Subtyping in DHOL

Colin Rothgang[1,2][0000–0001–9751–8989] and Florian Rabe[3][0000–0003–3040–3655]

[1] Imdea Software Institute, Madrid, Spain
[2] Universidad Politécnica de Madrid, Madrid, Spain
[3] Computer Science, FAU Erlangen-Nürnberg, Germany

Abstract. The recently introduced dependent typed higher-order logic (DHOL) offers an interesting compromise between expressiveness and automation support. It sacrifices the decidability of its type-system in order to significantly extend its expressiveness over standard HOL. Yet it retains strong automated theorem proving support via a sound and complete translation to HOL.

We leverage this design to extend DHOL with refinement and quotient types. Both of these are commonly requested by practitioners but rarely provided by automated theorem provers. This is because they inherently require undecidable typing and thus are very difficult to retrofit to decidable type systems. But with DHOL already doing the heavy lifting, adding them is not only possible but elegant and simple.

Concretely, we add refinement and quotient types as special cases of subtyping. Crucially, this makes the associated canonical inclusion resp. projection identity maps and avoids costly changes in representation. We present the syntax, semantics, and translation to HOL for the extended language, including the proofs of soundness and completeness.

1 Introduction and Related Work

Motivation Recently dependently-typed higher-order logic (DHOL) was introduced [16]. It is a variant of HOL [4,1] that uses dependent function types $\Pi x{:}A.\ B$ instead of simple function types $A \to B$. It is designed to remain as simple and as close to HOL and ATPs as possible while meeting the frequent user demand of dependent types. Notably, contrary to typical formulations of dependent type theory, DHOL features a straightforward equality and classical Booleans at the cost of making typing undecidable.

Concretely, DHOL uses a type bool of propositions in the style of HOL, and equality $s =_A t : \mathsf{bool}$ of typed terms is a proposition, whose truth may depend on axioms in the theory or assumptions in the context. Equality $A \equiv B$ of types (which is not a proposition but a meta-level judgment) uses a straightforward congruence rule: if a dependent type constructor is applied to equal arguments, it produces equal types. Thus, equality of types and typing are undecidable. To yield practical tool support, DHOL reduces typing judgments to a series of proof obligations, and [16] gives a sound and complete translation to HOL that allows using existing automated theorem provers for HOL to discharge these.

While undecidable typing is not used by most current ATPs or ITPs, it is justified by the pragmatic consideration that the ultimate task of theorem proving is undecidable anyway, and the difficulty of typing-related proof obligations is often small in comparison. Follow-up work on DHOL includes a native ATP for DHOL [11] and extensions with a choice operator [14] and polymorphism [15].

Contribution The present paper leverages this key design choice and extends DHOL's expressivity at low cost by adding refinement and quotient types. Both work elegantly in languages with undecidable typing so that DHOL, for which the necessary meta-theory and infrastructure already exist, is a good base to support them. Indeed, the necessary changes to DHOL's syntax and semantics turned out to be few and simple.

Refinement types $A|_p$ consist of the terms of type A satisfying the predicate $p{:}A \to \mathsf{bool}$. They correspond to comprehension in set theory. They were already proposed in [16] (with ad-hoc subtyping rules), and here we give a systematic treatment. Critically, our refinement types avoid a change in representation: the injection $A|_p \to A$ is always a no-op. This is in contrast to encodings of refinement types in decidable type theories, such as using the type $\Sigma x{:}A.p\, x$, or in set-theory, where, e.g., the injection $(A \to B) \to (A|_p \to B)$ is not a no-op.

Quotient types A/r, intuitively, consist of all equivalence classes of the equivalence relation $r{:}A \to A \to \mathsf{bool}$. Again we avoid representation changes: We use all terms of type A as terms of type A/r and adjust the equality $=_{A/r}$ to obtain the quotient semantics. Thus, the projection $A \to A/r$ is a no-op and $A \prec: A/r$. In contrast, the usual definitions in set theory (via equivalence classes) or in decidable type theories (via setoids) require expensive changes in representation.

The statement $A \prec: A/r$ may look odd. It is sound because we use a different equality relation at the two types: $x =_A y$ implies $x =_{A/r} y$ but not the other way round. This approach captures the mathematical practice of using elements of A as elements of the quotient, often to the point that readers do not even notice anymore they are technically working with equivalence classes.

Together, this yields a subtype hierarchy of refinements and quotients of A: $A|_{\lambda x:A.\ \mathsf{false}} \prec: \ldots \prec: A|_p \prec: \ldots \prec: A|_{\lambda x:A.\ \mathsf{true}} \equiv A \equiv A/{=_A} \prec: \ldots \prec: A/r \prec: \ldots \prec: A/\lambda x, y{:}A.\ \mathsf{true}$ from initial (empty) type to terminal (singleton) types.

Related Work In formal systems, the approach of quotients as supertypes has been adopted only occasionally, e.g., in Nurpl's quotients [5] or in Quotient Haskell [2]. Nuprl's type theory also features refinement types similar to ours.

PVS [12] subsumes DHOL and refinement types with polymorphism. It does not support quotients, but its record subtyping resembles our quotient subtyping. Notably, it treats refinement subtyping and record subtyping as two separate judgments with slightly different rules.

In soft type systems, all types are refinements of a fixed universe of objects. For example, Mizar's [3] type system is inherently undecidable and supports dependent types and refinement types. It supports quotient types but only with a change in representation and not as supertypes.

Most ITPs allow users to construct refinement and quotient types at the cost of representation changes. Systems based on decidable dependent type theory like Coq [6] or Lean [7] typically use Σ-types for refinement and setoids for quotients. Lean provides some kernel support for quotients. Systems based on HOL [9] use the subtype definition principle to introduce types isomorphic to $A|_p$.

[15] adds polymorphism to DHOL, and in future work we want to combine both features. The key challenge will be to support *subtype-bounded* polymorphism.

Overview We give a self-contained definition of DHOL in Sect. 2. Then we add subtyping in Sect. 3, refinements in Sect. 4, and quotients in Sect. 5. We develop the meta-theory in Sect. 6 (type normalization) and Sect. 7 (soundness/completeness). We present an application to typed set theory in Sect. 8.

2 Preliminaries: Dependently Type Higher-Order Logic

The DHOL [16] **grammar** uses terms and types. A theory T declares typed constants $\mathtt{c}{:}A$, axioms $\triangleright F$, and dependent type symbols of the form $\mathtt{a}{:}\Pi x_1{:}A_1.\ \ldots \Pi x_n{:}A_n.\,\mathtt{tp}$, which are applied to terms to obtain base types $\mathtt{a}\ t_1\ \ldots\ t_n$. Contexts declare typed variables $x{:}A$ and local assumptions $\triangleright F$ (but no new types). Dependent functions $\lambda x{:}A.\ t$ of type $\Pi x{:}A.\ B$ (written $A \to B$ if x does not occur free in B) map terms $x{:}A$ to terms of type $B(x)$. We recover HOL as the fragment in which all base types $\mathtt{a}$ have arity 0, in which case all function types are simple.

T	$::=$	$\circ \mid T,\ \mathtt{a}{:}(\Pi x{:}A.)^*\mathtt{tp} \mid T,\ \mathtt{c}{:}A \mid T,\ \triangleright F$	theories
Γ	$::=$	$. \mid \Gamma,\ x{:}A \mid \Gamma,\ \triangleright F$	contexts
A, B	$::=$	$\mathtt{a}\ t^* \mid \Pi x{:}A.\ B \mid \mathsf{bool}$	types
s, t, F, G	$::=$	$\mathtt{c} \mid x \mid \lambda x{:}A.\ t \mid s\ t \mid s =_A t \mid F \Rightarrow G$	terms (incl. propositions)

Following typical HOL-style [1], DHOL defines all connectives and quantifiers from the equality connective $s =_A t$. However, DHOL needs *dependent* binary connectives: e.g., in an implication $F \Rightarrow G$, the well-formedness of G may depend on the truth of F. Because this cannot be defined from equality alone, DHOL must make one dependent connective an additional primitive.

DHOL uses axiomatic equality $s =_A t$ in the style of FOL and HOL with a straightforward congruence rule for base types: type equality $\mathtt{a}\ s_1\ \ldots\ s_n \equiv \mathtt{a}\ t_1\ \ldots\ t_n$ holds if each s_i is equal to t_i. This makes type equality and thus typing undecidable. In line with HOL's simplicity and unlike some dependent type theories, there is no support for type-valued computation like large elimination.

Example 1 (Lists). As an accessible running example, we show a formalization of lists over some type $\mathtt{obj}$, both plain lists list and lists $\mathit{llist}\ n$ with fixed length. Notably, the well-typedness of the statement of associativity of lconc now requires the associativity of plus.

$\mathrm{nat}\colon \mathtt{tp}$, $\mathrm{zero}\colon \mathrm{nat}$, $\mathrm{succ}\colon \mathrm{nat} \to \mathrm{nat}$, $\mathrm{plus}\colon \mathrm{nat} \to \mathrm{nat} \to \mathrm{nat}$,
$\mathtt{obj}\colon \mathtt{tp}$, $\mathrm{list}\colon \mathtt{tp}$, $\mathrm{nil}\colon \mathrm{list}$, $\mathrm{cons}\colon \mathtt{obj} \to \mathrm{list} \to \mathrm{list}$, $\mathrm{conc}\colon \mathrm{list} \to \mathrm{list} \to \mathrm{list}$,
$\mathrm{llist}\colon \mathrm{nat} \to \mathtt{tp}$, $\mathrm{lnil}\colon \mathrm{llist}\ \mathrm{zero}$,
$\mathrm{lcons}\colon \Pi n{:}\mathrm{nat}.\ \mathtt{obj} \to \mathrm{llist}\ n \to \mathrm{llist}\ (\mathrm{succ}\ n)$,
$\mathrm{lconc}\colon \Pi m, n{:}\mathrm{nat}.\ \mathrm{llist}\ m \to \mathrm{llist}\ n \to \mathrm{llist}\ (\mathrm{plus}\ m\ n)$

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

Fig. 1. DHOL Judgments

DHOL uses the **judgments** given in Fig. 1 and the **rules** listed in Fig. 2. Note that equality of terms is a special case of validity, whereas equality of types is not a Boolean but a separate judgment. Thus, users cannot state axioms equating types, and type equality is defined only by congruence. The rules are straightforward. In particular, type equality is checked structurally and reduced to a set of term equalities, which must then be discharged by an ATP.

The **semantics** for DHOL and a **practical ATP workflow** are given by a sound and complete translation to HOL. The translation is dependency erasure e.g., translating dependent types $\mathtt{a}\ t_1\ \ldots\ t_n$ to simple types $\mathtt{a}$, effectively "'merging"' all instances of a dependent type into a large simple type. The table below gives the key invariants, Fig. 3 defines the details.

DHOL	HOL
type A	type $\overline{A}$ and PER $A^*{:}\overline{A} \to \overline{A} \to \mathsf{bool}$
term $t{:}A$	term $\overline{t}{:}\overline{A}$ satisfying $A^*\ \overline{t}\ \overline{t}$

Typing and equality at A are recovered by generating a partial equivalence relation (PER) A^* for every HOL-type $\overline{A}$. A PER is a symmetric-transitive relation and the same as an equivalence relation on a subtype of $\overline{A}$. Thus, A corresponds in HOL to the quotient of the appropriate subtype of $\overline{A}$ by A^*.

DHOL terms are translated to their HOL analogues except that equality is translated to the respective PER: $\overline{s =_A t} := A^*\ \overline{s}\ \overline{t}$. In particular, the predicate $A^*\ \overline{t}\ \overline{t}$ captures whether t is a term of type A. For n-ary type symbols $\mathtt{a}$, the translation generates an $n+2$-ary predicate a^* such that $a^*\ \overline{t_1}\ \ldots\ \overline{t_n}$ is the PER

Theories and contexts:

$$\frac{}{\vdash \circ\ \mathsf{Thy}} \qquad \frac{\vdash_{\mathsf{T}} x_1{:}A_1,\ \dots,\ x_n{:}A_n\ \mathsf{Ctx}}{\vdash T,\ \mathsf{a}{:}\Pi x_1{:}A_1.\ \dots \Pi x_n{:}A_n.\ \mathsf{tp}\ \mathsf{Thy}} \qquad \frac{\vdash_{\mathsf{T}} A\ \mathsf{tp}}{\vdash T,\ \mathsf{c}{:}A\ \mathsf{Thy}} \qquad \frac{\vdash_{\mathsf{T}} F{:}\mathsf{bool}}{\vdash T,\ \triangleright F\ \mathsf{Thy}}$$

$$\frac{\vdash T\ \mathsf{Thy}}{\vdash_{\mathsf{T}} .\ \mathsf{Ctx}} \qquad \frac{\Gamma \vdash_{\mathsf{T}} A\ \mathsf{tp}}{\vdash_{\mathsf{T}} \Gamma,\ x{:}A\ \mathsf{Ctx}} \qquad \frac{\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool}}{\vdash_{\mathsf{T}} \Gamma,\ \triangleright F\ \mathsf{Ctx}}$$

Well-formedness and equality of types:

$$\frac{\mathsf{a}{:}\Pi x_1{:}A_1.\ \dots \Pi x_n{:}A_n.\ \mathsf{tp}\ \text{in}\ T \quad \Gamma \vdash_{\mathsf{T}} t_1{:}A_1 \quad \dots \quad \Gamma \vdash_{\mathsf{T}} t_n{:}A_n[x_1/t_1]\dots[x_{n-1}/t_{n-1}]}{\Gamma \vdash_T\ \mathsf{a}\ t_1\ \dots\ t_n\ \mathsf{tp}} \qquad \frac{\vdash_{\mathsf{T}} \Gamma\ \mathsf{Ctx}}{\Gamma \vdash_{\mathsf{T}} \mathsf{bool}\ \mathsf{tp}} \qquad \frac{\Gamma \vdash_{\mathsf{T}} A\ \mathsf{tp} \quad \Gamma,\ x{:}A \vdash_{\mathsf{T}} B\ \mathsf{tp}}{\Gamma \vdash_{\mathsf{T}} \Pi x{:}A.\ B\ \mathsf{tp}}$$

$$\frac{\mathsf{a}{:}\Pi x_1{:}A_1.\ \dots \Pi x_n{:}A_n.\ \mathsf{tp}\ \text{in}\ T \quad \Gamma \vdash_{\mathsf{T}} s_1 =_{A_1} t_1 \quad \dots \quad \Gamma \vdash_{\mathsf{T}} s_n =_{A_n[x_1/t_1]\dots[x_{n-1}/t_{n-1}]} t_n}{\Gamma \vdash_{\mathsf{T}} \mathsf{a}\ s_1\ \dots\ s_n \equiv \mathsf{a}\ t_1\ \dots t_n} \qquad \frac{\vdash_{\mathsf{T}} \Gamma\ \mathsf{Ctx}}{\Gamma \vdash_{\mathsf{T}} \mathsf{bool} \equiv \mathsf{bool}} \qquad \frac{\Gamma \vdash_{\mathsf{T}} A \equiv A' \quad \Gamma, x{:}A \vdash_{\mathsf{T}} B \equiv B'}{\Gamma \vdash_{\mathsf{T}} \Pi x{:}A.\ B \equiv \Pi x{:}A'.\ B'}$$

Typing:

$$\frac{c{:}A'\ \text{in}\ T \quad \Gamma \vdash_{\mathsf{T}} A' \equiv A}{\Gamma \vdash_{\mathsf{T}} \mathsf{c}{:}A} \qquad \frac{\Gamma,\ x{:}A \vdash_{\mathsf{T}} t{:}B \quad A' \equiv A}{\Gamma \vdash_{\mathsf{T}} (\lambda x{:}A.\ t){:}\Pi x{:}A'.\ B} \qquad \frac{\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool} \quad \Gamma,\ \triangleright F \vdash_{\mathsf{T}} G{:}\mathsf{bool}}{\Gamma \vdash_{\mathsf{T}} F \Rightarrow G{:}\mathsf{bool}}$$

$$\frac{x{:}A'\ \text{in}\ \Gamma \quad \Gamma \vdash_{\mathsf{T}} A' \equiv A}{\Gamma \vdash_{\mathsf{T}} x{:}A} \qquad \frac{\Gamma \vdash_{\mathsf{T}} f{:}\Pi x{:}A.\ B \quad \Gamma \vdash_{\mathsf{T}} t{:}A}{\Gamma \vdash_{\mathsf{T}} f\ t{:}B[x/t]} \qquad \frac{\Gamma \vdash_{\mathsf{T}} s{:}A \quad \Gamma \vdash_{\mathsf{T}} t{:}A}{\Gamma \vdash_{\mathsf{T}} s =_A t{:}\mathsf{bool}}$$

Equality: congruence, reflexivity, symmetry, β, η (derivable: transitivity, functional extensionality):

$$\frac{\Gamma \vdash_{\mathsf{T}} A \equiv A' \quad \Gamma,\ x{:}A \vdash_{\mathsf{T}} t =_B t'}{\Gamma \vdash_{\mathsf{T}} \lambda x{:}A.\ t =_{\Pi x:A.\ B} \lambda x{:}A'.\ t'} \qquad \frac{\Gamma \vdash_{\mathsf{T}} t =_A t' \quad \Gamma \vdash_{\mathsf{T}} f =_{\Pi x:A.\ B} f'}{\Gamma \vdash_{\mathsf{T}} f\ t =_B f'\ t'}$$

$$\frac{\Gamma \vdash_{\mathsf{T}} t{:}A}{\Gamma \vdash_{\mathsf{T}} t =_A t} \qquad \frac{\Gamma \vdash_{\mathsf{T}} t =_A s}{\Gamma \vdash_{\mathsf{T}} s =_A t} \qquad \frac{\Gamma \vdash_{\mathsf{T}} (\lambda x{:}A.\ s)\ t{:}B}{\Gamma \vdash_{\mathsf{T}} (\lambda x{:}A.\ s)\ t =_B s[x/t]} \qquad \frac{\Gamma \vdash_{\mathsf{T}} t{:}\Pi x{:}A.\ B}{\Gamma \vdash_{\mathsf{T}} t =_{\Pi x:A.\ B} \lambda x{:}A.\ t\ x}$$

Rules for validity: lookup, implication, Boolean equality and extensionality

$$\frac{\triangleright F\ \text{in}\ T \quad \vdash_{\mathsf{T}} \Gamma\ \mathsf{Ctx}}{\Gamma \vdash_{\mathsf{T}} F} \qquad \frac{\Gamma,\ \triangleright F \vdash_{\mathsf{T}} G}{\Gamma \vdash_{\mathsf{T}} F \Rightarrow G} \qquad \frac{\Gamma \vdash_{\mathsf{T}} F =_{\mathsf{bool}} F' \quad \Gamma \vdash_{\mathsf{T}} F'}{\Gamma \vdash_{\mathsf{T}} F}$$

$$\frac{\triangleright F\ \text{in}\ \Gamma \quad \vdash_{\mathsf{T}} \Gamma\ \mathsf{Ctx}}{\Gamma \vdash_{\mathsf{T}} F} \qquad \frac{\Gamma \vdash_{\mathsf{T}} F \Rightarrow G \quad \Gamma \vdash_{\mathsf{T}} F}{\Gamma \vdash_{\mathsf{T}} G} \qquad \frac{\Gamma \vdash_{\mathsf{T}} p\ \mathsf{true} \quad \Gamma \vdash_{\mathsf{T}} p\ \mathsf{false}}{\Gamma, x{:}\mathsf{bool} \vdash_{\mathsf{T}} p\ x}$$

Fig. 2. DHOL Rules

Theories and contexts: $\quad \overline{\circ} := \circ \qquad \overline{T,\ D} := \overline{T},\ \overline{D} \qquad \overline{.} := . \qquad \overline{\Gamma,\ D} := \overline{\Gamma},\ \overline{D}$

$$\overline{\mathsf{a}{:}\Pi x_1{:}A_1.\ \dots \Pi x_n{:}A_n.\ \mathsf{tp}} := \mathsf{a}{:}\mathsf{tp},\ a^*{:}\overline{A_1} \to \dots \to \overline{A_n} \to \mathsf{a} \to \mathsf{a} \to \mathsf{bool},$$
$$\triangleright\forall\, x_1{:}\overline{A_1}.\ \dots \forall\, x_n{:}\overline{A_n}.\ \forall\, u, v{:}\mathsf{a}.\ a^*\ x_1\ \dots\ x_n\ u\ v \Rightarrow u =_a v$$

$$\overline{\mathsf{c}{:}A} := \mathsf{c}{:}\overline{A},\ \triangleright A^*\ \mathsf{c}\ \mathsf{c} \qquad \overline{x{:}A} := x{:}\overline{A},\ \triangleright A^*\ x\ x$$

$$\overline{\triangleright F} := \triangleright \overline{F} \qquad \overline{\triangleright F} := \triangleright \overline{F}$$

Types: $\quad \overline{\mathsf{a}\ t_1\ \dots\ t_n} := \mathsf{a} \qquad (\mathsf{a}\ t_1\ \dots\ t_n)^*\ s\ t := a^*\ \overline{t_1}\ \dots\ \overline{t_n}\ s\ t$

$$\overline{\Pi x{:}A.\ B} := \overline{A} \to \overline{B} \qquad (\Pi x{:}A.\ B)^*\ f\ g := \forall\, x, y{:}\overline{A}.\ A^*\ x\ y \Rightarrow B^*\ (f\ x)\ (g\ y)$$

$$\overline{\mathsf{bool}} := \mathsf{bool} \qquad \mathsf{bool}^*\ s\ t := s =_{\mathsf{bool}} t$$

Terms: $\quad \overline{\mathsf{c}} := \mathsf{c} \qquad \overline{x} := x \qquad \overline{\lambda x{:}A.\ t} := \lambda x{:}\overline{A}.\ \overline{t} \qquad \overline{f\ t} := \overline{f}\ \overline{t}$

$$\overline{s =_A t} := A^*\ \overline{s}\ \overline{t} \qquad \overline{F \Rightarrow G} := \overline{F} \Rightarrow \overline{G}$$

Fig. 3. Definition of the Translation DHOL→HOL

for $\mathtt{a}\ t_1\ \ldots\ t_n$. For function types, the PER is the usual condition for logical relations: functions are related if they map related inputs to related outputs.

3 Subtyping

The treatment of quotients as supertypes and the use of different equality relations at different types are subtly difficult. Thus, we first introduce subtyping by its defining extensional property, from which we will derive all subtyping rules:

Definition 1 (Subtyping). *$\Gamma \vdash_{\mathsf{T}} A \prec: B$ abbreviates $\Gamma, x{:}A \vdash_{\mathsf{T}} x{:}B$.*

Lemma 1. *In any extension of DHOL, $\Gamma \vdash_{\mathsf{T}} A \prec: B$ iff $\dfrac{\Gamma \vdash_{\mathsf{T}} t{:}A}{\Gamma \vdash_{\mathsf{T}} t{:}B}$ is derivable.*

Proof. Left-to-right: We construct the function $\lambda x{:}A.\ x{:}A \to B$ and derive the desired rule using the typing rule for function application.
Right-to-left: We start with $\Gamma, x{:}A \vdash_{\mathsf{T}} x{:}A$ and apply the derivable rule.

This subtyping relation prevents *incidental* subtype instances, for which the rule from Lem. 1 is admissible but not derivable. For example, $A|_{\lambda x:A.\ \mathsf{false}}$ is a subtype of all refinements of A, but not of all types. More generally, this definition precludes using induction on the terms of A to conclude $A \prec: B$. This restriction ensures that subtyping is preserved under, e.g., theory extensions, substitution, or language extensions. Importantly, subtyping preserves equality:

Lemma 2. *Assume an extension of DHOL in which $\Gamma \vdash_{\mathsf{T}} x =_B x$ implies $\Gamma \vdash_{\mathsf{T}} x : B$. Let $F := \forall x{:}A.\ \forall y{:}A.\ x =_A y \Rightarrow x =_B y$. Then $\Gamma \vdash_{\mathsf{T}} A \prec: B$ iff $\Gamma \vdash_{\mathsf{T}} F : \mathsf{bool}$, and then $\Gamma \vdash_{\mathsf{T}} F$.*

Proof. Left-to-right: The assumption yields $\Gamma, x{:}A,\ y{:}A,\ \triangleright x =_A y \vdash_{\mathsf{T}} (\lambda x{:}A.\ x){:}A \to B$. We get $\Gamma, x{:}A,\ y{:}A,\ \triangleright x =_A y \vdash_{\mathsf{T}} (\lambda x{:}A.\ x)\ x =_B (\lambda x{:}A.\ x)\ y$ from congruence of function application and reflexivity and $x =_B y$ by β-reduction.
Right-to-left: Assume $x : A$. Instantiating F twice with x and applying modus ponens with $x =_A x$ yields $x =_B x$, from which we get $x : B$.

Lemma 3 (Preorder of Types). *In any extension of DHOL, subtyping is reflexive (in the sense that $\Gamma \vdash_{\mathsf{T}} A \equiv B$ implies $\Gamma \vdash_{\mathsf{T}} A \prec: B$) and transitive.*

Proof. Reflexivity: The assumption yields $\Gamma \vdash_{\mathsf{T}} \lambda x{:}A.\ x{:}A \to B$ and we also have $\Gamma \vdash_{\mathsf{T}} \lambda x{:}A.\ x{:}A \to A$. Applying both to a term t of type A and β-reducing yields the rule from Lem. 1. Transitivity follows immediately from Lem. 1.

To make subtyping an order, we need anti-symmetry with respect to $\equiv$. This is not derivable directly, i.e., we might have $\Gamma \vdash_{\mathsf{T}} A \prec: B$ and $\Gamma \vdash_{\mathsf{T}} B \prec: A$, in which case A and B would have the same terms, without being equal. We avoid this by *adding* the anti-symmetry rule

$$\frac{\Gamma \vdash_{\mathsf{T}} A \prec: B \qquad \Gamma \vdash_{\mathsf{T}} B \prec: A}{\Gamma \vdash_{\mathsf{T}} A \equiv B}\text{STantisym}$$

Notably, this is the only *change* made to DHOL so far — everything before has just been abbreviations. This change is conservative in the following sense:

Theorem 1 (Conservativity). *As defined so far, we have $A \prec: B$ iff $A \equiv B$.*

Proof. We show by induction on derivations that each term has a unique type up to type equality and that all term equality axioms satisfy subject reduction.

Theorem 2 (Congruence and Variance for Function Types). *The usual rules for function types are derivable:*

$$\frac{\Gamma \vdash_{\mathsf{T}} A' \prec: A \qquad \Gamma,\ x{:}A' \vdash_{\mathsf{T}} B \prec: B'}{\Gamma \vdash_{\mathsf{T}} \Pi x{:}A.\ B \prec: \Pi x{:}A'.\ B'} \qquad \frac{\Gamma \vdash_{\mathsf{T}} A' \equiv A \qquad \Gamma,\ x{:}A' \vdash_{\mathsf{T}} B \equiv B'}{\Gamma \vdash_{\mathsf{T}} \Pi x{:}A.\ B \equiv \Pi x{:}A'.\ B'}$$

The second rule is primitive in DHOL but derivable in DHOL with subtyping.

