

# Theorem Proving in Dependently-Typed Higher-Order Logic

Colin Rothgang<sup>1</sup>[0000-0001-9751-8989], Florian Rabe<sup>2</sup>[0000-0003-3040-3655], and  
Christoph Benzmler<sup>3,1</sup>[0000-0002-3392-3093]

<sup>1</sup> Mathematics and Computer Science, FU Berlin, Germany

<sup>2</sup> Computer Science, University Erlangen-Nürnberg, Germany

<sup>3</sup> AI Systems Engineering, University Bamberg

**Abstract.** Higher-order logic HOL offers a very simple syntax and semantics for representing and reasoning about typed data structures. But its type system lacks advanced features where types may depend on terms. Dependent type theory offers such a rich type system, but has rather substantial conceptual differences to HOL, as well as comparatively poor proof automation support.

We introduce a dependently-typed extension DHOL of HOL that retains the style and conceptual framework of HOL. Moreover, we build a translation from DHOL to HOL and implement it as a preprocessor to a HOL theorem prover, thereby obtaining a theorem prover for DHOL.

## 1 Introduction and Related Work

Theorem proving in higher-order logic (HOL) [5,11] has been a long-running research strand producing multiple mature interactive provers [17,13,10] and automated provers [2,22,4]. Similarly, many, mostly interactive, theorem provers are available for various versions of dependent type theory (DTT) [7,15,9,18]. However, it is (maybe surprisingly) difficult to develop theorem provers for dependently-typed higher-order logic (DHOL).

In this paper, we use HOL to refer to a version of Church’s *simply*-typed  $\lambda$ -calculus with a base type `bool` for Booleans, simple function types  $\rightarrow$ , and equality  $=_A : A \rightarrow A \rightarrow \text{bool}$ . This already suffices to define the usual logical quantifiers and connectives.<sup>4</sup> Intuitively, it is straightforward to develop DHOL accordingly on top of the *dependently*-typed  $\lambda$ -calculus, which uses a dependent function type  $\Pi x : A. B$  instead of  $\rightarrow$ . However, several subtleties arise that seem deceptively minor at first but end up presenting fundamental theoretical issues. They come up already in the elementary expression  $x =_A y \Rightarrow f(x) =_{B(x)} f(y)$  for some dependent function  $f : \Pi x : A. B(x)$ .

**Firstly**, the equality  $f(x) =_{B(x)} f(y)$  is not even well-typed because the terms  $f(x) : B(x)$  and  $f(y) : B(y)$  do not have the same type. Intuitively, it is obvious that the type system can (and maybe should) be adjusted so that the equality  $x =_A y$  between terms

---

<sup>4</sup> We do not assume a choice operator or the axiom of infinity.

carries over to an equality  $B(x) \equiv B(y)$  between types.<sup>5</sup> However, this means that the undecidability of equality leaks into the equality of types and thus into type-checking.

While some interactive provers successfully use undecidable type systems [16,6], most formal systems for DTT commit to keeping type-checking decidable. The typical approach goes back to Martin-Löf type theory [14] and the calculus of constructions [8] and uses two separate equality relations, a decidable meta-level equality for use in the type-checker and a stronger undecidable one subject to theorem proving. Moreover, it favors the propositions-as-types representation and deemphasizes or omits a type of classical Booleans. This approach has been studied extensively [7,15,9] and is not the subject of this paper.

Instead, our motivation is to retain a single equality relation and classical Booleans. This is arguably more intuitive to users, especially to those outside the DTT community such as typical HOL users or mathematicians, and it is certainly much closer to the logics of the strongest available ATP systems. This means we have to pay the price of undecidable type-checking. The current paper was prompted by the observation that this price may be acceptable for two reasons:

1. If our ultimate interest is theorem proving, undecidability comes up anyway. Indeed, it is plausible that the cost of showing the well-typedness of a conjecture will be negligible compared to the cost of proving it.
2. As the strength of ATPs for HOL increases, the practical drawbacks of undecidable type-checking decrease, which indicates revisiting the trade-off from time to time. Indeed, if we position DHOL close to an existing HOL ATP, it is plausible that the price will, in practice, be affordable.

**Secondly**, even if we add a rule like “if  $\vdash x =_A y$ , then  $\vdash B(x) \equiv B(y)$ ” to our type system, the above expression is still not well-typed: Above, the equality  $x =_A y$  on the left of  $\Rightarrow$  is needed to show the well-typedness of the equality  $f(x) =_{B(x)} f(y)$  on the right. This intertwines theorem proving and type-checking even further. Concretely, we need a *dependent implication*, where the first argument is assumed to hold while checking the well-typedness of the second one. Formally, this means that to show  $\vdash F \Rightarrow G : \text{bool}$ , we require  $\vdash F : \text{bool}$  and  $F \vdash G : \text{bool}$ . Similarly, we need a dependent conjunction. And if we are classical, we may also opt to add a dependent disjunction  $F \vee G$ , where  $\neg F$  is assumed in  $G$ . Naturally, dependent conjunction and disjunction are not commutative anymore. This may feel disruptive, but similar behavior of connectives is well-known from short-circuit evaluation in programming languages.

The meta-logical properties of dependent connectives are straightforward. However, interestingly, these connectives can no longer be defined from just equality. At least one of them (we will choose dependent implication) must be taken as an additional primitive in DHOL along with  $=_A$ .

**Finally**, the above generalizations require a notion of DHOL-contexts that is more complex than for HOL. HOL-contexts can be stratified into (a) a set of variable declarations

<sup>5</sup> Note that while term equality  $=_A$  is a bool-valued connective, type equality  $\equiv$  is not. Instead, in HOL,  $\equiv$  is a judgment at the same level as the typing judgment  $t : A$ .

$x_i : A_i$ , and (b) a set of logical assumptions  $F$  possibly using the variables  $x_i$ . Moreover, the former are often not explicitly listed at all and instead inferred from the remainder of the sequent. But in DHOL, the well-formedness of an  $A_i$  may now depend on previous logical assumptions. To linearize this inter-dependency, DHOL contexts must consist of a single list alternating between variable declarations and assumptions.

*Contribution.* Our contribution is twofold. Firstly, we introduce a new logic DHOL designed along the lines described above. Moreover, we further extend DHOL with predicate subtypes  $A|_p$  for a predicate  $p : A \rightarrow \text{bool}$  on the type  $A$ . Besides dependent types, these constitute a second important source of terms occurring in types. Because they also make typing undecidable, they are often avoided. The most prominent exception is PVS [16], whose kernel essentially arises by adding predicate subtypes to HOL. In current HOL ITPs going back to [10], their use is usually restricted to the subtype definition principle: here a definition  $b := A|_p$  may occur on toplevel and is elaborated into a fresh type  $b$  that is axiomatized to mimic the subtype  $A|_p$ . Because we are committed to undecidable typing anyway, predicate subtypes fit naturally into our approach.

Secondly, we develop and implement a sound and complete translation of DHOL into HOL. This setup allows the use of DHOL as the expressive user-facing language and HOL as the internal theorem-proving language. We position our implementation close to an existing HOL ATP, namely the LEO-III system. From the LEO-III perspective, DHOL serves as an additional input language that is translated into HOL by an external logic embedding tool [20,21] in the LEO-III ecosystem. Because LEO-III already supports such embeddings and because the TPTP syntax [23] foresees the use of dependent types in ATPs and provides syntax for them (albeit without a normative semantics), we were able to implement the translation with no disruptions to existing workflows.

The general idea of our translation of dependent into simple type theory is not new [3]. In that work, Martin-Löf-style dependent type theory is translated into Gordon’s HOL ITP [10]. This work differs critically from ours because it uses DTT in propositions-as-types style. Our work builds DHOL with classical Booleans and equality predicate, which makes the task of proving the translation sound and complete very different. Moreover, their work targets an interactive prover while ours targets automated ones.

*Overview.* In Sect. 2 we recap the HOL logic. In Sect. 3 we extend it to DHOL and define our translation from DHOL to HOL. In Sect. 4 we add subtyping and predicate subtypes. In Sect. 5 we prove the soundness and completeness of the translation. In Sect. 6 we describe how to use our translation and a HOL ATP to implement a theorem prover for DHOL.

*Acknowledgments.* Chad Brown and Alexander Steen provided valuable feedback on earlier versions of this paper.

## 2 Preliminaries: Higher-Order Logic

We introduce the syntax and rules of HOL. Our definitions are standard except that we tweak a few details in order to later present the extension to DHOL more succinctly. We

use the following grammar for HOL:

$T$	$::= \circ \mid T, a : \text{tp} \mid T, c : A \mid T, c : F$	theories
$\Gamma$	$::= \cdot \mid \Gamma, x : A \mid \Gamma, x : F$	contexts
$A, B$	$::= a \mid A \rightarrow B \mid \text{bool}$	types
$s, t, f, F, G$	$::= c \mid x \mid \lambda x : A. t \mid f \ t \mid s =_A t \mid F \Rightarrow G$	terms

A theory  $T$  is a list of base type declarations  $a : \text{tp}$ , typed constant declarations  $c : A$ , and named axioms  $c : F$  asserting the formula  $F$ . A context  $\Gamma$  has the same form except that no type variables are allowed. It is not strictly necessary to use named axioms and assumptions, but it makes our extensions to DHOL later on simpler. We write  $\circ$  and  $\cdot$  for the empty theory and context, respectively. At this point, it is possible to normalize contexts into a set of variable declarations followed by a set of assumptions because the well-formedness of a type  $A$  can never depend on a variable or an assumption. But that property will change when going to DHOL, which is why we allow  $\Gamma$  to alternate between variables and assumptions.

Types  $A$  are either user-declared types  $a$ , the built-in base type  $\text{bool}$ , or function types  $A \rightarrow B$ . Terms are constants  $c$ , variables  $x$ ,  $\lambda$ -abstractions  $\lambda x : A. t$ , function applications  $f \ t$ , or obtained from the built-in  $\text{bool}$ -valued connectives  $=_A$  or  $\Rightarrow$ . As usual [1], this suffices to define all the usual quantifiers and connectives  $\text{true}$ ,  $\text{false}$ ,  $\neg$ ,  $\wedge$ ,  $\vee$ ,  $\forall$  and  $\exists$ . This includes  $\Rightarrow$ , but we make it a primitive here because we will change it in DHOL. As usual,  $E[x/i]$  denotes the capture-avoiding substitution of the variable  $x$  with the term  $t$  within expression  $E$ .

The type and proof system uses the judgments given below. Note that we need a meta-level judgment for the equality of types because  $\equiv$  is not a  $\text{bool}$ -valued connective. On the contrary, the equality of terms  $\vdash s =_A t$  is a special case of the validity judgment  $\vdash F$ . In HOL,  $\equiv$  is trivial, and the judgment is redundant. But we include it here already because it will become non-trivial in DHOL.

Name	Judgment	Intuition
theories	$\vdash T \text{ Thy}$	$T$ is well-formed theory
contexts	$\vdash_T \Gamma \text{ Ctx}$	$\Gamma$ is well-formed context
types	$\Gamma \vdash_T A \text{ tp}$	$A$ is well-formed type
typing	$\Gamma \vdash_T t : A$	$t$ is a well-formed term of type well-formed type $A$
validity	$\Gamma \vdash_T F$	well-formed Boolean $F$ is provable
equality of types	$\Gamma \vdash_T A \equiv B$	well-formed types $A$ and $B$ are equal

The rules are given in Figure 1. We assume that all names in a theory or a context are unique without making that explicit in the rules. Following common practice, we further assume that HOL types are non-empty. See also Appendix A for a detailed definition description.

### 3 Dependent Function Types

#### 3.1 Language

We have carefully defined HOL in such a way that only a few surgical changes are needed to define DHOL. A consolidated definition of DHOL is given in Appendix A. The **gram-**

Theories and contexts:

$$\frac{}{\vdash \circ \text{Thy}} \quad \frac{\vdash T \text{ Thy}}{\vdash T, a \text{ tp Thy}} \quad \frac{\vdash_T A \text{ tp}}{\vdash T, c : A \text{ Thy}} \quad \frac{\vdash_T F : \text{bool}}{\vdash T, c : F \text{ Thy}}$$

$$\frac{\vdash T \text{ Thy}}{\vdash_T \cdot \text{Ctx}} \quad \frac{\Gamma \vdash_T A \text{ tp}}{\vdash_T \Gamma, x : A \text{ Ctx}} \quad \frac{\Gamma \vdash_T F : \text{bool}}{\vdash_T \Gamma, x : F \text{ Ctx}}$$

Lookup in theory and context:

$$\frac{a : \text{tp in } T \quad \vdash_T \Gamma \text{ Ctx}}{\Gamma \vdash_T a \text{ tp}} \quad \frac{c : A' \text{ in } T \quad \Gamma \vdash_T A' \equiv A}{\Gamma \vdash_T c : A} \quad \frac{c : F \text{ in } T \quad \vdash_T \Gamma \text{ Ctx}}{\Gamma \vdash_T F}$$

$$\frac{x : A' \text{ in } \Gamma \quad \Gamma \vdash_T A' \equiv A}{\Gamma \vdash_T x : A} \quad \frac{x : F \text{ in } \Gamma \quad \vdash_T \Gamma \text{ Ctx}}{\Gamma \vdash_T F}$$

Well-formedness and equality of types:

$$\frac{\vdash_T \Gamma \text{ Ctx}}{\Gamma \vdash_T \text{bool tp}} \quad \frac{\Gamma \vdash_T A \text{ tp} \quad \Gamma \vdash_T B \text{ tp}}{\Gamma \vdash_T A \rightarrow B \text{ tp}} \quad \frac{\Gamma \vdash_T A \text{ tp}}{\Gamma \vdash_T A \equiv A} \quad \frac{\Gamma \vdash_T A \equiv A' \quad \Gamma \vdash_T B \equiv B'}{\Gamma \vdash_T A \rightarrow B \equiv A' \rightarrow B'}$$

Typing:

$$\frac{\Gamma, x : A \vdash_T t : B}{\Gamma \vdash_T (\lambda x : A. t) : A \rightarrow B} \quad \frac{\Gamma \vdash_T f : A \rightarrow B \quad \Gamma \vdash_T t : A}{\Gamma \vdash_T f t : B} \quad \frac{\Gamma \vdash_T s : A \quad \Gamma \vdash_T t : A}{\Gamma \vdash_T s =_A t : \text{bool}}$$

Term equality: congruence, reflexivity, symmetry,  $\beta$ ,  $\eta$

$$\frac{\Gamma \vdash_T A \equiv A' \quad \Gamma, x : A \vdash_T t =_B t'}{\Gamma \vdash_T \lambda x : A. t =_{A \rightarrow B} \lambda x : A'. t'} \quad \frac{\Gamma \vdash_T t =_A t' \quad \Gamma \vdash_T f =_{A \rightarrow B} f'}{\Gamma \vdash_T f t =_B f' t'}$$

$$\frac{\Gamma \vdash_T t : A}{\Gamma \vdash_T t =_A t} \quad \frac{\Gamma \vdash_T t =_A s}{\Gamma \vdash_T s =_A t} \quad \frac{\Gamma \vdash_T (\lambda x : A. s) t : B}{\Gamma \vdash_T (\lambda x : A. s) t =_B s[x/t]} \quad \frac{\Gamma \vdash_T t : A \rightarrow B \quad x \text{ not in } \Gamma}{\Gamma \vdash_T t =_{A \rightarrow B} \lambda x : A. t x}$$

Rules for implication:

$$\frac{\Gamma \vdash_T F : \text{bool} \quad \Gamma \vdash_T G : \text{bool}}{\Gamma \vdash_T F \Rightarrow G : \text{bool}} \quad \frac{\Gamma \vdash_T F : \text{bool} \quad \Gamma, x : F \vdash_T G}{\Gamma \vdash_T F \Rightarrow G} \quad \frac{\Gamma \vdash_T F \Rightarrow G \quad \Gamma \vdash_T F}{\Gamma \vdash_T G}$$

Congruence for validity, Boolean extensionality, and non-emptiness of types:

$$\frac{\Gamma \vdash_T F =_{\text{bool}} F' \quad \Gamma \vdash_T F'}{\Gamma \vdash_T F} \quad \frac{\Gamma \vdash_T p \text{ true} \quad \Gamma \vdash_T p \text{ false}}{\Gamma, x : \text{bool} \vdash_T p x} \quad \frac{\Gamma \vdash_T F : \text{bool} \quad \Gamma, x : A \vdash_T F}{\Gamma \vdash_T F}$$

**Fig. 1.** HOL Rules

**mar** is as follows where unchanged parts are shaded out:

$T$	$::=$	$\circ \mid T, a : (\Pi x : A.)^* \text{tp} \mid T, c : A \mid T, c : F$	theories
$\Gamma$	$::=$	$\cdot \mid \Gamma, x : A \mid \Gamma, \text{ass} : F$	contexts
$A, B$	$::=$	$a \ t_1 \dots t_n \mid \Pi x : A. B \mid \text{bool}$	types
$s, t, f, F, G$	$::=$	$c \mid x \mid \lambda x : A. t \mid f \ t \mid s =_A t \mid F \Rightarrow G$	terms

Concretely, base types  $a$  may now take term arguments and simple function types  $A \rightarrow B$  are replaced with dependent function types  $\Pi x : A. B$ . As usual we will retain the notation  $A \rightarrow B$  for the latter if  $x$  does not occur free in  $B$ . DHOL is a conservative extension of HOL, and we recover HOL as the fragment of DHOL in which all base types  $a$  have arity 0.

*Example 1 (Category Theory).* As a running example, we formalize the theory of a category in DHOL. It declares the base type *obj* for objects and the dependent base type *mor*  $a$   $b$  for morphisms. Further it declares the constants *id* and *comp* for identity and composition, and the axioms for neutrality. We omit the associativity axiom for brevity.

```

obj : tp
mor :  $\Pi x, y : \text{obj}. \text{tp}$ 
id :  $\Pi a : \text{obj}. \text{mor } a \ a$ 
comp :  $\Pi a, b, c : \text{obj}. \text{mor } a \ b \rightarrow \text{mor } b \ c \rightarrow \text{mor } a \ c$ 
neutL :  $\forall x, y : \text{obj}. \forall m : \text{mor } x \ y. \text{moid}_x =_{\text{mor } x \ y} m$ 
neutR :  $\forall x, y : \text{obj}. \forall m : \text{mor } x \ y. \text{id}_y \circ m =_{\text{mor } x \ y} m$ 

```

Here we use a few intuitive notational simplifications such as writing  $\Pi x, y : \text{obj}.$  for binding two variables of the same type. We also use the notations  $\text{id}_x$  for  $\text{id } x$  and  $\text{hog}$  for  $\text{comp } \_ \_ g \ h$  where the  $\_$  denote inferable arguments of type *obj*.

The **judgments** stay the same and we only make minor changes to the **rules**, which we explain in the sequel. Firstly we replace all rules for  $\rightarrow$  with the ones for  $\Pi$ :

$$\begin{array}{c}
\frac{\Gamma \vdash_T A \text{ tp} \quad \Gamma, x : A \vdash_T B \text{ tp}}{\Gamma \vdash_T \Pi x : A. B \text{ tp}} \quad \frac{\Gamma \vdash_T A \equiv A' \quad \Gamma, x : A \vdash_T B \equiv B'}{\Gamma \vdash_T \Pi x : A. B \equiv \Pi x : A'. B'} \\
\frac{\Gamma, x : A \vdash_T t : B}{\Gamma \vdash_T (\lambda x : A. t) : \Pi x : A. B} \quad \frac{\Gamma \vdash_T f : \Pi x : A. B \quad \Gamma \vdash_T t : A}{\Gamma \vdash_T f \ t : B[x/i]} \\
\frac{\Gamma \vdash_T A \equiv A' \quad \Gamma, x : A \vdash_T t =_B t'}{\Gamma \vdash_T \lambda x : A. t =_{\Pi x : A. B} \lambda x : A'. t'} \quad \frac{\Gamma \vdash_T t =_A t' \quad \Gamma \vdash_T f =_{\Pi x : A. B} f'}{\Gamma \vdash_T f \ t =_B f' \ t'} \\
\frac{\Gamma \vdash_T t : \Pi x : A. B}{\Gamma \vdash_T t =_{\Pi x : A. B} \lambda x : A. t \ x}
\end{array}$$

Then we replace the rules for declaring, using, and equating base types with the ones where base types are applied to arguments:

$$\frac{\vdash_T x_1 : A_1, \dots, x_n : A_n \text{ Ctx}}{\vdash_T, a : \Pi x_1 : A_1. \dots \Pi x_n : A_n. \text{tp} \text{ Thy}}$$

$$\begin{array}{c}
\frac{\begin{array}{c} \vdash_T \Gamma \text{Ctx } a : \Pi x_1 : A_1. \dots \Pi x_n : A_n. \text{tp in } T \\ \Gamma \vdash_T t_1 : A_1 \dots \Gamma \vdash_T t_n : A_n[x_1/t_1] \dots [x_{n-1}/t_{n-1}] \end{array}}{\Gamma \vdash_T a t_1 \dots t_n \text{tp}} \\
\\
\frac{\begin{array}{c} \vdash_T \Gamma \text{Ctx } a : \Pi x_1 : A_1. \dots \Pi x_n : A_n. \text{tp in } T \\ \Gamma \vdash_T s_1 =_{A_1} t_1 \dots \Gamma \vdash_T s_n =_{A_n[x_1/t_1] \dots [x_{n-1}/t_{n-1}]} t_n \end{array}}{\Gamma \vdash_T a s_1 \dots s_n \equiv a t_1 \dots t_n}
\end{array}$$

The last of these is the critical rule via which term equality leaks into type equality. Thus, typing of expressions may now depend on equality assumptions and thus typing becomes undecidable.

*Example 2 (Undecidability of Typing).* Continuing Ex. 1, consider terms  $\vdash f : \text{mor } u \ v$  and  $\vdash g : \text{mor } v' \ w$  for terms  $\vdash u, v, v', w : \text{obj}$ . Then  $\vdash g \circ f : \text{mor } u \ w$  holds iff  $\vdash f : \text{mor } u \ v'$ , which holds iff  $\vdash v =_{\text{obj}} v'$ . Depending on the axioms present, this may be arbitrarily difficult to prove.

Finally, we modify the rule for the non-emptiness of types: we allow the existence of empty dependent types and only require that for each HOL type in the image of the translation there exists one non-empty DHOL type translated to it (rather than requiring all dependent types translated to it to be non-empty). And we replace the typing rule for implication with the dependent one. The proof rules for implications are unchanged.

$$\frac{\Gamma \vdash_T F : \text{bool} \quad \Gamma, x : F \vdash_T G : \text{bool}}{\Gamma \vdash_T F \Rightarrow G : \text{bool}}$$

*Example 3 (Dependent Implication).* Continuing Ex. 1, consider the formula

$$x : \text{obj}, y : \text{obj} \vdash x =_{\text{obj}} y \Rightarrow \text{id}_x =_{\text{mor } x \ x} \text{id}_y : \text{bool}$$

which expresses that equal objects have equal identity morphisms. It is easy to prove. But it is only well-typed because the typing rule for dependent implication allows using  $x =_{\text{obj}} y$  while type-checking  $\text{id}_x =_{\text{mor } x \ x} \text{id}_y : \text{bool}$ , which requires deriving  $\text{id}_y : \text{mor } x \ x$  and thus  $\text{mor } y \ y \equiv \text{mor } x \ x$ .

All the usual connectives and quantifiers can be defined in any of the usual ways now. However, the details matter for the dependent versions of the connectives. In particular, we choose  $F \wedge G := \neg(F \Rightarrow \neg G)$  and  $F \vee G := \neg F \Rightarrow G$  in order to obtain the dependent versions of conjunction and disjunction, in which the well-formedness of  $G$  may depend on the truth or falsity of  $F$ , respectively.

### 3.2 Translation

We define a translation function  $X \mapsto \overline{X}$  that maps any DHOL-syntax  $X$  to HOL-syntax. Its intuition is to erase type dependencies by translating all types  $a t_1 \dots, t_n$  to  $a$  and replacing every  $\Pi$  with  $\rightarrow$ . To recover the information of the erased dependencies,

we additionally define a partial equivalence relation (PER)  $A^*$  on  $\bar{A}$  for every DHOL-type  $A$ .

In general, a PER  $r$  on type  $U$  is a symmetric and transitive relation on  $U$ . This is equivalent to  $r$  being an equivalence relation on a subtype of  $U$ . The intuitive meaning of our translation is that the DHOL-type  $A$  corresponds in HOL to the quotient of the appropriate subtype of  $\bar{A}$  by the equivalence  $A^*$ . In particular, the predicate  $A^* t t$  captures whether  $t$  represents a term of type  $A$ . More formally, the correspondence is:

DHOL	HOL
type $A$	type $\bar{A}$ and PER $A^* : \bar{A} \rightarrow \bar{A} \rightarrow \text{bool}$
term $t : A$	term $\bar{t} : \bar{A}$ satisfying $A^* \bar{t} \bar{t}$

**Definition 1 (Translation).** We translate DHOL-syntax by induction on the grammar. Theories and contexts are translated declaration-wise:

$$\bar{o} := o \quad \bar{T}, \bar{D} := T, D \quad \bar{\cdot} := \cdot \quad \bar{T}, \bar{D} := T, D$$

where  $\bar{D}$  is a list of declarations.

The translation  $\bar{a} : \Pi x_1 : A_1. \dots \Pi x_n : A_n. \text{tp}$  of a base type declaration is given by

$$a : \text{tp}, \quad a^* : \bar{A}_1 \rightarrow \dots \rightarrow \bar{A}_n \rightarrow a \rightarrow a \rightarrow \text{bool}$$

$$a_{PER} : \forall x_1 : \bar{A}_1. \dots \forall x_n : \bar{A}_n. \forall u, v : a. a^* x_1 \dots x_n u v \Rightarrow u =_a v$$

Thus,  $a$  is translated to a base type of the same name without arguments and a trivial PER for every argument tuple. Intuitively,  $a^* \bar{t}_1 \dots \bar{t}_n u u$  defines the subtype of the HOL-type  $a$  corresponding to the DHOL-type  $a t_1 \dots t_n$ .

Constant and variable declarations are translated by adding the assumptions that they are in the PER of their type, and axioms and assumptions are translated straightforwardly:

$$\begin{aligned} \bar{c} : \bar{A} &:= c : \bar{A}, c^* : A^* c c & \bar{x} : \bar{A} &:= x : \bar{A}, x^* : A^* x x \\ \bar{c} : \bar{F} &:= c : \bar{F} & \bar{x} : \bar{F} &:= x : \bar{F} \end{aligned}$$

The cases of  $\bar{A}$  and  $A^*$  for types  $A$  are:

$$\begin{aligned} \overline{a t_1 \dots t_n} &:= a & (a t_1 \dots t_n)^* s t &:= a^* \bar{t}_1 \dots \bar{t}_n s t \\ \overline{\Pi x : A. B} &:= \bar{A} \rightarrow \bar{B} & (\Pi x : A. B)^* f g &:= \forall x, y : \bar{A}. A^* x y \Rightarrow B^* (f x) (g y) \\ \overline{\text{bool}} &:= \text{bool} & \text{bool}^* s t &:= s =_{\text{bool}} t \end{aligned}$$

Finally, the cases for terms are straightforward except for, crucially, translating equality to the respective PER:

$$\begin{aligned} \bar{c} &:= c & \bar{x} &:= x & \overline{\lambda x : A. t} &:= \lambda x : \bar{A}. \bar{t} & \overline{f t} &:= \bar{f} \bar{t} \\ \overline{F \Rightarrow G} &:= \bar{F} \Rightarrow \bar{G} & \overline{s =_A t} &:= A^* \bar{s} \bar{t} \end{aligned}$$



*Example 4 (Translating Derived Connectives).* If we define `true`, `false`,  $\neg$  as usual in HOL and use the definition for dependent conjunction from above, it is straightforward to show that all DHOL-connectives are translated to their HOL-counterparts. For example, we have (up to logical equivalence in HOL) that  $\overline{F \wedge G} = \overline{F} \wedge \overline{G}$ .

We also define the quantifiers in the usual way, e.g., using  $\forall x : A. F(x) := \lambda x : A. F(x) =_{A \rightarrow \text{bool}} \lambda x : A. \text{true}$ . Then applying our translation yields

$$\begin{aligned} \overline{\forall x : A. F(x)} &= (A \rightarrow \text{bool})^* \overline{\lambda x : A. F(x)} \overline{\lambda x : A. \text{true}} \\ &= \forall x, y : \overline{A}. A^* x y \Rightarrow \text{bool}^* F(x) \text{true} \end{aligned}$$

This looks clunky, but (because  $A^*$  is a PER as shown in Theorem 1) is equivalent to  $\forall x : \overline{A}. A^* x x \Rightarrow F(x)$ . Thus, DHOL- $\forall$  is translated to HOL- $\forall$  relativized using  $A^* x x$ . The corresponding rule  $\overline{\exists x : A. F(x)} = \exists x : \overline{A}. A^* x x \wedge F(x)$  can be shown accordingly.

*Example 5 (Categories in HOL).* We give a fragment of the translation of Ex. 1:

```
obj : tp          obj* : obj → obj → bool
mor : tp          mor* : obj → obj → mor → mor → bool
id : obj → mor   id* : ∀x, y : obj. obj* x y ⇒ mor* x x (id x) (id y)
comp : obj → obj → obj → mor → mor → mor
neutL : ∀x : obj. obj* x x ⇒ ∀y : obj. obj* y y ⇒
      ∀m : mor. mor* x y m m ⇒ mor* x y (comp x x y (id x) m) m
```

Here, for brevity, we have omitted  $\text{obj}_{PER}$ ,  $\text{mor}_{PER}$ , and  $\text{comp}^*$  and have already used the translation rule for  $\forall$  from Ex. 4. The result is structurally close to what a native formalization of categories in HOL would look like, but somewhat clunkier.

## 4 Predicate Subtypes

To add predicate subtypes, we extend the **grammar** with the production  $A ::= A|_F$ . No new productions for terms are needed because the inhabitants of  $A|_F$  use the same syntax as those of  $A$ .

*Example 6 (Isomorphisms).* We continue Example 1 and use predicate subtypes to write the type `isomorphisms`  $u$  of automorphisms on  $u$  as a subtype of `mor`  $u$   $u$ . We can define `isomorphisms`  $u := (\text{mor } u \text{ } u)|_p$  where the predicate  $p$  is given by

$$\lambda m : \text{mor } u \text{ } u. \exists i : \text{mor } u \text{ } u. (iom =_{\text{mor } u \text{ } u} id_u) \wedge (moi =_{\text{mor } u \text{ } u} id_u)$$

Adding subtyping requires a few extensions to our type system. First we add a **judgment**  $\Gamma \vdash_T A <: B$  and replace the lookup rules for variables and constants with their subtyping-aware variants:

$$\frac{c : A' \text{ in } T \quad \Gamma \vdash_T A' <: A}{\Gamma \vdash_T c : A} \quad \frac{x : A' \text{ in } \Gamma \quad \Gamma \vdash_T A' <: A}{\Gamma \vdash_T x : A}$$

Typing rules for predicate subtypes:

$$\frac{\Gamma \vdash_T p : \Pi x : A. \text{bool}}{\Gamma \vdash_T A|_p \text{ tp}} \quad \frac{\Gamma \vdash_T t : A \quad \Gamma \vdash_T p t}{\Gamma \vdash_T t : A|_p} \quad \frac{\Gamma \vdash_T t : A|_p}{\Gamma \vdash_T p t}$$

Congruence and variance rule for predicate subtypes:

$$\frac{\Gamma \vdash_T A \equiv A' \quad \Gamma \vdash_T p =_{\Pi x:A. \text{bool}} p'}{\Gamma \vdash_T A|_p \equiv A'|_{p'}} \quad \frac{\Gamma \vdash_T A <: A' \quad \Gamma, x : A \vdash_T p x \Rightarrow p' x}{\Gamma \vdash_T A|_p <: A'|_{p'}}$$

Rules that relate  $A$  and  $A|_p$ :

$$\frac{\Gamma \vdash_T A <: A'}{\Gamma \vdash_T A|_p <: A'} \quad \frac{\Gamma \vdash_T A \text{ tp}}{\Gamma \vdash_T A \equiv A|_{\lambda x:A. \text{true}}} \quad \frac{\Gamma \vdash_T A \text{ tp}}{\Gamma \vdash_T A|_{\lambda x:A. \text{true}} \equiv A}$$

Variance rules for other DHOL types:

$$\frac{\Gamma \vdash_T A \equiv A'}{\Gamma \vdash_T A <: A'} \quad \frac{\Gamma \vdash_T A' <: A \quad \Gamma, x : A' \vdash_T B <: B'}{\Gamma \vdash_T \Pi x : A. B <: \Pi x : A'. B'}$$

Rules for normalizing certain subtypes:

$$\frac{\Gamma \vdash_T A \text{ tp} \quad \Gamma, x : A \vdash_T B \text{ tp} \quad \Gamma, x : A \vdash_T p : \Pi y : B. \text{bool}}{\Gamma \vdash_T \Pi x : A. (B|_p) \equiv (\Pi x : A. B)|_{\lambda f. \forall x:A. p (f x)}} \quad \frac{\Gamma \vdash_T A \text{ tp} \quad \Gamma \vdash_T p : \Pi x : A. \text{bool} \quad \Gamma \vdash_T q : \Pi x : (A|_p). \text{bool}}{\Gamma \vdash_T A|_p|_q \equiv A|_{\lambda x:A. p \wedge q x}}$$

**Fig. 2.** Additional Rules for Predicate Subtypes

Then we add the **rules** given in Figure 2. These induce an algorithm for deciding subtyping relative to an oracle for the undecidable validity judgment. The latter enters the algorithm when two predicate subtypes are compared. Note that the type-equality rule for  $A|_p|_q$  uses a dependent conjunction.

