

# Soundness of the Q0 proof system for higher-order logic

Anders Schlichtkrull

## Abstract

This entry formalizes the Q0 proof system for higher-order logic (also known as simple type theory) from the book “An Introduction to Mathematical Logic and Type Theory: To Truth Through Proof” by Peter B. Andrews [And13] together with the system’s soundness. Most of the used theorems and lemmas are also from his book. The soundness proof is with respect to general models and as a consequence also holds for standard models. Higher-order logic is given a semantics by porting to Isabelle/HOL the specification of set theory from the CakeML project [KAMO14, KAMO16]. The independently developed AFP entry “Metatheory of Q0” by Javier Díaz [Día23] also formalizes Q0 in Isabelle/HOL. I highly recommend the reader to also take a look at his formalization!

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Set Theory</b>	<b>3</b>
2.1	CakeML License . . . . .	3
2.2	Set theory specification . . . . .	3
<b>3</b>	<b>Isabelle/HOLZF lives up to CakeML’s set theory specification</b>	<b>12</b>
<b>4</b>	<b>ZFC_in_HOL lives up to CakeML’s set theory specification</b>	<b>12</b>
<b>5</b>	<b>Q0 abbreviations</b>	<b>12</b>
<b>6</b>	<b>Syntax and typing</b>	<b>13</b>
<b>7</b>	<b>Replacement</b>	<b>14</b>
<b>8</b>	<b>Defined wffs</b>	<b>16</b>
8.1	Common expressions . . . . .	16
8.2	Equality symbol . . . . .	16
8.3	Description or selection operator . . . . .	16
8.4	Equality . . . . .	17
8.5	Truth . . . . .	17
8.6	Falsity . . . . .	17
8.7	Pi . . . . .	17
8.8	Forall . . . . .	18
8.9	Conjunction symbol . . . . .	18
8.10	Conjunction . . . . .	19
8.11	Implication symbol . . . . .	19
8.12	Implication . . . . .	19
<b>9</b>	<b>The Q0 proof system</b>	<b>20</b>
<b>10</b>	<b>Semantics</b>	<b>21</b>
<b>11</b>	<b>Semantics of defined wffs</b>	<b>24</b>
<b>12</b>	<b>Soundness</b>	<b>37</b>

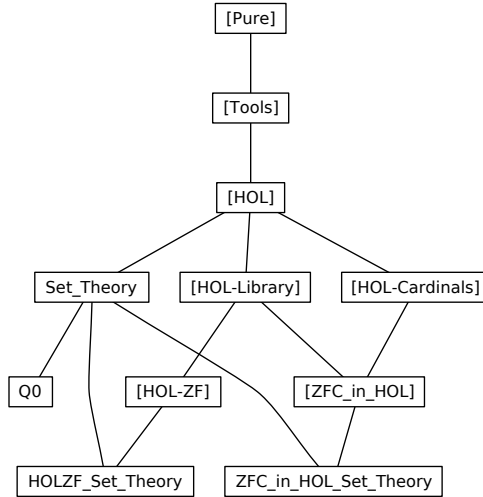


Figure 1: Theory dependency graph

## 1 Introduction

This entry formalizes the Q0 proof system for higher-order logic (also called simple type theory) and its soundness. Both the system and most of the proven lemmas and theorems are from Peter B. Andrews’ book [And13]. In the book’s chapter on type theory, Andrews explains that type theory was invented by Russell [Rus08] and that Whitehead and Russell [WR13] showed that fundamental parts of mathematics could be formalized in type theory. As influences on the type theory presented in Andrews’ chapter he mentions Church [Chu40], Henkin [Hen50, Hen63] and earlier works by himself [And63, And72]. The present Isabelle formalization of higher-order logic is given a semantics by using a port to Isabelle/HOL of CakeML’s specification of set theory [KAMO16]. The specification is formalized as a locale that fixes a type of set theoretic sets and a number of functions (powerset, union, separation) and the set membership predicate. The soundness proof is with respect to general models and as a consequence it also holds for standard models. Variables are implemented simply using named variables rather than e.g. De Bruijn indices or nominal techniques. It is well-known that named variables require the definition of substitution to rename variables, but since substitution is derived in Q0 rather than built into the proof system this complication is essentially circumvented in the present formalization. As a curiosity the present AFP entry also proves that the set theory specification is fulfilled by the sets axiomatized in Isabelle/HOLZF [Obu06] and also by the sets axiomatized by the AFP entry on Zermelo Fraenkel Set Theory in Higher-Order Logic [Pau19]. The theory files of the present entry appeared in the IsaFoL effort [Sch23].

In the literature we find other formalizations of the metatheory of higher-order logics and type theories. Independently from my work here, Javier Díaz also formalizes Q0 in Isabelle/HOL. His work is available in the AFP entry “Metatheory of Q0” [Día23]. I highly recommend the reader to take a look also at his very thorough formalization! Arthan specifies HOL [Art14a, Art14b, Art02] in ProofPower but does not prove soundness. John Harrison formalizes the soundness of the proof system of HOL Light [Har06] in HOL Light and Kumar et al. [KAMO14, KAMO16, AMKS22, AM23] formalize it in HOL4 as part of the CakeML project including also definitions and a verified implementation. Roßkopf and Nipkow [NR21a, NR21b, RN23] formalize a proof system for terms in Isabelle’s metalogic together with an implementation of a proof checker and prove that the proof checker indeed implements this proof system. There are also a number of works using Coq to formalize metatheory of the calculus of constructions and the calculus of inductive constructions [Bar96b, Bar96a, BW96, Bar97, SBF+20]. Worth mentioning is also the formalization in Coq of second-order logic which also formalizes general models [KK22].

There are plenty of opportunities to go further with the present formalization. The present formalization proves soundness of Q0 theorems (i.e.  $\vdash A$  implies  $\models A$ ), but not soundness of Q0 derivability (i.e.  $M \models G$  and  $G \vdash A$  implies  $M \models A$ ). Other interesting lemmas and theorems from Andrews’ book could also be proved such as e.g. derived inference rules and completeness.

## 2 Set Theory

theory Set\_Theory imports Main begin

### 2.1 CakeML License

CakeML Copyright Notice, License, and Disclaimer.

Copyright 2013-2023 by Anthony Fox, Google LLC, Ramana Kumar, Magnus Myreen, Michael Norrish, Scott Owens, Yong Kiam Tan, and other contributors listed at <https://cakeml.org>

All rights reserved.

CakeML is free software. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

\* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

\* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

\* The names of the copyright holders and contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### 2.2 Set theory specification

This formal document is the set theory from <https://github.com/CakeML/cakeml/blob/master/candle/set-theory/set-SpecScript.sml> ported to Isabelle/HOL and extended.

```
locale set_theory =
  fixes mem :: "'s ⇒ 's ⇒ bool" (infix "∈:" 67)
  fixes sub :: "'s ⇒ ('s ⇒ bool) ⇒ 's" (infix "suchthat" 67)
  fixes pow :: "'s ⇒ 's"
  fixes uni :: "'s ⇒ 's" ("∪:_:" [900] 900)
  fixes upair :: "'s ⇒ 's ⇒ 's" (infix "+:" 67)
  assumes extensional: "∧x y. x = y ⟷ (∀a. a ∈: x ⟷ a ∈: y)"
  assumes mem_sub[simp]: "∧x P a. a ∈: (x suchthat P) ⟷ a ∈: x ∧ P a"
  assumes mem_pow[simp]: "∧x a. a ∈: (pow x) ⟷ (∀b. b ∈: a ⟶ b ∈: x)"
  assumes mem_uni[simp]: "∧x a. a ∈: ∪: x ⟷ (∃b. a ∈: b ∧ b ∈: x)"
  assumes mem_upair[simp]: "∧x y a. a ∈: (x +: y) ⟷ a = x ∨ a = y"
begin
```

```
lemma seperation_unique:
  assumes "∀x P a. a ∈: (sub2 x P) ⟷ a ∈: x ∧ P a"
  shows "sub2 = sub"
proof
  fix x
  show "sub2 x = (suchthat) x"
    using assms extensional by auto
qed
```

```
lemma pow_unique:
  assumes "∀x a. a ∈: (pow2 x) ⟷ (∀b. b ∈: a ⟶ b ∈: x)"
  shows "pow2 = pow"
```

```

using assms extensional by auto

lemma uni_unique:
  assumes " $\forall x a. a \in: \text{uni2 } x \longleftrightarrow (\exists b. a \in: b \wedge b \in: x)$ "
  shows " $\text{uni2} = \text{uni}$ "
  using assms extensional by auto

lemma upair_unique:
  assumes " $\forall x y a. a \in: \text{upair2 } x y \longleftrightarrow a = x \vee a = y$ "
  shows " $\text{upair2} = \text{upair}$ "
proof
  fix x
  show " $\text{upair2 } x = (+:) x$ "
    using assms extensional by auto
qed

definition empty :: 's ("∅") where
  "∅ = undefined suchthat ( $\lambda x. \text{False}$ )"

lemma mem_empty[simp]: " $\neg x \in: \emptyset$ "
  unfolding empty_def using mem_sub by auto

definition unit :: "'s  $\Rightarrow$  's" where
  "unit x = x +: x"

lemma mem_unit[simp]: " $x \in: (\text{unit } y) \longleftrightarrow x = y$ "
  unfolding unit_def using mem_upair by auto

lemma unit_inj: " $\text{unit } x = \text{unit } y \longleftrightarrow x = y$ "
  using extensional unfolding unit_def by auto

definition one :: 's where
  "one = unit ∅"

lemma mem_one[simp]: " $x \in: \text{one} \longleftrightarrow x = \emptyset$ "
  unfolding one_def by auto

definition two :: 's where
  "two = ∅ +: one"

lemma mem_two[simp]: " $\forall x. x \in: \text{two} \longleftrightarrow x = \emptyset \vee x = \text{one}$ "
  unfolding two_def by auto

definition pair :: "'s  $\Rightarrow$  's  $\Rightarrow$  's" (infix " ,:" 50) where
  "(x ,: y) = (unit x) +: (x +: y)"

lemma upair_inj:
  "a +: b = c +: d  $\longleftrightarrow$  a = c  $\wedge$  b = d  $\vee$  a = d  $\wedge$  b = c"
  using extensional by auto

```

```

lemma unit_eq_upair:
  "unit x = y +: z  $\longleftrightarrow$  x = y  $\wedge$  y = z"
  using extensional mem_unit mem_upair by metis

lemma pair_inj:
  "(a,:b) = (c,:d)  $\longleftrightarrow$  a = c  $\wedge$  b = d"
  using pair_def upair_inj unit_inj unit_eq_upair by metis

definition binary_uni (infix "U:" 67) where
  "x U: y =  $\bigcup$ : (x +: y)"

lemma mem_binary_uni[simp]:
  "a  $\in$ : (x U: y)  $\longleftrightarrow$  a  $\in$ : x  $\vee$  a  $\in$ : y"
  unfolding binary_uni_def by auto

definition product :: "'s  $\Rightarrow$  's  $\Rightarrow$  's" (infix "x:" 67) where
  "x x: y = (pow (pow (x U: y)) suchthat ( $\lambda$ a.  $\exists$ b c. b  $\in$ : x  $\wedge$  c  $\in$ : y  $\wedge$  a = (b,:c)))"\in: (x x: y)  $\longleftrightarrow$  ( $\exists$ b c. a = (b,:c)  $\wedge$  b  $\in$ : x  $\wedge$  c  $\in$ : y)"
  using product_def pair_def by auto

definition relspace where
  "relspace x y = pow (x x: y)"

definition funspace where
  "funspace x y =
    (relspace x y suchthat
      ( $\lambda$ f.  $\forall$ a. a  $\in$ : x  $\longrightarrow$  ( $\exists$ !b. (a,:b)  $\in$ : f)))"\Rightarrow 's  $\Rightarrow$  's" (infixl "." 68) where
  "(x.y) = (SOME a. (y,:a)  $\in$ : x)"

definition boolset where
  "boolset  $\equiv$  two"

definition true where
  "true =  $\emptyset$ "

definition false where
  "false = one"

lemma true_neq_false:
  "true  $\neq$  false"
  using true_def false_def extensional one_def by auto

lemma mem_boolset[simp]:
  "x  $\in$ : boolset  $\longleftrightarrow$  ((x = true)  $\vee$  (x = false))"
  using true_def false_def boolset_def by auto

```

```

definition boolean :: "bool  $\Rightarrow$  's" where
  "boolean b = (if b then true else false)"

lemma boolean_in_boolset:
  "boolean b  $\in$ : boolset"
  using boolean_def one_def true_def false_def by auto

lemma boolean_eq_true:
  "boolean b = true  $\longleftrightarrow$  b"
  using boolean_def true_neq_false by auto

definition "holds s x  $\longleftrightarrow$  s  $\cdot$  x = true"

definition abstract where
  "abstract doma rang f = ((doma  $\times$ : rang) suchthat ( $\lambda$ x.  $\exists$ a. x = (a, :f a)))"

lemma apply_abstract[simp]:
  "x  $\in$ : s  $\implies$  f x  $\in$ : t  $\implies$  abstract s t f  $\cdot$  x = f x"
  using apply_def abstract_def pair_inj by auto

lemma apply_abstract_matchable:
  "x  $\in$ : s  $\implies$  f x  $\in$ : t  $\implies$  f x = u  $\implies$  abstract s t f  $\cdot$  x = u"
  using apply_abstract by auto

lemma apply_in_rng:
  assumes "x  $\in$ : s"
  assumes "f  $\in$ : funspace s t"
  shows "f  $\cdot$  x  $\in$ : t"
proof -
  from assms have "f  $\in$ : (relspace s t suchthat ( $\lambda$ f.  $\forall$ a. a  $\in$ : s  $\longrightarrow$  ( $\exists!$ b. (a, : b)  $\in$ : f)))"
  unfolding funspace_def by auto
  then have f_p: "f  $\in$ : relspace s t  $\wedge$  ( $\forall$ a. a  $\in$ : s  $\longrightarrow$  ( $\exists!$ b. (a, : b)  $\in$ : f))"
  by auto
  then have fxf: "(x, : f  $\cdot$  x)  $\in$ : f"
  using someI assms apply_def by metis
  from f_p have "f  $\in$ : pow (s  $\times$ : t)"
  unfolding relspace_def by auto
  then have "(x, : f  $\cdot$  x)  $\in$ : (s  $\times$ : t)"
  using fxf by auto
  then show ?thesis
  using pair_inj by auto
qed

lemma abstract_in_funspace[simp]:
  " $(\forall$ x. x  $\in$ : s  $\longrightarrow$  f x  $\in$ : t)  $\implies$  abstract s t f  $\in$ : funspace s t"
  using funspace_def relspace_def abstract_def pair_inj by auto

lemma abstract_in_funspace_matchable:
  " $(\forall$ x. x  $\in$ : s  $\longrightarrow$  f x  $\in$ : t)  $\implies$  fs = funspace s t  $\implies$  abstract s t f  $\in$ : fs"
  using abstract_in_funspace by auto

lemma abstract_eq:
  assumes " $\forall$ x. x  $\in$ : s  $\longrightarrow$  f x  $\in$ : t1  $\wedge$  g x  $\in$ : t2  $\wedge$  f x = g x"
  shows "abstract s t1 f = abstract s t2 g"

```

```

proof (rule iffD2[OF extensional], rule)
  fix a
  from assms show "a ∈: abstract s t1 f = a ∈: abstract s t2 g"
    unfolding abstract_def using pair_inj by auto
qed

lemma abstract_extensional:
  assumes "∀x. x ∈: s ⟶ f x ∈: t ∧ f x = g x"
  shows "abstract s t f = abstract s t g"
proof (rule iffD2[OF extensional], rule)
  fix a
  from assms show "a ∈: abstract s t f = a ∈: abstract s t g"
    unfolding abstract_def using pair_inj by auto
qed

lemma abstract_extensional':
  assumes "∧x. x ∈: s ⟹ f x ∈: t"
  assumes "∧x. x ∈: s ⟹ f x = g x"
  shows "abstract s t f = abstract s t g"
proof (rule iffD2[OF extensional], rule)
  fix a
  from assms show "a ∈: abstract s t f = a ∈: abstract s t g"
    unfolding abstract_def using pair_inj by auto
qed

lemma abstract_cong:
  assumes "∀x. x ∈: s ⟶ f x ∈: t ∧ g x ∈: t"
  assumes "abstract s t f = abstract s t g"
  assumes "x ∈: s"
  shows "f x = g x"
  using assms
  by (metis apply_abstract_matchable)

lemma abstract_cong_specific:
  assumes "x ∈: s"
  assumes "f x ∈: t"
  assumes "abstract s t f = abstract s t g"
  assumes "g x ∈: t"
  shows "f x = g x"
proof -
  have "f x = abstract s t f · x"
    using apply_abstract[of x s f t]
    using assms by auto
  also have "... = abstract s t g · x"
    using assms by auto
  also have "... = g x"
    using apply_abstract[of x s g t]
    using assms by auto
  finally show ?thesis
    by auto
qed

lemma abstract_iff_extensional:
  assumes "∀x. x ∈: s ⟶ f x ∈: t ∧ g x ∈: t"
  shows "(abstract s t f = abstract s t g) ⟷ (∀x. x ∈: s ⟶ f x ∈: t ∧ f x = g x)"
  using assms abstract_cong
  abstract_extensional by meson

lemma in_funspace_abstract[simp]:
  assumes "z ∈: funspace s t"
  shows "∃f. z = abstract s t f ∧ (∀x. x ∈: s ⟶ f x ∈: t)"
proof -
  define f where "f = (λx. SOME y. (x, :y) ∈: z)"

```

```

have "∀x. x ∈: z ↔ x ∈: (abstract s t f)"
proof (rule, rule)
  fix x
  assume xz: "x ∈: z"
  moreover
  have "∀b. b ∈: z → (∃ba c. b = (ba ,: c) ∧ ba ∈: s ∧ c ∈: t)"
    using xz assms
    unfolding funspace_def relspace_def by (auto)
  moreover
  have "∀a. a ∈: s → (∃!b. (a ,: b) ∈: z)"
    using xz using assms
    unfolding funspace_def relspace_def by auto
  ultimately
  have "∃a. x = (a ,: f a)"
    using assms f_def someI_ex unfolding funspace_def relspace_def by (metis (no_types, lifting))
  then show "x ∈: abstract s t f"
    using xz assms unfolding funspace_def relspace_def abstract_def by auto
next
fix x
assume xf: "x ∈: abstract s t f"
then have "(∃b c. x = (b ,: c) ∧ b ∈: s ∧ c ∈: t)"
  unfolding abstract_def by simp
moreover
have "(∃a. x = (a ,: (SOME y. (a ,: y) ∈: z)))"
  using xf f_def unfolding abstract_def by simp
moreover
have "(∀a. a ∈: s → (∃!b. (a ,: b) ∈: z))"
  using assms unfolding funspace_def by simp
ultimately
show "x ∈: z"
  using f_def by (metis pair_inj someI_ex)
qed
then have "z = abstract s t f"
  using extensional by auto
moreover
from f_def have "∀x. x ∈: s → f x ∈: t"
  using apply_in_rng assms local.apply_def by force
ultimately
show ?thesis
  by auto
qed

```

```

theorem axiom_of_choice:
  assumes "∀a. a ∈: x → (∃b. b ∈: a)"
  shows "∃f. ∀a. a ∈: x → f · a ∈: a"
proof -
  define f where "f = (λa. SOME b. mem b a)"
  define fa where "fa = abstract x (uni x) f"

  have "∀a. a ∈: x → fa · a ∈: a"
  proof (rule, rule)
    fix a
    assume "a ∈: x"
    moreover
    have "f a ∈: ∪: x"
      by (metis (full_types) assms calculation f_def mem_uni someI_ex)
    moreover
    have "f a ∈: a"
      using assms calculation(1) f_def someI_ex by force
    ultimately
    show "fa · a ∈: a"
      unfolding fa_def using apply_abstract by auto
  qed

```



```

then show ?thesis
  by auto
qed

```

```

definition is_infinite where
  "is_infinite s = infinite {a. a ∈: s}"

```

```

lemma funspace_inhabited:
  "( $\exists x. x \in: s$ )  $\implies$  ( $\exists x. x \in: t$ )  $\implies$  ( $\exists f. f \in: \text{funspace } s \ t$ )"
  apply (rule exI[of _ "abstract s t ( $\lambda x. \text{SOME } x. x \in: t$ )"])
  using abstract_in_funspace
  using someI by metis

```

```

fun tuple where
  "tuple [] =  $\emptyset$ " |
  "tuple (a#as) = (a, : tuple as)"

```

```

lemma pair_not_empty:
  "(x, :y)  $\neq \emptyset$ "
  apply rule
  unfolding extensional using mem_empty pair_def mem_upair by metis

```

```

lemma tuple_empty:
  "tuple ls =  $\emptyset$   $\longleftrightarrow$  ls = []"
  using pair_not_empty by (cases ls) auto

```

```

lemma tuple_inj:
  "tuple l1 = tuple l2  $\longleftrightarrow$  l1 = l2"
proof (induction l1 arbitrary: l2)
  case Nil
  then show ?case
    using tuple_empty by metis
next
  case (Cons a l1)
  then show ?case
    using pair_not_empty pair_inj by (metis tuple.elims tuple.simps(2))
qed

```

```

fun bigcross where
  "bigcross [] = one" |
  "bigcross (a#as) = a  $\times$ : (bigcross as)"

```

```

lemma mem_bigcross[simp]:
  "x ∈: (bigcross ls)  $\longleftrightarrow$  ( $\exists xs. x = \text{tuple } xs \wedge \text{list\_all2 mem } xs \ ls$ )"
proof (induction ls arbitrary: x)
  case Nil
  then show ?case
    using mem_one mem_product by simp
next
  case (Cons l ls)
  show ?case
  proof
    assume "x ∈: bigcross (l # ls)"
    then obtain b c where bc_p: "x = (b, : c)  $\wedge$  b ∈: l  $\wedge$  c ∈: bigcross ls"
      by auto
    then obtain xs' where "c = tuple xs'  $\wedge$  list\_all2 ( $\in:$ ) xs' ls"

