![T]\!]_{\sigma,\rho[X\mapsto[\![T']\!]_{\sigma,\rho}]}$. By Lemma 13, this is equivalent to the required $[\sigma|t|]_{c\beta\eta} \in [\![[T'/X]T]\!]_{\sigma,\rho}$, using also the definition of erasure.

Case:

$$\frac{T \rightsquigarrow^*_{\mathbf{n}} \forall\, x{:}T_1.\, T_2 \quad \Gamma, x : T_1 \vdash t \Leftarrow T_2 \quad x \notin FV(|t|)}{\Gamma \vdash \Lambda\, x.\, t \Leftarrow T}$$

By the IH applied to the second premise, we have $[\sigma[x \mapsto \zeta(E)]|t|]_{c\beta\eta} \in [\![T_2]\!]_{\sigma[x\mapsto\zeta(E)],\rho}$, for any $E \in [\![T_1]\!]_{\sigma,\rho}$. This is because $[\![T_1]\!]_{\sigma,\rho} \in \mathcal{R}$, since $[\![\forall\, x{:}T_1.\, T_2]\!]_{\sigma,\rho}$ is in $\mathcal{R}$ and hence defined, by assumption. Since $x \notin FV(|t|)$,

we know $[[\sigma[x \mapsto \zeta(E)]|t|]]_{c\beta\eta} = [\sigma|t|]_{c\beta\eta}$. By the semantics of $\forall$-types and definition of erasure, this suffices to show the desired conclusion.

Case:

$$\frac{\Gamma \vdash t \overset{\rightsquigarrow^*_{\mathbf{n}}}{\Rightarrow} \forall\, x{:}T'.\, T \quad \Gamma \vdash t' \Leftarrow T'}{\Gamma \vdash t\ \text{-}t' \Rightarrow [t'/x]^{T'} T}$$

The result follows easily by the IH applied to the premises, the semantics of $\forall$-types, definition of erasure, and Lemma 12.

Case:

$$\frac{\begin{array}{cc} T \rightsquigarrow^*_{\mathbf{n}} \iota\, x{:}T_1.\, T_1 & \Gamma \vdash t_1 \Leftarrow T_1 \\ \Gamma \vdash t_2 \Leftarrow [t/x]^{T_1}\ T_2 & |t_1| =_{\beta\eta} |t_2| \end{array}}{\Gamma \vdash [t_1, t_2] \Leftarrow T}$$

By the IH, we have $[\sigma|t_1|]_{c\beta\eta} \in [\![T_1]\!]_{\sigma,\rho}$ and $[\sigma|t_2|]_{c\beta\eta} \in [\![[t_1/x]T_2]\!]_{\sigma,\rho}$. By Lemma 12, the latter is equivalent to $[\sigma|t|]_{c\beta\eta} \in [\![T_2]\!]_{\sigma[x\mapsto\zeta([\sigma|t|]_{c\beta\eta}),\rho}$. These two facts about $[\sigma|t|]_{c\beta\eta}$ are sufficient, by the semantics of ι-types, for the desired conclusion, using also the fact (from the fourth premise) that $\sigma|t| =_{c\beta\eta} \sigma|t'|$.

Case:

$$\frac{\Gamma \vdash t \overset{\rightsquigarrow^*_{\mathbf{n}}}{\Rightarrow} \iota\, x{:}T.\, T'}{\Gamma \vdash t.1 \Rightarrow T}$$

The desired conclusion follows easily from the IH and the semantics of ι-types.

Case:

$$\frac{\Gamma \vdash t \overset{\rightsquigarrow^*_{\mathbf{n}}}{\Rightarrow} \iota\, x{:}T.\, T'}{\Gamma \vdash t.2 \Rightarrow [t.1/x]T'}$$

Similar to the previous case, additionally using Lemma 12.

Case:

$$\frac{T \rightsquigarrow^*_{\mathbf{n}} \{t_1 \simeq t_2\} \quad FV(t') \subseteq dom(\Gamma) \quad |t_1| =_{\beta\eta} |t_2|}{\Gamma \vdash \beta\{t'\} \Leftarrow T}$$

By the third premise $|t_1| =_{\beta\eta} |t_2|$ it follows that $\sigma|t_1| =_{\beta\eta} \sigma|t_2|$, and also by the second premise and the fact that $\sigma \in [\![\Gamma]\!]$ it follows that $FV(t_1\ t_2) \subseteq dom(\sigma)$. Also, we see $\sigma|t'|$ is a closed term. So, $[\sigma|t'|]_{c\beta\eta} \in [\![\{t_1 \simeq t_2\}]\!]_{\sigma,\rho}$ follows directly from the semantics of equality types.

Case:

$$\frac{\Gamma \vdash t \Rightarrow T' \quad T' \cong \{\lambda\, x.\, \lambda\, y.\, x \simeq \lambda\, x.\, \lambda\, y.\, y\}}{\Gamma \vdash \delta\ \text{-}\ t \Leftarrow T}$$

By the inductive hypothesis, $[\sigma|t|]_{c\beta\eta} \in [\![T']\!] \in \mathcal{R}$. It is easy to see that the meaning of $\{\lambda\, x.\, \lambda\, y.\, x \simeq \lambda\, x.\, \lambda\, y.\, \}$ exists and is in $\mathcal{R}$, and is in fact the empty set. By mutual induction on the second premise we have $[\sigma|t|]_{c\beta\eta} \in [\![\{\lambda\, x.\, \lambda\, y.\, x \simeq \lambda\, x.\, \lambda\, y.\, \}]\!]_{\sigma,\rho}$, a contradiction.

Case:

$$\frac{\begin{array}{ccc} \Gamma \vdash t \overset{\rightsquigarrow^*_{\mathbf{n}}}{\Rightarrow} \{t_1 \simeq t_2'\} & FV(t_2) \subseteq dom(\Gamma) & |t_2'| =_{\beta\eta} |t_2| \\ \Gamma \vdash [t_2/x]T' \Rightarrow \star & \Gamma \vdash t' \Leftarrow [t_2/x]T' & [t_1/x]T' \cong T \end{array}}{\Gamma \vdash \rho\ t\ @x\langle t_2\rangle.T'\ \text{-}\ t' \Leftarrow T}$$

By the IH applied to the first premise in the first row, $\sigma|t_1| =_{c\beta\eta} \sigma|t_2'|$. With the second and third premise, and from the assumption $\sigma \in [\![\Gamma]\!]$, we have $\sigma|t_2'| =_{c\beta\eta} \sigma|t_2|$ (and $\sigma|t_2|$ is closed), so we obtain $[\sigma|t_1|]_{c\beta\eta} = [\sigma|t_2|]_{c\beta\eta}$. By the IH applied to the first premise of the second row, $[\![[t_2/x]T]\!]_{\sigma,\rho} \in \mathcal{R}$ and so is defined. By the IH applied to the second premise in the second row, $[\sigma|t'|]_{c\beta\eta} \in [\![[t_2/x]T']\!]_{\sigma,\rho}$. By the IH applied to the second premise in the second row, $[\![T]\!]_{\sigma,\rho} = [\![[t_1/x]T']\!]_{\sigma,\rho}$. The result then follows by applying Lemma 12.

Case:

$$\frac{\Gamma \vdash T \Rightarrow \star \quad \Gamma \vdash t \Leftarrow T}{\Gamma \vdash \chi\ T\ \text{-}\ t\ \Rightarrow T}$$

We apply the IH for the first premise to get that $[\![T]\!]_{\sigma,\rho}$ is in $\mathcal{R}$ and hence defined. Using this, we apply the IH on the second premise to get $[\sigma|t|]_{c\beta\eta} \in [\![T]\!]_{\sigma,\rho}$, which by the definition of erasure is what we must show.

Case:

$$\frac{\Gamma \vdash t \Leftarrow \{t' \simeq t''\} \quad \Gamma \vdash t' \Leftrightarrow T \quad FV(t'') \subseteq dom(\Gamma)}{\Gamma \vdash \varphi\ t\ \text{-}\ t'\ \{t''\} \Leftrightarrow T}$$

By the IH for the first premise, $\sigma|t'| =_{c\beta\eta} \sigma|t''|$ (we can see that $FV(t'\ t'') \subseteq \Gamma$, so $[\![\{t' \simeq t''\}]\!]_{\sigma,\rho}$ is defined). By the IH for the second premise, $[\sigma|t'|]_{c\beta\eta} \in [\![T]\!]_{\sigma,\rho}$ (in the case of type synthesis, the IH also tells us $[\![T]\!]_{\sigma,\rho}$ is defined). This suffices for the desired conclusion, using also the definition of erasure ($|\varphi\ t\ \text{-}\ t'\{t''\}| = |t''|$).

Proof of part (5)

We show the cases for the non-congruential rules of Figure 6.