Proof. The first rule follows from the definition of subtyping and η-expanding the function under consideration. The second rule is derived by (STantisym), establishing the hypotheses using the variance rule and reflexivity of subtyping.

4 Refinement types

To add refinement types, we add only one production to the **grammar**:

$$A ::= \quad A|_p \quad \text{type } A \text{ refined by predicate } p \text{ on } A$$

Note that we do not add productions for terms — refinement types only provide new typing properties for the existing terms.

The **rules** for, respectively, formation, introduction, elimination (two rules), and equality for refinement types are:

$$\frac{\Gamma \vdash_{\mathsf{T}} p{:}A \to \mathsf{bool}}{\Gamma \vdash_{\mathsf{T}} A|_p \ \mathsf{tp}} \qquad \frac{\Gamma \vdash_{\mathsf{T}} t{:}A \qquad \Gamma \vdash_{\mathsf{T}} p\ t}{\Gamma \vdash_{\mathsf{T}} t{:}A|_p}$$

$$\frac{\Gamma \vdash_{\mathsf{T}} t{:}A|_p}{\Gamma \vdash_{\mathsf{T}} t{:}A} \qquad \frac{\Gamma \vdash_{\mathsf{T}} t{:}A|_p}{\Gamma \vdash_{\mathsf{T}} p\ t} \qquad \frac{\Gamma \vdash_{\mathsf{T}} s =_A t \qquad \Gamma \vdash_{\mathsf{T}} p\ s}{\Gamma \vdash_{\mathsf{T}} s =_{A|_p} t}$$

Example 2 (Refining Lists by Length). We extend Ex. 1 by defining fixed-length lists as a refinement of lists. First, we axiomatize a predicate length on lists:

$$\mathrm{length}\colon \mathrm{list} \to \mathrm{nat} \qquad \triangleright\ \mathrm{length\ nil} =_{\mathrm{nat}} \mathrm{zero}$$
$$\triangleright\ \forall x{:}\mathtt{obj}.\ \forall l{:}\mathrm{list}.\ \mathrm{length}\ (\mathrm{cons}\ x\ l) =_{\mathrm{nat}} \mathrm{succ}\ (\mathrm{length}\ l)$$

Then we define llist n := $\text{list}|_{\lambda l:\text{list}.\ \text{length}\ l =_{\text{nat}} n}$, and we can derive

$$\vdash \text{nil}:\text{llist zero} \qquad n:\text{nat} \vdash \text{cons} : \Pi x:\texttt{obj}.\ \Pi l:\text{llist}\ n.\ \text{llist}\ (\text{succ}\ n)$$

Theorem 3 (Congruence and Variance). *The following rules are derivable (if the involved types are well-formed):*

$$\frac{\Gamma \vdash_{\mathsf{T}} A \prec: A' \quad \Gamma,\ x:A,\ \triangleright p\ x \vdash_{\mathsf{T}} p'\ x}{\Gamma \vdash_{\mathsf{T}} A|_p \prec: A'|_{p'}} \qquad \frac{\Gamma \vdash_{\mathsf{T}} A\ \mathsf{tp}}{\Gamma \vdash_{\mathsf{T}} A \equiv A|_{\lambda x:A.\ \mathsf{true}}}$$

$$\frac{\Gamma \vdash_{\mathsf{T}} A \equiv A' \quad \Gamma \vdash_{\mathsf{T}} p =_{A \to \mathsf{bool}} p'}{\Gamma \vdash_{\mathsf{T}} A|_p \equiv A'|_{p'}} \qquad \frac{\Gamma \vdash_{\mathsf{T}} A|_p\ \mathsf{tp}}{\Gamma \vdash_{\mathsf{T}} A|_p \prec: A}$$

Proof. To derive the first rule, we assume the hypotheses and $x:A|_p$. The elimination rules yield $x:A$ and $p\ x$, then the first hypothesis yields $x:A'$ and $p'\ x$, then the introduction rule yields $x:A|_p$.
To derive the second rule, we apply (STantisym) and use the introduction/elimination rules to show the two subtype relationships.
These then imply the other rules.

5 Quotient types

To add quotient types we also extend the grammar with only one production:

$$A ::= \ {}^{A}/_{r} \quad \text{quotient of } A \text{ by equivalence relation } r$$

The rules for, respectively, formation, introduction, elimination, and equality for quotient types are:

$$\frac{\Gamma \vdash_{\mathsf{T}} A\ \mathsf{tp} \quad \Gamma \vdash_{\mathsf{T}} r:A \to A \to \mathsf{bool} \quad \Gamma \vdash_{\mathsf{T}} \mathrm{EqRel}(r)}{\Gamma \vdash_{\mathsf{T}} {}^{A}/_{r}\ \mathsf{tp}} \qquad \frac{\Gamma \vdash_{\mathsf{T}} t:A \quad \Gamma \vdash_{\mathsf{T}} {}^{A}/_{r}\ \mathsf{tp}}{\Gamma \vdash_{\mathsf{T}} t:{}^{A}/_{r}}$$

$$\frac{\Gamma \vdash_{\mathsf{T}} s:{}^{A}/_{r} \quad \Gamma,\ x:A,\ \triangleright x =_{A/r} s \vdash_{\mathsf{T}} t:B \quad \Gamma,\ x:A,\ x':A,\ \triangleright x =_{A/r} s,\ \triangleright x' =_{A/r} s \vdash_{\mathsf{T}} t =_B t[{}^{x}/_{x'}]}{\Gamma \vdash_{\mathsf{T}} t[{}^{x}/_{s}]:B[{}^{x}/_{s}]}$$

$$\frac{\Gamma \vdash_{\mathsf{T}} s:A \quad \Gamma \vdash_{\mathsf{T}} t:A \quad \Gamma \vdash_{\mathsf{T}} r:A \to A \to \mathsf{bool} \quad \Gamma \vdash_{\mathsf{T}} \mathrm{EqRel}(r)}{\Gamma \vdash_{\mathsf{T}} (s =_{A/r} t) =_{\mathsf{bool}} (r\ s\ t)}$$

where $\mathrm{EqRel}(r)$ abbreviates that r is an equivalence relation.

Example 3 (Sets). We extend Ex. 1 by obtaining sets as a quotient of lists. First, we axiomatize a predicate for containing an element:

$\text{contains}: \text{list} \to \texttt{obj} \to \mathsf{bool}$
$\triangleright \forall x:\texttt{obj}.\ \neg(\text{contains nil}\ x)$
$\triangleright \forall x:\texttt{obj}.\ \forall y:\texttt{obj}.\ \forall l:\text{list}.\ (\text{contains}\ (\text{cons}\ y\ l)\ x) =_{\mathsf{bool}} (x =_{\texttt{obj}} y \lor \text{contains}\ l\ x)$

Now we can define $\text{set} := {}^{\text{list}}/\lambda l{:}\text{list}.\ \lambda m{:}\text{list}.\ \forall\, x{:}\texttt{obj}.\ \text{contains}\ l\ x =_{\textsf{bool}} \text{contains}\ m\ x$ as the type of lists containing the same elements. The equality at set immediately yields extensionality $\vdash \forall\, x, y{:}\text{set}.\ \ x =_{\text{set}} y \ \ \Leftrightarrow (\forall\, z{:}\texttt{obj}.\ \text{contains}\ x\ z =_{\textsf{bool}} \text{contains}\ y\ z)$.

Any $l{:}\text{list}$ can be used as a representative of the respective equivalence class in set, and operations on sets can be defined via operations on lists, e.g., we can establish $\vdash \text{conc} : \text{set} \to \text{set} \to \text{set}$. To derive this, we assume $u{:}\text{set}$ and apply the elimination rule twice. First we apply it with $B = \text{list} \to \text{set}$ and $t = \text{conc}\ u$; we have to show $\text{conc}\ x =_{\text{list}\to\text{set}} \text{conc}\ x'$ under the assumption that x and y are equal as sets. That yields a term $\text{conc}\ u : \text{list} \to \text{set}$. We assume $v{:}\text{set}$ and apply the elimination rule again with $B = \text{set}$ to obtain $\text{conc}\ u\ v{:}\text{set}$, and then conclude via λ-abstraction and η-reduction.

The elimination rule above looks overly complex. It can be understood best by comparing it to the following, simpler and more intuitive rule

$$\frac{\Gamma,\ x{:}A \vdash_{\mathsf{T}} t{:}B \qquad \Gamma,\ x{:}A,\ x'{:}A,\ \triangleright r\ x\ x' \vdash_{\mathsf{T}} t =_B t[{}^{x}/_{x'}]}{\Gamma,\ x{:}{}^{A}/r \vdash_{\mathsf{T}} t{:}B}\,(*)$$

This rule captures the well-known condition that a function t on A may be used as a function on ${}^{A}/r$ if t maps equivalent representatives x, x' equally. It follows from our elimination rule by putting $s = x$, but is subtly weaker:

Example 4. Continuing Ex. 3, assume a total order on $\texttt{obj}$ and a function $g{:}\text{list}|_{\text{nonEmpty}} \to \texttt{obj}$ picking the maximum from a non-empty list. We should be able to apply g to some $s{:}\text{set}$ that we know to be non-empty. But if we try to apply $(*)$ to obtain $g\ s{:}\texttt{obj}$, we get stuck trying to prove $g\ x =_{\texttt{obj}} g\ x'$ for any x, x' that are representatives of an *arbitrary* equivalence class of lists. We cannot use the condition that s is non-empty and thus only non-empty lists need to be considered. Thus, we cannot derive the well-formedness of $g\ x$.

Our elimination rule remedies that: here we need to show $g\ x =_{\texttt{obj}} g\ x'$ for any x, x' that are representatives of *the class of* s. Thus, we can use that x and x' are non-empty and that thus $g\ x$ is well-formed.

In dependent type theory, the two elimination rules are equivalent because we can use $\Pi s{:}{}^{A}/r.\ s = x \to B$ as the return type. This is not possible in DHOL because equality is not a type but a Boolean.

Theorem 4 (Congruence and Variance). *The following rules are derivable if the involved types are well-formed and r, r' are equivalence relations:*

$$\frac{\Gamma \vdash_{\mathsf{T}} A \prec: A' \qquad \Gamma,\ x{:}A,\ y{:}A,\ \triangleright r\ x\ y \vdash_{\mathsf{T}} r'\ x\ y}{\Gamma \vdash_{\mathsf{T}} {}^{A}/r \prec: {}^{A'}/r'} \qquad \frac{\Gamma \vdash_{\mathsf{T}} A\ \textsf{tp}}{\Gamma \vdash_{\mathsf{T}} A \equiv {}^{A}/\lambda x{:}A.\ \lambda y{:}A.\ x =_A y}$$

$$\frac{\Gamma \vdash_{\mathsf{T}} {}^{A}/r\ \textsf{tp}}{\Gamma \vdash_{\mathsf{T}} A \prec: {}^{A}/r} \qquad \frac{\Gamma \vdash_{\mathsf{T}} A \equiv A' \qquad \Gamma \vdash_{\mathsf{T}} r =_{A\to A\to\textsf{bool}} r'}{\Gamma \vdash_{\mathsf{T}} {}^{A}/r \equiv {}^{A'}/r'}$$

Proof. First rule: Assume the hypotheses and $s{:}{}^{A}\!/r$. We use the elimination rule with $B = A'/r'$ and $t = x$. We prove $x{:}A,\ y{:}A,\ \triangleright x =_{A/r} s,\ \triangleright x' =_{A/r} s \vdash_{\mathsf{T}} x =_{A'/r'} x'$ by using the equality rule, which requires $x, x'{:}A'$ (shown using $A \prec: A'$) and $r'\ x\ x'$, our second assumption.
Second rule: Apply (STantisym) and use the introduction/elimination rules to show the two subtype relationships.
These then imply the other rules.

6 Normalizing Types

To build a type-checker, we derive normalization rules that reduce subtyping conditions to validity conditions that can then be discharged via an ATP. First we see that we can merge consecutive refinements and quotients:

Theorem 5 (Repeated Refinement/Quotient). *The following are derivable whenever the LHS is well-formed*

$$\vdash (A|_p)|_{p'} \ \equiv\ A|_{\lambda x:A.\ p\ x \wedge p'\ x} \qquad \vdash ({}^{A}\!/r)/r' \ \equiv\ {}^{A}\!/\lambda x{:}A.\ \lambda y{:}A.\ r'\ x\ y$$
$$\vdash ({}^{A}\!/r)|_p \ \equiv\ (A|_p)/r$$

Proof. *Refinement-refinement*: first show the RHS is well-formed: well-formedness of the LHS yields $p{:}A \to \mathsf{bool}$ and $p'{:}A|_p \to \mathsf{bool}$ and thus $p'\ x$ is well-formed as $\wedge$ is a *dependent* conjunction and $p\ x$ can be assumed while checking $p'\ x$. Verifying the equality is straightforward by showing subtyping in both directions.
Quotient-quotient: we first show that the RHS is well-formed: well-formedness of the LHS yields $r{:}A \to A \to \mathsf{bool}$ and $r'{:}{}^{A}\!/r \to {}^{A}\!/r \to \mathsf{bool}$, and $r'\ x\ y$ is well-formed because $A \prec: {}^{A}\!/r$. The relation on the RHS is an equivalence relation because r' is. To verify the type equality, we use Lem. 2 and show that both types induce the same equality on A. In particular, the type of r' already guarantees that it subsumes r.
Refinement-quotient: we first show that the RHS is well-formed: well-formedness of the LHS yields $r{:}A \to A \to \mathsf{bool}$ and $p{:}{}^{A}\!/r \to \mathsf{bool}$. That implies $r{:}A|_p \to A|_p \to \mathsf{bool}$ and $p{:}A \to \mathsf{bool}$, which is needed for the well-formedness of the RHS. (Note the other direction does not hold in general.) To show the equality, we show both subtyping directions. For LHS $\prec:$ RHS, we assume $x{:}{}^{A}\!/r$ and $p\ x$ and apply the elimination rule for quotients using $t = x$ and $B = (A|_p)/r$. (Critically, this step would not go through if we had only used the weaker rule $*$ in Sect. 5.) For RHS $\prec:$ LHS, we assume $x{:}(A|_p)/r$ and apply the elimination rule for quotients using $t = x$.

Similarly, we can derive rules for the 4 possible combinations of a function type with a refinement or quotient:

Theorem 6 (Refinement/Quotient in a Function Type). *The following are derivable if either side is well-formed:*

$$\vdash \Pi x{:}A.\ (B|_p) \ \equiv\ (\Pi x{:}A.\ B)|_{\lambda f:\Pi x:A.\ B.\ \forall x:A.\ p\ (f\ x)}$$

$$\vdash \Pi x{:}A/r.\ B \equiv (\Pi x{:}A.\ B)|_{\lambda f:\Pi x:A.\ B.\ \forall x,y:A.\ r\ x\ y \Rightarrow (f\ x) =_B (f\ y)}$$

$$\vdash \Pi x{:}A.\ B/r :\succ (\Pi x{:}A.\ B)/\lambda f, g{:}\Pi x{:}A.\ B.\ \forall x{:}A.\ r\ (f\ x)\,(g\ x)$$

The following is derivable if the RHS is well-formed:

$$\vdash \Pi x{:}A|_p.\ B :\succ (\Pi x{:}A.\ B)/\lambda f, g{:}\Pi x{:}A.\ B.\ \forall x{:}A.\ p\ x \Rightarrow (f\ x) =_B (g\ x)$$

Proof. Refined codomain: Both subtyping directions are straightforward, as terms on either side are given by $\lambda x{:}A.\ t$ where t has type B and satisfies p.
Quotiented domain: Both subtyping directions are straightforward, as both sides are subtypes of $\Pi x{:}A.\ B$ so their elements must preserve r.
Quotiented codomain: We assume a term f of RHS-type and show $x{:}A \vdash f\ x{:}B/r$ using the quotient elimination rule.
Refined domain: Assume a term f of RHS-type and show $x{:}A|_p \vdash f\ x{:}B$ using the quotient elimination rule. The well-formedness of the LHS does not imply the well-formedness of the RHS since the well-formedness of B can rely on $p\ x$.

Maybe surprisingly, two of the subtyping laws in Thm. 6 are not equalities. The law for the refined domain *must not* be an equality:

> *Example 5 (Refined Domain).* The assumption $p\ x$ makes more terms well-typed and thus there may be functions $\Pi x{:}A|_p.\ B$ that are not a restriction of a function $\Pi x{:}A.\ B$. Consider the theory $\mathsf{a}{:}\mathsf{bool} \to \mathsf{tp}$, $\mathsf{c}{:}\mathsf{a}\ \mathsf{true}$. Then $\mathsf{a}\ \mathsf{false}$ is empty and so are $\Pi x{:}\mathsf{bool}.\ \mathsf{a}\ x$ and its quotients. But with $p = \lambda x{:}\mathsf{bool}.\ x$, we have $\vdash \lambda x{:}\mathsf{bool}|_p.\ \mathsf{c} : \Pi x{:}\mathsf{bool}|_p.\ \mathsf{a}\ x$.

The law for the quotiented codomain *may or may not* be an equality. This is related to the axiom of choice. Consider the two statements

$$\vdash_{\mathsf{T}} \exists\, repr{:}B/r \to B.\ repr =_{B/r \to B/r} \lambda x{:}B/r.\ x$$

$$f{:}\Pi x{:}A.\ B/r \vdash_{\mathsf{T}} \exists\, g{:}\Pi x{:}A.\ B.\ f =_{\Pi x:A.\ B/r} g$$

(Note that the first one is well-typed because $B \prec: B/r$.) Both have a claim to be called the axiom of choice: The first one expresses that every equivalence relation has a system of representatives. The second generalizes this to a family of equivalence relations. The latter implies the former (put $A := B/r$ and $f := \lambda x{:}B/r.\ x$). In the simply-typed case the former also implies the latter (pick $repr \circ f$ for g); but in the dependently-typed case, B and r may depend on x and the implication might not hold.

Both statements construct a new term from an existing one ($repr$ behaves like the identity, and g like f) that has a different type but behaves the same up to quotienting. If the direction $\prec:$ were to hold in the law for the refined codomain, it would not only imply the existence of g from f but also allow using f as a representative of the equivalence class of possible values for g. That is in keeping with our goal of avoiding changes of representation. Therefore:

Definition 2 (Quotiented Codomain). *We adopt the subtyping rule below (which is an equality in conjunction with Thm. 6) as an additional axiom whenever either side is well-formed:*

$$\vdash \Pi x{:}A.\ B/r \prec: (\Pi x{:}A.\ B)/\lambda f, g{:}\Pi x{:}A.\ B.\ \forall x{:}A.\ r\ \ (f\ \ x)\,(g\ \ x)$$

Aggregating the above laws, we obtain a normalization algorithm for types:

Theorem 7 (Normalizing Types). *Every type is equal to a type of the form* $(A|_p)/r$ *where* $A, B ::= \mathsf{bool} \mid \mathsf{a}\ t^* \mid \Pi x{:}A|_p.\ B$*. In particular, if a type does not use refined domains, it is equal to a quotient of a refinement of a DHOL type.*

Proof. Using Thm. 6 with the axiom from Def. 2, all refinements and quotients can be pushed out of all function types except for a single refinement of the domain; if there is no such refinement, we can use $p := \lambda x{:}A.\ \mathsf{true}$. And using Thm. 5, those can be collected into a single quotient+refinement.

Together with the equality and variance rules from Thm. 2, 3, 4, this induces a **subtype-checking algorithm** that reduces subtyping to validity without ever expanding Def. 1. The latter is important because expanding Def. 1 would recurse into a computationally expensive problem. This algorithm is obviously sound as it only chains derived rules. We are confident that it is also complete in the sense that subtyping can always be derived by using only our derived rules (i.e., without Def. 1) and a sound and complete oracle for validity (which we obtain in Sect. 7). But we have so far been unable to finish the proof.

It may be surprising and certainly complicates subtype-checking that we need to allow for refined domains in the normal forms. This limitation echoes an observation first made in [10] about combining dependent types and refinements. Effectively, the culprit are partial dependent functions that cannot be extended to total functions because the return type is well-defined and non-empty only for the refined domain. For future work, it is interesting to use a higher-order logic with partial functions as a translation target, like the one of [8]. But we have not considered that option due to the lack of ATP support for such logics.

7 Soundness and Completeness

We extend the translation from Fig. 3 with cases for our two new productions:

$$\begin{array}{ll} \overline{A|_p} := \overline{A} & \qquad (A|_p)^*\ \ s\ t := A^*\ \ s\ t \wedge \overline{p}\ \ s \wedge \overline{p}\ \ t \\ \overline{A/r} := \overline{A} & \qquad (A/r)^*\ \ s\ t := \overline{r}\ \ s\ t \wedge A^*\ \ s\ s \wedge A^*\ \ t\ t \end{array}$$

These definitions are not surprising as PERs in HOL are known to be closed under refinements and quotients. Like in [16], this translation yields a sound (defined as in the previous paper) and complete theorem prover:

Theorem 8 (Completeness). *HOL can prove the translations of all derivable DHOL judgments:*

if in DHOL	*then in HOL*		
$\vdash T$ Thy	$\vdash \overline{T}$ Thy		
$\vdash_T \Gamma$ Ctx	$\vdash_{\overline{T}} \overline{\Gamma}$ Ctx		
$\Gamma \vdash_T A$ tp	$\overline{\Gamma} \vdash_{\overline{T}} \overline{A}$ tp	*and*	$\overline{\Gamma} \vdash_{\overline{T}} A^* : \overline{A} \to \overline{A} \to \mathsf{bool}$ *and* A^* *is a PER*
$\Gamma \vdash_T A \equiv B$	$\overline{\Gamma} \vdash_{\overline{T}} \overline{A} \equiv \overline{B}$	*and*	$\overline{\Gamma},\ x, y{:}\overline{A} \vdash_{\overline{T}} A^*\ x\ y =_{\mathsf{bool}} B^*\ x\ y$
$\Gamma \vdash_T A \prec: B$	$\overline{\Gamma} \vdash_{\overline{T}} \overline{A} \equiv \overline{B}$	*and*	$\overline{\Gamma},\ x, y{:}\overline{B} \vdash_{\overline{T}} A^*\ x\ y \Rightarrow B^*\ x\ y$
$\Gamma \vdash_T t{:}A$	$\overline{\Gamma} \vdash_{\overline{T}} \overline{t}{:}\overline{A}$	*and*	$\overline{\Gamma} \vdash_{\overline{T}} A^*\ \overline{t}\ \overline{t}$
$\Gamma \vdash_T F$	$\overline{\Gamma} \vdash_{\overline{T}} \overline{F}$		

Proof. The subtyping claim is a slightly strengthened version of the claim obtained by expanding the definition of $\prec:$. The proof, given in Appendix C, adapts the proof from [16] with additional cases for new productions and rules.

Example 6 (PERs for a Quotiented Codomain). We calculate the PERs for both sides of the law for quotiented codomains in Thm. 6:

$$\begin{aligned}&(\Pi x{:}A.\ {}^{B}/_{r})^*\ f\ g = \\ &\forall\, x, y{:}\overline{A}.\ A^*\ x\ y \Rightarrow (\overline{r}\ (f\ x)\ (g\ y) \wedge B^*\ (f\ x)\ (f\ x) \wedge B^*\ (g\ y)\ (g\ y)) = \\ &\forall\, x{:}\overline{A}.\ A^*\ x\ x \Rightarrow \overline{r}\ (f\ x)\ (g\ x) \wedge B^*\ (f\ x)\ (f\ x) \wedge B^*\ (g\ y)\ (g\ y)\end{aligned}$$

That is exactly what we get when we unfold

$$((\Pi x{:}A.\ B)/\lambda f, g{:}\Pi x{:}A.\ B.\ \forall\, x{:}A.\ r\ \ (f\ x)\,(g\ x))^*\ f\ g$$

This justifies adopting the axiom in Def. 2.

Example 7 (PERs for the a Refined Domain). We calculate the PERs for both sides of the law for refined domains in Thm. 6:

$$(\Pi x{:}A|_p.\ B)^*\ f\ g = \forall\, x, y{:}\overline{A}.\ A^*\ x\ y \wedge \overline{p}\ x \wedge \overline{p}\ y \Rightarrow B^*\ (f\ x)\ (g\ y)$$

$$\begin{aligned}&((\Pi x{:}A.\ B)/\lambda f, g{:}\Pi x{:}A.\ B.\ \forall\, x{:}A.\ p\ x \Rightarrow (f\ x) =_B (g\ x))^*\ f\ g = \\ &\forall\, x{:}\overline{A}.\ A^*\ x\ x \Rightarrow (\overline{p}\ x \Rightarrow B^*\ (f\ x)\ (g\ x)) \wedge \\ &\big(\forall\, x, y{:}\overline{A}.\ A^*\ x\ y \Rightarrow B^*\ (f\ x)\ (f\ y)\big) \wedge \\ &\big(\forall\, x, y{:}\overline{A}.\ A^*\ x\ y \Rightarrow B^*\ (g\ x)\ (g\ y)\big)\end{aligned}$$

These are indeed not equivalent in line with our observation from Ex. 5.

As in [16], the converse of Thm. 8 is much harder to state and prove. First we need a technical assumption: We call a type symbol $\mathtt{a}$ *inhabited* if at least one of its instances is provably non-empty.

Theorem 9 (Soundness). *In a well-formed DHOL-theory* $\vdash T$ Thy *in which every type symbol is inhabited:*

$$\textit{If } \Gamma \vdash^{\mathsf{DHOL}}_{\mathsf{T}} F : \mathsf{bool} \textit{ and } \overline{\Gamma} \vdash^{HOL}_{\overline{T}} \overline{termF}, \textit{ then } \Gamma \vdash^{\mathsf{DHOL}}_{\mathsf{T}} F$$

Proof. The key idea is to transform a HOL-proof of $\overline{F}$ 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 Appendix D. We expect the inhabitation requirement to be redundant, but have not been able to complete the proof without it yet. In any case, it is harmless because it is satisfied by all practical examples.

It is now straightforward to extend the DHOL implementation we gave in [16]: First we use a bidirectional type-checker for DHOL, combined with the subtyping-checker sketched in Sect. 6, to establish that a theory and conjecture are well-typed. Then we translate the generated proof obligations and the conjecture to HOL and apply a HOL ATP.

8 Application to Typed Set Theory

DHOL with subtyping enables a novel formalization of typed set-theory:

$$\mathrm{set}{:}\mathsf{tp}, \qquad \in\, : \mathrm{set} \to \mathrm{set} \to \mathsf{bool}, \qquad elem\ s := \mathrm{set}|_{\lambda x:\mathrm{set}.\ x \in s}$$

The key idea is that $elem\, s$ is the DHOL *type* of set-theoretical elements of the *set* s. Leveraging that refinements and quotients do not require change of representation, we obtain a powerful combination of elegant high-level typed formalization and efficient low-level reasoning.