The resulting system is a conservative extension of the variants of HOL and DHOL without subtyping: we recover these systems as the fragments that do not use  $A|_p$ . In particular, in that case  $A <: B$  is trivial and holds iff  $A \equiv B$  holds.

Finally, we extend our **translation** by adding the cases for predicate subtypes:

**Definition 2 (Translation).** We extend Def. 1 with

$$\overline{A|_p} := \overline{A} \quad (A|_p)^* s t := A^* s t \wedge \overline{p} s \wedge \overline{p} t$$

## 5 Soundness and Completeness

Now we establish that our translation is faithful, i.e. sound and complete. We will use the terms *sound* and *complete* from the perspective of using a HOL-ATP for theorem prov-

ing in DHOL, e.g., *sound* means if  $\bar{F}$  is a HOL-theorem, then  $F$  is a DHOL-theorem, and *complete* is the dual.<sup>6</sup>

The completeness theorem states that our translation preserves all DHOL-judgments. Moreover, the theorem statement clarifies the intuition behind the translations invariants:

**Theorem 1 (Completeness).** *We have*

<i>if in DHOL</i>	<i>then in HOL</i>
$\vdash_T T \text{ Thy}$	$\vdash \bar{T} \text{ Thy}$
$\vdash_T \Gamma \text{ Ctx}$	$\vdash_{\bar{T}} \bar{\Gamma} \text{ Ctx}$
$\Gamma \vdash_T A \text{ tp}$	$\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \text{ tp} \quad \text{and} \quad \bar{\Gamma} \vdash_{\bar{T}} A^* : \bar{A} \rightarrow \bar{A} \rightarrow \text{bool} \text{ and } A^* \text{ is PER}$
$\Gamma \vdash_T A \equiv B$	$\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \bar{B} \quad \text{and} \quad \bar{\Gamma}, x, y : \bar{A} \vdash_{\bar{T}} A^* x y =_{\text{bool}} B^* x y$
$\Gamma \vdash_T A <: B$	$\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \bar{B} \quad \text{and} \quad \bar{\Gamma}, x, y : \bar{A} \vdash_{\bar{T}} A^* x y \Rightarrow B^* x y$
$\Gamma \vdash_T t : A$	$\bar{\Gamma} \vdash_{\bar{T}} \bar{t} : \bar{A} \quad \text{and} \quad \bar{\Gamma} \vdash_{\bar{T}} A^* \bar{t} \bar{t}$
$\Gamma \vdash_T F$	$\bar{\Gamma} \vdash_{\bar{T}} \bar{F}$

Additionally the substitution lemma holds, i.e.,

$$\Gamma, x : A \vdash_T t : B \text{ and } \Gamma \vdash u : A \quad \text{implies} \quad \bar{\Gamma} \vdash_{\bar{T}} \bar{t}[\bar{x}/\bar{u}] =_{\bar{B}} \bar{t}[\bar{x}/\bar{u}]$$

*Proof.* The proof proceeds by induction on derivations. It is given in the appendix.

The reverse direction is much trickier. To understand why, we look at two canaries in the coal mine that we have used to reject multiple intuitive but untrue conjectures:

*Example 7 (Non-Injectivity of the Translation).* Continuing Ex. 1, assume terms  $u, v : \text{obj}$  and consider the identify functions  $I_u := \lambda f : \text{mor } u \text{ } u.f$  and  $I_v := \lambda f : \text{mor } v \text{ } v.f$ . Both are translated to the same HOL-term  $\bar{I}_u = \bar{I}_v = \lambda f : \text{mor}.f$  (because  $I_u$  and  $I_v$  only differ in the type indices, which are erased by our translation).

Consequently, the ill-typed DHOL-Boolean  $b := I_u =_{\text{mor } u \text{ } u \rightarrow \text{mor } u \text{ } u} I_v$  is translated to the HOL-Boolean  $\lambda f : \text{mor}.f =_{\text{mor} \rightarrow \text{mor}} \lambda f : \text{mor}.f$ , which is not only well-typed but even a theorem.

To better understand the underlying issue we introduce the notion of *spurious* terms. The well-typed translation  $\bar{t}$  of a DHOL-term  $t$  is called **spurious** if  $t$  is ill-typed (otherwise it is called *proper*). Intuitively, we should be able to use the PERs  $A^*$  to deal with spurious terms: to type-check  $t : A$  in DHOL, we want to use  $A^* \bar{t} \bar{t}$  in HOL. But even that is tricky:

<sup>6</sup> If, however, we think of our translation as an interpretation function that maps syntax to semantics, we could also justify swapping the names of the theorems.

*Example 8 (Trivial PERs for Built-In Base Types).* Consider the property  $\text{bool}^* x x$ . Our translation guarantees  $\text{bool}^* \text{true true}$  and  $\text{bool}^* \text{false false}$ . Thus, we can use Boolean extensionality to prove in HOL that  $\forall x : \text{bool}. \text{bool}^* x x$ , making the property trivial. In particular, we can prove  $\text{bool}^* \bar{b} \bar{b}$  for the spurious Boolean  $b$  from Ex. 7. Even worse, the property  $(\Pi x : A. B)^* x x$  is trivial in this way whenever it is for  $B$  and thus for all  $n$ -ary  $\text{bool}$ -valued function types.

More generally, this degeneration effect occurs for every base type that is built into both DHOL and HOL and that is translated to itself.  $\text{bool}$  is the simplest example of that kind, and the only one in the setting described here. But reasonable language extensions like built-in base types  $a$  for numbers, strings, etc. would suffer from the same issue. This is because all of these types would come with built-in induction principles that derive a universal property from its ground instances, at which point  $a^* x x$  becomes trivial.

Note, however, that the degeneration effect does *not* occur for *user-declared* base types. For example, consider a theory that declares a base type  $N$  for the natural numbers and an induction axiom for it.  $N$  would not be translated to itself but to a fresh HOL-type in whose induction axiom the quantifier  $\forall$  is relativized by  $N^* x x$ . Consequently,  $N^* x x$  is not trivial and can be used to reject spurious terms.

These examples show that we cannot expect the reverse directions of the statements in Thm. 4 to hold in general. However, we can show the following property that is sufficient to make our translation well-behaved:

**Theorem 2 (Soundness).** *Assume a well-formed DHOL-theory  $\vdash T$  Thy.*

$$\text{If } \Gamma \vdash_T F : \text{bool} \text{ and } \bar{\Gamma} \vdash_{\bar{T}} \bar{F}, \text{ then } \Gamma \vdash_T F$$

*In particular, if  $\Gamma \vdash_T s : A$  and  $\Gamma \vdash_T t : A$  and  $\bar{\Gamma} \vdash_{\bar{T}} A^* \bar{s} \bar{t}$ , then  $\Gamma \vdash s =_A t$ .*

*Proof.* The key idea is to transform a HOL-proof of  $\bar{F}$  into one that is in the image of the translation, at which point we can read off a DHOL-proof of  $F$ . The full proof is given in the appendix.

Intuitively, the reverse directions of Thm. 4 hold if we have already established that all involved expressions are well-typed in DHOL. Thus, we *can* use a HOL-ATP to prove DHOL-conjectures if we validate independently that the conjecture is well-typed to begin with. In the remainder of this section, we develop the necessary type-checking algorithm for DHOL.

*Type-Checking* Inspecting the rules of DHOL, we observe that all DHOL-judgments would be decidable if we had an oracle for the validity judgment  $\Gamma \vdash_T F$ . Indeed, our DHOL-rules are already written in a way that essentially allows reading off a bidirectional type-checking algorithm. It only remains to split the typing judgment  $\Gamma \vdash_T t : A$  into two algorithms for type-inference (which computes  $A$  from  $t$ ) and type-checking (which takes  $t$  and  $A$  and returns yes or no) and to aggregate the rules for subtyping into an appropriate pattern-match.

The construction is routine, and we have implemented the resulting algorithm in our MMT/LF logical framework [19,12].<sup>7</sup> The oracle for the validity judgment is provided by our translation and a theorem prover for HOL (see Sect. 6). It remains to show that whenever the algorithm calls the oracle for  $\Gamma \vdash_T F$ , we do in fact have that  $\Gamma \vdash_T F : \text{bool}$  so that Thm. 2 is applicable. Formally, we show the following:

**Theorem 3.** *Relative to an oracle for  $\Gamma \vdash_T F$ , consider a derivation of some DHOL-judgment, in which the children of each node are ordered according to the left-to-right order of the assumptions in the statement of the applied rule.*

*If the oracle calls are made in depth-first order, then each such call satisfies  $\Gamma \vdash_T F : \text{bool}$ .*

*Proof.* We actually prove, by induction on derivations, the more general statement requires that each rule preserves the following preconditions:

Judgment	Precondition
$\vdash_T \Gamma \text{Ctx}$	$\vdash T \text{Thy}$
$\Gamma \vdash_T A \text{tp}$	$\vdash_T \Gamma \text{Ctx}$
$\Gamma \vdash_T t : A$	$\Gamma \vdash_T A \text{tp}$ (post-condition when used as type-inference)
$\Gamma \vdash_T F$	$\Gamma \vdash_T F : \text{bool}$
$\Gamma \vdash_T A \equiv B$ or $\Gamma \vdash_T A <: B$	$\Gamma \vdash_T A \text{tp}$ and $\Gamma \vdash_T B \text{tp}$

Note that rules whose conclusion is a validity judgment can be ignored because they are replaced by the oracle anyway.

The most interesting case is the rule for  $\Gamma \vdash_T a s_1 \dots s_n \equiv a t_1 \dots t_n$ . Here, the left-to-right order of assumptions is critical because  $\Gamma \vdash_T s_1 =_{A_1} t_1$  may be needed to show, e.g.,  $\Gamma \vdash_T s_2 =_{A_2[s_1/i_1]} t_2 : \text{bool}$ .

## 6 Theorem Prover Implementation

We have integrated our translation as a preprocessor to the HOL ATP LEO-III [22]. We chose this ATP because its existing preprocessor infrastructure already includes a powerful logic embedding tool [20,21].<sup>8</sup> However, with a little more effort, other HOL ATPs work as well.

Furthermore, we developed a bridge between the MMT logical framework [19] and LEO-III (both of which are written in the same programming language).<sup>9</sup> This allows us to

<sup>7</sup> The formalization of DHOL in MMT is available at [https://gl.mathhub.info/MMT/LATIN2/-/blob/devel/source/logic/hol\\_like/dhol.mmt](https://gl.mathhub.info/MMT/LATIN2/-/blob/devel/source/logic/hol_like/dhol.mmt). The example theories given throughout this paper and a few example conjectures are available at <https://gl.mathhub.info/MMT/LATIN2/-/blob/devel/source/casestudies/2023-cade>.

<sup>8</sup> Our implementation can be found at <https://github.com/leoprover/logic-embedding/blob/master/embedding-runtime/src/main/scala/leo/modules/embeddings/DHOLEmbedding.scala>.

<sup>9</sup> Our implementation can be found at <https://gl.mathhub.info/MMT/LATIN2/-/tree/devel/scala/latin2/tptp>.

use our MMT-based type-checker for DHOL with our Leo-III-based theorem prover to obtain a full-fledge implementation of DHOL. Moreover, this system can immediately use MMT’s logic-independent frontend features like IDE and module system.

Alternatively, we can use LEO-III as a general purpose DHOL-ATP that accepts input in TPTP. Even though TPTP does not officially sanction DHOL as a logic, it anticipates dependent function types and already provides syntax for them (although — to our knowledge — no ATP system has made use of it so far). Concretely, TPTP represents the type  $\Pi x : A. B$  as  $!>[X:A]:B$  and a base type  $a\ t_1 \dots t_n$  as  $@\ t_1 \dots @\ t_n$ . TPTP does not yet provide syntax for predicate subtypes, i.e., this approach is currently limited to the no-subtyping fragment of DHOL. But extending the TPTP syntax with predicate subtypes would be straightforward, e.g., by using  $A\ ?| \ p$  to represent the type  $A|_p$ .

The encoding of the conjecture given in Ex. 3 using the theory from Ex. 1 is given at <https://gl.mathhub.info/MMT/LATIN2/-/blob/devel/source/casestudies/2023-cade/CategoryTheory/category-theory-lemmas-dhol.p> (which also includes further example conjectures relative to the same theory). Running the logic embedding tool translates it into the TPTP TH0 problem given at <https://gl.mathhub.info/MMT/LATIN2/-/blob/devel/source/casestudies/2023-cade/CategoryTheory/category-theory-lemmas-hol.p>. Unsurprisingly, LEO-III can prove this simple theorem easily.

*Practical evaluation* In order to evaluate the practical usefulness of the translation we studied various example conjectures about function composition in set theory and category theory. We considered 5 further lemmas based on the theory in Ex. 1 which are written directly in TPTP and can all be proven by E, Vampire and cvc5. We also studied various harder lemmas about function composition and category theory. Those examples are written in MMT and take advantage of advanced MMT features to improve readability, such as definitions, user-defined notations, and implicit arguments that are inferred by the prover.

The examples can be found at <https://gl.mathhub.info/MMT/LATIN2/-/blob/devel/source/casestudies/2023-cade>. The MMT prover successfully type-checks all problems and translates them into TPTP problems to be solved by HOL ATPs.

Since LEO-III can solve none of the 6 function composition examples, we also tested other HOL ATPs on the generated TPTP problems. Running all HOL ATP provers supported at <https://www.tptp.org/cgi-bin/SystemOnTPTP> on the function composition problems shows that many provers can solve 3 of the problems, Vampire can solve 4 of them, and 5 out of the 6 conjectures can be solved by at least one HOL ATP.

We also studied 6 more difficult theorems about limits in category theory including the uniqueness, commutativity, and associativity of some limits. To better evaluate the usefulness of our translation, we also formalized these lemmas in native HOL (in MMT) and compared the results. Naturally, the DHOL formalization is significantly more readable and benefits from the more expressive type system that can help spot mistakes in the formalization. Running the HOL ATPs from <https://www.tptp.org/cgi-bin/SystemOnTPTP> on the generated TPTP problems (with 60 second timeout) yields the

results in the table below (where we omit provers that proved none of the theorems in either formalization).

HOL ATP	lemma 1 proven		lemma 2 proven		lemma 3 proven	
	DHOL	native HOL	DHOL	native HOL	DHOL	native HOL
agsyHOL	yes	no	no	no	yes	no
cocATP	yes	no	no	no	no	no
cvc5	yes	yes	no	no	yes	no
cvc5-SAT	yes	no	no	no	no	no
E	yes	yes	no	no	no	yes
HOLyHammer	yes	yes	no	no	yes	yes
Lash	yes	yes	no	no	no	no
LEO-II	yes	no	no	no	no	no
Leo-III	yes	yes	no	no	no	no
Leo-III-SAT	yes	yes	no	no	no	no
Satallax	yes	yes	no	no	yes	no
Vampire	yes	yes	no	no	no	yes
Zipperpin	yes	yes	no	no	yes	yes
total	13	9	0	0	5	4

HOL ATP	lemma 4 proven		lemma 5 proven		lemma 6 proven	
	DHOL	native HOL	DHOL	native HOL	DHOL	native HOL
agsyHOL	no	no	no	no	no	no
cocATP	no	no	no	no	no	no
cvc5	no	yes	no	no	no	no
cvc5-SAT	no	no	no	no	no	no
E	no	yes	no	yes	no	yes
HOLyHammer	no	yes	no	no	no	yes
Lash	no	no	no	no	no	no
LEO-II	no	no	no	no	no	no
Leo-III	no	no	no	no	no	no
Leo-III-SAT	no	no	no	no	no	no
Satallax	no	no	yes	no	no	no
Vampire	no	yes	no	yes	no	yes
Zipperpin	no	yes	yes	yes	no	yes
total	0	5	2	3	0	4

Overall more problems generated from the native HOL formalization can be solved by some HOL ATP (5/6 compared to 3/6 for the DHOL formalization). The HOL ATPs found 25 successful proofs for the native HOL problems and 20 for the DHOL problems. This suggests that current HOL ATPs can prove native HOL problems somewhat better than their translated DHOL counterparts, but not much better. In 8 cases a prover can prove the DHOL conjecture but not the native HOL analogue, indicating that the two formalizations have different advantages.

Furthermore, our translation has so far been engineered for generality and soundness/completeness and not for ATP efficiency. Indeed, future work has multiple options to boost the ATP performance on translated DHOL, e.g., by

- developing sufficient criteria for when simpler HOL theories can be produced
- inserting lemmas into the translated theories that guide proof search in ATPs, e.g., to speed up equality reasoning
- adding definitions to translated DHOL problems and developing better criteria when to expand them

Thus, we consider the test results to be very promising. In particular, the translation could serve as a useful basis for type-checkers and hammer tools for DHOL ITPs.

## 7 Conclusion and Future Work

We have combined two features of standard languages, higher-order logic HOL and dependent type theory DTT, thereby obtaining the new dependently-typed higher-order logic DHOL. Contrary to HOL, DHOL allows for *dependent* function types. Contrary to DTT, DHOL retains the simplicity of classical Booleans and standard equality.

On the downside, we have to accept that DHOL, unlike both HOL and DTT, has an undecidable type system. Further work will show how big this disadvantage weighs in practical theorem proving applications. But we anticipate that the drawback is manageable, especially if, as in our case, an implementation of DHOL is coupled tightly with a strong ATP system. We accomplish this with a sound and complete translation from DHOL into HOL that enables using existing HOL ATPs to discharge the proof obligations that come up during type-checking. We have implemented our novel translation as a TPTP-to-TPTP preprocessor for HOL ATP systems and outlined the implementation of a type-checker and hammer tool for DHOL based on the resulting prover.

Moreover, once this design is in place, it opens up the possibility to add certain type constructors to DHOL that are often requested by users but difficult to provide for system developers because they automatically make typing undecidable. We have shown an extension of DHOL with predicate subtypes as an example. Quotients, partial functions, or fixed-length lists are other examples that can be supported in future work.

We expect our translation remains sound and complete if DHOL is extended with other features underlying common HOL systems such as built-in types for numbers, the axiom of infinity, or the subtype definition principle. How to extend DHOL with a choice operator remains a question for future work — if solved, this would allow extending existing HOL ITPs to DHOL.

## References

1. Andrews, P.: An Introduction to Mathematical Logic and Type Theory: To Truth Through Proof. Academic Press (1986)
2. Andrews, P., Bishop, M., Issar, S., Nesmith, D., Pfenning, F., Xi, H.: TPS: A Theorem-Proving System for Classical Type Theory. *Journal of Automated Reasoning* **16**(3), 321–353 (1996)



3. Bart, J., Melham, T.: Translating dependent type theory into higher order logic. In: Bezem, M., Groote, J.F. (eds.) *Typed Lambda Calculi and Applications*. p. 209–229. Springer Berlin, Heidelberg (1993)
4. Brown, C.E.: Satallax: An automatic higher-order prover. In: Gramlich, B., Miller, D., Sattler, U. (eds.) *Automated Reasoning*. p. 111–117. Springer Berlin, Heidelberg (2012)
5. Church, A.: A Formulation of the Simple Theory of Types. *Journal of Symbolic Logic* **5**(1), 56–68 (1940)
6. Constable, R., Allen, S., Bromley, H., Cleaveland, W., Cremer, J., Harper, R., Howe, D., Knoblock, T., Mendler, N., Panangaden, P., Sasaki, J., Smith, S.: *Implementing Mathematics with the Nuprl Development System*. Prentice-Hall (1986)
7. Coq Development Team: *The Coq Proof Assistant: Reference Manual*. Tech. rep., INRIA (2015)
8. Coquand, T., Huet, G.: The Calculus of Constructions. *Information and Computation* **76**(2/3), 95–120 (1988)
9. de Moura, L., Kong, S., Avigad, J., van Doorn, F., von Raumer, J.: The Lean Theorem Prover (System Description). In: Felty, A., Middeldorp, A. (eds.) *Automated Deduction*. p. 378–388. Springer International Publishing, Cham (2015)
10. Gordon, M.: HOL: A Proof Generating System for Higher-Order Logic. In: Birtwistle, G., Subrahmanyam, P. (eds.) *VLSI Specification, Verification and Synthesis*, p. 73–128. Kluwer-Academic Publishers (1988)
11. Gordon, M., Pitts, A.: The HOL Logic. In: Gordon, M., Melham, T. (eds.) *Introduction to HOL, Part III*, p. 191–232. Cambridge University Press (1993)
12. Harper, R., Honsell, F., Plotkin, G.: A framework for defining logics. *Journal of the Association for Computing Machinery* **40**(1), 143–184 (1993)
13. Harrison, J.: HOL Light: A Tutorial Introduction. In: *Proceedings of the First International Conference on Formal Methods in Computer-Aided Design*. p. 265–269. Springer Berlin, Heidelberg (1996)
14. Martin-Löf, P.: An Intuitionistic Theory of Types: Predicative Part. In: *Proceedings of the '73 Logic Colloquium*, pp. 73–118. North-Holland (1974)
15. Norell, U.: The Agda Wiki (2005), <http://wiki.portal.chalmers.se/agda>
16. Owre, S., Rushby, J., Shankar, N.: PVS: A Prototype Verification System. In: Kapur, D. (ed.) *11th International Conference on Automated Deduction (CADE)*. pp. 748–752. Springer (1992)
17. Paulson, L.: Isabelle: A Generic Theorem Prover, *Lecture Notes in Computer Science*, vol. 828. Springer Berlin, Heidelberg (1994)
18. Pfenning, F., Schürmann, C.: System description: Twelf — a meta-logical framework for deductive systems. In: Ganzinger, H. (ed.) *Automated Deduction*. p. 202–206 (1999)
19. Rabe, F.: A Modular Type Reconstruction Algorithm. *ACM Transactions on Computational Logic* **19**(4), 1–43 (2018)
20. Steen, A.: An extensible logic embedding tool for lightweight non-classical reasoning (2022). <https://doi.org/10.48550/ARXIV.2203.12352>, [arXiv:2203.12352](https://arxiv.org/abs/2203.12352)
21. Steen, A.: Logic embedding tool 1.7 (2022), <https://doi.org/10.5281/zenodo.6139916>
22. Steen, A., Benz Müller, C.: Extensional higher-order paramodulation in Leo-III. *Journal of Automated Reasoning* **65**(6), 775–807 (2021)
23. Sutcliffe, G.: The TPTP Problem Library and Associated Infrastructure: The FOF and CNF Parts, v3.5.0. *Journal of Automated Reasoning* **43**(4), 337–362 (2009)

## A Summary of logics and translations

In this section we collect the inference rules of the logics and the definition of the overall translation. We name the rules and enumerate the cases in the definition of the translation for reference in the proofs in the subsequent appendices. We use DHOL and DHOL to refer to the variants without and with predicate subtypes.

### A.1 HOL rules

Theories and contexts:

$$\begin{array}{c} \frac{}{\vdash \circ \text{Thy}} \text{thyEmpty} \quad \frac{\vdash T \text{Thy}}{\vdash T, a \text{tp} \text{Thy}} \text{thyType} \quad \frac{\vdash_T A \text{tp}}{\vdash T, c : A \text{Thy}} \text{thyConst} \quad \frac{\vdash_T F : \text{bool}}{\vdash T, c : F \text{Thy}} \text{thyAxiom} \\[10pt] \frac{\vdash T \text{Thy}}{\vdash_T \cdot \text{Ctx}} \text{ctxEmpty} \quad \frac{\vdash_T A \text{tp}}{\vdash_T \Gamma, x : A \text{Ctx}} \text{ctxVar} \quad \frac{\vdash_T F : \text{bool}}{\vdash_T \Gamma, x : F \text{Ctx}} \text{ctxAssume} \end{array}$$

Lookup in theory and context:

$$\begin{array}{c} \frac{a : \text{tp in } T \quad \vdash_T \Gamma \text{Ctx}}{\vdash_T a \text{tp}} \text{type} \quad \frac{c : A' \text{ in } T \quad \vdash_T A' \equiv A}{\vdash_T c : A} \text{const} \quad \frac{c : F \text{ in } T \quad \vdash_T \Gamma \text{Ctx}}{\vdash_T F} \text{axiom} \\[10pt] \frac{x : A' \text{ in } \Gamma \quad \vdash_T A' \equiv A}{\vdash_T x : A} \text{var} \quad \frac{x : F \text{ in } \Gamma \quad \vdash_T \Gamma \text{Ctx}}{\vdash_T F} \text{assume} \end{array}$$

Well-formedness and equality of types:

$$\frac{\vdash_T \Gamma \text{Ctx}}{\vdash_T \text{bool tp}} \text{bool} \quad \frac{\vdash_T A \text{tp} \quad \vdash_T B \text{tp}}{\vdash_T A \rightarrow B \text{tp}} \text{arrow} \quad \frac{\vdash_T A \text{tp}}{\vdash_T A \equiv A} \text{congBase} \quad \frac{\vdash_T A \equiv A' \quad \vdash_T B \equiv B'}{\vdash_T A \rightarrow B \equiv A' \rightarrow B'} \text{cong} \rightarrow$$

Typing:

$$\frac{\Gamma, x : A \vdash_T t : B}{\vdash_T (\lambda x : A. t) : A \rightarrow B} \text{lambda} \quad \frac{\Gamma \vdash_T f : A \rightarrow B \quad \Gamma \vdash_T t : A}{\vdash_T f t : B} \text{appl} \quad \frac{\Gamma \vdash_T s : A \quad \Gamma \vdash_T t : A}{\vdash_T s =_A t : \text{bool}} \text{=type}$$

Term equality: congruence, reflexivity, symmetry,  $\beta$ ,  $\eta$

$$\begin{array}{c} \frac{\Gamma \vdash_T A \equiv A' \quad \Gamma, x : A \vdash_T t =_B t'}{\vdash_T \lambda x : A. t =_{A \rightarrow B} \lambda x : A'. t'} \text{cong} \lambda \text{ (xi)} \quad \frac{\Gamma \vdash_T t =_A t' \quad \Gamma \vdash_T f =_{A \rightarrow B} f'}{\vdash_T f t =_B f' t'} \text{congAppl} \\[10pt] \frac{\Gamma \vdash_T t : A}{\vdash_T t =_A t} \text{refl} \quad \frac{\Gamma \vdash_T t =_A s}{\vdash_T s =_A t} \text{sym} \quad \frac{\Gamma \vdash_T (\lambda x : A. s) t : B}{\vdash_T (\lambda x : A. s) t =_B s[t/x]} \text{beta} \quad \frac{\Gamma \vdash_T t : A \rightarrow B \quad x \text{ not in } \Gamma}{\vdash_T t =_{A \rightarrow B} \lambda x : A. t x} \text{eta} \end{array}$$

Rules for implication:

$$\frac{\Gamma \vdash_T F : \text{bool} \quad \Gamma \vdash_T G : \text{bool}}{\vdash_T F \Rightarrow G : \text{bool}} \Rightarrow \text{type} \quad \frac{\Gamma \vdash_T F : \text{bool} \quad \Gamma, x : F \vdash_T G}{\vdash_T F \Rightarrow G} \Rightarrow \text{I} \quad \frac{\Gamma \vdash_T F \Rightarrow G \quad \Gamma \vdash_T F}{\vdash_T G} \Rightarrow \text{E}$$

Congruence for validity, Boolean extensionality, and non-emptiness of types:

$$\frac{\Gamma \vdash_T F =_{\text{bool}} F' \quad \Gamma \vdash_T F'}{\vdash_T F} \text{cong} \vdash \quad \frac{\Gamma \vdash_T p \text{ true} \quad \Gamma \vdash_T p \text{ false}}{\vdash_T x : \text{bool} \vdash_T p x} \text{boolExt} \quad \frac{\Gamma \vdash_T F : \text{bool} \quad \Gamma, x : A \vdash_T F}{\vdash_T F} \text{nonempty}$$

Fig. 3. HOL Rules

## A.2 DHOL rules

$$\begin{array}{c}
\frac{\vdash_T x_1 : A_1, \dots, x_n : A_n \text{ Ctx}}{\vdash_T, a : \Pi x_1 : A_1. \dots \Pi x_n : A_n. \text{tp} \text{ Thy}} \text{thyType}' \\
\frac{a : \Pi x_1 : A_1. \dots \Pi x_n : A_n. \text{tp} \text{ in } T \vdash_T \Gamma \text{ Ctx} \quad \Gamma \vdash_T t_1 : A_1 \quad \dots \quad \Gamma \vdash_T t_n : A_n[x_1/i_1] \dots [x_{n-1}/i_{n-1}]}{\Gamma \vdash_T a t_1 \dots t_n \text{tp}} \text{type}' \\
\frac{\Gamma \vdash_T A \text{tp} \quad \Gamma, x : A \vdash_T B \text{tp}}{\Gamma \vdash_T \Pi x : A. B \text{tp}} \text{pi} \quad \frac{\Gamma \vdash_T A \equiv A' \quad \Gamma, x : A \vdash_T B \equiv B'}{\Gamma \vdash_T \Pi x : A. B \equiv \Pi x : A'. B'} \text{congPi} \\
\frac{a : \Pi x_1 : A_1. \dots \Pi x_n : A_n. \text{tp} \text{ in } T \vdash_T \Gamma \text{ Ctx} \quad \Gamma \vdash_T s_1 =_{A_1} t_1 \quad \dots \quad \Gamma \vdash_T s_n =_{A_n[x_1/i_1] \dots [x_{n-1}/i_{n-1}]} t_n}{\Gamma \vdash_T a s_1 \dots s_n \equiv a t_1 \dots t_n} \text{congBase}' \\
\frac{\Gamma, x : A \vdash_T t : B}{\Gamma \vdash_T (\lambda x : A. t) : \Pi x : A. B} \text{lambda}' \quad \frac{\Gamma \vdash_T f : \Pi x : A. B \quad \Gamma \vdash_T t : A}{\Gamma \vdash_T f t : B[x/i]} \text{appl}' \\
\frac{\Gamma \vdash_T F : \text{bool} \quad \Gamma, \text{ass} : F \vdash_T G : \text{bool}}{\Gamma \vdash_T F \Rightarrow G : \text{bool}} \Rightarrow \text{type}' \\
\frac{\Gamma \vdash_T t =_A t' \quad \Gamma \vdash_T f =_{\Pi x : A. B} f'}{\Gamma \vdash_T f t =_B f' t'} \text{congAppl}' \quad \frac{\Gamma \vdash_T A \equiv A' \quad \Gamma, x : A \vdash_T t =_B t'}{\Gamma \vdash_T \lambda x : A. t =_{\Pi x : A. B} \lambda x : A'. t'} \text{cong}\lambda' \\
\frac{\Gamma \vdash_T t : \Pi x : A. B}{\Gamma \vdash_T t =_{\Pi x : A. B} \lambda x : A. t x} \text{etaPi}
\end{array}$$

## A.3 DHOL rules

$$\begin{array}{c}
\frac{c : A' \text{ in } T \quad \Gamma \vdash_T A' <: A}{c : A} \text{const}' \quad \frac{x : A' \text{ in } \Gamma \quad \Gamma \vdash_T A' <: A}{x : A} \text{var}' \\
\frac{\Gamma \vdash_T A' <: A \quad \Gamma, x : A' \vdash_T B <: B'}{\Gamma \vdash_T \Pi x : A. B <: \Pi x : A'. B'} <:\text{Pi} \\
\frac{\Gamma \vdash_T A <: A' \quad \Gamma, x : A \vdash_T p x \Rightarrow p' x}{\Gamma \vdash_T A|_p <: A'|_{p'}} <:|_p \quad \frac{\Gamma \vdash_T A <: A'}{\Gamma \vdash_T A|_p <: A'} <:\text{Top} \\
\frac{\Gamma \vdash_T A \equiv A'}{\Gamma \vdash_T A <: A'} <:\text{I} \quad \frac{\Gamma \vdash_T A \text{tp}}{\Gamma \vdash_T A \equiv A|_{\lambda x : A. \text{true}}} |_{\text{triv}} \quad \frac{\Gamma \vdash_T A \text{tp}}{\Gamma \vdash_T A|_{\lambda x : A. \text{true}}} |_{\text{triv}}' \\
\frac{\Gamma \vdash_T A \text{tp} \quad \Gamma, x : A \vdash_T B \text{tp} \quad \Gamma, x : A \vdash_T p : \Pi y : B. \text{bool}}{\Gamma \vdash_T \Pi x : A. B|_p \equiv \Pi x : A. B|_{\lambda f : \Pi x : A. B. \forall x : A. p(f x)}} \pi|_p \text{Cod} \\
\frac{\Gamma \vdash_T A \text{tp} \quad \Gamma \vdash_T p : \Pi x : A. \text{bool} \quad \Gamma \vdash_T q : \Pi x : A. \text{bool}}{\Gamma \vdash_T A|_p|_q \equiv A|_{\lambda x : A. p x \wedge q x}} |_p|_q \\
\frac{\Gamma \vdash_T p : \Pi x : A. \text{bool}}{\Gamma \vdash_T A|_p \text{tp}} |_p \text{tp} \quad \frac{\Gamma \vdash_T A \equiv A' \quad \Gamma \vdash_T p =_{\Pi x : A. \text{bool}} p'}{\Gamma \vdash_T A|_p \equiv A'|_{p'}} |_p \equiv \\
\frac{\Gamma \vdash_T t : A \quad \Gamma \vdash_T p t}{\Gamma \vdash_T t : A|_p} |_p \text{I} \quad \frac{\Gamma \vdash_T t : A|_p}{\Gamma \vdash_T p t} |_p \text{E}
\end{array}$$

#### A.4 The translation from DHOL into HOL

**Definition 3 (Translation).** We define a translation from DHOL to HOL syntax by induction on the Grammar.

We use the notation  $\overline{x : A}, \overline{\Pi x : A.}$  and  $\overline{A}, \overline{x}$  to denote  $x : A_1, \dots, x_n : A_n, \Pi x_1 : A_1. \dots \Pi x_n : A_n$ , and  $A_1 \rightarrow \dots \rightarrow A_n, x_1 \dots x_n$  respectively.