Case:

$$\frac{T_1 \rightsquigarrow_{\mathbf{n}}^* T_1' \not\rightsquigarrow_{\mathbf{n}} \quad T_2 \rightsquigarrow_{\mathbf{n}}^* T_2' \not\rightsquigarrow_{\mathbf{n}} \quad T_1' \cong^{\mathrm{t}} T_2'}{T_1 \cong T_2}$$

By Lemma 14, we have

$$\begin{array}{rcl} [\![T_1]\!]_{\sigma,\rho} & = & [\![T_1']\!]_{\sigma,\rho} \\ [\![T_2]\!]_{\sigma,\rho} & = & [\![T_2']\!]_{\sigma,\rho} \end{array}$$

By the IH for the third premise, we have $[\![T_1']\!]_{\sigma,\rho} = [\![T_2']\!]_{\sigma,\rho}$, which suffices.

Case:

$$\frac{T_1 \cong^{\mathrm{t}} T_1 \quad |t_1| =_{\beta\eta} |t_2|}{T_1\ t_1 \cong^{\mathrm{t}} T_2\ t_2}$$

By the semantics, $[\![T_1\ t_1]\!]_{\sigma,\rho} = [\![T_1]\!]_{\sigma,\rho}([\sigma|t_1|]_{c\beta\eta})$. By the second premise and the IH for the first premise, this equals $[\![T_2]\!]_{\sigma,\rho}([\sigma|t_2|]_{c\beta\eta})$, as required.

Case:

$$\frac{|t_1| =_{\beta\eta} |t_1'| \quad |t_2| =_{\beta\eta} |t_2'|}{\{t_1 \simeq t_2\} \cong^{\mathrm{t}} \{t_1' \simeq t_2'\}}$$

This follows easily from the premises and the semantics of equality types.

Proof of Part (6)

The convertibility relation for kinds consists entirely of congruential rules for quantification over types and kinds.

□

B Proof of Theorem 4

Proof (of Theorem 4). Theorem 1 implies that since $t'\ t$ is closed and of type $\Pi x : T_1.\ T_2$, we have $[|t'\ t|]_{c\beta\eta} \in [\![\Pi x : T_1.\ T_2]\!]_{\cdot,\rho}$, where $[|t'\ t|]_{c\beta\eta}$ is the set of closed terms which are $\beta\eta$-equivalent to $|t'\ t|$; and $(\cdot, \rho) \in [\![\Gamma]\!]$ gives interpretations $\cdot$ for term- and ρ for type-variables in Γ. By the semantics of types defined in Figure 7, the interpretation of a Π-type consists of sets of the form $[\lambda x.\, t']_{c\beta\eta}$. So we have that $|t'\ t|$ is $\beta\eta$-equivalent to $\lambda x.\, t'$ for some x, t'. Since $|t'\ t|$ is β-equivalent to t, we know $t =_{\beta\eta} \lambda x.\, t'$. It is then an easy consequence of the standardization theorem for untyped lambda calculus that $|t|$ is call-by-name normalizing (cf. [7]). □

C Proof of Theorems 6 and 7

First a few lemmas (easy cases omitted):

Lemma 15. *Let κ_1, κ_1' be kinds such that $\kappa_1 \cong \kappa_1'$.*

- *If $\Gamma_1, X : \kappa_1, \Gamma_2 \vdash \kappa_2$ and $\Gamma_1 \vdash \kappa_1'$ then $\Gamma_1, X : \kappa_1', \Gamma_2 \vdash \kappa_2$*
- *If $\Gamma_1, X : \kappa_1, \Gamma_2 \vdash T \Rightarrow \kappa_2$ and $\Gamma_1 \vdash \kappa_1'$ then $\Gamma_1, X : \kappa_1', \Gamma_2 \vdash T \Rightarrow \kappa_2'$ for some $\kappa_2' \cong \kappa_2$*
- *If $T_3 \cong T_4$ and $\Gamma_1, X : \kappa_1, \Gamma_2 \vdash t \Leftarrow T_3$ then $\Gamma_1, X : \kappa_1', \Gamma_2 \vdash t \Leftarrow T_4$*
- *If $\Gamma_1, X : \kappa_1, \Gamma_2 \vdash t \Rightarrow T$ and $\Gamma_1 \vdash \kappa_1'$ then $\Gamma_1, X : \kappa_1', \Gamma_2 \vdash t \Rightarrow T$.*

Furthermore, the resulting typing derivations have depths no larger than the assumed ones.

Proof. By mutual induction on the assumed derivation, and mutually with Lemma 16. The measure, which omits the size of derivations of the convertibility relation, is used to ensure that each mutually inductive call is well-founded. We show the interesting cases.

Case:

$$\frac{(X : \kappa) \in \Gamma_1, X_1 : \kappa_1, \Gamma_2}{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash X \Rightarrow \kappa}$$

We have two subcases to consider. If $X = X_1$, then by the rule we obtain $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash X_1 \Rightarrow \kappa_1'$, as desired. Otherwise, by the rule we obtain $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash X \Rightarrow \kappa$. In both cases, the resulting derivation has the same depth (i.e., 1) as we started with.

Case:

$$\frac{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash T \Rightarrow \star \quad \Gamma_1, X_1 : \kappa_1, \Gamma_2, x : T \vdash T' \Rightarrow \kappa}{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash \lambda\, x{:}T.\, T' \Rightarrow \Pi\, x{:}T.\, \kappa}$$

By the IH on the first premise, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash T \Rightarrow \star$ at no greater depth (note $\star$ is convertible only with itself). By the IH on the second premise, $\Gamma_1, X_1 : \kappa_1', \Gamma_2, x : T \vdash T' \Rightarrow \kappa'$ (at no greater depth) for some $\kappa' \cong \kappa$. By the rule, we have $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash \lambda\, x{:}T.\, T' \Rightarrow \Pi\, x{:}T.\, \kappa'$, which is congruent with the original type in the conclusion. We see that the measure is preserved.

Case:

$$\frac{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash \kappa \quad \Gamma_1, X_1 : \kappa_1, \Gamma_2, X : \kappa \vdash T' \Rightarrow \kappa'}{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash \lambda\, X{:}\kappa.\, T' \Rightarrow \Pi\, X{:}\kappa.\, \kappa'}$$

By the IH on the first premise, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash \kappa$. By the IH on the second premise, $\Gamma_1, X_1 : \kappa_1', \Gamma_2, X : \kappa \vdash T' \Rightarrow \kappa''$ for some $\kappa'' \cong \kappa'$. By the rule, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash \lambda\, X{:}\kappa.\, T' \Rightarrow \Pi\, X{:}\kappa.\, \kappa''$, which is convertible with the original kind synthesized for this type. Since the depths of the premises for the resulting derivation are the same as the depths for the premises of the assumed one, the measure is preserved.

Case:

$$\frac{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash T \Rightarrow \Pi\, x{:}T'.\, \kappa \quad \Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash t \Leftarrow T'}{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash T\ t \Rightarrow [t/x]^{T'}\kappa}$$

By the IH on the first premise, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash T \Rightarrow \Pi\, x{:}T''.\, \kappa''$ for some $T'' \cong T'$ and $\kappa'' \cong \kappa$. By the IH on the second premise, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash t \Leftarrow T''$. By the rule, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash T\ t \Rightarrow [t/x]^{T''}\kappa''$, convertible with the given type $[t/x]^{T'}\kappa$. We see that the measure is preserved.

Case:

$$\frac{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash T \Rightarrow \Pi\, X{:}\kappa'.\, \kappa \quad \Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash T' \Rightarrow \kappa'' \quad \kappa' \cong \kappa''}{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash T \cdot T' \Rightarrow [T'/X]\kappa}$$

By the IH on the first premise, $\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash T \Rightarrow \Pi\, X{:}\kappa_2'.\, \kappa_2$ for some $\kappa_2' \cong \kappa'$, $\kappa_2 \cong \kappa$. By the IH on the second premise, $\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash T' \Rightarrow \kappa_2''$ for some $\kappa_2'' \cong \kappa''$. By transitivity and the third premise, $\kappa_2' \cong \kappa_2''$. By the rule, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash T \cdot T' \Rightarrow [T'/X]\kappa_2$, with this kind convertible to $[T'/X]\kappa$ by congruence. We see the measure is preserved.

Case:

$$\frac{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash t \Rightarrow T' \quad T' \cong T_3}{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash t \Leftarrow T_3}$$

By the IH on the first premise, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash t \Rightarrow T'$. By assumption and transitivity of congruence, $T' \cong T_4$ (where T_4 is the type given to us in the proof). By the rule, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash t \Leftarrow T_4$, and we see the measure is preserved.