All the routine constructions of untyped set theory can be lifted to their typed counterparts. For example, for products, it contains definitions for untyped operators $\times{:}\mathrm{set} \to \mathrm{set} \to \mathrm{set}$ and $pair{:}\mathrm{set} \to \mathrm{set} \to \mathrm{set}$ with the property that $\rhd \forall x, y, s, t{:}\mathrm{set}.\ x \in s \wedge y \in t \Rightarrow pair\ x\ y \in s \times t$. On top of that, we can now elegantly define the corresponding typed operators

$$tpair : \Pi s, t{:}\mathrm{set}.\ elem\ s \to elem\ t \to elem\ s \times t \quad := \quad \lambda s, t, x, y. pair\, x\, y$$

We obtain the proof obligation $x{:}elem\ s,\ y{:}elem\ t \vdash pair\ x\ y : elem\ s \times t$ during type-checking, which is exactly the corresponding untyped theorem.

We can also use DHOL-functions $\mathrm{set} \to \mathrm{set}$ as set-theoretical functions between sets s and t without a change in representation as the type $Functions\, s\, t := (\mathrm{set} \to \mathrm{set})|_p /r$ where $p\ f = \forall x{:}\mathrm{set}.\ x \in s \Rightarrow (f\ x) \in t$ and $r\ f\ g = \forall x{:}\mathrm{set}.\ x \in s \Rightarrow (f\ x) =_{\mathrm{set}} (g\ x)$. This allows us to represent set-theoretical function application . and composition $\circ$ directly as DHOL application/composition.

Consequently, theorem proving in typed set theory becomes very strong because a large share of the proving workload can be outsourced into typing-obligations.

For example, the property that the composition of functions $f : \mathit{Functions}\ s\ t$ and $g : \mathit{Functions}\ t\ u$ has type $\mathit{Functions}\ s\ u$ becomes

$$\triangleright\forall\, s,t,u{:}\mathrm{set}.\ \forall\, f{:}\mathit{Functions}\ s\ t.\ \forall\, g{:}\mathit{Functions}\ t\ u.\ \forall\, x{:}\mathrm{set}.\ x \in s \Rightarrow ((g \circ f)\ x) \in u$$

which yields in HOL the conjecture below that current HOL ATPs solve easily.

$$\begin{aligned}
&\triangleright\forall\, s{:}\mathrm{set}.\ \mathit{set_rel}\ s\ s \Rightarrow \forall\, t{:}\mathrm{set}.\ \mathit{set_rel}\ t\ t \Rightarrow \forall\, u{:}\mathrm{set}.\ \mathit{set_rel}\ u\ u \Rightarrow\\
&\quad \forall\, f{:}\mathrm{set} \to \mathrm{set}.\ \forall\, x{:}\mathrm{set}.\ x \in s \Rightarrow \mathit{set_rel}(f\ x)(f\ x) \wedge (\forall\, x{:}\mathrm{set}.\ x \in s \Rightarrow (f\ x) \in t) \Rightarrow\\
&\quad \forall\, g{:}\mathrm{set} \to \mathrm{set}.\ \forall\, x{:}\mathrm{set}.\ x \in t \Rightarrow \mathit{set_rel}(g\ x)(g\ x) \wedge (\forall\, x{:}\mathrm{set}.\ x \in t \Rightarrow (g\ x) \in u) \Rightarrow\\
&\quad \forall\, x{:}\mathrm{set}.\ \mathit{set_rel}\ u \Rightarrow x \in s \Rightarrow ((g\ (f\ x)) \in u)
\end{aligned}$$

Below is the HOL translation of the conjecture that function composition is associative. It is similarly easily proved by current ATPs:

$$\begin{aligned}
&\triangleright\forall\, s{:}\mathrm{set}.\ \mathit{set_rel}\ s\ s \Rightarrow \forall\, t{:}\mathrm{set}.\ \mathit{set_rel}\ t\ t \Rightarrow \forall\, u{:}\mathrm{set}.\ \mathit{set_rel}\ u\ u \Rightarrow \forall\, v{:}\mathrm{set}.\ \mathit{set_rel}\ v\ v \Rightarrow\\
&\quad \forall\, f{:}\mathrm{set} \to \mathrm{set}.\ \forall\, x{:}\mathrm{set}.\ x \in s \Rightarrow \mathit{set_rel}(f\ x)(f\ x) \wedge (\forall\, x{:}\mathrm{set}.\ x \in s \Rightarrow (f\ x) \in t) \Rightarrow\\
&\quad \forall\, g{:}\mathrm{set} \to \mathrm{set}.\ \forall\, x{:}\mathrm{set}.\ x \in t \Rightarrow \mathit{set_rel}(g\ x)(g\ x) \wedge (\forall\, x{:}\mathrm{set}.\ x \in t \Rightarrow (g\ x) \in u) \Rightarrow\\
&\quad \forall\, h{:}\mathrm{set} \to \mathrm{set}.\ \forall\, x{:}\mathrm{set}.\ x \in u \Rightarrow \mathit{set_rel}(h\ x)(h\ x) \wedge (\forall\, x{:}\mathrm{set}.\ x \in t \Rightarrow (h\ x) \in v) \Rightarrow\\
&\quad \forall\, x{:}\mathrm{set}.\ \mathit{set_rel}\ x\ x \Rightarrow x \in s \Rightarrow (\mathit{set_rel}\ (h\ (g\ (f\ x)))\ (h\ (g\ (f\ x))))
\end{aligned}$$

The corresponding TPTP files are available at `https://gl.mathhub.info/MMT/LATIN2/-/tree/master/source/casestudies/2025-cade`.

9 Conclusion and Future Work

DHOL combines higher-order logic with dependent types, obtaining an intuitive and expressive language, albeit with undecidable typing. We double down on this design by elegantly extending DHOL with two practically important type constructors that thrive in that setting: refinement and quotient types. Like dependent function types, these two require terms occurring in types. Both are near-impossible to add as an afterthought to a type theory with decidable typing.

We translate the resulting logic to HOL, obtaining a practical automated theorem proving workflow for DHOL with refinement and quotient types. Our main result is the proof of soundness and completeness of this translation.

We used an extensional subtyping approach, where $A \prec: B$ holds iff all A-terms also have type B. This allows combining typed representations and efficient reasoning. We established all the expected variance and normalization laws except for function types with refined domains. Future work must investigate how to improve on this to make normalizing types and thus subtype-checking simpler.

We also want to carry our results for DHOL over to existing refinement/quotient type systems for programming languages like Quotient Haskell, where DHOL-like axioms are used as lightweight specifications.

References

1. Andrews, P.: An Introduction to Mathematical Logic and Type Theory: To Truth Through Proof. Academic Press (1986)
2. B. Hewer and G. Hutton: Quotient Haskell: Lightweight Quotient Types for All. Proc. ACM Program. Lang. **8**(POPL) (2024). https://doi.org/10.1145/3632869, https://doi.org/10.1145/3632869
3. Bancerek, G., Byliński, C., Grabowski, A., Korniłowicz, A., R. Matuszewski, A.N., Pak, K., Urban, J.: Mizar: State-of-the-art and beyond. In: Kerber, M., Carette, J., Kaliszyk, C., Rabe, F., Sorge, V. (eds.) Intelligent Computer Mathematics. p. 261–279. Springer International Publishing, Cham (2015)
4. Church, A.: A Formulation of the Simple Theory of Types. Journal of Symbolic Logic **5**(1), 56–68 (1940)
5. 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)
6. Coq Development Team: The Coq Proof Assistant: Reference Manual. Tech. rep., INRIA (2015)
7. 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)
8. Farmer, W.: A simple type theory with partial functions and subtypes. Annals of Pure and Applie Logic **64**(3), 211–240 (1993)
9. 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)
10. Hurd, J.: Predicate subtyping with predicate sets. In: Boulton, R., Jackson, P. (eds.) Theorem Proving in Higher Order Logics. pp. 265–280 (2001)
11. Niederhauser, J., Brown, C., Kaliszyk, C.: Tableaux for automated reasoning in dependently-typed higher-order logic. In: Benzmüller, C., Heule, M., Schmidt, R. (eds.) Automated Reasoning. Springer (2024)
12. 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)
13. Rabe, F.: A Modular Type Reconstruction Algorithm. ACM Transactions on Computational Logic **19**(4), 1–43 (2018)
14. Ranalter, D., Brown, C., Kaliszyk, C.: Experiments with choice in dependently-typed higher-order logic. In: Bjørner, N., Heule, M., Voronkov, A. (eds.) Logic for Programming, Artificial Intelligence and Reasoning. pp. 311–320 (2024)
15. Ranalter, D., Rabe, F., Kaliszyk, C.: Polymorphic theorem proving for dhol
16. Rothgang, C., Rabe, F., Benzmüller, C.: Theorem Proving in Dependently Typed Higher-Order Logic. In: Pientka, B., Tinelli, C. (eds.) Automated Deduction. pp. 438–455. Springer (2023)

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.

A.1 HOL rules

A.2 Derived rules

Using the rules given in Figure 4 we can derive a number of additional useful rules.

A.3 Admissible rules for HOL

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

Lemma 4. *Given the inference rules for HOL (cfg. Figure 4), the following rules are admissible:*

$$\frac{\vdash_{\mathsf{T}} \Gamma\ \mathsf{Ctx}}{\vdash T\ \mathsf{Thy}}\,ctxThy \qquad \frac{\Gamma \vdash_{\mathsf{T}} A\ \mathsf{tp}}{\vdash_{\mathsf{T}} \Gamma\ \mathsf{Ctx}}\,tpCtx \qquad \frac{\Gamma \vdash_{\mathsf{T}} t{:}A}{\Gamma \vdash_{\mathsf{T}} A\ \mathsf{tp}}\,typingTp \qquad \frac{\Gamma \vdash_{\mathsf{T}} F}{\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool}}\,validTyping$$

$$\frac{\mathsf{c}{:}A\ \ in\ T}{\Gamma \vdash_{\mathsf{T}} \mathsf{c}{:}A}\,constS \qquad \frac{x{:}A\ \ in\ \Gamma}{\Gamma \vdash_{\mathsf{T}} x{:}A}\,varS$$

$$\frac{\Gamma \vdash_{\mathsf{T}} A\ \mathsf{tp}}{\Gamma \vdash_{\mathsf{T}} A \equiv A}\equiv refl \qquad \frac{\Gamma \vdash_{\mathsf{T}} A \equiv A'}{\Gamma \vdash_{\mathsf{T}} A' \equiv A}\equiv sym \qquad \frac{\Gamma \vdash_{\mathsf{T}} A \equiv A' \quad \Gamma \vdash_{\mathsf{T}} A' \equiv A''}{\Gamma \vdash_{\mathsf{T}} A \equiv A''}\equiv trans$$

$$\frac{\Gamma \vdash_{\mathsf{T}} s =_A t}{\Gamma \vdash_{\mathsf{T}} s{:}A}\,eqTyping \qquad \frac{\Gamma \vdash_{\mathsf{T}} F \Rightarrow G}{\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool}}\,implTypingL \qquad \frac{\Gamma \vdash_{\mathsf{T}} F \Rightarrow G}{\Gamma \vdash_{\mathsf{T}} G{:}\mathsf{bool}}\,implTypingR$$

$$\frac{\Gamma \vdash_{\mathsf{T}} s{:}A \quad \Gamma \vdash_{\mathsf{T}} s{:}A'}{\Gamma \vdash_{\mathsf{T}} A \equiv A'}\,typesUnique \qquad \frac{\Gamma \vdash_{\mathsf{T}} f\ t{:}B \quad \Gamma \vdash_{\mathsf{T}} f{:}A \to B}{\Gamma \vdash_{\mathsf{T}} t{:}A}\,typingWf$$

$$\frac{\Gamma \vdash_{\mathsf{T}} t{:}A \quad \Gamma \vdash_{\mathsf{T}} f\ t{:}B}{\Gamma \vdash_{\mathsf{T}} f{:}A \to B}\,applType \qquad \frac{\Gamma,\ x{:}B \vdash_{\mathsf{T}} s{:}A \quad \Gamma \vdash_{\mathsf{T}} t{:}B}{\Gamma \vdash_{\mathsf{T}} s[{}^{x}/{}_{t}]{:}A}\,rewriteTyping$$

$$\frac{\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool} \quad \Gamma \vdash_{\mathsf{T}} G}{\Gamma,\ \triangleright F \vdash_{\mathsf{T}} G}\,monotonic\vdash \qquad \frac{\Gamma \vdash_{\mathsf{T}} A\ \mathsf{tp} \quad \Gamma \vdash_{\mathsf{T}} J \quad \textit{for any statement} \vdash_{\mathsf{T}} J}{\Gamma,\ x{:}A \vdash_{\mathsf{T}} J}\,var\vdash$$

$$\frac{\Gamma,\ x{:}A \vdash_{\mathsf{T}} F{:}\mathsf{bool}}{\Gamma \vdash_{\mathsf{T}} \forall x{:}A.\ F{:}\mathsf{bool}}\forall type \qquad \frac{\Gamma,\ x{:}A \vdash_{\mathsf{T}} F}{\Gamma \vdash_{\mathsf{T}} \forall x{:}A.\ F}\forall I \qquad \frac{\Gamma \vdash_{\mathsf{T}} \forall x{:}A.\ F \quad \Gamma \vdash_{\mathsf{T}} t{:}A}{\Gamma \vdash_{\mathsf{T}} F[{}^{x}/{}_{t}]}\forall E$$

$$\frac{\Gamma\ \mathsf{Ctx} \quad F\ \ in\ \Gamma}{\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool}}\,assTyping \qquad \frac{\Gamma \vdash_{\mathsf{T}} t =_A t' \quad \Gamma \vdash_{\mathsf{T}} A \equiv A' \quad \Gamma \vdash_{\mathsf{T}} t{:}A'}{\Gamma \vdash_{\mathsf{T}} t'{:}A'}\,cong{:}$$

$$\frac{\Gamma \vdash_{\mathsf{T}} F =_{\mathsf{bool}} \mathsf{true}}{\Gamma \vdash_{\mathsf{T}} F} = \mathsf{true} \qquad \frac{\Gamma \vdash_{\mathsf{T}} F}{\Gamma \vdash_{\mathsf{T}} F =_{\mathsf{bool}} \mathsf{true}}\,\mathsf{true} = \qquad \frac{\Gamma,\ \triangleright F \vdash_{\mathsf{T}} G \quad \Gamma,\ \triangleright G \vdash_{\mathsf{T}} F}{\Gamma \vdash_{\mathsf{T}} F =_{\mathsf{bool}} G}\,propExt$$

$$\frac{\Gamma,\ x{:}A \vdash_{\mathsf{T}} f\ x =_B f'\ x \quad \Gamma \vdash_{\mathsf{T}} f{:}A \to B \quad \Gamma \vdash_{\mathsf{T}} f'{:}A \to B}{\Gamma \vdash_{\mathsf{T}} f =_{A \to B} f'}\,extensionality$$

$$\frac{\Gamma \vdash_T s =_A t \quad \Gamma \vdash_T t =_A u}{\Gamma \vdash_T s =_A u} \mathit{trans} \qquad \frac{\Gamma \vdash_T s =_A s' \quad \Gamma \vdash_T t =_A t'}{\Gamma \vdash_T (s =_A t) =_{\mathsf{bool}} (s' =_A t')} = \mathit{cong}$$

$$\frac{\Gamma \vdash_T A \equiv A' \quad \Gamma,\ x{:}A \vdash_T F =_{\mathsf{bool}} F'}{\Gamma \vdash_T \forall x{:}A.\ F =_{\mathsf{bool}} \forall x{:}A'.\ F'} \forall \mathit{cong} \qquad \frac{\Gamma \vdash_T F =_{\mathsf{bool}} F' \quad \Gamma \vdash_T G =_{\mathsf{bool}} G'}{\Gamma \vdash_T F \Rightarrow G =_{\mathsf{bool}} F' \Rightarrow G'} \Rightarrow \mathit{cong}$$

$$\frac{\Gamma,\ x{:}A \vdash_T F \Rightarrow G}{\Gamma \vdash_T \forall x{:}A.\ F \Rightarrow \forall x{:}A.\ G} \forall\Rightarrow \qquad \frac{\Gamma \vdash_T G \Rightarrow G' \quad \Gamma \vdash_T F' \Rightarrow F}{\Gamma \vdash_T (F \Rightarrow G) \Rightarrow (F' \Rightarrow G')} \Rightarrow \mathit{Funct}$$

$$\frac{\Gamma \vdash_T F =_{\mathsf{bool}} F' \quad \Gamma \vdash_T F}{\Gamma \vdash_T F'} \vdash \mathit{cong} \qquad \frac{\Gamma \vdash_T F[^x/_t] \quad \Gamma \vdash_T t =_A t' \quad \Gamma,\ x{:}A \vdash_T F{:}\mathsf{bool}}{\Gamma \vdash_T F[^x/_{t'}]} \mathit{rewrite}$$

This Lemma 4 is already proven for the version of HOL in the paper[16] that originally introduced DHOL. Definitions for the existential quantifier and the connectives are also given in [16]. Due to it's prominent appearance, we will repeat the definition of $\forall$:

$$\forall x{:}A.\ F := \lambda x{:}A.\ F =_{\Pi x{:}A.\ \mathsf{bool}} \lambda x{:}A.\ \mathsf{true}$$

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

$$\frac{\Gamma \vdash_T F{:}\mathsf{bool} \quad \Gamma \vdash_T G{:}\mathsf{bool}}{\Gamma \vdash_T F \wedge G{:}\mathsf{bool}} \wedge \qquad \frac{\Gamma \vdash_T F =_{\mathsf{bool}} F' \quad \Gamma \vdash_T F =_{\mathsf{bool}} F'}{\Gamma \vdash_T (F \wedge G) =_{\mathsf{bool}} (F' \wedge G')} \wedge\mathrm{Cong}$$

$$\frac{\Gamma \vdash_T F \quad \Gamma \vdash_T G}{\Gamma \vdash_T F \wedge G} \wedge\mathrm{I} \qquad \frac{\Gamma \vdash_T F \wedge G}{\Gamma \vdash_T F} \wedge\mathrm{El} \qquad \frac{\Gamma \vdash_T F \wedge G}{\Gamma \vdash_T G} \wedge\mathrm{Er}$$

and similar rules for the other boolean connectives.

Remark 1 *Observe that many of the rules derived for HOL in Lemma 4 still hold in DHOL. In particular, the rules (ctxThy), (tpCtx), (typingTp) and (validTyping) can be proven by the same method. The rules (monotonic$\vdash$), (var$\vdash$), ($\forall$type), ($\forall$E), ($\forall$I), (assTyping), (= true), (true =), (propExt), (extensionality), ($\forall$cong), ($\forall\Rightarrow$), ($\Rightarrow$Funct), ($\vdash$ cong), (rewrite) and the introduction and elimination rules for the (dependent) conjunction can be derived in DHOL with the same proofs. Also the rules ($\equiv$ refl) and ($\equiv$ sym) can be proven easily in DHOL by induction on the type equality rules.*

A.4 DHOL rules

Theories and contexts:

$$\frac{}{\vdash \circ\ \mathsf{Thy}} \mathrm{thyEmpty} \qquad \frac{\vdash_T x_1{:}A_1,\ \ldots,x_n{:}A_n\ \mathsf{Ctx}}{\vdash T,\ \mathsf{a}{:}\Pi x_1{:}A_1.\ \ldots \Pi x_n{:}A_n.\ \mathsf{tp}\ \mathsf{Thy}} \mathrm{thyType'}$$

$$\frac{\vdash_T A\ \mathsf{tp}}{\vdash T,\ \mathsf{c}{:}A\ \mathsf{Thy}} \mathrm{thyConst} \qquad \frac{\vdash_T F{:}\mathsf{bool}}{\vdash T,\ \triangleright F\ \mathsf{Thy}} \mathrm{thyAxiom}$$

$$\frac{\vdash T\ \mathsf{Thy}}{\vdash_T .\ \mathsf{Ctx}} \mathrm{ctxEmpty} \qquad \frac{\Gamma \vdash_T A\ \mathsf{tp}}{\vdash_T \Gamma,\ x{:}A\ \mathsf{Ctx}} \mathrm{ctxVar} \qquad \frac{\Gamma \vdash_T F{:}\mathsf{bool}}{\vdash_T \Gamma,\ \triangleright F\ \mathsf{Ctx}} \mathrm{ctxAssume}$$

Well-formedness and equality of types:

$$\frac{\begin{array}{c}\mathsf{a}{:}\Pi x_1{:}A_1.\ \ldots \Pi x_n{:}A_n.\ \mathsf{tp}\ \text{in}\ T\\ \Gamma\vdash_{T} t_1{:}A_1\ \ \ldots\ \ \Gamma\vdash_{T} t_n{:}A_n[^{x_1}/_{t_1}]\ldots[^{x_{n-1}}/_{t_{n-1}}]\end{array}}{\Gamma\vdash_{T}\ \mathsf{a}\ t_1\ \ldots\ t_n\ \mathsf{tp}}\text{type'}$$

$$\frac{\Gamma\vdash_{T} p{:}\Pi x{:}A.\ \mathsf{bool}}{\Gamma\vdash_{T} A|_p\ \mathsf{tp}}|_p\,\mathsf{tp}\qquad \frac{\vdash_{T}\Gamma\ \mathsf{Ctx}}{\Gamma\vdash_{T}\mathsf{bool}\ \mathsf{tp}}\text{bool}\qquad \frac{\Gamma\vdash_{T} A\ \mathsf{tp}\quad \Gamma,\ x{:}A\vdash_{T} B\ \mathsf{tp}}{\Gamma\vdash_{T}\Pi x{:}A.\ B\ \mathsf{tp}}\text{pi}$$

$$\frac{\Gamma\vdash_{T} A\ \mathsf{tp}\quad \Gamma\vdash_{T} r{:}\Pi x_1{:}A.\ \Pi x_2{:}A.\ \mathsf{bool}\quad \Gamma\vdash_{T}\mathrm{EqRel}(r)}{\Gamma\vdash_{T} {}^{A}/_{r}\ \mathsf{tp}}\text{Q}$$

Type equality:

$$\frac{\begin{array}{c}\mathsf{a}{:}\Pi x_1{:}A_1.\ \ldots \Pi x_n{:}A_n.\ \mathsf{tp}\ \text{in}\ T\\ \Gamma\vdash_{T} s_1 =_{A_1} t_1\ \ \ldots\ \ \Gamma\vdash_{T} s_n =_{A_n[^{x_1}/_{t_1}]\ldots[^{x_{n-1}}/_{t_{n-1}}]} t_n\end{array}}{\Gamma\vdash_{T}\mathsf{a}\ s_1\ \ldots\ s_n\ \equiv\ \mathsf{a}\ t_1\ \ldots t_n}\text{congBase'}\qquad \frac{\Gamma\vdash A\ \prec:\ B\quad \Gamma\vdash B\ \prec:\ A}{\Gamma\vdash_{T} A\ \equiv\ B}\text{STantisym}$$

$$\frac{\vdash_{T}\Gamma\ \mathsf{Ctx}}{\Gamma\vdash_{T}\mathsf{bool}\ \equiv\ \mathsf{bool}\ \mathsf{tp}}\equiv\ \mathsf{bool}\qquad \frac{\Gamma\vdash_{T} A\ \equiv\ A'\quad \Gamma, x{:}A\vdash_{T} B\ \equiv\ B'}{\Gamma\vdash_{T}\Pi x{:}A.\ B\ \equiv\ \Pi x{:}A'.\ B'}\text{cong}\Pi$$

Typing:

$$\frac{c{:}A'\ \text{in}\ T\quad \Gamma\vdash_{T} A'\ \equiv\ A}{\Gamma\vdash_{T}\mathsf{c}{:}A}\text{const'}\qquad \frac{x{:}A'\ \text{in}\ \Gamma\quad \Gamma\vdash_{T} A'\ \equiv\ A}{\Gamma\vdash_{T} x{:}A}\text{var'}$$

$$\frac{\Gamma,\ x{:}A\vdash_{T} t{:}B\quad \Gamma\vdash_{T} A\ \equiv\ A'}{\Gamma\vdash_{T}(\lambda x{:}A.\ t){:}\Pi x{:}A'.\ B}\text{lambda'}\qquad \frac{\Gamma\vdash_{T} f{:}\Pi x{:}A.\ B\quad \Gamma\vdash_{T} t{:}A}{\Gamma\vdash_{T} f\ t{:}B[^{x}/_{t}]}\text{appl'}$$

$$\frac{\Gamma\vdash_{T} F{:}\mathsf{bool}\quad \Gamma,\ \rhd F\vdash_{T} G{:}\mathsf{bool}}{\Gamma\vdash_{T} F\ \Rightarrow\ G{:}\mathsf{bool}}\Rightarrow\text{type'}\qquad \frac{\Gamma\vdash_{T} s{:}A\quad \Gamma\vdash_{T} t{:}A}{\Gamma\vdash_{T} s =_A t{:}\mathsf{bool}}=\text{type}$$

$$\frac{\Gamma\vdash_{T} t{:}A\quad \Gamma\vdash_{T} p\ t}{\Gamma\vdash_{T} t{:}A|_p}|_p\,\text{I}\qquad \frac{\Gamma\vdash_{T} t{:}A|_p}{\Gamma\vdash_{T} t{:}A}|_p\,\text{E1}\qquad \frac{\Gamma\vdash_{T} t{:}A\quad \Gamma\vdash_{T}\mathrm{EqRel}(r)}{\Gamma\vdash_{T} t{:}{}^{A}/_{r}}\text{QI}$$

$$\frac{\Gamma\vdash_{T} s{:}{}^{A}/_{r}\quad \Gamma,\ x{:}A,\ x =_{A/r} s\vdash_{T} t{:}B\quad \Gamma,\ x{:}A,\ x'{:}A,\ x =_{A/r} s,\ x' =_{A/r} s\vdash_{T} t =_B t[^{x}/_{x'}]}{\Gamma\vdash_{T} t[^{x}/_{s}]{:}B[^{x}/_{s}]}\text{quotE}$$

Term equality; congruence, reflexivity, symmetry, β, η:

$$\frac{\Gamma\vdash_{T} A\ \equiv\ A'\quad \Gamma,\ x{:}A\vdash_{T} t =_B t'}{\Gamma\vdash_{T}\lambda x{:}A.\ t =_{\Pi x:A.\ B}\lambda x{:}A'.\ t'}\text{cong}\lambda\text{'}\qquad \frac{\Gamma\vdash_{T} t =_A t'\quad \Gamma\vdash_{T} f =_{\Pi x:A.\ B} f'}{\Gamma\vdash_{T} f\ t =_B f'\ t'}\text{congAppl'}$$

$$\frac{\Gamma\vdash_{T} t{:}A}{\Gamma\vdash_{T} t =_A t}\text{refl}\qquad \frac{\Gamma\vdash_{T} t =_A s}{\Gamma\vdash_{T} s =_A t}\text{sym}\qquad \frac{\Gamma\vdash_{T}(\lambda x{:}A.\ s)\ t{:}B}{\Gamma\vdash_{T}(\lambda x{:}A.\ s)\ t =_B s[^{x}/_{t}]}\text{beta}\qquad \frac{\Gamma\vdash_{T} t{:}\Pi x{:}A.\ B}{\Gamma\vdash_{T} t =_{\Pi x:A.\ B}\lambda x{:}A.\ t\ x}\text{etaPi}$$

$$\frac{\Gamma\vdash_{T} s =_A t\quad \Gamma\vdash_{T} p\ s}{\Gamma\vdash_{T} s =_{A|_p} t}|_p\,\text{Eq}\qquad \frac{\Gamma\vdash_{T} s{:}A\quad \Gamma\vdash_{T} t{:}A\quad \Gamma\vdash_{T} r{:}A\to A\to\mathsf{bool}\quad \mathrm{EqRel}(r)}{\Gamma\vdash_{T}(s =_{A/r} t) =_{\mathsf{bool}}(r\ s\ t)}\text{Q}=$$

Rules for validity:

$$\frac{\rhd F\ \text{in}\ T\quad \vdash_{T}\Gamma\ \mathsf{Ctx}}{\Gamma\vdash_{T} F}\text{axiom}\qquad \frac{\rhd F\ \text{in}\ \Gamma\quad \vdash_{T}\Gamma\ \mathsf{Ctx}}{\Gamma\vdash_{T} F}\text{assume}$$

$$\frac{\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool} \qquad \Gamma,\ \triangleright F \vdash_{\mathsf{T}} G}{\Gamma \vdash_{\mathsf{T}} F \Rightarrow G} \Rightarrow\mathrm{I} \qquad \frac{\Gamma \vdash_{\mathsf{T}} F \Rightarrow G \qquad \Gamma \vdash_{\mathsf{T}} F}{\Gamma \vdash_{\mathsf{T}} G} \Rightarrow\mathrm{E}$$

$$\frac{\Gamma \vdash_{\mathsf{T}} F =_{\mathsf{bool}} F' \qquad \Gamma \vdash_{\mathsf{T}} F'}{\Gamma \vdash_{\mathsf{T}} F} \mathrm{cong}\vdash \qquad \frac{\Gamma \vdash_{\mathsf{T}} p\ \mathsf{true} \qquad \Gamma \vdash_{\mathsf{T}} p\ \mathsf{false}}{\Gamma, x{:}\mathsf{bool} \vdash_{\mathsf{T}} p\ x} \mathrm{boolExt}$$

$$\frac{\Gamma \vdash_{\mathsf{T}} t{:}A|_p}{\Gamma \vdash_{\mathsf{T}} p\ t} |_p\,\mathrm{E2}$$

We also have the axiom from Definition 2.