The cases for theories and contexts are:

$$\begin{aligned} \overline{0} &:= 0 & (PT1) \\ \overline{T}, \overline{D} &:= \overline{T}, \overline{D} & \text{where} \\ \overline{a : \Pi x : A. tp} &:= a : tp, \\ \overline{a^* : \overline{A} \rightarrow a \rightarrow a \rightarrow \text{bool}}, \\ \overline{a_{trans} : \forall x : \overline{A}. \forall u, v, w : a. (a \overline{x})^* u v \Rightarrow ((a \overline{x})^* v w \Rightarrow (a \overline{x})^* u w)}, \\ \overline{a_{sym} : \forall x : \overline{A}. \forall u, v : a. (a \overline{x})^* u v \Rightarrow (a \overline{x})^* v u}, \\ \overline{a_{PER} : \forall x : \overline{A}. \forall u, v : a. (a \overline{x})^* u v \Rightarrow (a \overline{x})^* u v =_{\text{bool}} u =_a v} & (PT2) \\ \overline{c : A} &:= c : \overline{A}, \quad \overline{c^* : A^* c c} & (PT3) \\ \overline{ax : F} &:= ax : \overline{F} & (PT4) \\ \overline{\vdots} &:= . & (PT5) \\ \overline{\Gamma, x : A} &:= \overline{\Gamma}, x : \overline{A}, x^* : A^* x x & (PT6) \\ \overline{\Gamma, ass : F} &:= \overline{\Gamma}, ass : \overline{F} & (PT7) \end{aligned}$$

The case of  $\overline{A}$  and  $A^* s t$  for types  $A$  are:

$$\begin{aligned} \overline{(a t_1 \dots t_n)} &:= a & (PT8) \\ \overline{(a t_1 \dots t_n)^* s t} &:= a^* \overline{t_1} \dots \overline{t_n} s t & (PT9) \\ \overline{\Pi x : A. B} &:= \overline{A} \rightarrow \overline{B} & (PT10) \\ \overline{(\Pi x : A. B)^* f g} &:= \forall x, y : \overline{A}. A^* x y \Rightarrow B^* (f x) (g y) & (PT11) \\ \overline{\text{bool}} &:= \text{bool} & (PT12) \\ \overline{\text{bool}^* s t} &:= s =_{\text{bool}} t & (PT13) \\ \overline{A|_p} &:= \overline{A} & (PT14) \\ \overline{(A|_p)^* s t} &:= A^* s t \wedge \overline{p} s \wedge \overline{p} t & (PT15) \end{aligned}$$

The cases for terms are:

$$\begin{aligned} \overline{c} &:= c & (PT16) \\ \overline{x} &:= x & (PT17) \\ \overline{\lambda x : A. t} &:= \lambda x : \overline{A}. \overline{t} & (PT18) \end{aligned}$$

$$\overline{f\ t} := \overline{f}\ \overline{t} \quad (\text{PT19})$$

$$\overline{F \Rightarrow G} := \overline{F} \Rightarrow \overline{G} \quad (\text{PT20})$$

$$\overline{s =_A t} := A^* \overline{s}\ \overline{t} \quad (\text{PT21})$$

### A.5 Admissible rules for HOL

The following lemma collects a few routine meta-theorems that we make use of later on:

**Lemma 1.** *Given the inference rules for HOL (cfg. Figure 3), the following rules are admissible:*

$$\begin{array}{c}
\frac{\Gamma \vdash_T \text{Ctx}}{\vdash T \text{Thy}} \text{ctxThy} \quad \frac{\Gamma \vdash_T A \text{tp}}{\vdash_T \Gamma \text{Ctx}} \text{tpCtx} \quad \frac{\Gamma \vdash_T t : A}{\vdash_T A \text{tp}} \text{typingTp} \quad \frac{\Gamma \vdash_T F}{\vdash_T F : \text{bool}} \text{validTyping} \\
\\
\frac{c : A \text{ in } T}{\vdash_T c : A} \text{constS} \quad \frac{x : A \text{ in } \Gamma}{\vdash_T x : A} \text{varS} \\
\frac{\Gamma \vdash_T A \text{tp}}{\vdash_T A \equiv A} \equiv \text{refl} \quad \frac{\Gamma \vdash_T A \equiv A'}{\vdash_T A' \equiv A} \equiv \text{sym} \quad \frac{\Gamma \vdash_T A \equiv A' \quad \Gamma \vdash_T A' \equiv A''}{\vdash_T A \equiv A''} \equiv \text{trans} \\
\frac{\Gamma \vdash_T s =_A t}{\vdash_T s : A} \text{eqTyping} \quad \frac{\Gamma \vdash_T F \Rightarrow G}{\vdash_T F : \text{bool}} \text{implTypingL} \quad \frac{\Gamma \vdash_T F \Rightarrow G}{\vdash_T G : \text{bool}} \text{implTypingR} \\
\frac{\Gamma \vdash_T s : A \quad \Gamma \vdash_T s : A'}{\vdash_T A \equiv A'} \text{typesUnique} \quad \frac{\Gamma \vdash_T f t : B \quad \Gamma \vdash_T f : A \rightarrow B}{\vdash_T t : A} \text{typingWf} \\
\frac{\Gamma \vdash_T t : A \quad \Gamma \vdash_T f t : B}{\vdash_T f : A \rightarrow B} \text{applType} \quad \frac{\Gamma, x : B \vdash_T s : A \quad \Gamma \vdash_T t : B}{\vdash_T s[x/i] : A} \text{rewriteTyping} \\
\frac{\Gamma \vdash_T F : \text{bool} \quad \Gamma \vdash_T G}{\vdash_T F \Rightarrow G} \text{monotonic} \vdash \quad \frac{\Gamma \vdash_T A \text{tp} \quad \Gamma \vdash_T J \quad \text{for any statement } \vdash_T J}{\vdash_T J} \text{var} \vdash \\
\frac{\Gamma, x : A \vdash_T F : \text{bool}}{\vdash_T \forall x : A. F : \text{bool}} \forall \text{type} \quad \frac{\Gamma, x : A \vdash_T F}{\vdash_T \forall x : A. F} \forall I \quad \frac{\Gamma \vdash_T \forall x : A. F \quad \Gamma \vdash_T t : A}{\vdash_T F[x/i]} \forall E \\
\frac{\Gamma \text{Ctx} \quad F \text{ in } \Gamma}{\vdash_T F : \text{bool}} \text{assTyping} \quad \frac{\Gamma \vdash_T t =_A t' \quad \Gamma \vdash_T A \equiv A' \quad \Gamma \vdash_T t : A'}{\vdash_T t' : A'} \text{cong} : \\
\frac{\Gamma, \text{ass} : F \vdash_T G \quad \Gamma, \text{ass}_G : G \vdash_T F}{\vdash_T F =_{\text{bool}} G} \text{propExt} \quad \frac{\Gamma, x : A \vdash_T f x =_B f' x}{\vdash_T f =_{A \rightarrow B} f'} \text{extensionality} \\
\frac{\Gamma \vdash_T s =_A t \quad \Gamma \vdash_T t =_A u}{\vdash_T s =_A u} \text{trans} \quad \frac{\Gamma \vdash_T s =_A s' \quad \Gamma \vdash_T t =_A t'}{\vdash_T (s =_A t) =_{\text{bool}} (s' =_A t')} = \text{cong} \\
\frac{\Gamma \vdash_T A \equiv A' \quad \Gamma, x : A \vdash_T F =_{\text{bool}} F'}{\vdash_T \forall x : A. F =_{\text{bool}} \forall x : A'. F'} \forall \text{cong} \quad \frac{\Gamma \vdash_T F =_{\text{bool}} F' \quad \Gamma \vdash_T G =_{\text{bool}} G'}{\vdash_T F \Rightarrow G =_{\text{bool}} F' \Rightarrow G'} \Rightarrow \text{cong} \\
\frac{\Gamma, x : A \vdash_T F \Rightarrow G}{\vdash_T \forall x : A. F \Rightarrow \forall x : A. G} \forall \Rightarrow \quad \frac{\Gamma \vdash_T G \Rightarrow G' \quad \Gamma \vdash_T F' \Rightarrow F}{\vdash_T (F \Rightarrow G) \Rightarrow (F' \Rightarrow G')} \Rightarrow \text{Funct} \\
\frac{\Gamma \vdash_T F =_{\text{bool}} F' \quad \Gamma \vdash_T F}{\vdash_T F'} \vdash \text{cong} \quad \frac{\Gamma \vdash_T F[x/i] \quad \Gamma \vdash_T t =_A t' \quad \Gamma, x : A \vdash_T F : \text{bool}}{\vdash_T F[x/i']} \text{rewrite}
\end{array}$$

*Proof (Proof of Lemma 1:).*

Regarding *(ctxThy)*, *(tpCtx)*, *(typingTp)* and *(validTyping)*: We can show these rules easily by induction on the inference rules of HOL. In each step of the induction we show that the assumptions of the rule and these four rules holding on the assumptions of the rule implies that these four rules also hold for the conclusion of the rule. In case of a validity rule this means that we need to show that the conclusion is well-typed, in case of a typing rule we need to show that the type of the term in the typing statement in the conclusion is well-formed, in case of a well-formedness rule for types we need to show that the context of the conclusion is well-formed and in case of a well-formedness rule for contexts we need to show that the theory relative to which the conclusion is stated is well-formed. These properties hold by construction of the inference rules (each inference rules makes whatever assumptions are necessary to guarantee that the inductive step in this proof works).

Regarding *(≡ refl)*, *(≡ sym)* and *(≡ trans)*: We can show them by induction on the two rules that allow showing type equality, namely *(congBase)* and *(cong→)*. The rule *(congBase)* only allows showing type equality for identical types (so symmetry is trivial and transitivity reduces to one of the two assumption of the transitivity rule). The rule *(cong→)* only allows showing type equality for  $\rightarrow$ -types  $A \rightarrow B$  and  $A' \rightarrow B'$  based on equal types  $A \equiv A'$  and  $B \equiv B'$ . Now, if the assumption of *(≡ sym)* is shown using rule *(cong→)*, by induction hypothesis we yield that the type equalities  $A \equiv A'$  and  $B \equiv B'$  satisfy symmetry and using *(cong→)* with the swapped type equalities yields  $A' \rightarrow B' \equiv A \rightarrow B$  as desired. Similarly, if  $A \rightarrow B \equiv A' \rightarrow B'$  and  $A' \rightarrow B' \equiv A'' \rightarrow B''$  are both shown using the rule *(cong→)* we have  $A \equiv A'$  and  $A' \equiv A''$  and hence by induction hypothesis  $A \equiv A''$  and  $B \equiv B''$ , so rule *(cong→)* implies  $A \rightarrow B \equiv A'' \rightarrow B''$  as desired.

Regarding *(eqTyping)*, *(implTypingL)* and *(implTypingR)*: By assumption we have  $\Gamma \vdash_T s =_A t$  resp.  $\Gamma \vdash_T F \Rightarrow G$ . By the rules *(ctxThy)*, *(tpCtx)*, *(typingTp)* and *(validTyping)* it follows that the theory  $T$  and context  $\Gamma$  must be well-formed. Since the well-formedness of a context with an additional assumption or of a theory with an additional axiom can only be shown by rule *(ctxAssume)* and *(thyAxiom)* respectively it follows that axioms in  $T$  and assumptions in  $\Gamma$  must be well-typed and that the proof of the axiom or assumption being well-typed must not use that assumption or axiom. We can then prove by induction on derivations that whenever  $\Gamma \vdash_T s =_A t$  is concluded in a step then the assumption of the step imply that  $\Gamma \vdash_T s : A$  and  $\Gamma \vdash_T t : A$  are derivable and whenever  $\Gamma \vdash_T F \Rightarrow G$  is concluded in a step  $\Gamma \vdash_T F : \text{bool}$  and  $\Gamma \vdash_T G : \text{bool}$  are derivable from the assumptions of the step and furthermore whenever we conclude a validity statement, the formula is well-typed and in all conclusions in the derivation all types and contexts are well-formed.

The the claim follows directly from using what we just proved for the step showing the assumption  $\Gamma \vdash_T s =_A t$  resp.  $\Gamma \vdash_T F \Rightarrow G$ .

Regarding *(cong:)*: This follows from the fact that provably equal types in HOL are necessarily identical, so whenever we have  $A \equiv A'$  and  $t : A$ , we already have that  $t : A'$  holds by assumption. We can show that provably equal types are identical by induction on the two type-equality rules in HOL namely *(congBase)* and *(cong→)*.

Regarding *(varS)* and *(constS)*: These follow from the fact identical types are equal (by rule *(congBase)*) and the rule *(var)* respectively *(const)*.

Regarding *(typesUnique)*: There is no rule allowing to show that a well-typed Boolean term has any other type than bool (since we only allow validity but not type equality or typing assumptions). Hence  $C, C'$  are not bool and  $s$  not of type bool. Continue by induction on the shape of  $s$ .

Depending on the shape of  $s$  at most one of the two assumption (wlog. (renaming) assume that it is  $\Gamma \vdash_T s : C$ ) can be concluded using one of the rules *(const)* or *(var)*. The other must be shown using one of the rules *(lambda)*, *(appl)* (since names of context variables and constants are mutually distinct).

In the case that rule *(lambda)* was used to show  $s : C'$  (with  $C' = A \rightarrow B'$  and  $s = \lambda x : A. t$ ) it follows from the shape of  $s$  that also  $C = A \rightarrow B$  for some type  $B$  with  $\Gamma, x : A \vdash_T t : B$  (as also  $s : C$  must be proven using rule *(lambda)*). By the induction hypothesis it follows that then  $\Gamma, x : A \vdash_T B \equiv B'$ . Since equal types in HOL must be identical (see proof of rule *(cong)*), it follows that  $\Gamma \vdash_T B \equiv B'$ . Rule *(cong $\rightarrow$ )* then implies the claim of  $\Gamma \vdash_T C \equiv C'$ .

In the case that rule *(appl)* was used to show  $s : C'$  (with  $C' = B'$  and  $s = f t$  and  $\Gamma \vdash_T f : A' \rightarrow B'$  and  $\Gamma \vdash_T t : A'$ ) it follows from the shape of  $s$  that also  $C = B$  for some type  $B$  with  $\Gamma \vdash_T f : A \rightarrow B$  and  $\Gamma \vdash_T t : A$ . By the induction hypothesis (applied to  $f$  and  $t$ ) it follows that  $\Gamma \vdash_T A \rightarrow B \equiv A' \rightarrow B'$  and  $\Gamma \vdash_T A \equiv A'$ . Since equal types in HOL are identical it follows that also  $\Gamma \vdash_T B \equiv B'$  holds, so by assumption the conclusion holds.

Regarding *(typingWf)*: The first assumption can only be proven using rule *(appl)*. In the first case the conclusion is an assumption of the rule used to prove  $\Gamma \vdash_T f t : B$  and must therefore hold.

Regarding *(monotonic $\vdash$ )* and *(var $\vdash$ )*: The idea for showing this is observing that adding additional variables or assumptions to the contexts occurring in a derivation will always result in another (equally valid) derivation. This can be shown by induction on derivations. If in a derivation some rule is used to conclude  $\Gamma \vdash_T F$  and adding additional variables and assumptions to  $\Gamma$  as well as the contexts of all judgements appearing in those derivations leaves those derivations valid, then we need to show that also the assumptions of the rule are still satisfied. Since we have valid derivations for all assumptions that are judgements themselves, we only need to check assumptions of rules that are not judgements. The only assumptions of this kind that appear in inference rules are assumptions that some variable or context assumption is contained in a context. Adding further assumptions or variables will not make this false if it was true initially.

This proves that *(monotonic $\vdash$ )* and *(var $\vdash$ )* hold.

Regarding *(rewriteTyping)*: This can be seen by applying the substitution  $\cdot[x/i]$  to the terms in the derivation (but not the variable declaration  $x$  in the context itself) of  $\Gamma, x : B \vdash_T s : A$ , using the fact that  $\Gamma \vdash_T t : B$  holds instead of rule *(var)* (that may be used

to conclude  $\Gamma, x : B \vdash_T x : B$  in the original declaration). This leads to a derivation of the conclusion  $\Gamma, x : A \vdash_T s[x/i] : A$ . Since  $x$  doesn't appear in the derivation, removing the variable declaration  $x : A$  from the context leads to a valid derivation of  $\Gamma \vdash_T s[x/i] : A$  as desired.

Regarding (*assTyping*):

$\vdash \Gamma \text{Ctx}$	by assumption	(1)
$\vdash F \text{ in } \Gamma$	by assumption	(2)
$\Gamma \vdash F$	( <i>assume</i> ),(2),(1)	(3)
$\Gamma \vdash F : \text{bool}$	( <i>validTyping</i> ),(3)	(4)

Regarding (*forallType*):

$\Gamma, x : A \vdash_T F : \text{bool}$	by assumption	(5)
$\Gamma \vdash_T \lambda x : A. F : A \rightarrow \text{bool}$	( <i>lambda</i> ),(5)	(6)
$\Gamma, x : A \vdash_T \text{true} : \text{bool}$	by definition	(7)
$\Gamma \vdash_T \lambda x : A. \text{true} : A \rightarrow \text{bool}$	( <i>lambda</i> ),(7)	(8)
$\Gamma \vdash_T \lambda x : A. F =_{\text{bool}} \lambda x : A. \text{true} : \text{bool}$	( <i>=type</i> ),(6),(8)	(9)
$\Gamma \vdash_T \forall x : A. F : \text{bool}$	by definition,(9)	(10)

Regarding (*forallE*):

$\Gamma \vdash_T \forall x : A. F$	by assumption	(11)
$\Gamma \vdash_T t : A$	by assumption	(12)
$\Gamma \vdash_T \lambda x : A. F =_{A \rightarrow \text{bool}} \lambda x : A. \text{true}$	by definition,(11)	(13)
$\Gamma \vdash_T t =_A t$	( <i>refl</i> ),(12)	(14)
$\Gamma \vdash_T (\lambda x : A. F) t =_{\text{bool}} (\lambda x : A. \text{true}) t$	( <i>congAppl</i> ),(13),(14)	(15)
$\Gamma \vdash_T (\lambda x : A. \text{true}) t =_{\text{bool}} (\lambda x : A. F) t$	( <i>sym</i> ),(15)	(16)
$\Gamma \vdash_T (\lambda x : A. F) t : \text{bool}$	( <i>eqTyping</i> ),(15)	(17)
$\Gamma \vdash_T (\lambda x : A. \text{true}) t : \text{bool}$	( <i>eqTyping</i> ),(16)	(18)
$\Gamma \vdash_T (\lambda x : A. F) t =_{\text{bool}} F[x/i]$	( <i>beta</i> ),(univE6)	(19)
$\Gamma \vdash_T (\lambda x : A. \text{true}) t =_{\text{bool}} \text{true}$	( <i>beta</i> ),(univE6)	(20)
$\Gamma \vdash_T F[x/i] =_{\text{bool}} (\lambda x : A. \text{true}) t$	( <i>rewrite</i> ),(15),(19)	(21)
$\Gamma \vdash_T F[x/i] =_{\text{bool}} \text{true}$	( <i>rewrite</i> ),(21),(20)	(22)
$\Gamma \vdash_T \text{true}$	( <i>refl</i> ),definition	(23)
$\Gamma \vdash_T F[x/i]$	( <i>congl</i> ),(20),(23)	(24)

Regarding (*propExt*):

$\Gamma, \text{ass}_F : F \vdash_T G$	by assumption	(25)
---------------------------------------	---------------	------



$\Gamma, ass_F : F \vdash_T G : \text{bool}$	(validTyping),(25)	(26)
$\vdash_T \Gamma, ass : F \text{ Ctx}$	(tpCtx),(26)	(27)
$\Gamma \vdash_T F : \text{bool}$	(assTyping),(27)	(28)
$\Gamma, ass_G : G \vdash_T F$	by assumption	(29)
$\Gamma, ass_G : G \vdash_T F : \text{bool}$	(validTyping),(25)	(30)
$\vdash_T \Gamma, ass_G : G \text{ Ctx}$	(tpCtx),(30)	(31)
$\Gamma \vdash_T G : \text{bool}$	(assTyping),(31)	(32)
$\Gamma \vdash_T \text{true} : \text{bool}$	by definition	(33)
$\Gamma \vdash_T \text{false} : \text{bool}$	by definition	(34)
$\Gamma \vdash_T F \Rightarrow G$	( $\Rightarrow I$ ),(28),(25)	(35)
$\Gamma \vdash_T G \Rightarrow F$	( $\Rightarrow I$ ),(32),(29)	(36)
$\Gamma \vdash_T \text{true} =_{\text{bool}} \text{true}$	(refl),(33)	(37)
$\Gamma \vdash_T \text{true} \Rightarrow \text{true} : \text{bool}$	( $\Rightarrow \text{type}$ ),(33),(33)	(38)
$\Gamma, ass1 : \text{true} \Rightarrow \text{true} \vdash_T \text{true} =_{\text{bool}} \text{true}$	(monotonic $\vdash$ ),(38),(37)	(39)
$\Gamma \vdash_T (\text{true} \Rightarrow \text{true}) \Rightarrow \text{true} =_{\text{bool}} \text{true}$	( $\Rightarrow I$ ),(38),(39)	(40)
$\Gamma, ass1 : \text{true} \Rightarrow \text{true} \vdash_T (\text{true} \Rightarrow \text{true}) \Rightarrow \text{true} =_{\text{bool}} \text{true}$	(monotonic $\vdash$ ),(38),(40)	(41)
$\Gamma \vdash_T (\text{true} \Rightarrow \text{true}) \Rightarrow ((\text{true} \Rightarrow \text{true}) \Rightarrow \text{true} =_{\text{bool}} \text{true})$	( $\Rightarrow I$ ),(38),(41)	(42)
Analogously we can show:		
$\Gamma \vdash_T (\text{false} \Rightarrow \text{false}) \Rightarrow ((\text{false} \Rightarrow \text{false}) \Rightarrow \text{false} =_{\text{bool}} \text{false})$	analogous to (42)	(43)
$\Gamma \vdash_T \text{true} \Rightarrow \text{false} : \text{bool}$	( $\Rightarrow \text{type}$ ),(33),(34)	(44)
$\vdash_T \Gamma, ass2 : \text{true} \Rightarrow \text{false} \text{ Ctx}$	(ctxAssume),(44)	(45)
$\Gamma, ass2 : \text{true} \Rightarrow \text{false} \vdash_T \text{true} \Rightarrow \text{false} : \text{bool}$	( $\Rightarrow \text{type}$ ),(monotonic $\vdash$ ),(44),(33),(monotonic $\vdash$ ),(44),(34)	(46)
$\Gamma \vdash_T \text{false} \Rightarrow \text{true} : \text{bool}$	( $\Rightarrow \text{type}$ ),(34),(33)	(47)
$\Gamma, ass2 : \text{false} \Rightarrow \text{true} \vdash_T \text{false} \Rightarrow \text{true} : \text{bool}$	( $\Rightarrow \text{type}$ ),(monotonic $\vdash$ ),(44),(34),(monotonic $\vdash$ ),(44),(33)	(48)
$\Gamma \vdash_T \text{true}$	(refl),(33)	(49)
$\Gamma, ass2 : \text{true} \Rightarrow \text{false} \vdash_T \text{true} \Rightarrow \text{false}$	(assume),(45)	(50)
$\Gamma, ass2 : \text{true} \Rightarrow \text{false} \vdash_T \text{false}$	( $\Rightarrow E$ ),(50),(49)	(51)
$\Gamma, ass2 : \text{true} \Rightarrow \text{false} \vdash_T \text{true}$	(monotonic $\vdash$ ),(44),(49)	(52)
$\Gamma, ass2 : \text{true} \Rightarrow \text{false}, y : \text{bool} \vdash_T y : \text{bool}$	(varS),(ctxVar),(45)	(53)

$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T \lambda y : \text{bool}. y : \text{bool} \rightarrow \text{bool}$	(lambda),(53)	(54)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T \text{true} : \text{bool}$	by definition	(55)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T \text{false} : \text{bool}$	by definition	(56)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T \text{false} =_{\text{bool}} \text{true} : \text{bool}$	(=type),(56),(55)	(57)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T (\lambda y : \text{bool}. y) \text{false} =_{\text{bool}} \text{true} : \text{bool}$	(appl),(54),(57)	(58)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T \text{true} =_{\text{bool}} \text{false} : \text{bool}$	(=type),(55),(56)	(59)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T (\lambda y : \text{bool}. y) \text{true} =_{\text{bool}} \text{false} : \text{bool}$	(appl),(54),(59)	(60)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T (\lambda y : \text{bool}. y) \text{true} : \text{bool}$	(appl),(54),(55)	(61)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T (\lambda y : \text{bool}. y) \text{false} : \text{bool}$	(appl),(54),(56)	(62)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T (\lambda x : \text{bool}. x) \text{false} =_{\text{bool}} \text{false}$	(beta),(62)	(63)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T (\lambda y : \text{bool}. y) \text{false}$	(congl-),(63),(51)	(64)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T (\lambda x : \text{bool}. x) \text{true} =_{\text{bool}} \text{true}$	(beta),(61)	(65)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T (\lambda y : \text{bool}. y) \text{true}$	(congl-),(65),(52)	(66)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T \forall x : \text{bool}. (\lambda y : \text{bool}. y) x$	(boolExt),(64),(66)	(67)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T (\lambda y : \text{bool}. y) (\text{true} =_{\text{bool}} \text{false})$	(vE),(67),(59)	(68)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T (\lambda y : \text{bool}. y) (\text{false} =_{\text{bool}} \text{true})$	(vE),(67),(57)	(69)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T (\lambda y : \text{bool}. y) (\text{true} =_{\text{bool}} \text{false})$		
$=_{\text{bool}} (\text{true} =_{\text{bool}} \text{false})$	(beta),(60)	(70)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T (\lambda y : \text{bool}. y) (\text{false} =_{\text{bool}} \text{true})$		
$=_{\text{bool}} (\text{false} =_{\text{bool}} \text{true})$	(beta),(58)	(71)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T (\text{true} =_{\text{bool}} \text{false})$		
$=_{\text{bool}} (\lambda y : \text{bool}. y) (\text{true} =_{\text{bool}} \text{false})$	(sym),(70)	(72)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T (\text{false} =_{\text{bool}} \text{true})$		
$=_{\text{bool}} (\lambda y : \text{bool}. y) (\text{false} =_{\text{bool}} \text{true})$	(sym),(71)	(73)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T \text{true} =_{\text{bool}} \text{false}$	(congl-),(72),(68)	(74)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T \text{false} =_{\text{bool}} \text{true}$	(congl-),(73),(69)	(75)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false}, \text{false} \Rightarrow \text{true} \vdash_T \text{true} =_{\text{bool}} \text{false}$	(monotonic-),(48),(74)	(76)
$\Gamma, \text{ass2} : \text{true} \Rightarrow \text{false} \vdash_T (\text{false} \Rightarrow \text{true}) \Rightarrow (\text{true} =_{\text{bool}} \text{false})$	( $\Rightarrow$ I),(46),(76)	(77)
$\Gamma \vdash_T (\text{true} \Rightarrow \text{false}) \Rightarrow (\text{false} =_{\text{bool}} \text{true})$	( $\Rightarrow$ I),(47),(75)	(78)
$\Gamma \vdash_T (\text{true} \Rightarrow \text{false}) \Rightarrow ((\text{false} \Rightarrow \text{true}) \Rightarrow \text{true} =_{\text{bool}} \text{false})$	( $\Rightarrow$ I),(44),(77)	(79)
$\Gamma, \text{ass3} : \text{false} \Rightarrow \text{true} \vdash_T (\text{true} \Rightarrow \text{false}) \Rightarrow (\text{true} =_{\text{bool}} \text{false})$	(monotonic-),(48),(78)	(80)
$\Gamma \vdash_T (\text{false} \Rightarrow \text{true}) \Rightarrow ((\text{true} \Rightarrow \text{false}) \Rightarrow \text{false} =_{\text{bool}} \text{true})$	( $\Rightarrow$ I),(48),(80)	(81)
$\Gamma \vdash_T \forall y : \text{bool}. (\text{true} \Rightarrow y) \Rightarrow ((y \Rightarrow \text{true}) \Rightarrow \text{true} =_{\text{bool}} y)$		

$$(\text{boolExt}), (42), (\text{congl-}), (\text{beta}), (79) \quad (82)$$

$$\Gamma \vdash_T \forall y : \text{bool}. (\text{false} \Rightarrow y) \Rightarrow ((y \Rightarrow \text{false}) \Rightarrow \text{false} =_{\text{bool}} y)$$

$$(\text{boolExt}), (81), (\text{congl-}), (\text{beta}), (43) \quad (83)$$

Showing that these terms are all well-typed:

$$\Gamma, x : \text{bool}, y : \text{bool} \vdash_T x : \text{bool} \quad (\text{varS}), (\text{ctxAssume}), (\text{ctxAssume}) \quad (84)$$

$$\Gamma, x : \text{bool}, y : \text{bool} \vdash_T y : \text{bool} \quad (\text{varS}), (\text{ctxAssume}), (\text{ctxAssume}) \quad (85)$$

$$\Gamma, x : \text{bool}, y : \text{bool} \vdash_T (x \Rightarrow y) : \text{bool} \quad (\Rightarrow \text{type}), (84), (85) \quad (86)$$

$$\Gamma, x : \text{bool}, y : \text{bool} \vdash_T (y \Rightarrow x) : \text{bool} \quad (\Rightarrow \text{type}), (85), (84) \quad (87)$$

$$\Gamma, x : \text{bool}, y : \text{bool} \vdash_T (x =_{\text{bool}} y) : \text{bool} \quad (= \text{type}), (84), (85) \quad (88)$$

$$\Gamma, x : \text{bool}, y : \text{bool} \vdash_T (y \Rightarrow x) \Rightarrow (x =_{\text{bool}} y) : \text{bool} \quad (\Rightarrow \text{type}), (87), (88) \quad (89)$$

$$\Gamma, x : \text{bool}, y : \text{bool} \vdash_T (x \Rightarrow y) \Rightarrow ((y \Rightarrow x) \Rightarrow x =_{\text{bool}} y) : \text{bool} \quad (\Rightarrow \text{type}), (86), (89) \quad (90)$$

$$\Gamma, x : \text{bool} \vdash_T \forall y : \text{bool}. (x \Rightarrow y) \Rightarrow ((y \Rightarrow x) \Rightarrow x =_{\text{bool}} y) : \text{bool} \quad (\forall \text{type}), (90) \quad (91)$$

$$\Gamma \vdash_T \lambda x : \text{bool}. \forall y : \text{bool}. (x \Rightarrow y) \Rightarrow ((y \Rightarrow x) \Rightarrow x =_{\text{bool}} y) : \text{bool} \rightarrow \text{bool} \quad (\text{lambda}), (91) \quad (92)$$

$$\Gamma \vdash_T (\lambda x : \text{bool}. \forall y : \text{bool}. (x \Rightarrow y) \Rightarrow ((y \Rightarrow x) \Rightarrow x =_{\text{bool}} y)) \text{true} : \text{bool} \quad (\text{appl}), (92), (33) \quad (93)$$

$$\Gamma \vdash_T (\lambda x : \text{bool}. \forall y : \text{bool}. (x \Rightarrow y) \Rightarrow ((y \Rightarrow x) \Rightarrow x =_{\text{bool}} y)) \text{false} : \text{bool} \quad (\text{appl}), (92), (34) \quad (94)$$