Case:

$$\frac{T_3 \rightsquigarrow_{\mathbf{n}}^* \Pi\, x{:}T_1.\, T_2 \quad \Gamma_1, X_1 : \kappa_1, \Gamma_2, x : T_1 \vdash t \Leftarrow T_2}{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash \lambda\, x.\, t \Leftarrow T_3}$$

By the first premise, $T_3 \cong \Pi\, x{:}T_1.\, T_2$. By assumption and transitivity of the convertibility relation, $T_4 \cong \Pi\, x{:}T_1.\, T_2$. This means $T_4 \rightsquigarrow_{\mathbf{n}}^* \Pi\, x{:}T_1'.\, T_2'$ for some $T_1' \cong T_1$ and $T_2' \cong T_2$. By mutual induction with Lemma 16 on the second premise, we have a derivation of $\Gamma_1, X_1 : \kappa_1, \Gamma_2, x : T_1' \vdash t \Leftarrow T_2'$ that is no deeper than that premise. So, we are entitled to use the IH on this new derivation to obtain $\Gamma_1, X_1 : \kappa_1', \Gamma_2, x : T_1' \vdash t \Leftarrow T_2'$, which is also no deeper. By the rule, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash \lambda\, x.\, t \Leftarrow T_4$, and the measure is preserved.

Case:

$$\frac{T_3 \rightsquigarrow_{\mathbf{n}}^* \forall\, X{:}\kappa.\, T \quad \Gamma_1, X_1 : \kappa_1, \Gamma_2, X : \kappa \vdash t \Leftarrow T}{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash \Lambda\, X.\, t \Leftarrow T_3}$$

By the first premise, $T_3 \cong \forall\, X{:}\kappa.\, T$, so by assumption and transitivity of convertibility, $T_4 \cong \forall\, X{:}\kappa.\, T$. This means $T_4 \rightsquigarrow_{\mathbf{n}}^* \forall\, X{:}\kappa'.\, T'$ for some $\kappa' \cong \kappa$ and $T' \cong T$. We apply the IH once on the second premise to obtain a derivation of $\Gamma_1, X_1 : \kappa_1, \Gamma_2, X : \kappa' \vdash t \Leftarrow T'$, and then again to obtain $\Gamma_1, X_1 : \kappa_1', \Gamma_2, X : \kappa' \vdash t \Leftarrow T'$, noting this derivation's depth is no greater than the second premise. By the rule, $\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash \Lambda\, X.\, t \Leftarrow T_4$, and the measure is preserved.

Case:

$$\frac{T_3 \rightsquigarrow_{\mathbf{n}}^* \{t_1 \simeq t_2\} \quad FV(t') \subseteq dom(\Gamma_1, X_1 : \kappa_1, \Gamma_2) \quad |t_1| =_{\beta\eta} |t_2|}{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash \beta\{t'\} \Leftarrow T_3}$$

From the first premise, assumption, and transitivity of convertibility, $T_4 \cong \{t_1 \simeq t_2\}$. This means that $T_4 \rightsquigarrow_{\mathbf{n}}^* \{t_3 \simeq t_4\}$ for some t_3, t_4 such that $|t_3| =_{\beta\eta} |t_1|$ and $|t_4| =_{\beta\eta} |t_2|$. From this, the third premise, and transitivity of convertibility, we obtain $|t_3| =_{\beta\eta} |t_4|$. We also see from the second premise that $FV(t') \subseteq dom(\Gamma_1, X_1 : \kappa_1', \Gamma_2)$. So, we use the rule to conclude that $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash \beta\{t'\} \Leftarrow T_4$, and the depth (1) is preserved.

Case:

$$\frac{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash t \overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow} \{t_1 \simeq t_2'\} \quad FV(t_2) \subseteq dom(\Gamma_1, X_1 : \kappa_1, \Gamma_2) \quad |t_2'| =_{\beta\eta} |t_2| \\ \Gamma_1, X_1 : \kappa_2, \Gamma_2 \vdash [t_2/x]T' \Rightarrow \star \quad \Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash t' \Leftarrow [t_2/x]T' \quad [t_1/x]T' \cong T}{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash \rho\ t\ @x\langle t_2\rangle.T' \text{ - } t' \Leftarrow T}$$

By the IH on the first premise, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash t' \overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow} \{t_1 \simeq t_2'\}$. By the IH on the first premise of the second row, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash [t_2/x]\ T \Rightarrow \star$ (as $\star$ is only convertible with itself). By the IH the second premise of the second row, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash t \Leftarrow [t_2/x]T'$. By assumption, the third premise of the second row, and transitivity of convertibility, we have $[t_1/x]T' \cong T_4$ (T_4 is the type we must check the entire expression against). We use the rule to conclude ($dom(\Gamma_1, X_1 : \kappa_1, \Gamma_2) = dom(\Gamma_1, X_1 : \kappa_1', \Gamma_2)$), noting that the measure is preserved.

Case:

$$\frac{T_3 \rightsquigarrow_{\mathbf{n}}^* \iota\, x{:}T_1.T_1 \qquad \Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash t_1 \Leftarrow T_1 \\ \Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash t_2 \Leftarrow [t/x]^{T_1}\ T_2 \qquad |t_1| =_{\beta\eta} |t_2|}{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash [t_1, t_2] \Leftarrow T_3}$$

From the first premise, assumption, and transitivity of the convertibility relation, $T_4 \cong \iota\, x : T_1.T_2$. This means that $T_4 \rightsquigarrow_{\mathbf{n}}^* \iota\, x{:}T_1'.T_2'$ for some $T_1' \cong T_1$ and $T_2' \cong T_2$. From this last congruence, we have $[t_1/x]^{T_1'}T_2' \cong [t_1/x]^{T_1}T_2$. By the IH on the second premise, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash t_1 \Leftarrow T_1'$. By the IH on the first premise, second row, we have $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash t_2 \Leftarrow [t/x]T_2'$. We use the rule to conclude, noting that the measure is preserved.

Case:

$$\frac{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash t \overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow} \Pi\, x{:}T'.T \quad \Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash t' \Leftarrow T'}{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash t\ t' \Rightarrow [t'/x]^{T'}T}$$

By the IH on the first premise, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash t \overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow} \Pi\, x : T'.T$. By the IH on the second premise, $\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash t' \Leftarrow T'$. By the rule, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash t\ t' \Rightarrow [t'/x]T$, and the measure is preserved.

Case:

$$\frac{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash t \overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow} \forall\, X{:}\kappa.T \quad \Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash T' \Rightarrow \kappa' \quad \kappa' \cong \kappa}{\Gamma_1, X_1 : \kappa_1, \Gamma_2 \vdash t \cdot T' \Rightarrow [T'/X]T}$$

By the IH on the first premise, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash t \overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow} \forall\, X{:}\kappa.T$. By the IH on the second premise, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash T' \Rightarrow \kappa''$ for some $\kappa'' \cong \kappa'$, from which we obtain $\kappa'' \cong \kappa$. By the rule, $\Gamma_1, X_1 : \kappa_1', \Gamma_2 \vdash t \cdot T' \Rightarrow [T'/X]T$, and the measure is preserved. □

Lemma 16. *Let T_1, T_2 be types such that $T_1 \cong T_2$.*

- *If $\Gamma_1, x : T_1, \Gamma_2 \vdash \kappa$ then $\Gamma_1, x : T_2, \Gamma_2 \vdash \kappa$*
- *If $\Gamma_1, x : T_1, \Gamma_2 \vdash T \Rightarrow \kappa_1$ then $\Gamma_1, x : T_2, \Gamma_2 \vdash T \Rightarrow \kappa_1$*
- *If $T_3 \cong T_4$ and $\Gamma_1, x : T_1, \Gamma_2 \vdash t \Leftarrow T_3$ then $\Gamma_1, x : T_2, \Gamma_2 \vdash t \Leftarrow T_4$*
- *If $\Gamma_1, x : T_1, \Gamma_2 \vdash t \Rightarrow T$ then $\Gamma_1, x : T_2, \Gamma_2 \vdash t \Rightarrow T'$ for some $T' \cong T$.*

Furthermore, the resulting typing derivations have depths no larger than the assumed ones.

Proof. By mutual induction on the assumed derivation (specifically, its depth), and mutually with Lemma 15. The measure, which omits the size of derivations of the convertibility relation, is used to ensure that each mutually inductive call is well-founded. We show the interesting cases.

Case:

$$\frac{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash T \Rightarrow \star \quad \Gamma_1, x_1 : T_1, \Gamma_2, x : T \vdash T' \Rightarrow \kappa}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash \lambda\, x{:}T.\, T' \Rightarrow \Pi\, x{:}T.\, \kappa}$$

By the IH on the first premise, $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash T \Rightarrow \star$. By the IH on the second premise, $\Gamma_1, x_1 : T_2, \Gamma_2, x : T \vdash T' \Rightarrow \kappa$. We also have that the depths of the resulting typing derivations are no greater than the those used to derive the premises, so we conclude using the rule.