Finally, we modify the rule (nonempty) 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). Observe that either restricting to the fragment HOL of DHOL or translating to it then yields the non-emptyness assumptions for HOL types.

B The translation from DHOL into HOL

Before actually going into the soundness and completeness proofs, we repeat and enumerate the cases in the definition of the translation, so we can reference them in the following.

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

We use the notation $\overrightarrow{x{:}A}$, $\overrightarrow{\Pi x{:}A.}$, $\overrightarrow{A}$ *and* $\overrightarrow{x}$ *to denote* $x{:}A_1, \ldots, x_n{:}A_n$, $\Pi x_1{:}A_1.\ \ldots \Pi x_n{:}A_n.$, $A_1 \to \ldots \to A_n$ *and* $x_1\ \ldots\ x_n$ *respectively.*

The cases for theories and contexts are:

$$\overline{\circ} := \circ \tag{PT1}$$

$$\overline{T,\ D} := \overline{T},\ \overline{D} \qquad \textit{where}$$

$$\begin{aligned}\overline{\mathsf{a}{:}\overrightarrow{\Pi x{:}A.}\ \mathsf{tp}} := \mathsf{a}{:}\mathsf{tp},\ & \\ & a^*{:}\overrightarrow{\overline{A}} \to \mathsf{a} \to \mathsf{a} \to \mathsf{bool}, \\ & \triangleright\forall \overrightarrow{x{:}\overline{A}}.\ \forall u, v, w{:}\mathsf{a}.\ (\mathsf{a}\ \overrightarrow{x})^*\ u\ v \Rightarrow \big((\mathsf{a}\ \overrightarrow{x})^*\ v\ w \Rightarrow (\mathsf{a}\ \overrightarrow{x})^*\ u\ w\big), \\ & \triangleright\forall \overrightarrow{x{:}\overline{A}}.\ \forall u, v{:}\mathsf{a}.\ (\mathsf{a}\ \overrightarrow{x})^*\ u\ v \Rightarrow (\mathsf{a}\ \overrightarrow{x})^*\ v\ u, \\ & \triangleright\forall \overrightarrow{x{:}\overline{A}}.\ \forall u, v{:}\mathsf{a}.\ (\mathsf{a}\ \overrightarrow{x})^*\ v\ v \Rightarrow (\mathsf{a}\ \overrightarrow{x})^*\ u\ v =_{\mathsf{bool}} u =_{\mathsf{a}} v\end{aligned} \tag{PT2}$$

$$\overline{\mathsf{c}{:}A} := \mathsf{c} : \overline{A}, \quad \triangleright A^*\ \mathsf{c}\ \mathsf{c} \tag{PT3}$$

$$\overline{\triangleright F} := \triangleright\overline{F} \tag{PT4}$$

$$\overline{.} := . \tag{PT5}$$

$$\overline{\Gamma, x{:}A} := \overline{\Gamma},\ x{:}\overline{A}, \triangleright A^*\ x\ x \tag{PT6}$$

$$\overline{\Gamma, \triangleright F} := \overline{\Gamma},\ \triangleright\overline{F} \tag{PT7}$$

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

$$\overline{(\mathsf{a}\ t_1\ \ldots\ t_n)} := \mathsf{a} \tag{PT8}$$
$$(\mathsf{a}\ t_1\ \ldots\ t_n)^*\ s\ t := a^*\ \overline{t_1}\ \ldots\ \overline{t_n}\ s\ t \tag{PT9}$$
$$\overline{\Pi x{:}A.\ B} := \overline{A} \to \overline{B} \tag{PT10}$$
$$(\Pi x{:}A.\ B)^*\ f\ g := \forall x, y{:}\overline{A}.\ A^*\ x\ y \Rightarrow B^*\ (f\ x)\ (g\ y) \tag{PT11}$$
$$\overline{\mathsf{bool}} := \mathsf{bool} \tag{PT12}$$
$$\mathsf{bool}^*\ s\ t := s =_{\mathsf{bool}} t \tag{PT13}$$

$$\overline{A|_p} := \overline{A} \tag{PT14}$$
$$(A|_p)^*\ s\ t := A^*\ s\ t \wedge \overline{p}\ s \wedge \overline{p}\ t \tag{PT15}$$
$$\overline{A/r} := \overline{A} \tag{PT16}$$
$$(A/r)^*\ s\ t := \overline{r}\ s\ t \wedge A^*\ s\ s \wedge A^*\ t\ t \tag{PT17}$$

The cases for terms are:

$$\overline{\mathsf{c}} := \mathsf{c} \tag{PT18}$$
$$\overline{x} := x \tag{PT19}$$
$$\overline{\lambda x{:}A.\ t} := \lambda x{:}\overline{A}.\ \overline{t} \tag{PT20}$$
$$\overline{f\ t} := \overline{f}\ \overline{t} \tag{PT21}$$
$$\overline{F \Rightarrow G} := \overline{F} \Rightarrow \overline{G} \tag{PT22}$$
$$\overline{s =_A t} := A^*\ \overline{s}\ \overline{t} \tag{PT23}$$

C Completeness proof

To simplify the inductive arguments, we will actually prove the following slightly stronger version of the theorem:

Theorem 10 (Completeness). *We have*

$$\vdash T\ \mathsf{Thy} \quad \textit{implies} \quad \vdash\ \overline{T}\ \mathsf{Thy} \tag{1}$$
$$\vdash_T \Gamma\ \mathsf{Ctx} \quad \textit{implies} \quad \vdash_{\overline{T}} \overline{\Gamma}\ \mathsf{Ctx} \tag{2}$$
$$\Gamma \vdash_T A\ \mathsf{tp} \quad \textit{implies}\ \overline{\Gamma} \vdash_{\overline{T}} \overline{A}\ \mathsf{tp} \quad \textit{and}\ \ \overline{\Gamma} \vdash_{\overline{T}} A^*{:}\overline{A} \to \overline{A} \to \mathsf{bool} \tag{3}$$
$$\Gamma \vdash_T A \equiv B \quad \textit{implies}\ \overline{\Gamma} \vdash_{\overline{T}} \overline{A} \equiv \overline{B} \quad \textit{and}\ \ \overline{\Gamma},\ x{:}\overline{A} \vdash_{\overline{T}} A^*\ x\ x =_{\mathsf{bool}} B^*\ x\ x \tag{4}$$
$$\Gamma \vdash_T t{:}A \quad \textit{implies}\ \overline{\Gamma} \vdash_{\overline{T}} \overline{t}{:}\overline{A} \quad \textit{and}\ \ \overline{\Gamma} \vdash_{\overline{T}} A^*\ \overline{t}\ \overline{t} \tag{5}$$

$$\Gamma \vdash_{\mathsf{T}} A \prec: B \quad \textit{implies } \overline{\Gamma} \vdash_{\overline{T}} \overline{A} \equiv \overline{B} \quad \textit{and } \overline{\Gamma},\ x, y{:}\overline{B} \vdash_{\overline{T}} A^*\ x\ y \Rightarrow B^*\ x\ y \tag{6}$$

$$\Gamma \vdash_{\mathsf{T}} F \qquad \textit{implies } \overline{\Gamma} \vdash_{\overline{T}} \overline{F} \tag{7}$$

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

$$\Gamma \vdash_{\mathsf{T}} t =_A t' \quad \textit{implies } \overline{\Gamma} \vdash_{\overline{T}} A^*\ \overline{t}\ \overline{t'} \quad \textit{and } \overline{\Gamma} \vdash_{\overline{T}} \overline{t}{:}\overline{A} \quad \textit{and } \overline{\Gamma} \vdash_{\overline{T}} \overline{t'}{:}\overline{A} \tag{8}$$

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

$$\Gamma \vdash_{\mathsf{T}} A\ \mathtt{tp} \quad \textit{implies} \quad \overline{\Gamma} \vdash_{\overline{T}} \forall x, y{:}\overline{A}.\ A^*\ x\ y \Rightarrow A^*\ y\ x \tag{9}$$

$$\Gamma \vdash_{\mathsf{T}} A\ \mathtt{tp} \quad \textit{implies} \quad \overline{\Gamma} \vdash_{\overline{T}} \forall x, y, z{:}\overline{A}.\ A^*\ x\ y \Rightarrow (A^*\ y\ z \Rightarrow A^*\ x\ z) \tag{10}$$

Moreover, the following substitution lemma holds, i.e.,

$$\Gamma,\ x{:}A \vdash_{\mathsf{T}} t{:}B \textit{ and } \Gamma \vdash u{:}A \quad \textit{implies} \quad \overline{\Gamma} \vdash_{\overline{T}} \overline{t[x/u]} =_{\overline{B}} \overline{t}[x/\overline{u}] \tag{11}$$

$$\Gamma,\ x{:}A \vdash_{\mathsf{T}} B\ \mathtt{tp} \textit{ and } \Gamma \vdash_{\mathsf{T}} u{:}B \quad \textit{implies} \quad \overline{\Gamma} \vdash_{\overline{T}} \overline{B[x/u]} \equiv \overline{B}[x/\overline{u}] \tag{12}$$

In the following line, we assume that if $t = \lambda y{:}C.\ s$ for s of type D, then $B = \Pi y{:}C.\ D$ (this is enough in practice and we cannot easily show more). In the presence of nontrivial subtyping we need this assumption that types "fit together exactly" to prove this part of the substitution lemma.

$$\Gamma,\ x{:}A \vdash_{\mathsf{T}} t{:}B \quad \textit{implies} \quad \overline{\Gamma},\ x, x'{:}\overline{A},\ \triangleright A^*\ x\ x' \vdash_{\overline{T}} B^*\ \overline{t}\ \overline{t}[x/x'] \tag{13}$$

Here Case 4 looks weaker than in the original statement, but is easily seen to be equivalent. The equivalence proof uses induction on the shape of the types (reducing the claim to base types), propositional extensionality and the PER axioms.

Proof (Proof of Theorem 10). 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 (=type), we also require the fact that for any (well-formed) type A in DHOL we have $A^*{:}\overline{A} \to \overline{A} \to \mathsf{bool}$. This follows directly from how the A^* are generated/defined in the translation.

C.1 Substitution lemma and symmetry and transitivity of the typing relations

Since the translation of types commutes with the type productions of the grammar (12) is obvious.

We show (11) by induction on the grammar of DHOL. If x is not a free variable in t, then $\overline{t[x/u]} = \overline{t} = \overline{t}[x/\overline{u}]$ and the claim (11) follows by rule (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) we have $t = x$ and thus $\overline{t[x/u]} = \overline{u} = \overline{t}[x/\overline{u}]$ so the claim follows by rule (refl).

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

If t is a function application $f\ s$, the induction hypothesis yields $\overline{\Gamma} \vdash_{\overline{T}} \overline{s[x/u]} =_{\overline{A}} \overline{s}[x/\overline{u}]$ and $\overline{\Gamma} \vdash_{\overline{T}} \overline{f[x/u]} =_{\overline{A} \to \overline{B}} \overline{f}[x/\overline{u}]$, where A is the type of s. From rule (congAppl), the claim of $\overline{\Gamma} \vdash_{\overline{T}} \overline{(f\ s)\,[x/u]} =_{\overline{B}} \overline{f\ s}[x/\overline{u}]$ follows.

If t is an equality $s =_A s'$, the induction hypothesis yields $\overline{\Gamma} \vdash_{\overline{T}} \overline{s[x/u]} =_{\overline{A}} \overline{s}[x/\overline{u}]$ and $\overline{\Gamma} \vdash_{\overline{T}} \overline{s'[x/u]} =_{\overline{A}} \overline{s'}[x/\overline{u}]$, where A is the type of s and s'. The claim of $\overline{\Gamma} \vdash_{\overline{T}} \overline{(s =_A s')\,[x/u]} =_{\mathsf{bool}} \overline{(s =_A s')}\,[x/\overline{u}]$ follows using rule ($=$cong).

Before we can show (13), we first need to prove the symmetry and transitivity of the typing relations: We can prove both by induction on the type A. The base cases are base types and equality, for which the claims follow by construction. [1] EdN:1

We show (13) by induction on the grammar: Without loss of generality we may assume that $B =: B'|_p$ for B' either a quotient–, a base– or a Π-type. This is due to the fact that quotinet–, base– and Π-types B' can be written as $B'|_{\lambda x:B'.\ \mathsf{true}}$ and types of the form $B''|_p|_q$ can be rewritten as $B''|_{\lambda x:B''.\ p\ x \wedge q\ x}$.

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

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

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

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

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

[1] EdNote: CR@FR: This proof is straightforward, but very tedious and practically unmaintainable. So I commented out the details here.

Since t is a λ-term, by assumption we have that $B \equiv B' = B|_{\lambda z:B.\ \mathsf{true}}$, 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 $B = D \equiv B' = B|_{\lambda z:B.\ \mathsf{true}}$, so it suffices to prove that

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

By induction hypothesis and (11) we then have:

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

and

$$\overline{\Gamma},\ x, x'{:}\overline{A},\ \triangleright A^*\ x\ x' \vdash_{\overline{T}} C^*\ \overline{s}\ \overline{s}[x/x']. \tag{14}$$

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

$$\overline{\Gamma},\ x, x'{:}\overline{A},\ \triangleright A^*\ x\ x' \vdash_{\overline{T}} \forall z, z'{:}\overline{C}.\ C^*\ z\ z' \Rightarrow (\Pi z{:}C.\ D)^*\ \overline{f}\ z\ \overline{f}[x/x']\ z'[x/x'] \tag{15}$$

Using the rules ($\forall$E) and ($\Rightarrow$E) (using (15)) to plug in $\overline{s}$ resp. $\overline{s}[x/x']$ for z, z' in (15), we yield:

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

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 (11), which is already proven above. It remains to consider the case of t being an equality $s =_C s'$ for $C \not\equiv \mathsf{bool}$. In this case, the induction hypothesis implies that

$$\overline{\Gamma},\ x, x'{:}\overline{A},\ \triangleright A^*\ x\ x' \vdash_{\overline{T}} C^*\ \overline{s}\ \overline{s}[x/x'] \tag{16}$$

and

$$\overline{\Gamma},\ x, x'{:}\overline{A},\ \triangleright A^*\ x\ x' \vdash_{\overline{T}} C^*\ \overline{s'}\ \overline{s'}[x/x'] \tag{17}$$

We need to prove

$$\overline{\Gamma},\ x, x'{:}\overline{A},\ \triangleright A^*\ x\ x' \vdash_{\overline{T}} C^*\ \overline{s}\ \overline{s'} =_{\mathsf{bool}} C^*\ \overline{s}[x/x']\ \overline{s'}[x/x'].$$

If we can show

$$\overline{\Gamma},\ x, x'{:}\overline{A},\ \triangleright A^*\ x\ x',\ \triangleright C^*\ \overline{s}\ \overline{s'} \vdash_{\overline{T}} C^*\ \overline{s}[x/x']\ \overline{s'}[x/x']$$

and similarly also

$$\overline{\Gamma},\ x, x'{:}\overline{A},\ \triangleright A^*\ x\ x',\ \triangleright C^*\ \overline{s}[x/x']\ \overline{s'}[x/x'] \vdash_{\overline{T}} C^*\ \overline{s}\ \overline{s'},$$

then the claim follows by rule (propExt).

Both follows from the transitivity (10) of the typing relation C^*.

C.2 Proof of remaining soundness theorem by induction on DHOL derivations

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

(thyEmpty):

$\vdash \circ\ \mathsf{Thy}$	(thyEmpty)	(18)
$\vdash^{\mathsf{H}} \overline{\circ}\ \mathsf{Thy}$	(thyEmpty)	

(thyType'):

$\vdash_{\mathsf{T}} x_1{:}A_1, \ldots, x_n{:}A_n\ \mathsf{Ctx}$	by assumption	(19)
$\vdash_{\overline{T}} x_1{:}\overline{A_1}, {A_1}^*\ x_1\ x_1, \ldots, x_n{:}\overline{A_n}, \rhd {A_n}^*\ x_n\ x_n\ \mathsf{Ctx}$	Induction hypothesis,(19)	(20)
$\vdash^{\mathsf{H}} \overline{T}\ \mathsf{Thy}$	(ctxThy),(20)	(21)
$\vdash^{\mathsf{H}} \overline{T},\ \mathsf{a}{:}\mathsf{tp}\ \mathsf{Thy}$	(thyType),(21)	(22)
$\vdash^{\mathsf{H}} \overline{T,\ \mathsf{a}{:}\Pi x_1{:}A_1.\ \ldots \Pi x_n{:}A_n.\ \mathsf{tp}}\ \mathsf{Thy}$	PT2,(22)	

(thyConst):

$\vdash_{\mathsf{T}} A\ \mathsf{tp}$	by assumption	(23)
$\vdash_{\overline{T}} \overline{A}\ \mathsf{tp}$	Induction hypothesis,(23)	(24)
$\vdash^{\mathsf{H}} \overline{T},\ \mathsf{c}{:}\overline{A}\ \mathsf{Thy}$	(thyConst),(24)	(25)
$\vdash^{\mathsf{H}} \overline{T,\ c{:}A}\ \mathsf{Thy}$	PT3,(25)	(26)

(thyAxiom):

$\vdash_{\mathsf{T}} F{:}\mathsf{bool}$	by assumption	(27)
$\vdash_{\overline{T}} \overline{F}{:}\mathsf{bool}$	Induction hypothesis,(27)	(28)
$\vdash^{\mathsf{H}} \overline{T},\ \rhd\overline{F}\ \mathsf{Thy}$	(thyAxiom),(28)	(29)
$\vdash^{\mathsf{H}} \overline{\overline{T},\ \rhd F}\ \mathsf{Thy}$	PT4,(29)	(30)

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

(ctxEmpty):

$\vdash T\ \mathsf{Thy}$	by assumption	(31)
$\vdash^{\mathsf{H}} \overline{T}\ \mathsf{Thy}$	Induction hypothesis,(31)	(32)
$\vdash_{\overline{T}} .\ \mathsf{Ctx}$	(ctxEmpty),(32)	(33)
$\vdash_{\overline{T}} \overline{.}\ \mathsf{Ctx}$	PT5,(33)	(34)

(ctxVar):

$$\Gamma \vdash_{\mathsf{T}} A \ \mathsf{tp} \quad \text{By Assumption} \quad (35)$$
$$\overline{\Gamma} \vdash_{\overline{T}} \overline{A} \ \mathsf{tp} \quad \text{Induction hypothesis,(35)} \quad (36)$$
$$\overline{\Gamma} \vdash_{\overline{T}} A^*{:}\overline{A} \to \overline{A} \to \mathsf{bool} \quad \text{Induction hypothesis,(35)} \quad (37)$$
$$\vdash_{\overline{T}} \overline{\Gamma},\ x{:}\overline{A} \ \mathsf{Ctx} \quad \text{(ctxVar),(36)} \quad (38)$$
$$\overline{\Gamma},\ x{:}\overline{A} \vdash_{\overline{T}} A^*{:}\overline{A} \to \overline{A} \to \mathsf{bool} \quad \text{(var}\vdash\text{),(36),(37)} \quad (39)$$
$$\overline{\Gamma},\ x{:}\overline{A} \vdash_{\overline{T}} A^*\ x\ x{:}\mathsf{bool} \quad \text{(appl),(39),(varS)} \quad (40)$$
$$\vdash_{\overline{T}} \overline{\Gamma},\ x{:}\overline{A},\ A^*\ x\ x \ \mathsf{Ctx} \quad \text{(ctxAssume),(40)} \quad (41)$$
$$\vdash_{\overline{T}} \overline{\Gamma,\ x{:}A} \ \mathsf{Ctx} \quad \text{PT6,(41)} \quad (42)$$

(ctxAssume):

$$\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool} \quad \text{by assumption} \quad (43)$$
$$\overline{\Gamma} \vdash_{\overline{T}} \overline{F}{:}\mathsf{bool} \quad \text{Induction hypothesis,(43)} \quad (44)$$
$$\vdash_{\overline{T}} \overline{\Gamma},\ \rhd\overline{F} \ \mathsf{Ctx} \quad \text{(ctxAssume),(44)} \quad (45)$$
$$\vdash_{\overline{T}} \overline{\Gamma,\ \rhd F} \ \mathsf{Ctx} \quad \text{PT7,(45)} \quad (46)$$

Well-formedness of types Well-formedness of types can be shown in DHOL using the rules (type'), (bool), (pi), (Q) and ($|_p$ tp):

(type'):

$$\mathsf{a}{:}\Pi x_1{:}A_1.\ \dots \Pi x_n{:}A_n.\ \mathsf{tp} \text{ in } T \quad \text{By Assumption} \quad (47)$$
$$\Gamma \vdash_{\mathsf{T}} t_1{:}A_1 \quad \text{By Assumption} \quad (48)$$
$$\vdots$$
$$\Gamma \vdash_{\mathsf{T}} t_n{:}A_n[{}^{x_1}/_{t_1}] \dots [{}^{x_n}/_{t_n}] \quad \text{By Assumption} \quad (49)$$
$$\overline{\Gamma} \vdash_{\overline{T}} \overline{t_1}{:}\overline{A_1} \quad \text{Induction hypothesis,(48)} \quad (50)$$
$$\vdots$$
$$\overline{\Gamma} \vdash_{\overline{T}} \overline{t_n}{:}\overline{A_n} \quad \text{Induction hypothesis,(49)} \quad (51)$$
$$\mathsf{a}{:}\mathsf{tp} \text{ in } \overline{T} \quad \text{PT2,(47)} \quad (52)$$
$$a^*{:}\overline{A_1} \to \dots \overline{A_n} \to \mathsf{a} \to \mathsf{a} \to \mathsf{bool} \text{ in } \overline{T} \quad \text{PT2,(47)} \quad (53)$$
$$\overline{\Gamma} \vdash_{\overline{T}} a^*{:}\overline{A_1} \to \dots \overline{A_n} \to \mathsf{a} \to \mathsf{a} \to \mathsf{bool} \quad \text{(constS),(53)} \quad (54)$$
$$\overline{\Gamma} \vdash_{\overline{T}} a^*\ \overline{t_1}{:}\overline{A_2} \to \dots \overline{A_n} \to \mathsf{a} \to \mathsf{a} \to \mathsf{bool} \quad \text{(appl),(54),(50)} \quad (55)$$
$$\vdots$$
$$\overline{\Gamma} \vdash_{\overline{T}} a^*\ \overline{t_1}\ \dots\ \overline{t_n}{:}\mathsf{a} \to \mathsf{a} \to \mathsf{bool} \quad \text{(appl),previous line,(51)} \quad (56)$$

$$\vdash_{\overline{T}} \overline{\Gamma}\ \mathsf{Ctx} \qquad \text{(tpCtx),(typingTp),(54)} \qquad (57)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \mathsf{a}\ \mathsf{tp} \qquad \text{(type),(52),(57)}$$

$$\overline{\Gamma} \vdash_{\overline{T}} (\mathsf{a}\ t_1\ \ldots\ t_n)^*{:}\overline{\mathsf{a}} \to \overline{\mathsf{a}} \to \mathsf{bool} \qquad \text{PT21,(56)}$$

(bool):

$$\vdash_{T} \Gamma\ \mathsf{Ctx} \qquad \text{By Assumption} \qquad (58)$$

$$\vdash_{\overline{T}} \overline{\Gamma}\ \mathsf{Ctx} \qquad \text{Induction hypothesis,(58)} \qquad (59)$$

$$\vdash_{\overline{T}} \mathsf{bool}\ \mathsf{tp} \qquad \text{(bool),(59)} \qquad (60)$$

$$\vdash_{\overline{T}} \overline{\mathsf{bool}}\ \mathsf{tp} \qquad \text{PT12,(60)}$$

bool^* is just a notation of $=_{\mathsf{bool}}$ which is of type $\mathsf{bool} \to \mathsf{bool} \to \mathsf{bool}$ in HOL, as desired.