```

```

    using Cons[of c] by auto
  then have "x = tuple (b#xs')  $\wedge$  list_all2 ( $\in$ :) (b#xs') (l # ls)"
    using bc_p by auto
  then show " $\exists$ xs. x = tuple xs  $\wedge$  list_all2 ( $\in$ :) xs (l # ls)"
    by metis
next
  assume " $\exists$ xs. x = tuple xs  $\wedge$  list_all2 ( $\in$ :) xs (l # ls)"
  then obtain xs where "x = tuple xs  $\wedge$  list_all2 ( $\in$ :) xs (l # ls)"
    by auto
  then obtain xs where "x = tuple xs  $\wedge$  list_all2 ( $\in$ :) xs (l # ls)"
    by auto
  then show "x  $\in$ : bigcross (l # ls)"
    using Cons list.distinct(1) list.rel_cases mem_product by fastforce
qed
qed

definition subs :: "'s  $\Rightarrow$  's  $\Rightarrow$  bool" (infix " $\subseteq$ :" 67) where
  "x  $\subseteq$ : y  $\longleftrightarrow$  x  $\in$ : pow y"

definition one_elem_fun :: "'s  $\Rightarrow$  's  $\Rightarrow$  's" where
  "one_elem_fun x d = abstract d boolset ( $\lambda$ y. boolean (x=y))"

definition iden :: "'s  $\Rightarrow$  's" where
  "iden D = abstract D (funspace D boolset) ( $\lambda$ x. one_elem_fun x D)"

lemma apply_id[simp]:
  assumes A_in_D: "A  $\in$ : D"
  assumes B_in_D: "B  $\in$ : D"
  shows "iden D  $\cdot$  A  $\cdot$  B = boolean (A = B)"
proof -
  have abstract_D: "abstract D boolset ( $\lambda$ y. boolean (A = y))  $\in$ : funspace D boolset"
    using boolean_in_boolset by auto
  have bool_in_two: "boolean (A = B)  $\in$ : boolset"
    using boolean_in_boolset by blast
  have "(boolean (A = B)) = (abstract D boolset ( $\lambda$ y. boolean (A = y))  $\cdot$  B)"
    using apply_abstract[of B D " $\lambda$ y. boolean (A = y)" two] B_in_D bool_in_two by auto
  also
  have "... = (abstract D (funspace D boolset) ( $\lambda$ x. abstract D boolset ( $\lambda$ y. boolean (x = y)))  $\cdot$  A)  $\cdot$  B"
    using A_in_D abstract_D
    apply_abstract[of A D " $\lambda$ x. abstract D boolset ( $\lambda$ y. boolean (x = y))" "funspace D boolset"]
    by auto
  also
  have "... = iden D  $\cdot$  A  $\cdot$  B"
    unfolding iden_def one_elem_fun_def ..
  finally
  show ?thesis
    by auto
qed

lemma apply_id_true[simp]:
  assumes A_in_D: "A  $\in$ : D"
  assumes B_in_D: "B  $\in$ : D"
  shows "iden D  $\cdot$  A  $\cdot$  B = true  $\longleftrightarrow$  A = B"
  using assms using boolean_def using true_neq_false by auto

lemma apply_if_pair_in:
  assumes "(a1, : a2)  $\in$ : f"
  assumes "f  $\in$ : funspace s t"
  shows "f  $\cdot$  a1 = a2"
  using assms
  by (smt abstract_def apply_abstract mem_product pair_inj set_theory.in_funspace_abstract
    set_theory.mem_sub set_theory_axioms)

```

```

lemma funspace_app_unique:
  assumes "f ∈: funspace s t"
  assumes "(a1, : a2) ∈: f"
  assumes "(a1, : a3) ∈: f"
  shows "a3 = a2"
  using assms apply_if_pair_in by blast

lemma funspace_extensional:
  assumes "f ∈: funspace s t"
  assumes "g ∈: funspace s t"
  assumes "∀x. x ∈: s ⟶ f · x = g · x"
  shows "f = g"
proof -
  have "∧a. a ∈: f ⟹ a ∈: g"
  proof -
    fix a
    assume af: "a ∈: f"
    from af have "∃a1 a2. a1 ∈: s ∧ a2 ∈: t ∧ (a1 ,: a2) = a"
      using assms unfolding funspace_def apply_def using relspace_def by force
    then obtain a1 a2 where a12:
      "a1 ∈: s ∧ a2 ∈: t ∧ (a1 ,: a2) = a"
      by blast
    then have "∃a3. a2 ∈: t ∧ (a1 ,: a3) ∈: g"
      using assms(2) funspace_def by auto
    then obtain a3 where a3: "a2 ∈: t ∧ (a1 ,: a3) ∈: g"
      by auto
    then have "a3 = a2"
      using a12 af assms(1,2,3) apply_if_pair_in by auto
    then show "a ∈: g"
      using a12 a3 by blast
  qed
  moreover
  have "∧a. a ∈: g ⟹ a ∈: f"
  proof -
    fix a
    assume ag: "a ∈: g"
    then have "∃a1 a2. a1 ∈: s ∧ a2 ∈: t ∧ (a1 ,: a2) = a"
      using assms unfolding funspace_def apply_def using relspace_def by force
    then obtain a1 a2 where a12:
      "a1 ∈: s ∧ a2 ∈: t ∧ (a1 ,: a2) = a"
      by blast
    then have "∃a3. a2 ∈: t ∧ (a1 ,: a3) ∈: f"
      using assms(1) funspace_def by auto
    then obtain a3 where a3: "a2 ∈: t ∧ (a1 ,: a3) ∈: f"
      by auto
    then have "a3 = a2"
      using a12 ag assms(1,2,3) apply_if_pair_in by auto
    then show "a ∈: f"
      using a3 a12 by blast
  qed
  ultimately
  show ?thesis
    using iffD2[OF extensional] by metis
qed

```

```

lemma funspace_difference_witness:
  assumes "f ∈: funspace s t"
  assumes "g ∈: funspace s t"
  assumes "f ≠ g"
  shows "∃z. z ∈: s ∧ f · z ≠ g · z"
  using assms(1,2,3) funspace_extensional by blast

```

end

end

### 3 Isabelle/HOLZF lives up to CakeML's set theory specification

```
theory HOLZF_Set_Theory imports "HOL-ZF.MainZF" Set_Theory begin
```

```
interpretation set_theory Elem Sep Power Sum Upair
  using Ext Sep Power subset_def Sum Upair by unfold_locales auto
```

end

### 4 ZFC\_in\_HOL lives up to CakeML's set theory specification

```
theory ZFC_in_HOL_Set_Theory imports ZFC_in_HOL.ZFC_in_HOL Set_Theory begin
```

```
interpretation set_theory "\x y. x \in elts y" "\x::V. \P. (inv elts) ({y. y \in elts x \wedge P y})" VPow
  "(\\Y. SOME Z. elts Z = \cup (elts ' (elts Y)))" "\x y::V. (inv elts) {x, y}"
```

```
apply unfold_locales
```

```
subgoal for x y
```

```
  apply blast
```

```
  done
```

```
subgoal for x P a
```

```
  apply (rule iffI)
```

```
  subgoal
```

```
    using mem_Collect_eq set_of_elts ZFC_in_HOL.set_def subsetI small_iff smaller_than_small
```

```
    apply smt
```

```
    done
```

```
  subgoal
```

```
    using elts_0 elts_of_set empty_iff f_inv_into_f mem_Collect_eq set_of_elts small_def
```

```
    small_elts subset_eq subset_iff_less_eq_V zero_V_def
```

```
    apply (smt ZFC_in_HOL.set_def down subsetI)
```

```
    done
```

```
  done
```

```
subgoal for x a
```

```
  apply blast
```

```
  done
```

```
subgoal for x a
```

```
  apply (metis (mono_tags) UN_iff elts_Sup small_elts tfl_some)
```

```
  done
```

```
subgoal for x y a
```

```
  apply (metis ZFC_in_HOL.set_def elts_of_set insert_iff singletonD small_upair)
```

```
  done
```

```
done
```

end

### 5 Q0 abbreviations

```
theory Q0
```

```
  imports Set_Theory
```

```
  abbrevs "App" = "."
```

```
    and "Abs" = "[\_ :\_ .\_]"
```

```
    and "Eq1" = "[\_ =\_]"
```

```
    and "Con" = "\^"
```

```
    and "Forall" = "[\V\_ :\_ .\_]"
```

```
    and "Imp" = "\longrightarrow"
```

```
    and "Fun" = "\longleftarrow"
```

```
begin
```

```
lemma arg_cong3: "a = b \implies c = d \implies e = f \implies h a c e = h b d f"
```

```
  by auto
```

## 6 Syntax and typing

```

datatype type_sym =
  Ind |
  Tv |
  Fun type_sym type_sym (infixl "<=" 80)

type_synonym var_sym = string
type_synonym cst_sym = string

datatype trm =
  Var var_sym type_sym |
  Cst cst_sym type_sym |
  App trm trm (infixl "." 80) |
  Abs var_sym type_sym trm ("[ $\lambda$ :_ . _]" [80,80,80])

fun vars :: "trm  $\Rightarrow$  (var_sym * type_sym) set" where
  "vars (Var x  $\alpha$ ) = {(x, $\alpha$ )}"
| "vars (Cst _ _) = {}"
| "vars (A  $\cdot$  B) = vars A  $\cup$  vars B"
| "vars ([ $\lambda$ x: $\alpha$ . A]) = {(x, $\alpha$ )}  $\cup$  vars A"

fun frees :: "trm  $\Rightarrow$  (var_sym * type_sym) set" where
  "frees (Var x  $\alpha$ ) = {(x, $\alpha$ )}"
| "frees (Cst _ _) = {}"
| "frees (A  $\cdot$  B) = frees A  $\cup$  frees B"
| "frees ([ $\lambda$ x: $\alpha$ . A]) = frees A - {(x, $\alpha$ )}"

lemma frees_subset_vars:
  "frees A  $\subseteq$  vars A"
  by (induction A) auto

inductive wff :: "type_sym  $\Rightarrow$  trm  $\Rightarrow$  bool" where
  wff_Var: "wff  $\alpha$  (Var _  $\alpha$ )"
| wff_Cst: "wff  $\alpha$  (Cst _  $\alpha$ )"
| wff_App: "wff ( $\alpha \Leftarrow \beta$ ) A  $\Longrightarrow$  wff  $\beta$  B  $\Longrightarrow$  wff  $\alpha$  (A  $\cdot$  B)"
| wff_Abs: "wff  $\alpha$  A  $\Longrightarrow$  wff ( $\alpha \Leftarrow \beta$ ) [ $\lambda$ x: $\beta$ . A]"

fun type_of :: "trm  $\Rightarrow$  type_sym" where
  "type_of (Var x  $\alpha$ ) =  $\alpha$ "
| "type_of (Cst c  $\alpha$ ) =  $\alpha$ "
| "type_of (A  $\cdot$  B) =
  (case type_of A of  $\beta \Leftarrow \alpha \Rightarrow \beta$ )"
| "type_of [ $\lambda$ x: $\alpha$ . A] = (type_of A)  $\Leftarrow$   $\alpha$ "

lemma type_of[simp]:
  "wff  $\alpha$  A  $\Longrightarrow$  type_of A =  $\alpha$ "
  by (induction rule: wff.induct) auto

lemma wff_Var'[simp, code]:
  "wff  $\beta$  (Var x  $\alpha$ )  $\longleftrightarrow$   $\beta = \alpha$ "
  using wff.cases wff_Var by auto

lemma wff_Cst'[simp, code]:
  "wff  $\beta$  (Cst c  $\alpha$ )  $\longleftrightarrow$   $\beta = \alpha$ "
  using wff.cases wff_Cst by auto

lemma wff_App'[simp]:
  "wff  $\alpha$  (A  $\cdot$  B)  $\longleftrightarrow$  ( $\exists \beta$ . wff ( $\alpha \Leftarrow \beta$ ) A  $\wedge$  wff  $\beta$  B)"
proof
  assume "wff  $\alpha$  (A  $\cdot$  B)"
  then show " $\exists \beta$ . wff ( $\alpha \Leftarrow \beta$ ) A  $\wedge$  wff  $\beta$  B"
    using wff.cases by fastforce
next

```

```

    assume "∃β. wff (α ⇐ β) A ∧ wff β B"
    then show "wff α (A · B)"
      using wff_App by auto
qed

lemma wff_Abs'[simp]:
  "wff γ ([λx:α. A]) ↔ (∃β. wff β A ∧ γ = β ⇐ α)"
proof
  assume "wff γ [λx:α. A]"
  then show "∃β. wff β A ∧ γ = β ⇐ α"
    using wff.cases by blast
next
  assume "∃β. wff β A ∧ γ = β ⇐ α"
  then show "wff γ [λx:α. A]"
    using wff_Abs by auto
qed

lemma wff_Abs_type_of[code]:
  "wff γ [λx:α. A] ↔ (wff (type_of A) A ∧ γ = (type_of A) ⇐ α)"
proof
  assume "wff γ [λx:α. A]"
  then show "wff (type_of A) A ∧ γ = (type_of A) ⇐ α"
    using wff.cases by auto
next
  assume "wff (type_of A) A ∧ γ = (type_of A) ⇐ α"
  then show "wff γ [λx:α. A]"
    using wff_Abs by auto
qed

lemma wff_App_type_of[code]:
  "wff γ ((A · B)) ↔ (wff (type_of A) A ∧ wff (type_of B) B ∧ type_of A = γ ⇐ (type_of B))"
proof
  assume "wff γ (A · B)"
  then show "wff (type_of A) A ∧ wff (type_of B) B ∧ type_of A = γ ⇐ (type_of B)"
    by auto
next
  assume "wff (type_of A) A ∧ wff (type_of B) B ∧ type_of A = γ ⇐ (type_of B)"
  then show "wff γ (A · B)"
    by (metis wff_App')
qed

lemma unique_type:
  "wff β A ⇒ wff α A ⇒ α = β"
proof (induction arbitrary: α rule: wff.induct)
  case (wff_Var α' y)
  then show ?case
    by simp
next
  case (wff_Cst α' c)
  then show ?case
    by simp
next
  case (wff_App α' β A B)
  then show ?case
    using wff_App' by blast
next
  case (wff_Abs β A α x)
  then show ?case
    using wff_Abs_type_of by blast
qed

```

## 7 Replacement

inductive replacement :: "trm ⇒ trm ⇒ trm ⇒ trm ⇒ bool" where

```

replace: "replacement A B A B"
| replace_App_left: "replacement A B C E  $\implies$  replacement A B (C  $\cdot$  D) (E  $\cdot$  D)"
| replace_App_right: "replacement A B D E  $\implies$  replacement A B (C  $\cdot$  D) (C  $\cdot$  E)"
| replace_Abs: "replacement A B C D  $\implies$  replacement A B [ $\lambda x:\alpha.$  C] [ $\lambda x:\alpha.$  D]"

```

lemma replacement\_preserves\_type:

```

  assumes "replacement A B C D"
  assumes "wff  $\alpha$  A"
  assumes "wff  $\alpha$  B"
  assumes "wff  $\beta$  C"
  shows "wff  $\beta$  D"
  using assms
proof (induction arbitrary:  $\alpha$   $\beta$  rule: replacement.induct)
  case (replace A B)
  then show ?case
    using unique_type by auto
next
  case (replace_App_left A B C E D)
  then have " $\exists \beta'. \text{wff } (\beta \Leftarrow \beta') C$ "
    by auto
  then obtain  $\beta'$  where wff_C: "wff ( $\beta \Leftarrow \beta')$  C"
    by auto
  then have e: "wff ( $\beta \Leftarrow \beta')$  E"
    using replace_App_left by auto
  define  $\alpha'$  where " $\alpha' = \beta \Leftarrow \beta'$ "
  have "wff  $\beta'$  D"
    using wff_C unique_type replace_App_left.prem3 by auto
  then have "wff  $\beta$  (E  $\cdot$  D)"
    using e by auto
  then show ?case
    by auto
next
  case (replace_App_right A B D E C)
  have " $\exists \beta'. \text{wff } (\beta \Leftarrow \beta') C$ "
    using replace_App_right.prem3 by auto
  then obtain  $\beta'$  where wff_C: "wff ( $\beta \Leftarrow \beta')$  C"
    by auto
  have wff_E: "wff  $\beta'$  E"
    using wff_C unique_type replace_App_right by fastforce
  define  $\alpha'$  where " $\alpha' = \beta \Leftarrow \beta'$ "
  have "wff  $\beta$  (C  $\cdot$  E)"
    using wff_C wff_E by auto
  then show ?case
    using  $\alpha'$  by auto
next
  case (replace_Abs A B C D x  $\alpha'$ )
  then have " $\exists \beta'. \text{wff } \beta' D$ "
    by auto
  then obtain  $\beta'$  where wff_D: "wff  $\beta' D$ "
    by auto
  have  $\beta$ : " $\beta = \beta' \Leftarrow \alpha'$ "
    using wff_D unique_type replace_Abs by auto
  have "wff ( $\beta' \Leftarrow \alpha'$ ) ( $[\lambda x:\alpha'. D]$ )"
    using wff_D by auto
  then show ?case
    using  $\beta$  by auto
qed

```

lemma replacement\_preserved\_type:

```

  assumes "replacement A B C D"
  assumes "wff  $\alpha$  A"
  assumes "wff  $\alpha$  B"
  assumes "wff  $\beta$  D"
  shows "wff  $\beta$  C"

```

```

using assms
proof (induction arbitrary:  $\alpha$   $\beta$  rule: replacement.induct)
  case (replace A B)
  then show ?case
    using unique_type by auto
next
  case (replace_App_left A B C E D)
  then obtain  $\gamma$  where  $\gamma$ : "wff ( $\beta \Leftarrow \gamma$ ) E  $\wedge$  wff  $\gamma$  D"
    by auto
  then have "wff ( $\beta \Leftarrow \gamma$ ) C"
    using replace_App_left by auto
  then show ?case
    using  $\gamma$  by auto
next
  case (replace_App_right A B D E C)
  then obtain  $\gamma$  where  $\gamma$ : "wff ( $\beta \Leftarrow \gamma$ ) C  $\wedge$  wff  $\gamma$  E"
    by auto
  then have "wff  $\gamma$  D"
    using replace_App_right by auto
  then show ?case
    using  $\gamma$  by auto
next
  case (replace_Abs A B C D x  $\alpha'$ )
  then obtain  $\gamma$  where "wff  $\gamma$  D"
    by auto
  then show ?case
    using unique_type replace_Abs by auto
qed

```

## 8 Defined wffs

### 8.1 Common expressions

abbreviation (input) Var\_yi (" $y_i$ ") where  
" $y_i \equiv \text{Cst } 'y'$ " Ind"

abbreviation (input) Var\_xo (" $x_o$ ") where  
" $x_o \equiv \text{Var } 'x'$ " Tv"

abbreviation (input) Var\_yo (" $y_o$ ") where  
" $y_o \equiv \text{Var } 'y'$ " Tv"

abbreviation (input) Fun\_oo (" $oo$ ") where  
" $oo \equiv \text{Tv} \Leftarrow \text{Tv}$ "

abbreviation (input) Fun\_ooo (" $ooo$ ") where  
" $ooo \equiv oo \Leftarrow \text{Tv}$ "

abbreviation (input) Var\_goo (" $g_{oo}$ ") where  
" $g_{oo} \equiv \text{Var } 'g'$ " oo"

abbreviation (input) Var\_gooo (" $g_{ooo}$ ") where  
" $g_{ooo} \equiv \text{Var } 'g'$ " ooo"

### 8.2 Equality symbol

abbreviation QQ :: "type\_sym  $\Rightarrow$  trm" ("Q") where  
" $Q \alpha \equiv \text{Cst } 'Q'$ "  $\alpha$ "

### 8.3 Description or selection operator

abbreviation  $\iota$  :: "trm" (" $\iota$ ") where  
" $\iota \equiv \text{Cst } 'i'$ " (Ind  $\Leftarrow$  (Tv  $\Leftarrow$  Ind))"



## 8.4 Equality

**definition** Eql :: "trm  $\Rightarrow$  trm  $\Rightarrow$  type\_sym  $\Rightarrow$  trm" where  
"Eql A B  $\alpha \equiv$  (Q (Tv  $\Leftarrow$   $\alpha \Leftarrow$   $\alpha$ ))  $\cdot$  A  $\cdot$  B"

**abbreviation** Eql' :: "trm  $\Rightarrow$  type\_sym  $\Rightarrow$  trm  $\Rightarrow$  trm" ("[\_ =\_ = \_]" [89]) where  
"[A = $\alpha$ = B]  $\equiv$  Eql A B  $\alpha$ "

**definition** LHS where  
"LHS EqlAB = (case EqlAB of (\_  $\cdot$  A  $\cdot$  \_)  $\Rightarrow$  A)"

**lemma** LHS\_def2[simp]: "LHS [A = $\alpha$ = B] = A"  
unfolding LHS\_def Eql\_def by auto

**definition** RHS where  
"RHS EqlAB = (case EqlAB of (\_  $\cdot$  B )  $\Rightarrow$  B)"

**lemma** RHS\_def2[simp]: "RHS ([A = $\alpha$ = B]) = B"  
unfolding RHS\_def Eql\_def by auto

**lemma** wff\_Eql[simp]:  
"wff  $\alpha$  A  $\Longrightarrow$  wff  $\alpha$  B  $\Longrightarrow$  wff Tv [A = $\alpha$ = B]"  
unfolding Eql\_def by force

**lemma** wff\_Eql\_iff[simp]:  
"wff  $\beta$  [A = $\alpha$ = B]  $\longleftrightarrow$  wff  $\alpha$  A  $\wedge$  wff  $\alpha$  B  $\wedge$   $\beta =$  Tv"  
using Eql\_def by auto

## 8.5 Truth

**definition** T :: trm where  
"T  $\equiv$  [(Q ooo) =ooo= (Q ooo)]"

**lemma** wff\_T[simp]: "wff Tv T"  
unfolding T\_def by auto

**lemma** wff\_T\_iff[simp]: "wff  $\alpha$  T  $\longleftrightarrow$   $\alpha =$  Tv"  
using unique\_type wff\_T by blast

## 8.6 Falsity

**abbreviation** F :: trm where  
"F  $\equiv$  [[ $\lambda$ 'x':Tv. T] = oo= [ $\lambda$ 'x':Tv. x<sub>o</sub>]]"

**lemma** wff\_F[simp]: "wff Tv F"  
by auto

**lemma** wff\_F\_iff[simp]: "wff  $\alpha$  F  $\longleftrightarrow$   $\alpha =$  Tv"  
using unique\_type wff\_F by blast

## 8.7 Pi

**definition** PI :: "type\_sym  $\Rightarrow$  trm" where  
"PI  $\alpha \equiv$  (Q (Tv  $\Leftarrow$  (Tv  $\Leftarrow$   $\alpha$ )  $\Leftarrow$  (Tv  $\Leftarrow$   $\alpha$ )))  $\cdot$  [ $\lambda$ 'x': $\alpha$ . T]"