Beta reduce and conclude claim:

$$\begin{aligned} \Gamma \vdash_T (\lambda x : \text{bool}. \forall y : \text{bool}. (x \Rightarrow y) \Rightarrow ((y \Rightarrow x) \Rightarrow x =_{\text{bool}} y)) \text{true} \\ =_{\text{bool}} \forall y : \text{bool}. (\text{true} \Rightarrow y) \Rightarrow ((y \Rightarrow \text{true}) \Rightarrow \text{true} =_{\text{bool}} y) \end{aligned} \quad (\text{beta}), (93) \quad (95)$$

$$\begin{aligned} \Gamma \vdash_T (\lambda x : \text{bool}. \forall y : \text{bool}. (x \Rightarrow y) \Rightarrow ((y \Rightarrow x) \Rightarrow x =_{\text{bool}} y)) \text{false} \\ =_{\text{bool}} \forall y : \text{bool}. (\text{false} \Rightarrow y) \Rightarrow ((y \Rightarrow \text{false}) \Rightarrow \text{false} =_{\text{bool}} y) \end{aligned} \quad (\text{beta}), (94) \quad (96)$$

$$\Gamma \vdash_T (\lambda x : \text{bool}. \forall y : \text{bool}. (x \Rightarrow y) \Rightarrow ((y \Rightarrow x) \Rightarrow x =_{\text{bool}} y)) \text{true} \quad (\text{congl-}), (95), (82) \quad (97)$$

$$\Gamma \vdash_T (\lambda x : \text{bool}. \forall y : \text{bool}. (x \Rightarrow y) \Rightarrow ((y \Rightarrow x) \Rightarrow x =_{\text{bool}} y)) \text{false} \quad (\text{congl-}), (96), (83) \quad (98)$$

$$\Gamma \vdash_T \forall x : \text{bool}. (\lambda x : \text{bool}. \forall y : \text{bool}. (x \Rightarrow y) \Rightarrow ((y \Rightarrow x) \Rightarrow x =_{\text{bool}} y)) x \quad (\text{boolExt}), (97), (98) \quad (99)$$

$$\Gamma \vdash_T \lambda x : \text{bool}. \forall y : \text{bool}. (x \Rightarrow y) \Rightarrow ((y \Rightarrow x) \Rightarrow x =_{\text{bool}} y) F \quad (\forall E), (99), (28) \quad (100)$$

$$\Gamma \vdash_T \lambda x : \text{bool}. \forall y : \text{bool}. (x \Rightarrow y) \Rightarrow ((y \Rightarrow x) \Rightarrow x =_{\text{bool}} y) F : \text{bool} \quad (\text{validTyping}), (100) \quad (101)$$

$$\begin{aligned} \Gamma \vdash_T \forall y : \text{bool}. (F \Rightarrow y) \Rightarrow ((y \Rightarrow F) \Rightarrow F =_{\text{bool}} y) =_{\text{bool}} \\ \lambda x : \text{bool}. \forall y : \text{bool}. (x \Rightarrow y) \Rightarrow ((y \Rightarrow x) \Rightarrow x =_{\text{bool}} y) F \end{aligned} \quad (\text{beta}), (101) \quad (102)$$

$$\Gamma \vdash_T \forall y : \text{bool}. (F \Rightarrow y) \Rightarrow ((y \Rightarrow F) \Rightarrow F =_{\text{bool}} y) \quad (\text{congl-}), (102), (100) \quad (103)$$

$$\Gamma \vdash_T (F \Rightarrow G) \Rightarrow ((G \Rightarrow F) \Rightarrow F =_{\text{bool}} G) \quad (\forall E), (103), (32) \quad (104)$$

$$\Gamma \vdash_T (G \Rightarrow F) \Rightarrow F =_{\text{bool}} G \quad (\Rightarrow E), (104), (35) \quad (105)$$

$$\Gamma \vdash_T F =_{\text{bool}} G \quad (\Rightarrow E), (105), (36) \quad (106)$$

*Regarding (VI):* Note that while this proof uses Lemma 2, this is not a problem since we only use those of the rules in this lemma that are shown in the above cases which don't assume (VI) or Lemma 2.

$$\Gamma, x : A \vdash_T F \quad \text{by assumption} \quad (107)$$

$$\Gamma, x : A \vdash_T F =_{\text{bool}} \text{true} \quad \text{lemma 2}, (107) \quad (108)$$

$$\Gamma \vdash_T A \equiv A \quad (\text{congBase}) \quad (109)$$

$$\Gamma \vdash_T \lambda x : A. F =_{A \rightarrow \text{bool}} \lambda x : A. \text{true} \quad (\text{cong}\lambda), (108), (109) \quad (110)$$

$$\Gamma \vdash_T \forall x : A. F \quad \text{by definition}, (110) \quad (111)$$

*Regarding (applType):*

$$\Gamma \vdash_T t : A \quad \text{by assumption} \quad (112)$$

$$\Gamma \vdash_T f : B \quad \text{by assumption} \quad (113)$$

Since typing of a function application can only be proven by rule (appl), the assumptions of the rule must be satisfied, so we yield:

$$\Gamma \vdash_T f : A' \rightarrow B \quad \text{see above} \quad (114)$$

$$\Gamma \vdash_T t : A' \quad \text{see above} \quad (115)$$

$$\Gamma \vdash_T A \equiv A' \quad (\text{typesUnique}), (115) \quad (116)$$

$$\Gamma \vdash_T A' \equiv A \quad (\equiv \text{sym}), (116) \quad (117)$$

$$\Gamma \vdash_T A' \rightarrow B \equiv A \rightarrow B \quad (\text{cong}\rightarrow), (117) \quad (118)$$

$$\Gamma \vdash_T f =_{A' \rightarrow B} f \quad (\text{refl}), (114) \quad (119)$$

$$\Gamma \vdash_T f : A \rightarrow B \quad (\text{cong:}), (119), (118), (114) \quad (120)$$

*Regarding (trans):*

$$\Gamma \vdash_T s =_A t \quad \text{by assumption} \quad (121)$$

$$\Gamma \vdash_T s =_A t : \text{bool} \quad (\text{validTyping}), (121) \quad (122)$$

$$\Gamma \vdash_T t =_A u \quad \text{by assumption} \quad (123)$$

$$\Gamma, eq : s =_A t \vdash_T s =_A t \quad (\text{assume}), (\text{ctxAssume}), (122) \quad (124)$$

$$\Gamma, eq : s =_A t, t =_A t \vdash_T s =_A t \quad (\text{monotonic-}), (122), (124) \quad (125)$$

$$\Gamma \vdash_T t =_A s \quad (\text{sym}), (121) \quad (126)$$

$$\Gamma \vdash_T t : A \quad (\text{eqTyping}), (126) \quad (127)$$

$$\Gamma \vdash_T A \text{ tp} \quad (\text{typingTp}), (127) \quad (128)$$

$\Gamma \vdash_T u =_A t$	(sym),(123)	(129)
$\Gamma \vdash_T u : A$	(eqTyping),(129)	(130)
$\Gamma \vdash_T t =_A t : \text{bool}$	(=type),(127),(127)	(131)
$\Gamma, eq : s =_A t \vdash_T t =_A t : \text{bool}$	(monotonic $\vdash$ ),(122),(131)	(132)
$\Gamma \vdash_T s : A$	(eqTyping),(121)	(133)
$\Gamma, eq : s =_A t \vdash_T t =_A t \Rightarrow s =_A t$	( $\Rightarrow$ I),(132),(125)	(134)
$\Gamma \vdash_T s =_A t \Rightarrow t =_A t \Rightarrow s =_A t$	( $\Rightarrow$ I),(122),(134)	(135)
$\Gamma, z : A \vdash_T s : A$	(var $\vdash$ ),(128),(133)	(136)
$\vdash_T \Gamma, z : A \text{ Ctx}$	(ctxVar),(tpCtx),(133),(128)	(137)
$\Gamma, z : A \vdash_T t : A$	(var $\vdash$ ),(128),(127)	(138)
$\Gamma, z : A \vdash_T z : A$	(varS),(137)	(139)
$\Gamma, z : A \vdash_T t =_A z : \text{bool}$	( $\Rightarrow$ I),(138),(139)	(140)
$\Gamma, z : A \vdash_T s =_A z : \text{bool}$	( $\Rightarrow$ I),(136),(139)	(141)
$\Gamma, z : A \vdash_T (t =_A z) \Rightarrow (s =_A z) : \text{bool}$	( $\Rightarrow$ I),(140),(141)	(142)
$\Gamma, z : A \vdash_T s =_A t : \text{bool}$	( $\Rightarrow$ I),(136),(138)	(143)
$\Gamma, z : A \vdash_T (s =_A t) \Rightarrow ((t =_A z) \Rightarrow (s =_A z)) : \text{bool}$	( $\Rightarrow$ type),(143),(142)	(144)
$\Gamma \vdash_T \lambda z : A. s =_A t \Rightarrow t =_A z \Rightarrow s =_A z : A \rightarrow \text{bool}$	(lambda),(144)	(145)
$\Gamma \vdash_T (\lambda z : A. s =_A t \Rightarrow t =_A z \Rightarrow s =_A z) t : \text{bool}$	(appl),(145),(127)	(146)
$\Gamma \vdash_T (\lambda z : A. s =_A t \Rightarrow t =_A z \Rightarrow s =_A z) t$		
$\quad =_{\text{bool}} s =_A t \Rightarrow t =_A t \Rightarrow s =_A t$	(beta),(146)	(147)
$\Gamma \vdash_T (\lambda z : A. s =_A t \Rightarrow t =_A z \Rightarrow s =_A z) t$	(cong $\vdash$ ), (135), (147)	(148)
$\Gamma \vdash_T (\lambda z : A. s =_A t \Rightarrow t =_A z \Rightarrow s =_A z) t$		
$\quad =_{\text{bool}} (\lambda z : A. s =_A t \Rightarrow t =_A z \Rightarrow s =_A z) u$	(congAppl), (121)	(149)
$\Gamma \vdash_T (\lambda z : A. s =_A t \Rightarrow t =_A z \Rightarrow s =_A z) u$		
$\quad =_{\text{bool}} (\lambda z : A. s =_A t \Rightarrow t =_A z \Rightarrow s =_A z) t$	(sym), (149)	(150)
$\Gamma \vdash_T (\lambda z : A. s =_A t \Rightarrow t =_A z \Rightarrow s =_A z) u$	(cong $\vdash$ ), (150), (148)	(151)
$\Gamma \vdash_T (\lambda z : A. s =_A t \Rightarrow t =_A z \Rightarrow s =_A z) t : \text{bool}$	(appl),(145),(130)	(152)
$\Gamma \vdash_T (\lambda z : A. s =_A t \Rightarrow t =_A z \Rightarrow s =_A z) u$		
$\quad =_{\text{bool}} s =_A t \Rightarrow t =_A u \Rightarrow s =_A u$	(beta),(152)	(153)
$\Gamma \vdash_T s =_A t \Rightarrow t =_A u \Rightarrow s =_A u$	(cong $\vdash$ ),(153), (151)	(154)
$\Gamma \vdash_T t =_A u \Rightarrow s =_A u$	( $\Rightarrow$ E),(154),(121)	(155)
$\Gamma \vdash_T s =_A u$	( $\Rightarrow$ E),(155),(123)	(156)

Regarding (*extensionality*):

$\Gamma, x : A \vdash_T f x =_B f' x$	by assumption	(157)
$\Gamma, x : A \vdash_T f x : B$	(eqTyping),(157)	(158)
$\Gamma, x : A \vdash_T f' x =_B f x$	(sym),(157)	(159)
$\Gamma, x : A \vdash_T f' x : B$	(eqTyping),(159)	(160)

$\Gamma, x : A \vdash_T x : A$	(varS),(tpCtx),(158)	(161)
$\Gamma, x : A \vdash_T f : A \rightarrow B$	(applType),(161),(158)	(162)
$\Gamma, x : A \vdash_T f' : A \rightarrow B$	(applType),(161),(160)	(163)
$\Gamma \vdash_T f =_{A \rightarrow B} \lambda x : A. f \ x$	(eta),(162)	(164)
$\Gamma \vdash_T \lambda x : A. f \ x =_{A \rightarrow B} \lambda x : A. f' \ x$	(cong $\lambda$ ), (157)	(165)
$\Gamma \vdash_T f =_{A \rightarrow B} \lambda x : A. f' \ x$	(trans), (164), (165)	(166)
$\Gamma \vdash_T f' =_{A \rightarrow B} \lambda x : A. f' \ x$	(eta),(163)	(167)
$\Gamma \vdash_T \lambda x : A. f' \ x =_{A \rightarrow B} f'$	(sym),(167)	(168)
$\Gamma \vdash_T f =_{A \rightarrow B} f'$	(trans), (166), (168)	(169)

Regarding ( $\forall$ cong):

$$\Gamma \vdash_T A \equiv A' \quad \text{by assumption} \quad (170)$$

By induction on derivations, it follows that  $A, A'$  well-typed

$\Gamma, x : A \vdash_T F =_{\text{bool}} F'$	by assumption	(171)
$\Gamma \vdash_T \forall x : A. F : \text{bool}$	(=type),(lambda),definition,(lambda),(eqTyping),(171)	(172)
$\Gamma, uqf : \forall x : A. F \vdash_T \forall x : A. F$	(assume),(ctxAssume),(172)	(173)
$\Gamma, uqf : \forall x : A. F, y : A' \vdash_T \forall x : A. F$	(var $\vdash$ ),(ctxVar),(173)	(174)
$\Gamma, uqf : \forall x : A. F, y : A', x' : A \vdash_T \forall x : A. F$	(var $\vdash$ ),(ctxVar),(174)	(175)
$\Gamma, uqf : \forall x : A. F, y : A', x' : A \vdash_T x' : A$	(varS),(ctxVar)	(176)
$\Gamma, uqf : \forall x : A. F, y : A', x : A \vdash_T F$	( $\forall$ E),(175),(176)	(177)
$\Gamma, uqf : \forall x : A. F, x : A \vdash_T F =_{\text{bool}} F'$	(monotonic $\vdash$ ),(171)	(178)
$\Gamma, uqf : \forall x : A. F, y : A', x : A \vdash_T F =_{\text{bool}} F'$	(var $\vdash$ ),(tpCtx),(176),(178)	(179)
$\Gamma, uqf : \forall x : A. F, y : A', x : A \vdash_T F'$	(cong $\vdash$ ),(179),(177)	(180)
$\Gamma, uqf : \forall x : A. F, y : A' \vdash_T \forall x : A. F'$	( $\forall$ I),(180)	(181)

Now we will prove that  $\Gamma, uqf : \forall x : A. F, y : A' \vdash_T y : A$

$\Gamma, uqf : \forall x : A. F, y : A' \vdash_T y : A'$	(varS),(ctxVar)	(182)
$\Gamma, uqf : \forall x : A. F, y : A' \vdash_T y =_{A'} y$	(refl),(182)	(183)
$\Gamma, uqf : \forall x : A. F, y : A' \vdash_T A \equiv A'$	(var $\vdash$ ),(monotonic $\vdash$ ),(ctxAssume),(172),(170)	(184)
$\Gamma, uqf : \forall x : A. F, y : A' \vdash_T A' \equiv A$	( $\equiv$ sym)	(185)
$\Gamma, uqf : \forall x : A. F, y : A' \vdash_T y : A$	(cong $\vdash$ ),(183),(185),(182)	(186)

Substitute  $y$  for  $x$  in (181) and move  $y$  from context into a  $\forall$  binder.

$$\Gamma, uqf : \forall x : A. F, y : A' \vdash_T F' [x/y] \quad (\forall E), (181), (186) \quad (187)$$

$$\Gamma, uqf : \forall x : A. F, x : A' \vdash_T F' \quad \text{renaming } y \text{ to } x \quad (188)$$

$$\Gamma, uqf : \forall x : A. F, x : A' \vdash_T x : A' \quad (\text{varS}), (\text{tpCtx}), (186) \quad (189)$$

$$\Gamma, uqf : \forall x : A. F \vdash_T \forall x : A'. F' \quad (\forall I), (188), (189) \quad (190)$$

Since term and type equality are both symmetric (and we can use the same trick as above to show that variables of type  $A'$  are also of type  $A$  and vice versa), we can prove the following formula analogously:

$$\Gamma, \forall x : A'. F' \vdash_T \forall x : A. F \quad \text{analogously} \quad (191)$$

$$\Gamma \vdash_T \forall x : A. F =_{\text{bool}} \forall x : A. F' \quad (\text{propExt}), (190), (191) \quad (192)$$

Regarding  $(\Rightarrow \text{cong})$ :

$$\Gamma \vdash_T F =_{\text{bool}} F' \quad \text{by assumption} \quad (193)$$

$$\Gamma \vdash_T G =_{\text{bool}} G' \quad \text{by assumption} \quad (194)$$

Introduce lambda function in two variables  $\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y$  show rule for it using  $(\text{congAppl})$  and use  $(\text{beta})$  and  $(\text{trans})$  to conclude the same about  $\Rightarrow$ :

$$\begin{aligned} \Gamma \vdash_T (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) \\ =_{\text{bool}} (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) \quad (\text{refl}), (\text{lambda}), (\text{lambda}), (\Rightarrow \text{type}), (\text{varS}), (\text{varS}) \end{aligned} \quad (195)$$

$$\begin{aligned} \Gamma \vdash_T (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F \\ =_{\text{bool}} (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F' \quad (\text{congAppl}), (195), (193) \end{aligned} \quad (196)$$

$$\begin{aligned} \Gamma \vdash_T (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F G \\ =_{\text{bool}} (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F' G' \quad (\text{congAppl}), (196), (194) \end{aligned} \quad (197)$$

Now we prove that  $\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y$  and its applications are well-typed to allow using the rule  $(\text{beta})$  for it:

$$\Gamma, x : \text{bool}, y : \text{bool} \vdash_T x : \text{bool} \quad (\text{varS}), (\text{ctxVar}), (\text{ctxVar}) \quad (198)$$

$$\Gamma, x : \text{bool}, y : \text{bool} \vdash_T y : \text{bool} \quad (\text{varS}), (\text{ctxVar}), (\text{ctxVar}) \quad (199)$$

$$\Gamma, x : \text{bool}, y : \text{bool} \vdash_T x \Rightarrow y : \text{bool} \quad (\Rightarrow \text{type}), (198), (199) \quad (200)$$

$$\Gamma, x : \text{bool} \vdash_T \lambda y : \text{bool}. (x \Rightarrow y) : \text{bool} \rightarrow \text{bool} \quad (\text{lambda}), (200) \quad (201)$$

$$\Gamma \vdash_T \lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y : \text{bool} \rightarrow \text{bool} \rightarrow \text{bool} \quad (\text{lambda}), (201) \quad (202)$$

$$\Gamma \vdash_T F : \text{bool} \quad (\text{eqTyping}), (193) \quad (203)$$

$$\begin{aligned}
\Gamma \vdash_T G &: \text{bool} && (\text{eqTyping}), (194) \\
&&& (204) \\
\Gamma \vdash_T F' &=_{\text{bool}} F && (\text{sym}), (193) \quad (205) \\
\Gamma \vdash_T G' &=_{\text{bool}} G && (\text{sym}), (194) \quad (206) \\
\Gamma \vdash_T F' &: \text{bool} && (\text{eqTyping}), (205) \\
&&& (207) \\
\Gamma \vdash_T G' &: \text{bool} && (\text{eqTyping}), (206) \\
&&& (208) \\
\Gamma \vdash_T (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F &: \text{bool} \rightarrow \text{bool} && (\text{appl}), (202), (203) \\
&&& (209) \\
\Gamma \vdash_T (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F' &: \text{bool} \rightarrow \text{bool} && (\text{appl}), (202), (207) \\
&&& (210) \\
\Gamma \vdash_T (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F G &: \text{bool} && (\text{appl}), (209), (204) \\
&&& (211) \\
\Gamma \vdash_T (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F' G' &: \text{bool} && (\text{appl}), (210), (208) \\
&&& (212)
\end{aligned}$$

Now we can use rule [\(beta\)](#) to show that the applications of  $\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y$  to  $F, G$  and  $F', G'$  respectively are equal to their [\(beta\)](#) reduced versions:

$$\begin{aligned}
\Gamma \vdash_T (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F &=_{\text{bool} \rightarrow \text{bool}} (\lambda y : \text{bool}. (F \Rightarrow y)) && (\text{beta}), (209) \quad (213) \\
\Gamma \vdash_T (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F' &=_{\text{bool} \rightarrow \text{bool}} (\lambda y : \text{bool}. (F' \Rightarrow y)) && (\text{beta}), (210) \quad (214)
\end{aligned}$$

And again:

$$\begin{aligned}
\Gamma \vdash_T \text{bool} \rightarrow \text{bool} &\equiv \text{bool} \rightarrow \text{bool} && (\text{congBase}) \quad (215) \\
\Gamma \vdash_T \lambda y : \text{bool}. (F \Rightarrow y) &: \text{bool} \rightarrow \text{bool} && (\text{cong}), (213), (215), (209) \\
&&& (216) \\
\Gamma \vdash_T \lambda y : \text{bool}. (F' \Rightarrow y) &: \text{bool} \rightarrow \text{bool} && (\text{cong}), (214), (215), (210) \\
&&& (217) \\
\Gamma \vdash_T \lambda y : \text{bool}. (F \Rightarrow y) G &: \text{bool} && (\text{appl}), (216), (204) \\
&&& (218) \\
\Gamma \vdash_T \lambda y : \text{bool}. (F' \Rightarrow y) G' &: \text{bool} && (\text{appl}), (217), (208) \\
&&& (219) \\
\Gamma \vdash_T (\lambda y : \text{bool}. (F \Rightarrow y)) G &=_{\text{bool}} ((F \Rightarrow G)) && (\text{beta}), (211) \quad (220) \\
\Gamma \vdash_T (\lambda y : \text{bool}. (F' \Rightarrow y)) G' &=_{\text{bool}} ((F' \Rightarrow G')) && (\text{beta}), (212) \quad (221) \\
\Gamma \vdash_T G &=_{\text{bool}} G && (\text{refl}), (204) \quad (222) \\
\Gamma \vdash_T G' &=_{\text{bool}} G' && (\text{refl}), (208) \quad (223) \\
\Gamma \vdash_T (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F G &=_{\text{bool}} \lambda y : \text{bool}. (F \Rightarrow y) G && (\text{congAppl}), (222), (213) \\
&&& (224) \\
\Gamma \vdash_T (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F' G' &=_{\text{bool}} \lambda y : \text{bool}. (F' \Rightarrow y) G' && (\text{congAppl}), (223), (214) \\
&&& (225) \\
\Gamma \vdash_T (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F G &=_{\text{bool}} (F \Rightarrow G) && (\text{trans}), (224), (220) \\
&&& (226)
\end{aligned}$$



$$\begin{aligned}
\Gamma \vdash_T (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F' G' &=_{\text{bool}} (F' \Rightarrow G') && (\text{trans}), (225), (221) \\
&&& (227) \\
\Gamma \vdash_T (F \Rightarrow G) &=_{\text{bool}} (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F G && (\text{sym}), (226) \\
&&& (228) \\
\Gamma \vdash_T (F \Rightarrow G) &=_{\text{bool}} (\lambda x : \text{bool}. \lambda y : \text{bool}. x \Rightarrow y) F' G' && (\text{trans}), (228), (197) \\
&&& (229) \\
\Gamma \vdash_T (F \Rightarrow F') &=_{\text{bool}} (G \Rightarrow G') && (\text{trans}), (229), (227) \\
&&& (230)
\end{aligned}$$

Regarding  $(\forall \Rightarrow)$ :

$$\begin{aligned}
\Gamma, x : A \vdash_T F \Rightarrow G &&& \text{by assumption} && (231) \\
\Gamma \vdash_T \forall z : A. F[x/z] \Rightarrow G[x/z] &&& \alpha\text{-renaming}, (\forall\text{I}), (231) && \\
&&& (232) \\
\Gamma, \text{suq} : \forall z : A. F[x/z], y : A \vdash_T F[x/y] &&& (\forall\text{E}), (\text{assume}), (\text{varS}) && \\
&&& (233) \\
\Gamma, \text{suq} : \forall z : A. F[x/z], y : A \vdash_T F[x/y] \Rightarrow G[x/y] &&& (\forall\text{E}), (232), (\text{varS}) && (234) \\
\Gamma, \text{suq} : \forall z : A. F[x/z], y : A \vdash_T G[x/y] &&& (\Rightarrow\text{E}), (234), (233) && (235) \\
\Gamma, \text{suq} : \forall z : A. F[x/z] \vdash_T \forall y : A. G[x/y] &&& (\forall\text{I}), (235) && (236) \\
\Gamma \vdash_T \forall z : A. F[x/z] \Rightarrow \forall y : A. G[x/y] &&& (\Rightarrow\text{I}), (236) && (237) \\
\Gamma \vdash_T \forall x : A. F \Rightarrow \forall x : A. G &&& \alpha\text{-renaming}, (237)
\end{aligned}$$

Regarding  $(\Rightarrow \text{Funct})$ :

$$\begin{aligned}
\Gamma \vdash_T G \Rightarrow G' &&& \text{by assumption} && (238) \\
\Gamma \vdash_T F' \Rightarrow F &&& \text{by assumption} && (239) \\
as : \Gamma F \Rightarrow G, , F' \vdash_T F &&& (\Rightarrow\text{E}), (239), (\text{assume}) && (240) \\
as : \Gamma F \Rightarrow G, , F' \vdash_T G &&& (\Rightarrow\text{E}), (\text{assume}), (240) && (241) \\
as : \Gamma F \Rightarrow G, , F' \vdash_T G' &&& (\Rightarrow\text{E}), (238), (241) && (242) \\
as : \Gamma F \Rightarrow G, \vdash_T F' \Rightarrow G' &&& (\Rightarrow\text{I}), (242) && (243) \\
\Gamma \vdash_T (F \Rightarrow G) \Rightarrow (F' \Rightarrow G') &&& (\Rightarrow\text{I}), (243)
\end{aligned}$$

Regarding  $(\vdash \text{cong})$ :

$$\begin{aligned}
\Gamma \vdash_T F &=_{\text{bool}} F' && \text{by assumption} && (244) \\
\Gamma \vdash_T F &&& \text{by assumption} && (245) \\
\Gamma \vdash_T F' &=_{\text{bool}} F && (\text{sym}), (244) && (246) \\
\Gamma \vdash_T F' &&& (\text{cong}\vdash), (246), (245) && (247)
\end{aligned}$$

Regarding  $(\text{rewrite})$ :

$$\begin{aligned}
\Gamma \vdash_T F[x/i] &&& \text{by assumption} && (248) \\
\Gamma \vdash_T t =_A t' &&& \text{by assumption} && (249) \\
\Gamma, y : A \vdash_T F[x/y] : \text{bool} &&& \text{by assumption} && (250)
\end{aligned}$$

$\Gamma \vdash_T \lambda y : A. F[x/y] : A \rightarrow \text{bool}$	(lambda),(250)	(251)
$\Gamma \vdash_T t : A$	(eqTyping),(249)	(252)
$\Gamma \vdash_T (\lambda y : A. F[x/y]) t : \text{bool}$	(appl),(251),(252)	(253)
$\Gamma \vdash_T (\lambda y : A. F[x/y]) t =_{\text{bool}} F[x/i]$	(beta),(253)	(254)
$\Gamma \vdash_T (\lambda y : A. F[x/y]) t$	(congl-),(254),(248)	(255)
$\Gamma \vdash_T \lambda y : A. F[x/y] =_{A \rightarrow \text{bool}} \lambda y : A. F[x/y]$	(refl),(251)	(256)
$\Gamma \vdash_T (\lambda y : A. F[x/y]) t =_{\text{bool}} (\lambda y : A. F[x/y]) t'$	(congAppl),(249),(256)	(257)
$\Gamma \vdash_T (\lambda y : A. F[x/y]) t'$	(l- cong),(257),(255)	(258)
$\Gamma \vdash_T t' : A$	(eqTyping),(sym),(249)	(259)
$\Gamma \vdash_T (\lambda y : A. F[x/y]) t' : \text{bool}$	(appl),(251),(259)	(260)
$\Gamma \vdash_T (\lambda y : A. F[x/y]) t' =_{\text{bool}} F[x/i]$	(beta),(260)	(261)
$\Gamma \vdash_T F[x/i]$	(l- cong),(261),(258)	(262)

**Lemma 2.** If  $F$  is a well-typed HOL formula we can show  $\Gamma \vdash_T F =_{\text{bool}} \text{true}$  iff  $\Gamma \vdash_T F$ .

*Proof (Proof of Lemma 2).* We start with the  $\Rightarrow$  direction:

$\Gamma \vdash_T \lambda x : \text{bool}. x =_{\text{bool} \rightarrow \text{bool}} \lambda x : \text{bool}. x$	(refl),(lambda),(varS)	(263)
$\Gamma \vdash_T \text{true}$	definition of true,(263)	(264)
$\Gamma \vdash_T F =_{\text{bool}} \text{true}$	by assumption	(265)
$\Gamma \vdash_T F$	(congl-),(265),(264)	(266)

Now the  $\Leftarrow$  direction:

$\Gamma \vdash_T F$	by assumption	(267)
$\Gamma \vdash_T F : \text{bool}$	by assumption	(268)
$\Gamma \vdash_T \text{true} : \text{bool}$	by definition	(269)
$\Gamma, \text{true} \vdash_T \text{ass} : F$	(monotonicl-),(267)	(270)
$\Gamma, \text{ass} : F \vdash_T \text{true}$	(monotonicl-),(264)	(271)
$\Gamma \vdash_T F =_{\text{bool}} \text{true}$	(propExt),(268),(269),(271),(270)	(272)

Finally, using the definitions of the connectives and quantifiers we can prove the rules:

$$\begin{array}{c}
\frac{\Gamma \vdash_T F \quad \Gamma \vdash_T G}{\Gamma \vdash_T F \wedge G} \wedge I \quad \frac{\Gamma \vdash_T F}{\Gamma \vdash_T F \vee G} \vee II \quad \frac{\Gamma \vdash_T G}{\Gamma \vdash_T F \vee G} \vee Ir \\
\\
\frac{\Gamma \vdash_T F \wedge G}{\Gamma \vdash_T F} \wedge El \quad \frac{\Gamma \vdash_T F \wedge G}{\Gamma \vdash_T G} \wedge Er \quad \frac{\Gamma \vdash_T t : A \quad \Gamma \vdash_T F[x/i]}{\Gamma \vdash_T \exists x : A. F} \exists I
\end{array}$$

**Remark 1** Observe that many of the rules derived for HOL in Lemma 1 still hold in DHOL. In particular, the rules (*ctxThy*), (*tpCtx*), (*typingTp*) and (*validTyping*) can be

proven by the same method. Also the rules ( $\equiv_{\text{refl}}$ ) and ( $\equiv_{\text{sym}}$ ) can be proven easily in DHOL by induction on the type equality rules (for the rule ( $\equiv_{\text{sym}}$ ) the proof easily generalizes to DHOL but proving it in DHOL is harder). Finally the rules ( $\text{monotonic+}$ ), ( $\text{var+}$ ), ( $\text{rewrite}$ ) and the introduction and elimination rules for the quantifier and defined logical connectives can be derived in DHOL with the same proofs.

## B Completeness proof

We will prove the following slightly stronger version of the theorem:

**Theorem 4 (Completeness).** *We have*

$$\vdash T \text{ Thy} \quad \text{implies} \quad \vdash \bar{T} \text{ Thy} \quad (273)$$

$$\vdash_T \Gamma \text{ Ctx} \quad \text{implies} \quad \vdash_{\bar{T}} \bar{\Gamma} \text{ Ctx} \quad (274)$$

$$\Gamma \vdash_T A \text{ tp} \quad \text{implies} \quad \bar{\Gamma} \vdash_{\bar{T}} \bar{A} \text{ tp} \text{ and } \bar{\Gamma} \vdash_{\bar{T}} A^* : \bar{A} \rightarrow \bar{A} \rightarrow \text{bool} \quad (275)$$

$$\Gamma \vdash_T A \equiv B \quad \text{implies} \quad \bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \bar{B} \text{ and } \bar{\Gamma}, x : \bar{A} \vdash_{\bar{T}} A^* x x =_{\text{bool}} B^* x x \quad (276)$$

$$\Gamma \vdash_T A <: B \quad \text{implies} \quad \bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \bar{B} \text{ and } \bar{\Gamma}, x, y : \bar{B} \vdash_{\bar{T}} A^* x y \Rightarrow B^* x y \quad (277)$$

$$\Gamma \vdash_T t : A \quad \text{implies} \quad \bar{\Gamma} \vdash_{\bar{T}} \bar{t} : \bar{A} \text{ and } \bar{\Gamma} \vdash_{\bar{T}} A^* \bar{t} \bar{t} \quad (278)$$

$$\Gamma \vdash_T F \quad \text{implies} \quad \bar{\Gamma} \vdash_{\bar{T}} \bar{F} \quad (279)$$

In case of term equality, we strengthen the claim to:

$$\Gamma \vdash_T t =_A t' \quad \text{implies} \quad \bar{\Gamma} \vdash_{\bar{T}} A^* \bar{t} \bar{t}' \text{ and } \bar{\Gamma} \vdash_{\bar{T}} \bar{t} : \bar{A} \text{ and } \bar{\Gamma} \vdash_{\bar{T}} \bar{t}' : \bar{A} \quad (280)$$

Furthermore, the typing relations  $A^*$  are symmetric and transitive on all well-formed types  $A$ :

$$\Gamma \vdash_T A \text{ tp} \quad \text{implies} \quad \bar{\Gamma} \vdash_{\bar{T}} \forall x, y : \bar{A}. A^* x y \Rightarrow A^* y x \quad (281)$$

$$\Gamma \vdash_T A \text{ tp} \quad \text{implies} \quad \bar{\Gamma} \vdash_{\bar{T}} \forall x, y, z : \bar{A}. A^* x y \Rightarrow (A^* y z \Rightarrow A^* x z) \quad (282)$$

Additionally the substitution lemma holds, i.e.,

$$\Gamma, x : A \vdash_T t : B \text{ and } \Gamma \vdash u : A \quad \text{implies} \quad \bar{\Gamma} \vdash_{\bar{T}} \overline{t[x/u]} =_{\bar{B}} \bar{t}[x/\bar{u}] \quad (283)$$

$$\Gamma, x : A \vdash_T B \text{ tp and } \Gamma \vdash_T u : B \quad \text{implies} \quad \bar{\Gamma} \vdash_{\bar{T}} \overline{B[x/u]} \equiv \bar{B}[x/\bar{u}] \quad (284)$$

In the following lines, we assume that if  $t = \lambda y : C. s$  for  $s$  of type  $D$ , then  $B = \Pi y : C. D$  (this is enough in practise and we cannot easily show more).

$$\Gamma, x : A \vdash_T t : B \quad \text{implies} \quad \bar{\Gamma}, x, x' : \bar{A}, x R x' : A^* x x' \vdash_{\bar{T}} B^* \bar{t} \bar{t}[x/x'] \quad (285)$$

Here Case 276 looks weaker than in the original statement, but is easily seen to be equivalent. The proof uses rule ( $<:I$ ), the completeness claim for the subtyping judgement and rule ( $\text{propExt}$ ) in HOL.