(pi):

$$\Gamma \vdash_{T} A\ \mathsf{tp} \qquad \text{By Assumption} \qquad (61)$$

$$\Gamma,\ x{:}A \vdash_{T} B\ \mathsf{tp} \qquad \text{By Assumption} \qquad (62)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{A}\ \mathsf{tp} \qquad \text{Induction hypothesis,(61)} \qquad (63)$$

$$\overline{\Gamma},\ x{:}\overline{A},\ \triangleright A^*\ x\ x \vdash_{\overline{T}} \overline{B}\ \mathsf{tp} \qquad \text{Induction hypothesis,(62)} \qquad (64)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{B}\ \mathsf{tp} \qquad \text{HOL types context independent,(64)} \qquad (65)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{A} \to \overline{B}\ \mathsf{tp} \qquad \text{(arrow),(63),(65)} \qquad (66)$$

$$\overline{\Gamma} \vdash_{\overline{T}} A^*{:}\overline{A} \to \overline{A} \to \mathsf{bool} \qquad \text{Induction hypothesis,(61)} \qquad (67)$$

$$\overline{\Gamma} \vdash_{\overline{T}} B^*{:}\overline{B} \to \overline{B} \to \mathsf{bool} \qquad \text{Induction hypothesis,(62)} \qquad (68)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{\Pi x{:}A.\ B}\ \mathsf{tp} \qquad \text{PT10,(66)}$$

$$\overline{\Gamma} \vdash_{\overline{T}} (\Pi x{:}A.\ B)^*{:}(\overline{\Pi x{:}A.\ B}) \to (\overline{\Pi x{:}A.\ B}) \to \mathsf{bool} \qquad \text{PT11,(67),(68)}$$

(Q):

$$\Gamma \vdash_{T} A\ \mathsf{tp} \qquad \text{By Assumption} \qquad (69)$$

$$\Gamma \vdash_{T} r{:}\Pi x_1{:}A.\ \Pi x_2{:}A.\ \mathsf{bool} \qquad \text{By Assumption} \qquad (70)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{A}\ \mathsf{tp} \qquad \text{Induction hypothesis,(69)} \qquad (71)$$

$$\overline{\Gamma} \vdash_{\overline{T}} A^*{:}\overline{A} \to \overline{A} \to \mathsf{bool} \qquad \text{Induction hypothesis,(69)} \qquad (72)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{r}{:}\overline{A} \to \overline{A} \to \mathsf{bool} \qquad \text{Induction hypothesis,(70)} \qquad (73)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{A/r}\ \mathsf{tp} \qquad \text{PT16,(71)}$$

$$\overline{\Gamma},\ x,y{:}\overline{A} \vdash_{\overline{T}} A^*\ x\ x{:}\mathsf{bool} \qquad \text{(appl),(appl),(72),(var),(var)} \qquad (74)$$

$$\overline{\Gamma},\ x,y{:}\overline{A} \vdash_{\overline{T}} A^*\ y\ y{:}\mathsf{bool} \qquad \text{(appl),(appl),(72),(var),(var)} \qquad (75)$$

$$\overline{\Gamma},\ x,y{:}\overline{A} \vdash_{\overline{T}} \overline{r}\ x\ x{:}\mathsf{bool} \qquad \text{(appl),(appl),(73),(var),(var)} \qquad (76)$$

$$\overline{\Gamma},\ x,y{:}\overline{A} \vdash_{\overline{T}} \overline{r}\ x\ y \wedge A^*\ x\ x \wedge A^*\ y\ y{:}\mathsf{bool} \qquad (\wedge)\text{,(76)},(\wedge)\text{,(74),(75)} \qquad (77)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \lambda x, y{:}\overline{A}.\ \overline{r}\ x\ y \wedge A^*\ x\ x \wedge A^*\ y\ y{:}\overline{A} \to \overline{A} \to \mathsf{bool}$$
(lambda),(lambda),(77) (78)

$$\overline{\Gamma} \vdash_{\overline{T}} ({}^{A}\!/\!{}_{r})^*{:}\overline{({}^{A}\!/\!{}_{r})} \to \overline{({}^{A}\!/\!{}_{r})} \to \mathsf{bool}$$ PT16,PT17,(78)

($|_p$ tp):

$\Gamma \vdash_T p{:}\Pi x{:}A.\ \mathsf{bool}$	By Assumption	(79)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{p}{:}\overline{A} \to \mathsf{bool}$	Induction hypothesis,(79)	(80)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{A} \to \mathsf{bool}\ \mathsf{tp}$	(typingTp),(80)	(81)

Since statements of shape $\vdash B \to C$ tp only provable using rule (arrow):

$\overline{\Gamma} \vdash_{\overline{T}} \overline{A}\ \mathsf{tp}$	see above,(81)	(82)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{A\|_p}\ \mathsf{tp}$	PT14,(82)	
$\overline{\Gamma} \vdash_{\overline{T}} \forall x, y{:}\overline{A}.\ A^*\ x\ y \Rightarrow \overline{p}\ x =_{\mathsf{bool}} \overline{p}\ y$	Induction hypothesis,PT11,(79)	(83)
$\overline{\Gamma},\ x, y{:}\overline{A} \vdash_{\overline{T}} A^*\ x\ y \Rightarrow \overline{p}\ x =_{\mathsf{bool}} \overline{p}\ y$	(monotonic$\vdash$),($\forall$E),(monotonic$\vdash$), ($\forall$E),(monotonic$\vdash$),(83),(var),(var)	(84)
$\overline{\Gamma},\ x, y{:}\overline{A} \vdash_{\overline{T}} A^*\ x\ y{:}\mathsf{bool}$	(implTypingL),(84)	(85)
$\overline{\Gamma},\ x, y{:}\overline{A} \vdash_{\overline{T}} A^*{:}\overline{A} \to \overline{A} \to \mathsf{bool}$	(applType),(var),(applType),(var),(85)	(86)

Since x, y don't occur in A^* and HOL types are context independent:

$\overline{\Gamma} \vdash_{\overline{T}} A^*{:}\overline{A} \to \overline{A} \to \mathsf{bool}$	see above,(86)	(87)
$\overline{\Gamma} \vdash_{\overline{T}} (A\|_p)^*{:}\overline{A} \to \overline{A} \to \mathsf{bool}$	PT15,(87)	

Type-equality Type-equality can be shown using the rules (congBase'),(STantisym), (congΠ) and ($\equiv$ bool): Observe that by the rules (var$\vdash$), (congAppl), (var), instead of proving $\overline{\Gamma},\ x, y{:}\overline{A} \vdash_{\overline{T}} A^*\ x\ y =_{\mathsf{bool}} A^*\ x\ y$ we may simply prove $\overline{\Gamma} \vdash_{\overline{T}} A^* =_{\overline{A} \to \overline{A} \to \mathsf{bool}} A'^*\ x\ y$.

(congBase'):

$\mathsf{a}{:}\Pi x_1{:}A_1.\ \ldots \Pi x_n{:}A_n.\ \mathsf{tp}$ in T	by assumption	(88)
$\Gamma \vdash_T s_1 =_{A_1} t_1$	by assumption	(89)
$\vdots$		
$\Gamma \vdash_T s_n =_{A_n[x_1/t_1]\ldots[x_{n-1}/t_{n-1}]} t_n$	By Assumption	(90)
$\mathsf{a}{:}\mathsf{tp}$ in $\overline{T}$	PT2,(88)	(91)
$a^*{:}\overline{A_1} \to \ldots \to \overline{A_n} \to \overline{\mathsf{a}} \to \overline{\mathsf{a}} \to \mathsf{bool}$ in $\overline{T}$	PT2,(88)	(92)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{s_1} =_{\overline{A_1}} \overline{t_1}$	Induction hypothesis,(89)	(93)
$\vdots$		

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{s_n} =_{\overline{A_n}} \overline{t_n} \quad \text{Induction hypothesis,(90)} \tag{94}$$

$$\vdash_{\overline{T}} \overline{\Gamma}\ \mathsf{Ctx} \quad \text{(tpCtx),(typingTp),(eqTyping),(93)} \tag{95}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \mathtt{a} \equiv \mathtt{a} \quad \text{(congBase),(95),(91)} \tag{96}$$

$$\overline{\Gamma} \vdash_{\overline{T}} a^* =_{\overline{A_1} \to \ldots \to \overline{A_n} \to \bar{\mathtt{a}} \to \bar{\mathtt{a}} \to \mathsf{bool}} a^* \quad \text{(refl),(constS),(92),(95)} \tag{97}$$

$$\overline{\Gamma} \vdash_{\overline{T}} a^*\ \overline{s_1} =_{\overline{A_2} \to \ldots \to \overline{A_n} \to \bar{\mathtt{a}} \to \bar{\mathtt{a}} \to \mathsf{bool}} a^*\ \overline{t_1} \quad \text{(congAppl),(93),(97)} \tag{98}$$

$$\vdots$$

$$\overline{\Gamma} \vdash_{\overline{T}} a^*\ \overline{s_1}\ \ldots\ \overline{s_n} =_{\bar{\mathtt{a}} \to \bar{\mathtt{a}} \to \mathsf{bool}} a^*\ \overline{t_1}\ \ldots\ \overline{t_n} \quad \text{(congAppl),(94),previous line} \tag{99}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{\mathtt{a}\ s_1\ \ldots\ s_n} \equiv \overline{\mathtt{a}\ t_1\ \ldots\ t_n} \quad \text{PT8,(96)}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \vdash_{\overline{T}} (\mathtt{a}\ s_1\ \ldots\ s_n)^* =_{\bar{\mathtt{a}} \to \bar{\mathtt{a}} \to \mathsf{bool}} (\mathtt{a}\ t_1\ \ldots\ t_n)^* \quad \text{PT9,(99)}$$

(STantisym):

$$\Gamma \vdash_T A \prec: A' \quad \text{By Assumption} \tag{100}$$

$$\Gamma \vdash_T A' \prec: A \quad \text{By Assumption} \tag{101}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{A} \equiv \overline{A'} \quad \text{Induction hypothesis,(100)} \tag{102}$$

$$\overline{\Gamma},\ x, y{:}\overline{A} \vdash_{\overline{T}} A^*\ x\ y \Rightarrow A'^*\ x\ y \quad \text{Induction hypothesis,(100)} \tag{103}$$

$$\overline{\Gamma},\ x{:}\overline{A} \vdash_{\overline{T}} A^*\ x\ x \Rightarrow A'^*\ x\ x \quad (\forall E),(\forall I),(103),(\text{var}) \tag{104}$$

$$\overline{\Gamma},\ x, y{:}\overline{A'} \vdash_{\overline{T}} A'^*\ x\ y \Rightarrow A^*\ x\ y \quad \text{Induction hypothesis,(101)} \tag{105}$$

$$\overline{\Gamma},\ x{:}\overline{A'} \vdash_{\overline{T}} A'^*\ x\ x \Rightarrow A^*\ x\ x \quad (\forall E),(\forall I),(105),(\text{var}) \tag{106}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \forall x{:}\overline{A}.\ A'^*\ x\ x \Rightarrow A^*\ x\ x \quad (\text{cong}\vdash),(\forall\text{cong}),(\equiv\text{trans}),(102),(\text{refl}),(\forall I),(106) \tag{107}$$

$$\overline{\Gamma},\ x{:}\overline{A} \vdash_{\overline{T}} A'^*\ x\ x \Rightarrow A^*\ x\ x \quad (\forall E),(\text{var}\vdash),(107),(\text{var}) \tag{108}$$

$$\overline{\Gamma},\ x{:}\overline{A} \vdash_{\overline{T}} A^*\ x\ x =_{\mathsf{bool}} A'^*\ x\ x \quad \text{(propExt),(104),(108)}$$

(congΠ):

$$\Gamma \vdash_T A \equiv A' \quad \text{By Assumption} \tag{109}$$

$$\Gamma,\ x{:}A \vdash_T B \equiv B' \quad \text{By Assumption} \tag{110}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{A} \equiv \overline{A'} \quad \text{Induction hypothesis,(109)} \tag{111}$$

$$\overline{\Gamma} \vdash_{\overline{T}} A^* =_{\overline{A} \to \overline{A} \to \mathsf{bool}} A'^* \quad \text{Induction hypothesis,(109)} \tag{112}$$

$$\overline{\Gamma},\ x{:}\overline{A},\ \triangleright A^*\ x\ x \vdash_{\overline{T}} \overline{B} \equiv \overline{B'} \quad \text{Induction hypothesis,(110)} \tag{113}$$

Since $\equiv$ is context independent in HOL:

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{B} \equiv \overline{B'} \quad \text{explanation,(113)} \tag{114}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{A} \to \overline{B} \equiv \overline{A'} \to \overline{B'} \quad (\text{cong}\to),(111),(114) \tag{115}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{\Pi x{:}A.\ B} \equiv \overline{\Pi x{:}A'.\ B'} \quad \text{PT10,(115)}$$

$$\overline{\Gamma},\ x{:}\overline{A},\ \triangleright A^*\ x\ x \vdash_{\overline{T}} B^* =_{\overline{B}\to\overline{B}\to\mathsf{bool}} B'^* \qquad \text{Induction hypothesis,(110)} \tag{116}$$

$$\begin{aligned}\overline{\Gamma},\ f{:}\overline{A}\to\overline{B},\ x{:}\overline{A} \vdash_{\overline{T}}\ & A^*\ x\ x \Rightarrow B^*\ (f\ x)\ (f\ x)\\ &=_{\mathsf{bool}} A'^*\ x\ x \Rightarrow B^*\ (f\ x)\ (f\ x) \qquad \text{(rewrite),(refl),(112)}\end{aligned} \tag{117}$$

$$\begin{aligned}\overline{\Gamma},\ f{:}\overline{A}\to\overline{B},\ x{:}\overline{A} \vdash_{\overline{T}}\ & A^*\ x\ x \Rightarrow B^*\ (f\ x)\ (f\ x)\\ &=_{\mathsf{bool}} A'^*\ x\ x \Rightarrow B'^*\ (f\ x)\ (f\ x) \qquad \text{(rewrite),(117),(116)}\end{aligned} \tag{118}$$

$$\begin{aligned}\overline{\Gamma},\ f{:}\overline{A}\to\overline{B} \vdash_{\overline{T}} & \forall x{:}\overline{A}.\ A^*\ x\ x \Rightarrow (B^*\ (f\ x)\ (f\ x)) =_{\mathsf{bool}}\\ & \forall x{:}\overline{A'}.\ A'^*\ x\ x \Rightarrow (B'^*\ (f\ x)\ (f\ x)) \qquad (\forall\text{cong}),(111),(118)\end{aligned} \tag{119}$$

$$\overline{\Gamma} \vdash_{\overline{T}} (\Pi x{:}A.\ B)^* =_{\overline{A}\to\overline{A}\to\mathsf{bool}} (\Pi x{:}A'.\ B')^* \qquad \text{PT20,(cong}\lambda\text{),(119)}$$

($\equiv$ bool):

$$\vdash_T \Gamma\ \mathsf{Ctx} \qquad \text{By Assumption} \tag{120}$$

$$\vdash_{\overline{T}} \overline{\Gamma}\ \mathsf{Ctx} \qquad \text{Induction hypothesis,(120)} \tag{121}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \mathsf{bool}\ \mathsf{tp} \qquad \text{(congbool),(121)}$$

bool^* is a well-typed relation on bool by definition.

Subtyping Subtyping can be shown using the axiom (2).

(2): We need to check that the translation of axiom (2) holds in HOL. (2) states that whenever either side is well-formed, we have:

$$\vdash \Pi x{:}A.\ {}^{B}/_{r} \prec: {}^{(\Pi x:A.\ B)}/_{\lambda f,\, g:\Pi x:A.\ B.\ \forall x:A.\ r\ \ (f\ x)\,(g\ x)}$$

If either side is well-formed it follows that A, B are well-formed and r is equivalence relation on A. We then need to prove that $\overline{\Pi x{:}A.\ {}^{B}/_{r}} \equiv \overline{{}^{(\Pi x:A.\ B)}/_{\lambda f,\, g:\Pi x:A.\ B.\ \forall x:A.\ r\ \ (f\ x)\,(g\ x)}}$ holds, which is immediate from the definition of the translation (both sides are just $\overline{A} \to \overline{B}$) and that in a context containing $x, y{:}\overline{B}$ we have

$$(\Pi x{:}A.\ {}^{B}/_{r})^*\ x\ y \Rightarrow ({}^{(\Pi x:A.\ B)}/_{\lambda f,\, g:\Pi x:A.\ B.\ \forall x:A.\ r\ \ (f\ x)\,(g\ x)})^*\ x\ y.$$

However, we have already shown in Example 6 that both PER applications reduce to the same formula, so the implication must be valid in HOL.

Typing Typing can be shown using the rules (const'), (var'), (quotE), (lambda'), (appl'), ($\Rightarrow$type'), (=type), ($|_p$ I), ($|_p$ E1), (QI):

(const'):

$$\mathsf{c}{:}A'\ \text{in}\ T \qquad \text{By Assumption} \tag{122}$$

$$\Gamma \vdash_T A' \equiv A \qquad \text{By Assumption} \tag{123}$$

$$\mathsf{c}{:}\overline{A'}\ \text{in}\ \overline{T} \qquad \text{PT3,(122)} \tag{124}$$

$$
\begin{array}{rlr}
\rhd {A'}^{*}\ \mathsf{c}\ \mathsf{c} \text{ in } \overline{T} & \text{PT3,(122)} & (125)\\
\overline{\Gamma} \vdash_{\overline{T}} \overline{A'} \equiv \overline{A} & \text{Induction hypothesis,(123)} & (126)\\
\overline{\Gamma},\ x{:}\overline{A'} \vdash_{\overline{T}} {A'}^{*}\ x\ x =_{\mathsf{bool}} A^{*}\ x\ x & \text{Induction hypothesis,(123)} & (127)\\
\overline{\Gamma} \vdash_{\overline{T}} \forall x{:}\overline{A}.\ {A'}^{*}\ x\ x =_{\mathsf{bool}} A^{*}\ x\ x & (\forall\mathrm{I}),(\forall\mathrm{I}),(127) & (128)\\
\overline{\Gamma} \vdash_{\overline{T}} \mathsf{c}{:}\overline{A} & \text{(const),(124),(126)} & (129)\\
\overline{\Gamma} \vdash_{\overline{T}} \overline{\mathsf{c}}{:}\overline{A} & \text{PT3,(129)} & \\
\overline{\Gamma} \vdash_{\overline{T}} {A'}^{*}\ \overline{\mathsf{c}}\ \overline{\mathsf{c}} & \text{PT3,(axiom),(125)} & (130)\\
\overline{\Gamma} \vdash_{\overline{T}} A^{*}\ \overline{\mathsf{c}}\ \overline{\mathsf{c}} & (\text{cong}\vdash),(\forall\mathrm{E}),(128),(130) &
\end{array}
$$

(var'):

$$
\begin{array}{rlr}
x{:}A' \text{ in } \Gamma & \text{By Assumption} & (131)\\
\Gamma \vdash_{T} A' \equiv A & \text{By Assumption} & (132)\\
x{:}\overline{A'} \text{ in } \overline{\Gamma} & \text{PT3,(131)} & (133)\\
\rhd {A'}^{*}\ x\ x \text{ in } \overline{\Gamma} & \text{PT3,(131)} & (134)\\
\overline{\Gamma} \vdash_{\overline{T}} \overline{A'} \equiv \overline{A} & \text{Induction hypothesis,(132)} & (135)\\
\overline{\Gamma},\ x{:}\overline{A'} \vdash_{\overline{T}} {A'}^{*}\ x\ x =_{\mathsf{bool}} A^{*}\ x\ x & \text{Induction hypothesis,(132)} & (136)\\
\overline{\Gamma} \vdash_{\overline{T}} \forall x{:}\overline{A}.\ {A'}^{*}\ x\ x =_{\mathsf{bool}} A^{*}\ x\ x & (\forall\mathrm{I}),(136) & (137)\\
\overline{\Gamma} \vdash_{\overline{T}} x{:}\overline{A} & \text{(var),(133),(135)} & (138)\\
\overline{\Gamma} \vdash_{\overline{T}} \overline{x}{:}\overline{A} & \text{PT3,(138)} & \\
\overline{\Gamma} \vdash_{\overline{T}} {A'}^{*}\ \overline{x}\ \overline{x} & \text{PT3,(assume),(134)} & (139)\\
\overline{\Gamma} \vdash_{\overline{T}} A^{*}\ \overline{x}\ \overline{x} & (\text{cong}\vdash),(\forall\mathrm{E}),(137),(139) &
\end{array}
$$

(quotE):

$$
\begin{array}{rlr}
\Gamma \vdash_{T} s{:}{}^{A}/_{r} & \text{By Assumption} & (140)\\
\Gamma,\ x{:}A,\ \rhd x =_{A/r} s \vdash_{T} t{:}B & \text{By Assumption} & (141)\\
\Gamma,\ x{:}A,\ x'{:}A,\ \rhd x =_{A/r} s,\ \rhd x' =_{A/r} s \vdash_{T} t =_{B} t[{}^{x}/_{x'}] & \text{By Assumption} & (142)\\
\overline{\Gamma} \vdash_{\overline{T}} \overline{s}{:}\overline{A} & \text{Induction hypothesis,(140)} & (143)\\
\overline{\Gamma},\ x{:}\overline{A},\ \rhd A^{*}\ x\ x,\ \rhd({}^{A}/_{r})^{*}\ \overline{x}\ \overline{s} \vdash_{\overline{T}} \overline{t}{:}\overline{B} & \text{Induction hypothesis,(141)} & (144)\\
\overline{\Gamma},\ x{:}A,\ \rhd A^{*}\ x\ x,\ x'{:}A,\ \rhd A^{*}\ x'\ x', & & \\
\rhd({}^{A}/_{r})^{*}\ x\ \overline{s},\ \rhd({}^{A}/_{r})^{*}\ x'\ \overline{s} \vdash_{\overline{T}} B^{*}\ \overline{t}\ \overline{t}[{}^{x}/_{x'}] & \text{Induction hypothesis,(142)} & (145)
\end{array}
$$

Since typing is context independent in HOL:

$$
\begin{array}{rlr}
\overline{\Gamma},\ x{:}\overline{A} \vdash_{\overline{T}} \overline{t}{:}\overline{B} & \text{explanation,(144)} & (146)\\
\overline{\Gamma} \vdash_{\overline{T}} \overline{t}[{}^{x}/_{\overline{s}}]{:}\overline{B} & \text{(rewriteTyping),(146),(143)} & (147)\\
\overline{\Gamma} \vdash_{\overline{T}} \overline{t}[{}^{x}/_{\overline{s}}]{:}\overline{B[{}^{x}/_{s}]} & \text{HOL types are simple,(147)} &
\end{array}
$$

Since B^{*} is transitive we can simplify (145) to:

$$\overline{\Gamma},\ x{:}A,\ \rhd A^{*}\ x\ x,$$

$$\triangleright({}^{A}/_{r})^{*}\ x\ \overline{s} \vdash_{\overline{T}} B^{*}\ \overline{t}\ \overline{t}[{}^{x}/_{\overline{s}}] \qquad \text{explanation,(145)} \qquad (148)$$

By symmetry and transitivity of B^{*}, we yield also $B^{*}\ \overline{t}[{}^{x}/_{\overline{s}}]\ \overline{t}[{}^{x}/_{\overline{s}}]$ in the same context. Since this formula no longer depends on x and an (known to be well-typed) equality assumption with an otherwise unused variable on one side is not useful for proving in HOL, the same must also be derivable in context $\overline{\Gamma}$.

$$\overline{\Gamma} \vdash_{\overline{T}} B^{*}\ \overline{t}[{}^{x}/_{\overline{s}}]\ \overline{t}[{}^{x}/_{\overline{s}}] \qquad \text{explanation,(148)}$$

(lambda'):

$$\Gamma,\ x{:}\overline{A} \vdash_{\mathsf{T}} t{:}B \qquad \text{By Assumption} \qquad (149)$$

$$\Gamma \vdash_{\mathsf{T}} A \equiv A' \qquad \text{By Assumption} \qquad (150)$$

$$\Gamma,\ x{:}\overline{A},\ \triangleright A^{*}\ x\ x \vdash_{\overline{T}} \overline{t}{:}\overline{B} \qquad \text{Induction hypothesis,PT6,(149)} \qquad (151)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{A} \equiv \overline{A'} \qquad \text{Induction hypothesis,(150)} \qquad (152)$$

$$\overline{\Gamma} \vdash_{\overline{T}} A^{*} =_{\overline{A}\to\overline{A}\to\mathsf{bool}} A'^{*} \qquad \text{Induction hypothesis,(150)} \qquad (153)$$

$$\Gamma,\ x{:}\overline{A},\ \triangleright A^{*}\ x\ x \vdash_{\overline{T}} B^{*}\ \overline{t}\ \overline{t} \qquad \text{Induction hypothesis,PT6,(149)} \qquad (154)$$

$$\Gamma,\ x,y{:}\overline{A},\ \triangleright A^{*}\ x\ y \vdash_{\overline{T}} B^{*}\ \overline{t}\ \overline{t}[{}^{x}/_{y}] \qquad \text{(13),(154)} \qquad (155)$$

$$\Gamma \vdash_{\mathsf{T}} \forall x,y{:}\overline{A}.\ A^{*}\ x\ y \Rightarrow B^{*}\ \overline{t}\ \overline{t}[{}^{x}/_{y}] \qquad (\forall\mathrm{I}),(\Rightarrow\mathrm{I}),(155) \qquad (156)$$

$$\Gamma \vdash_{\mathsf{T}} \forall x,y{:}\overline{A}.\ A'^{*}\ x\ y \Rightarrow B^{*}\ \overline{t}\ \overline{t}[{}^{x}/_{y}] \qquad \text{(rewrite),(156),(153)} \qquad (157)$$

$$\Gamma,\ x{:}A \vdash_{\overline{T}} \overline{t}{:}\overline{B} \qquad \text{typing independent of assumptions,(151)} \qquad (158)$$

$$\overline{\Gamma} \vdash_{\overline{T}} (\lambda x{:}\overline{A}.\ \overline{t}){:}\overline{A} \to \overline{B} \qquad \text{(lambda),(158)} \qquad (159)$$

Since in HOL equal types are necessarily identical, it follows:

$$\overline{\Gamma} \vdash_{\overline{T}} (\lambda x{:}\overline{A}.\ \overline{t}){:}\overline{A'} \to \overline{B} \qquad \text{explanation,(159),(152)} \qquad (160)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{\lambda x{:}A.\ t}{:}\overline{\Pi x{:}A'.\ B} \qquad \text{PT20,PT10,(160)}$$

$$\overline{\Gamma} \vdash_{\overline{T}} (\Pi x{:}A'.\ B)^{*}\quad \overline{\lambda x{:}A.\ t} \qquad \text{PT11,(157)}$$

(appl'):

$$\Gamma \vdash_{\mathsf{T}} f{:}\Pi x{:}A.\ B \qquad \text{By Assumption} \qquad (161)$$

$$\Gamma \vdash_{\mathsf{T}} t{:}A \qquad \text{By Assumption} \qquad (162)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{f}{:}\overline{A} \to \overline{B} \qquad \text{Induction hypothesis,PT10,(161)} \qquad (163)$$

$$\overline{\Gamma} \vdash_{\overline{T}} (\Pi x{:}A.\ B)^{*}\ \overline{f}\ \overline{f} \qquad \text{Induction hypothesis,PT10,(161)} \qquad (164)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \forall x{:}\overline{A}.\ \forall y{:}\overline{A}.$$

$$A^{*}\ x\ y \Rightarrow B^{*}\ (\overline{f}\ x)\ (\overline{f}\ y) \qquad \text{PT11,(164)} \qquad (165)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{t}{:}\overline{A} \qquad \text{Induction hypothesis,(162)} \qquad (166)$$

$$\overline{\Gamma} \vdash_{\overline{T}} A^{*}\ \overline{t}\ \overline{t} \qquad \text{Induction hypothesis,(162)} \qquad (167)$$

$$\overline{\Gamma} \vdash_{\overline{T}} A^{*}\ \overline{t}\ \overline{t} \Rightarrow B^{*}\ (\overline{f}\ \overline{t})\ (\overline{f}\ \overline{t}) \qquad (\forall\mathrm{E}),(\forall\mathrm{E}),(165),(166),(166) \qquad (168)$$

$$\overline{\Gamma} \vdash_{\overline{T}} B^{*}\ (\overline{f}\ \overline{t})\ (\overline{f}\ \overline{t}) \qquad (\Rightarrow\mathrm{E}),(168),(167) \qquad (169)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{f}\ \overline{t}{:}\overline{B} \qquad \text{(appl),(163),(166)} \qquad (170)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{f\ t}{:}\overline{B} \qquad \text{PT21,(170)}$$

$$\overline{\Gamma} \vdash_{\overline{T}} B^{*}\ \overline{f\ t}\ \overline{f\ t} \qquad \text{PT21,(168)}$$