**lemma** wff\_PI[simp]: "wff (Tv  $\Leftarrow$  (Tv  $\Leftarrow$   $\alpha$ )) (PI  $\alpha$ )"  
unfolding PI\_def by auto

**lemma** wff\_PI\_subterm[simp]: "wff (Tv  $\Leftarrow$   $\alpha$ ) [ $\lambda$ 'x': $\alpha$ . T]"  
by auto

**lemma** wff\_PI\_subterm\_iff[simp]:  
"wff  $\beta$  [ $\lambda$ 'x': $\alpha$ . T]  $\longleftrightarrow$   $\beta =$  (Tv  $\Leftarrow$   $\alpha$ )"  
by auto

## 8.8 Forall

definition Forall :: "string  $\Rightarrow$  type\_sym  $\Rightarrow$  trm  $\Rightarrow$  trm" ("[ $\forall$ \_:\_. \_]" [80,80,80]) where  
 "[ $\forall x:\alpha. A$ ] = (PI  $\alpha$ )  $\cdot$  [ $\lambda x:\alpha. A$ ]"

lemma wff\_Forall[simp]: "wff Tv A  $\implies$  wff Tv [ $\forall x:\alpha. A$ ]"  
 unfolding Forall\_def by force

lemma wff\_Forall\_iff[simp]: "wff  $\beta$  [ $\forall x:\alpha. A$ ]  $\longleftrightarrow$  wff Tv A  $\wedge$   $\beta =$  Tv"

proof

assume "wff  $\beta$  [ $\forall x:\alpha. A$ ]"

then show "wff Tv A  $\wedge$   $\beta =$  Tv"

by (smt Forall\_def unique\_type type\_sym.inject wff\_Abs' wff\_App' wff\_PI)

next

assume "wff Tv A  $\wedge$   $\beta =$  Tv"

then show "wff  $\beta$  [ $\forall x:\alpha. A$ ]"

unfolding Forall\_def by force

qed

## 8.9 Conjunction symbol

definition Con\_sym :: trm where

"Con\_sym  $\equiv$

[ $\lambda'x':Tv. [\lambda'y':Tv.$

[[ $\lambda'g':ooo. g_{ooo} \cdot T \cdot T$ ] =Tv  $\Leftarrow$  ooo= [ $\lambda'g':ooo. g_{ooo} \cdot x_o \cdot y_o$ ]]

]"

lemma wff\_Con\_sym[simp]: "wff ooo Con\_sym"

unfolding Con\_sym\_def by auto

lemma wff\_Con\_sym'[simp]: "wff  $\alpha$  Con\_sym  $\longleftrightarrow$   $\alpha =$  ooo"

unfolding Con\_sym\_def by auto

lemma wff\_Con\_sym\_subterm0[simp]:

"wff Tv A  $\implies$  wff Tv B  $\implies$  wff (Tv  $\Leftarrow$  ooo) [ $\lambda'g':ooo. g_{ooo} \cdot A \cdot B$ ]"

by force

lemma wff\_Con\_sym\_subterm0\_iff[simp]:

"wff  $\beta$  [ $\lambda'g':ooo. g_{ooo} \cdot A \cdot B$ ]  $\longleftrightarrow$  wff Tv A  $\wedge$  wff Tv B  $\wedge$   $\beta =$  (Tv  $\Leftarrow$  ooo)"

proof

assume wff: "wff  $\beta$  [ $\lambda'g':ooo. g_{ooo} \cdot A \cdot B$ ]"

then have "wff Tv A"

by auto

moreover

from wff have "wff Tv B"

by auto

moreover

from wff have " $\beta =$  Tv  $\Leftarrow$  ooo"

by auto

ultimately show "wff Tv A  $\wedge$  wff Tv B  $\wedge$   $\beta =$  Tv  $\Leftarrow$  ooo"

by auto

next

assume "wff Tv A  $\wedge$  wff Tv B  $\wedge$   $\beta =$  Tv  $\Leftarrow$  ooo"

then show "wff  $\beta$  [ $\lambda'g':ooo. g_{ooo} \cdot A \cdot B$ ]"

by force

qed

lemma wff\_Con\_sym\_subterm1[simp]:

"wff Tv [[ $\lambda'g':ooo. g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda'g':ooo. g_{ooo} \cdot x_o \cdot y_o$ ]]"

by auto

lemma wff\_Con\_sym\_subterm1\_iff[simp]:

"wff  $\alpha$  [[ $\lambda'g':ooo. g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda'g':ooo. g_{ooo} \cdot x_o \cdot y_o$ ]]  $\longleftrightarrow$   $\alpha =$  Tv"

using unique\_type wff\_Con\_sym\_subterm1 by blast

```
lemma wff_Con_sym_subterm2[simp]:
  "wff oo [ $\lambda$  'y':Tv. [[ $\lambda$ 'g':ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda$ 'g':ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]]]"
  by auto
```

```
lemma wff_Con_sym_subterm2_iff[simp]:
  "wff  $\alpha$  [ $\lambda$  'y':Tv. [[ $\lambda$ 'g':ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda$ 'g':ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]]]  $\longleftrightarrow$   $\alpha = oo$ "
  by auto
```

## 8.10 Conjunction

```
definition Con :: "trm  $\Rightarrow$  trm  $\Rightarrow$  trm" (infix " $\wedge$ " 80) where
  "A  $\wedge$  B = Con_sym  $\cdot$  A  $\cdot$  B"
```

```
lemma wff_Con[simp]: "wff Tv A  $\Longrightarrow$  wff Tv B  $\Longrightarrow$  wff Tv (A  $\wedge$  B)"
  unfolding Con_def by auto
```

```
lemma wff_Con_iff[simp]: "wff  $\alpha$  (A  $\wedge$  B)  $\longleftrightarrow$  wff Tv A  $\wedge$  wff Tv B  $\wedge$   $\alpha = Tv$ "
  unfolding Con_def by auto
```

## 8.11 Implication symbol

```
definition Imp_sym :: trm where
  "Imp_sym  $\equiv$  [ $\lambda$ 'x':Tv. [ $\lambda$ 'y':Tv. [ $x_o =Tv= (x_o \wedge y_o)$ ]]]"
```

```
lemma wff_Imp_sym[simp]:
  "wff ooo Imp_sym"
  unfolding Imp_sym_def by auto
```

```
lemma wff_Imp_sym_iff[simp]:
  "wff  $\alpha$  Imp_sym  $\longleftrightarrow$   $\alpha = ooo$ "
  unfolding Imp_sym_def by auto
```

```
lemma wff_Imp_sym_subterm0[simp]:
  "wff Tv ( $x_o \wedge y_o$ )"
  by auto
```

```
lemma wff_Imp_sym_subterm0_iff[simp]:
  "wff  $\alpha$  ( $x_o \wedge y_o$ )  $\longleftrightarrow$   $\alpha = Tv$ "
  by auto
```

```
lemma wff_Imp_sym_subterm1[simp]:
  "wff Tv [ $x_o =Tv= (x_o \wedge y_o)$ ]"
  by auto
```

```
lemma wff_Imp_sym_subterm1_iff[simp]:
  "wff  $\alpha$  [ $x_o =Tv= (x_o \wedge y_o)$ ]  $\longleftrightarrow$   $\alpha = Tv$ "
  using unique_type wff_Imp_sym_subterm1 by blast
```

```
lemma wff_Imp_sym_subterm2[simp]:
  "wff oo [ $\lambda$  'y':Tv. [ $x_o =Tv= (x_o \wedge y_o)$ ]]]"
  by auto
```

```
lemma wff_Imp_sym_subterm2_iff[simp]:
  "wff  $\alpha$  [ $\lambda$  'y':Tv. [ $x_o =Tv= (x_o \wedge y_o)$ ]]  $\longleftrightarrow$   $\alpha = oo$ "
  by auto
```

## 8.12 Implication

```
definition Imp :: "trm  $\Rightarrow$  trm  $\Rightarrow$  trm" (infix " $\longrightarrow$ " 80) where
  "A  $\longrightarrow$  B = Imp_sym  $\cdot$  A  $\cdot$  B"
```

```
lemma wff_Imp[simp]: "wff Tv A  $\Longrightarrow$  wff Tv B  $\Longrightarrow$  wff Tv (A  $\longrightarrow$  B)"
  unfolding Imp_def by auto
```

```
lemma wff_Imp_iff[simp]: "wff  $\alpha$  (A  $\longrightarrow$  B)  $\longleftrightarrow$  wff Tv A  $\wedge$  wff Tv B  $\wedge$   $\alpha$  = Tv"
  using Imp_def by auto
```

## 9 The Q0 proof system

```
definition axiom_1 :: trm where
  "axiom_1  $\equiv$  [( $g_{oo} \cdot T$ )  $\wedge$  ( $g_{oo} \cdot F$ )] =Tv= [ $\forall$  'x':Tv.  $g_{oo} \cdot x_o$ ]"
```

```
lemma wff_axiom_1[simp]: "wff Tv axiom_1"
  unfolding axiom_1_def by auto
```

```
definition axiom_2 :: "type_sym  $\Rightarrow$  trm" where
  "axiom_2  $\alpha$   $\equiv$ 
    [(Var 'x'  $\alpha$ ) = $\alpha$ = (Var 'y'  $\alpha$ )]  $\longrightarrow$ 
    [( $(\text{Var 'h' (Tv  $\Leftarrow$   $\alpha$ )) \cdot (\text{Var 'x'  $\alpha$ )}$ ) =Tv= ((Var 'h' (Tv  $\Leftarrow$   $\alpha$ )) \cdot (\text{Var 'y'  $\alpha$ )})]"
```

```
definition axiom_3 :: "type_sym  $\Rightarrow$  type_sym  $\Rightarrow$  trm" where
  "axiom_3  $\alpha$   $\beta$   $\equiv$ 
    [( $(\text{Var 'f' ( $\alpha$   $\Leftarrow$   $\beta$ )) = $\alpha$   $\Leftarrow$   $\beta$ = (Var 'g' ( $\alpha$   $\Leftarrow$   $\beta$ ))] =Tv=
    [ $\forall$  'x': $\beta$ . [( $(\text{Var 'f' ( $\alpha$   $\Leftarrow$   $\beta$ )) \cdot (\text{Var 'x'  $\beta$ )}$ ) = $\alpha$ = ((Var 'g' ( $\alpha$   $\Leftarrow$   $\beta$ )) \cdot (\text{Var 'x'  $\beta$ )})]]"$ 
```

```
definition axiom_4_1 :: "var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$  trm" where
  "axiom_4_1 x  $\alpha$  B  $\beta$  A  $\equiv$  [( $(\lambda x:\alpha. B) \cdot A$ ) = $\beta$ = B]"
```

```
definition axiom_4_1_side_condition :: "var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$  bool" where
  "axiom_4_1_side_condition x  $\alpha$  B  $\beta$  A  $\equiv$  ( $\exists c. B = \text{Cst } c \beta$ )  $\vee$  ( $\exists y. B = \text{Var } y \beta \wedge (x \neq y \vee \alpha \neq \beta)$ )"
```

```
definition axiom_4_2 :: "var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$  trm" where
  "axiom_4_2 x  $\alpha$  A = [( $(\lambda x:\alpha. \text{Var } x \alpha) \cdot A$ ) = $\alpha$ = A]"
```

```
definition axiom_4_3 :: "var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$ 
  type_sym  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$  trm  $\Rightarrow$  trm" where
  "axiom_4_3 x  $\alpha$  B  $\beta$   $\gamma$  C A = [( $(\lambda x:\alpha. B \cdot C) \cdot A$ ) = $\beta$ = (( $(\lambda x:\alpha. B) \cdot A$ ) \cdot (( $(\lambda x:\alpha. C) \cdot A$ )))]"
```

```
definition axiom_4_4 :: "var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$  trm" where
  "axiom_4_4 x  $\alpha$  y  $\gamma$  B  $\delta$  A = [( $(\lambda x:\alpha. [\lambda y:\gamma. B]) \cdot A$ ) = $\delta$   $\Leftarrow$   $\gamma$ = [ $\lambda y:\gamma. [\lambda x:\alpha. B] \cdot A$ ]]"
```

```
definition axiom_4_4_side_condition :: "var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$ 
bool" where
  "axiom_4_4_side_condition x  $\alpha$  y  $\gamma$  B  $\delta$  A  $\equiv$  ( $x \neq y \vee \alpha \neq \gamma$ )  $\wedge$  ( $y, \gamma \notin \text{vars } A$ )"
```

```
definition axiom_4_5 :: "var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$  trm" where
  "axiom_4_5 x  $\alpha$  B  $\delta$  A = [( $(\lambda x:\alpha. [\lambda x:\alpha. B]) \cdot A$ ) = $\delta$   $\Leftarrow$   $\alpha$ = [ $\lambda x:\alpha. B$ ]]"
```

```
definition axiom_5 where
  "axiom_5 = [( $\iota \cdot ((Q (\text{Tv} \Leftarrow \text{Ind} \Leftarrow \text{Ind})) \cdot y_i)) =\text{Ind}= y_i]"$ 
```

```
inductive axiom :: "trm  $\Rightarrow$  bool" where
  by_axiom_1:
    "axiom axiom_1"
  | by_axiom_2:
    "axiom (axiom_2  $\alpha$ )"
  | by_axiom_3:
    "axiom (axiom_3  $\alpha$   $\beta$ )"
  | by_axiom_4_1:
    "wff  $\alpha$  A  $\implies$ 
      wff  $\beta$  B  $\implies$ 
      axiom_4_1_side_condition x  $\alpha$  B  $\beta$  A  $\implies$ 
      axiom (axiom_4_1 x  $\alpha$  B  $\beta$  A)"
  | by_axiom_4_2:
    "wff  $\alpha$  A  $\implies$ 
      axiom (axiom_4_2 x  $\alpha$  A)"
  | by_axiom_4_3:
    "wff  $\alpha$  A  $\implies$ 
```

```

wff ( $\beta \Leftarrow \gamma$ ) B  $\implies$ 
wff  $\gamma$  C  $\implies$ 
axiom (axiom_4_3 x  $\alpha$  B  $\beta$   $\gamma$  C A)"
| by_axiom_4_4:
"wff  $\alpha$  A  $\implies$ 
wff  $\delta$  B  $\implies$ 
axiom_4_4_side_condition x  $\alpha$  y  $\gamma$  B  $\delta$  A  $\implies$ 
axiom (axiom_4_4 x  $\alpha$  y  $\gamma$  B  $\delta$  A)"
| by_axiom_4_5:
"wff  $\alpha$  A  $\implies$ 
wff  $\delta$  B  $\implies$ 
axiom (axiom_4_5 x  $\alpha$  B  $\delta$  A)"
| by_axiom_5:
"axiom (axiom_5)"

inductive rule_R :: "trm  $\Rightarrow$  trm  $\Rightarrow$  trm  $\Rightarrow$  bool" where
"replacement A B C D  $\implies$  rule_R C ([A = $\alpha$ = B]) D"

definition "proof" :: "trm  $\Rightarrow$  trm list  $\Rightarrow$  bool" where
"proof A p  $\longleftrightarrow$  (p  $\neq$  []  $\wedge$  last p = A  $\wedge$ 
( $\forall i < \text{length p. axiom (p ! i)}$ 
 $\vee (\exists j < i. \exists k < i. \text{rule\_R (p ! j) (p ! k) (p ! i)}))$ )"

inductive "theorem" :: "trm  $\Rightarrow$  bool" where
by_axiom: "axiom A  $\implies$  theorem A"
| by_rule_R: "theorem A  $\implies$  theorem B  $\implies$  rule_R A B C  $\implies$  theorem C"

definition axiom_4_1_variant_cst :: "var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$  trm" where
"axiom_4_1_variant_cst x  $\alpha$  c  $\beta$  A  $\equiv$  [( $\lambda x:\alpha. \text{Cst c } \beta$ ]  $\cdot$  A) = $\beta$ = (Cst c  $\beta$ )]"

definition axiom_4_1_variant_var :: "var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$  trm" where
"axiom_4_1_variant_var x  $\alpha$  y  $\beta$  A  $\equiv$  [( $\lambda x:\alpha. \text{Var y } \beta$ ]  $\cdot$  A) = $\beta$ = Var y  $\beta$ ]"

definition axiom_4_1_variant_var_side_condition :: "var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  trm  $\Rightarrow$  bool"
where
"axiom_4_1_variant_var_side_condition x  $\alpha$  y  $\beta$  A  $\equiv$  x  $\neq$  y  $\vee$   $\alpha \neq \beta$ "

```

## 10 Semantics

```

type_synonym 's frame = "type_sym  $\Rightarrow$  's"
type_synonym 's denotation = "cst_sym  $\Rightarrow$  type_sym  $\Rightarrow$  's"
type_synonym 's asg = "var_sym * type_sym  $\Rightarrow$  's"

definition agree_off_asg :: "'s asg  $\Rightarrow$  's asg  $\Rightarrow$  var_sym  $\Rightarrow$  type_sym  $\Rightarrow$  bool" where
"agree_off_asg  $\varphi$   $\psi$  x  $\alpha$   $\longleftrightarrow$  ( $\forall y \beta. (y \neq x \vee \beta \neq \alpha) \longrightarrow \varphi (y, \beta) = \psi (y, \beta)$ )"

lemma agree_off_asg_def2:
"agree_off_asg  $\psi$   $\varphi$  x  $\alpha$   $\longleftrightarrow$  ( $\exists xa. \varphi((x, \alpha) := xa) = \psi$ )"
unfolding agree_off_asg_def by force

lemma agree_off_asg_disagree_var_sym[simp]:
"agree_off_asg  $\psi$   $\varphi$  x  $\alpha$   $\implies$  x  $\neq$  y  $\implies$   $\psi(y, \beta) = \varphi(y, \beta)$ "
unfolding agree_off_asg_def by auto

lemma agree_off_asg_disagree_type_sym[simp]:
"agree_off_asg  $\psi$   $\varphi$  x  $\alpha$   $\implies$   $\alpha \neq \beta \implies \psi(y, \beta) = \varphi(y, \beta)$ "
unfolding agree_off_asg_def by auto

context set_theory

```

begin

definition wf\_frame :: "'s frame  $\Rightarrow$  bool" where

"wf\_frame D  $\longleftrightarrow$  D Tv = boolset  $\wedge$  ( $\forall \alpha \beta. D (\alpha \Leftarrow \beta) \subseteq$ : funspace (D  $\beta$ ) (D  $\alpha$ ))  $\wedge$  ( $\forall \alpha. D \alpha \neq \emptyset$ )"

definition inds :: "'s frame  $\Rightarrow$  's" where

"inds Fr = Fr Ind"

inductive wf\_interp :: "'s frame  $\Rightarrow$  's denotation  $\Rightarrow$  bool" where

"wf\_frame D  $\Longrightarrow$   
 $\forall c \alpha. I c \alpha \in$ : D  $\alpha \Longrightarrow$   
 $\forall \alpha. I \text{''Q''} (Tv \Leftarrow \alpha \Leftarrow \alpha) = \text{iden (D } \alpha) \Longrightarrow$   
(I  $\text{''i''}$  (Ind  $\Leftarrow$  (Tv  $\Leftarrow$  Ind)))  $\in$ : funspace (D (Tv  $\Leftarrow$  Ind)) (D Ind)  $\Longrightarrow$   
 $\forall x. x \in$ : D Ind  $\longrightarrow$  (I  $\text{''i''}$  (Ind  $\Leftarrow$  (Tv  $\Leftarrow$  Ind)))  $\cdot$  one\_elem\_fun x (D Ind) = x  $\Longrightarrow$   
wf\_interp D I"

definition asg\_into\_frame :: "'s asg  $\Rightarrow$  's frame  $\Rightarrow$  bool" where

"asg\_into\_frame  $\varphi$  D  $\longleftrightarrow$  ( $\forall x \alpha. \varphi (x, \alpha) \in$ : D  $\alpha$ )"

abbreviation(input) asg\_into\_interp :: "'s asg  $\Rightarrow$  's frame  $\Rightarrow$  's denotation  $\Rightarrow$  bool" where

"asg\_into\_interp  $\varphi$  D I  $\equiv$  asg\_into\_frame  $\varphi$  D"

fun val :: "'s frame  $\Rightarrow$  's denotation  $\Rightarrow$  's asg  $\Rightarrow$  trm  $\Rightarrow$  's" where

"val D I  $\varphi$  (Var x  $\alpha$ ) =  $\varphi (x, \alpha)$ "  
| "val D I  $\varphi$  (Cst c  $\alpha$ ) = I c  $\alpha$ "  
| "val D I  $\varphi$  (A  $\cdot$  B) = val D I  $\varphi$  A  $\cdot$  val D I  $\varphi$  B"  
| "val D I  $\varphi$  [ $\lambda x:\alpha. B$ ] = abstract (D  $\alpha$ ) (D (type\_of B)) ( $\lambda z. \text{val D I } (\varphi((x, \alpha) := z)) B$ )"

fun general\_model :: "'s frame  $\Rightarrow$  's denotation  $\Rightarrow$  bool" where

"general\_model D I  $\longleftrightarrow$  wf\_interp D I  $\wedge$  ( $\forall \varphi A \alpha. \text{asg\_into\_interp } \varphi$  D I  $\longrightarrow$  wff  $\alpha$  A  $\longrightarrow$  val D I  $\varphi$  A  $\in$ : D  $\alpha$ )"

fun standard\_model :: "'s frame  $\Rightarrow$  's denotation  $\Rightarrow$  bool" where