*Proof (Proof of Theorem 4).* Firstly, we will prove the substitution lemma by induction on the grammar, i.e. by induction on the shape of the terms and types.

Afterwards, we will prove completeness of the translation w.r.t. all DHOL judgements by induction on the derivations. This means that we consider the inference rules of DHOL and prove that if completeness holds for the assumptions of a DHOL inference rule, then it also holds for the conclusion of the rule. For the inductive steps for some typing rules, namely ( $=\text{type}$ ) and ( $\text{cong}:$ ), we also require the fact that for any (well-formed) type  $A$  in DHOL we have  $A^* : \bar{A} \rightarrow \bar{A} \rightarrow \text{bool}$ . This follows directly from how the  $A^*$  are generated/defined in the translation.

*Substitution lemma and symmetry and transitivity of the typing relations* Since the translation of types commutes with the type productions of the grammar (284) is obvious.

We show (283) by induction on the grammar of DHOL. If  $x$  is not a free variable in  $t$ , then  $\overline{t[x/u]} = \bar{t} = \bar{t}[x/\bar{u}]$  and the claim (283) follows by rule ( $\text{refl}$ ). So assume that  $x$  is a free variable of  $t$ .

If  $t$  is a variable, then by assumption (that  $x$  is a free variable in  $t$ ) it follows that  $t = x$  and thus  $\overline{t[x/u]} = \bar{u} = \bar{t}[x/\bar{u}]$  and the claim follows by rule ( $\text{refl}$ ).

If  $t$  is a  $\lambda$ -term  $\lambda y : A. s$ , then by induction hypothesis we have  $\bar{\Gamma}, y : \bar{A} \vdash_{\bar{T}} \overline{s[x/u]} =_{\bar{A}} \bar{s}[x/\bar{u}]$ , where  $A$  is the type of  $s$ . By rule ( $\text{cong}\lambda$ ), the claim of  $\bar{\Gamma} \vdash_{\bar{T}} \overline{\lambda y : A. s[x/u]} =_{\bar{B}} \overline{\lambda y : A. s}[x/\bar{u}]$  follows.

If  $t$  is a function application  $f s$ , then by induction hypothesis we have  $\bar{\Gamma} \vdash_{\bar{T}} \overline{s[x/u]} =_{\bar{A}} \bar{s}[x/\bar{u}]$  and  $\bar{\Gamma} \vdash_{\bar{T}} \overline{f[x/u]} =_{\bar{A} \rightarrow \bar{B}} \bar{f}[x/\bar{u}]$ , where  $T$  is the type of  $s$ . By rule ( $\text{congApp}$ ), the claim of  $\bar{\Gamma} \vdash_{\bar{T}} \overline{(f s)[x/u]} =_{\bar{B}} \overline{f s}[x/\bar{u}]$  follows.

If  $t$  is an equality  $s =_A s'$ , then by induction hypothesis we have  $\bar{\Gamma} \vdash_{\bar{T}} \overline{s[x/u]} =_{\bar{A}} \bar{s}[x/\bar{u}]$  and  $\bar{\Gamma} \vdash_{\bar{T}} \overline{s'[x/u]} =_{\bar{A}} \bar{s}'[x/\bar{u}]$ , where  $A$  is the type of  $s$  and  $s'$ . By rule ( $=\text{cong}$ ), the claim of  $\bar{\Gamma} \vdash_{\bar{T}} \overline{(s =_A s')[x/u]} =_{\text{bool}} \overline{(s =_A s')}[x/\bar{u}]$  follows.

Before we can show (285), we first need to prove the symmetry and transitivity of the typing relations: We can prove both by induction on the type  $A$ . Denote  $\Delta := \bar{\Gamma}, x, y : \bar{A}, xRy : A^* x y$  and  $\Theta := \bar{\Gamma}, x, y, z : \bar{A}, xRy : A^* x y, yRz : A^* y z$  respectively. If we can show  $\Delta \vdash_{\bar{T}} A^* y x$  and  $\Theta \vdash_{\bar{T}} A^* x z$  respectively, then the claims (281) and (282) follows by the rules ( $\Rightarrow I$ ), ( $\forall I$ ), ( $\text{varS}$ ) and ( $\text{assume}$ ). Those are therefore the claims we are going to show.

Observe that for types declared in the theory  $T$ , the symmetry and transitivity of  $A^*$  follows from the axiom generated by the translation (in case (PT2)) of the type declaration declaring  $A$ . This follows from the symmetry and transitivity of equality and (283).

If  $A$  is `bool`, the typing relation is  $=_{\text{bool}}$  which is symmetric and transitive by the rules [\(sym\)](#) and [\(trans\)](#) respectively. In these cases the claims follows by the rule [\(assume\)](#) and rule [\(sym\)](#) resp. by rule [\(assume\)](#) and rule [\(trans\)](#).

If  $A$  is a  $\Pi$ -type  $\Pi x : C. D$  we have  $C^* f g = \forall x, y : \bar{C}. C^* x y \Rightarrow D^* f x g y$ . Then we have

$$\Delta = \bar{\Gamma}, x, y : \bar{A}, x R y : \forall w : \bar{C}. \forall w' : \bar{C}. C^* w w' \Rightarrow D^* (x w) (y w')$$

and

$$\begin{aligned} \Theta = \bar{\Gamma}, x, y, z : \bar{A}, x R y : \forall w : \bar{C}. \forall w' : \bar{C}. C^* w w' \Rightarrow D^* (x z) (y z'), \\ y R z : \forall w : \bar{C}. \forall w' : \bar{C}. C^* w w' \Rightarrow D^* (y w) (z w'). \end{aligned}$$

The claim is

$$\Delta \vdash_{\bar{T}} \forall w, w' : \bar{C}. C^* w w' \Rightarrow D^* (y w) (x w')$$

and

$$\Delta \vdash_{\bar{T}} \forall w, w' : \bar{C}. C^* w w' \Rightarrow D^* (x w) (z w')$$

respectively.

We can prove the claim for [\(281\)](#) by

$$\begin{aligned} \Delta, w, w' : \bar{C}, w R w' : C^* w w' \vdash_{\bar{T}} \\ C^* w w' \Rightarrow D^* (x w) (y w') \quad (\forall E), (\forall E), (\text{assume}) \end{aligned} \quad (286)$$

$$\begin{aligned} \Delta, w, w' : \bar{C}, w R w' : C^* w w' \vdash_{\bar{T}} \\ D^* (x w) (y w') \quad (\Rightarrow E), (286), (\text{assume}) \end{aligned} \quad (287)$$

$$\begin{aligned} \Delta, w, w' : \bar{C}, w R w' : C^* w w' \vdash_{\bar{T}} \\ D^* (x w) (y w') \Rightarrow D^* (y w) (x w') \quad \text{induction hypothesis} \end{aligned} \quad (288)$$

$$\begin{aligned} \Delta, w, w' : \bar{C}, w R w' : C^* w w' \vdash_{\bar{T}} \\ D^* (x w) (y w') \quad (\Rightarrow E), (288), (287) \end{aligned} \quad (289)$$

$$\Delta, w, w' : \bar{C} \vdash_{\bar{T}} C^* w w' \Rightarrow D^* (y w) (x w') \quad (\Rightarrow I), (289) \quad (290)$$

$$\Delta \vdash_{\bar{T}} \forall w, w' : \bar{C}. C^* w w' \Rightarrow D^* (y w) (x w') \quad (\forall I), (\forall I), (290)$$

We can prove the claim for [\(282\)](#) similarly. For this denote  $\Lambda := \Theta, w, w' : \bar{C}, w R w' : C^* w w'$ .

$$\Lambda \vdash_{\bar{T}} C^* w w' \Rightarrow D^* (x w) (y w') \quad (\forall E), (\forall E), (\text{assume}) \quad (291)$$

$$\Lambda \vdash_{\bar{T}} C^* w w' \Rightarrow D^* (y w) (z w') \quad (\forall E), (\forall E), (\text{assume}) \quad (292)$$

$$\Lambda \vdash_{\bar{T}} D^* (x w) (y w') \quad (\Rightarrow E), (291), (\text{assume}) \quad (293)$$

$$\Lambda \vdash_{\bar{T}} D^* (y w) (z w') \quad (\Rightarrow E), (292), (\text{assume}) \quad (294)$$

$$\Lambda \vdash_{\bar{T}} D^* (x w) (y w') \Rightarrow (D^* (y w) (z w'))$$

$$\Rightarrow D^* (x w) (z w') \quad \text{induction hypothesis} \quad (295)$$

$$\Lambda \vdash_{\overline{T}} D^* (y w) (z w') \Rightarrow D^* (x w) (z w') \quad (\Rightarrow E), (295), (293) \quad (296)$$

$$\Lambda \vdash_{\overline{T}} D^* (x w) (z w') \quad (\Rightarrow E), (296), (294) \quad (297)$$

$$\Theta, w, w' : \overline{C} \vdash_{\overline{T}} C^* w w' \Rightarrow D^* (x w) (z w') \quad (\Rightarrow E), (297), (\text{assume}) \quad (298)$$

$$\Theta \vdash_{\overline{T}} \forall w, w' : \overline{C}. C^* w w' \Rightarrow D^* (x w) (z w') \quad (\forall I), (\forall I), (298)$$

It remains to consider the case of  $A = B|_p$ . In this case, the claim is  $\Delta \vdash_{\overline{T}} B^* y x \wedge \overline{p} y \wedge \overline{p} x$  respectively  $\Theta \vdash_{\overline{T}} B^* x z \wedge \overline{p} x \wedge \overline{p} z$ . Applying the induction hypothesis for type  $B$  yields  $\Delta \vdash_{\overline{T}} B^* y x$  respectively  $\Theta \vdash_{\overline{T}} B^* x z$ . So it remains to show that  $\Delta \vdash_{\overline{T}} \overline{p} y \wedge \overline{p} x$  and  $\Theta \vdash_{\overline{T}} \overline{p} x \wedge \overline{p} z$  respectively hold. We can show them using rule  $(\wedge I)$  given  $\Delta \vdash_{\overline{T}} \overline{p} y$  and  $\Delta \vdash_{\overline{T}} \overline{p} x$  respectively  $\Theta \vdash_{\overline{T}} \overline{p} x$  and  $\Theta \vdash_{\overline{T}} \overline{p} z$ . Those statements follow from rule  $(\text{assume})$  and the elimination rules of  $\wedge$ .

This concludes the proof of (281) and (282).

We show (285) by induction on the grammar: Without loss of generality we may assume that  $B = B'|_p$  for  $B'$  either a base or a  $\Pi$ -type. This is due to the fact that base types and  $\Pi$ -types  $B'$  can be written as  $B'|_{\lambda x : B'. \text{true}}$  and types of the form  $B''|_p|_q$  can be rewritten as  $B''|_{\lambda x : B''. p \wedge q \ x}$ .

If  $t$  is a constant or variable then  $\bar{t}[x/x'] = \bar{t}$  and by case (PT6) resp. by case (PT4) in the definition of the translation, we have  $A^* \bar{t} \bar{t}$ . So the claim holds.

If  $t$  is a  $\lambda$ -term  $\lambda y : C. s$  and  $B' = \Pi z : C. D$ , then by induction hypothesis we have

$$\overline{\Gamma}, x, x' : \overline{A}, x R x' : A^* x x' \vdash_{\overline{T}} D^* \overline{s} \overline{s}[x/x'].$$

By the rules  $(\forall I), (\Rightarrow I)$ , we yield

$$\overline{\Gamma} \vdash_{\overline{T}} \forall x, y : \overline{A}. A^* x y \Rightarrow D^* \overline{s} \overline{s}[x/x'].$$

By definition (PT11) this is exactly

$$\overline{\Gamma}, x, x' : \overline{A}, x R x' : A^* x x' \vdash_{\overline{T}} B'^* \bar{t} \bar{t}[x/x'].$$

Since  $t$  is a  $\lambda$ -term, by assumption we have that  $B \equiv B' = B|_{\lambda z : B. \text{true}}$ , so the claim follows trivially.

If  $t$  is a function application  $f s$  with  $f$  of type  $\Pi z : C. D$  and  $s$  of type  $C$ , then by assumption  $B = D \equiv B' = B|_{\lambda z : B. \text{true}}$ , so it suffices to prove that

$$\overline{\Gamma}, x, x' : \overline{A}, x R x' : A^* x x' \vdash_{\overline{T}} D^* \overline{f} \overline{s} \overline{s}[x/x'].$$

By induction hypothesis and (283) we then have:

$$\overline{\Gamma}, x, x' : \overline{A}, x R x' : A^* x x' \vdash_{\overline{T}} (\Pi z : C. D)^* \overline{f} \overline{s}[x/x']$$

and

$$\bar{\Gamma}, x, x' : \bar{A}, xRx' : A^* x x' \vdash_{\bar{T}} C^* \bar{s} \bar{s}[x/x']. \quad (299)$$

By definition (PT11), we can unpack the former to:

$$\bar{\Gamma}, x, x' : \bar{A}, xRx' : A^* x x' \vdash_{\bar{T}} \forall z, z' : \bar{C}. C^* z z' \Rightarrow (\Pi z : C. D)^* \bar{f} z \bar{f}[x/x'] z'[x/x'] \quad (300)$$

Using the rules ( $\forall E$ ) and ( $\Rightarrow E$ ) (using (300)) to plug in  $\bar{s}$  resp.  $\bar{s}[x/x']$  for  $z, z'$  in (300), we yield:

$$\bar{\Gamma}, x, x' : \bar{A}, xRx' : A^* x x' \vdash_{\bar{T}} (\Pi z : C. D)^* \bar{f} \bar{s} \bar{f}[x/x'] \bar{s}[x/x']$$

which is exactly the desired result.

By definition (PT13), the typing relation for type `bool` is ordinary equality, so the cases of  $t$  being an implication or Boolean equality are in fact special cases of (283), which is already proven above. It remains to consider the case of  $t$  being an equality  $s =_C s'$  for  $C \neq \text{bool}$ . In this case, the induction hypothesis implies that

$$\bar{\Gamma}, x, x' : \bar{A}, xRx' : A^* x x' \vdash_{\bar{T}} C^* \bar{s} \bar{s}[x/x'] \quad (301)$$

and

$$\bar{\Gamma}, x, x' : \bar{A}, xRx' : A^* x x' \vdash_{\bar{T}} C^* \bar{s}' \bar{s}'[x/x'] \quad (302)$$

We need to prove

$$\bar{\Gamma}, x, x' : \bar{A}, xRx' : A^* x x' \vdash_{\bar{T}} C^* \bar{s} \bar{s}' =_{\text{bool}} C^* \bar{s}[x/x'] \bar{s}'[x/x'].$$

If we can show

$$\bar{\Gamma}, x, x' : \bar{A}, xRx' : A^* x x', sRs' : C^* \bar{s} \bar{s}' \vdash_{\bar{T}} C^* \bar{s}[x/x'] \bar{s}'[x/x']$$

and similarly also

$$\bar{\Gamma}, x, x' : \bar{A}, xRx' : A^* x x', \text{subrel} : C^* \bar{s}[x/x'] \bar{s}'[x/x'] \vdash_{\bar{T}} C^* \bar{s} \bar{s}',$$

then the claim follows by rule (`propExt`).

Both follows from the transitivity (282) of the typing relation  $C^*$ .

*Well-formedness of theories* Well-formedness of DHOL theories can be shown using the rules (`thyEmpty`), (`thyType'`), (`thyConst`) and (`thyAxiom`):

(`thyEmpty`):

$$\begin{array}{ll} \vdash \circ \text{Thy} & (\text{thyEmpty}) \\ \vdash^H \bar{\circ} \text{Thy} & (\text{thyEmpty}) \end{array} \quad (303)$$

(thyType’):

$$\vdash_T x_1 : A_1, \dots, x_n : A_n \text{ Ctx} \quad \text{by assumption} \quad (304)$$

$$\vdash_{\overline{T}} x_1 : \overline{A_1}, A_1^* x_1 x_1, \dots, x_n : \overline{A_n}, x_n^* : A_n^* x_n x_n \text{ Ctx} \quad \text{induction hypothesis, (304)} \quad (305)$$

$$\vdash^{H\overline{T}} \text{Thy} \quad (\text{ctxThy}), (305) \quad (306)$$

$$\vdash^{H\overline{T}}, a : \text{tp Thy} \quad (\text{thyType}), (306) \quad (307)$$

$$\vdash^{H\overline{T}}, a : \Pi x_1 : A_1. \dots \Pi x_n : A_n. \text{tp Thy} \quad \text{PT2, (307)}$$

(thyConst):

$$\vdash_T A \text{ tp} \quad \text{by assumption} \quad (308)$$

$$\vdash_{\overline{T}} \overline{A} \text{ tp} \quad \text{induction hypothesis, (308)} \quad (309)$$

$$\vdash^{H\overline{T}}, c : \overline{A} \text{ Thy} \quad (\text{thyConst}), (309) \quad (310)$$

$$\vdash^{H\overline{T}}, c : A \text{ Thy} \quad \text{PT3, (310)} \quad (311)$$

(thyAxiom):

$$\vdash_T F : \text{bool} \quad \text{by assumption} \quad (312)$$

$$\vdash_{\overline{T}} \overline{F} : \text{bool} \quad \text{induction hypothesis, (312)} \quad (313)$$

$$\vdash^{H\overline{T}}, \text{ass} : \overline{F} \text{ Thy} \quad (\text{thyAxiom}), (313) \quad (314)$$

$$\vdash^{H\overline{T}}, \text{ax} : F \text{ Thy} \quad \text{PT4, (314)} \quad (315)$$

*Well-formedness of contexts* Well-formedness of contexts can be concluded using the rules (ctxEmpty), (ctxVar) and (ctxAssume):

(ctxEmpty):

$$\vdash_T \text{Thy} \quad \text{by assumption} \quad (316)$$

$$\vdash^{H\overline{T}} \text{Thy} \quad \text{induction hypothesis, (316)} \quad (317)$$

$$\vdash_{\overline{T}} \text{Ctx} \quad (\text{ctxEmpty}), (317) \quad (318)$$

$$\vdash_{\overline{T}} \text{Ctx} \quad \text{PT5, (318)} \quad (319)$$

(ctxVar):

$$\Gamma \vdash_T A \text{ tp} \quad \text{by assumption} \quad (320)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{A} \text{ tp} \quad \text{induction hypothesis, (320)} \quad (321)$$

$$\overline{\Gamma} \vdash_{\overline{T}} A^* : \overline{A} \rightarrow \overline{A} \rightarrow \text{bool} \quad \text{induction hypothesis, (320)} \quad (322)$$

$$\vdash_{\overline{T}} \overline{\Gamma}, x : \overline{A} \text{ Ctx} \quad (\text{ctxVar}), (321) \quad (323)$$



$$\bar{\Gamma}, x : \bar{A} \vdash_{\bar{T}} A^* : \bar{A} \rightarrow \bar{A} \rightarrow \text{bool} \quad (\text{var}\vdash), (321), (322) \quad (324)$$

$$\bar{\Gamma}, x : \bar{A} \vdash_{\bar{T}} A^* x x : \text{bool} \quad (\text{appl}), (324), (\text{varS}) \quad (325)$$

$$\vdash_{\bar{T}} \bar{\Gamma}, x : \bar{A}, A^* x x \text{ Ctx} \quad (\text{ctxAssume}), (325) \quad (326)$$

$$\vdash_{\bar{T}} \overline{\Gamma, x : \bar{A} \text{ Ctx}} \quad \text{PT6}, (326) \quad (327)$$

(ctxAssume):

$$\Gamma \vdash_T F : \text{bool} \quad \text{by assumption} \quad (328)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{F} : \text{bool} \quad \text{induction hypothesis}, (328) \quad (329)$$

$$\vdash_{\bar{T}} \bar{\Gamma}, \text{ass} : \bar{F} \text{ Ctx} \quad (\text{ctxAssume}), (329) \quad (330)$$

$$\vdash_{\bar{T}} \overline{\Gamma, \text{ass} : F \text{ Ctx}} \quad \text{PT7}, (330) \quad (331)$$

*Well-formedness of types* Well-formedness of types can be shown in DHOL using the rules (type'), (pi) and ( $|_p \text{tp}$ ):

(type'):

$$a : \Pi x_1 : A_1. \dots \Pi x_n : A_n. \text{tp in } T \quad \text{by assumption} \quad (332)$$

$$\Gamma \vdash_T \Gamma \text{ Ctx} \quad \text{by assumption} \quad (333)$$

$$\vdash_{\bar{T}} \bar{\Gamma} \text{ Ctx} \quad \text{induction hypothesis}, (333) \quad (334)$$

$$a : \text{tp in } \bar{T} \quad \text{PT2}, (332) \quad (335)$$

$$a^* : a \rightarrow a \rightarrow \text{bool in } \bar{T} \quad \text{PT2}, (332) \quad (336)$$

$$\bar{\Gamma} \vdash_{\bar{T}} a \text{ tp} \quad (\text{type}), (335), (334) \quad (337)$$

$$\bar{\Gamma} \vdash_{\bar{T}} a^* : a \rightarrow a \rightarrow \text{bool} \quad (\text{constS}), (336) \quad (337)$$

$$\bar{\Gamma} \vdash_{\bar{T}} a^* : \bar{a} \rightarrow \bar{a} \rightarrow \text{bool} \quad \text{PT19}, (337)$$

(pi):

$$\Gamma \vdash_T A \text{ tp} \quad \text{by assumption} \quad (338)$$

$$\Gamma, x : A \vdash_T B \text{ tp} \quad \text{by assumption} \quad (339)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \text{ tp} \quad \text{induction hypothesis}, (338) \quad (340)$$

$$\bar{\Gamma}, x : \bar{A}, x^* : A^* x x \vdash_{\bar{T}} \bar{B} \text{ tp} \quad \text{induction hypothesis}, (339) \quad (341)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{B} \text{ tp} \quad \text{HOL types context independent}, (341) \quad (342)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \rightarrow \bar{B} \text{ tp} \quad (\text{arrow}), (340), (342) \quad (343)$$

$$\bar{\Gamma} \vdash_{\bar{T}} A^* : \bar{A} \rightarrow \bar{A} \rightarrow \text{bool} \quad \text{induction hypothesis}, (338) \quad (344)$$

$$\bar{\Gamma} \vdash_{\bar{T}} B^* : \bar{B} \rightarrow \bar{B} \rightarrow \text{bool} \quad \text{induction hypothesis}, (339) \quad (345)$$

$$\begin{aligned} \bar{\Gamma} \vdash_{\bar{T}} \overline{\Pi x : A. B} \text{ tp} & \quad \text{PT10,(343)} \\ \bar{\Gamma} \vdash_{\bar{T}} (\Pi x : A. B)^* : : (\overline{\Pi x : A. B}) \rightarrow (\overline{\Pi x : A. B}) \rightarrow \text{bool} & \quad \text{PT11,(344),(345)} \end{aligned}$$

( $|_p \text{tp}$ ):

$$\begin{aligned} \Gamma \vdash_T A \text{ tp} & \quad \text{by assumption} \quad (346) \\ \Gamma \vdash_T p : A \rightarrow \text{bool} & \quad \text{by assumption} \quad (347) \\ \bar{\Gamma} \vdash_{\bar{T}} \bar{A} \text{ tp} & \quad \text{induction hypothesis,(346)} \quad (348) \\ \bar{\Gamma} \vdash_{\bar{T}} \overline{A|_p} \text{ tp} & \quad \text{PT14,(348)} \\ \bar{\Gamma} \vdash_{\bar{T}} A^* : \bar{A} \rightarrow \bar{A} \rightarrow \text{bool} & \quad \text{induction hypothesis,(346)} \quad (349) \\ \bar{\Gamma} \vdash_{\bar{T}} (A|_p)^* : \bar{A} \rightarrow \bar{A} \rightarrow \text{bool} & \quad \text{PT15,(349)} \end{aligned}$$

*Type-equality* Type-equality can be shown using the rules ( $\text{congBase}'$ ), ( $\text{congII}$ ), ( $|_{\text{triv}}$ ), ( $|_{\text{triv}}'$ ), ( $\pi|_p \text{Cod}$ ), ( $|_p|_q$ ) and ( $|_p \equiv$ ):

( $|_p \equiv$ ):

$$\begin{aligned} \Gamma \vdash_T A \equiv A' & \quad \text{by assumption} \quad (350) \\ \Gamma \vdash_T p =_{\Pi x:A. \text{bool}} p' & \quad \text{by assumption} \quad (351) \\ \bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \bar{A}' & \quad \text{induction hypothesis,(350)} \quad (352) \\ \bar{\Gamma} \vdash_{\bar{T}} A^* =_{\bar{A} \rightarrow \bar{A} \rightarrow \text{bool}} A'^* & \quad \text{induction hypothesis,(350)} \quad (353) \\ \bar{\Gamma} \vdash_{\bar{T}} \bar{p} =_{\bar{A} \rightarrow \text{bool}} \bar{p}' & \quad \text{induction hypothesis,(351)} \quad (354) \\ \bar{\Gamma} \vdash_{\bar{T}} (A|_p)^* =_{\bar{A} \rightarrow \bar{A} \rightarrow \text{bool}} (A|_p)^* & \quad (\text{refl}), \text{PT15,(eqTyping),(353)} \quad (355) \\ \bar{\Gamma} \vdash_{\bar{T}} (A|_p)^* =_{\bar{A} \rightarrow \bar{A} \rightarrow \text{bool}} (A|_{p'})^* & \quad (\text{rewrite),(355),(354)} \quad (356) \\ \bar{\Gamma} \vdash_{\bar{T}} (A|_p)^* =_{\bar{A} \rightarrow \bar{A} \rightarrow \text{bool}} (A'|_{p'})^* & \quad \text{PT15,(rewrite),(356),(353)} \\ \bar{\Gamma} \vdash_{\bar{T}} \overline{A|_p} \equiv \overline{A'|_{p'}} & \quad \text{PT14,(352)} \end{aligned}$$

( $\text{congBase}'$ ):

$$\begin{aligned} a : \Pi x_1 : A_1. \dots \Pi x_n : A_n. \text{ tp in } T & \quad \text{by assumption} \quad (357) \\ \Gamma \vdash_T s_1 =_{A_1} t_1 & \quad \text{by assumption} \quad (358) \\ \vdots & \\ \Gamma \vdash_T s_n =_{A_n[x_1/t_1, \dots, x_{n-1}/t_{n-1}]} t_n & \quad \text{by assumption} \quad (359) \\ \vdash_T \Gamma \text{ Ctx} & \quad \text{by assumption} \quad (360) \\ a : \text{ tp in } \bar{T} & \quad \text{PT2,(357)} \quad (361) \\ a^* : \bar{A}_1 \rightarrow \dots \rightarrow \bar{A}_n \rightarrow \bar{a} \rightarrow \bar{a} \rightarrow \text{bool in } \bar{T} & \quad \text{PT2,(357)} \quad (362) \\ \bar{\Gamma} \vdash_{\bar{T}} \bar{s}_1 =_{\bar{A}_1} \bar{t}_1 & \quad \text{induction hypothesis,(358)} \quad (363) \end{aligned}$$

$$\begin{array}{ll}
\vdots & \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{s}_n =_{\bar{A}_n} \bar{t}_n & \text{induction hypothesis, (359)} \quad (364) \\
\vdash_{\bar{T}} \bar{\Gamma} \text{Ctx} & \text{induction hypothesis, (360)} \quad (365) \\
\bar{\Gamma} \vdash_{\bar{T}} a : \text{tp} & (\text{type}), (361), (365) \quad (366) \\
\bar{\Gamma} \vdash_{\bar{T}} a \equiv a & (\text{congBase}), (366) \quad (367) \\
\bar{\Gamma} \vdash_{\bar{T}} a^* =_{\bar{A}_1 \rightarrow \dots \rightarrow \bar{A}_n \rightarrow \bar{a} \rightarrow \bar{a} \rightarrow \text{bool}} a^* & (\text{refl}), (\text{constS}), (362), (365) \quad (368) \\
\bar{\Gamma} \vdash_{\bar{T}} a^* \bar{s}_1 =_{\bar{A}_2 \rightarrow \dots \rightarrow \bar{A}_n \rightarrow \bar{a} \rightarrow \bar{a} \rightarrow \text{bool}} a^* \bar{t}_1 & (\text{congAppl}), (363), (368) \quad (369) \\
\vdots & \\
\bar{\Gamma} \vdash_{\bar{T}} a^* \bar{s}_1 \dots \bar{s}_n =_{\bar{a} \rightarrow \bar{a} \rightarrow \text{bool}} a^* \bar{t}_1 \dots \bar{t}_n & (\text{congAppl}), (364), \text{previous line} \quad (370) \\
\bar{\Gamma} \vdash_{\bar{T}} \overline{a s_1 \dots s_n} \equiv \overline{a t_1 \dots t_n} & \text{PT8, (367)} \\
\bar{\Gamma} \vdash_{\bar{T}} (a s_1 \dots s_n)^* =_{\overline{a s_1 \dots s_n} \rightarrow \overline{a s_1 \dots s_n} \rightarrow \text{bool}} (a t_1 \dots t_n)^* & \text{PT9, (370)}
\end{array}$$

(congΠ):

$$\begin{array}{ll}
\Gamma \vdash_T A \equiv A' & \text{by assumption} \quad (371) \\
\Gamma, x : A \vdash_T B \equiv B & \text{by assumption} \quad (372) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \bar{A}' & \text{induction hypothesis, (371)} \quad (373) \\
\bar{\Gamma} \vdash_{\bar{T}} A^* =_{\bar{A} \rightarrow \bar{A} \rightarrow \text{bool}} A'^* & \text{induction hypothesis, (371)} \quad (374) \\
\bar{\Gamma}, x : \bar{A}, x^* : A^* x x \vdash_{\bar{T}} \bar{B} \equiv \bar{B}' & \text{induction hypothesis, (372)} \quad (375)
\end{array}$$

Since  $\equiv$  is context independent in HOL:

$$\begin{array}{ll}
\bar{\Gamma} \vdash_{\bar{T}} \bar{B} \equiv \bar{B}' & \text{explanation, (375)} \quad (376) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \rightarrow \bar{B} \equiv \bar{A}' \rightarrow \bar{B}' & (\text{cong}\rightarrow), (373), (376) \quad (377) \\
\bar{\Gamma} \vdash_{\bar{T}} \overline{\Pi x : A. B} \equiv \overline{\Pi x : A'. B'} & \text{PT10, (377)}
\end{array}$$

$$\bar{\Gamma}, x : \bar{A}, x^* : A^* x x \vdash_{\bar{T}} B^* =_{\bar{B} \rightarrow \bar{B} \rightarrow \text{bool}} B'^* \quad \text{induction hypothesis, (372)} \quad (378)$$

$$\begin{array}{ll}
\bar{\Gamma}, f : \bar{A} \rightarrow \bar{B}, x : \bar{A} \vdash_{\bar{T}} A^* x x \Rightarrow B^* (f x) (f x) & \\
=_{\text{bool}} A'^* x x \Rightarrow B^* (f x) (f x) & (\text{rewrite}), (\text{refl}), (374) \quad (379)
\end{array}$$

$$\begin{array}{ll}
\bar{\Gamma}, f : \bar{A} \rightarrow \bar{B}, x : \bar{A} \vdash_{\bar{T}} A^* x x \Rightarrow B^* (f x) (f x) & \\
=_{\text{bool}} A'^* x x \Rightarrow B'^* (f x) (f x) & (\text{rewrite}), (379), (378) \quad (380)
\end{array}$$

$$\begin{array}{ll}
\bar{\Gamma}, f : \bar{A} \rightarrow \bar{B} \vdash_{\bar{T}} \forall x : \bar{A}. A^* x x \Rightarrow (B^* (f x) (f x)) =_{\text{bool}} & \\
\forall x : \bar{A}'. A'^* x x \Rightarrow (B'^* (f x) (f x)) & (\forall \text{cong}), (373), (380) \quad (381)
\end{array}$$

$$\bar{\Gamma} \vdash_{\bar{T}} (\Pi x : A. B)^* =_{\bar{A} \rightarrow \bar{A} \rightarrow \text{bool}} (\Pi x : A'. B')^* \quad \text{PT18, (cong}\lambda), (381)$$

( $\text{Irriv}$ ):

$$\begin{array}{ll}
\Gamma \vdash_T A \text{ tp} & \text{by assumption} \quad (382) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \text{ tp} & \text{induction hypothesis, (382)} \quad (383) \\
\bar{\Gamma} \vdash_{\bar{T}} A^* : \bar{A} \rightarrow \bar{A} \rightarrow \text{bool} & \text{induction hypothesis, (382)} \quad (384) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \bar{A} & (\equiv \text{refl}), (383) \quad (385) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \overline{A|_{\lambda x:A. \text{true}}} & (\text{PT14}), (385) \\
\bar{\Gamma}, x : \bar{A} \vdash_{\bar{T}} \lambda x : A. \text{true } x & \text{Lemma 2, (beta)} \quad (386) \\
\bar{\Gamma}, x : \bar{A}, x^* : A^* x x \vdash_{\bar{T}} A^* x x \wedge \lambda x : A. \text{true } x & (\wedge \text{I}), (\text{assume}), (386) \quad (387) \\
\bar{\Gamma}, x : \bar{A}, x^* : A^* x x \wedge \lambda x : A. \text{true } x \vdash_{\bar{T}} A^* x x & (\wedge \text{E}), (\text{assume}) \quad (388) \\
\bar{\Gamma}, x : \bar{A} \vdash_{\bar{T}} A^* x x =_{\text{bool}} (A|_{\lambda x:A. \text{true}})^* x x & (\text{propExt}), (387), (388)
\end{array}$$