Case:

$$\frac{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash \kappa \quad \Gamma_1, x_1 : T_1, \Gamma_2, X : \kappa \vdash T' \Rightarrow \kappa'}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash \lambda\, X{:}\kappa.\, T' \Rightarrow \Pi\, X{:}\kappa.\, \kappa'}$$

By the IH on the first premise, $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash T \Rightarrow \kappa$. By the IH on the second premise, $\Gamma_1, x_1 : T_2, \Gamma_2, X : \kappa \vdash T' \Rightarrow \kappa'$. We also have that the depths of the resulting derivations are no greater than the those used to derive the premises, so we conclude using the rule.

Case:

$$\frac{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash T \Rightarrow \Pi\, x{:}T'.\, \kappa \quad \Gamma_1, x_1 : T_1, \Gamma_2 \vdash t \Leftarrow T'}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash T\ t \Rightarrow [t/x]^{T'}\kappa}$$

By the IH on the first premise, $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash T \Rightarrow \Pi\, x{:}T'.\, \kappa$. By the IH on the second premise, $\Gamma_2, x_1 : T_2, \Gamma_2 \vdash t \Leftarrow T'$. We also have that the depths of the resulting derivations are no greater than the those used to derive the premises, so we conclude using the rule.

Case:

$$\frac{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash T \Rightarrow \Pi\, X{:}\kappa'.\, \kappa \quad \Gamma_1, x_1 : T_1, \Gamma_2 \vdash T_2 \Rightarrow \kappa'' \quad \kappa'' \cong \kappa'}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash T \cdot T' \Rightarrow [T'/X]\kappa}$$

By the IH on the first premise, $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash T \Rightarrow \Pi\, X : \kappa'.\, \kappa$. By the IH on the second premise, $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash T_2 \Rightarrow \kappa''$. We also have that the depths of the resulting derivations are no greater than the those used to derive the premises, so we conclude using the rule, keeping the third premise.

Case:

$$\frac{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash t \Rightarrow T' \quad T' \cong T}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash t \Leftarrow T}$$

By the IH on the first premise, $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash t \Rightarrow T''$ for some $T'' \cong T'$. By transitivity of convertibility and the second premise, $T'' \cong T$. By transitivity again, $T'' \cong T_4$ (where $T_4 \cong T$ is given to us). We also have that the depths of the resulting derivations are no greater than the those used to derive the premises, so we conclude using the rule.

Case:

$$\frac{T \rightsquigarrow^*_{\mathbf{n}} \Pi\, x{:}T_5.\, T_6 \quad \Gamma_1, x_1 : T_1, \Gamma_2, x : T_5 \vdash t \Leftarrow T_6}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash \lambda\, x.\, t \Leftarrow T}$$

From the first premise, we have $T \cong \Pi\, x{:}T_5.\, T_6$, so by transitivity of convertibility and assumption, $T_4 \cong \Pi\, x{:}T_5.\, T_6$. This means that $T_4 \rightsquigarrow^*_{\mathbf{n}} \Pi\, x{:}T'_5.\, T'_6$ for some $T'_5 \cong T_5$ and $T'_6 \cong T_6$. By one use of the IH on the first premise, we have $\Gamma_1, x_1 : T_2, \Gamma_2, x : T_5 \vdash t \Leftarrow T'_6$. By another use, we have $\Gamma_1, x_1 : T_2, \Gamma_2, x : T'_5 \vdash t \Leftarrow T'_6$ (this is well-founded, because the depth of the typing derivation this second use is applied to is no greater that the depth of the premise). We also have that the depths of the resulting derivations are no greater than the those used to derive the premises, so we conclude using the rule.

Case:

$$\frac{T' \rightsquigarrow^*_{\mathbf{n}} \forall\, X{:}\kappa.\, T \quad \Gamma_1, x_1 : T_1, \Gamma_2, X : \kappa \vdash t \Leftarrow T}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash \Lambda\, X.\, t \Leftarrow T'}$$

From the first premise, $T' \cong \forall\, X{:}\kappa.\, T$. From transitivity of convertibility and assumption, $T_4 \cong \forall\, X{:}\kappa.\, T$. This means that $T_4 \rightsquigarrow^*_{\mathbf{n}} \forall\, X{:}\kappa''.\, T''$ for some $\kappa'' \cong \kappa$ and $T'' \cong T$. By mutual induction with Lemma 15 on the second premise, $\Gamma_1, x_1 : T_1, \Gamma_2, X : \kappa'' \vdash t \Leftarrow T$, and this derivation is no deeper than the second premise. By the IH, $\Gamma_1, x_1 : T_1, \Gamma_2, X : \kappa'' \vdash t \Leftarrow T''$, and this derivation is no deeper than the second premise. We conclude using the rule, with the measure preserved.

Case:

$$\frac{\begin{array}{cc} T_3 \rightsquigarrow^*_{\mathbf{n}} \iota\, x{:}T.\, T' & \Gamma_1, x_1 : T_1, \Gamma_2 \vdash t \Leftarrow T \\ \Gamma_1, x_1 : T_1, \Gamma_2 \vdash t' \Leftarrow [t/x]^T\ T' & |t| =_{\beta\eta} |t| \end{array}}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash [t, t'] \Leftarrow T_3}$$

From the first premise, $T_3 \cong \iota\, x{:}T.\, T'$. From transitivity of convertibility and assumption, $T_4 \cong \iota\, x{:}T.\, T'$. This means $T_4 \rightsquigarrow^*_{\mathbf{n}} \iota\, x{:}T''.\, T'''$ for some $T'' \cong T$ and $T''' \cong T'$. By the IH, $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash t \Leftarrow T''$ with depth no greater than the second premise (read left to right, then top to bottom). By the IH, $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash t' \Leftarrow T'''$ with depth no greater than the third premise. We conclude using the rule, keeping the fourth premise as-is and noting the measure is preserved.

Case:

$$\frac{T_3 \rightsquigarrow^*_{\mathbf{n}} \{t_1 \simeq t_2\} \quad FV(t') \subseteq dom(\Gamma_1, x_1 : T_1, \Gamma_2) \quad |t_1| =_{\beta\eta} |t_2|}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash \beta\{t'\} \Leftarrow T_3}$$

From the first premise, $T_3 \cong \{t_1 \simeq t_2\}$. From transitivity of the convertibility relation and assumption, $T_3 \cong \{t_1 \simeq t_2\}$. This means $T_4 \rightsquigarrow^*_{\mathbf{n}} \{t_3 \simeq t_4\}$ for some t_3, t_4 such that $|t_3| =_{\beta\eta} |t_1|$ and $|t_4| =_{\beta\eta} |t_2|$. From the third premise and transitivity of convertibility, we have $|t_3| =_{\beta\eta} |t_4|$. From the second premise, we obtain that $FV(t') \subseteq dom(\Gamma_1, x_1 : T_2, \Gamma_2)$. We conclude using the rule, noting that the depth remains 1.

Case:

$$\frac{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash t \Leftarrow \{t' \simeq t''\} \quad \Gamma_1, x_1 : T_1, \Gamma_2 \vdash t' \Leftrightarrow T_3 \quad FV(t'') \subseteq dom(\Gamma_1, x_1 : T_1, \Gamma_2)}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash \varphi\ t \text{ - } t'\ \{t''\} \Leftrightarrow T_3}$$

By the IH on the first premise (first row), $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash t \Leftarrow \{t' \simeq t''\}$ (with no greater depth). If this is type synthesis, then by the second premise $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash t' \Rightarrow T_4$ for some $T_4 \cong T_3$. If this is type checking, by the second premise $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash t' \Leftarrow T_4$ since T_4 (given to us in this case) is convertible with T_3. Either way, we use the rule to conclude (note $dom(\Gamma_1, x_1 : T_1, \Gamma_2) = dom(\Gamma_1, x_1 : T_2, \Gamma_2)$), and the measure is preserved.

Case:

$$\frac{\begin{array}{ccc} \Gamma_1, x_1 : T_1, \Gamma_2 \vdash t \overset{\rightsquigarrow^*_{\mathbf{n}}}{\Rightarrow} \{t_1 \simeq t_2'\} & FV(t_2) \subseteq dom(\Gamma_1, x_1 : T_1, \Gamma_2) & |t_2'| =_{\beta\eta} |t_2| \\ \Gamma_1, x_1 : T_1, \Gamma_2 \vdash [t_2/x]T' \Rightarrow \star & \Gamma_1, x_1 : T_1, \Gamma_2 \vdash t' \Leftarrow [t_2/x]T' & [t_1/x]T' \cong T \end{array}}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash \rho\ t\ @x\langle t_2\rangle.T' \text{ - } t' \Leftarrow T}$$

By the IH on the first premise, $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash t \Rightarrow T''$ (with no greater depth) for some $T'' \cong \{t_1 \simeq t_2'\}$. That means $T'' \rightsquigarrow^*_{\mathbf{n}} \{t_3 \simeq t_4\}$ for some t_3, t_4 such that $|t_3| =_{\beta\eta} |t_1|$ and $|t_4| =_{\beta\eta} |t_2'|$. So we further obtain that $|t_4| =_{\beta\eta} |t_2|$. By the IH on the first premise of the second row, $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash [t_2/x]T \Rightarrow \star$. By the IH on the second premise of the second row, $\Gamma, x_1 : T_2, \Gamma_2 \vdash t \Leftarrow [t_2/x]T'$. By assumption, the third premise of the second row, and transitivity of convertibility, we have $[t_1/x]T' \cong T_4$. We conclude with the rule, preserving the measure.