"standard\_model D I  $\longleftrightarrow$  wf\_interp D I  $\wedge$  ( $\forall \alpha \beta. D (\alpha \Leftarrow \beta) = \text{funspace (D } \beta) (D \alpha)$ )"

lemma asg\_into\_frame\_fun\_upd:

assumes "asg\_into\_frame  $\varphi$  D"  
assumes "xa  $\in$ : D  $\alpha$ "  
shows "asg\_into\_frame ( $\varphi((x, \alpha) := xa)$ ) D"  
using assms unfolding asg\_into\_frame\_def by auto

lemma asg\_into\_interp\_fun\_upd:

assumes "general\_model D I"  
assumes "asg\_into\_interp  $\varphi$  D I"  
assumes "wff  $\alpha$  A"  
shows "asg\_into\_interp ( $\varphi((x, \alpha) := \text{val D I } \varphi A)$ ) D I"  
using assms asg\_into\_frame\_fun\_upd by auto

lemma standard\_model\_is\_general\_model:

assumes "standard\_model D I"  
shows "general\_model D I"

proof -

have "wf\_interp D I"  
using assms by auto  
moreover  
have "wff  $\alpha$  A  $\Longrightarrow$  asg\_into\_interp  $\varphi$  D I  $\Longrightarrow$  val D I  $\varphi$  A  $\in$ : D  $\alpha$ " for  $\varphi \alpha A$   
proof (induction arbitrary:  $\varphi$  rule: wff.induct)  
case (wff\_Var  $\alpha$  uu)  
then show ?case  
unfolding asg\_into\_frame\_def using assms by auto  
next  
case (wff\_Cst  $\alpha$  uv)  
then show ?case  
using assms using wf\_interp.simps by auto

```

next
  case (wff_App  $\alpha$   $\beta$  A B)
  then show ?case
  using apply_in_rng assms by fastforce
next
  case (wff_Abs  $\beta$  A  $\alpha$  x)
  then show ?case
  using assms abstract_in_funspace asg_into_frame_fun_upd by force
qed
ultimately
have "general_model D I"
  unfolding general_model.simps by auto
then show "general_model D I"
  by auto
qed

```

abbreviation agree\_on\_asg :: "'s asg  $\Rightarrow$  's asg  $\Rightarrow$  var\_sym  $\Rightarrow$  type\_sym  $\Rightarrow$  bool" where  
"agree\_on\_asg  $\varphi$   $\psi$  x  $\alpha$  == ( $\varphi$  (x,  $\alpha$ ) =  $\psi$  (x,  $\alpha$ )")

```

proposition prop_5400:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "asg_into_interp  $\psi$  D I"
  assumes "wff  $\alpha$  A"
  assumes " $\forall$  (x, $\alpha$ )  $\in$  frees A. agree_on_asg  $\varphi$   $\psi$  x  $\alpha$ "
  shows "val D I  $\varphi$  A = val D I  $\psi$  A"
  using assms(4) assms(1-3,5)
proof (induction arbitrary:  $\varphi$   $\psi$  rule: wff.induct)
  case (wff_Var  $\alpha$  x)
  then show ?case by auto
next
  case (wff_Cst  $\alpha$  c)
  then show ?case by auto
next
  case (wff_App  $\alpha$   $\beta$  A B)
  show ?case
  using wff_App(1,2,5,6,7,8) wff_App(3,4)[of  $\varphi$   $\psi$ ] by auto
next
  case (wff_Abs  $\beta$  A  $\alpha$  x)
  have "abstract (D  $\alpha$ ) (D  $\beta$ ) ( $\lambda$ z. val D I ( $\varphi$ ((x,  $\alpha$ ) := z)) A) =
    abstract (D  $\alpha$ ) (D  $\beta$ ) ( $\lambda$ z. val D I ( $\psi$ ((x,  $\alpha$ ) := z)) A)"
  proof (rule abstract_extensional, rule, rule)
    fix xa
    assume "xa  $\in$ : D  $\alpha$ "
    then have "val D I ( $\varphi$ ((x,  $\alpha$ ) := xa)) A  $\in$ : D  $\beta$ "
      using wff_Abs asg_into_frame_fun_upd by auto
    moreover
    {
      have "asg_into_frame ( $\psi$ ((x,  $\alpha$ ) := xa)) D"
        using <xa  $\in$ : D  $\alpha$ > asg_into_frame_fun_upd wff_Abs by auto
      moreover
      have "asg_into_frame ( $\varphi$ ((x,  $\alpha$ ) := xa)) D"
        using <xa  $\in$ : D  $\alpha$ > asg_into_frame_fun_upd wff_Abs by auto
      moreover
      have "( $\forall$ y $\in$ frees A. ( $\varphi$ ((x,  $\alpha$ ) := xa)) y = ( $\psi$ ((x,  $\alpha$ ) := xa)) y)"
        using wff_Abs by auto
      ultimately
      have "val D I ( $\varphi$ ((x,  $\alpha$ ) := xa)) A = val D I ( $\psi$ ((x,  $\alpha$ ) := xa)) A"
        using assms wff_Abs by (smt case_prodI2)
    }
  ultimately
show "val D I ( $\varphi$ ((x,  $\alpha$ ) := xa)) A  $\in$ : D  $\beta$   $\wedge$  val D I ( $\varphi$ ((x,  $\alpha$ ) := xa)) A = val D I ( $\psi$ ((x,  $\alpha$ ) := xa)) A"
  by auto

```

```

qed
then show ?case
  using wff_Abs by auto
qed

```

```

abbreviation satisfies :: "'s frame  $\Rightarrow$  's denotation  $\Rightarrow$  's asg  $\Rightarrow$  trm  $\Rightarrow$  bool" where
  "satisfies D I  $\varphi$  A  $\equiv$  (val D I  $\varphi$  A = true)"

```

```

definition valid_in_model :: "'s frame  $\Rightarrow$  's denotation  $\Rightarrow$  trm  $\Rightarrow$  bool" where
  "valid_in_model D I A  $\equiv$  ( $\forall \varphi$ . asg_into_interp  $\varphi$  D I  $\longrightarrow$  val D I  $\varphi$  A = true)"

```

```

definition valid_general :: "trm  $\Rightarrow$  bool" where
  "valid_general A  $\equiv$   $\forall$  D I. general_model D I  $\longrightarrow$  valid_in_model D I A"

```

```

definition valid_standard :: "trm  $\Rightarrow$  bool" where
  "valid_standard A  $\equiv$   $\forall$  D I. standard_model D I  $\longrightarrow$  valid_in_model D I A"

```

## 11 Semantics of defined wffs

```

lemma lemma_5401_a:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "wff  $\alpha$  A" "wff  $\beta$  B"
  shows "val D I  $\varphi$  ([ $\lambda x:\alpha$ . B]  $\cdot$  A) = val D I ( $\varphi$ ((x, $\alpha$ ):=val D I  $\varphi$  A)) B"
proof -
  have val_A: "val D I  $\varphi$  A  $\in$ : D  $\alpha$ "
    using assms by simp
  have "asg_into_interp ( $\varphi$ ((x,  $\alpha$ ) := val D I  $\varphi$  A)) D I"
    using assms asg_into_frame_fun_upd by force
  then have val_B: "val D I ( $\varphi$ ((x,  $\alpha$ ) := val D I  $\varphi$  A)) B  $\in$ : D  $\beta$ "
    using assms by simp

  have "val D I  $\varphi$  ([ $\lambda x:\alpha$ . B]  $\cdot$  A) =
    (abstract (D  $\alpha$ ) (D  $\beta$ ) ( $\lambda z$ . val D I ( $\varphi$ ((x,  $\alpha$ ) := z)) B))  $\cdot$  val D I  $\varphi$  A"
    using assms by auto
  also
  have "... = val D I ( $\varphi$ ((x,  $\alpha$ ) := val D I  $\varphi$  A)) B"
    using apply_abstract val_A val_B by auto
  finally
  show ?thesis
    by auto
qed

```

```

lemma lemma_5401_b_variant_1:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "wff  $\alpha$  A" "wff  $\alpha$  B"
  shows "val D I  $\varphi$  ([A = $\alpha$ = B]) = (boolean (val D I  $\varphi$  A = val D I  $\varphi$  B))"
proof -
  have "val D I  $\varphi$  ([A = $\alpha$ = B]) = (I ''Q'' (Tv  $\Leftarrow$   $\alpha$   $\Leftarrow$   $\alpha$ ))  $\cdot$  val D I  $\varphi$  A  $\cdot$  val D I  $\varphi$  B"
    unfolding Eql_def by auto
  have "... = (iden (D  $\alpha$ ))  $\cdot$  val D I  $\varphi$  A  $\cdot$  val D I  $\varphi$  B"
    using assms general_model.simps wf_interp.simps by auto
  also
  have "... = boolean (val D I  $\varphi$  A = val D I  $\varphi$  B)"
    using apply_id using assms general_model.simps by blast
  finally show ?thesis
    unfolding Eql_def by simp
qed

```

```

lemma lemma_5401_b:

```



```

assumes "general_model D I"
assumes "asg_into_interp  $\varphi$  D I"
assumes "wff  $\alpha$  A" "wff  $\alpha$  B"
shows "val D I  $\varphi$  ([A = $\alpha$ = B]) = true  $\longleftrightarrow$  val D I  $\varphi$  A = val D I  $\varphi$  B"
using lemma_5401_b_variant_1[OF assms] boolean_eq_true by auto

lemma lemma_5401_b_variant_2: — Just a reformulation of lemma_5401_b's directions
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "wff  $\alpha$  A" "wff  $\alpha$  B"
  assumes "val D I  $\varphi$  A = val D I  $\varphi$  B"
  shows "val D I  $\varphi$  ([A = $\alpha$ = B]) = true"
  using assms(5) lemma_5401_b[OF assms(1,2,3,4)] by auto

lemma lemma_5401_b_variant_3: — Just a reformulation of lemma_5401_b's directions
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "wff  $\alpha$  A" "wff  $\alpha$  B"
  assumes "val D I  $\varphi$  A  $\neq$  val D I  $\varphi$  B"
  shows "val D I  $\varphi$  ([A = $\alpha$ = B]) = false"
  using assms(5) lemma_5401_b_variant_1[OF assms(1,2,3,4)] by (simp add: boolean_def)

lemma lemma_5401_c:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  shows "val D I  $\varphi$  T = true"
  using assms lemma_5401_b[OF assms(1,2)] unfolding T_def by auto

lemma lemma_5401_d:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  shows "val D I  $\varphi$  F = false"
proof -
  have "iden boolset  $\in$ : D ooo"
  using assms general_model.simps wf_interp.simps wf_frame_def by metis
  then have "(val D I  $\varphi$  [ $\lambda$ 'x'':Tv. T])  $\cdot$  false  $\neq$  (val D I  $\varphi$  [ $\lambda$ 'x'':Tv. xo])  $\cdot$  false"
  using assms wf_interp.simps wf_frame_def true_neq_false
  apply_id[of "iden boolset" "(D ooo)" "iden boolset"]
  unfolding boolean_def Eq1_def T_def by auto
  then have neqLR: "val D I  $\varphi$  [ $\lambda$ 'x'':Tv. T]  $\neq$  val D I  $\varphi$  [ $\lambda$ 'x'':Tv. xo]"
  by metis
  have "val D I  $\varphi$  F = boolean (val D I  $\varphi$  ([ $\lambda$ 'x'':Tv. T]) = val D I  $\varphi$  [ $\lambda$ 'x'':Tv. xo])"
  using lemma_5401_b_variant_1[OF assms(1,2),
  of "oo" "([ $\lambda$ 'x'':Tv. T])" "[ $\lambda$ 'x'':Tv. xo]" ] assms
  by auto
  also
  have "... = boolean False"
  using neqLR by auto
  also
  have "... = false"
  unfolding boolean_def by auto
  finally
  show ?thesis
  by auto
qed

lemma asg_into_interp_fun_upd_true:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  shows "asg_into_interp ( $\varphi$ ((x, Tv) := true)) D I"

```

```

using asg_into_interp_fun_upd[OF assms wff_T, of x] lemma_5401_c[OF assms(1,2)] by auto

lemma asg_into_interp_fun_upd_false:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  shows "asg_into_interp ( $\varphi((x, Tv) := \text{false})$ ) D I"
  using asg_into_interp_fun_upd[OF assms wff_F, of x] lemma_5401_d[OF assms] by auto

lemma lemma_5401_e_1:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  shows "(val D I  $\varphi$  Con_sym)  $\cdot$  true  $\cdot$  true = true"
proof -
  define  $\varphi'$  where " $\varphi' \equiv \varphi((x', Tv) := \text{val D I } \varphi T)$ "
  define  $\varphi''$  where " $\varphi'' \equiv \varphi((y', Tv) := \text{val D I } \varphi' T)$ "
  define  $\varphi'''$  where " $\varphi''' \equiv \lambda z. \varphi''((g', ooo) := z)$ "
  have  $\varphi'_{\text{asg\_into}}$ : "asg_into_interp  $\varphi'$  D I"
    unfolding  $\varphi'_{\text{def}}$  using asg_into_interp_fun_upd[OF assms wff_T] by blast
  have  $\varphi''_{\text{asg\_into}}$ : "asg_into_interp  $\varphi''$  D I"
    unfolding  $\varphi''_{\text{def}}$  using asg_into_interp_fun_upd[OF assms(1)  $\varphi'_{\text{asg\_into}}$  wff_T] by blast

  have "(val D I  $\varphi$  Con_sym)  $\cdot$  true  $\cdot$  true = val D I  $\varphi$  (Con_sym  $\cdot$  T  $\cdot$  T)"
    using lemma_5401_c[OF assms(1,2)] by auto
  also
  have "... = val D I  $\varphi$  ([[ $\lambda'x'$ ]:Tv. [ $\lambda'y'$ ]:Tv. [[ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]]]  $\cdot$  T  $\cdot$  T)"
    unfolding Con_sym_def by auto
  also
  have "... = (val D I  $\varphi$  ([[ $\lambda'x'$ ]:Tv. [ $\lambda'y'$ ]:Tv. [[ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]]]  $\cdot$  T))  $\cdot$  val D I  $\varphi$  T"
    by simp
  also
  have "... = (val D I ( $\varphi((x', Tv) := \text{val D I } \varphi T)$ ) ([[ $\lambda'y'$ ]:Tv. [[ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]]))  $\cdot$  val D I  $\varphi$  T"
    by (metis lemma_5401_a[OF assms(1,2)] wff_Con_sym_subterm2 wff_T)
  also
  have "... = (val D I  $\varphi'$  ([[ $\lambda'y'$ ]:Tv. [[ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]]))  $\cdot$  val D I  $\varphi$  T"
    unfolding  $\varphi'_{\text{def}}$  ..
  also
  have "... = (val D I  $\varphi'$  ([[ $\lambda'y'$ ]:Tv. [[ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]]))  $\cdot$  val D I  $\varphi'$  T"
    using  $\varphi'_{\text{asg\_into}}$  assms(2) lemma_5401_c[OF assms(1)] by auto
  also
  have "... = (val D I  $\varphi'$  ([[ $\lambda'y'$ ]:Tv. [[ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]]  $\cdot$  T))"
    by simp
  also
  have "... = (val D I ( $\varphi((y', Tv) := \text{val D I } \varphi' T)$ ) ([[ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]))"
    by (meson  $\varphi'_{\text{asg\_into}}$  assms(1) lemma_5401_a[OF assms(1)] wff_Con_sym_subterm1 wff_T)
  also
  have "... = (val D I  $\varphi''$  ([[ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]))"
    unfolding  $\varphi''_{\text{def}}$  ..
  also
  have "... = true"
proof (rule lemma_5401_b_variant_2[OF assms(1)])
  show "wff (Tv  $\Leftarrow$  ooo) [ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot T \cdot T$ "
    by auto
next
  show "wff (Tv  $\Leftarrow$  ooo) [ $\lambda'g'$ ]:ooo.  $g_{ooo} \cdot x_o \cdot y_o$ "
    by auto
next

```

```

show "asg_into_frame  $\varphi$ ' D"
  using  $\varphi$ '_asg_into by blast
next
have "val D I  $\varphi$ ' [λ'g'' : $g_{ooo} \cdot T \cdot T$ ] = abstract (D ooo) (D Tv)
  (λz. val D I ( $\varphi$ '(g'', ooo) := z))
  (gooo · T · T)"
  by (simp only: val.simps(4) type_of.simps type_sym.case)
also
have "... = abstract (D ooo) (D Tv)
  (λz. val D I ( $\varphi$ ' z) (gooo · T · T))"
  unfolding  $\varphi$ '_def ..
also
have "... = abstract (D ooo) (D Tv)
  (λz. val D I ( $\varphi$ ' z) gooo · val D I ( $\varphi$ ' z) T
  · val D I ( $\varphi$ ' z) T)"
  unfolding val.simps(3) ..
also
have "... = abstract (D ooo) (D Tv)
  (λz. val D I ( $\varphi$ ' z) gooo · true · true)"
proof (rule abstract_extensional')
  fix x
  assume "x ∈: D ooo"
  then have "val D I ( $\varphi$ ' x) (gooo · T · T) ∈: D Tv"
    using  $\varphi$ '_def  $\varphi$ '_asg_into asg_into_frame_fun_upd assms(1)
    general_model.elims(2) type_sym.inject wff_Abs_type_of wff_Con_sym_subterm0 wff_T
    by (metis wff_App wff_Var)
  then show "val D I ( $\varphi$ ' x) gooo · val D I ( $\varphi$ ' x) T ·
    val D I ( $\varphi$ ' x) T
    ∈: D Tv"
    by simp
next
  fix x
  assume "x ∈: D ooo"
  then have "val D I ( $\varphi$ ' x) T = true"
    unfolding  $\varphi$ '_def using  $\varphi$ '_asg_into asg_into_frame_fun_upd
    lemma_5401_c[OF assms(1)] by blast
  then show "val D I ( $\varphi$ ' x) gooo · val D I ( $\varphi$ ' x) T ·
    val D I ( $\varphi$ ' x) T =
    val D I ( $\varphi$ ' x) gooo · true · true" by auto
qed
also
have "... = abstract (D ooo) (D Tv)
  (λz. val D I ( $\varphi$ ' z) gooo ·
  val D I ( $\varphi$ ' z) xo · val D I ( $\varphi$ ' z) yo)"
proof (rule abstract_extensional')
  fix x
  assume x_in_D: "x ∈: D ooo"
  then have "val D I ( $\varphi$ ' x) (gooo · T · T) ∈: D Tv"
    using  $\varphi$ '_def  $\varphi$ '_asg_into asg_into_frame_fun_upd assms(1)
    general_model.elims(2) type_sym.inject wff_Abs_type_of wff_Con_sym_subterm0 wff_T
    by (metis wff_App wff_Var)
  then have "val D I ( $\varphi$ ' x) gooo · val D I ( $\varphi$ ' x) T ·
    val D I ( $\varphi$ ' x) T ∈: D Tv"
    by simp
  then show "val D I ( $\varphi$ ' x) gooo · true · true ∈: D Tv"
    by (metis  $\varphi$ '_def  $\varphi$ '_asg_into lemma_5401_c[OF assms(1)] asg_into_frame_fun_upd x_in_D)
next
  fix x
  assume x_in_D: "x ∈: D ooo"
  then have "val D I ( $\varphi$ ' x) xo = true"
    unfolding  $\varphi$ '_def  $\varphi$ '_def  $\varphi$ '_def using lemma_5401_c[OF assms(1,2)] by auto
  moreover
  from x_in_D have "val D I ( $\varphi$ ' x) yo = true"
    unfolding  $\varphi$ '_def  $\varphi$ '_def using  $\varphi$ '_asg_into lemma_5401_c[OF assms(1)] by auto

```

```

ultimately
show "val D I ( $\varphi'''$  x)  $g_{ooo} \cdot \text{true} \cdot \text{true} =$ 
  val D I ( $\varphi'''$  x)
     $g_{ooo} \cdot$ 
    val D I ( $\varphi'''$  x)  $x_o \cdot$  val D I ( $\varphi'''$  x)  $y_o$ "
  by auto
qed
also
have "... = abstract (D ooo) (D Tv) ( $\lambda z.$  val D I ( $\varphi'''$  z)
  ( $g_{ooo} \cdot x_o \cdot y_o$ ))"
  unfolding val.simps(3) ..
also
have "... = abstract (D ooo) (D Tv)
  ( $\lambda z.$  val D I ( $\varphi'''$ ( $'g''$ , ooo) := z))
  ( $g_{ooo} \cdot x_o \cdot y_o$ )"
  unfolding  $\varphi'''$ _def ..
also
have "... = val D I  $\varphi''$  [ $\lambda 'g''$ :ooo.
   $g_{ooo} \cdot x_o \cdot y_o$ ]"
  by (simp only: val.simps(4) type_of.simps type_sym.case)
finally
show "val D I  $\varphi''$  [ $\lambda 'g''$ :ooo.  $g_{ooo} \cdot T \cdot T$ ] = val D I  $\varphi''$  [ $\lambda 'g''$ :ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]"
  .
qed
finally show ?thesis .
qed

```

lemma lemma\_5401\_e\_2:

```

assumes "general_model D I"
assumes "asg_into_interp  $\varphi$  D I"
assumes "y = true  $\vee$  y = false"
shows "(val D I  $\varphi$  Con_sym)  $\cdot$  false  $\cdot$  y = false"

```

proof -

```

define give_x :: trm where "give_x = [ $\lambda 'y'$ :Tv.  $x_o$ ]"
define give_fst :: trm where "give_fst = [ $\lambda 'x'$ :Tv. give_x]"
define val_give_fst :: 's where "val_give_fst = val D I  $\varphi$  give_fst"
have wff_give_x: "wff oo give_x"
  unfolding give_x_def by auto

```

```

have " $\wedge$  a b. a  $\in$ : D Tv  $\implies$ 
  b  $\in$ : D Tv  $\implies$ 
  val D I ( $\varphi$ ( $'x'$ , Tv) := a) give_x  $\in$ : D (type_of give_x)"
  using wff_give_x asg_into_frame_def assms(1,2) by auto

```

moreover

```

have " $\wedge$  a b. a  $\in$ : D Tv  $\implies$  b  $\in$ : D Tv  $\implies$  val D I ( $\varphi$ ( $'x'$ , Tv) := a) give_x  $\cdot$  b = a"
  unfolding give_x_def by auto

```

ultimately

```

have " $\wedge$  a b. a  $\in$ : D Tv  $\implies$ 
  b  $\in$ : D Tv  $\implies$ 
  abstract (D Tv) (D (type_of give_x)) ( $\lambda z.$  val D I ( $\varphi$ ( $'x'$ , Tv) := z) give_x)  $\cdot$  a  $\cdot$  b
  = a"

```

by auto

```

then have val_give_fst_simp: " $\wedge$  a b. a  $\in$ : D Tv  $\implies$  b  $\in$ : D Tv  $\implies$  val_give_fst  $\cdot$  a  $\cdot$  b = a"
  unfolding val_give_fst_def give_fst_def by auto

```

```

have wff_give_fst: "wff ooo give_fst"

```

unfolding give\_fst\_def give\_x\_def by auto

```

then have val_give_fst_fun: "val_give_fst  $\in$ : D ooo"

```

unfolding val\_give\_fst\_def using assms by auto

```

have "val D I ( $\varphi$ ( $'x'$ , Tv) := false,
  ( $'y'$ , Tv) := y,
  ( $'g''$ , ooo) := val_give_fst)) T  $\in$ : D Tv"