($\Rightarrow$type'):

$\Gamma \vdash_{T} F{:}\mathsf{bool}$	By Assumption	(171)
$\Gamma,\ \rhd F \vdash_{T} G{:}\mathsf{bool}$	By Assumption	(172)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F}{:}\mathsf{bool}$	Induction hypothesis,(171)	(173)
$\overline{\Gamma},\ \overline{F} \vdash_{\overline{T}} \overline{G}{:}\mathsf{bool}$	Induction hypothesis,(172)	(174)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{G}{:}\mathsf{bool}$	typing is independent of assumptions,(174)	(175)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F} \Rightarrow \overline{G}{:}\mathsf{bool}$	($\Rightarrow$type),(173),(175)	(176)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F \Rightarrow G}{:}\mathsf{bool}$	PT22,(176)	(177)
$\overline{\Gamma} \vdash_{\overline{T}} \mathsf{bool}^*\ \overline{F \Rightarrow G}\ \overline{F \Rightarrow G}$	(PT13),(refl),(177)	

(=type):

$\Gamma \vdash_{T} s{:}A$	By Assumption	(178)
$\Gamma \vdash_{T} t{:}A$	By Assumption	(179)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{s}{:}\overline{A}$	Induction hypothesis,(178)	(180)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{t}{:}\overline{A}$	Induction hypothesis,(179)	(181)
$\overline{\Gamma} \vdash_{\overline{T}} A^*\ \overline{s}\ \overline{s}$	Induction hypothesis,(178)	(182)
$\overline{\Gamma} \vdash_{\overline{T}} A^*\ \overline{s}\ \overline{s}{:}\mathsf{bool}$	(validTyping),(182)	(183)
$\overline{\Gamma} \vdash_{\overline{T}} A^*{:}\overline{A} \to \overline{A} \to \mathsf{bool}$	(applType),(182),(applType),(182),(183)	(184)
$\overline{\Gamma} \vdash_{\overline{T}} A^*\ \overline{s}\ \overline{t}{:}\mathsf{bool}$	(appl),(appl),(184),(180),(181)	(185)
$\overline{\Gamma} \vdash_{\overline{T}} \mathsf{bool}^*\ \left(A^*\ \overline{s}\ \overline{t}\right)\ \left(A^*\ \overline{s}\ \overline{t}\right)$	(PT13),(refl),(185)	

($|_p$ I):

$\Gamma \vdash_{T} t{:}A$	By Assumption	(186)
$\Gamma \vdash_{T} p\ t$	By Assumption	(187)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{t}{:}\overline{A}$	Induction hypothesis,(186)	(188)
$\overline{\Gamma} \vdash_{\overline{T}} A^*\ \overline{t}\ \overline{t}$	Induction hypothesis,(186)	(189)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{p}\ \overline{t}$	Induction hypothesis,(187)	(190)
$\overline{\Gamma} \vdash_{\overline{T}} (A\vert_p)^*\ \overline{t}\ \overline{t}$	PT15,($\wedge$I),(189),($\wedge$I),(190),(190)	
$\overline{\Gamma} \vdash_{\overline{T}} \overline{t}{:}\overline{A\vert_p}$	PT14,(188)	

($|_p$ E1):

$\Gamma \vdash_{T} t{:}A\vert_p$	By Assumption	(191)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{t}{:}\overline{A}$	Induction hypothesis,(191)	
$\overline{\Gamma} \vdash_{\overline{T}} A^*\ \overline{t}\ \overline{t} \wedge \overline{p}\ \overline{t}$	Induction hypothesis,(191)	(192)
$\overline{\Gamma} \vdash_{\overline{T}} A^*\ \overline{t}\ \overline{t}$	($\wedge$El),(192)	

(QI):

$$\Gamma \vdash_{\mathrm{T}} t{:}A \qquad \text{By Assumption} \tag{193}$$

$$\Gamma \vdash_{\mathrm{T}} \mathrm{EqRel}(r) \qquad \text{By Assumption} \tag{194}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{t}{:}\overline{A} \qquad \text{Induction hypothesis,(193)} \tag{195}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{t}{:}\overline{(A/r)} \qquad \text{PT15,(195)}$$

$$\overline{\Gamma} \vdash_{\overline{T}} A^*\ \overline{t}\ \overline{t} \qquad \text{Induction hypothesis,(193)} \tag{196}$$

As shown as Subsection C.1 (194) implies that $\overline{r}$ is an equivalence on terms x satisfying $A^*\ x\ x$. It follows that $\overline{r}\ \overline{t}\ \overline{t}$ holds.

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{r}\ \overline{t}\ \overline{t} \qquad \text{explanation,(196)} \tag{197}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{r}\ \overline{t}\ \overline{t} \wedge A^*\ \overline{t}\ \overline{t} \wedge A^*\ \overline{t}\ \overline{t} \qquad \text{definition of } \wedge\text{,(197),(196)} \tag{198}$$

$$\overline{\Gamma} \vdash_{\overline{T}} (A/r)^*\ \overline{t}\ \overline{t} \qquad \text{PT17,(198)}$$

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

Term equality can be shown using the rules (congλ'), (congAppl'), (refl), (sym), (beta), (etaPi) and (Q$=$) in DHOL.

(congλ') This case will use (13).

$$\Gamma \vdash_{\mathrm{T}} A \equiv A' \qquad \text{By Assumption} \tag{199}$$

$$\Gamma,\ x{:}A \vdash_{\mathrm{T}} t =_B t' \qquad \text{By Assumption} \tag{200}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{A} \equiv \overline{A'} \qquad \text{Induction hypothesis,(199)} \tag{201}$$

$$\overline{\Gamma},\ x{:}\overline{A},\ \triangleright A^*\ x\ x \vdash_{\overline{T}} B^*\ \overline{t}\ \overline{t'} \qquad \text{Induction hypothesis,(200)} \tag{202}$$

$$\overline{\Gamma},\ z{:}\overline{A},\ \triangleright A^*\ z\ z \vdash_{\overline{T}} B^*\ \overline{t}[{}^{x}/{}_{z}]\ \overline{t'}[{}^{x}/{}_{z}] \qquad \alpha\text{-renaming,(202)} \tag{203}$$

$$\overline{\Gamma},\ z{:}\overline{A} \vdash_{\overline{T}} A^*\ z\ z \Rightarrow B^*\ \overline{t}[{}^{x}/{}_{z}]\ \overline{t'}[{}^{x}/{}_{z}] \qquad (\Rightarrow\text{I}),(203) \tag{204}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \forall z{:}\overline{A}.\ A^*\ z\ z \Rightarrow B^*\ \overline{t}[{}^{x}/{}_{z}]\ \overline{t'}[{}^{x}/{}_{z}] \qquad (\forall\text{I}),(204) \tag{205}$$

$$\overline{\Gamma},\ x, y{:}\overline{A} \vdash_{\overline{T}} \forall z{:}\overline{A}.\ A^*\ z\ z \Rightarrow B^*\ \overline{t}[{}^{x}/{}_{z}]\ \overline{t'}[{}^{x}/{}_{z}] \qquad (\text{var}\vdash),(\text{var}\vdash),(205) \tag{206}$$

$$\overline{\Gamma},\ x, y{:}\overline{A} \vdash_{\overline{T}} A^*\ x\ x \Rightarrow B^*\ \overline{t}\ \overline{t'} \qquad (\text{var}\vdash),(\text{var}\vdash),(206) \tag{207}$$

$$\overline{\Gamma},\ x, y{:}\overline{A},\ \triangleright A^*\ x\ y \vdash_{\overline{T}} A^*\ x\ x \Rightarrow B^*\ \overline{t}\ \overline{t'} \qquad (\text{monotonic}\vdash),(207) \tag{208}$$

$$\overline{\Gamma},\ x, y{:}\overline{A},\ \triangleright A^*\ x\ y \vdash_{\overline{T}} A^*\ x\ x \qquad (13),(\text{assume}),(\text{assume}) \tag{209}$$

$$\overline{\Gamma},\ x, y{:}\overline{A},\ \triangleright A^*\ x\ y \vdash_{\overline{T}} B^*\ \overline{t}\ \overline{t'} \qquad (\Rightarrow\text{E}),(208),(209) \tag{210}$$

$$\overline{\Gamma},\ x, y{:}\overline{A},\ \triangleright A^*\ x\ y \vdash_{\overline{T}} B^*\ \overline{t}\ \overline{t'}[{}^{x}/{}_{y}] \qquad (13),(210),(\text{assume}) \tag{211}$$

$$\overline{\Gamma},\ x,y{:}\overline{A} \vdash_{\overline{T}} A^*\ x\ y \Rightarrow B^*\ \bar{t}\ \overline{t'}[^x/_y] \qquad (\Rightarrow\mathrm{I}),(211) \tag{212}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \forall\, x{:}\overline{A}.\ \forall\, y{:}\overline{A}.\ A^*\ x\ y \Rightarrow B^*\ \bar{t}\ \overline{t'}[^x/_y] \qquad (\forall\mathrm{I}),(\forall\mathrm{I}),(212) \tag{213}$$

$$\overline{\Gamma},\ x{:}\overline{A},\ \triangleright A^*\ x\ x \vdash_{\overline{T}} \bar{t}{:}\overline{B} \qquad \text{Induction hypothesis},(221) \tag{214}$$

$$\overline{\Gamma},\ x{:}\overline{A},\ \triangleright A^*\ x\ x \vdash_{\overline{T}} \overline{t'}{:}\overline{B} \qquad \text{Induction hypothesis},(221) \tag{215}$$

Since in HOL typing is independent of context assumptions:

$$\overline{\Gamma},\ x{:}\overline{A} \vdash_{\overline{T}} \bar{t}{:}\overline{B} \qquad \text{explanation},(214) \tag{216}$$

$$\overline{\Gamma},\ x{:}\overline{A} \vdash_{\overline{T}} \overline{t'}{:}\overline{B} \qquad \text{explanation},(215) \tag{217}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \lambda x{:}\overline{A}.\ \bar{t}{:}\overline{A} \to \overline{B} \qquad (\text{lambda}),(216) \tag{218}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \lambda x{:}\overline{A}.\ \overline{t'}{:}\overline{A} \to \overline{B} \qquad (\text{lambda}),(217) \tag{219}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{\lambda x{:}A.\ t =_{\Pi x:A.\ B} \lambda x{:}A'.\ t'} \qquad (\mathrm{PT23}),(213)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{\lambda x{:}A.\ t}{:}\overline{\Pi x{:}A.\ B} \qquad (\mathrm{PT10}),(\mathrm{PT20}),(218)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{\lambda x{:}A.\ t'}{:}\overline{\Pi x{:}A.\ B} \qquad (\mathrm{PT10}),(\mathrm{PT20}),(219)$$

(congAppl'):

$$\Gamma \vdash_{T} t =_A t' \qquad \text{By Assumption} \tag{220}$$

$$\Gamma \vdash_{T} f =_{\Pi x:A.\ B} f' \qquad \text{By Assumption} \tag{221}$$

$$\overline{\Gamma} \vdash_{\overline{T}} A^*\ \bar{t}\ \overline{t'} \qquad \text{Induction hypothesis},(220) \tag{222}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \forall\, x{:}\overline{A}.\ \forall\, y{:}\overline{A}.\ A^*\ x\ y \Rightarrow (\Pi z{:}A.\ B)^*\ \bar{f}\ x\ \overline{f'}\ y \qquad \text{Induction hypothesis},(221) \tag{223}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \bar{t}{:}\overline{A} \qquad \text{Induction hypothesis},(220) \tag{224}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{t'}{:}\overline{A} \qquad \text{Induction hypothesis},(220) \tag{225}$$

$$\overline{\Gamma} \vdash_{\overline{T}} A^*\ \bar{t}\ \overline{t'} \Rightarrow (\Pi z{:}A.\ B)^*\ \bar{f}\ \bar{t}\ \overline{f'}\ \overline{t'} \qquad (\forall\mathrm{E}),(\forall\mathrm{E}),(223),(224),(225) \tag{226}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \bar{f}{:}\overline{A} \to \overline{B} \qquad \text{Induction hypothesis},(221) \tag{227}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{f'}{:}\overline{A} \to \overline{B} \qquad \text{Induction hypothesis},(221) \tag{228}$$

$$\overline{\Gamma} \vdash_{\overline{T}} (\Pi z{:}A.\ B)^*\ \bar{f}\ \bar{t}\ \overline{f'}\ \overline{t'} \qquad (\Rightarrow\mathrm{E}),(226),(222)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \bar{f}\ \bar{t}{:}\overline{B} \qquad (\text{appl}),(227),(224)$$

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{f'}\ \overline{t'}{:}\overline{B} \qquad (\text{appl}),(227),(224)$$

(refl):

$$\Gamma \vdash_{T} t{:}A \qquad \text{By Assumption} \tag{229}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \bar{t}{:}\overline{A} \qquad \text{Induction hypothesis},(229) \tag{230}$$

$$\overline{\Gamma} \vdash_{\overline{T}} \bar{t} =_{\overline{A}} \bar{t} \qquad (\text{refl}),(230)$$

$$\overline{\Gamma} \vdash_{\overline{T}} A^*\ \bar{t}\ \bar{t} \qquad \text{Induction hypothesis},(229)$$

(sym):

$$\Gamma \vdash_{T} s =_{A} t \qquad \text{By Assumption} \tag{231}$$
$$\overline{\Gamma} \vdash_{\overline{T}} A^{*}\ \overline{s}\ \overline{t} \qquad \text{Induction hypothesis,(231)} \tag{232}$$
$$\overline{\Gamma} \vdash_{\overline{T}} \overline{t}{:}\overline{A} \qquad \text{Induction hypothesis,(231)} \tag{233}$$
$$\overline{\Gamma} \vdash_{\overline{T}} \overline{s}{:}\overline{A} \qquad \text{Induction hypothesis,(231)} \tag{234}$$
$$\overline{\Gamma} \vdash_{\overline{T}} A^{*}\ \overline{t}\ \overline{s} \qquad (\forall E),(\forall E),(\Rightarrow E),(9),(232),(233),(234)$$

(beta):

$$\Gamma \vdash_{T} (\lambda x{:}A.\ s)\ t{:}B \qquad \text{By Assumption} \tag{235}$$
$$\overline{\Gamma} \vdash_{\overline{T}} (\lambda x{:}\overline{A}.\ \overline{s})\ \overline{t}{:}\overline{B} \qquad \text{Induction hypothesis,PT20,(235)} \tag{236}$$
$$\overline{\Gamma} \vdash_{\overline{T}} (\lambda x{:}\overline{A}.\ \overline{s})\ \overline{t} =_{\overline{B}} \overline{s}[{}^{x}/_{\overline{t}}] \qquad \text{(beta),(236)} \tag{237}$$
$$\overline{\Gamma} \vdash_{\overline{T}} (\lambda x{:}\overline{A}.\ \overline{s})\ \overline{t} =_{\overline{B}} \overline{s[{}^{x}/_{t}]} \qquad (11),(237) \tag{238}$$
$$\overline{\Gamma} \vdash_{\overline{T}} \overline{(\lambda x{:}A.\ s)\ t} =_{\overline{B}} \overline{s[{}^{x}/_{t}]} \qquad \text{PT20,PT21,(238)}$$
$$\overline{\Gamma} \vdash_{\overline{T}} (\Pi x{:}A.\ B)^{*}\ \ ((\lambda x{:}A.\ s)\ t)\ \ ((\lambda x{:}A.\ s)\ t) \qquad \text{Induction hypothesis,(235)}$$

(etaPi):

$$\Gamma \vdash_{T} t{:}\Pi x{:}A.\ B \qquad \text{By Assumption} \tag{239}$$
$$\overline{\Gamma} \vdash_{\overline{T}} \overline{t}{:}\overline{A} \to \overline{B} \qquad \text{PT10,Induction hypothesis,(239)} \tag{240}$$
$$\overline{\Gamma} \vdash_{\overline{T}} \overline{t} =_{\overline{A} \to \overline{B}} \lambda x{:}\overline{A}.\ \overline{t}\ x \qquad \text{(eta),(240)} \tag{241}$$
$$\overline{\Gamma} \vdash_{\overline{T}} \overline{t} =_{\overline{\Pi x:A.\ B}} \overline{\lambda x{:}A.\ t\ x} \qquad \text{PT20,PT10,(241)}$$
$$\overline{\Gamma} \vdash_{\overline{T}} (\Pi x{:}A.\ B)^{*}\ \overline{t}\ \overline{t} \qquad \text{Induction hypothesis,(240)}$$

($|_p$ Eq):

$$\Gamma \vdash_{T} s =_{A} t \qquad \text{By Assumption} \tag{242}$$
$$\Gamma \vdash_{T} p\ s \qquad \text{By Assumption} \tag{243}$$
$$\overline{\Gamma} \vdash_{\overline{T}} A^{*}\ \overline{s}\ \overline{t} \qquad \text{Induction hypothesis,(242)} \tag{244}$$
$$\overline{\Gamma} \vdash_{\overline{T}} \overline{p}\ \overline{s} \qquad \text{Induction hypothesis,(243)} \tag{245}$$

By (14) it follows:

$$\overline{\Gamma} \vdash_{\overline{T}} \overline{p}\ \overline{t} \qquad \text{explanation,(243),(244)} \tag{246}$$
$$\overline{\Gamma} \vdash_{\overline{T}} A^{*}\ \overline{s}\ \overline{t} \wedge \overline{p}\ \overline{s} \wedge \overline{p}\ \overline{t} \qquad \text{definition of } \wedge\text{,(244),(245),(246)} \tag{247}$$
$$\overline{\Gamma} \vdash_{\overline{T}} (A|_{p})^{*}\ s\ t \qquad \text{PT15,(247)}$$
$$\overline{\Gamma} \vdash_{\overline{T}} \overline{s}{:}\overline{({}^{A}/_{p})} \qquad \text{(validTyping),}(\wedge El)\text{,(247)}$$

(Q=):

$$\Gamma \vdash_{T} s{:}A \qquad \text{By Assumption} \tag{248}$$
$$\Gamma \vdash_{T} t{:}A \qquad \text{By Assumption} \tag{249}$$

$\Gamma \vdash_{T} r{:}A \to A \to \mathsf{bool}$	By Assumption	(250)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{s}{:}\overline{A}$	Induction hypothesis,(248)	(251)
$\overline{\Gamma} \vdash_{\overline{T}} A^{*}\ \overline{s}\ \overline{s}$	Induction hypothesis,(248)	(252)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{t}{:}\overline{A}$	Induction hypothesis,(249)	(253)
$\overline{\Gamma} \vdash_{\overline{T}} A^{*}\ \overline{t}\ \overline{t}$	Induction hypothesis,(248)	(254)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{r}{:}\overline{A} \to \overline{A} \to \mathsf{bool}$	Induction hypothesis,(250)	(255)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{r}\ \overline{s}\ \overline{t}{:}\mathsf{bool}$	(appl),(appl),(255),(251),(253)	(256)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{r}\ \overline{s}\ \overline{t} =_{\mathsf{bool}} \overline{r}\ \overline{s}\ \overline{t}$	(refl),(256)	(257)
$\overline{\Gamma} \vdash_{\overline{T}} \left(\overline{r}\ \overline{s}\ \overline{t} \wedge A^{*}\ \overline{s}\ \overline{s} \wedge A^{*}\ \overline{t}\ \overline{t}\right) =_{\mathsf{bool}} \overline{r}\ \overline{s}\ \overline{t}$	definition of $\wedge$, (252),(254),(257)	(258)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{s =_{(A/r)} t}$	PT17,PT13,(258)	
$\overline{\Gamma} \vdash_{\overline{T}} \overline{s}{:}\overline{(A/r)}$	PT17,(253)	

Validity Validity can be shown using the rules (axiom), (assume), ($\Rightarrow$I), ($\Rightarrow$E), (cong$\vdash$), (boolExt) and ($|_p$ E2).

(axiom)

$\triangleright F$ in T	By Assumption	(259)
$\vdash_{T} \Gamma$ Ctx	By Assumption	(260)
$\triangleright \overline{F}$ in $\overline{T}$	PT4,(259	(261)
$\vdash_{\overline{T}} \overline{\Gamma}$ Ctx	Induction hypothesis,260	(262)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F}$	(axiom),(261),(262)	

(assume)

$\triangleright F$ in Γ	By Assumption	(263)
$\vdash_{T} \Gamma$ Ctx	By Assumption	(264)
$\triangleright \overline{F}$ in $\overline{\Gamma}$	PT7,(263	(265)
$\vdash_{\overline{T}} \overline{\Gamma}$ Ctx	Induction hypothesis,264	(266)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F}$	(assume),(265),(266)	

($\Rightarrow$I)

$\Gamma \vdash_{T} F{:}\mathsf{bool}$	By Assumption	(267)
$\Gamma,\ \triangleright F \vdash_{T} G$	By Assumption	(268)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F}{:}\mathsf{bool}$	Induction hypothesis,(267)	(269)
$\overline{\Gamma},\ \overline{F} \vdash_{\overline{T}} \overline{G}$	Induction hypothesis,PT7,(268)	(270)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F} \Rightarrow \overline{G}$	($\Rightarrow$I),(269),(270)	(271)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F \Rightarrow G}$	PT22,(271)	

(⇒E)

$\Gamma \vdash_{\mathsf{T}} F \Rightarrow G$	By Assumption	(272)
$\Gamma \vdash_{\mathsf{T}} F$	By Assumption	(273)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F} \Rightarrow \overline{G}$	Induction hypothesis,PT22,(272)	(274)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F}$	Induction hypothesis,(273)	(275)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{G}$	(⇒E),(274),(275)	

(cong⊢)

$\Gamma \vdash_{\mathsf{T}} F =_{\mathsf{bool}} F'$	By Assumption	(276)
$\Gamma \vdash_{\mathsf{T}} F'$	By Assumption	(277)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F} =_{\mathsf{bool}} \overline{F'}$	(PT13),Induction hypothesis,(276)	(278)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F'}$	Induction hypothesis,(277)	(279)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{F}$	(cong⊢),(278),(279)	

(boolExt)

$\Gamma \vdash_{\mathsf{T}} p \ \mathsf{true}$	By Assumption	(280)
$\Gamma \vdash_{\mathsf{T}} p \ \mathsf{false}$	By Assumption	(281)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{p} \ \mathsf{true}$	Induction hypothesis,PT21,(280)	(282)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{p} \ \mathsf{false}$	Induction hypothesis,PT21,(281)	(283)
$\overline{\Gamma} \vdash_{\overline{T}} \forall z{:}\mathsf{bool}.\ \overline{p}\ z$	(boolExt),(282),(283)	(284)
$\overline{\Gamma},\ x{:}\mathsf{bool} \vdash_{\overline{T}} \forall z{:}\mathsf{bool}.\ \overline{p}\ z$	(var⊢),(284)	(285)
$\overline{\Gamma},\ x{:}\mathsf{bool} \vdash_{\overline{T}} \overline{p}\ x$	(∀E),(285),(assume)	(286)
$\overline{\Gamma},\ x, y{:}\mathsf{bool},\ \rhd x =_{\mathsf{bool}} y \vdash_{\mathsf{T}} \overline{p}\ x$	(monotonic⊢),(var⊢),(286)	(287)
$\overline{\Gamma},\ x, y{:}\mathsf{bool},\ \rhd x =_{\mathsf{bool}} y \vdash_{\mathsf{T}} \overline{p}\ y$	(rewrite),(287),(assume)	(288)
$\overline{\Gamma},\ x, y{:}\mathsf{bool} \vdash_{\mathsf{T}} \mathsf{bool}^*\ x\ y \Rightarrow \overline{p}\ y$	(PT13),(⇒I),(288)	(289)
$\overline{\Gamma} \vdash_{\overline{T}} \forall x{:}\mathsf{bool}.\ \forall y{:}\mathsf{bool}.\ \mathsf{bool}^*\ x\ y \Rightarrow \overline{p}\ y$	(∀I),(∀I),(289)	(290)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{\forall x{:}\mathsf{bool}.\ p\ x}$	(PT23),(PT11),(290)	

($|_p$ E2)

$\Gamma \vdash_{\mathsf{T}} t{:}A\vert_p$	By Assumption	(291)
$\overline{\Gamma} \vdash_{\overline{T}} (A\vert_p)^*\ \overline{t}\ \overline{t}$	Induction hypothesis,(291)	(292)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{p}\ \overline{t}$	(∧Er),(∧Er),PT15,(292)	(293)
$\overline{\Gamma} \vdash_{\overline{T}} \overline{p\ t}$	PT21,(293)	

D Soundness proof

The idea of the soundness proof is to transform HOL-proofs into DHOL-proofs.

The key idea is to transform a HOL-proof of $\overline{F}$ into one only using terms in the well-typed image of the translation, at which point we can read off a (partial) DHOL-proof of F. This DHOL proof will be missing sub-proofs to showing the well-typedness of terms occurring in the proof. Using the (assumed) well-typedness of the DHOL problem and induction, we can show that all terms occurring in the partial DHOL proof are in fact well-typed, yielding the existence of a complete DHOL proof. We proceed in multiple steps:

1. prove that the translation is injective for terms of equal given DHOL type,
2. define quasi-preimages for terms not in image of translation,
3. given valid HOL derivation of translation of well-typed validity conjecture, choose DHOL types of quasi-preimages of terms in it,
4. modify derivation to make terms in it (almost) proper,
5. lift modified HOL derivation to DHOL derivation.

D.1 Type-wise injectivity of the translation

Definition 4. *Let t be an ill-typed DHOL term with well-typed image $\overline{t}$ in HOL. In this case we will say that $\overline{t}$ is a* spurious *term w.rt. its preimage t. If the preimage is unique or clear from the context we will simply say that $\overline{t}$ is spurious. Similarly, a term $\overline{s}$ in HOL that is the image of a well-typed term s, will be called* proper *w.r.t its preimage s. A term tm in HOL that is not the image of any (well-typed or not) term is said to be* improper.

Lemma 5. *Let Δ be a DHOL context and let Γ denote its translation. Given two DHOL terms s, t of type A and assuming s and t are not identical, it follows that $\overline{s}$ and $\overline{t}$ are not identical.*

Proof (Proof of Lemma 5). 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 subterms 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 over the 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 Π-types either the domain type or the codomain type must differ by rule (congΠ). 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 refinement types $A|_p$ and $A'|_{p'}$ where not both $A = A'$ and $p = p'$. If $p \neq p'$, then the translations have different subterms $\overline{p}\ s$ and $\overline{p'}\ s'$ 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. The case of equalities over quotient types works analogously.