( $\text{Irriv}'$ ):

$$\begin{array}{ll}
\Gamma \vdash_T A \text{ tp} & \text{by assumption} \quad (389) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \text{ tp} & \text{induction hypothesis, (389)} \quad (390) \\
\bar{\Gamma} \vdash_{\bar{T}} A^* : \bar{A} \rightarrow \bar{A} \rightarrow \text{bool} & \text{induction hypothesis, (389)} \quad (391) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \bar{A} & (\equiv \text{refl}), (390) \quad (392) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \overline{A|_{\lambda x:A. \text{true}}} & (\text{PT14}), (392) \\
\bar{\Gamma}, x : \bar{A} \vdash_{\bar{T}} \lambda x : A. \text{true } x & \text{Lemma 2, (beta)} \quad (393) \\
\bar{\Gamma}, x : \bar{A}, x^* : A^* x x \vdash_{\bar{T}} A^* x x \wedge \lambda x : A. \text{true } x & (\wedge \text{I}), (\text{assume}), (393) \quad (394) \\
\bar{\Gamma}, x : \bar{A}, x^* : A^* x x \wedge \lambda x : A. \text{true } x \vdash_{\bar{T}} A^* x x & (\wedge \text{E}), (\text{assume}) \quad (395) \\
\bar{\Gamma}, x : \bar{A} \vdash_{\bar{T}} (A|_{\lambda x:A. \text{true}})^* x x =_{\text{bool}} A^* x x & (\text{propExt}), (395), (394)
\end{array}$$

( $\pi|_p \text{Cod}$ ):

$$\begin{array}{ll}
\Gamma \vdash_T A \text{ tp} & \text{by assumption} \quad (396) \\
\Gamma, x : A \vdash_T B \text{ tp} & \text{by assumption} \quad (397) \\
\Gamma, x : A \vdash_T p : \Pi y : B. \text{bool} & \text{by assumption} \quad (398) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \text{ tp} & \text{induction hypothesis, (396)} \quad (399) \\
\bar{\Gamma} \vdash_{\bar{T}} A^* : \bar{A} \rightarrow \bar{A} \rightarrow \text{bool} & \text{induction hypothesis, (396)} \quad (400) \\
\bar{\Gamma}, x : \bar{A}, x^* : A^* x x \vdash_{\bar{T}} \bar{B} \text{ tp} & \text{induction hypothesis, (397)} \quad (401) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{B} \text{ tp} & \text{HOL types context independent, (401)} \quad (402) \\
\bar{\Gamma}, x : \bar{A}, x^* : A^* x x \vdash_{\bar{T}} B^* : \bar{B} \rightarrow \bar{B} \rightarrow \text{bool} & \text{induction hypothesis, (397)} \quad (403) \\
\bar{\Gamma} \vdash_{\bar{T}} B^* : \bar{B} \rightarrow \bar{B} \rightarrow \text{bool} & \text{HOL types context independent, (403)} \quad (404) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \rightarrow \bar{B} \text{ tp} & (\text{arrow}), (399), (402) \quad (405)
\end{array}$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \rightarrow \bar{B} \equiv \bar{A} \rightarrow \bar{B} \quad (\text{congBase}), (405) \quad (406)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \overline{\Pi x : A. B}|_p \equiv \overline{(\Pi x : A. B)|_{\lambda f : \Pi x : A. B. \forall x : A. p(f x)}} \quad (\text{PT14}), (\text{PT10}), (406)$$

Denote  $F := \forall x, x' : \bar{A}. A^* x x' \Rightarrow B^*(f x)(f x') \wedge \forall x, x' : \bar{A}. A^* x x' \Rightarrow \bar{p}(f x)$ ,  
 $G := \forall x, x' : \bar{A}. A^* x x' \Rightarrow (B^*(f x)(f x') \wedge \bar{p}(f x))$ . Further denote  $\Delta := \bar{\Gamma}, f : \bar{A} \rightarrow \bar{B}$ ,

$$\Theta := \Delta, \text{ass}_F : F, x, x' : \bar{A}, x R x' : A^* x x'$$

and

$$\Lambda := \Delta, \text{ass}_G : G, x, x' : \bar{A}, x R x' : A^* x x'.$$

$$\Theta \vdash_{\bar{T}} B^*(f x)(f x') \quad (\forall E), (\Rightarrow E), (\wedge E), (\text{assume}), (\text{assume}) \quad (407)$$

$$\Theta \vdash_{\bar{T}} \bar{p}(f x) \quad (\forall E), (\Rightarrow E), (\wedge E), (\text{assume}), (\text{assume}) \quad (408)$$

$$\Theta \vdash_{\bar{T}} B^*(f x)(f x') \wedge \bar{p}(f x) \quad (\wedge I), (407), (408) \quad (409)$$

$$\Delta, \text{ass}_F : F \vdash_{\bar{T}} G \quad (\forall I), (\forall I), (\Rightarrow I), (409) \quad (410)$$

$$\Lambda \vdash_{\bar{T}} B^*(f x)(f x') \wedge \bar{p}(f x) \quad (\Rightarrow E), (\forall E), (\forall E), (\text{assume}), (\text{assume}) \quad (411)$$

$$\Lambda \vdash_{\bar{T}} B^*(f x)(f x') \quad (\wedge E), (411) \quad (412)$$

$$\Lambda \vdash_{\bar{T}} \bar{p}(f x) \quad (\wedge E), (411) \quad (413)$$

$$\Delta, \text{ass}_G : G \vdash_{\bar{T}} \forall x, x' : \bar{A}. A^* x x' \Rightarrow B^*(f x)(f x') \quad (\forall I), (\forall I), (\Rightarrow I), (411) \quad (414)$$

$$\Delta, \text{ass}_G : G \vdash_{\bar{T}} \forall x, x' : \bar{A}. A^* x x' \Rightarrow \bar{p}(f x) \quad (\forall I), (\forall I), (\Rightarrow I), (412) \quad (415)$$

$$\Delta, \text{ass}_G : G \vdash_{\bar{T}} F \quad (\wedge I), (414), (415) \quad (416)$$

$$\Delta \vdash_{\bar{T}} F =_{\text{bool}} G \quad (\text{propExt}), (416), (416) \quad (417)$$

$$\Delta \vdash_{\bar{T}} \lambda f : (\Pi x : A. B). \forall x : A. p(f x) f =_{\text{bool}} \forall x, x' : \bar{A}. A^* x x' \Rightarrow \bar{p}(f x) \quad (\text{beta}) \quad (418)$$

$$\Delta \vdash_{\bar{T}} (\Pi x : A. B)|_{\lambda f : (\Pi x : A. B). \forall x : A. p(f x)}^* f f =_{\text{bool}} F \quad (\text{rewrite}), (\text{refl}), (418) \quad (419)$$

$$\Delta \vdash_{\bar{T}} (\Pi x : A. B)|_{\lambda f : (\Pi x : A. B). \forall x : A. p(f x)}^* f f =_{\text{bool}} G \quad (\text{trans}), (419), (417) \quad (420)$$

$$\Delta \vdash_{\bar{T}} (\Pi x : A. B)|_p^* f f =_{\text{bool}} ((\Pi x : A. B)|_{\lambda f : (\Pi x : A. B). \forall x : A. p(f x)})^* f f \quad (\text{PT11}), (\text{PT15}), (420)$$

$(|_p|_q)$ :

$$\Gamma \vdash_T A \text{ tp} \quad \text{by assumption} \quad (421)$$

$$\Gamma \vdash_T p : \Pi y : B. \text{bool} \quad \text{by assumption} \quad (422)$$

$$\begin{array}{ll}
\Gamma \vdash_T q : \Pi y : B. \text{bool} & \text{by assumption} \quad (423) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \text{ tp} & \text{induction hypothesis, (421)} \\
& (424) \\
\bar{\Gamma} \vdash_{\bar{T}} A^* : \bar{A} \rightarrow \bar{A} \rightarrow \text{bool} & \text{induction hypothesis, (421)} \\
& (425) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{p} : \bar{B} \rightarrow \text{bool} & \text{induction hypothesis, (422)} \\
& (426) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{q} : \bar{B} \rightarrow \text{bool} & \text{induction hypothesis, (422)} \\
& (427) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \bar{A} & (\text{congBase}), (424) \quad (428) \\
\bar{\Gamma} \vdash_{\bar{T}} \overline{A|_p|_q} \equiv \overline{A|_{\lambda x:A. p \ x \wedge q \ x}} & (\text{PT14}), (428) \\
\bar{\Gamma}, x : \bar{A} \vdash_{\bar{T}} A^* \ x \ x \wedge \bar{p} \ x \wedge \bar{q} \ x : \text{bool} & (\text{appl}) \text{ repeatedly, (varS), (426), (427)} \\
& (429) \\
\bar{\Gamma}, x : \bar{A} \vdash_{\bar{T}} A^* \ x \ x \wedge \bar{p} \ x \wedge \bar{q} \ x =_{\text{bool}} & \\
A^* \ x \ x \wedge \bar{p} \ x \wedge \bar{q} \ x & (\text{refl}), (429) \quad (430) \\
\bar{\Gamma}, x : \bar{A} \vdash_{\bar{T}} \left( \lambda x : \bar{A}. \bar{p} \ x \wedge \bar{q} \ x \right) x : \text{bool} & (\text{appl}), (\text{lambda}), (429), (\text{varS}) \\
& (431) \\
\bar{\Gamma}, x : \bar{A} \vdash_{\bar{T}} \left( \lambda x : \bar{A}. \bar{p} \ x \wedge \bar{q} \ x \right) x & \\
=_{\text{bool}} \bar{p} \ x \wedge \bar{q} \ x & (\text{beta}), (431) \quad (432) \\
\bar{\Gamma}, x : \bar{A} \vdash_{\bar{T}} (A|_p|_q)^* \ x \ x =_{\text{bool}} (A|_{\lambda x:A. p \ x \wedge q \ x})^* \ x \ x & (\text{rewrite}), (430), (432)
\end{array}$$

*Subtyping* Subtyping can be shown using the rules ( $<:\text{Top}$ ), ( $<:\text{I}$ ), ( $<:\text{Pi}$ ) and ( $<:|_p$ ).

( $<:\text{Top}$ ):

$$\begin{array}{ll}
\Gamma \vdash_T A <: A' & \text{by assumption} \quad (433) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \bar{A}' & \text{induction hypothesis, (433)} \\
\bar{\Gamma}, x, y : \bar{A} \vdash_{\bar{T}} A^* \ x \ y \Rightarrow A'^* \ x \ y & \text{induction hypothesis, (433)} \quad (434) \\
\bar{\Gamma}, x, y : \bar{A}, x R y : (A|_p)^* \ x \ y \vdash_{\bar{T}} A'^* \ x \ y & (\Rightarrow E), (434), (\wedge E), \text{PT15}, (\text{assume}) \\
& (435) \\
\bar{\Gamma}, x, y : \bar{A} \vdash_{\bar{T}} (A|_p)^* \ x \ y \Rightarrow A'^* \ x \ y & (\Rightarrow I), (435)
\end{array}$$

( $<:\text{I}$ ):

$$\begin{array}{ll}
\Gamma \vdash_T A \equiv A' & \text{by assumption} \quad (436) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \bar{A}' & \text{induction hypothesis, (436)} \quad (437)
\end{array}$$

$$\bar{\Gamma} \vdash_{\bar{T}} A^* =_{\bar{A} \rightarrow \bar{A} \rightarrow \text{bool}} A'^* \quad \text{induction hypothesis, (436)} \quad (438)$$

$$\bar{\Gamma}, x, y : \bar{A}, xRy : A^* x y \vdash_{\bar{T}} A'^* x y \quad (\text{rewrite}), (\text{assume}), (438) \quad (439)$$

$$\bar{\Gamma}, x, y : \bar{A} \vdash_{\bar{T}} A^* x y \Rightarrow A'^* x y \quad (\Rightarrow I), (439)$$

( $< : Pi$ ):

$$\Gamma \vdash_T A' < : A \quad \text{by assumption} \quad (440)$$

$$\Gamma, x : A' \vdash_T B < : B' \quad \text{by assumption} \quad (441)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{A}' \equiv \bar{A} \quad \text{induction hypothesis, (440)} \quad (442)$$

Since HOL types cannot depend on terms:

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{B}' \equiv \bar{B} \quad \text{induction hypothesis, (441)} \quad (443)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \rightarrow \bar{B} \equiv \bar{A}' \rightarrow \bar{B}' \quad (\text{cong} \rightarrow), (442), (443)$$

$$\bar{\Gamma}, x, y : \bar{A} \vdash_{\bar{T}} A'^* x y \Rightarrow A^* x y \quad \text{induction hypothesis, (440)} \quad (444)$$

$$\bar{\Gamma}, x, y : \bar{A}', xRy : A'^* x y, z, z' : \bar{B}' \vdash_{\bar{T}} B^* z z' \Rightarrow B'^* z z' \quad \text{induction hypothesis, (441)} \quad (445)$$

$$\bar{\Gamma}, x, y : \bar{A}', x^* : A'^* x x \vdash_{\bar{T}} \forall z, z' : \bar{B}'. B^* z z' \Rightarrow B'^* z z' \quad (\forall I), (\forall I), (445) \quad (446)$$

$$\bar{\Gamma}, f : \overline{\Pi x : A. B}, x, y : \bar{A}', xRy : A'^* x y \vdash_{\bar{T}}$$

$$B^* (f x) (f y) \Rightarrow B'^* (f x) (f y) \quad (\forall E), (\forall E), (446) \quad (447)$$

$$\bar{\Gamma}, f : \overline{\Pi x : A. B}, x, y : \bar{A}' \vdash_{\bar{T}} (A^* x y \Rightarrow B^* (f x) (f y) \Rightarrow$$

$$(A'^* x y \Rightarrow B'^* (f x) (f y)) \quad (\Rightarrow \text{Funct}), (444), (447) \quad (448)$$

$$\bar{\Gamma}, f : \overline{\Pi x : A. B} \vdash_{\bar{T}} \left( \forall x, y : \bar{A}'. A^* x y \Rightarrow B^* (f x) (f y) \right) \Rightarrow$$

$$\left( \forall x, y : \bar{A}'. A'^* x y \Rightarrow B'^* (f x) (f y) \right) \quad (\forall \Rightarrow), (\forall \Rightarrow), (448) \quad (449)$$

$$\bar{\Gamma}, f : \overline{\Pi x : A. B} \vdash_{\bar{T}} (\Pi x : A. B)^* f f \Rightarrow (\Pi x : A'. B')^* f f \quad \text{PT11, (449)}$$

( $< : |_p$ ):

$$\Gamma \vdash_T A < : A' \quad \text{by assumption} \quad (450)$$

$$\Gamma, x : A \vdash_T p x \Rightarrow p' x \quad \text{by assumption} \quad (451)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \bar{A}' \quad \text{induction hypothesis, (450)}$$

$$\bar{\Gamma}, x, y : \bar{A} \vdash_{\bar{T}} A^* x y \Rightarrow A'^* x y \quad \text{induction hypothesis, (450)} \quad (452)$$

$$\bar{\Gamma}, x : \bar{A}, x^* : A^* x x \vdash_{\bar{T}} \bar{p} x \Rightarrow \bar{p}' x \quad \text{induction hypothesis, (451)} \quad (453)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \forall x : \bar{A}. A^* x x \Rightarrow \bar{p} x \Rightarrow \bar{p}' x \quad (\forall I), (\Rightarrow I), (453) \quad (454)$$

$$\bar{\Gamma}, x, y : \bar{A}', xRy : (A|_p)^* x y \vdash_{\bar{T}} \bar{p} x \wedge \bar{p} y \quad (\wedge E), (\text{assume}) \quad (455)$$

$$\bar{\Gamma}, x, y : \bar{A}', xRy : (A|_p)^* x y \vdash_{\bar{T}} A^* x y \quad (\wedge E), (\text{assume}) \quad (456)$$

$$\bar{\Gamma}, x, y : \bar{A}', xRy : (A|_p)^* x y \vdash_{\bar{T}} A^* x y =_{\text{bool}} A^* x x \quad (285), \text{PT13, (refl)}, (456) \quad (457)$$

$$\bar{\Gamma}, x, y : \bar{A}', xRy : (A|_p)^* x y \vdash_{\bar{T}} A^* x y =_{\text{bool}} A^* y y \quad (285), \text{PT13}, (\text{refl}), (456) \quad (458)$$

$$\bar{\Gamma}, x, y : \bar{A}', xRy : (A|_p)^* x y \vdash_{\bar{T}} A^* x x \quad (\text{cong}\vdash), (457), (456) \quad (459)$$

$$\bar{\Gamma}, x, y : \bar{A}', xRy : (A|_p)^* x y \vdash_{\bar{T}} A^* y y \quad (\text{cong}\vdash), (458), (456) \quad (460)$$

$$\bar{\Gamma}, x, y : \bar{A}', xRy : (A|_p)^* x y, \text{ass} : \bar{p} x \wedge \bar{p} y \vdash_{\bar{T}} \bar{p}' x \quad (\Rightarrow E), (\forall E), (453) \quad (461)$$

$$\bar{\Gamma}, x, y : \bar{A}', xRy : (A|_p)^* x y, \text{ass} : \bar{p} x \wedge \bar{p} y \vdash_{\bar{T}} \bar{p}' y \quad (\Rightarrow E), (\forall E), (453) \quad (462)$$

$$\bar{\Gamma}, x, y : \bar{A}', xRy : (A|_p)^* x y \vdash_{\bar{T}} \bar{p} x \wedge \bar{p} y \Rightarrow \bar{p}' x \wedge \bar{p}' y \quad (\Rightarrow I), (\wedge I), (461), (462) \quad (463)$$

$$\bar{\Gamma}, x, y : \bar{A}', (A|_p)^* x x \vdash_{\bar{T}} \bar{p}' x \wedge \bar{p}' y \quad (\Rightarrow E), (463), (455) \quad (464)$$

$$\bar{\Gamma}, x, y : \bar{A}', xRy : (A|_p)^* x y \vdash_{\bar{T}} A'^* x y \quad (\Rightarrow E), (452), (456) \quad (465)$$

$$\bar{\Gamma}, x, y : \bar{A}', xRy : (A|_p)^* x y \vdash_{\bar{T}} (A'|_{p'})^* x x \quad (\wedge I), (\wedge I), (465), (464), (464) \quad (466)$$

$$\bar{\Gamma}, x, y : \bar{A}'|_{p'} \vdash_{\bar{T}} (A|_p)^* x y \Rightarrow (A'|_{p'})^* x y \quad \text{PT14}, (\Rightarrow I), (466)$$

*Typing* Typing can be shown using the rules ( $|_p I$ ), ( $|_p E$ ), ( $\text{lambda}'$ ), ( $\text{appl}'$ ), ( $\Rightarrow \text{type}'$ ), ( $\text{const}$ ), ( $\text{cong}$ ), ( $\text{var}$ ), ( $= \text{type}$ ):

( $|_p I$ ):

$$\Gamma \vdash_T t : A \quad \text{by assumption} \quad (467)$$

$$\Gamma \vdash_T p t \quad \text{by assumption} \quad (468)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{t} : \bar{A} \quad \text{induction hypothesis}, (467) \quad (469)$$

$$\bar{\Gamma} \vdash_{\bar{T}} A^* \bar{t} \quad \text{induction hypothesis}, (467) \quad (470)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{p} \bar{t} \quad \text{induction hypothesis}, (468) \quad (471)$$

$$\bar{\Gamma} \vdash_{\bar{T}} (A|_p)^* \bar{t} \quad \text{PT15}, (\wedge I), (470), (\wedge I), (471), (471)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{t} : \bar{A}|_p \quad \text{PT14}, (469)$$

( $|_p E$ ):

$$\Gamma \vdash_T t : A \quad \text{by assumption} \quad (472)$$

$$\Gamma \vdash_T A <: A' \quad \text{by assumption} \quad (473)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{t} : \bar{A} \quad \text{induction hypothesis}, (472) \quad (474)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \bar{A}' \quad \text{induction hypothesis}, (473) \quad (475)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{t} : \bar{A}' \quad (\text{cong}), (474), (475)$$

$$\bar{\Gamma} \vdash_{\bar{T}} A^* \bar{t} \bar{t} \quad \text{induction hypothesis}, (474) \quad (476)$$

$$\bar{\Gamma}, x : \bar{A}' \vdash_{\bar{T}} A^* x x \Rightarrow (A')^* x x \quad \text{induction hypothesis}, (473) \quad (477)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \forall x : \bar{A}'. A^* x x \Rightarrow (A')^* x x \quad \text{induction hypothesis}, (473) \quad (478)$$

$$\bar{\Gamma} \vdash_{\bar{T}} (A')^* t t \quad (\Rightarrow E), (\forall E), (478), (476)$$



(*lambda'*):

$$\begin{array}{ll}
\Gamma, x : \bar{A} \vdash_T t : B & \text{by assumption} \quad (479) \\
\Gamma, x : \bar{A}, x^* : A^* x x \vdash_{\bar{T}} \bar{t} : \bar{B} & \text{induction hypothesis, PT6, (479)} \quad (480) \\
\Gamma, x : \bar{A}, x^* : A^* x x \vdash_{\bar{T}} B^* \bar{t} \bar{t} & \text{induction hypothesis, PT6, (479)} \quad (481) \\
\Gamma, x, y : \bar{A}, x R y : A^* x y \vdash_{\bar{T}} B^* \bar{t} \bar{t} [x/y] & (285), (481) \quad (482) \\
\Gamma \vdash_T \forall x, y : \bar{A}. A^* x y \Rightarrow B^* \bar{t} \bar{t} [x/y] & (\Rightarrow I), (VI), (481) \quad (483) \\
\Gamma, x : A \vdash_{\bar{T}} \bar{t} : \bar{B} & \text{typing independent of assumptions, (480)} \quad (484) \\
\bar{\Gamma} \vdash_{\bar{T}} (\lambda x : \bar{A}. \bar{t}) : \bar{A} \rightarrow \bar{B} & (\text{lambda}), (484) \quad (485) \\
\bar{\Gamma} \vdash_{\bar{T}} \lambda x : A. t : \Pi x : A. B & \text{PT18, PT10, (485)} \\
\bar{\Gamma} \vdash_{\bar{T}} (\Pi x : A. B)^* \quad \lambda x : A. t & \text{PT11, (482)}
\end{array}$$

(*appl'*):

$$\begin{array}{ll}
\Gamma \vdash_T f : \Pi x : A. B & \text{by assumption} \quad (486) \\
\Gamma \vdash_T t : A & \text{by assumption} \quad (487) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{f} : \bar{A} \rightarrow \bar{B} & \text{induction hypothesis, PT10, (486)} \quad (488) \\
\bar{\Gamma} \vdash_{\bar{T}} (\Pi x : A. B)^* \bar{f} \bar{f} & \text{induction hypothesis, PT10, (486)} \quad (489) \\
\bar{\Gamma} \vdash_{\bar{T}} \forall x : \bar{A}. \forall y : \bar{A}. & \\
A^* x y \Rightarrow B^* (\bar{f} x) (\bar{f} y) & \text{PT11, (489)} \quad (490) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{t} : \bar{A} & \text{induction hypothesis, (487)} \quad (491) \\
\bar{\Gamma} \vdash_{\bar{T}} A^* \bar{t} \bar{t} & \text{induction hypothesis, (487)} \quad (492) \\
\bar{\Gamma} \vdash_{\bar{T}} A^* \bar{t} \bar{t} \Rightarrow B^* (\bar{f} \bar{t}) (\bar{f} \bar{t}) & (\forall E), (\forall E), (490), (491), (491) \quad (493) \\
\bar{\Gamma} \vdash_{\bar{T}} B^* (\bar{f} \bar{t}) (\bar{f} \bar{t}) & (\Rightarrow E), (493), (492) \quad (494) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{f} \bar{t} : \bar{B} & (\text{appl}), (488), (491) \quad (495) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{f} \bar{t} : \bar{B} & \text{PT19, (495)} \\
\bar{\Gamma} \vdash_{\bar{T}} B^* \bar{f} \bar{t} \bar{f} \bar{t} & \text{PT19, (493)}
\end{array}$$

(*=>type'*):

$$\begin{array}{ll}
\Gamma \vdash_T F : \text{bool} & \text{by assumption} \quad (496) \\
\Gamma, \text{ass} : F \vdash_T G : \text{bool} & \text{by assumption} \quad (497) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{F} : \text{bool} & \text{induction hypothesis, (496)} \quad (498) \\
\bar{\Gamma}, \bar{F} \vdash_{\bar{T}} \bar{G} : \text{bool} & \text{induction hypothesis, (497)} \quad (499) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{G} : \text{bool} & \text{typing is independent of assumptions, (499)} \quad (500)
\end{array}$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{F} \Rightarrow \bar{G} : \text{bool} \quad (\Rightarrow \text{type}), (498), (500) \quad (501)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \overline{F \Rightarrow G} : \text{bool} \quad \text{PT20}, (501) \quad (502)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \text{bool}^* \overline{F \Rightarrow G} \overline{F \Rightarrow G} \quad (\text{PT13}), (\text{refl}), (502)$$

(*const'*):

$$c : A' \text{ in } T \quad \text{by assumption} \quad (503)$$

$$\Gamma \vdash_T A' <: A \quad \text{by assumption} \quad (504)$$

$$c : \bar{A}' \text{ in } \bar{T} \quad \text{PT3}, (503) \quad (505)$$

$$c^* : A'^* c \text{ in } \bar{T} \quad \text{PT3}, (503) \quad (506)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{A}' \equiv \bar{A} \quad \text{induction hypothesis}, (504) \quad (507)$$

$$\bar{\Gamma}, x, y : \bar{A}' \vdash_{\bar{T}} A'^* x y \Rightarrow A^* x y \quad \text{induction hypothesis}, (504) \quad (508)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \forall x, y : \bar{A}. A'^* x y \Rightarrow A^* x y \quad (\forall \text{I}), (\forall \text{I}), (508) \quad (509)$$

$$\bar{\Gamma} \vdash_{\bar{T}} c : \bar{A} \quad (\text{const}), (505), (507) \quad (510)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{c} : \bar{A} \quad \text{PT3}, (510)$$

$$\bar{\Gamma} \vdash_{\bar{T}} A'^* \bar{c} \bar{c} \quad \text{PT3}, (\text{axiom}), (506) \quad (511)$$

$$\bar{\Gamma} \vdash_{\bar{T}} A^* \bar{c} \bar{c} \quad (\forall \text{E}), (\forall \text{E}), (\Rightarrow \text{E}), (509), (511)$$

(*var'*):

$$x : A' \text{ in } \Gamma \quad \text{by assumption} \quad (512)$$

$$\Gamma \vdash_T A' <: A \quad \text{by assumption} \quad (513)$$

$$c : \bar{A}' \text{ in } \bar{\Gamma} \quad \text{PT3}, (512) \quad (514)$$

$$c^* : A'^* c \text{ in } \bar{\Gamma} \quad \text{PT3}, (512) \quad (515)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{A}' \equiv \bar{A} \quad \text{induction hypothesis}, (513) \quad (516)$$

$$\bar{\Gamma}, x, y : \bar{A}' \vdash_{\bar{T}} A'^* x y \Rightarrow A^* x y \quad \text{induction hypothesis}, (513) \quad (517)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \forall x, y : \bar{A}. A'^* x y \Rightarrow A^* x y \quad (\forall \text{I}), (\forall \text{I}), (517) \quad (518)$$

$$\bar{\Gamma} \vdash_{\bar{T}} c : \bar{A} \quad (\text{var}), (514), (516) \quad (519)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{c} : \bar{A} \quad \text{PT3}, (519)$$

$$\bar{\Gamma} \vdash_{\bar{T}} A'^* \bar{c} \bar{c} \quad \text{PT3}, (\text{assume}), (515) \quad (520)$$

$$\bar{\Gamma} \vdash_{\bar{T}} A^* \bar{c} \bar{c} \quad (\forall \text{E}), (\forall \text{E}), (\Rightarrow \text{E}), (518), (520)$$

(*=type*):

$$\Gamma \vdash_T s : A \quad \text{by assumption} \quad (521)$$

$$\Gamma \vdash_T t : A \quad \text{by assumption} \quad (522)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{s} : \bar{A} \quad \text{induction hypothesis, (521)} \quad (523)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{t} : \bar{A} \quad \text{induction hypothesis, (522)} \quad (524)$$

$$\bar{\Gamma} \vdash_{\bar{T}} A^* \bar{s} \bar{s} \quad \text{induction hypothesis, (521)} \quad (525)$$

$$\Gamma \vdash_T A \text{ tp} \quad (\text{typingTp}), (521) \quad (526)$$

Since we are proving completeness w.r.t. the individual judgements one by one, we may assume here that the translation is complete w.r.t. those judgements, for which we already proved completeness. We are therefore allowed to use completeness w.r.t. well-formedness of types here.

$$\bar{\Gamma} \vdash_{\bar{T}} A^* : \bar{A} \rightarrow \bar{A} \rightarrow \text{bool} \quad \text{completeness w.r.t. well-formedness of } A, (526) \quad (527)$$

$$\bar{\Gamma} \vdash_{\bar{T}} A^* \bar{s} \bar{t} : \text{bool} \quad (\text{appl}), (\text{appl}), (527), (523), (524) \quad (528)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \text{bool}^* A^* \bar{s} \bar{t} A^* \bar{s} \bar{t} \quad (\text{PT13}), (\text{refl}), (528)$$

*Term equality* Fix a context. By rule [\(rewrite\)](#), if we can show for two DHOL terms  $s, t : A$  that  $\bar{s} =_{\bar{A}} \bar{t}$  and additionally that  $A^* \bar{s} \bar{s}$ , then  $A^* \bar{t} \bar{t}$  and  $A^* \bar{s} \bar{t}$  follow. By rule [\(eqTyping\)](#) and rule [\(sym\)](#) we further yield  $\bar{s} : \bar{A}$  and  $\bar{t} : \bar{A}$ . This reduces the completeness claim for a term-equality  $s =_A t$  to showing  $\bar{s} =_{\bar{A}} \bar{t}$  and  $A^* \bar{s} \bar{s}$ .

Term equality can be shown using the rules [\(congAppl'\)](#), [\(congλ'\)](#), [\(etaPi\)](#), [\(refl\)](#), [\(sym\)](#) and [\(beta\)](#) in DHOL.