```

```

by (smt Pair_inject wff_give_fst assms(1,2,3) fun_upd_twist general_model.simps
  asg_into_interp_fun_upd[OF assms(1,2)] asg_into_interp_fun_upd_true[OF assms(1)]
  asg_into_interp_fun_upd_false[OF assms(1)] type_sym.distinct(5) val_give_fst_def wff_T)
then have val_give_fst_D:

```

```

"val_give_fst · val D I (φ(('x''', Tv) := false,
  ('y''', Tv) := y,
  ('g''', ooo) := val_give_fst)) T ·
  val D I (φ(('x''', Tv) := false,
  ('y''', Tv) := y,
  ('g''', ooo) := val_give_fst)) T

```

```

∈: D Tv"

```

```

using val_give_fst_simp[of
  "val D I (φ(('x''', Tv) := false,
  ('y''', Tv) := y,
  ('g''', ooo) := val_give_fst)) T"
  "val D I (φ(('x''', Tv) := false,
  ('y''', Tv) := y,
  ('g''', ooo) := val_give_fst)) T" ]

```

```

by auto

```

```

have false_y_TV: "false ∈: D Tv ∧ y ∈: D Tv"
  using assms(1) assms(3) wf_frame_def wf_interp.simps by auto
then have val_give_fst_in_D: "val_give_fst · false · y ∈: D Tv"
  using val_give_fst_simp by auto

```

```

have "true ∈: D Tv"

```

```

  by (metis assms(1) assms(2) general_model.simps lemma_5401_c[OF assms(1,2)] wff_T)
from this val_give_fst_in_D false_y_TV have "val_give_fst · true · true ≠ val_give_fst · false · y"
  using val_give_fst_simp true_neq_false by auto

```

```

then have val_give_fst_not_false:

```

```

"val_give_fst · val D I (φ(('x''', Tv) := false,
  ('y''', Tv) := y,
  ('g''', ooo) := val_give_fst)) T
  · val D I (φ(('x''', Tv) := false,
  ('y''', Tv) := y,
  ('g''', ooo) := val_give_fst)) T

```

```

≠ val_give_fst · false · y"

```

```

using asg_into_frame_fun_upd assms(1) assms(2) lemma_5401_c false_y_TV val_give_fst_fun by auto

```

```

have Con_sym_subterm0TT_neq_Con_sym_subterm0xy:

```

```

"val D I (φ(('x''', Tv) := false, ('y''', Tv) := y)) [λ'g''':ooo. g_ooo · T · T] ≠
  val D I (φ(('x''', Tv) := false, ('y''', Tv) := y)) [λ'g''':ooo. g_ooo · x_o · y_o]"

```

```

using abstract_cong_specific[of

```

```

  val_give_fst
  "(D ooo)"
  "(λz. z · val D I (φ(('x''', Tv) := false,
  ('y''', Tv) := y,
  ('g''', ooo) := z)) T
  · val D I (φ(('x''', Tv) := false,
  ('y''', Tv) := y,
  ('g''', ooo) := z)) T)"
  "(D Tv)"
  "(λz. z · false · y)" ]

```

```

using val_give_fst_fun val_give_fst_D val_give_fst_in_D val_give_fst_not_false by auto

```

```

have "asg_into_frame (φ(('x''', Tv) := false, ('y''', Tv) := y)) D"

```

```

  using asg_into_interp_fun_upd_false[OF assms(1)] general_model.simps[of D I] assms wff_Con_sym_subterm1
  asg_into_interp_fun_upd_true[OF assms(1)] by auto

```

```

then have val_Con_sym_subterm1: "val D I (φ(('x''', Tv) := false, ('y''', Tv) := y)) [[λ'g''':ooo. g_ooo · T
· T] =(Tv ← ooo)= [λ'g''':ooo. g_ooo · x_o · y_o]] = false"

```

```

  using Con_sym_subterm0TT_neq_Con_sym_subterm0xy lemma_5401_b_variant_3[OF assms(1)]
  by auto

```

```

have "y ∈: D Tv"

```

```

  using general_model.simps lemma_5401_d[OF assms(1,2)] wff_F assms

```

```

    by (metis lemma_5401_c[OF assms(1,2)] wff_T)
  moreover
  have "val D I ( $\varphi$ (( $'x'$ ), Tv) := false, ( $'y'$ ), Tv) := y) [[ $\lambda$ 'g':ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda$ 'g':ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]]  $\in$ : D Tv"
    using asg_into_interp_fun_upd_false[OF assms(1)] general_model.simps[of D I] assms wff_Con_sym_subterm1
    asg_into_interp_fun_upd_true[OF assms(1)] by auto
  moreover
  have "val D I ( $\varphi$ (( $'x'$ ), Tv) := false, ( $'y'$ ), Tv) := y) [[ $\lambda$ 'g':ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda$ 'g':ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]] = false"
    using val_Con_sym_subterm1 by auto
  ultimately
  have val_y: "(val D I ( $\varphi$ (( $'x'$ ), Tv) := false)) [ $\lambda$ 'y':Tv. [[ $\lambda$ 'g':ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda$ 'g':ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]]]  $\cdot$  y = false"
    by simp

  have 11: "val D I ( $\varphi$ (( $'x'$ ), Tv) := false)) [ $\lambda$ 'y':Tv. [[ $\lambda$ 'g':ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda$ 'g':ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]]]  $\in$ : D oo"
    using asg_into_interp_fun_upd_false[OF assms(1,2)] general_model.simps[of D I] assms
    wff_Con_sym_subterm2 by blast
  moreover
  have "val D I ( $\varphi$ (( $'x'$ ), Tv) := false)) [ $\lambda$ 'y':Tv. [[ $\lambda$ 'g':ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda$ 'g':ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]]]  $\cdot$  y = false"
    using val_y by auto
  ultimately
  have "(val D I  $\varphi$  [ $\lambda$ 'x':Tv. [ $\lambda$ 'y':Tv. [[ $\lambda$ 'g':ooo.  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$  ooo) = [ $\lambda$ 'g':ooo.  $g_{ooo} \cdot x_o \cdot y_o$ ]]]])  $\cdot$  false  $\cdot$  y = false"
    using false_y_TV by simp
  then show "(val D I  $\varphi$  Con_sym)  $\cdot$  false  $\cdot$  y = false"
    unfolding Con_sym_def by auto
qed

```

lemma lemma\_5401\_e\_3:

```

  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "x = true  $\vee$  x = false"
  shows "(val D I  $\varphi$  Con_sym)  $\cdot$  x  $\cdot$  false = false"

```

proof -

```

  define give_y :: trm where "give_y = ([ $\lambda$ 'y':Tv.  $y_o$ ])"
  define give_snd :: trm where "give_snd = [ $\lambda$ 'x':Tv. give_y]"
  define val_give_snd :: 's where "val_give_snd = val D I  $\varphi$  give_snd"
  have wff_give_y: "wff oo give_y"
    unfolding give_y_def by auto

```

```

  have " $\bigwedge$ a b. a  $\in$ : D Tv  $\implies$  b  $\in$ : D Tv  $\implies$  a  $\in$ : D Tv"
    by simp

```

moreover

```

  have " $\bigwedge$ a b. a  $\in$ : D Tv  $\implies$  b  $\in$ : D Tv  $\implies$  val D I ( $\varphi$ (( $'x'$ ), Tv) := a) give_y  $\in$ : D (type_of give_y)"
    using wff_give_y asg_into_frame_def assms(1) assms(2) by auto

```

moreover

```

  have " $\bigwedge$ a b. a  $\in$ : D Tv  $\implies$  b  $\in$ : D Tv  $\implies$  val D I ( $\varphi$ (( $'x'$ ), Tv) := a) give_y  $\cdot$  b = b"
    unfolding give_y_def by auto

```

ultimately

```

  have val_give_snd_simp: " $\bigwedge$ a b. a  $\in$ : D Tv  $\implies$  b  $\in$ : D Tv  $\implies$  val_give_snd  $\cdot$  a  $\cdot$  b = b"
    unfolding val_give_snd_def give_snd_def by auto

```

```

  have wff_give_snd: "wff ooo give_snd"

```

```

    unfolding give_snd_def give_y_def by auto

```

```

  then have val_give_snd_in_D: "val_give_snd  $\in$ : D ooo"

```

```

    unfolding val_give_snd_def using assms
    by auto

```

```

  then have "val D I ( $\varphi$ (( $'x'$ ), Tv) := x,

```

```

      (''y'', Tv) := false,
      (''g'', ooo) := val_give_snd)) T ∈: D Tv"
by (smt Pair_inject wff_give_snd assms(1,2,3)
  fun_upd_twist general_model.simps asg_into_interp_fun_upd[OF assms(1,2)]
  asg_into_interp_fun_upd_false[OF assms(1)] asg_into_interp_fun_upd_true[OF assms(1)]
  type_sym.distinct(5) val_give_snd_def wff_T)
then have val_give_snd_app_in_D:
  "val_give_snd · val D I (φ(''x'', Tv) := x,
    (''y'', Tv) := false,
    (''g'', ooo) := val_give_snd)) T
  · val D I (φ(''x'', Tv) := x,
    (''y'', Tv) := false,
    (''g'', ooo) := val_give_snd)) T
  ∈: D Tv"
using val_give_snd_simp[of
  "val D I (φ(''x'', Tv) := x,
    (''y'', Tv) := false,
    (''g'', ooo) := val_give_snd)) T"
  "val D I (φ(''x'', Tv) := x,
    (''y'', Tv) := false,
    (''g'', ooo) := val_give_snd)) T" ]
by auto

have false_and_x_in_D: "false ∈: D Tv ∧ x ∈: D Tv"
  using assms(1,3) wf_frame_def wf_interp.simps by auto
then have val_give_snd_app_x_false_in_D: "val_give_snd · x · false ∈: D Tv"
  using val_give_snd_simp by auto

have "true ∈: D Tv"
  by (metis assms(1) assms(2) general_model.simps lemma_5401_c[OF assms(1,2)] wff_T)
then have "val_give_snd · true · true ≠ val_give_snd · x · false"
  using val_give_snd_simp true_neq_false val_give_snd_app_in_D false_and_x_in_D by auto
then have
  "val_give_snd · val D I (φ(''x'', Tv) := x,
    (''y'', Tv) := false,
    (''g'', ooo) := val_give_snd)) T
  · val D I (φ(''x'', Tv) := x,
    (''y'', Tv) := false,
    (''g'', ooo) := val_give_snd)) T ≠
  val_give_snd · x · false"
  using asg_into_frame_fun_upd assms(1) assms(2) lemma_5401_c false_and_x_in_D val_give_snd_in_D
  by auto
then have "val D I (φ(''x'', Tv) := x, (''y'', Tv) := false)) [λ''g'':ooo. gooo · T · T] ≠
  val D I (φ(''x'', Tv) := x, (''y'', Tv) := false))
  [λ''g'':ooo. gooo · xo · yo]"
  using abstract_cong_specific[of
    val_give_snd
    "(D ooo)"
    "(λz. z · val D I (φ(''x'', Tv) := x, (''y'', Tv) := false, (''g'', ooo) := z))
      T · val D I (φ(''x'', Tv) := x, (''y'', Tv) := false, (''g'', ooo) := z)) T)"
    "(D Tv)"
    "(λz. z · x · false)"
  ]
  using val_give_snd_in_D val_give_snd_app_x_false_in_D val_give_snd_app_in_D by auto
then have "val D I (φ(''x'', Tv) := x, (''y'', Tv) := false)) [[λ''g'':ooo. gooo · T · T] = (Tv ← ooo) = [λ''g'':ooo. gooo · xo · yo]] = false"
  using asg_into_frame_fun_upd assms(1,2) lemma_5401_b_variant_3 false_and_x_in_D by auto
then have val_Con_sym_subterm2_false: "(val D I (φ(''x'', Tv) := x)) [λ''y'':Tv. [[λ''g'':ooo. gooo · T ·
T] = (Tv ← ooo) = [λ''g'':ooo. gooo · xo · yo]]] · false = false"
  using false_and_x_in_D by simp

have "x ∈: D Tv"
  by (simp add: false_and_x_in_D)
moreover

```

```

have "val D I ( $\varphi$ (( $'x'$ ), Tv) := x) [ $\lambda$   $'y'$ :Tv. [[ $\lambda$   $'g'$ : $ooo$ .  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$   $ooo$ ) = [ $\lambda$   $'g'$ : $ooo$ .  $g_{ooo} \cdot x_o \cdot y_o$ ]]]  $\in$ : D  $oo$ "
  by (metis assms(1,3) general_model.simps lemma_5401_c[OF assms(1,2)]
      asg_into_interp_fun_upd[OF assms(1,2)] asg_into_interp_fun_upd_false[OF assms(1,2)]
      wff_Con_sym_subterm2 wff_T)
moreover
have "val D I ( $\varphi$ (( $'x'$ ), Tv) := x) [ $\lambda$   $'y'$ :Tv. [[ $\lambda$   $'g'$ : $ooo$ .  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$   $ooo$ ) = [ $\lambda$   $'g'$ : $ooo$ .  $g_{ooo} \cdot x_o \cdot y_o$ ]]]  $\cdot$  false = false"
  using val_Con_sym_subterm2_false by auto
ultimately
have "(val D I  $\varphi$  [ $\lambda$   $'x'$ :Tv. [ $\lambda$   $'y'$ :Tv. [[ $\lambda$   $'g'$ : $ooo$ .  $g_{ooo} \cdot T \cdot T$ ] = (Tv  $\Leftarrow$   $ooo$ ) = [ $\lambda$   $'g'$ : $ooo$ .  $g_{ooo} \cdot x_o \cdot y_o$ ]]])  $\cdot$  x  $\cdot$  false = false"
  by auto
then show "(val D I  $\varphi$  Con_sym)  $\cdot$  x  $\cdot$  false = false"
  unfolding Con_sym_def by auto
qed

```

```

lemma lemma_5401_e_variant_1:
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "general_model D I"
  assumes "y = true  $\vee$  y = false"
  assumes "x = true  $\vee$  x = false"
  shows "(val D I  $\varphi$  Con_sym)  $\cdot$  x  $\cdot$  y = boolean (x = true  $\wedge$  y = true)"
proof (cases "y = true")
  case True
  note True_outer = this
  then show ?thesis
  proof (cases "x = true")
    case True
    then show ?thesis
      using True_outer assms lemma_5401_e_1 unfolding boolean_def by auto
  next
    case False
    then show ?thesis
      using True_outer assms lemma_5401_e_2 unfolding boolean_def by auto
  qed
next
  case False
  note False_outer = this
  then show ?thesis
  proof (cases "x = true")
    case True
    then show ?thesis
      using False_outer assms lemma_5401_e_3 unfolding boolean_def by auto
  next
    case False
    then show ?thesis
      using False_outer assms lemma_5401_e_2 unfolding boolean_def by auto
  qed
qed

```

```

lemma asg_into_interp_is_true_or_false:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  shows " $\varphi$  (x, Tv) = true  $\vee$   $\varphi$  (x, Tv) = false"
proof -
  have "wff Tv (Var x Tv)"
  by auto
  then have "val D I  $\varphi$  (Var x Tv)  $\in$ : D Tv"
  using assms general_model.simps by blast
  then have "val D I  $\varphi$  (Var x Tv)  $\in$ : boolset"
  using assms unfolding general_model.simps wf_interp.simps wf_frame_def by auto
  then show ?thesis

```



```

    using mem_boolset by simp
qed

lemma wff_Tv_is_true_or_false:
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "general_model D I"
  assumes "wff Tv A"
  shows "val D I  $\varphi$  A = true  $\vee$  val D I  $\varphi$  A = false"
proof -
  have "val D I  $\varphi$  A  $\in$ : D Tv"
  using assms by auto
  then have "val D I  $\varphi$  A  $\in$ : boolset"
  using assms unfolding general_model.simps wf_interp.simps wf_frame_def by force
  then show ?thesis
  using mem_boolset by blast
qed

lemma lemma_5401_e_variant_2:
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "general_model D I"
  assumes "wff Tv A"
  assumes "wff Tv B"
  shows "(val D I  $\varphi$  (A  $\wedge$  B)) = boolean (satisfies D I  $\varphi$  A  $\wedge$  satisfies D I  $\varphi$  B)"
  using assms wff_Tv_is_true_or_false[of  $\varphi$  D I] lemma_5401_e_variant_1 unfolding Con_def by auto

lemma lemma_5401_f_1:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "y = true  $\vee$  y = false"
  shows "(val D I  $\varphi$  Imp_sym)  $\cdot$  false  $\cdot$  y = true"
proof -
  define Imp_subterm2 :: trm where
    "Imp_subterm2  $\equiv$  [ $\lambda$  'y':Tv. [ $x_o$  =Tv= (x_o  $\wedge$  y_o)]]"

  have val_Imp_subterm0_false: "val D I ( $\varphi$ (('x', Tv) := false, ('y', Tv) := y)) (x_o  $\wedge$  y_o) = false"
  using assms asg_into_interp_fun_upd_false[OF assms(1)] asg_into_interp_fun_upd_true[OF assms(1)]
  boolean_def lemma_5401_e_variant_2 by auto

  have "asg_into_frame ( $\varphi$ (('x', Tv) := false, ('y', Tv) := y)) D"
  using assms(1, 2, 3) lemma_5401_c[OF assms(1)] asg_into_interp_fun_upd wff_T
  asg_into_interp_fun_upd_false by metis
  then have "val D I ( $\varphi$ (('x', Tv) := false, ('y', Tv) := y)) [ $x_o$  =Tv= (x_o  $\wedge$  y_o)] = true"
  using lemma_5401_b_variant_1[OF assms(1)] val_Imp_subterm0_false unfolding boolean_def by auto
  then have val_Imp_subterm2_true: "(val D I ( $\varphi$ (('x', Tv) := false)) [ $\lambda$  'y':Tv. [ $x_o$  =Tv= (x_o  $\wedge$  y_o)])  $\cdot$  y
  = true"
  using assms(1,3) wf_frame_def wf_interp.simps by auto

  have "val D I  $\varphi$  [ $\lambda$  'x':Tv. [ $\lambda$  'y':Tv. [ $x_o$  =Tv= (x_o  $\wedge$  y_o)]]]  $\cdot$  false  $\cdot$  y = true"
  proof -
    have "false  $\in$ : D Tv"
    by (metis asg_into_frame_def asg_into_interp_fun_upd_false assms(1) assms(2) fun_upd_same)
    then have "val D I ( $\varphi$ (('x', Tv) := false)) [ $\lambda$  'y':Tv. [ $x_o$  =Tv= (x_o  $\wedge$  y_o)]] = val D I  $\varphi$  [ $\lambda$  'x':Tv. [ $\lambda$ 
    'y':Tv. [ $x_o$  =Tv= (x_o  $\wedge$  y_o)]]]  $\cdot$  false"
    using asg_into_interp_fun_upd_false assms(1,2) Imp_subterm2_def[symmetric] wff_Imp_sym_subterm2_iff by
  force
  then show ?thesis
  by (metis val_Imp_subterm2_true)
  qed
  then show "(val D I  $\varphi$  Imp_sym)  $\cdot$  false  $\cdot$  y = true"
  unfolding Imp_sym_def Imp_subterm2_def by auto
qed

```

```

lemma lemma_5401_f_2:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "x = true  $\vee$  x = false"
  shows "(val D I  $\varphi$  Imp_sym)  $\cdot$  x  $\cdot$  true = true"
proof -
  have asg: "asg_into_frame ( $\varphi$ (( $'x'$ ), Tv) := x, ( $'y'$ ), Tv) := true)) D"
    using assms(1,2,3) asg_into_interp_fun_upd_false asg_into_interp_fun_upd_true[OF assms(1)] by blast
  then have "val D I ( $\varphi$ (( $'x'$ ), Tv) := x, ( $'y'$ ), Tv) := true)) ( $x_o \wedge y_o$ ) = x"
    using lemma_5401_e_variant_2 assms unfolding boolean_def by auto
  then have val_Imp_subterm1_true: "val D I ( $\varphi$ (( $'x'$ ), Tv) := x, ( $'y'$ ), Tv) := true)) [ $x_o =Tv= (x_o \wedge y_o)$ ] =
  true"
    using asg lemma_5401_b_variant_1[OF assms(1)] boolean_eq_true by auto

  have val_Imp_subterm2_true: "val D I ( $\varphi$ (( $'x'$ ), Tv) := x)) [ $\lambda$   $'y'$ :Tv. [ $x_o =Tv= (x_o \wedge y_o)$ ]]  $\cdot$  true = true"
    using val_Imp_subterm1_true assms(1) wf_frame_def wf_interp.simps by auto

  have "x  $\in$ : D Tv"
    by (metis asg_into_frame_def assms(1) assms(3) fun_upd_same asg_into_interp_fun_upd_false
      asg_into_interp_fun_upd_true[OF assms(1,2)])
  moreover
  have "val D I ( $\varphi$ (( $'x'$ ), Tv) := x)) [ $\lambda$   $'y'$ :Tv. [ $x_o =Tv= (x_o \wedge y_o)$ ]]  $\in$ : D oo"
    using wff_Imp_sym_subterm2
    by (metis assms(1,2,3) general_model.simps lemma_5401_c[OF assms(1,2)]
      asg_into_interp_fun_upd[OF assms(1,2)] asg_into_interp_fun_upd_false wff_T)
  ultimately
  have "(val D I  $\varphi$  [ $\lambda$   $'x'$ :Tv. [ $\lambda$   $'y'$ :Tv. [ $x_o =Tv= (x_o \wedge y_o)$ ]])  $\cdot$  x  $\cdot$  true = true"
    using val_Imp_subterm2_true by auto
  then show "(val D I  $\varphi$  Imp_sym)  $\cdot$  x  $\cdot$  true = true"
    unfolding Imp_sym_def by auto
qed