D.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 replacement* $\mathsf{repl}\,[t]$ *of t by first matching line below:*

$$\mathsf{repl}\left[\overline{t}\right] := t \tag{PT24}$$

$$\mathsf{repl}\left[\mathsf{repl}\left[s\right]\right] := \mathsf{repl}\left[s\right] \tag{PT25}$$

$$\mathsf{repl}\left[A^*\ s\right] := \lambda y{:}\overline{A}.\ A^*\ s\ y \tag{PT26}$$

$$\mathsf{repl}\,[A^*] := \lambda x{:}\overline{A}.\ \lambda y{:}\overline{A}.\ A^*\ x\ y \tag{PT27}$$
$$\mathsf{repl}\,[c] := \mathsf{c} \tag{PT28}$$
$$\mathsf{repl}\,[x] := x \tag{PT29}$$
$$\mathsf{repl}\,[f\ \ t] := \mathsf{repl}\,[f]\ \ \mathsf{repl}\,[t] \tag{PT30}$$
$$\mathsf{repl}\,[\lambda x{:}C.\ t] := \lambda x{:}C.\ \mathsf{repl}\,[t] \tag{PT31}$$

If F not of shape $A^*x'\ x \Rightarrow \_$ (for x' a variable bound in a universal quantifier whose body is this term) or of shape $\forall\, x'{:}\overline{A}.\ A^*\ x\ x' \Rightarrow \_$:

$$\mathsf{repl}\left[\forall\, x{:}\overline{A}.\ A^*\ x\ x{\Rightarrow}F\right] := \forall\, x, x'{:}\overline{A}.\ A^*\ x\ x'{\Rightarrow}\mathsf{repl}\,[F] \tag{PT32}$$
$$\mathsf{repl}\left[\forall\, x{:}\overline{A}.\ F\right] := \forall\, x, x'{:}\overline{A}.\ A^*\ x\ x'{\Rightarrow}\mathsf{repl}\,[F] \tag{PT33}$$

Otherwise $\forall\, x{:}\overline{A}.\ F$ is the translation of a universal quantifier and (PT24) applies.

$$\mathsf{repl}\,[s =_{\overline{A}} t] := A^*\ s\ t \tag{PT34}$$
$$\mathsf{repl}\,[s \Rightarrow t] := \mathsf{repl}\,[s] \Rightarrow \mathsf{repl}\,[t] \tag{PT35}$$

For terms t in the image of the translation, we define the normalization of t be be t itself.

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

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

Given a proper HOL context Δ and a well-typed HOL formula φ over Δ, we say that φ is quasi-proper *iff $\mathsf{repl}\,[\varphi] = \overline{F}$ for $\Gamma \vdash_{T} F : \mathsf{bool}$ and Γ is a quasi-preimage of Δ. In that case, we call F a* quasi-preimage *of φ.*

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

1. *Δ is proper,*
2. *φ is quasi-proper in context Δ*

In this case, we will call $\overline{\Gamma} \vdash_{\overline{T}} \overline{F}$ a relativization *of $\Delta \vdash_{\overline{T}} \varphi$ and $\Gamma \vdash_{T} F$ a* quasi-preimage *of the statement $\Delta \vdash_{\overline{T}} \varphi$, where Γ is a quasi-preimage of Δ and F a quasi-preimage of φ. Additionally, for HOL terms with preimages we consider these preimages to be quasi-preimages of the HOL term as well.*

D.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 (w.r.t. a given quasi-preimage) and contains no spurious subterms, otherwise it is said to be* unnormalizably spurious*. This means that improper terms are almost proper iff their given quasi-preimage is well-typed. Since proper terms have well-typed preimages, they are almost proper (w.r.t. this preimage) as well.*

In order to lift a HOL derivation to DHOL, we first have to choose (quasi)-preimage types for all term occuring in it (at which point we use the notions of spurious and almost proper terms w.r.t. these DHOL types).

Choosing (quasi-)preimage types for a HOL derivation

Lemma 6 (Indexing lemma). *Assume that* $\Gamma \vdash_{\mathsf{T}} F : \mathsf{bool}$ *holds in DHOL. Given a valid HOL derivation* D *of the statement* $\overline{\Gamma} \vdash_{\overline{T}} \overline{F}$*, we can choose a DHOL type* $T(t)$ *(called type index) for each occurence of a HOL term* t *in* D*, s.t. the following properties hold:*

1. $T(\overline{t}) = A'$ *with* $\overline{A} = \overline{A'}$ *for any DHOL term* t *satisfying* $\Gamma \vdash_{\mathsf{T}} t : A$*,*
2. $T(\mathsf{c}) = A$ *if* $\mathsf{c} : A$ *is a constant in* T*,*
3. $T(x) = A$ *if* $x : A$ *is variable declaration in* Γ*,*
4. $T(s) = T(t)$ *for* s, t *within an equality of the form* $s =_A t$ *for some HOL type* A*,*
5. $T(s) = T(t) = \mathsf{bool}$ *for* s, t *within an implication of the form* $s \Rightarrow t$*,*
6. $T(x) = A$ *for* x *in* $(\lambda x{:}\mathbb{B}.\ s)\ \ t$ *if* $T(t) = A$*,*
7. $T(s =_A t) = \mathsf{bool}$*,*
8. *when variables are moved from the context into a* λ*-binder or vice versa the index of said variable is preserved*
9. *whenever a term* t *occurs both in the assumptions and conclusions of a step* S *in* D*, the index of* t *is the same all those occurrences of* t *in* S*,*
10. *if* x, t *in* $\lambda x{:}\overline{B}.\ t$ *satisfy* $T(x) = A$ *and* $T(t) = B$*, then* $T(\lambda x{:}B.\ t) = \Pi x{:}A.\ B$*,*
11. $T(t) = A$ *implies* t *has type* $\overline{A}$ *and* A *is non-empty.*

Proof (Proof by induction of the shape of D). This lemma only holds for well-formed derivations of translations of well-typed conjectures over well-formed theories. It will not hold for arbitrary formulae (as can be seen by considering equalities between constants of equal HOL but different DHOL types). The proof of the lemma will therefore use that fact that the final statement in the derivation is the translation of a well-typed DHOL statement (which already determines the "correct" indices for the terms within that statement) and then show that for each step in a well-formed HOL proof concluding a statement that we can correctly index, the assumptions of that step can also be indexed correctly. We will thus proceed by "backwards induction" on the shape of the derivation D.

The assumptions of the theory and contexthood rules only contain terms already contained in the conclusions, so the associated cases in the proof are all trivial.

Similarly the assumptions of lookup rules, type well-formedness and type equality rules contain no additional terms, so those cases are also trivial.

The typing rules are about forming larger terms from subterms, so if those larger terms can be consistently (i.e. according to the claim of the lemma) indexed, then the same is necessarily also true for the subterms. Thus the typing rules also have only trivial cases. By the same arguments the cases for the congruence rules (congλ), (congAppl), the symmetry and transitivity rules for term equality and the rules (beta), (eta), ($\Rightarrow$type) and ($\Rightarrow$I) are also all trivial.

It remains to consider the cases for the rules ($\Rightarrow$E), (cong$\vdash$), (boolExt) and (nonempty).

Regarding ($\Rightarrow$E): Here the assumptions of the rule contain the additional terms F and $F \Rightarrow G$. However as both terms are of type bool all their (quasi)-preimages have type bool as well and picking indices according to any of the quasi-preimages of $F \Rightarrow G$ will work.

Regarding (cong$\vdash$): Here the assumptions of the rule contain the additional terms F' and $F =_{\mathsf{bool}} F'$. Both terms are of type bool, so by the same argument as in the previous case, we can index them consistently with the claim of this lemma.

Regarding (boolExt): Here the assumptions of the rule contain the additional terms $p\ \mathsf{true}$ and $p\ \mathsf{false}$ and true and false. All these terms are of type bool, so by the same argument as in the previous two cases, we can index them consistently with the claim of this lemma.

Regarding (nonempty): Here the second assumption contains an additional variable of type A. As this variable doesn't occur in any other terms, we can index it by the type of any of its (quasi)-preimages. By assumption, the DHOL theory is partially inhabited, so we can chose this type index to be inhabited.

Remark 2 *In the following, we will use the term* type index *to refer to a choice of DHOL types for each HOL term in a derivation satisfying the properties of the previous lemma.*

Transforming unnormalizably spurious terms into almost proper terms in HOL derivations

Definition 8. *A valid HOL derivation is called* admissible *iff we can choose quasi-preimages for all terms occurring in it s.t. all terms in the derivation are almost proper w.r.t. their chosen quasi-preimages.*

This definition is useful, since admissible derivations are precisely those HOL derivations that allow us to consistently lift the terms occurring in them to well-typed DHOL terms.

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. Similarly an* indexed statement transformation *is a map that maps HOL statements with indexed terms to HOL statements.*

Definition 10. *A* macro-step M for *an (indexed) statement transformation T* replacing *a step S in a derivation is a sequence of steps $S_1, \ldots, S_n$ (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*.*

Thus we we can replace each step in a derivation by a macro step replacing that step, we can transform that derivation to a derivation in which the given indexed statement transformation is applied to all statements. This is useful to simplify and normalize derivations to derivations with certain additional properties. In our case, we want to normalize a given HOL derivation into an admissible HOL derivation. Thus, we need to define an indexed statement transformation for which all terms in the image of the transformation are almost proper and the replace all steps in the derivation by macro steps for that statement transformation.

Since the notion of a quasi-proper term only makes sense once we fix a choice of type indices (in the sense of Lemma 6), the indexed statement transformation will actually depend on the choice of type indices.

The idea for our transformation is that given a choice of type indices according to Lemma 6, the only remaining "source" of spuriousness are ill-typed function applications. There are two cases of such function applications, either they are applications that can be beta reduced to non-spurious terms or they can not. As it turns out in the second case the proof cannot meaningfully depend on that term, so we can simply replace it with a proper one. The below definition simply spells this out in detail.

Definition 11. *A* normalizing statement transformation $\mathsf{sRed}\,(\cdot)$ *is defined to be an indexed statement transformation that replaces terms in statements as described below. The definition of the transformation of a term depends on its type index — a DHOL-type A (called* preimage type*) — for each term t. We will write those types as indices to the HOL terms, so for instance t_A indicates a HOL term t of type $\overline{A}$ and preimage type A.*

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

Since variables and lambda binders are the sole cause for HOL terms having multiple quasi-preimages, choosing indices for variables in HOL terms induces unique quasi-preimages (respecting those type indices). This uniqueness is a direct consequence of (the proof of) Lemma 5.

We will consider only those quasi-preimages that respect type indices, for the notions of unnormalizably spurious and almost proper terms.

With respect to these choices, the transformation will do the following 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 $\overline{B}$, defined as the translation of a fixed DHOL term of type B (whose existence follows from the last property of Lemma 6).*

As we are assuming a valid HOL derivation indexed according to Lemma 6, we will only define this transformation on well-typed HOL terms with preimage types consistent with the indexing lemma. We can then define the transformation of t_A (denoted by $\mathsf{sRed}\,(t_A)$) by first matching line for t_A as follows:

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

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

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

$$\mathsf{sRed}\,(t_A) := \mathsf{sRed}\left(t_A^{\beta\eta}\right) \quad \textit{if } t \textit{ is beta or eta reducible} \tag{SR3}$$

$$
\begin{aligned}
&\mathsf{sRed}\,(s_A =_{\overline{A}} t_{A'}) && := \mathsf{sRed}\,(s_A) =_{\overline{A}} \mathsf{sRed}\,(t_A) && \text{(SR4)}\\
&\mathsf{sRed}\,(F_{\mathsf{bool}} \Rightarrow G_{\mathsf{bool}}) && := \mathsf{sRed}\,(F_{\mathsf{bool}}) \Rightarrow \mathsf{sRed}\,(G_{\mathsf{bool}}) && \text{(SR5)}\\
&\mathsf{sRed}\,(\lambda x{:}A.\ s_B) && := \lambda x{:}A.\ \mathsf{sRed}\,(s_B) && \text{(SR6)}\\
&\mathsf{sRed}\,((f_{\Pi_{x:A.\ B}}\ t_{A'})_{B'}) && := w_B \qquad \textit{if } A \neq A' \textit{ or } B \neq B' && \text{(SR7)}\\
&\mathsf{sRed}\,(t_A[{}^{x_B}/_{s_B}]) && := \mathsf{sRed}\,(t_A)\,[{}^{x}/_{\mathsf{sRed}\,(s_B)}] && \text{(SR8)}\\
&\mathsf{sRed}\,(t_A) && := t && \text{(SR9)}
\end{aligned}
$$

Since $\mathsf{sRed}\,(\cdot)$ *of a term is always almost proper by (SR1), it follows that* $\mathsf{sRed}\,(\mathsf{sRed}\,(\cdot))$ *is the same as* $\mathsf{sRed}\,(\cdot)$*.*

Lemma 7. *Assume a well-typed DHOL theory T and a conjecture $\Gamma \vdash_{T} \varphi$ with Γ well-formed and φ well-typed. Assume a valid HOL derivation D of $\overline{\Gamma} \vdash_{\overline{T}} \overline{\varphi}$. Choose type indices for the terms in D according to the properties of the indexing lemma (Lemma 6). Then, for any steps S in D we can construct 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 occurring in the derivation are almost proper (w.r.t. the quasi-preimages determined by the type indices).*

Proof (Proof of Lemma 7). We will show this by induction on the shape of D.

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 (those steps can be replaced by a macro step containing exactly this single step).

Regarding the type indices: We observe that the properties of the type indices provided by Lemma 6 ensure that the smallest unnormalizably spurious terms (i.e. without unnormalizably spurious proper subterms) are function applications in which function and argument are both almost proper. Furthermore, in such a case the function is not a λ-function.

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

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

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

(=type):

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(s)_A : \overline{A} \qquad \text{By Assumption} \qquad (294)$$
$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(t)_A : \overline{A} \qquad \text{By Assumption} \qquad (295)$$
$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(s)_A =_{\overline{A}} \mathsf{sRed}\,(t)_A : \mathsf{bool} \qquad (=\text{type}),(294),(295) \qquad (296)$$
$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(s_A =_{\overline{A}} t_A)_{\mathsf{bool}} : \mathsf{bool} \qquad \text{SR4},(296)$$

(lambda):

$$\Delta,\ x_A{:}\overline{A} \vdash_{\overline{T}} \mathsf{sRed}\,(t_B)_B : \overline{B} \qquad \text{By Assumption} \qquad (297)$$
$$\Delta \vdash_{\overline{T}} \left(\lambda x_A{:}\overline{A}.\ \mathsf{sRed}\,(t_B)_B\right) : \overline{A} \to \overline{B} \qquad (\text{lambda}),(297) \qquad (298)$$

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

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(\lambda x_A{:}\overline{A}.\ \mathsf{sRed}\,(t_B)_B\right) : \overline{A} \to \overline{B} \qquad \text{SR6},(298)$$

Else by (SR3) we have $\mathsf{sRed}\left(\lambda x_A{:}\overline{A}.\ \mathsf{sRed}\,(t_B)_B\right) = \mathsf{sRed}\,(f_{\Pi y:A.\ B})$. By the remark about the type of $\mathsf{sRed}\,(\cdot)$ it follows that $\mathsf{sRed}\,(f_{\Pi y:A.\ B})$ has type $\overline{\Pi y{:}A.\ B} = \overline{A} \to \overline{B}$.

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(f_{\Pi y:A'.\ B}) : \overline{A} \to \overline{B} \qquad \text{see above} \qquad (299)$$
$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(\lambda x_A{:}\overline{A}.\ \mathsf{sRed}\,(t_B)_B\right) : \overline{A} \to \overline{B} \qquad (\text{SR3}),(299)$$

(appl):

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(f_{\Pi x:A.\ B}) : \overline{A} \to \overline{B} \qquad \text{By Assumption} \qquad (300)$$
$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(t_{A'}) : \overline{A} \qquad \text{By Assumption} \qquad (301)$$

If $A \equiv A'$:

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(f_{\Pi x:A.\ B}\ t_{A'}) : \overline{B} \qquad \text{SR1},(\text{lambda}),(300),(301)$$

If $A \not\equiv A'$ then Lemma 6(6) implies that f is not a lambda function and thus $\mathsf{sRed}\,(f_{\Pi x:A.\ B})\ \ \mathsf{sRed}\,(t_{A'})$ is not beta reducible. Thus by (SR7) we have

$$\mathsf{sRed}\,(f_{\Pi x:A.\ B}\ t_{A'}) = \mathsf{sRed}\,(\mathsf{sRed}\,(f_{\Pi x:A.\ B})_{\Pi x:A.\ B}\ \ \mathsf{sRed}\,(\mathsf{sRed}\,(t_{A'})_{A'})) = w_{\overline{B}}.$$

By construction we have $w_{\overline{B}}{:}\overline{B}$:

$$\Delta \vdash_{\overline{T}} w_{\overline{B}}{:}\overline{B} \qquad \text{By Construction} \qquad (302)$$
$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(f_{\Pi x:A.\ B}\ \mathsf{sRed}\,(t_{A'})) : \overline{B} \qquad (\text{SR2}),(\text{SR7}),(302)$$

($\Rightarrow$type):

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(F)_{\mathsf{bool}} : \mathsf{bool} \quad \text{By Assumption} \quad (303)$$
$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(G)_{\mathsf{bool}} : \mathsf{bool} \quad \text{By Assumption} \quad (304)$$
$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(F)_{\mathsf{bool}} \Rightarrow \mathsf{sRed}\,(G)_{\mathsf{bool}} : \mathsf{bool} \quad (\Rightarrow\text{type}),(303),(304) \quad (305)$$
$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(F_{\mathsf{bool}} \Rightarrow F_{\mathsf{bool}}) : \mathsf{bool} \quad \text{SR5},(305)$$

(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. Otherwise:

$$\triangleright \mathsf{sRed}\,(F_{\mathsf{bool}}) \text{ in } \Delta \quad \text{By Assumption} \quad (306)$$
$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(F_{\mathsf{bool}}) \quad (\text{assume}),(306)$$

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

(congλ):

$$\Delta \vdash_{\overline{T}} A \equiv A' \quad \text{By Assumption} \quad (307)$$
$$\Delta,\ x_A{:}\overline{A} \vdash_{\overline{T}} \mathsf{sRed}\,(t_B =_{\overline{B}} t'_B)_{\mathsf{bool}} \quad \text{By Assumption} \quad (308)$$
$$\Delta,\ x_A{:}\overline{A} \vdash_{\overline{T}} \mathsf{sRed}\,(t_B)_B =_{\overline{B}} \mathsf{sRed}\,(t'_B)_B \quad \text{SR4},(308) \quad (309)$$
$$\Delta \vdash_{\overline{T}} \lambda x_A{:}\overline{A}.\ \mathsf{sRed}\,(t_B)_B =_{\overline{A}\to\overline{B}} \lambda x_A{:}\overline{A}.\ \mathsf{sRed}\,(t'_B)_B \quad (\text{cong}\lambda),(307),(309) \quad (310)$$

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

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(\lambda x_A{:}\overline{A}.\ t_B =_{\overline{A}\to\overline{B}} \lambda x_A{:}\overline{A}.\ t'_B\right) \quad \text{SR6},\text{SR4},(310)$$

(congAppl):

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(t_A =_{\overline{A}} t'_A) \quad \text{By Assumption} \quad (311)$$
$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(t_A)_A =_{\overline{A}} \mathsf{sRed}\,(t'_A)_A \quad \text{SR4},(311) \quad (312)$$
$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(f_{\Pi x:A'.\ B} =_{\overline{A}\to\overline{B}} f'_{\Pi x:A'.\ B}) \quad \text{By Assumption} \quad (313)$$
$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(f)_{\Pi x:A'.\ B} =_{\overline{A}\to\overline{B}} \mathsf{sRed}\,(f')_{\Pi x:A'.\ B} \quad \text{SR4},(313) \quad (314)$$

Assume $A \not\equiv A'$. By property 6. in Lemma 6 $\mathsf{sRed}\,(f)$ and $\mathsf{sRed}\,(f')$ are not λ-functions. Consequently, the applications $\mathsf{sRed}\,(f)\ \mathsf{sRed}\,(s)$ and $\mathsf{sRed}\,(f')\ \mathsf{sRed}\,(s')$ are not beta or eta reducible. Thus,

$$\mathsf{sRed}\,(f_{\Pi x:A'.\ B}\ t_A) = w_{\overline{B}}$$

and

$$\mathsf{sRed}\left(f'_{\Pi x:A'.\ B} t_A\right) = w_{\overline{B}}$$

and we yield:

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

Otherwise (if $A \equiv A'$) the terms $\mathsf{sRed}\,(f)_{\Pi x:A.\ B}\ \mathsf{sRed}\,(t_A)$ and $\mathsf{sRed}\,(f')_{\Pi x:A.\ B}\ \mathsf{sRed}\,(t'_A)$ are almost proper with quasi-preimages consistent with type indices. It follows:

$$\mathsf{sRed}\,(f_{\Pi x:A.\ B}\ \mathsf{sRed}\,(t_A)) = \mathsf{sRed}\,(f_{\Pi x:A.\ B})\ \ \mathsf{sRed}\,(t_A)$$

and

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

and thus:

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(f_{\Pi x:A.\ B}\ t_A) =_{\overline{B}} \mathsf{sRed}\,(f')_{\Pi x:A.\ B}\ \ t'_A \qquad (\text{congAppl}),(312),(314)$$

In either case, we concluded

$$\mathsf{sRed}\,(f_{\Pi x:A.\ B}\ t_A) =_{\overline{B}} \mathsf{sRed}\,(f'_{\Pi x:A.\ B}\ t'_A)\,.$$

By SR4 this is already the desired conclusion of:

$$\mathsf{sRed}\,(f_{\Pi x:A.\ B}\ t_A =_{\overline{B}} f'_{\Pi x:A.\ B}\ t'_A)\,.$$

(refl):

$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(t_A)_A :\overline{A}$	By Assumption	(315)
$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(t_A)_A =_{\overline{A}} \mathsf{sRed}\,(t_A)_A$	(refl),(315)	(316)
$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(\mathsf{sRed}\,(t_A)_A =_{\overline{A}} \mathsf{sRed}\,(t_A)_A)$	SR4,(316)	

(sym):

$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(t_A =_{\overline{A}} s_A)$	By Assumption	(317)
$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(t_A)_A =_{\overline{A}} \mathsf{sRed}\,(s_A)_A$	SR4,(317)	(318)
$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(s_A)_A =_{\overline{A}} \mathsf{sRed}\,(t_A)_A$	(sym),(318)	(319)
$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(s_A =_{\overline{A}} t_A)$	SR4,(319)	

(beta):

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(\left(\lambda x_A{:}\overline{A}.\ s_B\right)\ t_{A'}\right)_{B'} :\overline{B} \qquad \text{By Assumption} \qquad (320)$$

By Lemma 6 (6), it follows that $A = A'$. If $\mathsf{sRed}\left(\left(\lambda x_A{:}\overline{A}.\ s_B\right)\ t_A\right)_{B'}$ is almost proper with quasi-preimage of type $B \equiv B'$, then $\mathsf{sRed}\left(\left(\lambda x_A{:}\overline{A}.\ s_B\right)\ t_A\right)_{B'} = \left(\lambda x_A{:}\overline{A}.\ s_B\right)\ t_A$ and thus:

$$\Delta \vdash_{\overline{T}} \left(\lambda x_A{:}\overline{A}.\ s_B\right)\ t_A{:}\overline{B} \qquad \text{SR1},(320) \qquad (321)$$

$$\Delta \vdash_{\overline{T}} (\lambda x_A{:}\overline{A}.\ s_B)\ \ t_A =_{\overline{B}} s_B[^{x_A}/_{t_A}] \quad \text{(beta),(321)} \tag{322}$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left((\lambda x_A{:}\overline{A}.\ s_B)\ \ t_A =_{\overline{B}} s_B[^{x_A}/_{t_A}]\right) \quad \text{SR4,SR1,(322)}$$

Otherwise by SR2 and SR8,

$$\mathsf{sRed}\left((\lambda x_A{:}\overline{A}.\ s_B)\ \ t_{A'}\right) = \mathsf{sRed}\left(s_B[^{x_A}/_{t_{A'}}]\right)$$

and we yield:

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left((\lambda x_A{:}\overline{A}.\ s_B)\ \ t_{A'}\right) =_{\overline{B}} \mathsf{sRed}\left(s_B[^{x_A}/_{t_{A'}}]\right) \quad \text{(refl),above observation} \tag{323}$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left((\lambda x_A{:}\overline{A}.\ s_B)\ \ t_{A'} =_{\overline{B}} s_B[^{x_A}/_{t_{A'}}]\right) \quad \text{SR4,(323)}$$

(eta):

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(t_{\Pi x:A.\ B}\right) : \overline{A} \to \overline{B} \quad \text{By Assumption} \tag{324}$$

$$x \text{ not in } \Delta \quad \text{By Assumption} \tag{325}$$

Since $\mathsf{sRed}\left(t_{\Pi x:A.\ B}\right)$ is almost proper with quasi-preimage of type $\Pi x{:}A.\ B$, it follows that $\lambda x_A{:}\overline{A}.\ \mathsf{sRed}\left(t_{\Pi x:A.\ B}\right)\ x_A$ is also almost proper with quasi-preimage of type $\Pi x{:}A.\ B$. It follows:

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(t_{\Pi x:A.\ B}\right) =_{\overline{A}\to\overline{B}} \lambda x_A{:}\overline{A}.\ \mathsf{sRed}\left(t_{\Pi x:A.\ B}\right)\ \ x_A \quad \text{(eta),(324),(325)} \tag{326}$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(t_{\Pi x:A.\ B} =_{\overline{A}\to\overline{B}} \lambda x_A{:}\overline{A}.\ t_{\Pi x:A.\ B}\ x_A\right) \quad \text{SR2,SR6,SR4,(326)}$$

(cong$\vdash$):

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(F_{\mathsf{bool}} =_{\mathsf{bool}} F'_{\mathsf{bool}}\right) \quad \text{By Assumption} \tag{327}$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(F'_{\mathsf{bool}}\right) \quad \text{By Assumption} \tag{328}$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(F_{\mathsf{bool}}\right) =_{\mathsf{bool}} \mathsf{sRed}\left(F'_{\mathsf{bool}}\right) \quad \text{SR4,(327)} \tag{329}$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(F_{\mathsf{bool}}\right) \quad \text{(cong}\vdash\text{),(329),(328)}$$

($\Rightarrow$I):

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(F_{\mathsf{bool}}\right) : \mathsf{bool} \quad \text{By Assumption} \tag{330}$$

$$\Delta,\ \triangleright\mathsf{sRed}\left(F_{\mathsf{bool}}\right) \vdash_{\overline{T}} \mathsf{sRed}\left(G_{\mathsf{bool}}\right) \quad \text{By Assumption} \tag{331}$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(F_{\mathsf{bool}}\right) \Rightarrow \mathsf{sRed}\left(G_{\mathsf{bool}}\right) \quad (\Rightarrow\text{I}),(330),(331) \tag{332}$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(F_{\mathsf{bool}} \Rightarrow G_{\mathsf{bool}}\right) \quad \text{SR5,(332)}$$

($\Rightarrow$E):

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(F_{\mathsf{bool}} \Rightarrow G_{\mathsf{bool}}\right) \quad \text{By Assumption} \tag{333}$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(F_{\mathsf{bool}}\right) \quad \text{By Assumption} \tag{334}$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(F_{\mathsf{bool}}\right) \Rightarrow \mathsf{sRed}\left(G_{\mathsf{bool}}\right) \quad \text{SR5,(333)} \tag{335}$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\left(G_{\mathsf{bool}}\right) \quad (\Rightarrow\text{E}),(335),(334)$$

(boolExt):

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(p_{\mathsf{bool}\to\mathsf{bool}}\ \mathsf{true}_{\mathsf{bool}}) \quad \text{By Assumption} \quad (336)$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(p_{\mathsf{bool}\to\mathsf{bool}}\ F_{\mathsf{bool}}) \quad \text{By Assumption} \quad (337)$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(p_{\mathsf{bool}\to\mathsf{bool}})\ \mathsf{true} \quad \text{(SR2),(SR1),(336)} \quad (338)$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(p_{\mathsf{bool}\to\mathsf{bool}})\ \mathsf{false} \quad \text{(SR2),(SR1),(337)} \quad (339)$$

$$\Delta \vdash_{\overline{T}} \forall\, x{:}\mathsf{bool}.\ \mathsf{sRed}\,(p_{\mathsf{bool}\to\mathsf{bool}})\ x \quad \text{(boolExt),(338),(339)} \quad (340)$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(\forall\, x{:}\mathsf{bool}.\ p_{\mathsf{bool}\to\mathsf{bool}}\ x) \quad \text{SR4,SR6,SR2,SR1,(340)}$$

(nonempty):

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(F_{\mathsf{bool}})\,{:}\mathsf{bool} \quad \text{By Assumption} \quad (341)$$

$$\Delta,\ x_A{:}\overline{A} \vdash_{\overline{T}} \mathsf{sRed}\,(F_{\mathsf{bool}}) \quad \text{By Assumption} \quad (342)$$

$$\Delta \vdash_{\overline{T}} \mathsf{sRed}\,(F_{\mathsf{bool}}) \quad \text{(nonempty),(341),(342)}$$

D.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 9). As shown in Lemma 7, we may assume that the proof of $\overline{\Gamma} \vdash_{\overline{T}} \overline{F}$ is admissible, so it only contains almost-proper terms. Consequently, whenever an equality $s =_{\overline{A}} t$ is derivable in HOL and s', t' are the quasi-preimages of s, t respectively, it follows that it's 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 5 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 $A_1, \ldots, A_n$, validity assumptions (assumptions that are validity statements) $V_1, \ldots, V_m$, non-judgement assumptions (meaning assumptions that something occurs in a context or theory) $N_1, \ldots, N_p$ 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 $\overline{F}$ is an axiom in $\overline{T}$, 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 (congλ), (eta), (congAppl), (cong$\vdash$), (beta), (refl), (sym), (assume), (axiom), ($\Rightarrow$I), ($\Rightarrow$E), (boolExt) and (nonempty).