Case:

$$\frac{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash t \Rightarrow T' \quad T' \cong \{\lambda\, x.\, \lambda\, y.\, x \simeq \lambda\, x.\, \lambda\, y.\, y\}}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash \delta\ \text{-}\ t \Leftarrow T_3}$$

By the IH on the first premise, $\Gamma_1, x : T_2, \Gamma_2 \vdash t \Rightarrow T''$ for some $T'' \cong T'$. By transitivity of convertibility and the second premise, $T'' \cong \{\lambda\, x.\, \lambda\, y.\, x \simeq \lambda\, x.\, \lambda\, y.\, y\}$. Using the δ rule, we conclude that $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash \delta\ \text{-}\ t \Leftarrow T_4$.

Case:

$$\frac{(x : T) \in \Gamma_1, x_1 : T_1, \Gamma_2}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash x \Rightarrow T}$$

We have two subcases to consider. If $x = x_1$, then we use the rule to produce a derivation of $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash x \Rightarrow T_2$, where by assumption $T_1 \cong T_2$. Otherwise, we use the rule to produce a derivation of $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash x \Rightarrow T$. In both cases, the measure (depth of 1) is preserved.

Case:

$$\frac{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash t \overset{\sim^*_{\mathbf{n}}}{\Rightarrow} \Pi\, x{:}T'.\, T \quad \Gamma_1, x_1 : T_1, \Gamma_2 \vdash t' \Leftarrow T'}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash t\ t' \Rightarrow [t'/x]^{T'} T}$$

By the IH on the premise, $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash t \Rightarrow T_3$ for some $T_3 \cong \Pi\, x : T'.\, T$, and the depth of this typing derivation is no greater than that of the first premise. From this we obtain that $T_3 \rightsquigarrow^*_{\mathbf{n}} \Pi\, x : T'_4.\, T_4$ for some $T'_4 \cong T'$ and $T_4 \cong T$. By the IH on the last premise, $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash t' \Leftarrow T'_4$, and the depth of this derivation is no greater than that of the last premise. We conclude with the rule to obtain $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash t\ t' \Rightarrow [t'/x]^{T'_4}\ T_4$, with the measure preserved ($[t'/x]^{T'_4}\ T_4$ is convertible with $[t'/x]^{T'}\ T$, since $|\chi\ T'_4\ \text{-}\ t'| =_{\beta\eta} |\chi\ T'\ \text{-}\ t'|$ by erasure and $T \cong T_4$).

Case:

$$\frac{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash t \overset{\sim^*_{\mathbf{n}}}{\Rightarrow} \forall\, X{:}\kappa.\, T \quad \Gamma_1, x_1 : T_1, \Gamma_2 \vdash T' \Rightarrow \kappa' \quad \kappa' \cong \kappa}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash t \cdot T' \Rightarrow [T'/X]T}$$

By the IH on the first premise, $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash t \Rightarrow T_3$ for some $T_3 \cong \forall\, X{:}\kappa.\, T$, with no greater depth. This means $T_3 \rightsquigarrow^*_{\mathbf{n}} \forall\, X : \kappa''.\, T''$ for some $\kappa'' \cong \kappa$ and $T'' \cong T$. By the IH on the second premise, $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash T' \Rightarrow \kappa'$, with no greater depth. By transitivity of convertibility, $\kappa' \cong \kappa''$. We use the rule to conclude $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash t \cdot T' \Rightarrow [T'/X]T''$, with the measure preserved and the synthesized type in the conclusion convertible with $[T'/X]T$ (since $T'' \cong T$).

Case:

$$\frac{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash T \Rightarrow \star \quad \Gamma_1, x_1 : T_1, \Gamma_2 \vdash t \Leftarrow T}{\Gamma_1, x_1 : T_1, \Gamma_2 \vdash \chi\ T\ \text{-}\ t\ \Rightarrow T}$$

By the IH on the first premise, $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash T \Rightarrow \star$ with no greater depth. By the IH on the second premise $\Gamma_1, x_1 : T_2, \Gamma_2 \vdash t \Leftarrow T$ at no greater depth. We conclude using the rule, with the measure preserved. □

Corollary 17. *If* $\vdash \Gamma_1, X : \kappa_1, \Gamma_2$ *and* $\Gamma_1 \vdash \kappa'_1$ *with* $\kappa'_1 \cong \kappa_1$ *then* $\vdash \Gamma_1, X : \kappa'_1, \Gamma_2$.

Corollary 18. *If* $\vdash \Gamma_1, x_1 : T_1, \Gamma_2$ *and* $\Gamma_1 \vdash T_2 \Rightarrow \star$ *with* $T_1 \cong T_2$ *then* $\vdash \Gamma_1, x_1 : T_2, \Gamma_2$.

Lemma 19. *Below, each statement separately universally quantifies over meta-variables, and it is assumed that typing contexts occurring in assumed derivations are well-formed.*

1. ***Kinds:***
   - *If* $\Gamma_1, x : T, \Gamma_2 \vdash \kappa$ *and* $\Gamma_1 \vdash t \Rightarrow T$ *then* $\Gamma_1, [t/x]\Gamma_2 \vdash [t/x]\kappa$

- *If* $\Gamma_1, X : \kappa', \Gamma_2 \vdash \kappa$ *and* $\Gamma_1 \vdash T \Rightarrow \kappa'$ *then* $\Gamma_1, [T/X]\Gamma_2 \vdash [T/X]\kappa$

2. ***Types***
   - *If* $\Gamma_1, x : T', \Gamma_2 \vdash T \Rightarrow \kappa$ *and* $\Gamma_1 \vdash t \Rightarrow T'$ *then* $\Gamma_1, [t/x]\Gamma_2 \vdash [t/x]T \Rightarrow [t/x]\kappa$
   - *If* $\Gamma_1, X : \kappa_2, \Gamma_2 \vdash T_1 \Rightarrow \kappa_1$ *and* $\Gamma_1 \vdash T_2 \Rightarrow \kappa_2$ *then* $\Gamma_1, [T_2/X]\Gamma_2 \vdash [T_2/X]T_1 \Rightarrow [T_2/X]\kappa_1$
3. ***Terms:***
   - *If* $\Gamma_1, x : T', \Gamma_2 \vdash t \Leftrightarrow T$ *and* $\Gamma_1 \vdash t' \Rightarrow T'$ *then* $\Gamma_1, [t'/x]\Gamma_2 \vdash [t'/x]t \Leftrightarrow [t'/x]T$
   - *If* $\Gamma_1, X : \kappa, \Gamma_2 \vdash t \Leftrightarrow T'$ *and* $\Gamma_1 \vdash T \Rightarrow \kappa$ *then* $\Gamma_1, [T/X]\Gamma_2 \vdash [T/X]t \Leftrightarrow [T/X]T'$

Proof. By mutual induction on the assumed derivations. We only show a few interesting cases, and we omit type annotations on substitutions when these are clear from context.

Case:

$$\frac{(X_1 : \kappa_1) \in \Gamma_1, X : \kappa, \Gamma_2}{\Gamma_1, X : \kappa, \Gamma_2 \vdash X_1 \Rightarrow \kappa_1}$$

We have two cases. If $X_1 = X$, then $\kappa_1 = \kappa$ and by assumption $\Gamma_1 \vdash T \Rightarrow \kappa$, and the desired result holds by weakening. Otherwise, either $(X_1 : \kappa_1) \in \Gamma_1$ and $X \notin FV(\kappa_1)$ (which we obtain from the assumption that the typing context is well-formed), or else $(X_1 : \kappa_1) \in \Gamma_2$. Either way, we have $\Gamma_1, [T/X]\Gamma_2 \vdash X_1 \Rightarrow [T/X]\kappa_1$.

Case:

$$\frac{\Gamma_1, x : T, \Gamma_2 \vdash T_2 \Rightarrow \Pi\, x_1 : T_1.\, \kappa \quad \Gamma_1, x : T, \Gamma_2 \vdash t_1 \Leftarrow T_1}{\Gamma_1, x : T, \Gamma_2 \vdash T_2\ t_1 \Rightarrow [t_1/x_1]^{T_1}\kappa}$$

By the IH, $\Gamma_1, [t/x]\Gamma_2 \vdash [t/x]T_2 \Rightarrow \Pi\, x_1 : [t/x]T_1.\, [t/x]\kappa$ and $\Gamma_1, [t/x]\Gamma_2 \vdash [t/x]t_1 \Leftarrow [t/x]T_1$. By the rule, we have $\Gamma_1, [t/x]\Gamma_2 \vdash [t/x]T_2\ [t/x]t_1 \Rightarrow [[t/x]t_1/x_1][t/x]\kappa$, where the synthesized kind is equal to the desired $[t/x][t_1/x_1]\kappa$.