```

```

lemma lemma_5401_f_3:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  shows "(val D I  $\varphi$  Imp_sym)  $\cdot$  true  $\cdot$  false = false"
proof -
  have asg: "asg_into_frame ( $\varphi$ (( $'x'$ ), Tv) := true, ( $'y'$ ), Tv) := false)) D"
    by (meson assms(1,2) asg_into_interp_fun_upd_false asg_into_interp_fun_upd_true)
  moreover
  have "false = true  $\vee$  false = false"
    unfolding boolean_def by auto
  moreover
  have "boolean (true = true  $\wedge$  false = true) = false"
    unfolding boolean_def by auto
  ultimately
  have 3: "val D I ( $\varphi$ (( $'x'$ ), Tv) := true, ( $'y'$ ), Tv) := false)) ( $x_o \wedge y_o$ ) = false"
    using lemma_5401_e_variant_2 assms by auto
  then have Imp_subterm1_false: "val D I ( $\varphi$ (( $'x'$ ), Tv) := true, ( $'y'$ ), Tv) := false)) [ $x_o =Tv= (x_o \wedge y_o)$ ] =
  false"
    using subst lemma_5401_b_variant_1[OF assms(1)] asg boolean_def by auto

  have asdff: "wff Tv [ $x_o =Tv= (x_o \wedge y_o)$ ]"
    by auto

  have false_Tv: "false  $\in$ : D Tv"
    using assms(1) wf_frame_def wf_interp.simps by auto
  moreover
  have "val D I ( $\varphi$ (( $'x'$ ), Tv) := true, ( $'y'$ ), Tv) := false)) [ $x_o =Tv= (x_o \wedge y_o)$ ]  $\in$ : D Tv"
    by (simp add: Imp_subterm1_false false_Tv)
  moreover
  have "val D I ( $\varphi$ (( $'x'$ ), Tv) := true, ( $'y'$ ), Tv) := false)) [ $x_o =Tv= (x_o \wedge y_o)$ ] = false"

```

```

    using Imp_subterm1_false by auto
  ultimately
  have Imp_subterm2_app_false: "val D I ( $\varphi$ (( $'x'$ ), Tv) := true)) [ $\lambda$   $'y'$ :Tv. [ $x_o$  =Tv= ( $x_o \wedge y_o$ )]]  $\cdot$  false =
false"
  by auto

  have wff_Imp_sym_subterm2: "wff oo [ $\lambda$   $'y'$ :Tv. [ $x_o$  =Tv= ( $x_o \wedge y_o$ )]]"
  by auto

  have "(val D I  $\varphi$  [ $\lambda$   $'x'$ :Tv. [ $\lambda$   $'y'$ :Tv. [ $x_o$  =Tv= ( $x_o \wedge y_o$ )]]])  $\cdot$  true  $\cdot$  false = false"
  proof -
    have "true  $\in$ : D Tv"
    by (metis assms(1) assms(2) general_model.simps lemma_5401_c[OF assms(1,2)] wff_T)
  moreover
  have "val D I ( $\varphi$ (( $'x'$ ), Tv) := true)) [ $\lambda$   $'y'$ :Tv. [ $x_o$  =Tv= ( $x_o \wedge y_o$ )]]  $\in$ : D oo"
  using wff_Imp_sym_subterm2
  by (metis assms(1) general_model.simps asg_into_interp_fun_upd_true[OF assms(1,2)])
  moreover
  have "val D I ( $\varphi$ (( $'x'$ ), Tv) := true)) [ $\lambda$   $'y'$ :Tv. [ $x_o$  =Tv= ( $x_o \wedge y_o$ )]]  $\cdot$  false = false"
  using Imp_subterm2_app_false by auto
  ultimately
  show ?thesis
  by auto
qed
then show "(val D I  $\varphi$  Imp_sym)  $\cdot$  true  $\cdot$  false = false"
  unfolding Imp_sym_def by auto
qed

```

```

lemma lemma_5401_f_variant_1:
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "general_model D I"
  assumes "x = true  $\vee$  x = false"
  assumes "y = true  $\vee$  y = false"
  shows "(val D I  $\varphi$  Imp_sym)  $\cdot$  x  $\cdot$  y = boolean (x = true  $\longrightarrow$  y = true)"
proof (cases "y = true")
  case True
  note True_outer = this
  then show ?thesis
  proof (cases "x = true")
    case True
    then show ?thesis
    using True_outer assms lemma_5401_f_2 unfolding boolean_def by auto
  next
  case False
  then show ?thesis
  using True_outer assms lemma_5401_f_2 unfolding boolean_def by auto
  qed
next
  case False
  note False_outer = this
  then show ?thesis
  proof (cases "x = true")
    case True
    then show ?thesis
    using False_outer assms lemma_5401_f_3 unfolding boolean_def by auto
  next
  case False
  then show ?thesis
  using False_outer assms lemma_5401_f_1 unfolding boolean_def by auto
  qed
qed

```

```

lemma lemma_5401_f_variant_2:
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "general_model D I"
  assumes "wff Tv A"
  assumes "wff Tv B"
  shows "(val D I  $\varphi$  (A  $\longrightarrow$  B)) = boolean (satisfies D I  $\varphi$  A  $\longrightarrow$  satisfies D I  $\varphi$  B)"
  using assms unfolding Imp_def
  by (simp add: lemma_5401_f_variant_1 wff_Tv_is_true_or_false)

lemma lemma_5401_g:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "wff Tv A"
  shows "satisfies D I  $\varphi$  [ $\forall x:\alpha. A$ ]  $\longleftrightarrow$ 
    ( $\forall \psi. \text{asg\_into\_interp } \psi \text{ D I} \longrightarrow \text{agree\_off\_asg } \psi \varphi x \alpha \longrightarrow \text{satisfies D I } \psi \text{ A})"$ 
proof -
  have "wff (Tv  $\Leftarrow$   $\alpha$ ) [ $\lambda$  'x': $\alpha. T$ ]"
  by auto
  then have PI_subterm_in_D: "val D I  $\varphi$  [ $\lambda$  'x': $\alpha. T$ ]  $\in$ : D (Tv  $\Leftarrow$   $\alpha$ )"
  using assms(1,2) general_model.simps by blast

  have "wff (Tv  $\Leftarrow$   $\alpha$ ) ( $[\lambda x:\alpha. A]$ )"
  using assms by auto
  moreover
  have " $\forall \varphi. \text{asg\_into\_frame } \varphi \text{ D} \longrightarrow (\forall A \alpha. \text{wff } \alpha \text{ A} \longrightarrow \text{val D I } \varphi \text{ A} \in: \text{D } \alpha)$ "
  using assms(1) by auto
  then have " $\forall t \text{ cs. val D I } \varphi$  [ $\lambda \text{cs:t. A}$ ]  $\in$ : D (Tv  $\Leftarrow$  t)"
  using wff_Abs assms(1,2,3) by presburger
  then have "abstract (D  $\alpha$ ) (D Tv) ( $\lambda u. \text{val D I } (\varphi((x, \alpha) := u)) \text{ A}$ )  $\in$ : D (Tv  $\Leftarrow$   $\alpha$ )"
  using assms(3) by simp
  ultimately
  have val_lambda_A: "val D I  $\varphi$  ( $[\lambda x:\alpha. A]$ )  $\in$ : D (Tv  $\Leftarrow$   $\alpha$ )"
  using assms by auto

  have true_and_A_in_D: " $\forall z. z \in: \text{D } \alpha \longrightarrow \text{true} \in: \text{D Tv} \wedge \text{val D I } (\varphi((x, \alpha) := z)) \text{ A} \in: \text{D Tv}$ "
  by (metis assms(1,2,3) general_model.simps lemma_5401_c[OF assms(1,2)] asg_into_frame_fun_upd wff_T)

  have "satisfies D I  $\varphi$  [ $\forall x:\alpha. A$ ]  $\longleftrightarrow$  val D I  $\varphi$  [ $\forall x:\alpha. A$ ] = true"
  by auto
  moreover have "...  $\longleftrightarrow$  val D I  $\varphi$  (PI  $\alpha$ )  $\cdot$  val D I  $\varphi$  [ $\lambda x:\alpha. A$ ] = true"
  unfolding Forall_def by simp
  moreover have "...  $\longleftrightarrow$  I 'Q' ((Tv  $\Leftarrow$  (Tv  $\Leftarrow$   $\alpha$ ))  $\Leftarrow$  (Tv  $\Leftarrow$   $\alpha$ ))
     $\cdot$  val D I  $\varphi$  [ $\lambda$  'x': $\alpha. T$ ]  $\cdot$  val D I  $\varphi$  [ $\lambda x:\alpha. A$ ] =
      true"
  unfolding PI_def by simp
  moreover have "...  $\longleftrightarrow$  (iden (D (Tv  $\Leftarrow$   $\alpha$ )))  $\cdot$  val D I  $\varphi$  [ $\lambda$  'x': $\alpha. T$ ]  $\cdot$  val D I  $\varphi$  [ $\lambda x:\alpha. A$ ] =
      true"
  unfolding PI_def using wf_interp.simps assms by simp
  moreover have "...  $\longleftrightarrow$  val D I  $\varphi$  [ $\lambda$  'x': $\alpha. T$ ] = val D I  $\varphi$  [ $\lambda x:\alpha. A$ ]"
  using PI_subterm_in_D val_lambda_A apply_id_true by auto
  moreover have "...  $\longleftrightarrow$  abstract (D  $\alpha$ ) (D Tv) ( $\lambda z. \text{val D I } (\varphi(('x', \alpha) := z)) \text{ T}$ ) = val D I  $\varphi$  [ $\lambda x:\alpha. A$ ]"
  using assms wff_T by simp
  moreover have "...  $\longleftrightarrow$  abstract (D  $\alpha$ ) (D Tv) ( $\lambda z. \text{true}$ ) = val D I  $\varphi$  [ $\lambda x:\alpha. A$ ]"
proof -
  have " $\forall x. x \in: \text{D } \alpha \longrightarrow \text{val D I } (\varphi(('x', \alpha) := x)) \text{ T} \in: \text{D Tv} \wedge \text{true} \in: \text{D Tv}$ "
  using true_and_A_in_D assms(1,2) asg_into_frame_fun_upd by auto
  moreover
  have " $\forall x. x \in: \text{D } \alpha \longrightarrow \text{val D I } (\varphi(('x', \alpha) := x)) \text{ T} \in: \text{D Tv} \wedge \text{satisfies D I } (\varphi(('x', \alpha) := x)) \text{ T}$ "
  using true_and_A_in_D assms(1) assms(2) lemma_5401_c[OF assms(1)] asg_into_frame_fun_upd by auto
  ultimately
  have "abstract (D  $\alpha$ ) (D Tv) ( $\lambda z. \text{val D I } (\varphi(('x', \alpha) := z)) \text{ T}$ ) = abstract (D  $\alpha$ ) (D Tv) ( $\lambda z. \text{true}$ )"
  using abstract_extensional by auto
  then show ?thesis

```

```

    by auto
qed
moreover have "...  $\longleftrightarrow$  abstract (D  $\alpha$ ) (D Tv) ( $\lambda z.$  true) = val D I  $\varphi$  ( $[\lambda x:\alpha. A]$ )"
  by auto
moreover have "...  $\longleftrightarrow$  abstract (D  $\alpha$ ) (D Tv) ( $\lambda z.$  true) =
  abstract (D  $\alpha$ ) (D Tv) ( $\lambda z.$  val D I ( $\varphi((x, \alpha) := z)$ ) A)"
  using assms by simp
moreover have "...  $\longleftrightarrow$  ( $\forall z. z \in: D \alpha \longrightarrow \text{true} \in: D \text{Tv} \wedge \text{true} = \text{val D I } (\varphi((x, \alpha) := z)) \text{ A}$ )"
proof -
  have " $\forall z. z \in: D \alpha \longrightarrow \text{true} \in: D \text{Tv} \wedge \text{val D I } (\varphi((x, \alpha) := z)) \text{ A} \in: D \text{Tv}$ "
    using true_and_A_in_D by auto
  then show ?thesis
    using abstract_iff_extensional by auto
qed
moreover have "...  $\longleftrightarrow$  ( $\forall z. z \in: D \alpha \longrightarrow \text{true} = \text{val D I } (\varphi((x, \alpha) := z)) \text{ A}$ )"
  by (metis assms(1,2) general_model.simps lemma_5401_c[OF assms(1,2)] wff_T)
moreover have "...  $\longleftrightarrow$  ( $\forall z. z \in: D \alpha \longrightarrow \text{satisfies D I } (\varphi((x, \alpha) := z)) \text{ A}$ )"
  by auto
moreover have "...  $\longleftrightarrow$  ( $\forall \psi. \text{asg\_into\_interp } \psi \text{ D I} \longrightarrow \text{agree\_off\_asg } \psi \varphi x \alpha \longrightarrow \text{satisfies D I } \psi \text{ A}$ )"
proof -
  show ?thesis
  proof
    assume A_sat: " $\forall z. z \in: D \alpha \longrightarrow \text{satisfies D I } (\varphi((x, \alpha) := z)) \text{ A}$ "
    show " $\forall \psi. \text{asg\_into\_frame } \psi \text{ D} \longrightarrow \text{agree\_off\_asg } \psi \varphi x \alpha \longrightarrow \text{satisfies D I } \psi \text{ A}$ "
    proof (rule; rule; rule)
      fix  $\psi$ 
      assume a1: "asg_into_frame  $\psi$  D"
      assume a2: "agree_off_asg  $\psi \varphi x \alpha$ "
      have " $\exists xa. (\varphi((x, \alpha) := xa)) = \psi$ "
        using a1 a2 agree_off_asg_def2 by blast
      then show "satisfies D I  $\psi$  A"
        using A_sat a1 a2 by (metis asg_into_frame_def fun_upd_same)
    qed
  next
    assume " $\forall \psi. \text{asg\_into\_frame } \psi \text{ D} \longrightarrow \text{agree\_off\_asg } \psi \varphi x \alpha \longrightarrow \text{satisfies D I } \psi \text{ A}$ "
    then show " $\forall z. z \in: D \alpha \longrightarrow \text{satisfies D I } (\varphi((x, \alpha) := z)) \text{ A}$ "
      using asg_into_frame_fun_upd asg_into_interp_fun_upd[OF assms(1,2)] assms(2) fun_upd_other
      unfolding agree_off_asg_def by auto
  qed
qed
ultimately show ?thesis
  by auto
qed

```

```

theorem lemma_5401_g_variant_1:
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "general_model D I"
  assumes "wff Tv A"
  shows "val D I  $\varphi$  [ $\forall x:\alpha. A$ ] =
    boolean ( $\forall \psi. \text{asg\_into\_interp } \psi \text{ D I} \longrightarrow \text{agree\_off\_asg } \psi \varphi x \alpha \longrightarrow \text{satisfies D I } \psi \text{ A}$ )"
proof -
  have "val D I  $\varphi$  [ $\forall x:\alpha. A$ ] = (if satisfies D I  $\varphi$  [ $\forall x:\alpha. A$ ] then true else false)"
    using assms wff_Forall wff_Tv_is_true_or_false by metis
  then show ?thesis
    using assms lemma_5401_g[symmetric] unfolding boolean_def by auto
qed

```

## 12 Soundness

```

lemma fun_sym_asg_to_funspace:
  assumes "asg_into_frame  $\varphi$  D"
  assumes "general_model D I"
  shows " $\varphi (f, \alpha \leftarrow \beta) \in: \text{funspace } (D \beta) (D \alpha)$ "

```

```

proof -
  have "wff ( $\alpha \Leftarrow \beta$ ) (Var f ( $\alpha \Leftarrow \beta$ ))"
    by auto
  then have "val D I  $\varphi$  (Var f ( $\alpha \Leftarrow \beta$ ))  $\in$ : D ( $\alpha \Leftarrow \beta$ )"
    using assms
    using general_model.simps by blast
  then show " $\varphi$  (f,  $\alpha \Leftarrow \beta$ )  $\in$ : funspace (D  $\beta$ ) (D  $\alpha$ )"
    using assms unfolding general_model.simps wf_interp.simps wf_frame_def
    by (simp add: subs_def)
qed

lemma fun_sym_interp_to_funspace:
  assumes "asg_into_frame  $\varphi$  D"
  assumes "general_model D I"
  shows "I f ( $\alpha \Leftarrow \beta$ )  $\in$ : funspace (D  $\beta$ ) (D  $\alpha$ )"
proof -
  have "wff ( $\alpha \Leftarrow \beta$ ) (Cst f ( $\alpha \Leftarrow \beta$ ))"
    by auto
  then have "val D I  $\varphi$  (Cst f ( $\alpha \Leftarrow \beta$ ))  $\in$ : D ( $\alpha \Leftarrow \beta$ )"
    using assms general_model.simps by blast
  then show "I f ( $\alpha \Leftarrow \beta$ )  $\in$ : funspace (D  $\beta$ ) (D  $\alpha$ )"
    using assms subs_def unfolding general_model.simps wf_interp.simps wf_frame_def by auto
qed

theorem theorem_5402_a_rule_R:
  assumes A_eql_B: "valid_general ([A = $\alpha$ = B])"
  assumes "valid_general C"
  assumes "rule_R C ([A = $\alpha$ = B]) C'"
  assumes "wff  $\alpha$  A"
  assumes "wff  $\alpha$  B"
  assumes "wff  $\beta$  C"
  shows "valid_general C'"
  unfolding valid_general_def
proof (rule allI, rule allI, rule impI)
  fix D :: "type_sym  $\Rightarrow$  's" and I :: "char list  $\Rightarrow$  type_sym  $\Rightarrow$  's"
  assume DI: "general_model D I"
  then have "valid_in_model D I ([A = $\alpha$ = B])"
    using A_eql_B unfolding valid_general_def by auto
  then have x: " $\forall \varphi$ . asg_into_frame  $\varphi$  D  $\longrightarrow$  (val D I  $\varphi$  A = val D I  $\varphi$  B)"
    unfolding valid_in_model_def using lemma_5401_b[OF DI, of _  $\alpha$  A B ] assms(4,5) by auto
  have r: "replacement A B C C'"
    using assms(3) using Eql_def rule_R.cases by fastforce
  from r have " $\forall \varphi$ . asg_into_frame  $\varphi$  D  $\longrightarrow$  (val D I  $\varphi$  C = val D I  $\varphi$  C)"
    using x assms(4,5,6)
  proof (induction arbitrary:  $\beta$  rule: replacement.induct)
    case (replace A B)
    then show ?case by auto
  next
    case (replace_App_left A B C E D')
    define  $\alpha'$  where " $\alpha'$  = type_of C"
    define  $\beta'$  where " $\beta'$  = type_of D'"
    show ?case
    proof (rule, rule)
      fix  $\varphi$ 
      assume asg: "asg_into_frame  $\varphi$  D"
      have  $\alpha'$ : " $\alpha'$  =  $\beta \Leftarrow \beta'$ "
        using trm.distinct(11) trm.distinct(3,7) trm.inject(3) replace_App_left.prem(4) wff.simps
        by (metis  $\alpha'$ _def  $\beta'$ _def wff_App_type_of)
      from asg have "wff  $\alpha'$  C"
        using replace_App_left trm.distinct(3,7,11) trm.inject(3) wff.simps
        by (metis  $\alpha'$   $\beta'$ _def type_of wff_App')
      then have "val D I  $\varphi$  C = val D I  $\varphi$  E"
        using asg replace_App_left by auto
    end
  end
end

```

```

    then show "val D I  $\varphi$  (C · D') = val D I  $\varphi$  (E · D')"
      using  $\alpha'$  by auto
  qed
next
case (replace_App_right A B D' E C)
define  $\alpha'$  where " $\alpha'$  = type_of C"
define  $\beta'$  where " $\beta'$  = type_of D'"
show ?case
proof (rule, rule)
  fix  $\varphi$ 
  assume asg: "asg_into_frame  $\varphi$  D"
  have  $\alpha'$ : " $\alpha'$  =  $\beta$   $\Leftarrow$   $\beta'$ "
    using trm.distinct(11) trm.distinct(3) trm.distinct(7) trm.inject(3)
    replace_App_right.prem(4) wff.simps by (metis  $\alpha'$ _def  $\beta'$ _def type_of wff_App')
  from asg have "wff  $\beta'$  D'"
    using  $\beta'$ _def replace_App_right.prem(4) by fastforce
  then have "val D I  $\varphi$  D' = val D I  $\varphi$  E"
    using asg replace_App_right by auto
  then show "val D I  $\varphi$  (C · D') = val D I  $\varphi$  (C · E)"
    using  $\alpha'$  by auto
  qed
next
case (replace_Abs A B C D' x  $\alpha'$ )
define  $\beta'$  where " $\beta'$  = type_of C"
show ?case
proof (rule, rule)
  fix  $\varphi$ 
  assume asg: "asg_into_frame  $\varphi$  D"
  then have val_C_eql_val_D':
    " $\forall z. z \in: D \ \alpha' \longrightarrow \text{val D I } (\varphi((x, \alpha') := z)) \ C = \text{val D I } (\varphi((x, \alpha') := z)) \ D'$ "
    using asg replace_App_right
    by (metis trm.distinct(11) trm.distinct(5) trm.distinct(9) trm.inject(4)
        asg_into_frame_fun_upd replace_Abs.IH replace_Abs.prem(1) replace_Abs.prem(2)
        replace_Abs.prem(3) replace_Abs.prem(4) wff.cases)
  have val_C_eql_val_D'_type:
    " $\forall z. z \in: D \ \alpha' \longrightarrow$ 
       $\text{val D I } (\varphi((x, \alpha') := z)) \ C \in: D \ (\text{type\_of } C) \wedge$ 
       $\text{val D I } (\varphi((x, \alpha') := z)) \ C = \text{val D I } (\varphi((x, \alpha') := z)) \ D'$ "
  proof (rule; rule)
    fix z
    assume a2: "z  $\in$ : D  $\alpha'$ "
    have "val D I  $\varphi$ ((x,  $\alpha'$ ) := z) C  $\in$ : D (type_of C)"
      using DI asg a2 asg_into_frame_fun_upd replace_Abs.prem(4) by auto
    moreover
    have "val D I  $\varphi$ ((x,  $\alpha'$ ) := z) C = val D I  $\varphi$ ((x,  $\alpha'$ ) := z) D'"
      using a2 val_C_eql_val_D' replace_Abs by auto
    ultimately
    show
      "val D I  $\varphi$ ((x,  $\alpha'$ ) := z) C  $\in$ : D (type_of C)  $\wedge$ 
      val D I  $\varphi$ ((x,  $\alpha'$ ) := z) C = val D I  $\varphi$ ((x,  $\alpha'$ ) := z) D'"
      by auto
    qed
  have "wff (type_of C) D'"
    using replacement_preserves_type replace_Abs.hyps replace_Abs.prem(2)
    replace_Abs.prem(3) replace_Abs.prem(4) wff_Abs_type_of by blast
  then have same_type:
    "abstract (D  $\alpha'$ ) (D (type_of C)) ( $\lambda z. \text{val D I } (\varphi((x, \alpha') := z)) \ D'$ ) =
    abstract (D  $\alpha'$ ) (D (type_of D')) ( $\lambda z. \text{val D I } (\varphi((x, \alpha') := z)) \ D'$ )"
    using type_of by presburger
  then show "val D I  $\varphi$  [ $\lambda x:\alpha'. C$ ] = val D I  $\varphi$  ([ $\lambda x:\alpha'. D'$ ])"
    using val_C_eql_val_D'_type same_type
    abstract_extensional[of _ _ _ " $\lambda x. \text{val D I } (\varphi((x, \alpha') := xa)) \ D'$ "]
    by (simp add: val_C_eql_val_D'_type same_type)