(congλ): 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

$$\overline{\Gamma} \vdash_{\overline{T}} \forall x{:}\overline{A}.\ \forall y{:}\overline{A}.\ A^*\ x\ y \Rightarrow B^*\ \tilde{t}\ \ x\ \widetilde{t'}\ \ y$$

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.

$\Gamma \vdash_{T} \lambda x{:}A.\ t{:}\Pi x{:}A.\ B$	see above	(343)
$\Gamma \vdash_{T} \lambda x{:}A.\ t'{:}\Pi x{:}A.\ B$	see above	(344)
$\Gamma,\ y{:}A \vdash_{T} (\lambda x{:}A.\ t)\ \ y{:}B$	(appl),(var⊢),(343),(assume)	(345)
$\Gamma,\ y{:}A \vdash_{T} (\lambda x{:}A.\ t')\ \ y{:}B$	(appl),(var⊢),(344),(assume)	(346)
$\Gamma,\ y{:}A \vdash_{T} (\lambda x{:}A.\ t)\ \ y =_{B} t[^{x}/_{y}]$	(beta),(345)	(347)
$\Gamma,\ y{:}A \vdash_{T} (\lambda x{:}A.\ t')\ \ y =_{B} t'[^{x}/_{y}]$	(beta),(346)	(348)
$\Gamma,\ x{:}A \vdash_{T} t{:}B$	α-renaming,(cong:),(347)	(349)
$\Gamma,\ x{:}A \vdash_{T} t'{:}B$	α-renaming,(cong:),(348)	(350)
$\Gamma,\ x{:}A \vdash_{T} t =_{B} t$	(=type),(349),(350)	

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:

$\Gamma,\ x{:}A \vdash_{T} t =_{B} t'$	By Assumption	(351)
$\Gamma \vdash_{T} A\ \equiv\ A$	(≡ refl),(typingTp),(351)	(352)
$\Gamma \vdash_{T} \lambda x{:}A.\ t =_{\Pi x:A.\ B} \lambda x{:}A.\ t'$	(congλ'),(352)	(353)

(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

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

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:

$\Gamma \vdash_{T} t{:}\Pi x{:}A.\ B$	see above	(354)
$\Gamma \vdash_{T} t =_{\Pi x:A.\ B} \lambda x{:}A.\ t\ x$	(etaPi),(354)	

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

$$\Gamma \vdash_{\mathsf{T}} f\ t =_B f'\ t'$$

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 $\Gamma \vdash_{\mathsf{T}} f\ t{:}B$ and $\Gamma \vdash_{\mathsf{T}} f'\ t'{:}B$ in DHOL. Obviously, $\Gamma \vdash_{\mathsf{T}} t =_A t'$ and $\Gamma \vdash_{\mathsf{T}} f =_{\Pi x:A.\ B} f'$ 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 $\Gamma \vdash_{\mathsf{T}} t =_A t'$ and $\Gamma \vdash_{\mathsf{T}} f =_{\Pi x:A.\ B} f'$ are well-formed in DHOL, so we have proven the first part of the claim.

Regarding the second part of the claim:

$$\Gamma \vdash_{\mathsf{T}} t =_A t' \qquad \text{By Assumption} \qquad (355)$$
$$\Gamma \vdash_{\mathsf{T}} f =_{\Pi x:A.\ B} f' \qquad \text{By Assumption} \qquad (356)$$
$$\Gamma \vdash_{\mathsf{T}} f\ t =_B f'\ t' \qquad \text{(congAppl),(355),(356)} \qquad (357)$$

This is what we had to show.

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

$$\Gamma \vdash_{\mathsf{T}} F$$

of the normalization

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

of the conclusion is well-formed. Thus we have $\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool}$. 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 $A = \overline{A} = \mathsf{bool}$), the induction hypothesis implies that the quasi-preimage of that assumption in which the equality is over type bool must be well-formed. Clearly, $\Gamma \vdash_{\mathsf{T}} F' =_{\mathsf{bool}} F$ and $\Gamma \vdash_{\mathsf{T}} F$ 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 $\Gamma \vdash_{\mathsf{T}} F' =_{\mathsf{bool}} F$ is well-formed. We have already seen that $\Gamma \vdash_{\mathsf{T}} F$ is well-typed. This shows the first part of the claim.

Regarding the second part:

$$\Gamma \vdash_{\mathsf{T}} F' =_{\mathsf{bool}} F \qquad \text{By Assumption} \qquad (358)$$
$$\Gamma \vdash_{\mathsf{T}} F' \qquad \text{By Assumption} \qquad (359)$$
$$\Gamma \vdash_{\mathsf{T}} F \qquad \text{(cong⊢),(358),(359)}$$

(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

$$\Gamma \vdash_{\mathsf{T}} (\lambda x{:}A.\ s)\ t =_{\Pi_{x:A.\ B}} s[x/t]$$

of the normalization

$$\overline{\Gamma} \vdash_{\overline{T}} B^*\ (\lambda x{:}\overline{A}.\ \tilde{s})\ \tilde{t}\ \ \tilde{s}\,[x/\tilde{t}\,]$$

of the conclusion is well-formed. By rule (eqTyping), we obtain $\Gamma \vdash_{\mathsf{T}} (\lambda x{:}A.\ s)\ t{:}B$ in DHOL. Clearly, $\Gamma \vdash_{\mathsf{T}} (\lambda x{:}A.\ s)\ t{:}B$ 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:

$$\Gamma \vdash_{\mathsf{T}} (\lambda x{:}A.\ s)\ t{:}B \qquad \text{see above} \qquad (360)$$

$$\Gamma \vdash_{\mathsf{T}} (\lambda x{:}A.\ s)\ t =_{\Pi_{x:A.\ B}} s[x/t] \qquad \text{(beta),(360)}$$

(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

$$\Gamma \vdash_{\mathsf{T}} t =_A t'$$

of the normalization

$$\overline{\Gamma} \vdash_{\overline{T}} A^*\ \tilde{t}\ \ \tilde{t}$$

of the conclusion is well-formed. By Lemma 5 it follows that t and t' are identical so the quasi-preimage is $\Gamma \vdash_{\mathsf{T}} =_A t$. By rule (eqTyping), we obtain $\Gamma \vdash_{\mathsf{T}} t{:}A$ in DHOL, the quasi-preimage of the assumption of the rule.

Regarding the second part of the claim:

$$\Gamma \vdash_{\mathsf{T}} t{:}A \qquad \text{see above} \qquad (361)$$

$$\Gamma \vdash_{\mathsf{T}} t =_A t \qquad \text{(refl),(361)}$$

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

$$\Gamma \vdash_{\mathsf{T}} t =_A s$$

of the normalization

$$\overline{\Gamma} \vdash_{\overline{T}} A^*\ \tilde{t}\ \ \tilde{s}$$

of the conclusion is well-formed. By the rules (eqTyping) and (sym) both $\Gamma \vdash_{\mathsf{T}} t{:}A$ and $\Gamma \vdash_{\mathsf{T}} s{:}A$ follow. By rule (=type) it follows that $\Gamma \vdash_{\mathsf{T}} s =_A t$ is well-formed. Clearly, $\Gamma \vdash_{\mathsf{T}} s =_A t$ is the quasi-preimages of the validity assumption, so we have proven the first part of the claim.

Regarding the second part:

$$\Gamma \vdash_{\mathsf{T}} t =_A s \qquad \text{By Assumption} \qquad (362)$$
$$\Gamma \vdash_{\mathsf{T}} s =_A t \qquad \text{(sym),(362)} \qquad (363)$$

(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

$$\Gamma \vdash_{\mathsf{T}} F$$

of the normalization

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

of the conclusion is well-formed and thus $\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool}$.

$$\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool} \qquad \text{see above} \qquad (364)$$
$$\Gamma \vdash_{\mathsf{T}} \mathsf{bool}\ \mathsf{tp} \qquad \text{(typingTp),(364)} \qquad (365)$$
$$\vdash_{\mathsf{T}} \Gamma\ \mathsf{Ctx} \qquad \text{(tpCtx),(365)} \qquad (366)$$

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 Γ. In that case, the second part of the claim $\Gamma \vdash_{\mathsf{T}} F$ can be concluded as follows:

$$\Gamma \vdash_{\mathsf{T}} x{:}A \qquad \text{(var')} \qquad (367)$$
$$\Gamma \vdash_{\mathsf{T}} x =_A t \qquad \text{(refl),(367)} \qquad (368)$$
$$\Gamma \vdash_{\mathsf{T}} F \qquad \text{By Assumption } F = A^*\ x\ x\text{,(368)}$$

Otherwise:

$$\triangleright F \text{ in } \Gamma \qquad \text{By Assumption} \qquad (369)$$
$$\Gamma \vdash_{\mathsf{T}} F \qquad \text{(assume),(369),(366)}$$

(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

$$\Gamma \vdash_{\mathsf{T}} F$$

of the normalization

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

of the conclusion is well-formed and thus $\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool}$.

$$\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool} \qquad \text{see above} \qquad (370)$$

$$\Gamma \vdash_{\mathsf{T}} \mathsf{bool}\ \mathsf{tp} \qquad \text{(typingTp),(370)} \tag{371}$$
$$\vdash_{\mathsf{T}} \Gamma\ \mathsf{Ctx} \qquad \text{(tpCtx),(371)} \tag{372}$$

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:

$$\triangleright F \text{ in } T \qquad \text{By Assumption} \tag{373}$$
$$\Gamma \vdash_{\mathsf{T}} F \qquad \text{(axiom),(373),(372)}$$

If the axiom is a typing axiom then its preimage states that some constant c of type A satisfies $\mathsf{c} =_A t$ 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.

(⇒I): Since the conclusion is proper, it follows that the preimage

$$\Gamma \vdash_{\mathsf{T}} F \Rightarrow G$$

of the normalization

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

of the conclusion is well-formed and thus $\Gamma \vdash_{\mathsf{T}} F \Rightarrow G{:}\mathsf{bool}$.

$$\Gamma \vdash_{\mathsf{T}} F \Rightarrow G{:}\mathsf{bool} \qquad \text{see above} \tag{374}$$
$$\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool} \qquad \text{(implTypingL),(374)} \tag{375}$$
$$\Gamma \vdash_{\mathsf{T}} G{:}\mathsf{bool} \qquad \text{(implTypingR),(374)} \tag{376}$$
$$\Gamma,\ \triangleright F \vdash_{\mathsf{T}} G{:}\mathsf{bool} \qquad \text{(monotonic}\vdash\text{),(376)}$$

Obviously $\Gamma,\ \triangleright F \vdash_{\mathsf{T}} G$ is a quasi-preimage of the validity assumption of the rule, so the first part of the claim is proven.

Regarding the second part:

$$\Gamma,\ \triangleright F \vdash_{\mathsf{T}} G \qquad \text{By Assumption} \tag{377}$$
$$\Gamma \vdash_{\mathsf{T}} F \Rightarrow G \qquad \text{(⇒I),(375),(377)}$$

(⇒E): Since the conclusion is proper, it follows that the preimage

$$\Gamma \vdash_{\mathsf{T}} G$$

of the normalization

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

of the conclusion is well-formed and thus $\Gamma \vdash_{\mathsf{T}} G{:}\mathsf{bool}$.

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. $\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool}$.

$$\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool} \qquad \widetilde{F} \text{ almost proper} \tag{378}$$
$$\Gamma \vdash_{\mathsf{T}} G{:}\mathsf{bool} \qquad \text{see above} \tag{379}$$
$$\Gamma \vdash_{\mathsf{T}} F \Rightarrow G{:}\mathsf{bool} \qquad (\Rightarrow\text{type'}),(378),(379)$$

Clearly, $\Gamma \vdash_{\mathsf{T}} F \Rightarrow G$ and $\Gamma \vdash_{\mathsf{T}} F$ 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:

$$\Gamma \vdash_{\mathsf{T}} F \Rightarrow G \qquad \text{By Assumption} \tag{380}$$
$$\Gamma \vdash_{\mathsf{T}} F \qquad \text{By Assumption} \tag{381}$$
$$\Gamma \vdash_{\mathsf{T}} G \qquad (\Rightarrow\text{E}),(380),(381)$$

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

$$\Gamma \vdash_{\mathsf{T}} \forall\, x{:}\mathsf{bool}.\ p\ x$$

of the normalization

$$\overline{\Gamma} \vdash_{\overline{T}} \forall\, x{:}\mathsf{bool}.\ \forall\, y{:}\mathsf{bool}.\ \mathsf{bool}^*\ x\ y \Rightarrow \mathsf{bool}^*\ \ (\lambda x{:}\mathsf{bool}.\ \mathsf{true})\ \ x\ \widetilde{\mathrm{p}}\ y$$

of the conclusion is well-formed and thus $\Gamma \vdash_{\mathsf{T}} \forall\, x{:}\mathsf{bool}.\ p\ x{:}\mathsf{bool}$. Expanding the definition of $\forall$ yields:

$$\Gamma \vdash_{\mathsf{T}} \lambda x{:}\mathsf{bool}.\ \mathsf{true} =_{\Pi x:\mathsf{bool}.\ \mathsf{bool}} \lambda x{:}\mathsf{bool}.\ p\ x{:}\mathsf{bool} \qquad \text{see above} \tag{382}$$
$$\Gamma \vdash_{\mathsf{T}} \lambda x{:}\mathsf{bool}.\ p\ x{:}\Pi x{:}\mathsf{bool}.\ \mathsf{bool} \qquad (\text{eqTyping}),(\text{sym}),(382) \tag{383}$$
$$\Gamma \vdash_{\mathsf{T}} (\lambda x{:}\mathsf{bool}.\ p\ x)\ \ \mathsf{true}{:}\mathsf{bool} \qquad (\text{appl}),(383) \tag{384}$$
$$\Gamma \vdash_{\mathsf{T}} (\lambda x{:}\mathsf{bool}.\ p\ x)\ \ F{:}\mathsf{bool} \qquad (\text{appl}),(383) \tag{385}$$
$$\Gamma \vdash_{\mathsf{T}} p\ \mathsf{true} =_{\mathsf{bool}} (\lambda x{:}\mathsf{bool}.\ p\ x)\ \ \mathsf{true} \qquad (\text{sym}),(\text{beta}),(384) \tag{386}$$
$$\Gamma \vdash_{\mathsf{T}} p\ \mathsf{false} =_{\mathsf{bool}} (\lambda x{:}\mathsf{bool}.\ p\ x)\ \ \mathsf{false} \qquad (\text{sym}),(\text{beta}),(385) \tag{387}$$
$$\Gamma \vdash_{\mathsf{T}} p\ \mathsf{true}{:}\mathsf{bool} \qquad (\text{eqTyping}),(386)$$
$$\Gamma \vdash_{\mathsf{T}} p\ F{:}\mathsf{bool} \qquad (\text{eqTyping}),(387)$$

Since $\Gamma \vdash_{\mathsf{T}} p$ true and $\Gamma \vdash_{\mathsf{T}} p$ 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:

$$\Gamma \vdash_{\mathsf{T}} p\ \mathsf{true} \qquad \text{By Assumption} \tag{388}$$
$$\Gamma \vdash_{\mathsf{T}} p\ \mathsf{false} \qquad \text{By Assumption} \tag{389}$$
$$\Gamma \vdash_{\mathsf{T}} \forall\, x{:}\mathsf{bool}.\ p\ x \qquad (\text{boolExt}),(388),(389) \tag{390}$$

(nonempty): Since the conclusion is well-formed, it follows that the preimage $\Gamma \vdash_{\mathsf{T}} F$ of the normalization

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

of the conclusion is well-formed. This also implies that $\Gamma,\ x : A \vdash_{\mathsf{T}} F : \mathsf{bool}$. Regarding the second part: By choice of the type indices (last property in Lemma 6) we know that the type A is non-empty in DHOL (this choice is possible since T is partially inhabited), so there is some term t with $\Gamma \vdash_{\mathsf{T}} t : A$.

$\Gamma,\ x : A \vdash_{\mathsf{T}} F$	By Assumption	(391)
$\Gamma \vdash_{\mathsf{T}} t : A$	By Assumption	(392)
$\Gamma \vdash_{\mathsf{T}} \forall\, x{:}A.\ F$	(∀I),(391)	(393)
$\Gamma \vdash_{\mathsf{T}} F$	(∀E),(393),(392)	

Theories and contexts:

$$\frac{}{\vdash \circ\ \mathsf{Thy}}\text{thyEmpty} \qquad \frac{\vdash T\ \mathsf{Thy}}{\vdash T,\ A\ \mathsf{tp}\ \mathsf{Thy}}\text{thyType} \qquad \frac{\vdash_{\mathsf{T}} A\ \mathsf{tp}}{\vdash T,\ \mathsf{c}{:}A\ \mathsf{Thy}}\text{thyConst} \qquad \frac{\vdash_{\mathsf{T}} F{:}\mathsf{bool}}{\vdash T,\ \triangleright F\ \mathsf{Thy}}\text{thyAxiom}$$

$$\frac{\vdash T\ \mathsf{Thy}}{\vdash_{\mathsf{T}} .\ \mathsf{Ctx}}\text{ctxEmpty} \qquad \frac{\Gamma \vdash_{\mathsf{T}} A\ \mathsf{tp}}{\vdash_{\mathsf{T}} \Gamma,\ x{:}A\ \mathsf{Ctx}}\text{ctxVar} \qquad \frac{\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool}}{\vdash_{\mathsf{T}} \Gamma,\ \triangleright F\ \mathsf{Ctx}}\text{ctxAssume}$$

Lookup in theory and context:

$$\frac{A{:}\mathsf{tp}\ \text{in}\ T \qquad \vdash_{\mathsf{T}} \Gamma\ \mathsf{Ctx}}{\Gamma \vdash_{\mathsf{T}} A\ \mathsf{tp}}\text{type} \qquad \frac{\mathsf{c}{:}A'\ \text{in}\ T \qquad \Gamma \vdash_{\mathsf{T}} A' \equiv A}{\Gamma \vdash_{\mathsf{T}} \mathsf{c}{:}A}\text{const} \qquad \frac{\triangleright F\ \text{in}\ T \qquad \vdash_{\mathsf{T}} \Gamma\ \mathsf{Ctx}}{\Gamma \vdash_{\mathsf{T}} F}\text{axiom}$$

$$\frac{x{:}A'\ \text{in}\ \Gamma \qquad \Gamma \vdash_{\mathsf{T}} A' \equiv A}{\Gamma \vdash_{\mathsf{T}} x{:}A}\text{var} \qquad \frac{\triangleright F\ \text{in}\ \Gamma \qquad \vdash_{\mathsf{T}} \Gamma\ \mathsf{Ctx}}{\Gamma \vdash_{\mathsf{T}} F}\text{assume}$$

Well-formedness and equality of types:

$$\frac{\vdash_{\mathsf{T}} \Gamma\ \mathsf{Ctx}}{\Gamma \vdash_{\mathsf{T}} \mathsf{bool}\ \mathsf{tp}}\text{bool} \qquad \frac{\Gamma \vdash_{\mathsf{T}} A\ \mathsf{tp} \qquad \Gamma \vdash_{\mathsf{T}} B\ \mathsf{tp}}{\Gamma \vdash_{\mathsf{T}} A \to B\ \mathsf{tp}}\text{arrow}$$

$$\frac{\Gamma\ \mathsf{Ctx} \qquad \mathsf{a} : \mathsf{tp}\ \text{in}\ T}{\Gamma \vdash_{\mathsf{T}} A \equiv A}\text{congBase} \qquad \frac{\vdash_{\mathsf{T}} \Gamma\ \mathsf{Ctx}}{\Gamma \vdash_{\mathsf{T}} \mathsf{bool} \equiv \mathsf{bool}}\text{congbool} \qquad \frac{\Gamma \vdash_{\mathsf{T}} A \equiv A' \qquad \Gamma \vdash_{\mathsf{T}} B \equiv B'}{\Gamma \vdash_{\mathsf{T}} A \to B \equiv A' \to B'}\text{cong}\to$$

Typing:

$$\frac{\Gamma,\ x{:}A \vdash_{\mathsf{T}} t{:}B}{\Gamma \vdash_{\mathsf{T}} (\lambda x{:}A.\ t){:}A \to B}\text{lambda} \qquad \frac{\Gamma \vdash_{\mathsf{T}} f{:}A \to B \qquad \Gamma \vdash_{\mathsf{T}} t{:}A}{\Gamma \vdash_{\mathsf{T}} f\ t{:}B}\text{appl} \qquad \frac{\Gamma \vdash_{\mathsf{T}} s{:}A \qquad \Gamma \vdash_{\mathsf{T}} t{:}A}{\Gamma \vdash_{\mathsf{T}} s =_A t{:}\mathsf{bool}}{=}\text{type}$$

Term equality, congruence, reflexivity, symmetry, β, η:

$$\frac{\Gamma \vdash_{\mathsf{T}} A \equiv A' \qquad \Gamma,\ x{:}A \vdash_{\mathsf{T}} t =_B t'}{\Gamma \vdash_{\mathsf{T}} \lambda x{:}A.\ t =_{A \to B} \lambda x{:}A'.\ t'}\text{cong}\lambda\ \text{(xi)} \qquad \frac{\Gamma \vdash_{\mathsf{T}} t =_A t' \qquad \Gamma \vdash_{\mathsf{T}} f =_{A \to B} f'}{\Gamma \vdash_{\mathsf{T}} f\ t =_B f'\ t'}\text{congAppl}$$

$$\frac{\Gamma \vdash_{\mathsf{T}} t{:}A}{\Gamma \vdash_{\mathsf{T}} t =_A t}\text{refl} \qquad \frac{\Gamma \vdash_{\mathsf{T}} t =_A s}{\Gamma \vdash_{\mathsf{T}} s =_A t}\text{sym} \qquad \frac{\Gamma \vdash_{\mathsf{T}} (\lambda x{:}A.\ s)\ t{:}B}{\Gamma \vdash_{\mathsf{T}} (\lambda x{:}A.\ s)\ t =_B s[{}^{x}/_{t}]}\text{beta} \qquad \frac{\Gamma \vdash_{\mathsf{T}} t{:}A \to B \qquad x\ \text{not in}\ \Gamma}{\Gamma \vdash_{\mathsf{T}} t =_{A \to B} \lambda x{:}A.\ t\ x}\text{eta}$$

Rules for implication:

$$\frac{\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool} \qquad \Gamma \vdash_{\mathsf{T}} G{:}\mathsf{bool}}{\Gamma \vdash_{\mathsf{T}} F \Rightarrow G{:}\mathsf{bool}}{\Rightarrow}\text{type} \qquad \frac{\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool} \qquad \Gamma,\ \triangleright F \vdash_{\mathsf{T}} G}{\Gamma \vdash_{\mathsf{T}} F \Rightarrow G}{\Rightarrow}\text{I} \qquad \frac{\Gamma \vdash_{\mathsf{T}} F \Rightarrow G \qquad \Gamma \vdash_{\mathsf{T}} F}{\Gamma \vdash_{\mathsf{T}} G}{\Rightarrow}\text{E}$$

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

$$\frac{\Gamma \vdash_{\mathsf{T}} F =_{\mathsf{bool}} F' \qquad \Gamma \vdash_{\mathsf{T}} F'}{\Gamma \vdash_{\mathsf{T}} F}\text{cong}\vdash \qquad \frac{\Gamma \vdash_{\mathsf{T}} p\ \mathsf{true} \qquad \Gamma \vdash_{\mathsf{T}} p\ \mathsf{false}}{\Gamma,\ x{:}\mathsf{bool} \vdash_{\mathsf{T}} p\ x}\text{boolExt} \qquad \frac{\Gamma \vdash_{\mathsf{T}} F{:}\mathsf{bool} \qquad \Gamma,\ x{:}A \vdash_{\mathsf{T}} F}{\Gamma \vdash_{\mathsf{T}} F}\text{nonempty}$$

In the soundness proof, we will occasionally use the existence of a HOL term of given type A (whose existence follows from rule (nonempty)), so we denote this term by w_A.

Fig. 4. HOL Rules