Case:

$$\frac{FV(t_1\ t_2) \subseteq dom(\Gamma_1, x : T, \Gamma_2)}{\Gamma_1, x : T, \Gamma_2 \vdash \{t_1 \simeq t_2\} : \star}$$

It suffices to show that $FV([t/x]t_1\ [t/x]t_2) \subseteq dom(\Gamma_1, [t/x]\Gamma_2)$. It is clear x is not a free variable of this expression, that the free variables of t are declared in Γ_1, and by assumption the other free variables of it are declared in $\Gamma_1, [t/x]\Gamma_2$.

Case:

$$\frac{(x_1 : T_1) \in \Gamma_1, x : T, \Gamma_2}{\Gamma_1, x : T, \Gamma_2 \vdash x_1 \Rightarrow T_1}$$

We elaborate on the case where $x_1 = x$. It is important that we assumed that $\Gamma_1 \vdash t \Rightarrow T$ (as opposed to having its type checked), as we may now replace the given rule with this assumed derivation without changing the definition of substitution.

Case:

$$\frac{FV(t') \subseteq dom(\Gamma_1, x : T, \Gamma_2) \quad |t_1| =_{\beta\eta} |t_2|}{\Gamma_1, x : T, \Gamma_2 \vdash \beta\{t'\} \Leftarrow \{t_1 \simeq t_2\}}$$

From our assumptions we may conclude $FV([t/x]t') \subseteq dom(\Gamma_1, [t/x]\Gamma_2)$, and from the second premise that $|[t/x]t_1| =_{\beta\eta} |[t/x]t_2|$. Thus, $\Gamma_1, [t/x]\Gamma_2 \vdash \beta\{[t/x]t'\} \Leftarrow \{[t/x]t_1 \simeq [t/x]t_2\}$.

Case:

$$\frac{\Gamma_1, x:T, \Gamma_2 \vdash t'' \overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow} \{t_1 \simeq t_2'\} \quad FV(t_2) \subseteq dom(\Gamma_1, x:T, \Gamma_2) \quad |t_2'| =_{\beta\eta} |t_2| \quad \Gamma_1, x:T, \Gamma_2 \vdash [t_2/x_1]T_2 \Rightarrow \star \quad \Gamma_1, x:T, \Gamma_2 \vdash t' \Leftarrow [t_2/x_1]T_2 \quad [t_1/x_1]T_2 \cong T_1}{\Gamma_1, x:T, \Gamma_2 \vdash \rho\ t''\ @x_1\langle t_2\rangle.T_2 \text{ - } t' \Leftarrow T_1}$$

From the IH, we have that $\Gamma_1, [t/x]\Gamma_2 \vdash [t/x]t'' \Rightarrow \{[t/x]t_1 \simeq [t/x]t_2'\}$, that $\Gamma_1, [t/x]\Gamma_2 \vdash [t/x][t_2/x_1]T_2 \Rightarrow \star$, and that $\Gamma_1, [t/x]\Gamma_2 \vdash [t/x]t' \Leftarrow [t/x][t_2/x_1]T_2$. From the last premise, we may conclude that $[t/x]T_1 \cong [t/x][t_1/x_1]T_1$. We also see from the premises that $FV([t/x]t_2) \subseteq dom(\Gamma_1, [t/x]\Gamma_2)$ and that $|[t/x]t_2'| =_{\beta\eta} |[t/x]t_2|$. Applying the rule and permuting substitutions gives us the desired result (note for example that $[t/x][t_2/x_1]T_1 = [[t/x]t_2/x_1][t/x]T_1$).

Case:

$$\frac{\Gamma_1, x:T, \Gamma_2 \vdash t \Rightarrow T_2' \quad T_2' \cong \{\lambda\, x.\, \lambda\, y.\, x \simeq \lambda\, x.\, \lambda\, y.\, y\}}{\Gamma_1, x:T, \Gamma_2 \vdash \delta \text{ - } t \Leftarrow T_2}$$

From the IH, we have that $\Gamma_1[t'/x]\Gamma_2 \vdash [t'/x]t \Rightarrow [t'/x]T_2'$. From the second premise, we have $[t'/x]T_2' \cong \{\lambda\, x.\, \lambda\, y.\, x \simeq \lambda\, x.\, \lambda\, y.\, y\}$. From the δ rule, we conclude that $\Gamma_1, [t'/x]\Gamma_2 \vdash \delta \text{ - } [t'/x]t \Leftarrow [t'/x]T_2$. □

Corollary 20.

- *If* $\vdash \Gamma_1, x:T, \Gamma_2$ *and* $\Gamma_1 \vdash t \Rightarrow T$ *then* $\vdash \Gamma_1, [t/x]\Gamma_2$
- *If* $\vdash \Gamma_1, X:\kappa, \Gamma_2$ *and* $\Gamma_1 \vdash T \Rightarrow \kappa$ *then* $\vdash \Gamma_1, [T/X]\Gamma_2$.

Proof. By induction on the assumed derivation, appealing to Lemma 19 at each step. □

C.1 Theorem 6

Proof (of Theorem 6). We may rule out the cases where T is a variable or formed by a type constructor, as this would contradict the assumption that $T \rightsquigarrow_{\mathbf{n}} T'$ for some T'. We omit type annotations from substitutions when they are clear from the context.

Case:

$$\frac{\Gamma \vdash T \Rightarrow \Pi\, x{:}T_1.\, \kappa_1 \quad \Gamma \vdash t \Leftarrow T_1}{\Gamma \vdash T\ t \Rightarrow [t/x]^{T_1}\kappa_1}$$

There are two subcases to consider for the derivation of $T\ t \rightsquigarrow_{\mathbf{n}} T'$. In the first case, we have $T \rightsquigarrow_{\mathbf{n}} T''$ for some T'' (so $T' = T''\ t$). By the IH, we have $\Gamma \vdash T'' \Rightarrow \Pi\, x{:}T_1'.\, \kappa_1'$ for some $T_1' \cong T_1$ and $\kappa_1' \cong \kappa_1$ (we have from that IH that kind of T'' must be convertible with $\Pi\, x{:}T_1.\, \kappa_1$). By Lemma 16, $\Gamma \vdash t \Leftarrow T_1'$. By the rule, $\Gamma \vdash T''\ t \Rightarrow [t/x]\kappa_1'$, and the synthesized kind is clearly convertible with $[t/x]\kappa_1$.

In the other subcase, the subject of kinding is of the form $(\lambda\, x:T_1.\, T'')\ t$ and our assumed reduction is to $[t/x]T''$. By inversion of the kinding derivation, we have $\Gamma, x:T_1 \vdash T'' \Rightarrow \kappa_1$. By Lemma 19, we have $\Gamma \vdash [t/x]T'' \Rightarrow [t/x]\kappa_1$.

Case:

$$\frac{\Gamma \vdash T_1 \Rightarrow \Pi\, X{:}\kappa_2.\, \kappa_1 \quad \Gamma \vdash T_2 \Rightarrow \kappa_2' \quad \kappa_2 \cong \kappa_2'}{\Gamma \vdash T_1 \cdot T_2 \Rightarrow [T_2/X]\kappa_1}$$

There are two subcases to consider for the derivation of $T_1 \cdot T_2 \rightsquigarrow_{\mathbf{n}} T'$. In the first subcase, we have $T_1 \rightsquigarrow_{\mathbf{n}} T_1''$ for some T_1'' (so $T' = T_1'' \cdot T_2$). By the IH, we have $\Gamma \vdash T_1'' \Rightarrow \Pi\, X{:}\kappa_2''.\, \kappa_1''$ for some $\kappa_2'' \cong \kappa_2$ and $\kappa_1'' \cong \kappa_1$ (we have from the IH that the kind of T_1'' must be convertible with $\Pi\, X{:}\kappa_2.\, \kappa_1$). By transitivity, we can conclude

$\kappa_2'' \cong \kappa_2'$. By the rule, we have $\Gamma \vdash T_1'' \cdot T_2 \Rightarrow [T_2/X]\kappa_1''$, and the synthesized kind is clearly convertible with $[T_2/X]\kappa_1$.