```

```

qed
qed
then show "valid_in_model D I C'"
  using assms(2) DI unfolding valid_in_model_def valid_general_def by auto
qed

theorem Fun_Tv_Tv_frame_subs_funspace:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  shows "D oo  $\subseteq$ : funspace (boolset) (boolset)"
  by (metis assms(1) general_model.elims(2) wf_frame_def wf_interp.simps)

theorem theorem_5402_a_axiom_1_variant:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  shows "satisfies D I  $\varphi$  axiom_1"
proof (cases " $(\varphi (''g'', oo)) \cdot \text{true} = \text{true} \wedge (\varphi (''g'', oo)) \cdot \text{false} = \text{true}$ ")
  case True
  then have val: "val D I  $\varphi ((g_{oo} \cdot T) \wedge (g_{oo} \cdot F)) = \text{true}$ "
    using assms lemma_5401_e_variant_2
    by (auto simp add: boolean_eq_true lemma_5401_c[OF assms(1,2)] lemma_5401_d[OF assms(1,2)])
  have " $\forall \psi. \text{asg\_into\_frame } \psi D \longrightarrow$ 
    agree_off_asg  $\psi \varphi ''x'' Tv \longrightarrow$ 
    satisfies D I  $\psi (g_{oo} \cdot x_o)$ "
  proof (rule; rule; rule)
    fix  $\psi$ 
    assume  $\psi$ : "asg_into_frame  $\psi D$ " "agree_off_asg  $\psi \varphi ''x'' Tv$ "
    then have " $\psi (''x'', Tv) = \text{true} \vee \psi (''x'', Tv) = \text{false}$ "
      using asg_into_interp_is_true_or_false assms
      by auto
    then show "satisfies D I  $\psi (g_{oo} \cdot x_o)$ "
      using True  $\psi$  unfolding agree_off_asg_def by auto
  qed
  then have "val D I  $\varphi ([\forall ''x'':Tv. (g_{oo} \cdot x_o)]) = \text{true}$ "
    using lemma_5401_g using assms by auto
  then show ?thesis
    unfolding axiom_1_def
    using lemma_5401_b[OF assms(1,2)] val by auto
next
  case False
  have " $\varphi (''g'', oo) \in: D oo$ "
    using assms
    by (simp add: asg_into_frame_def)
  then have 0: " $\varphi (''g'', oo) \in: \text{funspace } (D Tv) (D Tv)$ "
    using assms(1) assms(2) fun_sym_asg_to_funspace by blast

  from False have " $(\varphi (''g'', oo)) \cdot \text{true} \neq \text{true} \vee (\varphi (''g'', oo)) \cdot \text{false} \neq \text{true}$ "
    by auto
  then have " $\exists z. \varphi (''g'', oo) \cdot z = \text{false} \wedge z \in: D Tv$ "
  proof
    assume a: " $\varphi (''g'', oo) \cdot \text{true} \neq \text{true}$ "
    have " $\varphi (''g'', oo) \cdot \text{true} \in: \text{boolset}$ "
      by (metis "0" apply_abstract assms(1) boolset_def general_model.elims(2) in_funspace_abstract
        mem_two true_def wf_frame_def wf_interp.simps)
    from this a have " $\varphi (''g'', oo) \cdot \text{true} = \text{false} \wedge \text{true} \in: D Tv$ "
      using assms(1) wf_frame_def wf_interp.simps by auto
    then show " $\exists z. \varphi (''g'', oo) \cdot z = \text{false} \wedge z \in: D Tv$ "
      by auto
  next
    assume a: " $\varphi (''g'', oo) \cdot \text{false} \neq \text{true}$ "
    have " $\varphi (''g'', oo) \cdot \text{false} \in: \text{boolset}$ "
      by (metis "0" apply_abstract assms(1) boolset_def general_model.elims(2) in_funspace_abstract
        mem_two false_def wf_frame_def wf_interp.simps)

```



```

from this a have "φ (''g'', oo) · false = false ∧ false ∈: D Tv"
  using assms(1) wf_frame_def wf_interp.simps by auto
then show "∃z. φ (''g'', oo) · z = false ∧ z ∈: D Tv"
  by auto
qed
then obtain z where z_p: "φ (''g'', oo) · z = false ∧ z ∈: D Tv"
  by auto
have "boolean (satisfies D I φ (goo · T)
  ∧ satisfies D I φ (goo · F)) = false"
  using False
  by (smt boolean_def val.simps(1) val.simps(3) lemma_5401_c[OF assms(1,2)]
    lemma_5401_d[OF assms(1,2)])
then have 1: "val D I φ (
  (goo · T) ∧
  (goo · F)) = false"
  using lemma_5401_e_variant_2 assms by auto
have 3: "asg_into_frame (φ(''x'', Tv) := z) D ∧
  agree_off_asg (φ(''x'', Tv) := z) φ ''x'' Tv ∧
  φ (''g'', oo) · (φ(''x'', Tv) := z) (''x'', Tv) ≠ true"
  using z_p Pair_inject agree_off_asg_def2 asg_into_frame_fun_upd assms(2) true_neq_false by fastforce
then have 2: "val D I φ ([∀ ''x'':Tv. (goo · xo)] = false"
  using lemma_5401_g_variant_1 assms boolean_def by auto
then show ?thesis
  unfolding axiom_1_def using 1 2 lemma_5401_b_variant_2[OF assms(1,2)] by auto
qed

```

```

theorem theorem_5402_a_axiom_1: "valid_general axiom_1"
  using theorem_5402_a_axiom_1_variant unfolding valid_general_def valid_in_model_def by auto

```

```

theorem theorem_5402_a_axiom_2_variant:
  assumes "general_model D I"
  assumes "asg_into_interp φ D I"
  shows "satisfies D I φ (axiom_2 α)"
proof (cases "φ(''x'', α) = φ(''y'', α)")
case True
  have "val D I φ ((Var ''h'' (Tv ← α)) · (Var ''x'' α)) =
    (φ (''h'', (Tv ← α))) · φ (''x'', α)"
    using assms by auto
  also
  have "... = φ (''h'', (Tv ← α)) · φ (''y'', α)"
    using True by auto
  also
  have "... = val D I φ ((Var ''h'' (Tv ← α)) · (Var ''y'' α))"
    using assms by auto
  finally
  show ?thesis
    unfolding axiom_2_def
    using lemma_5401_f_variant_2 assms lemma_5401_b_variant_1[OF assms(1,2)] boolean_def by auto
next
case False
  have "asg_into_frame φ D"
    using assms(2) by blast
  moreover
  have "general_model D I"
    using assms(1) by blast
  ultimately
  have
    "boolean (satisfies D I φ [Var ''x'' α =α= Var ''y'' α] →
      satisfies D I φ
        [(Var ''h'' (Tv ← α) · Var ''x'' α) =Tv= Var ''h'' (Tv ← α) · Var ''y'' α]) =
      true"
    using boolean_eq_true lemma_5401_b by auto

```

```

then
show ?thesis
  using assms lemma_5401_f_variant_2 unfolding axiom_2_def by auto
qed

theorem theorem_5402_a_axiom_2: "valid_general (axiom_2  $\alpha$ )"
  using theorem_5402_a_axiom_2_variant unfolding valid_general_def valid_in_model_def by auto

theorem theorem_5402_a_axiom_3_variant:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  shows "satisfies D I  $\varphi$  (axiom_3  $\alpha$   $\beta$ )"
proof (cases " $\varphi$  (''f'',  $\alpha \Leftarrow \beta$ ) =  $\varphi$  (''g'',  $\alpha \Leftarrow \beta$ )")
case True
{
  fix  $\psi$ 
  assume agree: "agree_off_asg  $\psi$   $\varphi$  ''x''  $\beta$ "
  assume asg: "asg_into_interp  $\psi$  D I"
  have "val D I  $\psi$  ((Var ''f'' ( $\alpha \Leftarrow \beta$ ))  $\cdot$  (Var ''x''  $\beta$ )) =  $\psi$  (''f'',  $\alpha \Leftarrow \beta$ )  $\cdot$   $\psi$  (''x'',  $\beta$ )"
    by auto
  also
  have "... =  $\varphi$  (''f'',  $\alpha \Leftarrow \beta$ )  $\cdot$   $\psi$  (''x'',  $\beta$ )"
    using agree by auto
  also
  have "... =  $\varphi$  (''g'',  $\alpha \Leftarrow \beta$ )  $\cdot$   $\psi$  (''x'',  $\beta$ )"
    using True by auto
  also
  have "... =  $\psi$  (''g'',  $\alpha \Leftarrow \beta$ )  $\cdot$   $\psi$  (''x'',  $\beta$ )"
    using agree by auto
  also
  have "... = val D I  $\psi$  ((Var ''g'' ( $\alpha \Leftarrow \beta$ ))  $\cdot$  (Var ''x''  $\beta$ ))"
    by auto
  finally
  have
    "val D I  $\psi$ 
      ([((Var ''f'' ( $\alpha \Leftarrow \beta$ ))  $\cdot$  (Var ''x''  $\beta$ )) = $\alpha$  ((Var ''g'' ( $\alpha \Leftarrow \beta$ ))  $\cdot$  (Var ''x''  $\beta$ ))])
      = true"
    using lemma_5401_b_variant_1[OF assms(1)] assms agree asg boolean_eq_true by auto
}
then have "satisfies D I  $\varphi$ 
  ([ $\forall$  ''x'': $\beta$ . [(Var ''f'' ( $\alpha \Leftarrow \beta$ ))  $\cdot$  Var ''x''  $\beta$ ] = $\alpha$  Var ''g'' ( $\alpha \Leftarrow \beta$ )  $\cdot$  Var ''x''  $\beta$ ])]"
  using assms lemma_5401_g by force
moreover
have "satisfies D I  $\varphi$  [Var ''f'' ( $\alpha \Leftarrow \beta$ ) = $\alpha \Leftarrow \beta$  = Var ''g'' ( $\alpha \Leftarrow \beta$ )]"
  using True assms using lemma_5401_b_variant_2 wff_Var by auto
ultimately
show ?thesis
  using axiom_3_def lemma_5401_b_variant_2 assms by auto
next
case False
then have " $\exists z. z \in: D \beta \wedge \varphi$  (''f'',  $\alpha \Leftarrow \beta$ )  $\cdot z \neq \varphi$  (''g'',  $\alpha \Leftarrow \beta$ )  $\cdot z$ "
  using funspace_difference_witness[of " $\varphi$  (''f'',  $\alpha \Leftarrow \beta$ )" "D  $\beta$ " "D  $\alpha$ " " $\varphi$  (''g'',  $\alpha \Leftarrow \beta$ )"]
  assms(1,2) fun_sym_asg_to_funspace by blast
then obtain z where
  z $\beta$ : "z  $\in: D \beta$ " and
  z_neq: " $\varphi$  (''f'',  $\alpha \Leftarrow \beta$ )  $\cdot z \neq \varphi$  (''g'',  $\alpha \Leftarrow \beta$ )  $\cdot z$ "
  by auto
define  $\psi$  where " $\psi = (\varphi((''x'', \beta) := z))$ "
have agree: "agree_off_asg  $\psi$   $\varphi$  ''x''  $\beta$ "
  using  $\psi$ _def agree_off_asg_def2 by blast
have asg: "asg_into_interp  $\psi$  D I"
  using z $\beta$   $\psi$ _def asg_into_frame_fun_upd assms(2) by blast

```

```

have "val D I  $\psi$  ((Var ''f'' ( $\alpha \Leftarrow \beta$ ))  $\cdot$  (Var ''x''  $\beta$ )) =  $\psi$  (''f'',  $\alpha \Leftarrow \beta$ )  $\cdot$   $\psi$  (''x'',  $\beta$ )"
  by auto
moreover
have "... =  $\varphi$  (''f'',  $\alpha \Leftarrow \beta$ )  $\cdot$  z"
  by (simp add:  $\psi\_def$ )
moreover
have "...  $\neq$   $\varphi$  (''g'',  $\alpha \Leftarrow \beta$ )  $\cdot$  z"
  using False z_neq by blast
moreover
have " $\varphi$  (''g'',  $\alpha \Leftarrow \beta$ )  $\cdot$  z =  $\psi$  (''g'',  $\alpha \Leftarrow \beta$ )  $\cdot$   $\psi$  (''x'',  $\beta$ )"
  by (simp add:  $\psi\_def$ )
moreover
have "... = val D I  $\psi$  ((Var ''g'' ( $\alpha \Leftarrow \beta$ ))  $\cdot$  (Var ''x''  $\beta$ ))"
  by auto
ultimately
have
  "val D I  $\psi$ 
    (((Var ''f'' ( $\alpha \Leftarrow \beta$ ))  $\cdot$  (Var ''x''  $\beta$ )) = $\alpha$ = ((Var ''g'' ( $\alpha \Leftarrow \beta$ ))  $\cdot$  (Var ''x''  $\beta$ )))
    = false"
  by (metis asg assms(1) lemma_5401_b_variant_3 wff_App wff_Var)
have "val D I  $\varphi$ 
  ([ $\forall$  ''x'': $\beta$ . [(Var ''f'' ( $\alpha \Leftarrow \beta$ )  $\cdot$  Var ''x''  $\beta$ ] = $\alpha$ = Var ''g'' ( $\alpha \Leftarrow \beta$ )  $\cdot$  Var ''x''  $\beta$ ]) = false"
  by (smt (verit) <val D I  $\psi$  [(Var ''f'' ( $\alpha \Leftarrow \beta$ )  $\cdot$  Var ''x''  $\beta$ ] = $\alpha$ = Var ''g'' ( $\alpha \Leftarrow \beta$ )  $\cdot$  Var ''x''  $\beta$ ] =
false>
  agree asg assms(1,2) lemma_5401_g wff_App wff_Eql wff_Forall wff_Tv_is_true_or_false wff_Var)
moreover
have "val D I  $\varphi$  [Var ''f'' ( $\alpha \Leftarrow \beta$ ) = $\alpha$   $\Leftarrow$   $\beta$ = Var ''g'' ( $\alpha \Leftarrow \beta$ )] = false"
  using False assms(1,2) lemma_5401_b_variant_3 wff_Var by auto
ultimately show ?thesis
  using assms(1,2) axiom_3_def lemma_5401_b by auto
qed

```

```

theorem theorem_5402_a_axiom_3: "valid_general (axiom_3  $\alpha$   $\beta$ )"
  using theorem_5402_a_axiom_3_variant unfolding valid_general_def valid_in_model_def by auto

```

```

theorem theorem_5402_a_axiom_4_1_variant_cst:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "wff  $\alpha$  A"
  shows "satisfies D I  $\varphi$  (axiom_4_1_variant_cst x  $\alpha$  c  $\beta$  A)"
proof -
  let ? $\psi$  = " $\varphi$ ((x, $\alpha$ ):=val D I  $\varphi$  A)"
  have "val D I  $\varphi$  ([ $\lambda$ x: $\alpha$ . (Cst c  $\beta$ )]  $\cdot$  A) = val D I ? $\psi$  (Cst c  $\beta$ )"
    by (rule lemma_5401_a[of _ _ _ _  $\beta$ ]; use assms in auto)
  then have "val D I  $\varphi$  ([ $\lambda$ x: $\alpha$ . Cst c  $\beta$ ]  $\cdot$  A) = val D I  $\varphi$  (Cst c  $\beta$ )"
    by auto
  moreover
  have "wff  $\beta$  ([ $\lambda$ x: $\alpha$ . Cst c  $\beta$ ]  $\cdot$  A)"
    using assms by auto
  ultimately
  show ?thesis
    unfolding axiom_4_1_variant_cst_def
    using lemma_5401_b_variant_2[OF assms(1,2)] by auto
qed

```

```

theorem theorem_5402_a_axiom_4_1_variant_var:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "wff  $\alpha$  A"
  assumes "axiom_4_1_variant_var_side_condition x  $\alpha$  y  $\beta$  A"
  shows "satisfies D I  $\varphi$  (axiom_4_1_variant_var x  $\alpha$  y  $\beta$  A)"

```

```

proof -
  let ? $\psi$  = " $\varphi((x,\alpha):=val D I \varphi A)$ "
  have "val D I  $\varphi$  ( $[\lambda x:\alpha. (Var y \beta)] \cdot A$ ) = val D I ? $\psi$  (Var y  $\beta$ )"
    by (rule lemma_5401_a[of _ _ _ _  $\beta$ ], use assms in auto)
  then have "val D I  $\varphi$  ( $[\lambda x:\alpha. Var y \beta] \cdot A$ ) = val D I  $\varphi$  (Var y  $\beta$ )"
    using assms unfolding axiom_4_1_variant_var_side_condition_def by auto
  moreover
  have "wff  $\beta$  ( $[\lambda x:\alpha. Var y \beta] \cdot A$ )"
    using assms by auto
  moreover
  have "wff  $\beta$  (Var y  $\beta$ )"
    using assms by auto
  ultimately
  show ?thesis
    unfolding axiom_4_1_variant_var_def
    using lemma_5401_b_variant_2[OF assms(1,2)] by auto
qed

```

```

theorem theorem_5402_a_axiom_4_1:
  assumes "asg_into_interp  $\varphi D I$ "
  assumes "general_model D I"
  assumes "axiom_4_1_side_condition x  $\alpha$  y  $\beta A$ "
  assumes "wff  $\alpha A$ "
  shows "satisfies D I  $\varphi$  (axiom_4_1 x  $\alpha$  y  $\beta A$ )"
  using assms theorem_5402_a_axiom_4_1_variant_cst theorem_5402_a_axiom_4_1_variant_var
  unfolding axiom_4_1_variant_cst_def axiom_4_1_variant_var_side_condition_def
    axiom_4_1_side_condition_def axiom_4_1_variant_var_def
    axiom_4_1_def by auto

```

```

theorem theorem_5402_a_axiom_4_2:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi D I$ "
  assumes "wff  $\alpha A$ "
  shows "satisfies D I  $\varphi$  (axiom_4_2 x  $\alpha A$ )"

```

```

proof -
  let ? $\psi$  = " $\varphi((x,\alpha):=val D I \varphi A)$ "
  have "wff  $\alpha$  ( $[\lambda x:\alpha. Var x \alpha] \cdot A$ )"
    using assms by auto
  moreover
  have "wff  $\alpha A$ "
    using assms by auto
  moreover
  have "val D I  $\varphi$  ( $[\lambda x:\alpha. Var x \alpha] \cdot A$ ) = val D I  $\varphi A$ "
    using lemma_5401_a[of _ _ _ _  $\alpha$  _] assms by auto
  ultimately
  show ?thesis
    unfolding axiom_4_2_def by (rule lemma_5401_b_variant_2[OF assms(1,2)])
qed

```

```

theorem theorem_5402_a_axiom_4_3:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi D I$ "
  assumes "wff  $\alpha A$ "
  assumes "wff ( $\beta \Leftarrow \gamma$ ) B"
  assumes "wff  $\gamma C$ "
  shows "satisfies D I  $\varphi$  (axiom_4_3 x  $\alpha B \beta \gamma C A$ )"

```

```

proof -
  let ? $\psi$  = " $\varphi((x,\alpha):=val D I \varphi A)$ "
  let ?E = "B  $\cdot$  C"

  have "val D I  $\varphi$  (LHS (axiom_4_3 x  $\alpha B \beta \gamma C A$ )) = val D I ? $\psi$  ?E"

```

```

    by (metis LHS_def2 assms(3) assms(4) assms(5) axiom_4_3_def lemma_5401_a[OF assms(1,2)] wff_App)
  moreover
  have "... = val D I ?ψ (B · C)"
    by simp
  moreover
  have "... = (val D I ?ψ B) · val D I ?ψ C"
    by simp
  moreover
  have "... = (val D I φ ([λx:α. B] · A)) · val D I φ (App [λx :α. C] A)"
    by (metis assms(3) assms(4) assms(5) lemma_5401_a[OF assms(1,2)])
  moreover
  have "... = val D I φ (RHS (axiom_4_3 x α B β γ C A))"
    unfolding axiom_4_3_def by auto
  ultimately
  have "val D I φ (LHS (axiom_4_3 x α B β γ C A)) = val D I φ (RHS (axiom_4_3 x α B β γ C A))"
    by auto
  then have "val D I φ ([λx:α. B · C] · A) = val D I φ ([λx:α. B] · A · ([λx:α. C] · A))"
    unfolding axiom_4_3_def by auto
  moreover
  have "wff β ([λx:α. B · C] · A)"
    using assms by auto
  moreover
  have "wff β ([λx:α. B] · A · ([λx:α. C] · A))"
    using assms by auto
  ultimately
  show ?thesis
    unfolding axiom_4_3_def using lemma_5401_b_variant_2[OF assms(1,2)] by auto
qed

```

lemma lemma\_to\_help\_with\_theorem\_5402\_a\_axiom\_4\_4:

```

  assumes lambda_eq_lambda_lambda:
    "∧z. z ∈: D γ ⇒ val D I ψ [λy:γ. B] · z = val D I φ [λy:γ. [λx:α. B] · A] · z"
  assumes ψ_eql: "ψ = φ((x, α) := val D I φ A)"
  assumes "asg_into_frame φ D"
  assumes "general_model D I"
  assumes "axiom_4_4_side_condition x α y γ B δ A"
  assumes "wff α A"
  assumes "wff δ B"
  shows "val D I ψ [λy:γ. B] = val D I φ [λy:γ. [λx:α. B] · A]"
proof -
  {
    fix e
    assume e_in_D: "e ∈: D γ"
    then have "val D I (ψ((y, γ) := e)) B ∈: D (type_of B)"
      using asg_into_frame_fun_upd assms(3,4,6,7) ψ_eql by auto
    then have val_lambda_B: "val D I ψ [λy:γ. B] · e = val D I (ψ((y, γ) := e)) B"
      using e_in_D by auto
    have
      "val D I φ [λy:γ. [λx:α. B] · A] · e =
      abstract (D α) (D (type_of B))
      (λz. val D I (φ((y, γ) := e, (x, α) := z)) B) · val D I (φ((y, γ) := e)) A"
      using apply_abstract e_in_D asg_into_frame_fun_upd assms(3,4,6,7) by auto
    then have "val D I (ψ((y, γ) := e)) B =
      abstract (D α) (D (type_of B))
      (λz. val D I (φ((y, γ) := e, (x, α) := z)) B) · val D I (φ((y, γ) := e)) A"
      using val_lambda_B lambda_eq_lambda_lambda e_in_D by metis
  }
  note val_eql_abstract = this