[\(congAppl'\)](#)

$$\Gamma \vdash_T t =_A t' \quad \text{by assumption} \quad (529)$$

$$\Gamma \vdash_T f =_{\Pi x:A. B} f' \quad \text{by assumption} \quad (530)$$

$$\bar{\Gamma} \vdash_{\bar{T}} A^* \bar{t} \bar{t}' \quad \text{induction hypothesis, (529)} \quad (531)$$

$$\begin{aligned} \bar{\Gamma} \vdash_{\bar{T}} \forall x : \bar{A}. \forall y : \bar{A}. A^* x y \Rightarrow \\ (\Pi z : A. B)^* \bar{f} x \bar{f}' x \end{aligned} \quad \text{induction hypothesis, (530)} \quad (532)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{t} : \bar{A} \quad \text{induction hypothesis, (529)} \quad (533)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{t}' : \bar{A} \quad \text{induction hypothesis, (529)} \quad (534)$$

$$\bar{\Gamma} \vdash_{\bar{T}} A^* \bar{t} \bar{t}' \Rightarrow (\Pi z : A. B)^* \bar{f} \bar{t} \bar{f}' \bar{t}' \quad (\forall E), (\forall E), (532), (533), (534) \quad (535)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{f} : \bar{A} \rightarrow \bar{B} \quad \text{induction hypothesis, (530)} \quad (536)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{f}' : \bar{A} \rightarrow \bar{B} \quad \text{induction hypothesis, (530)} \quad (537)$$

$$\bar{\Gamma} \vdash_{\bar{T}} (\Pi z : A. B)^* \bar{f} \bar{t} \bar{f}' \bar{t}' \quad (\Rightarrow E), (535), (531)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{f} \bar{t} : \bar{B} \quad (\text{appl}), (536), (533)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{f}' \bar{t}' : \bar{B} \quad (\text{appl}), (536), (533)$$

(*congλ'*) This case will use (285).

$$\begin{array}{lll}
\Gamma \vdash_T A \equiv A' & \text{by assumption} & (538) \\
\Gamma, x : A \vdash_T t =_B t' & \text{by assumption} & (539) \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{A} \equiv \bar{A}' & \text{induction hypothesis, (538)} & (540) \\
\bar{\Gamma}, x : \bar{A}, x^* : A^* x x \vdash_{\bar{T}} B^* \bar{t} \bar{t}' & \text{induction hypothesis, (539)} & (541) \\
\bar{\Gamma}, z : \bar{A}, z^* : A^* z z \vdash_{\bar{T}} B^* \bar{t}[x/z] \bar{t}'[x/z] & \alpha\text{-renaming, (541)} & (542) \\
\bar{\Gamma}, z : \bar{A} \vdash_{\bar{T}} A^* z z \Rightarrow & & \\
\quad B^* \bar{t}[x/z] \bar{t}'[x/z] & (\Rightarrow I), (542) & (543) \\
\bar{\Gamma} \vdash_{\bar{T}} \forall z : \bar{A}. A^* z z \Rightarrow & & \\
\quad B^* \bar{t}[x/z] \bar{t}'[x/z] & (\forall I), (543) & (544) \\
\bar{\Gamma}, x, y : \bar{A} \vdash_{\bar{T}} \forall z : \bar{A}. A^* z z \Rightarrow & & \\
\quad B^* \bar{t}[x/z] \bar{t}'[x/z] & (\text{var} \vdash), (\text{var} \vdash), (544) & (545) \\
\bar{\Gamma}, x, y : \bar{A} \vdash_{\bar{T}} A^* x x \Rightarrow B^* \bar{t} \bar{t}' & (\text{var} \vdash), (\text{var} \vdash), (545) & (546) \\
\bar{\Gamma}, x, y : \bar{A}, x R y : A^* x y \vdash_{\bar{T}} A^* x x \Rightarrow B^* \bar{t} \bar{t}' & (\text{monotonic} \vdash), (546) & (547) \\
\bar{\Gamma}, x, y : \bar{A}, x R y : A^* x y \vdash_{\bar{T}} A^* x x & (285), (\text{assume}), (\text{assume}) & (548) \\
\bar{\Gamma}, x, y : \bar{A}, x R y : A^* x y \vdash_{\bar{T}} B^* \bar{t} \bar{t}' & (\Rightarrow E), (547), (548) & (549) \\
\bar{\Gamma}, x, y : \bar{A}, x R y : A^* x y \vdash_{\bar{T}} B^* \bar{t} \bar{t}'[x/y] & (285), (549), (\text{assume}) & (550) \\
\bar{\Gamma}, x, y : \bar{A} \vdash_{\bar{T}} A^* x y \Rightarrow B^* \bar{t} \bar{t}'[x/y] & (\Rightarrow I), (550) & (551) \\
\bar{\Gamma} \vdash_{\bar{T}} \forall x : \bar{A}. \forall y : \bar{A}. A^* x y & & \\
\quad \Rightarrow B^* \bar{t} \bar{t}'[x/y] & (\forall I), (\forall I), (551) & (552) \\
\bar{\Gamma}, x : \bar{A}, x^* : A^* x x \vdash_{\bar{T}} \bar{t} : \bar{B} & \text{induction hypothesis, (530)} & (553) \\
\bar{\Gamma}, x : \bar{A}, x^* : A^* x x \vdash_{\bar{T}} \bar{t}' : \bar{B} & \text{induction hypothesis, (530)} & (554)
\end{array}$$

Since in HOL typing is independent of context assumptions:

$$\begin{array}{lll}
\bar{\Gamma}, x : \bar{A} \vdash_{\bar{T}} \bar{t} : \bar{B} & \text{explanation, (553)} & (555) \\
\bar{\Gamma}, x : \bar{A} \vdash_{\bar{T}} \bar{t}' : \bar{B} & \text{explanation, (554)} & (556) \\
\bar{\Gamma} \vdash_{\bar{T}} \lambda x : \bar{A}. \bar{t} : \bar{A} \rightarrow \bar{B} & (\text{lambda}), (555) & (557) \\
\bar{\Gamma} \vdash_{\bar{T}} \lambda x : \bar{A}. \bar{t}' : \bar{A} \rightarrow \bar{B} & (\text{lambda}), (556) & (558) \\
\bar{\Gamma} \vdash_{\bar{T}} \overline{\lambda x : A. t =_{\Pi x.A. B} \lambda x : A'. t'} & (\text{PT21}), (552) & \\
\bar{\Gamma} \vdash_{\bar{T}} \overline{\lambda x : A. t : \Pi x : A. B} & (\text{PT10}), (\text{PT18}), (557) & \\
\bar{\Gamma} \vdash_{\bar{T}} \overline{\lambda x : A. t' : \Pi x : A. B} & (\text{PT10}), (\text{PT18}), (558) &
\end{array}$$

(*etaPi*)

$$\Gamma \vdash_T t : \Pi x : A. B \quad \text{by assumption} \quad (559)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{t} : \bar{A} \rightarrow \bar{B} \quad \text{PT10, induction hypothesis, (559)} \quad (560)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{t} =_{\bar{A} \rightarrow \bar{B}} \lambda x : \bar{A}. \bar{t} x \quad (\text{eta}), (560) \quad (561)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{t} =_{\Pi x : A. B} \overline{\lambda x : A. t x} \quad \text{PT18, PT10, (561)}$$

$$\bar{\Gamma} \vdash_{\bar{T}} (\Pi x : A. B)^* \bar{t} \bar{t} \quad \text{induction hypothesis, (560)}$$

(*refl*)

$$\Gamma \vdash_T t : A \quad \text{by assumption} \quad (562)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{t} : \bar{A} \quad \text{induction hypothesis, (562)} \quad (563)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{t} =_{\bar{A}} \bar{t} \quad (\text{refl}), (563)$$

$$\bar{\Gamma} \vdash_{\bar{T}} A^* \bar{t} \bar{t} \quad \text{induction hypothesis, (562)}$$

(*sym*)

$$\Gamma \vdash_T s =_A t \quad \text{by assumption} \quad (564)$$

$$\bar{\Gamma} \vdash_{\bar{T}} A^* \bar{s} \bar{t} \quad \text{induction hypothesis, (564)} \quad (565)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{t} : \bar{A} \quad \text{induction hypothesis, (564)} \quad (566)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{s} : \bar{A} \quad \text{induction hypothesis, (564)} \quad (567)$$

$$\bar{\Gamma} \vdash_{\bar{T}} A^* \bar{t} \bar{s} \quad (\forall E), (\forall E), (\Rightarrow E), (281), (565), (566), (567)$$

(*beta*)

$$\Gamma \vdash_T (\lambda x : A. s) t : B \quad \text{by assumption} \quad (568)$$

$$\bar{\Gamma} \vdash_{\bar{T}} (\lambda x : \bar{A}. \bar{s}) \bar{t} : \bar{B} \quad \text{induction hypothesis, PT18, (568)} \quad (569)$$

$$\bar{\Gamma} \vdash_{\bar{T}} (\lambda x : \bar{A}. \bar{s}) \bar{t} =_{\bar{B}} \bar{s}[\bar{x}/\bar{t}] \quad (\text{beta}), (569) \quad (570)$$

$$\bar{\Gamma} \vdash_{\bar{T}} (\lambda x : \bar{A}. \bar{s}) \bar{t} =_{\bar{B}} \overline{s[x/t]} \quad (283), (570) \quad (571)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \overline{(\lambda x : A. s) t} =_{\bar{B}} \overline{s[x/t]} \quad \text{PT18, PT19, (571)}$$

$$\bar{\Gamma} \vdash_{\bar{T}} (\Pi x : A. B)^* ((\lambda x : A. s) t) ((\lambda x : A. s) t) \quad \text{induction hypothesis, (568)}$$

*Validity* Validity can be shown using the rules ( $|_p E$ ), (*axiom*), (*assume*), (*congl-*), ( $\Rightarrow I$ ) and ( $\Rightarrow E$ ).

( *$|_p E$* )

$$\Gamma \vdash_T t : A|_p \quad \text{by assumption} \quad (572)$$

$$\bar{\Gamma} \vdash_{\bar{T}} (A|_p)^* \bar{t} \bar{t} \quad \text{induction hypothesis, (572)} \quad (573)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \bar{p} \bar{t} \quad (\wedge E), (\wedge E), \text{PT15, (573)} \quad (574)$$

$$\bar{\Gamma} \vdash_{\bar{T}} \overline{p} \bar{t} \quad \text{PT19, (574)}$$

(*axiom*)

$ax : F \text{ in } T$	by assumption	(575)
$\vdash_T \Gamma \text{ Ctx}$	by assumption	(576)
$ax : \overline{F} \text{ in } \overline{T}$	PT4,(575)	(577)
$\vdash_{\overline{T}} \overline{\Gamma} \text{ Ctx}$	induction hypothesis,(576)	(578)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F}$	(axiom),(577),(578)	

(*assume*)

$ass : F \text{ in } \Gamma$	by assumption	(579)
$\vdash_T \Gamma \text{ Ctx}$	by assumption	(580)
$ass : \overline{F} \text{ in } \overline{\Gamma}$	PT7,(579)	(581)
$\vdash_{\overline{T}} \overline{\Gamma} \text{ Ctx}$	induction hypothesis,(580)	(582)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F}$	(assume),(581),(582)	

(*congl<sub>⊢</sub>*)

$\Gamma \vdash_T F =_{\text{bool}} F'$	by assumption	(583)
$\Gamma \vdash_T F'$	by assumption	(584)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F} =_{\text{bool}} \overline{F}'$	(PT13),induction hypothesis,(583)	(585)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F}'$	induction hypothesis,(584)	(586)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F}$	(congl <sub>⊢</sub> ),(585),(586)	

(*⇒I*)

$\Gamma \vdash_T F : \text{bool}$	by assumption	(587)
$\Gamma, ass : F \vdash_T G$	by assumption	(588)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F} : \text{bool}$	induction hypothesis,(587)	(589)
$\overline{\Gamma}, \overline{F} \vdash_{\overline{T}} \overline{G}$	induction hypothesis,PT7,(588)	(590)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F} \Rightarrow \overline{G}$	(⇒I),(589),(590)	(591)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F \Rightarrow G}$	PT20,(591)	

(*⇒E*)

$\Gamma \vdash_T F \Rightarrow G$	by assumption	(592)
$\Gamma \vdash_T F$	by assumption	(593)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F} \Rightarrow \overline{G}$	induction hypothesis,PT20,(592)	(594)

$$\begin{array}{ll}
\bar{\Gamma} \vdash_{\bar{T}} \bar{F} & \text{induction hypothesis, (593)} \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{G} & (\Rightarrow E), (594), (595)
\end{array} \tag{595}$$

(boolExt)

$$\begin{array}{ll}
\Gamma \vdash_T p \text{ true} & \text{by assumption} \\
\Gamma \vdash_T p \text{ false} & \text{by assumption} \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{p} \text{ true} & \text{induction hypothesis, PT19, (596)} \\
\bar{\Gamma} \vdash_{\bar{T}} \bar{p} \text{ false} & \text{induction hypothesis, PT19, (597)} \\
\bar{\Gamma} \vdash_{\bar{T}} \forall z : \text{bool}. \bar{p} z & (\text{boolExt}), (598), (599) \\
\bar{\Gamma}, x : \text{bool} \vdash_{\bar{T}} \forall z : \text{bool}. \bar{p} z & (\text{var}^+), (600) \\
\bar{\Gamma}, x : \text{bool} \vdash_{\bar{T}} \bar{p} x & (\forall E), (601), (\text{assume}) \\
\bar{\Gamma}, x, y : \text{bool}, x =_{\text{bool}} y \vdash_T \bar{p} x & (\text{monotonic}^+), (\text{var}^+), (602) \\
\bar{\Gamma}, x, y : \text{bool}, x =_{\text{bool}} y \vdash_T \bar{p} y & (\text{rewrite}), (603), (\text{assume}) \\
\bar{\Gamma}, x, y : \text{bool} \vdash_T \text{bool}^* x y \Rightarrow \bar{p} y & (\text{PT13}), (\Rightarrow I), (604) \\
\bar{\Gamma} \vdash_{\bar{T}} \forall x : \text{bool}. \forall y : \text{bool}. & \\
\quad \text{bool}^* x y \Rightarrow \bar{p} y & (\forall I), (\forall I), (605) \\
\bar{\Gamma} \vdash_{\bar{T}} \overline{\forall x : \text{bool}. p x} & (\text{PT21}), (\text{PT11}), (606)
\end{array}$$

## C Soundness proof

The idea of the soundness proof is to transform HOL-proofs into DHOL-proofs. The proof is very involved, and we proceed in multiple steps.

### C.1 Type-wise injectivity of the translation

**Definition 4.** Let  $t$  be an ill-typed DHOL term with well-typed image  $\bar{t}$  in HOL. In this case we will say that  $\bar{t}$  is a spurious term. A term  $\bar{s}$  in HOL that is the image of a well-typed term  $s$ , will be called proper. A term  $tm$  in HOL that is not the image of any (well-typed or not) term is said to be improper.

**Lemma 3.** Let  $\Delta$  be a DHOL context and let  $\Gamma$  denote its translation. Given two DHOL terms  $s, t$  of type  $A$  and assuming  $s$  and  $t$  are not identical, it follows that  $\bar{s}$  and  $\bar{t}$  are not identical.

*Proof (Proof of Lemma 3).* We prove this by induction on the shape of the types both equalities are over—in case both terms are equalities—and by subinduction on the shape of the two translated terms otherwise. We observe that terms created using a different top-level production are non-identical and will remain that way in the image. So

we can go over the productions one by one and assuming type-wise injectivity for sub-terms show injectivity of applying them. Different constants are mapped to different constants and different variables to different variables, so in those cases there is nothing to prove. If two function applications or implications differ in DHOL then one of the two pairs of corresponding arguments must differ as well. By induction hypothesis so will the images of the terms in that pair. Since function application and implication both commute with the translation, it follows that the images of the function applications or implications also differ. Since the translations of the terms on both sides of an equality also show up in the translation, the same argument also works for two equalities over the same type. Similarly for lambda functions of same type.

Consider now two equalities over different types that get identified by dependency-erasure.

In case of equalities over different base types, the typing relations that are applied in the images are different, so the images of the equalities differ. For equalities over different  $\Pi$ -types either the domain type or the codomain type must differ by rule (congII). If the domain types differ then the typing assumption after the two universal quantifiers of the translated equalities will differ. If the codomain types are different then the applications of the typing relations on the right of the  $\Rightarrow$  of the translated equalities are the translations of the equalities yielded by applying the functions on both sides of the equalities to a freshly bound variable of the domain type. The translations of the equalities are only identical if those "inner equalities" are identical. Furthermore, the inner equalities are over types that are the codomain of the type the equalities are over. The claim then follows from the induction hypothesis.

Finally it remains to consider the case of equalities  $s =_{A|_p} t$  and  $s' =_{A'|_{p'}} t'$  over non-identical predicate subtypes  $A|_p$  and  $A'|_{p'}$  where not both  $A = A'$  and  $p = p'$ . If  $p \neq p'$ , then the translations have different subterms  $\bar{p} s$  and  $\bar{p'} s'$  and thus differ. If  $A \neq A'$ , then the first conjuncts in the translated equalities are the translations of equalities over the types  $A$  and  $A'$  respectively, which by the induction hypothesis have different translations. So in any case, the equalities have different images.

## C.2 Quasi-preimages for terms and validity statements in admissible HOL derivations

Firstly, we will consider the preimage of a typing relations  $A^*$  to be the equality symbol  $\lambda x : A. \lambda y : A. x =_A y$  (if equality is treated as a (parametric) binary predicate rather than a production of the grammar this eta reduces to the symbol  $=_A$ ).

Using this convention, we define the normalization of an improper HOL term, which is either a proper term or a spurious term. The normalization of an improper HOL term is defined by:

**Definition 5.** *Let  $t$  be an improper HOL term. Then we define the normalization norm  $[t]$  of  $t$  by induction on the shape of  $t$ :*



$$\begin{aligned}
\text{norm } [\bar{t}] &:= t & (\text{PT22}) \\
\text{norm } [\text{norm } [s]] &:= \text{norm } [s] & (\text{PT23}) \\
\text{norm } [A^* s] &:= \lambda y : \bar{A}. A^* s y & (\text{PT24}) \\
\text{norm } [A^*] &:= \lambda x : \bar{A}. \lambda y : \bar{A}. A^* x y & (\text{PT25}) \\
\text{norm } [c] &:= c & (\text{PT26}) \\
\text{norm } [x] &:= x & (\text{PT27}) \\
\text{norm } [f t] &:= \text{norm } [f] \text{ norm } [t] & (\text{PT28}) \\
\text{norm } [\lambda x : C. t] &:= \lambda x : C. \text{norm } [t] & (\text{PT29})
\end{aligned}$$

If  $F$  not of shape  $A^* \_ \Rightarrow \_$  or  $\forall x' : \bar{A}. A^* x x' \Rightarrow \_$ :

$$\begin{aligned}
\text{norm } [\forall x : \bar{A}. F] &:= \text{norm } [\forall x : \bar{A}. A^* x x F] & (\text{PT30}) \\
\text{norm } [\forall x : \bar{A}. A^* x x \Rightarrow G] &:= \forall x, x' : \bar{A}. A^* x x' \Rightarrow G & (\text{PT31}) \\
\text{norm } [s =_{\bar{A}} t] &:= A^* s t & (\text{PT32}) \\
\text{norm } [s \Rightarrow t] &:= \text{norm } [s] \Rightarrow \text{norm } [t] & (\text{PT33})
\end{aligned}$$

For proper and spurious terms  $t$ , we define the normalization of  $t$  be  $t$  itself.

**Definition 6.** Assume a well-formed DHOL theory  $T$ .

We say that an HOL context  $\Delta$  is proper (relative to  $\bar{T}$ ), iff there exists a well-formed HOL context  $\Theta$  (relative to  $\bar{T}$ ), s.t. there is a well-formed DHOL context  $\Gamma$  (relative to  $T$ ) with  $\bar{\Gamma} = \Theta$  and  $\Theta$  can be obtained from  $\Delta$  by adding well-typed typing assumptions. In this case,  $\Gamma$  is called a quasi-preimage of  $\Delta$ . Inspecting the translation, it becomes clear that  $\Gamma$  is uniquely determined by the choices of the preimages of the types of variables without a typing assumption in  $\Delta$ .

Given a proper HOL context  $\Delta$  and a well-typed HOL formula  $\varphi$  over  $\Delta$ , we say that  $\varphi$  is quasi-proper iff  $\text{norm } [\varphi] = \bar{F}$  for  $\Gamma \vdash_T F : \text{bool}$  and  $\Gamma$  is a quasi-preimage of  $\Delta$ . In that case, we call  $F$  a quasi-preimage of  $\varphi$ .

Finally, we call a validity judgement  $\Delta \vdash_{\bar{T}} \varphi$  in HOL proper iff

1.  $\Delta$  is proper,
2.  $\varphi$  is quasi-proper in context  $\Delta$

In this case, we will call  $\bar{\Gamma} \vdash_{\bar{T}} \bar{F}$  a relativization of  $\Delta \vdash_{\bar{T}} \varphi$  and  $\Gamma \vdash_T F$  a quasi-preimage of the statement  $\Delta \vdash_{\bar{T}} \varphi$ , where  $\Gamma$  is a quasi-preimage of  $\Delta$  and  $F$  a quasi-preimage of  $\varphi$ .

### C.3 Transforming HOL derivations into admissible HOL derivations

It will be useful to distinguish between two different kinds of improper terms.

**Definition 7.** *An improper term is called almost proper iff its normalization isn't spurious and contains no spurious subterms, otherwise it is said to be unnormalizably spurious. This means that improper terms are almost proper iff they have a well-typed quasi-preimage (i.e. if they are quasi-proper). We consider proper terms to be almost proper as well.*

**Definition 8.** *A valid HOL derivation is called admissible iff all terms occurring in it are almost proper.*

In the following we describe a proof transformation which maps HOL derivations to admissible HOL derivations.

**Definition 9.** *A statement transformation in a given logic is a map that maps statements in the logic to statements in the logic.*

**Definition 10.** *A macro-step  $M$  for a statement transformation  $T$  replacing a step  $S$  in a derivation is a sequence of steps  $S_1, \dots, S_n$  (called micro-steps of  $M$ ) s.t. the assumptions of the  $S_i$  that are not concluded by  $S_j$  with  $j < i$  are results of applying  $T$  to assumptions of step  $S$  and furthermore the conclusion of step  $S_n$  is the result of applying  $T$  to the conclusion of  $S$ . The assumptions of those  $S_j$  that are not concluded by previous micro-steps of  $M$  are called the assumptions of macro-step  $M$  and the conclusion of the last micro-step  $S_n$  of  $M$  is called the conclusion of macro-step  $M$ .*

**Definition 11.** *A normalizing statement transformation  $\text{sRed}(\cdot)$  is defined to be a transformation that replaces terms in statements (including their contexts) as described below. The definition of the transformation of a term additionally depends on a DHOL-type  $A$  (called the preimage type) for each term  $t$ . We will write those types as indices to the HOL terms, so for instance  $t_A$  would indicate an HOL term  $t$  of type  $\bar{A}$  and preimage type  $A$ .*

*These indices are used to effectively associate to each term a type of a possible quasi-preimage, which is useful as for  $\lambda$ -functions there are quasi-preimages of potentially many different types. We require that for an indexed term  $t_A$ , term  $t$  has type  $\bar{A}$  and that for almost proper terms  $t_A$  with unique quasi-preimage the quasi-preimage has type  $A$ .*

*Intuitively the transformation will do two things (in this order) in order to "normalize" unnormalizably spurious terms to almost proper ones:*

1. *apply beta and eta reductions and in case this doesn't yield almost proper terms*
2. *replace unnormalizably spurious function applications of type  $B$  by the "default terms"  $w_B$  of type  $B$  which is proper and whose existence is assumed for all HOL types.*

Additionally we will choose the index types to ensure we yield almost proper terms of same index on both sides of equalities.

As we are assuming a valid derivation, we will only define this transformation on well-typed HOL terms. We can then define the transformation of  $t_A$  (denoted by  $\text{sRed}(t_A)$ ) by induction on the shape of  $t_A$  as follows:

$$\text{sRed}(t_A) \quad := t_A \quad \text{if } t \text{ has quasi-preimage of type } A \quad (\text{SR1})$$

$$\text{sRed}(f_{\Pi x:A. B} t_A) := \text{sRed}(f_{\Pi x:A. B}) \text{sRed}(t_A) \quad \text{if } f_{\Pi x:A. B} t_A \text{ not beta or eta reducible} \quad (\text{SR2})$$

In the following cases, we assume that the term  $t_A$  in  $\text{sRed}(\cdot)$  on the left of  $:=$  isn't almost proper with a quasi-preimage of type  $A$ :

$$\text{sRed}(t_A) \quad := \text{sRed}(t_A^{\beta\eta}) \quad \text{if } t \text{ is beta or eta reducible} \quad (\text{SR3})$$

$$\text{sRed}(s_A =_A t_{A'}) \quad := \text{sRed}(s_A) =_A \text{sRed}(t_{A'}) \quad (\text{SR4})$$

$$\text{sRed}(F_{\text{bool}} \Rightarrow G_{\text{bool}}) \quad := \text{sRed}(F_{\text{bool}}) \Rightarrow \text{sRed}(G_{\text{bool}}) \quad (\text{SR5})$$

$$\text{sRed}(\lambda x : A. s_B) \quad := \lambda x : A. \text{sRed}(s_B) \quad (\text{SR6})$$

$$\text{sRed}\left(\left(\text{sRed}(f_{\Pi x:A. B})_{\Pi x:A. B} \text{sRed}(t_{A'})_{A'}\right)_{B'}\right) \quad := w_{\overline{B}} \quad \text{if } A \neq A' \text{ or } B \neq B' \quad (\text{SR7})$$

**Lemma 4.** Assume a well-typed DHOL theory  $T$  and a conjecture  $\Gamma \vdash_T \varphi$  with  $\Gamma$  well-formed and  $\varphi$  well-typed. Assume a valid HOL derivation of  $\overline{\Gamma} \vdash_{\overline{T}} \overline{\varphi}$ . Then, we can index the terms in the derivation s.t. any steps  $S$  in the derivation can be replaced by a macro-step for the normalizing statement transformation replacing step  $S$  s.t. after replacing all steps by their macro-steps:

- the resulting derivation is valid,
- all terms occuring in the derivation are almost proper.

*Proof (Proof of Lemma 4).* We will show this by induction on the inference rules.

Firstly, we observe that there are no dependent types in HOL and the context and axioms contain no spurious subterms. Hence, well-formedness (of theories, contexts, types) and type-equality judgements are unaffected by the transformation. So there is nothing to prove for the well-formedness and type-equality rules.

*Regarding the indices for the terms:* We start indexing the term at the end of the derivation and go up line by line. Whenever we need to pick an index for a term we already encountered (in a later step) in the derivation we will pick the same index. Whenever we need to pick an index for a constant or variable that is the translation of a variable in the context of the DHOL conjecture, we pick as the index the type of the (unique) preimage of the constant or variable. Whenever we need to pick indices for terms on both sides of an equality, we pick the same index. Whenever we need to pick an index for a non-atomic term we pick indices for the atomic subterms in the term and then choose a type

of the quasi-preimage (given the type by termwise-injectivity (see Lemma 3) the quasi-preimage is unique) for which the quasi-preimages of the subterm have the types they are indexed with. If we can choose indices in a way such that there exists a well-typed quasi-preimage of that type, we do. In particular, this means for an equality between  $\lambda$ -functions that we will pick the same types for both  $\lambda$ -functions if possible. We choose the indices for the normalizing statement transformation of a term indexed by  $A$  to also be  $A$ , unless we have already picked a different index. If we have to pick an index for a variable that is part of a  $\lambda$ -function, we pick the index consistently with the domain of the index of the entire  $\lambda$ -function if an index is already chosen for it. In that case, we also pick the codomain of the index of the entire  $\lambda$ -function as the index of the body of the  $\lambda$ -function. If no index is chosen for the  $\lambda$ -function, but it is applied to an argument, we pick the index of that argument for the variable bound by the  $\lambda$  (this choice ensures that our transformation changes as little as necessary and is also consistent with the indexing of variables in proper terms). Otherwise, we pick the index arbitrarily (but satisfying the already stated requirements).

It remains to consider the typing and validity rules and to construct macro steps for the steps in the derivation using them for the normalizing statement transformation.

Since terms indexed by a type  $A$  have type  $\bar{A}$  it is easy to see from Definition 11 that the normalizing statement transformation replaces terms of type  $\bar{A}$  by terms of type  $\bar{A}$ .

(*const*): Since constants are proper terms, there is nothing to prove.

(*var*): Since context variables are proper terms, there is nothing to prove.

(*=type*):

$$\Delta \vdash_{\bar{T}} \text{sRed}(s)_A : \bar{A} \quad \text{by assumption} \quad (607)$$

$$\Delta \vdash_{\bar{T}} \text{sRed}(t)_A : \bar{A} \quad \text{by assumption} \quad (608)$$

$$\Delta \vdash_{\bar{T}} \text{sRed}(s)_A =_{\bar{A}} \text{sRed}(t)_A : \text{bool} \quad (=type), (607), (608) \quad (609)$$

$$\Delta \vdash_{\bar{T}} \text{sRed}(s_A =_{\bar{A}} t_A)_{\text{bool}} : \text{bool} \quad \text{SR4}, (609)$$

(*lambda*):

$$\Delta, x_A : \bar{A} \vdash_{\bar{T}} \text{sRed}(t_B)_B : \bar{B} \quad \text{by assumption} \quad (610)$$

$$\Delta \vdash_{\bar{T}} (\lambda x_A : \bar{A}. \text{sRed}(t_B)_B) : \bar{A} \rightarrow \bar{B} \quad (\text{lambda}), (610) \quad (611)$$

If  $\text{sRed}(t)_B$  isn't an unnormalizably spurious function application  $\text{sRed}(f_{\Pi y:A'. B}) x_A$  for which  $x$  doesn't appear in  $f$ :

$$\Delta \vdash_{\bar{T}} \text{sRed}(\lambda x_A : \bar{A}. \text{sRed}(t_B)_B) : \bar{A} \rightarrow \bar{B} \quad \text{SR6}, (611)$$

Else by (SR3) we have  $\text{sRed}(\lambda x_A : \bar{A}. \text{sRed}(t_B)_B) = \text{sRed}(f_{\Pi y:A. B})$ . By the remark about the type of  $\text{sRed}(\cdot)$  it follows that  $\text{sRed}(f_{\Pi y:A. B})$  has type  $\bar{\Pi}y : A. \bar{B} = \bar{A} \rightarrow \bar{B}$ .

$$\Delta \vdash_{\bar{T}} \text{sRed}(f_{\Pi y:A'. B}) : \bar{A} \rightarrow \bar{B} \quad \text{see above}$$

(*appl*):

$$\Delta \vdash_{\bar{T}} \text{sRed}(f_{\Pi x:A. B}) : \bar{A} \rightarrow \bar{B} \quad \text{by assumption} \quad (612)$$

$$\Delta \vdash_{\bar{T}} \text{sRed}(t_{A'}) : \bar{A} \quad \text{by assumption} \quad (613)$$

Unless  $\text{sRed}(f_{\Pi x:A. B}) \text{sRed}(t'_A)$  beta reducible or not satisfying  $A \equiv A'$ :

$$\Delta \vdash_{\bar{T}} \text{sRed}(f_{\Pi x:A. B} t_{A'}) : \bar{B} \quad \text{SR1, (lambda), (612), (613)}$$

If  $\text{sRed}(f_{\Pi x:A. B}) \text{sRed}(t'_A)$  not beta reducible but also not satisfying  $A \equiv A'$ , then by (SR2) and (SR7) we have

$$\text{sRed}(f_{\Pi x:A. B} t'_A) = \text{sRed}(\text{sRed}(f_{\Pi x:A. B})_{\Pi x:A. B} \text{sRed}(\text{sRed}(t'_A)'_A)) = w_{\bar{B}}.$$

By the axiom schema asserting the existence of  $w_{\bar{B}}$  we have  $w_{\bar{B}} : \bar{B}$ :

$$\Delta \vdash_{\bar{T}} w_{\bar{B}} : \bar{B} \quad \text{assumption}$$

Otherwise if  $\text{sRed}(f_{\Pi x:A. B}) \text{sRed}(t'_A)$  beta reducible with  $f_{\Pi x:A. B} = \lambda x_A : \bar{A}. \text{sRed}(s)_B$  and not satisfying  $A \equiv A'$ , it follows that

$$\text{sRed}(f_{\Pi x:A. B} t_{A'}) = \text{sRed}(\text{sRed}(s_B) [x_A / \text{sRed}(t_{A'})]) = \text{sRed}(s_B) [x_A / \text{sRed}(t_{A'})].$$

Observe that  $\Delta, x : \bar{A} \vdash_{\bar{T}} \text{sRed}(s) : \bar{B}$  must be derivable (otherwise  $f$  not well-typed) and thus:

$$\Delta \vdash_{\bar{T}} \text{sRed}(s)_B [x_A / \text{sRed}(t_{A'})] : \bar{B} \quad (\text{rewriteTyping}), \text{assumption}, (613)$$

Observe that by induction hypothesis the derivations of  $\Delta \vdash_{\bar{T}} \text{sRed}(f_{\Pi x:A. B}) : \bar{A} \rightarrow \bar{B}$  (and thus of  $\Delta \vdash_{\bar{T}} \text{sRed}(s)_B : \bar{B}$ ) and of  $\Delta \vdash_{\bar{T}} \text{sRed}(t)_A : \bar{A}$  are almost proper with quasi-preimages for terms of indexed types. Consequently, the steps in the derivation obtained by plugging in the proof of rule (*rewriteTyping*) into this case will also be almost proper with quasi-preimages of indexed types (as the terms in it for corresponding steps have the same types and indices as in the derivation for  $\Delta \vdash_{\bar{T}} \text{sRed}(s)_B : \bar{B}$  and steps in the derivation of  $\Delta \vdash_{\bar{T}} \text{sRed}(t)_A : \bar{A}$  which occur in this derivation are unchanged). Therefore treating rule (*rewriteTyping*) like a primitive rule is harmless here (we can replace a step using the rule by the steps in the derivation of the rule) and we are done.

( $\Rightarrow$ type):

$$\Delta \vdash_{\overline{T}} \text{sRed}(F)_{\text{bool}} : \text{bool} \quad \text{by assumption} \quad (614)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(G)_{\text{bool}} : \text{bool} \quad \text{by assumption} \quad (615)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(F)_{\text{bool}} \Rightarrow \text{sRed}(G)_{\text{bool}} : \text{bool} \quad (\Rightarrow\text{type}), (614), (615) \quad (616)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(F_{\text{bool}} \Rightarrow F_{\text{bool}}) : \text{bool} \quad \text{SR5}, (616)$$

(*axiom*): Since translations of axioms to HOL are always proper terms and the additionally generated axioms are almost proper, there is nothing to prove here.

(*assume*): If the axiom is a typing axiom generated by the translation, it follows that it is almost proper. Similarly, if it is an axiom for a base type it will Otherwise:

$$\text{ass} : \text{sRed}(F_{\text{bool}}) \text{ in } \Delta \quad \text{by assumption} \quad (617)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(F_{\text{bool}}) \quad (\text{assume}), (617)$$

By assumption  $\text{sRed}(F)$  almost proper (with a quasi-preimage of type bool), so the conclusion of the rule is almost proper and there is nothing to prove here.