In the other subcase, the subject of kinding is of the form $(\lambda X{:}\kappa_2.\, T_1'') \cdot T_2$ and our assumed reduction is to $[T_2/X]T_1''$. By inversion of the kinding derivation, we have $\Gamma, X : \kappa_2 \vdash T_1'' \Rightarrow \kappa_1$. By Lemma 15, we have $\Gamma, X : \kappa_2' \vdash T_1'' \Rightarrow \kappa_1'$ for some $\kappa_1' \cong \kappa_1$, and from this and Lemma 19 we have $\Gamma \vdash [T_2/X]T_1'' \Rightarrow [T_2/X]\kappa_1'$. This is clearly convertible with $[T_2/X]\kappa_1$, as desired. □

Corollary 21. *If* $\Gamma \vdash T \Rightarrow \kappa$ *and* $T \rightsquigarrow_{\mathbf{n}}^* T'$ *then* $\Gamma \vdash T' \Rightarrow \kappa'$ *for some* $\kappa' \cong \kappa$.

C.2 Theorem 7

Proof (of Theorem 7). By induction on the assumed derivation, making implicit use of Corollary 21 for the shorthand $\Gamma \vdash t \overset{\rightsquigarrow_{\mathbf{n}}^*}{\Rightarrow} T$ and mostly omitting annotated substitutions when these are clear from context (we show the first one that occurs). We show a few interesting cases.

Case:

$$\frac{(X : \kappa) \in \Gamma}{\Gamma \vdash X \Rightarrow \kappa}$$

By an easy inductive argument on the assumption $\vdash \Gamma$ and weakening, we obtain $\Gamma \vdash \kappa$.

Case:

$$\frac{\Gamma \vdash T \Rightarrow \star \quad \Gamma, x : T \vdash T' \Rightarrow \kappa}{\Gamma \vdash \lambda x{:}T.\, T' \Rightarrow \Pi x{:}T.\, \kappa}$$

By assumption, the first premise, and the context formation rules, we have $\vdash \Gamma, x : T$. By the IH, we have $\Gamma, x : T \vdash \kappa$. Thus, we obtain $\Gamma \vdash \Pi x{:}T.\, \kappa$.

Case:

$$\frac{\Gamma \vdash \kappa \quad \Gamma, X : \kappa \vdash T' \Rightarrow \kappa'}{\Gamma \vdash \lambda X{:}\kappa.\, T' \Rightarrow \Pi X{:}\kappa.\, \kappa'}$$

By assumption, the first premise, and the context formation rules, we have $\vdash \Gamma, X : \kappa$. From this and the IH on the second premise, we have $\Gamma, X : \kappa \vdash \kappa'$. We can then conclude that $\Gamma \vdash \Pi X{:}\kappa.\, \kappa'$

Case:

$$\frac{\Gamma \vdash T_1 \Rightarrow \Pi X{:}\kappa_2.\, \kappa_1 \quad \Gamma \vdash T_2 \Rightarrow \kappa_2' \quad \kappa_2 \cong \kappa_2'}{\Gamma \vdash T_1 \cdot T_2 \Rightarrow [T_2/X]\kappa_1}$$

By the IH on the first premise, we have $\Gamma \vdash \Pi X{:}\kappa_2.\, \kappa_1$, and by inversion this gives us $\Gamma \vdash \kappa_2$, which yields $\vdash \Gamma, X : \kappa_2$, and $\Gamma, X : \kappa_2 \vdash \kappa_1$. By the IH on the second premise, $\Gamma \vdash \kappa_2'$. By Lemma 15 using the third premise, $\Gamma, X : \kappa_2' \vdash \kappa_1$. By Lemma 19, $\Gamma \vdash [T_2/X]\kappa_1$.

Case:

$$\frac{\Gamma \vdash T \Rightarrow \Pi x{:}T'.\, \kappa \quad \Gamma \vdash t \Leftarrow T'}{\Gamma \vdash T\ t \Rightarrow [t/x]^{T'}\kappa}$$

By the IH on the first premise, $\Gamma \vdash \Pi x{:}T'.\, \kappa$. By inversion, $\Gamma \vdash T' \Rightarrow \star$ and $\Gamma, x : T' \vdash \kappa$. So, from the first of these and by context formation $\vdash \Gamma, x : T'$. From the second premise and the χ rule, $\Gamma \vdash \chi\ T\ \text{-}\ t \Rightarrow T$. Finally, by Lemma 19, $\Gamma \vdash [t/x]^T\kappa$.

Case:

$$\frac{\Gamma \vdash t \overset{\rightsquigarrow^*_{\mathrm{n}}}{\Rightarrow} \Pi\, x{:}T'.\, T \quad \Gamma \vdash t' \Leftarrow T'}{\Gamma \vdash t\ t' \Rightarrow [t'/x]^{T'}T}$$

By the IH on the first premise, $\Gamma \vdash \Pi\, x{:}T'.\, T \Rightarrow \star$. By inversion of this, we obtain both $\Gamma \vdash T' \Rightarrow \star$, and that $\Gamma, x : T' \vdash T \Rightarrow \star$. From the first of these and the context formation rules, we have $\vdash \Gamma, x : T'$. Finally, from Lemma 19 we have $\Gamma \vdash [t'/x]T \Rightarrow \star$.

Case:

$$\frac{\Gamma \vdash t \overset{\rightsquigarrow^*_{\mathrm{n}}}{\Rightarrow} \forall\, X{:}\kappa.\, T \quad \Gamma \vdash T' \Rightarrow \kappa' \quad \kappa' \cong \kappa}{\Gamma \vdash t \cdot T' \Rightarrow [T'/X]T}$$

From the IH on the first premise, $\Gamma \vdash \forall\, X : \kappa.\, T \Rightarrow \star$. By inversion of this, we have both $\Gamma \vdash \kappa$ and $\Gamma, X : \kappa \vdash T \Rightarrow \star$. From the first of these, context formation rules, and assumption we have $\vdash \Gamma, X : \kappa$. By the IH on the second premise, we also have $\Gamma \vdash \kappa'$, and from this we have $\vdash \Gamma, X : \kappa'$. We combine this with the earlier derivation of $\Gamma, X : \kappa \vdash T \Rightarrow \star$, the third premise, and Lemma 15 to obtain $\Gamma, X : \kappa' \vdash T \Rightarrow \star$. Finally, we use Lemma 19 to obtain $\Gamma \vdash [T'/X]T \Rightarrow \star$.

Case:

$$\frac{\Gamma \vdash T \Rightarrow \star \quad \Gamma \vdash t \Leftarrow T}{\Gamma \vdash \chi\ T \text{ - } t\ \Rightarrow T}$$

Give to us by the first premise. □

D Refinement types proposal

The following is a proposal to replace dependent intersections with refinement types.

$$\frac{\Gamma \vdash T_1 \Rightarrow \star \quad \Gamma, x : T_1 \vdash T_2 \Rightarrow \star}{\Gamma \vdash \{x : T_1 \mid T_2\} \Rightarrow \star} \qquad \frac{T_1 \cong S_1 \quad T_2 \cong S_2}{\{x : T_1 \mid T_2\} \cong^{\mathrm{t}} \{x : S_1 \mid S_2\}}$$

$$\frac{\Gamma \vdash t_1 \Leftarrow T_1 \quad \Gamma \vdash t_2 \Leftarrow [t_1/x]T_2}{\Gamma \vdash [t_1 \mid t_2] \Leftarrow \{x : T_1 \mid T_2\}} \qquad \frac{\Gamma \vdash t \Rightarrow \{x : T_1 \mid T_2\}}{\Gamma \vdash\uparrow t \Rightarrow T_1}$$

$$\frac{\begin{array}{c}\Gamma \vdash t_1 \Rightarrow \{x : T_1 \mid T_2\} \quad y \notin FV(|t_2|) \\ y \notin FV(T) \quad \Gamma, y : T_2[\uparrow t_1/x] \vdash t_2 \Leftrightarrow T\end{array}}{\Gamma \vdash \epsilon\ t_1\ -\ y.t_2 \Leftrightarrow T}$$

$$\begin{array}{lcllcl} |[t_1 \mid t_2]| & = & |t_1| & |\uparrow t| & = & |t| \\ |\epsilon\ t_1\ -\ y.t_2| & = & |t_2| & & & \end{array}$$

$$[\![\{x : T_1 \mid T_2\}]\!]_{\sigma,\rho} \quad = \quad \{E_1 \in [\![T_1]\!]_{\sigma,\rho} \mid \exists E_2 \in [\![T_2]\!]_{\sigma[x \mapsto \zeta(E)],\rho}\}$$

Figure 9: Refinement types

Theorem 1. **Case:**

$$\frac{\Gamma \vdash T_1 \Rightarrow \star \quad \Gamma, x : T_1 \vdash T_2 \Rightarrow \star}{\Gamma \vdash \{x : T_1 \mid T_2\} \Rightarrow \star}$$

The set $[\![\{x : T_1 \mid T_2\}]\!]_{\sigma,\rho}$ is explicitly defined to be a subset of $[\![T_1]\!]_{\sigma,\rho}$, which is in $\mathcal{R}$, by the IH applied to the first premise. Since for any $A \subseteq \mathcal{L}$, $[A]_{c\beta\eta}$ is in $\mathcal{R}$, to show that $[\![\{x : T_1 \mid T_2\}]\!]_{\sigma,\rho}$ is also in $\mathcal{R}$ it suffices to show definedness of $[\![T_2]\!]_{\sigma[x\mapsto\zeta(E)],\rho}\}$ (which is used in the predicate picking out the particular subset of $[\![T_1]\!]_{\sigma,\rho}$), for $E \in [\![T_1]\!]_{\sigma,\rho}$. For such E, $\zeta(E)$ is defined (since $[\![T_1]\!]_{\sigma,\rho} \in \mathcal{R}$ and hence $E \in [\![T_1]\!]_{\sigma,\rho}$ is nonempty) and in E, so $\sigma[x \mapsto \zeta(E)] \in [\![\Gamma, x : T_1]\!]$. So by the IH for the second premise, $[\![T_2]\!]_{\sigma[x\mapsto\zeta(E),\rho]}$ is defined.