```

have

```

  "∀e. e ∈: D γ →
  val D I (ψ((y, γ) := e)) B ∈: D (type_of B) ∧
  val D I (ψ((y, γ) := e)) B =
  abstract (D α) (D (type_of B))

```

```

      (λza. val D I (φ((y, γ) := e, (x, α) := za)) B) · val D I (φ((y, γ) := e)) A"
using asg_into_frame_fun_upd assms(3,4,6,7) ψ_eq1 val_eq1_abstract by auto
then have
  "abstract (D γ) (D (type_of B)) (λz. val D I (ψ((y, γ) := z)) B) =
  abstract (D γ) (D (type_of B))
  (λz. abstract (D α) (D (type_of B))
  (λza. val D I (φ((y, γ) := z, (x, α) := za)) B) · val D I (φ((y, γ) := z)) A)"
  by (rule abstract_extensional)
then show ?thesis
  by auto
qed

```

```

theorem theorem_5402_a_axiom_4_4:
  assumes "general_model D I"
  assumes "asg_into_interp φ D I"
  assumes "axiom_4_4_side_condition x α y γ B δ A"
  assumes "wff α A"
  assumes "wff δ B"
  shows "satisfies D I φ (axiom_4_4 x α y γ B δ A)"
proof -
  define ψ where "ψ = φ((x,α):=val D I φ A)"
  let ?E = "[λy:γ. B]"
  have fr: "(y, γ) ∉ vars A"
    using assms(3) axiom_4_4_side_condition_def by blast
  {
    fix z
    assume z_in_D: "z ∈: D γ"
    define φ' where "φ' = φ((y,γ) := z)"
    have "asg_into_frame φ' D"
      using assms z_in_D unfolding asg_into_frame_def φ'_def by auto
    moreover
    have "∀ (x, α) ∈ vars A. agree_on_asg φ φ' x α"
      using fr unfolding φ'_def by auto
    ultimately
    have "val D I φ A = val D I φ' A"
      using prop_5400[OF assms(1), of _ _ α] assms(2) assms(4) frees_subset_vars by blast
    then have Az: "φ'((x,α):=(val D I φ' A)) = ψ((y,γ):=z)"
      using assms(3) unfolding axiom_4_4_side_condition_def
      by (simp add: fun_upd_twist φ'_def ψ_def)
    then have "abstract (D γ) (D (type_of B)) (λz. val D I (ψ((y, γ) := z)) B) · z =
      val D I (ψ((y, γ) := z)) B"
      using apply_abstract_matchable assms(1,2,4,5) type_of asg_into_frame_fun_upd
      general_model.elims(2) z_in_D by (metis φ'_def)
    then have "(val D I ψ ?E) · z = (val D I (ψ((y,γ):=z)) B)"
      by auto
    moreover
    have "... = val D I φ' ([λx:α. B] · A)"
      using assms(1,2,4,5) asg_into_frame_fun_upd lemma_5401_a z_in_D
      by (metis Az φ'_def)
    moreover
    have "... = val D I φ [λy:γ. [λx:α. B] · A] · z"
  }
proof -
  have valA: "val D I φ' A ∈: D α"
    using φ'_def asg_into_frame_fun_upd z_in_D assms by simp
  have valB: "val D I (φ'((x, α) := val D I φ' A)) B ∈: D (type_of B)"
    using asg_into_frame_fun_upd z_in_D assms by (simp add: Az ψ_def)
  have valA': "val D I (φ((y, γ) := z)) A ∈: D α"
    using z_in_D assms asg_into_frame_fun_upd valA unfolding ψ_def φ'_def
    by blast
  have valB':
    "val D I (φ((y, γ) := z, (x, α) := val D I (φ((y, γ) := z)) A)) B
    ∈: D (type_of B)"
    using asg_into_frame_fun_upd z_in_D assms valB φ'_def by blast

```

```

have
  "val D I ( $\varphi'((x, \alpha) := \text{val D I } \varphi' A)$ ) B =
    val D I ( $\varphi((y, \gamma) := z, (x, \alpha) := \text{val D I } (\varphi((y, \gamma) := z)) A)$ ) B"
  unfolding  $\psi\_def$   $\varphi'\_def$  by (metis apply_abstract asg_into_frame_fun_upd)
then have valB_eql_abs:
  "val D I ( $\varphi'((x, \alpha) := \text{val D I } \varphi' A)$ ) B =
    abstract (D  $\alpha$ ) (D (type_of B))
      ( $\lambda z a. \text{val D I } (\varphi((y, \gamma) := z, (x, \alpha) := za)) B$ )  $\cdot$  val D I ( $\varphi((y, \gamma) := z)$ ) A"
  using valA' valB' by auto
then have "abstract (D  $\alpha$ ) (D (type_of B))
  ( $\lambda z a. \text{val D I } (\varphi((y, \gamma) := z, (x, \alpha) := za)) B$ )  $\cdot$  val D I ( $\varphi((y, \gamma) := z)$ ) A
   $\in$ : D (type_of B)"
  using valB assms z_in_D by auto
then have
  "val D I ( $\varphi'((x, \alpha) := \text{val D I } \varphi' A)$ ) B =
    abstract (D  $\gamma$ ) (D (type_of B))
      ( $\lambda z. \text{abstract (D } \alpha) (D (\text{type\_of B}))$ )
      ( $\lambda z a. \text{val D I } (\varphi((y, \gamma) := z, (x, \alpha) := za)) B$ )  $\cdot$  val D I ( $\varphi((y, \gamma) := z)$ ) A  $\cdot$  z"
  using z_in_D valB_eql_abs by auto
then show "val D I  $\varphi' ([\lambda x:\alpha. B] \cdot A) = \text{val D I } \varphi [\lambda y:\gamma. [\lambda x:\alpha. B] \cdot A] \cdot z"$ 
  using valA valB by auto
qed
ultimately
have "val D I  $\psi [\lambda y:\gamma. B] \cdot z = \text{val D I } \varphi [\lambda y:\gamma. [\lambda x:\alpha. B] \cdot A] \cdot z"$ 
  by simp
}
note lambda_eql_lambda_lambda = this
have equal_funs: "val D I  $\psi ?E = \text{val D I } \varphi ([\lambda y:\gamma. ([\lambda x:\alpha. B]) \cdot A])"$ 
  using lambda_eql_lambda_lambda  $\psi\_def$  assms lemma_to_help_with_theorem_5402_a_axiom_4_4 by metis
have "val D I  $\varphi ([\lambda x:\alpha. [\lambda y:\gamma. B]] \cdot A) = \text{val D I } \varphi [\lambda y:\gamma. [\lambda x:\alpha. B] \cdot A]"$ 
  using equal_funs by (metis  $\psi\_def$  assms(1,2,4,5) lemma_5401_a wff_Abs)
then have "satisfies D I  $\varphi ([[\lambda x:\alpha. [\lambda y:\gamma. B]] \cdot A) = \delta \Leftarrow \gamma = [\lambda y:\gamma. [\lambda x:\alpha. B] \cdot A]"$ 
  using lemma_5401_b[OF assms(1,2)] assms by auto
then show ?thesis
  unfolding axiom_4_4_def .
qed

theorem theorem_5402_a_axiom_4_5:
  assumes "general_model D I"
  assumes "asg_into_interp  $\varphi$  D I"
  assumes "wff  $\alpha$  A"
  assumes "wff  $\delta$  B"
  shows "satisfies D I  $\varphi$  (axiom_4_5 x  $\alpha$  B  $\delta$  A)"
proof -
  define  $\psi$  where " $\psi = \varphi((x, \alpha) := \text{val D I } \varphi A)$ "
  let ?E = " $[\lambda x:\alpha. B]$ "
  {
    assume val: " $\forall \varphi. \text{asg\_into\_frame } \varphi D \longrightarrow (\forall A \alpha. \text{wff } \alpha A \longrightarrow \text{val D I } \varphi A \in: D \alpha)"$ "
    assume asg: "asg_into_frame  $\varphi$  D"
    assume wffA: "wff  $\alpha$  A"
    assume wffB: "wff  $\delta$  B"
    have valA: "val D I  $\varphi A \in: D \alpha$ "
      using val asg wffA by blast
    have " $\forall t$  cs. val D I  $\varphi [\lambda cs:t. B] \in: D (\delta \Leftarrow t)"$ "
      using val asg wffB wff_Abs by blast
    then have "abstract (D  $\alpha$ ) (D ( $\delta \Leftarrow \alpha$ ))
      ( $\lambda u. \text{abstract (D } \alpha) (D \delta) (\lambda u. \text{val D I } (\varphi((x, \alpha) := u)) B)$ )  $\cdot$  val D I  $\varphi A =$ 
      abstract (D  $\alpha$ ) (D  $\delta) (\lambda u. \text{val D I } (\varphi((x, \alpha) := u)) B)"$ 
      using valA wffB by simp
  }
  note abstract_eql = this

```

```

have "val D I  $\psi$  ?E = val D I  $\varphi$  ?E"
  using prop_5400[OF assms(1), of _ _ " $\delta \Leftarrow \alpha$ "]  $\psi$ _def assms(2) by auto
then show ?thesis
  unfolding axiom_4_5_def using lemma_5401_b[OF assms(1,2)] assms abstract_eq1 by auto
qed

```

theorem theorem\_5402\_a\_axiom\_5:

```

assumes "general_model D I"
assumes "asg_into_interp  $\varphi$  D I"
shows "satisfies D I  $\varphi$  (axiom_5)"
proof -
  have iden_eq1: "iden (D Ind) · I ''y'' Ind = one_elem_fun (I ''y'' Ind) (D Ind)"
  proof -
    have "I ''y'' Ind  $\in$ : D Ind"
      using assms unfolding general_model.simps wf_interp.simps[simplified] iden_def one_elem_fun_def
      by auto
    moreover
    have "abstract (D Ind) boolset ( $\lambda y$ . boolean (I ''y'' Ind = y))  $\in$ : funspace (D Ind) boolset"
      using boolean_in_boolset by auto
    ultimately
    show ?thesis
      unfolding iden_def one_elem_fun_def by auto
  qed

```

```

have "val D I  $\varphi$  ( $\iota \cdot ((Q (Tv \Leftarrow Ind \Leftarrow Ind)) \cdot y_i)) =$ 
  val D I  $\varphi$   $\iota \cdot$  val D I  $\varphi$  ( $(Q (Tv \Leftarrow Ind \Leftarrow Ind)) \cdot y_i$ )"
  by auto
moreover
have "... = val D I  $\varphi$   $y_i$ "
  using assms iden_eq1 unfolding general_model.simps wf_interp.simps[simplified] by auto
ultimately
show ?thesis
  unfolding axiom_5_def using lemma_5401_b[OF assms(1,2)] by auto
qed

```

lemma theorem\_isa\_Tv:

```

assumes "theorem A"
shows "wff Tv A"
using assms proof (induction)
  case (by_axiom A)
  then show ?case
  proof (induction)
    case by_axiom_1
    then show ?case
      unfolding axiom_1_def by auto
  next
    case (by_axiom_2  $\alpha$ )
    then show ?case
      unfolding axiom_2_def by auto
  next
    case (by_axiom_3  $\alpha$   $\beta$ )
    then show ?case
      unfolding axiom_3_def by auto
  next
    case (by_axiom_4_1  $\alpha$  A  $\beta$  B x)
    then show ?case
      unfolding axiom_4_1_def by auto
  next
    case (by_axiom_4_2  $\alpha$  A x)
    then show ?case
      unfolding axiom_4_2_def by auto
  next
    case (by_axiom_4_3  $\alpha$  A  $\beta$   $\gamma$  B C x)

```



```

    then show ?case
      unfolding axiom_4_3_def by auto
  next
    case (by_axiom_4_4  $\alpha$  A  $\delta$  B x y  $\gamma$ )
    then show ?case
      unfolding axiom_4_4_def by auto
  next
    case (by_axiom_4_5  $\alpha$  A  $\delta$  B x)
    then show ?case
      unfolding axiom_4_5_def by auto
  next
    case by_axiom_5
    then show ?case
      unfolding axiom_5_def by auto
  qed
next
case (by_rule_R A B C)
then show ?case
  by (smt replacement_preserves_type rule_R.cases wff_Eql_iff)
qed

```

```

theorem theorem_5402_a_general:
  assumes "theorem A"
  shows "valid_general A"
  using assms
proof (induction)
  case (by_axiom A)
  then show ?case
  proof (induction)
    case by_axiom_1
    then show ?case
      using theorem_5402_a_axiom_1 by auto
  next
    case (by_axiom_2  $\alpha$ )
    then show ?case
      using theorem_5402_a_axiom_2 by auto
  next
    case (by_axiom_3  $\alpha$   $\beta$ )
    then show ?case
      using theorem_5402_a_axiom_3 by auto
  next
    case (by_axiom_4_1  $\alpha$  A  $\beta$  B x)
    then show ?case
      using theorem_5402_a_axiom_4_1
      unfolding valid_general_def valid_in_model_def by auto
  next
    case (by_axiom_4_2  $\alpha$  A x)
    then show ?case
      using theorem_5402_a_axiom_4_2
      unfolding valid_general_def valid_in_model_def by auto
  next
    case (by_axiom_4_3  $\alpha$  A  $\beta$   $\gamma$  B C x)
    then show ?case
      using theorem_5402_a_axiom_4_3
      unfolding valid_general_def valid_in_model_def by auto
  next
    case (by_axiom_4_4  $\alpha$  A  $\delta$  B x y  $\gamma$ )
    then show ?case
      using theorem_5402_a_axiom_4_4
      unfolding valid_general_def valid_in_model_def by auto
  next
    case (by_axiom_4_5  $\alpha$  A  $\delta$  B x)
    then show ?case

```

```

    using theorem_5402_a_axiom_4_5
    unfolding valid_general_def valid_in_model_def by auto
next
  case by_axiom_5
  then show ?case
    using theorem_5402_a_axiom_5
    unfolding valid_general_def valid_in_model_def by auto
qed
next
  case (by_rule_R C AB C')
  then have C_isa_Tv: "wff Tv C"
    using theorem_isa_Tv by blast
  have "∃A B β. AB = [A =β= B] ∧ wff β A ∧ wff β B"
    using by_rule_R rule_R.simps theorem_isa_Tv by fastforce
  then obtain A B β where A_B_β_p: "AB = [A =β= B] ∧ wff β A ∧ wff β B"
    by blast
  then have R: "rule_R C [A =β= B] C'"
    using by_rule_R by auto
  then have "replacement A B C C'"
    using Eq1_def rule_R.cases by fastforce
  show ?case
    using theorem_5402_a_rule_R[of A B β C C' Tv] by_rule_R.IH R
    A_B_β_p C_isa_Tv by auto
qed

theorem theorem_5402_a_standard:
  assumes "theorem A"
  shows "valid_standard A"
  using theorem_5402_a_general assms standard_model_is_general_model valid_general_def
  valid_standard_def by blast

end

end

```

## References

- [AM23] Oskar Abrahamsson and Magnus O. Myreen. Fast, verified computation for Candle. In Adam Naumowicz and René Thiemann, editors, *14th International Conference on Interactive Theorem Proving, ITP 2023, July 31 to August 4, 2023, Białystok, Poland*, volume 268 of *LIPICs*, pages 4:1–4:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023.
- [AMKS22] Oskar Abrahamsson, Magnus O. Myreen, Ramana Kumar, and Thomas Sewell. Candle: A verified implementation of HOL Light. In June Andronick and Leonardo de Moura, editors, *13th International Conference on Interactive Theorem Proving, ITP 2022, August 7-10, 2022, Haifa, Israel*, volume 237 of *LIPICs*, pages 3:1–3:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.
- [And63] Peter Andrews. A reduction of the axioms for the theory of propositional types. *Fundamenta Mathematicae*, 52:345–350, 1963.
- [And72] Peter B Andrews. General models and extensionality. *The Journal of Symbolic Logic*, 37(2):395–397, 1972.
- [And13] Peter B. Andrews. *An introduction to mathematical logic and type theory: to truth through proof*, volume 27 of *Applied Logic Series*. Springer Science & Business Media, 2nd edition, 2013.
- [Art02] Rob Arthan. HOL formalised: Deductive system, 1993, revised 2002. <http://www.lemma-one.com/ProofPower/specs/specs.html>.
- [Art14a] Rob Arthan. HOL formalised: Language and overview, 1993, revised 2014. <http://www.lemma-one.com/ProofPower/specs/specs.html>.
- [Art14b] Rob Arthan. HOL formalised: Semantics, 1993, revised 2014. <http://www.lemma-one.com/ProofPower/specs/specs.html>.

- [Bar96a] Bruno Barras. Coq en Coq. Research Report RR-3026, INRIA, 1996. Projet COQ, <https://inria.hal.science/inria-00073667>.
- [Bar96b] Bruno Barras. Verification of the interface of a small proof system in Coq. In Eduardo Giménez and Christine Paulin-Mohring, editors, *Types for Proofs and Programs, International Workshop TYPES'96, Aussois, France, December 15-19, 1996, Selected Papers*, volume 1512 of *Lecture Notes in Computer Science*, pages 28–45. Springer, 1996.
- [Bar97] Bruno Barras. coq-in-coq. In *coq-contribs*, 1997. <https://github.com/coq-contribs/coq-in-coq>.
- [BW96] Bruno Barras and Benjamin Werner. Coq in Coq (manuscript). Technical report, 1996. <http://www.lix.polytechnique.fr/Labo/Bruno.Barras/publi/coqincoq.pdf>.
- [Chu40] Alonzo Church. A formulation of the simple theory of types. *The journal of symbolic logic*, 5(2):56–68, 1940.
- [Día23] Javier Díaz. Metatheory of Q0. *Archive of Formal Proofs*, November 2023. [https://isa-afp.org/entries/Q0\\_Metatheory.html](https://isa-afp.org/entries/Q0_Metatheory.html), Formal proof development.
- [Har06] John Harrison. Towards self-verification of HOL Light. In Ulrich Furbach and Natarajan Shankar, editors, *Automated Reasoning, Third International Joint Conference, IJCAR 2006, Seattle, WA, USA, August 17-20, 2006, Proceedings*, volume 4130 of *Lecture Notes in Computer Science*, pages 177–191. Springer, 2006.
- [Hen50] Leon Henkin. Completeness in the theory of types. *The Journal of Symbolic Logic*, 15(2):81–91, 1950.
- [Hen63] Leon Henkin. A theory of propositional types. *Fundamenta Mathematicae*, 52:323–344, 1963.
- [KAMO14] Ramana Kumar, Rob Arthan, Magnus O. Myreen, and Scott Owens. HOL with definitions: Semantics, soundness, and a verified implementation. In Gerwin Klein and Ruben Gamboa, editors, *Interactive Theorem Proving - 5th International Conference, ITP 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 14-17, 2014. Proceedings*, volume 8558 of *Lecture Notes in Computer Science*, pages 308–324. Springer, 2014.
- [KAMO16] Ramana Kumar, Rob Arthan, Magnus O. Myreen, and Scott Owens. Self-formalisation of higher-order logic - semantics, soundness, and a verified implementation. *J. Autom. Reason.*, 56(3):221–259, 2016.
- [KK22] Mark Koch and Dominik Kirst. Undecidability, incompleteness, and completeness of second-order logic in coq. In Andrei Popescu and Steve Zdancewic, editors, *CPP '22: 11th ACM SIGPLAN International Conference on Certified Programs and Proofs, Philadelphia, PA, USA, January 17 - 18, 2022*, pages 274–290. ACM, 2022.
- [NR21a] Tobias Nipkow and Simon Roßkopf. Isabelle’s metalogic: Formalization and proof checker. In André Platzer and Geoff Sutcliffe, editors, *Automated Deduction - CADE 28 - 28th International Conference on Automated Deduction, Virtual Event, July 12-15, 2021, Proceedings*, volume 12699 of *Lecture Notes in Computer Science*, pages 93–110. Springer, 2021.
- [NR21b] Tobias Nipkow and Simon Roßkopf. Isabelle’s metalogic: Formalization and proof checker. *Archive of Formal Proofs*, April 2021. [https://isa-afp.org/entries/Metalogic\\_ProofChecker.html](https://isa-afp.org/entries/Metalogic_ProofChecker.html), Formal proof development.
- [Obu06] Steven Obua. Partizan games in Isabelle/HOLZF. In Kamel Barkaoui, Ana Cavalcanti, and Antonio Cerone, editors, *Theoretical Aspects of Computing - ICTAC 2006, Third International Colloquium, Tunis, Tunisia, November 20-24, 2006, Proceedings*, volume 4281 of *Lecture Notes in Computer Science*, pages 272–286. Springer, 2006.
- [Pau19] Lawrence C. Paulson. Zermelo Fraenkel set theory in higher-order logic. *Archive of Formal Proofs*, October 2019. [https://isa-afp.org/entries/ZFC\\_in\\_HOL.html](https://isa-afp.org/entries/ZFC_in_HOL.html), Formal proof development.
- [RN23] Simon Roßkopf and Tobias Nipkow. A formalization and proof checker for Isabelle’s metalogic. *J. Autom. Reason.*, 67(1):1, 2023.
- [Rus08] Bertrand Russell. Mathematical logic as based on the theory of types. *American journal of mathematics*, 30(3):222–262, 1908.

- [SBF<sup>+</sup>20] Matthieu Sozeau, Simon Boulter, Yannick Forster, Nicolas Tabareau, and Théo Winterhalter. Coq Coq correct! verification of type checking and erasure for Coq, in Coq. *Proc. ACM Program. Lang.*, 4(POPL):8:1–8:28, 2020.
- [Sch23] Anders Schlichtkrull. Q0. *IsaFoL*, Jan 4th 2022 - Nov 2023. Now at GitHub <https://github.com/IsaFoL/IsaFoL/tree/master/Q0> but formerly at BitBucket <https://bitbucket.org/isafol/isafol/src/master/Q0/>. Formal proof development.
- [WR13] Alfred North Whitehead and Bertrand Russell. *Principia Mathematica*. Cambridge University Press, Cambridge England, 1913. 3 volumes; first edition 1913, second edition 1927.