(*cong* $\lambda$ ):

$$\Delta \vdash_{\overline{T}} A \equiv A' \quad \text{by assumption} \quad (618)$$

$$\Delta, x_A : \overline{A} \vdash_{\overline{T}} \text{sRed}(t_B =_{\overline{B}} t'_B)_{\text{bool}} \quad \text{by assumption} \quad (619)$$

$$\Delta, x_A : \overline{A} \vdash_{\overline{T}} \text{sRed}(t)_B =_{\overline{B}} \text{sRed}(t')_B \quad \text{SR4}, (619) \quad (620)$$

$$\begin{aligned} \Delta \vdash_{\overline{T}} \lambda x_A : \overline{A}. \text{sRed}(t)_B &=_{\overline{A} \rightarrow \overline{B}} \\ \lambda x_A : \overline{A}. \text{sRed}(t')_B &\quad (\text{cong}\lambda), (618), (620) \end{aligned} \quad (621)$$

By assumption  $\text{sRed}(t)_B =_{\overline{B}} \text{sRed}(t')_B$  almost proper with quasi-preimage consistent with type indices and  $A \equiv A'$ , thus also  $\lambda x_A : \overline{A}. \text{sRed}(t)_B =_{\overline{A} \rightarrow \overline{B}} \lambda x_A : \overline{A}. \text{sRed}(t')_B$  almost proper with quasi-preimage consistent with type indices.

$$\Delta \vdash_{\overline{T}} \text{sRed}(\lambda x_A : \overline{A}. \text{sRed}(t)_B =_{\overline{A} \rightarrow \overline{B}} \lambda x_A : \overline{A}. \text{sRed}(t')_B) \quad \text{SR6}, \text{SR4}, (621)$$

(*congApp*):

$$\Delta \vdash_{\overline{T}} \text{sRed}(t_A =_{\overline{A}} t'_A) \quad \text{by assumption} \quad (622)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(t)_A =_{\overline{A}} \text{sRed}(t')_A \quad \text{SR4}, (622) \quad (623)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(f_{\Pi x:A'. B} =_{\overline{A} \rightarrow \overline{B}} f'_{\Pi x:A'. B}) \quad \text{by assumption} \quad (624)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(f)_{\Pi x:A'. B} =_{\overline{A} \rightarrow \overline{B}} \text{sRed}(f')_{\Pi x:A'. B} \quad \text{SR4}, (624) \quad (625)$$

Assume that  $A \not\equiv A'$ . Our choice of type indices then implies  $\text{sRed}(f)$  and  $\text{sRed}(f')$  are not  $\lambda$ -functions. Consequently, the applications  $\text{sRed}(f) \text{sRed}(s)$  and  $\text{sRed}(f') \text{sRed}(s')$  are not beta or eta reducible. Thus,  $\text{sRed}(\text{sRed}(f)_{\Pi x:A. B} \text{sRed}(t)_{A'}) = w_{\overline{B}}$  and  $\text{sRed}(\text{sRed}(f')_{\Pi x:A. B} \text{sRed}(t')_{A'}) = w_{\overline{B}}$  and we yield:

$$\Delta \vdash_{\overline{T}} \text{sRed}(\text{sRed}(f)_{\Pi x:A'. B} \text{sRed}(t)_A) =_{\overline{B}} \text{sRed}(\text{sRed}(f')_{\Pi x:A'. B} \text{sRed}(t')_A) \quad (\text{refl})$$

Otherwise the applications  $\text{sRed}(f)_{\Pi x:A. B} \text{sRed}(t)_{A'}$  and  $\text{sRed}(f')_{\Pi x:A. B} \text{sRed}(t')_{A'}$  are almost proper with quasi-preimages consistent with type indices. It follows:

$$\text{sRed}(\text{sRed}(f)_{\Pi x:A. B} \text{sRed}(t)_{A'}) = \text{sRed}(f)_{\Pi x:A. B} \text{sRed}(t)_{A'}$$

and

$$\text{sRed}(\text{sRed}(f')_{\Pi x:A. B} \text{sRed}(t')_{A'}) = \text{sRed}(f')_{\Pi x:A. B} \text{sRed}(t')_{A'}$$

and thus:

$$\begin{aligned} \Delta \vdash_{\overline{T}} \text{sRed}(\text{sRed}(f)_{\Pi x:A. B} \text{sRed}(t)_{A'}) &=_{\overline{B}} \\ \text{sRed}(\text{sRed}(f')_{\Pi x:A. B} \text{sRed}(t')_{A'}) &\quad (\text{congAppl}), (623), (625) \quad (626) \\ \Delta \vdash_{\overline{T}} \text{sRed}(\text{sRed}(f)_{\Pi x:A. B} \text{sRed}(t)_{A'}) &=_{\overline{B}} \text{sRed}(f')_{\Pi x:A. B} \text{sRed}(t')_{A'} \quad \text{SR4}, (626) \end{aligned}$$

(*refl*):

$$\Delta \vdash_{\overline{T}} \text{sRed}(t)_A : \overline{A} \quad \text{by assumption} \quad (627)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(t)_A =_{\overline{A}} \text{sRed}(t)_A \quad (\text{refl}), (627) \quad (628)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(\text{sRed}(t)_A =_{\overline{A}} \text{sRed}(t)_A) \quad \text{SR4}, (628)$$

(*sym*):

$$\Delta \vdash_{\overline{T}} \text{sRed}(t_A =_{\overline{A}} s_A) \quad \text{by assumption} \quad (629)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(t_A)_A =_{\overline{A}} \text{sRed}(s_A)_A \quad \text{SR4}, (629) \quad (630)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(s_A)_A =_{\overline{A}} \text{sRed}(t_A)_A \quad (\text{sym}), (630) \quad (631)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(s_A =_{\overline{A}} t_A) \quad \text{SR4}, (631)$$

(*beta*):

$$\Delta \vdash_{\overline{T}} \text{sRed}\left(\left(\lambda x_A : \overline{A}. s_B\right) t'_A\right)_{B'} : \overline{B} \quad \text{by assumption} \quad (632)$$

By (SR6) and choice of type indices, it follows that  $\text{sRed}\left(\left(\lambda x_A : \overline{A}. s_B\right)\right) = \lambda x_A : \overline{A}. \text{sRed}(s_B)_B$ . If  $\left(\lambda x_A : \overline{A}. \text{sRed}(s_B)_B\right) t_{A'}$  is almost proper with quasi-preimage of type  $B \equiv B'$ , then we yield:

$$\Delta \vdash_{\overline{T}} \left(\lambda x_A : \overline{A}. \text{sRed}(s_B)\right) \text{sRed}(t_A) : \overline{B} \quad \text{SR2}, (632) \quad (633)$$

$$\begin{aligned}
& \Delta \vdash_{\overline{T}} \left( \lambda x_A : \overline{A}. \text{sRed}(s_B) \right) \text{sRed}(t_A) =_{\overline{B}} \\
& \quad \text{sRed}(s_B) [x_A / \text{sRed}(t_A)] \quad (\text{beta}), (633) \quad (634) \\
& \Delta \vdash_{\overline{T}} \text{sRed} \left( \left( \lambda x_A : \overline{A}. \text{sRed}(s_B) \right) \text{sRed}(t_A) =_{\overline{B}} \text{sRed}(s_B) [x_A / \text{sRed}(t_A)] \right) \quad \text{SR4, SR1}, (634)
\end{aligned}$$

Otherwise,

$$\text{sRed} \left( \left( \lambda x_A : \overline{A}. s_B \right) t'_A \right) = \text{sRed} \left( \text{sRed}(s_B) [x_A / \text{sRed}(t'_A)] \right) = \text{sRed}(s_B) [x_A / \text{sRed}(t'_A)]$$

and we yield:

$$\Delta \vdash_{\overline{T}} \text{sRed}(s_B) [x_A / \text{sRed}(t_A)] =_{\overline{B}} \text{sRed}(s_B) [x_A / \text{sRed}(t_A)] \quad (\text{refl}) \quad (635)$$

By induction hypothesis, we yield that  $\text{sRed}(s_B) [x_A / \text{sRed}(t_A)]$  is has a quasi-preimage of type  $B'$ . By choice of indeces it then follows that  $B \equiv B'$ . Therefore, we can conclude:

$$\Delta \vdash_{\overline{T}} \text{sRed} \left( \left( \lambda x_A : \overline{A}. \text{sRed}(s_B) \right) \text{sRed}(t_A) =_{\overline{B}} \text{sRed}(s_B) [x_A / \text{sRed}(t_A)] \right) \quad \text{SR4}, (635)$$

(*eta*):

$$\Delta \vdash_{\overline{T}} \text{sRed}(t_{\Pi x:A. B}) : \overline{A} \rightarrow \overline{B} \quad \text{by assumption} \quad (636)$$

$$x \text{ not in } \Delta \quad \text{by assumption} \quad (637)$$

$\lambda x_A : \overline{A}. \text{sRed}(t_{\Pi x:A. B}) x_A$  is by choice of indeces (determined by the equality concluded in this step of the proof) almost proper with quasi-preimage of type  $\Pi x : A. B$ . It follows:

$$\Delta \vdash_{\overline{T}} \text{sRed}(t_{\Pi x:A. B}) =_{\overline{A} \rightarrow \overline{B}} \lambda x_A : \overline{A}. \text{sRed}(t_{\Pi x:A. B}) x_A \quad (\text{eta}), (636), (637) \quad (638)$$

$$\Delta \vdash_{\overline{T}} \text{sRed} \left( \text{sRed}(t_{\Pi x:A. B}) =_{\overline{A} \rightarrow \overline{B}} \lambda x_A : \overline{A}. \text{sRed}(t_{\Pi x:A. B}) x_A \right) \quad \text{SR2, SR6, SR4}, (638)$$

(*congl*):

$$\Delta \vdash_{\overline{T}} \text{sRed}(F_{\text{bool}} =_{\text{bool}} F'_{\text{bool}}) \quad \text{by assumption} \quad (639)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(F'_{\text{bool}}) \quad \text{by assumption} \quad (640)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(F_{\text{bool}}) =_{\text{bool}} \text{sRed}(F'_{\text{bool}}) \quad \text{SR4}, (639) \quad (641)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(F_{\text{bool}}) \quad (\text{congl}), (641), (640)$$

( $\Rightarrow I$ ):

$$\Delta \vdash_{\overline{T}} \text{sRed}(F_{\text{bool}}) : \text{bool} \quad \text{by assumption} \quad (642)$$

$$\Delta, \text{ass}_F : \text{sRed}(F_{\text{bool}}) \vdash_{\overline{T}} \text{sRed}(G_{\text{bool}}) \quad \text{by assumption} \quad (643)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(F_{\text{bool}}) \Rightarrow \text{sRed}(G_{\text{bool}}) \quad (\Rightarrow I), (642), (643) \quad (644)$$

$$\Delta \vdash_{\overline{T}} \text{sRed}(F_{\text{bool}} \Rightarrow G_{\text{bool}}) \quad \text{SR5}, (644)$$



( $\Rightarrow E$ ):

$$\Delta \vdash_{\bar{T}} \text{sRed} (F_{\text{bool}} \Rightarrow G_{\text{bool}}) \quad \text{by assumption} \quad (645)$$

$$\Delta \vdash_{\bar{T}} \text{sRed} (F_{\text{bool}}) \quad \text{by assumption} \quad (646)$$

$$\Delta \vdash_{\bar{T}} \text{sRed} (F_{\text{bool}}) \Rightarrow \text{sRed} (G_{\text{bool}}) \quad \text{SR5}, (645) \quad (647)$$

$$\Delta \vdash_{\bar{T}} \text{sRed} (G_{\text{bool}}) \quad (\Rightarrow E), (647), (646)$$

(*boolExt*):

$$\Delta \vdash_{\bar{T}} \text{sRed} (p_{\text{bool} \rightarrow \text{bool}} \text{true}_{\text{bool}}) \quad \text{by assumption} \quad (648)$$

$$\Delta \vdash_{\bar{T}} \text{sRed} (p_{\text{bool} \rightarrow \text{bool}} \text{false}_{\text{bool}}) \quad \text{by assumption} \quad (649)$$

$$\Delta \vdash_{\bar{T}} \text{sRed} (p_{\text{bool} \rightarrow \text{bool}}) \text{true} \quad (\text{SR2}), (\text{SR1}), (648) \quad (650)$$

$$\Delta \vdash_{\bar{T}} \text{sRed} (p_{\text{bool} \rightarrow \text{bool}}) \text{false} \quad (\text{SR2}), (\text{SR1}), (649) \quad (651)$$

$$\Delta \vdash_{\bar{T}} \forall x : \text{bool}. \text{sRed} (p_{\text{bool} \rightarrow \text{bool}}) x \quad (\text{boolExt}), (650), (651) \quad (652)$$

$$\Delta \vdash_{\bar{T}} \text{sRed} (\forall x : \text{bool}. \text{sRed} (p_{\text{bool} \rightarrow \text{bool}}) x) \quad \text{SR4}, (\text{SR2}), (\text{SR1}), (652)$$

#### C.4 Lifting admissible HOL derivations of validity statements to DHOL

We finally have all required results to prove the soundness of the translation from DHOL to HOL.

*Proof (Proof of Theorem 2).* As shown in Lemma 4, we may assume that the proof of  $\bar{\Gamma} \vdash_{\bar{T}} \bar{F}$  is admissible, so it only contains almost-proper terms. Consequently, whenever an equality  $s =_A t$  is derivable in HOL and  $s', t'$  are the quasi-preimages of  $s, t$  respectively, it follows that its quasi-preimage  $s' =_A t'$  is well-typed in DHOL and thus  $s' : A$  and  $t' : A$ . Without loss of generality (adding extra assumptions throughout the proof) we may assume that the context of the (final) conclusion is the translation of a DHOL context. By Lemma 3 the translation is term-wise injective.

Therefore, the translated conjecture is a proper validity statement with unique (quasi)-preimage in DHOL. If we can lift a derivation of the translated conjecture to a valid DHOL derivation of its quasi-preimage, the resulting derivation is a valid derivation of the original conjecture. This means, that it suffices to prove that we can lift admissible derivations of a proper validity statement  $S$  in HOL to a derivation of a quasi-preimage of  $S$ .

We prove this claim by induction on the validity rules of HOL as follows:

Given a validity rule  $R$  with assumptions  $A_1, \dots, A_n$ , validity assumptions (assumptions that are validity statements)  $V_1, \dots, V_m$ , non-judgement assumptions (meaning assumptions that something occurs in a context or theory)  $N_1, \dots, N_p$  and conclusion  $C$  we will show the following:

*Claim.* Assuming that the  $A_i$  and the  $N_j$  hold.

1. Assume that the conclusion  $C$  is proper with quasi-preimage  $C^{-1}$ . Then the contexts  $C_i$  of the  $V_i$  are proper and the quasi-preimages of the  $V_i$  are well-formed.
2. Assume that whenever an  $V_i$  is proper its quasi-preimage (where we choose the same preimages for identical terms and types with several possible preimages) holds in DHOL and that the conclusion  $C$  is proper with quasi-preimage  $C^{-1}$ . Then,  $C^{-1}$  holds in DHOL.

Consider the first part of this claim, namely that if  $C$  is proper then the  $V_i$  are proper. Since all formulae appearing in the derivation are almost proper, this implies that the  $V_i$  themselves are proper and by construction (choice of quasi-preimage) the contexts of their quasi-preimages fit together with the context of  $C^{-1}$ .

The translation clearly implies that if an  $N_j$  holds in HOL, the corresponding non-judgement assumption  $N_j^{-1}$  holds in DHOL (e.g. if  $\bar{F}$  is an axiom in  $\bar{T}$ , then  $F$  must be an axiom in  $T$ ).

Since the validity judgement being derived is proper, it follows from this first part of the claim that the validity assumptions of all validity rules in the derivation are proper.

By induction on the validity rules, if given an arbitrary validity rule  $R$  whose assumptions hold and whose validity assumptions all satisfy a property  $P$  we can show that  $P$  holds on the conclusion of  $R$ , then all derivable validity judgments have property  $P$ . Since all the validity assumptions and conclusions of validity rules in the derivation are proper, the property of having a derivable quasi-preimage is such a property. By this induction principle, it suffices to prove the claim for the validity rules in HOL.

We will therefore consider the validity rules one by one. For each rule we first prove the first part of the claim. Sometimes we also need that the quasi-preimages of some non-validity (typically typing) assumptions hold, so we will prove that this also follows from the conclusion being proper. Then the assumption of the second part, combined with the first part implies that the quasi-preimages of the  $V_i$  hold in DHOL and it is easy to prove that also  $C^{-1}$  holds in DHOL.

Throughout this proof we will use the notation  $\tilde{t}$  to denote that  $t$  is some quasi-preimage of  $\tilde{t}$ . Since the translation is surjective on type-level we will only need this notation on term-level.

Validity can be shown using the rules ([cong \$\lambda\$](#) ), ([eta](#)), ([congAppl](#)), ([cong \$\vdash\$](#) ), ([beta](#)), ([refl](#)), ([sym](#)), ([assume](#)), ([axiom](#)), ( [\$\Rightarrow\$ I](#)), ( [\$\Rightarrow\$ E](#)) and ([boolExt](#)).

([cong \$\lambda\$](#) ): Since the conclusion is proper, it follows that the preimage

$$\Gamma \vdash_T \lambda x : A. t =_{\Pi x:A. B} \lambda x : A. t'$$

of the normalization

$$\bar{\Gamma} \vdash_{\bar{T}} \forall x : \bar{A}. \forall y : \bar{A}. A^* x y \Rightarrow B^* \tilde{t} x \tilde{t} y$$

of the conclusion is well-formed. By rule ([eqTyping](#)) and rule ([sym](#)) we obtain  $\Gamma \vdash_T \lambda x : A. t : \Pi x : A. B$  and  $\Gamma \vdash_T \lambda x : A. t' : \Pi x : A. B$  in DHOL.

$$\begin{array}{lll}
\Gamma \vdash_T \lambda x : A. t : \Pi x : A. B & \text{see above} & (653) \\
\Gamma \vdash_T \lambda x : A. t' : \Pi x : A. B & \text{see above} & (654) \\
\Gamma, y : A \vdash_T (\lambda x : A. t) y : B & (\text{appl}), (\text{var}\vdash), (653), (\text{assume}) & (655) \\
\Gamma, y : A \vdash_T (\lambda x : A. t') y : B & (\text{appl}), (\text{var}\vdash), (654), (\text{assume}) & (656) \\
\Gamma, y : A \vdash_T (\lambda x : A. t) y =_B t[x/y] & (\text{beta}), (655) & (657) \\
\Gamma, y : A \vdash_T (\lambda x : A. t') y =_B t'[x/y] & (\text{beta}), (656) & (658) \\
\Gamma, x : A \vdash_T t : B & \alpha\text{-renaming}, (\text{cong}\vdash), (657) & (659) \\
\Gamma, x : A \vdash_T t' : B & \alpha\text{-renaming}, (\text{cong}\vdash), (658) & (660) \\
\Gamma, x : A \vdash_T t =_B t & (=type), (659), (660) & 
\end{array}$$

Clearly,  $\Gamma, x : A \vdash_T t =_B t'$  is a quasi-preimage of the validity assumption, so this proves the first part of the claim.

Regarding the second part:

$$\begin{array}{lll}
\Gamma, x : A \vdash_T t =_B t' & \text{by assumption} & (661) \\
\Gamma \vdash_T A \equiv A & (\equiv \text{refl}), (\text{typingTp}), (661) & (662) \\
\Gamma \vdash_T \lambda x : A. t =_{\Pi x : A. B} \lambda x : A. t' & (\text{cong}\lambda'), (662) & (663)
\end{array}$$

([eta](#)): Since the rule has no validity assumption, the first part of the claim holds.

For the second part, we still need the quasi-preimage of the assumption to hold, so we will show that it follows from the conclusion being proper.

Since the conclusion is proper, it follows that the preimage

$$\Gamma \vdash_T t =_{\Pi x : A. B} \lambda x : A. t x$$

of the normalization

$$\bar{\Gamma} \vdash_{\bar{T}} \forall x : \bar{A}. \forall y : \bar{A}. A^* x y \Rightarrow B^* \tilde{t} x \left( \lambda x : \bar{A}. \tilde{t} x \right) y$$

of the conclusion is well-formed. By rule ([eqTyping](#)) and rule ([sym](#)) we obtain  $\Gamma \vdash_T t : \Pi x : A. B$  and  $\Gamma \vdash_T \lambda x : A. t x : \Pi x : A. B$  in DHOL. Clearly,  $\Gamma \vdash_T t : \Pi x : A. B$  is a quasi-preimage of the validity assumption, so this proves the quasi-preimage of the assumption of the rule.

Regarding the second part:

$$\begin{array}{lll}
\Gamma \vdash_T t : \Pi x : A. B & \text{see above} & (664) \\
\Gamma \vdash_T t =_{\Pi x : A. B} \lambda x : A. t x & (\text{etaPi}), (664) & 
\end{array}$$

(*congAppl*): Since the conclusion is proper, it follows that the preimage

$$\Gamma \vdash_T f \ t =_B f' \ t'$$

of the normalization

$$B^* \widetilde{f} \widetilde{t} \widetilde{f'} \widetilde{t'}$$

of the conclusion is well-formed. By rule (*eqTyping*) and rule (*sym*) we obtain  $\Gamma \vdash_T f \ t : B$  and  $\Gamma \vdash_T f' \ t' : B$  in DHOL. Obviously,  $\Gamma \vdash_T t =_A t'$  and  $\Gamma \vdash_T f =_{\Pi x:A. B} f'$  are quasi-preimages of the validity assumptions.

Since the validity assumptions use the same context as the conclusion, it follows that they are both proper with uniquely determined context. As observed in the beginning of the proof if a proper assumption of a rule is an equality over a type  $\overline{A}$ , the induction hypothesis implies that the quasi-preimage of that assumption in which the equality is over type  $A$  must be well-formed. Hence both  $\Gamma \vdash_T t =_A t'$  and  $\Gamma \vdash_T f =_{\Pi x:A. B} f'$  are well-formed in DHOL, so we have proven the first part of the claim.

Regarding the second part of the claim:

$$\Gamma \vdash_T t =_A t' \quad \text{by assumption} \quad (665)$$

$$\Gamma \vdash_T f =_{\Pi x:A. B} f' \quad \text{by assumption} \quad (666)$$

$$\Gamma \vdash_T f \ t =_B f' \ t' \quad (\text{congAppl}), (665), (666) \quad (667)$$

This is what we had to show.

(*cong+*): Since the conclusion is proper, it follows that the preimage

$$\Gamma \vdash_T F$$

of the normalization

$$\overline{\Gamma} \vdash_{\overline{T}} \widetilde{F}$$

of the conclusion is well-formed. Thus we have  $\Gamma \vdash_T F : \text{bool}$ . Since the validity assumptions use the same context as the conclusion, it follows that they are both proper with uniquely determined. As observed in the beginning of the proof if a proper assumption of a rule is an equality over a type  $\overline{A}$  (here  $A = \overline{A} = \text{bool}$ ), the induction hypothesis implies that the quasi-preimage of that assumption in which the equality is over type  $\text{bool}$  must be well-formed. Clearly,  $\Gamma \vdash_T F' =_{\text{bool}} F$  and  $\Gamma \vdash_T F$  are the quasi-preimages of the two validity assumptions. Since the former is a validity statement about the quasi-preimage of an equality, it follows that  $\Gamma \vdash_T F' =_{\text{bool}} F$  is well-formed. We have already seen that  $\Gamma \vdash_T F$  is well-typed. This shows the first part of the claim.

Regarding the second part:

$$\Gamma \vdash_T F' =_{\text{bool}} F \quad \text{by assumption} \quad (668)$$

$$\Gamma \vdash_T F' \quad \text{by assumption} \quad (669)$$

$$\Gamma \vdash_T F \quad (\text{cong+}), (668), (669)$$

(*beta*): Since the rule has no validity assumptions, the first part of the claim trivially holds.

Since the conclusion is proper, it follows that the preimage

$$\Gamma \vdash_T (\lambda x : A. s) t =_{\Pi x:A. B} s[x/t]$$

of the normalization

$$\bar{\Gamma} \vdash_{\bar{T}} B^* (\lambda x : \bar{A}. \tilde{s}) \tilde{t} \tilde{s}[x/\tilde{t}]$$

of the conclusion is well-formed. By rule (*eqTyping*), we obtain  $\Gamma \vdash_T (\lambda x : A. s) t : B$  in DHOL. Clearly,  $\Gamma \vdash_T (\lambda x : A. s) t : B$  is a quasi-preimage of the assumption of the rule, so we have proven that the quasi-preimage of the assumption of the rule holds in DHOL.

Regarding the second part:

$$\begin{array}{ll} \Gamma \vdash_T \Gamma \vdash_T (\lambda x : A. s) t : B & \text{see above} \quad (670) \\ \Gamma \vdash_T \Gamma \vdash_T (\lambda x : A. s) t =_{\Pi x:A. B} s[x/t] & (\text{beta}), (670) \end{array}$$

(*refl*): Once again the rule has no validity assumptions, so the first part of the claim trivially holds.

Since the conclusion is proper, it follows that the preimage

$$\Gamma \vdash_T t =_A t'$$

of the normalization

$$\bar{\Gamma} \vdash_{\bar{T}} A^* \tilde{t} \tilde{t}$$

of the conclusion is well-formed. By Lemma 3 it follows that  $t$  and  $t'$  are identical so the quasi-preimage is  $\Gamma \vdash_T =_A t$ . By rule (*eqTyping*), we obtain  $\Gamma \vdash_T t : A$  in DHOL, the quasi-preimage of the assumption of the rule.

Regarding the second part of the claim:

$$\begin{array}{ll} \Gamma \vdash_T t : A & \text{see above} \quad (671) \\ \Gamma \vdash_T t =_A t & (\text{refl}), (671) \end{array}$$

(*sym*): Since the conclusion is proper, it follows that the preimage

$$\Gamma \vdash_T t =_A s$$

of the normalization

$$\bar{\Gamma} \vdash_{\bar{T}} A^* \tilde{t} \tilde{s}$$

of the conclusion is well-formed. By the rules (*eqTyping*) and (*sym*) both  $\Gamma \vdash_T t : A$  and  $\Gamma \vdash_T s : A$  follow. By rule (*=type*) it follows that  $\Gamma \vdash_T s =_A t$  is well-formed. Clearly,  $\Gamma \vdash_T s =_A t$  is the quasi-preimages of the validity assumption, so we have proven the first part of the claim.

Regarding the second part:

$$\Gamma \vdash_T t =_A s \quad \text{by assumption} \quad (672)$$

$$\Gamma \vdash_T s =_A t \quad (\text{sym}), (672) \quad (673)$$

(*assume*): Once again, there are no validity assumption, so the first part of the claim is trivial.

Since the conclusion is proper, it follows that the preimage

$$\Gamma \vdash_T F$$

of the normalization

$$\bar{\Gamma} \vdash_{\bar{T}} \widetilde{F}$$

of the conclusion is well-formed and thus  $\Gamma \vdash_T F : \text{bool}$ .

$$\Gamma \vdash_T F : \text{bool} \quad \text{see above} \quad (674)$$

$$\Gamma \vdash_T \text{bool tp} \quad (\text{typingTp}), (674) \quad (675)$$

$$\vdash_T \Gamma \text{ Ctx} \quad (\text{tpCtx}), (675) \quad (676)$$

The context assumption may be the translation of a context assumption in DHOL or a typing assumption added by the translation. In the latter case,  $F$  is of the form  $F = A^* x x$  for  $x : A$  in  $\Gamma$ . In that case, the second part of the claim  $\Gamma \vdash_T F$  can be concluded as follows:

$$\Gamma \vdash_T x : A \quad (\text{var}'), (<:\mathbb{I}) \quad (677)$$

$$\Gamma \vdash_T x =_A t \quad (\text{refl}), (677) \quad (678)$$

$$\Gamma \vdash_T F \quad \text{by assumption } F = A^* x x, (678)$$

Otherwise:

$$ass : F \text{ in } \Gamma \quad \text{by assumption} \quad (679)$$

$$\Gamma \vdash_T F \quad (\text{assume}), (679), (676)$$

(*axiom*): Once again, there are no validity assumption, so the first part of the claim is trivial.

Since the conclusion is proper, it follows that the preimage

$$\Gamma \vdash_T F$$

of the normalization

$$\bar{\Gamma} \vdash_{\bar{T}} \widetilde{F}$$

of the conclusion is well-formed and thus  $\Gamma \vdash_T F : \text{bool}$ .

$$\Gamma \vdash_T F : \text{bool} \quad \text{see above} \quad (680)$$

$$\Gamma \vdash_T \text{bool tp} \quad (\text{typingTp}), (680) \quad (681)$$

$$\vdash_T \Gamma \text{Ctx} \quad (\text{tpCtx}), (681) \quad (682)$$

The axiom may be the translation of an axiom in  $T$ , a typing axiom added by the translation or an axiom added for some base type  $A$ . In the first case, the second part of the claim follows by:

$$\begin{array}{ll} ax : F \text{ in } T & \text{by assumption} \\ \Gamma \vdash_T F & (\text{axiom}), (683), (682) \end{array} \quad (683)$$

If the axiom is a typing axiom then its preimage states that some constant  $c$  of type  $A$  satisfies  $c =_A t$  which follows by rule (refl).

If the axiom is the PER axiom generated for some  $A$  type declared in  $T$ , then it's quasi-preimage states that equality on  $A$  implies itself which is obviously true.

( $\Rightarrow I$ ): Since the conclusion is proper, it follows that the preimage

$$\Gamma \vdash_T F \Rightarrow G$$

of the normalization

$$\bar{\Gamma} \vdash_{\bar{T}} \tilde{F} \Rightarrow \tilde{G}$$

of the conclusion is well-formed and thus  $\Gamma \vdash_T F \Rightarrow G : \text{bool}$ .

$$\Gamma \vdash_T F \Rightarrow G : \text{bool} \quad \text{see above} \quad (684)$$

$$\Gamma \vdash_T F : \text{bool} \quad (\text{implTypingL}), (684) \quad (685)$$

$$\Gamma \vdash_T G : \text{bool} \quad (\text{implTypingR}), (684) \quad (686)$$

$$\Gamma, \text{ass} : F \vdash_T G : \text{bool} \quad (\text{monotonic}\vdash), (686)$$

Obviously  $\Gamma, \text{ass} : F \vdash_T G$  is a quasi-preimage of the validity assumption of the rule, so the first part of the claim is proven.

Regarding the second part:

$$\Gamma, \text{ass} : F \vdash_T G \quad \text{by assumption} \quad (687)$$

$$\Gamma \vdash_T F \Rightarrow G \quad (\Rightarrow I), (685), (687)$$

( $\Rightarrow E$ ): Since the conclusion is proper, it follows that the preimage

$$\Gamma \vdash_T G$$

of the normalization

$$\bar{\Gamma} \vdash_{\bar{T}} \tilde{G}$$

of the conclusion is well-formed and thus  $\Gamma \vdash_T G : \text{bool}$ .

Since the validity assumptions use the same context as the conclusion, it follows that they are both proper and uniquely determined.

Since the formula  $\widetilde{F}$  (where  $\overline{\Gamma} \vdash_{\overline{T}} \widetilde{F}$  is the second validity assumption) must be almost proper, it follows that its preimage  $F$  is well-typed i.e.  $\Gamma \vdash_T F : \text{bool}$ .

$$\begin{array}{ll} \Gamma \vdash_T F : \text{bool} & \widetilde{F} \text{ almost proper} \quad (688) \\ \Gamma \vdash_T G : \text{bool} & \text{see above} \quad (689) \\ \Gamma \vdash_T F \Rightarrow G : \text{bool} & (\Rightarrow \text{type}'), (688), (689) \end{array}$$

Clearly,  $\Gamma \vdash_T F \Rightarrow G$  and  $\Gamma \vdash_T F$  are quasi-preimages of the two validity assumptions of the rule, so we have proven the first part of the claim.

Regarding the second part:

$$\begin{array}{ll} \Gamma \vdash_T F \Rightarrow G & \text{by assumption} \quad (690) \\ \Gamma \vdash_T F & \text{by assumption} \quad (691) \\ \Gamma \vdash_T G & (\Rightarrow E), (690), (691) \end{array}$$

(*boolExt*): Since the conclusion is proper, it follows that the preimage

$$\Gamma \vdash_T \forall x : \text{bool}. p \ x$$

of the normalization

$$\overline{\Gamma} \vdash_{\overline{T}} \forall x : \text{bool}. \forall y : \text{bool}. \text{bool}^* x \ y \Rightarrow \text{bool}^* (\lambda x : \text{bool}. \text{true}) x \ \widetilde{p} \ y$$

of the conclusion is well-formed and thus  $\Gamma \vdash_T \forall x : \text{bool}. p \ x : \text{bool}$ . Expanding the definition of  $\forall$  yields:

$$\begin{array}{ll} \Gamma \vdash_T \lambda x : \text{bool}. \text{true} =_{\Pi x : \text{bool}. \text{bool}} \lambda x : \text{bool}. p \ x : \text{bool} & \text{see above} \quad (692) \\ \Gamma \vdash_T \lambda x : \text{bool}. p \ x : \Pi x : \text{bool}. \text{bool} & (\text{eqTyping}), (\text{sym}), (692) \quad (693) \\ \Gamma \vdash_T (\lambda x : \text{bool}. p \ x) \text{true} : \text{bool} & (\text{appl}), (693) \quad (694) \\ \Gamma \vdash_T (\lambda x : \text{bool}. p \ x) \text{false} : \text{bool} & (\text{appl}), (693) \quad (695) \\ \Gamma \vdash_T p \text{true} =_{\text{bool}} (\lambda x : \text{bool}. p \ x) \text{true} & (\text{sym}), (\text{beta}), (694) \quad (696) \\ \Gamma \vdash_T p \text{false} =_{\text{bool}} (\lambda x : \text{bool}. p \ x) \text{false} & (\text{sym}), (\text{beta}), (695) \quad (697) \\ \Gamma \vdash_T p \text{true} : \text{bool} & (\text{eqTyping}), (696) \\ \Gamma \vdash_T p \text{false} : \text{bool} & (\text{eqTyping}), (697) \end{array}$$

Since  $\Gamma \vdash_T p \text{true}$  and  $\Gamma \vdash_T p \text{false}$  are clearly quasi-preimages of the two validity assumptions of the rule, we have proven the first part of the claim.

Regarding the second part:

$$\begin{array}{ll} \Gamma \vdash_T p \text{true} & \text{by assumption} \quad (698) \\ \Gamma \vdash_T p \text{false} & \text{by assumption} \quad (699) \\ \Gamma \vdash_T \forall x : \text{bool}. p \ x & (\text{boolExt}), (698), (699) \quad (700) \end{array}$$