Case:

$$\frac{\Gamma \vdash t_1 \Leftarrow T_1 \quad \Gamma \vdash t_2 \Leftarrow [t/x]^{T_1}\ T_2}{\Gamma \vdash [t_1 \mid t_2] \Leftarrow \{x : T_1 \mid T_2\}}$$

By the IH, we have $[\sigma|t_1|]_{c\beta\eta} \in [\![T_1]\!]_{\sigma,\rho}$ and $[\sigma|t_2|]_{c\beta\eta} \in [\![[t_1/x]T_2]\!]_{\sigma,\rho}$. By Lemma 12, the latter is equivalent to $[\sigma|t_1|]_{c\beta\eta} \in [\![T_2]\!]_{\sigma[x\mapsto\zeta([\sigma|t_1|]_{c\beta\eta}),\rho}$. Thus, we exhibit $[\sigma|t|]_{c\beta\eta}$ for the existentially quantified E_2 in the definition of $[\![\{x : T_1 \mid T_2\}]\!]_{\sigma,\rho}$. So, we see that $[\sigma|t_1|] = [\sigma|[t_1 \mid t_2]|] \in [\![\{x : T_1 \mid T_2\}]\!]_{\sigma,\rho}$, as desired.

Case:

$$\frac{\Gamma \vdash t \Rightarrow \{x : T_1 \mid T_2\}}{\Gamma \vdash\uparrow t \Rightarrow T}$$

The desired conclusion follows easily from the IH and the semantics of refinement types.

Case:

$$\frac{\Gamma \vdash t_1 \Rightarrow \{x : T_1 \mid T_2\} \quad y \notin FV(|t_2|) \quad y \notin FV(T) \quad \Gamma, y : [\uparrow t_1/x]T \vdash t_2 \Leftrightarrow T}{\Gamma \vdash \epsilon\ t_1\ -\ y.t_2 \Leftrightarrow T}$$

By the IH on the first premise, $[\sigma|t_1|] \in [\![\{x : T_1 \mid T_2\}]\!]$. This means that there exists $E_2 \in [\![T_2]\!]_{\sigma[x\mapsto\zeta([\sigma|t_1|])]}$. By Lemma 12, $E_2 \in [\![[\uparrow t_1/x]T_2]\!]_{\sigma,\rho}$. Thus, $(\sigma \uplus [y \mapsto \zeta(E_2), \rho]) \in [\![\Gamma, y : [\uparrow t_1/x]T_2]\!]$, and by the IH on the fourth premise $\sigma[y \mapsto \zeta(E_2)]|t_2| \in [\![T]\!]_{\sigma[y\mapsto\zeta(E_2)],\rho}$. Since $y \notin FV(|t_2|)$ and $y \notin FV(T)$, we have $\sigma|t_2| = \sigma|\epsilon\ t_1\ -\ y.t_2| \in [\![T]\!]_{\sigma,\rho}$ as desired.

□

D.1 Dependent intersections

$$\begin{array}{lcl} \iota\, x{:}T_1.T_2 & = & \{x : T_1 \mid \{y : T_2 \mid \{y \simeq x\}\}\} \\ [t_1, t_2] & = & [t_1 \mid [t_2 \mid \beta]] \\ t.1 & = & \uparrow t \\ t.2 & = & \epsilon\ t\ -\ y.\epsilon\ y\ -z.\varphi\ z\ -\ (\uparrow y)\{t\} \end{array}$$

Figure 10: Dependent intersections

Figure 10 shows an encoding of dependent intersections using refinement types. Abusing notation, let $\mathcal{E}$ be the natural extension of these rules to types, kinds, contexts, and terms.

Theorem 22.

- *Let u be an untyped λ-calculus term. If $|t| = u$ then $|\mathcal{E}(t)| = u$*
- $\mathcal{E}([t/x]T) = [\mathcal{E}(t)/x]\mathcal{E}(T)$
- *1. If $\vdash \Gamma$ then $\vdash \mathcal{E}(\Gamma)$*
  2. If $\Gamma \vdash \kappa$ then $\mathcal{E}(\Gamma) \vdash \mathcal{E}(\kappa)$

3. *If* $\Gamma \vdash T \Rightarrow \kappa$ *then* $\mathcal{E}(\Gamma) \vdash \mathcal{E}(T) \Rightarrow \mathcal{E}(\kappa)$

4. *If* $\Gamma \vdash t \Leftrightarrow T$ *then* $\mathcal{E}(\Gamma) \vdash \mathcal{E}(t) \Leftrightarrow \mathcal{E}(T)$

Proof. We show a few interesting cases.

Case:

$$\textit{If } \Gamma \vdash [t_1, t_2] \Leftarrow \iota\, x{:}T_1.\, T_2 \textit{ then } \mathcal{E}(\Gamma) \vdash \mathcal{E}([t_1, t_2]) \Leftarrow \mathcal{E}(\iota\, x{:}T_1.\, T_2)$$

We have $|t_1| =_{\beta\eta} |t_2|$ from the fourth premise of the assumed derivation. By the erasure lemma, this means $|\mathcal{E}(t_1)| =_{\beta\eta} |\mathcal{E}(t_2)|$. Appeal to the IH on the two typing premises of the derivation to obtain $\mathcal{D}_1 :: \mathcal{E}(\Gamma) \vdash \mathcal{E}(t_1) \Leftarrow \mathcal{E}(T_1)$ and $\mathcal{D}_2 :: \mathcal{E}(\Gamma) \vdash \mathcal{E}(t_2) \Leftarrow \mathcal{E}([t_1/x]T_2)$. By the substitution lemma, this means $\mathcal{E}(t_2)$ checks against type $[\mathcal{E}(t_1)/x]\mathcal{E}(T_2)$. We build the following derivation.

$$\dfrac{\mathcal{D}_1 :: \mathcal{E}(\Gamma) \vdash \mathcal{E}(t_1) \Leftarrow \mathcal{E}(T_1) \qquad \dfrac{\mathcal{D}_2 :: \mathcal{E}(\Gamma) \vdash \mathcal{E}(T_2) \Leftarrow [\mathcal{E}(t_1)/x]\mathcal{E}(T_2) \qquad \dfrac{|\mathcal{E}(t_1)| = |\mathcal{E}(t_2)|}{\mathcal{E}(\Gamma) \vdash \beta \Leftarrow \{\mathcal{E}(t_1) \simeq \mathcal{E}(t_2)\}}}{\mathcal{E}(\Gamma) \vdash [t_2 \mid \beta] \Leftarrow \{y : T_2 \mid \{y \simeq x\}\}}}{\mathcal{E}(\Gamma) \vdash [\mathcal{E}(t_1) \mid [\mathcal{E}(t_2) \mid \beta]] \Leftarrow \{x : \mathcal{E}(T_1) \mid \{y : \mathcal{E}(T_2) \mid \{y \simeq x\}\}\}}$$

Case:

$$\textit{If } \Gamma \vdash t.1 \Rightarrow T \textit{ then } \mathcal{E}(\Gamma) \vdash \mathcal{E}(t.1) \Rightarrow \mathcal{E}(T)$$

Appeal to the IH on the premise of the assumed typing derivation to obtain $\mathcal{D} :: \mathcal{E}(\Gamma) \vdash \mathcal{E}(t) \Rightarrow \mathcal{E}(\iota\, x{:}T_1.\, T_2)$. By the definition of $\mathcal{E}$ we therefore have that $\mathcal{E}(t)$ synthesizes type $\{x : \mathcal{E}(T_1) \mid \{y : \mathcal{E}(T_2) \mid \{y \simeq x\}\}\}$. The goal is to derive $\mathcal{E}(\Gamma) \vdash \mathcal{E}(t.1) \Rightarrow \mathcal{E}(T_1)$.

$$\dfrac{\mathcal{D} :: \mathcal{E}(\Gamma) \vdash t \Rightarrow \{x : \mathcal{E}(T_1) \mid \{y : \mathcal{E}(T_2) \mid \{y \simeq x\}\}\}}{\mathcal{E}(\Gamma) \vdash \uparrow \mathcal{E}(t) \Rightarrow \mathcal{E}(T_1)}$$

□